Lineare Algebra

Mitschrift von www.kuertz.name

Hinweis: Dies ist **kein offizielles Script**, sondern nur eine private Mitschrift. Die Mitschriften sind teweilse **unvollständig, falsch oder inaktuell**, da sie aus dem Zeitraum 2001–2005 stammen. Falls jemand einen Fehler entdeckt, so freue ich mich dennoch über einen kurzen Hinweis per E-Mail – vielen Dank!

Klaas Ole Kürtz (klaasole@kuertz.net)

Inhaltsverzeichnis

1 Grundlagen

1.1 Mengen

- Menge, Teilmenge, Element, $\mathbb{N} \subseteq \mathbb{N}_0 \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, leere/nichtleere Mengen, endliche/unendliche Mengen, Betrag/Mächtigkeit
- *Potenzmenge*: Menge aller Teilmengen
  - $\mathcal{P}(A) := \{U | U \subseteq M\}$
  - $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$
  - $|\mathcal{P}(M)| = 2^{|M|}$
- Bildung neuer Mengen
  - Sei I eine *Indexmenge* und seien M_i, $i \in I$, Mengen
  - *Vereinigung:* $\bigcup\limits_{i \in I} := \{x | x \in M_i \text{ für ein } i \in I\} = M_1 \cup M_2 \cup \ldots$
  - *Durchschnitt:* $\bigcap\limits_{i \in I} := \{x | x \in M_i \text{ für alle } i \in I\} = M_1 \cap M_2 \cap \ldots$
  - *kartes. Produkt:* $\bigotimes\limits_{i \in I} := \{(x_1, \ldots, x_r) | x_i \in M_i, i \in I\} = M_1 \times M_2 \times \ldots$
  - *Differenz:* $M \setminus N := x | x \in M \wedge x \notin N$, eine Differenzmenge $M \setminus N$ heißt *Komplement* von N in M, falls $N \subseteq M$.
  - Regeln von *de Morgan*:
    * Sei $\mathcal{N} \subseteq \mathcal{P}(M)$.
    * kurzfristige Sondernotation: $\overline{N} := M \setminus N$
    * $M \setminus \bigcap\limits_{N \in \mathcal{N}} N = \bigcup\limits_{N \in \mathcal{N}} (M \setminus N) \Leftrightarrow \overline{\bigcap\limits_{N \in \mathcal{N}} N} = \bigcup\limits_{N \in \mathcal{N}} \overline{N}$
    * $M \setminus \bigcup\limits_{N \in \mathcal{N}} N = \bigcap\limits_{N \in \mathcal{N}} (M \setminus N) \Leftrightarrow \overline{\bigcup\limits_{N \in \mathcal{N}} N} = \bigcap\limits_{N \in \mathcal{N}} \overline{N}$
    * $A \subseteq B \Rightarrow \overline{B} \subseteq \overline{A}$
- Eine (Klasseneinteilung) ist eine vollständige Aufteilung einer Menge in Teilmengen ohne Schnittmengen. Wenn für $\mathcal{N} \subseteq \mathcal{P}(M)$ gilt: $\bigcup\limits_{N \in \mathcal{N}} N = M \wedge \bigcap\limits_{N \in \mathcal{N}} N = \emptyset$, so ist $\mathcal{N}$ eine Partition von M.

1.2 Relationen

Sei M eine Menge. Sei σ eine Relation auf M. Seien $x, y, z \in M$.

- Eigenschaften von Relationen
  - Reflexivität: $x\sigma x$
  - Symmetrie: $x\sigma y \Leftrightarrow y\sigma x$
  - Anti-Symmetrie: $x\sigma y\sigma x \Leftrightarrow x = y$
  - Transitivität: $x\sigma y\sigma z \Leftrightarrow x\sigma z$

RSAT Die *Gleichheit* ist eine Relation, die alle Eigenschaften erfüllt.

RST Eine Relation, die reflexiv, symmetrisch und transitiv ist, heißt *Äquivalenzrelation* (z.B. $\backsim$, siehe 1.2.1).

RAT Eine Relation, die reflexiv, anti-symmetrisch und transitiv ist, heißt *Ordnungsrelation* (z.B. $\leq, \geq, \subseteq$)

T Relationen können rein transitiv sein (z.B. $<, >, \subset$).

1.2.1 Eigenschaft von Äquivalenzrelationen

Definition einer Relation: $x \backsim y :\Leftrightarrow (x, y) \in A$ mit $A \subseteq M \times M$.
Die zugehörige Äquivalenzklasse: $\tilde{x} := \{y \in M | x \backsim y\}$.
Es gilt für alle $x, y \in M$:

(a) $x \in \tilde{x}$

(b) $M = \bigcup\limits_{z \in M} \tilde{z}$

(c) $a \backsim b$ für alle $a, b \in \tilde{x}$

(d) $\tilde{x} = \tilde{y} \lor \tilde{x} \cap \tilde{y} = \emptyset$

Beweise:

(a) $x \backsim x \Rightarrow x \in \tilde{x}$

(b) $\bigcup\limits_{z \in M} \tilde{z} \subseteq M$
$\land M \subseteq \bigcup\limits_{z \in M} \tilde{z}$
$\Rightarrow M = \bigcup\limits_{z \in M} \tilde{z}$

(c) $a \in \tilde{x} \Rightarrow x \backsim a$
$\wedge\, b \in \tilde{x} \Rightarrow x \backsim b$
$\wedge\, x \backsim a \Rightarrow a \backsim x$
$\Rightarrow a \backsim x \wedge x \backsim b \Rightarrow a \backsim b$

(d) Entweder gibt es kein Element aus $\tilde{x}$, das auch in $\tilde{y}$ enthalten ist $\Rightarrow \tilde{x} \cap \tilde{y} = \emptyset$ (1). Andernfalls gibt es ein Element $a \in \tilde{x}$, für das dann gilt: $x \backsim a \wedge a \backsim \tilde{y} \Rightarrow x\tilde{y}$. Daraus folgt: $b \in \tilde{x} \Rightarrow b \backsim x \wedge x \backsim y \Rightarrow b \backsim y \Rightarrow b \in \tilde{y}$ und $c \in \tilde{y} \Rightarrow c \backsim y \wedge y \backsim x \Rightarrow c \backsim x \Rightarrow c \in \tilde{x}$. Da alle Elemente aus $\tilde{x}$ auch in $\tilde{y}$ enthalten sind und umgekehrt, gilt $\tilde{x} = \tilde{y}$ (2). Aus (1) und (2) folgt: $\tilde{x} = \tilde{y} \vee \tilde{x} \cap \tilde{y} = \emptyset$

Beispiele für/gegen Äquivalenzrelationen:

- Ist $A = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} | p | x - y\}$ eine Äquivalenzmenge?
  - Reflexivität: ja, da $x - x = 0$ immer durch p teilbar ist.
  - Symmetrie: ja, da $(x - y) = -(y - x)$ gilt, d.h. falls $(x - y)$ durch p teilbar ist, ist auch $(y - x)$ teilbar.
  - Transitivität: $(x - y)$ ist teilbar, $(y - z)$ auch, d.h. deren Summe auch: $(x - y) + (y - z) = (x - z)$.

  $\Rightarrow$ A ist eine Äquivalenzmenge!

- E ist die Menge aller endlichen Teilmengen von $\mathbb{Z}$. Ist $A \subseteq E \times E; A := \{(x, y) \in E \times E | |x| = |y|\}$ eine Äquivalenzmenge?
  - Reflexivität: ja, da $|x| = |y|$.
  - Symmetrie: ja, da $|x| = |y| \Leftrightarrow |y| = |z|$.
  - Transitivität: ja, da $|x| = |y| \wedge |y| = |x| \Rightarrow |x| = |y|$.

  $\Rightarrow$ A ist eine Äquivalenzmenge!

- Ist $A = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} | |x - y| \leq 5\}$ eine Äquivalenzmenge?
  - Transitivität: scheitert, da $|1-5| \leq 5 \wedge |5-10| \leq 5$, aber $|1-10| \geq 5$.

  $\Rightarrow$ A ist keine Äquivalenzmenge!

- Ist $A = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} | x teilt y\}$ eine Äquivalenzmenge?
  - Symmetrie: scheitert, da $1|7$ aber $7 \nmid 1$.

  $\Rightarrow$ A ist keine Äquivalenzmenge!

- Ist $A = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} | ggT(x, y) = \pm 1\}$ eine Äquivalenzmenge?

- Reflexivität: scheitert, da $ggt(5,5) = 5 \neq \pm 1$
- Symmetrie: scheiter, da ...
- Transitivität: scheiter, da ...

$\Rightarrow$ A ist keine Äquivalenzmenge!

1.3 Abbildungen

Seien M und N Mengen. Eine Abbildung φ von M in N ordnet jedem Element aus M genau ein Element aus N zu, welches *Bild* heißt und mit $x\varphi$ bezeichnet wird. $x \in M$ ist ein *Urbild*. Die Zuordnungsvorschrift kann geschrieben werden als: $\varphi : x \mapsto x\varphi$. $M\varphi$ heißt das $Bild\varphi$.
Sei $T \subseteq M$. Dann ist $T\varphi := \{x\varphi | x \in T\}$, und φ ist eingeschränkt auf T, Schreibweise $\varphi|_T$.
Spezialfall: $\emptyset\varphi = \emptyset$.

1.3.1 Beispiele für Abbildungen

- $\varphi : \{1,2,3\} \mapsto \{A,B\}$ mit $1\varphi = A, 2\varphi = B, 3\varphi = A$. Jedem Urbild wird eindeutig ein Bild zugeordnet, jedem Bild können jedoch mehrere Urbilder zugeordnet sein.
- $\varphi : \mathbb{Z} \mapsto \mathbb{Z}$ mit $x\varphi = 0$ für alle $x \in Z$.
- $\varphi : \mathbb{Z} \mapsto \mathbb{Z}$ mit $x\varphi = x + 1$ für alle $x \in Z$ (eineindeutige Zuordnung).
- $\varphi : \mathbb{Z} \times \mathbb{Z} \mapsto \mathbb{Q}$ mit $(x,y)\varphi = \frac{x}{y}$ für alle $y \neq 0$ und $(x,y)\varphi = 0$ für $y = 0$.
- $\varphi : \mathbb{M} \mapsto \mathbb{M}$ mit $x\varphi = x$ für alle $x \in Z$ (*identische Abbildung bzw. Identität*, id_M).

1.3.2 Spezielle Eigenschaften von Abbildungen

- φ heißt , falls gilt: Jedes Bild besitzt genau ein Urbild ($m, n \in M, m\varphi = n\varphi \Rightarrow m = n$).
- φ heißt *surjektiv*, falls gilt: Jedem Element der Menge N (in der die Bilder enthalten sind) ist mindestens einem Urbild zugeordnet ($Bild\varphi = \mathbb{N}$).
- φ heißt *bijektiv*, falls eine Abbildung injektiv und surjektiv ist.
- ◦ Genau dann ist eine Abbildung $\varphi : A \mapsto B$ zwischen englichen Mengen A, B mit $|A| = |B|$ injektiv, wenn sie surjektiv sind.

Sei $\varphi : M \to N$.

- Die Abbildung soll *surjektiv* werden. Da in N Elemente enthalten sein können, die zu keinem Element aus M das Bild darstellen, darf nur ein Teil von N verwendet werden: M $\varphi : M \to Bild\varphi$ ist surjektiv, da $Bild\varphi \subseteq N$.

- Die Abbildung soll *injektiv* gemacht werden: Es muß M verändert werden, damit nicht mehrere Elemente aus M demselben Element aus N zugeordnet sein können. Man definiert dazu eine Äquivalenzrelation $A := \{(x, y) \in M \times M | x\varphi = y\varphi\}$. Die dazugehörige Menge aller Äquivalenzklassen ist $M/ \backsim = \{\tilde{x} | x \in M\}$. Die neue Abbildung $\tilde{\varphi}$ wird definiert als: $\tilde{\varphi} : M/ \backsim \to N$, d.h. $\tilde{x} \mapsto x\varphi$, wobei $x\varphi$ ja einem Element aus N entspricht.
  Nun ist zu zeigen, daß $\tilde{\varphi}$ injektiv ist. Das heiß, dass zwei gleiche Bilder auch gleiche Urbilder haben. Die zwei gleichen Bilder seien $x\varphi = y\varphi$. Aus der Definition von A folgt: $(x, y) \in A$. Damit ist $x \backsim y \Leftrightarrow y \in \tilde{x}$. Wenn jedoch y in der Menge $\tilde{x}$ enthalten ist, so ist sind die Mengen $\tilde{x}$ und $\tilde{y}$ gleich, da zwei Äquivalenzklassen entweder kein gemeinsames Element haben oder gleich sind (siehe 1.2.1). Damit sind also die Urbilder von $x\varphi$ und $y\varphi$ gleich.

1.3.3 Hintereinanderausführung

Sei $\phi : M \to N$ und $\psi : N \to R$. Dann ist $\phi\psi : M \to R$ mit $m(\phi\psi) := (m\phi)\psi$. Sind ϕ und ψ injektiv/surjektiv/bijektiv, so ist auch $\phi\psi$ injektiv/surjektiv/-bijektiv. Beweis:

1. ϕ ist injektiv.

2. ψ ist injektiv.

3. $m(\phi\psi) = m'(\phi\psi)$
   $\Rightarrow (m\phi)\psi = (m'\phi)\psi$

4. mit (2) folgt: $m\phi = m'\phi$.

5. mit (1) folgt: $m = m'$.

1.3.4 Assoziativität der Hintereinanderausführung

$\phi : M \to N; \psi : N \to P; \mu : P \to S \Rightarrow (\phi\psi)\mu = \phi(\psi\mu)$ Daraus folt auch: $|N| \leq |M|$ und $|M| \leq |P| \Rightarrow |N| \leq |P|$ (siehe 1.3.9).

1.3.5 inverse Abbildung

Sei $\phi : M \to N$ eine bijektive Abbildung. Dann existiert genau eine bijektive Abbildung $\phi^* : N \to M$ mit $m\phi\phi^* = m$ für alle $m \in M$ und $n\phi^*\phi = n$ für alle $n \in N$. Beweis:

1. Da ϕ surjektiv ist, existiert ein Urbild von n, und da ϕ injektiv ist, ist dieses Urilbd eindeutig bestimmt. Wir bezeichnen dieses Urbild von n mit m_n und definieren: $n\phi^* := m_n$ für alle $n \in N$. Wegen der Eindeutigkeit des Urbildes m_n ist ϕ^* eine Abbildung, und es gilt:
   (a) $m\phi\phi^* = m_{m\phi} = m$ für alle $m \in M$
   (b) $n\phi^*\phi = n_m\phi = n$ für alle $n \in N$
2. Seien $n, n' \in N$ und $n\phi^* = n'\phi^*$. Wendet man ϕ auf beiden Seiten der Gleichung an, so erhält man wegen (b) $n = n'$, d.g. ϕ^* ist injektiv; und wegen (b) ist ϕ^* auch surjektiv. Damit ist ϕ^* bijektiv.
3. Sei $\phi^{**} : N \to M$ eine Abbildung mit $m\phi\phi^* * = m$ für alle $m \in M$. Dann gilt $(m\phi)\phi^* = m\phi\phi^* = m = m\phi\phi^* * = m(\phi)\phi^* *$. Das heißt, daß ϕ^* und $\phi^* *$ tun das gleiche auf $Bild\phi$. Aus der Surjektivität von ϕ folgt $Bild\phi = N$ und damit $\phi^* = \phi^* *$.

Die beschriebene Abbildung ϕ^* heißt *inverse Abbildung* ϕ^{-1}.

1.3.6 Nicht-Surjektivität jeder Abbildung von M in $\mathcal{P}(M)$

Es existiert keine surjektive Abbildung von M in $\mathcal{P}(M)$. Beweis siehe Script.

1.3.7 Definition für endliche Mengen

Eine Menge M ist genau dann endlich, wenn jede injektive Abbildung von M in M auch bijektiv ist.
Gegenbeispiel: Die injektive Abbildung $\psi : \mathbb{N} \to \mathbb{N}$ mit $n\psi := 2n$ ist nicht surjektiv, z.B. gibt es zu 2 kein Urbild, also ist $\mathbb{N}$ nicht endlich.

1.3.8 Satz von Schröder-Bernstein

Seien M und N Mengen. Es existiere eine injektive Abbildung von M in N und eine injektive Abbildung von N in M. Dann existiert eine bijektive Abbildung von N in M (und umgekehrt, siehe (1.3.5)). Andere Schreibweise: $|N| \leq |M| \wedge |M| \leq |N| \Rightarrow |N| = |M|$ (siehe 1.3.9).

1.3.9 Mächtigkeit von Mengen

Es gilt genau eine der drei Aussagen über die Mengen M und N:

1. $|M| = |N|$: Es existiert eine bijektive Abbildung von M in N (und umgekehrt).
2. $|M| < |N|$: Es existiert eine injektive Abbildung von M in N, aber keine injektive Abbildung von N in M.
3. $|M| > |N|$: Es existiert keine injektive Abbildung von M in N, aber eine injektive Abbildung von N in M.

1.3.10 Mächtigkeit der Zahlenmengen

Satz: $|\mathbb{N}| = |\mathbb{Q}|$ (siehe Übungsaufgabe)
Behauptung: $|\mathbb{N}| < |\mathbb{R}|$
Beweis: Annahme, $|\mathbb{N}| = |\mathbb{R}|$. Nach Schröder-Bernstein existiert also eine bijektive Abbildung $\varphi : \mathbb{R} \to \mathbb{N}$. Wir betrachten nur das Intervall $]0,1[$. Die eingeschränkte Abbildung $\varphi|_{]0,1[} \to \mathbb{N}$ ist injektiv. Sei $\varphi' : \mathbb{N} \to]0,1[$ mit $n \mapsto \frac{1}{n+1}$. Zudem existiert eine bijektive Abbildung $\mu : \mathbb{N} \to]0,1[$. Dann ist $1\mu = 0,k_{11}k_{12}...k_{1n}$ und $m\mu = 0,k_{m1}k_{m2}...k_{mn}$. Sei $b = 0,b_1b_2b_3...b_n$ mit $b_1 \in \{0,...,9\}$ und $b_i \neq k_{ii}$ für alle i (und mindestens ein $b_i \neq 0$). Damit ist $b \neq n\mu$ für alle $n \in \mathbb{N}$, insofern kann b nicht in $]0,1[$ liegen - tut es aber: Widerspruch Es existiert also keine surjektive (und damit auch keine injektive) Abbildung μ.

1.4 Vollständige Induktion

Sei $r \in \mathbb{Z}$ und $\mathbb{Z}_{\geq r} = \{x \in \mathbb{Z} | x \geq r\}$. Damit ist $\mathbb{N} = \mathbb{Z}_{\geq 1}$ und $\mathbb{N}_0 = \mathbb{Z}_{\geq 0}$. Wir benutzen folgende Eigenschaft: Sei M eine nichtleere Teilmenge von $\mathbb{Z}_{\geq r}$. Dann existiert in M ein kleinstes Element.

1.4.1 Prinzip des minimalen Gegenbeispiels

Sei M' eine Teilmenge von $\mathbb{Z}_{\geq r}$ mit $M' \subset \mathbb{Z}_{\geq r}$ (echte Teilmenge). Dann existiert ein $z_0 \in \mathbb{Z}_{\geq r}$ mit

(i) $z_0 \notin M'$ und

(ii) $\forall\, z \in \mathbb{Z}_{\geq r} \mid z < z_0 : \ z \in M'$.

d.h. also das kleinste Element aus $\mathbb{Z}_{\geq r}$, das nicht in M' liegt.

Beweis: Sei $M = \mathbb{Z}_{\geq r} \setminus M'$. M ist nichtleer, da $M' \neq \mathbb{Z}_{\geq r}$. Ex existiert also ein kleinstes Element $z_0 \in M$. z_0 erfüllt (i) und (ii).

1.4.2 Prinzip der vollständigen Induktion, erste Version

Sei $M \subseteq \mathbb{Z}_{\geq r}$. Es gelte:

(i) $r \in M$ und

(ii) $z \in M \Rightarrow z+1 \in M$.

Dann ist $M = \mathbb{Z}_{\geq r}$ (d.h. wenn das kleinste Element in M liegt und man beweisen kann, daß auch jeder Nachfolger eines Elementes aus M in M liegt, müssen alle in M liegen).

Beweis: Annahme, $M \neq \mathbb{Z}_{\geq r}$. Sei $M' = \mathbb{Z}_{\geq r} \setminus M$. Dann ist $M' \neq \emptyset$. Wende 1.4.1 an: Es existiert $z_0 \in M'$ mit $z \in M'$ für alle $z \in \mathbb{Z}_{\geq r}$ und $z < z_0$. Aus (i) folgt: $r \neq z_0$, d.h. $r < z_0$ und $z_0 - 1 \in \mathbb{Z}_{\geq r}$, damit gilt auch: $z_0 - 1 < z_0 \Rightarrow z_0 - 1 \notin M'$. Wende (ii) auf $z_0 - 1$ an, dann liegt $z_0 - 1 + 1$ in M, also $z_0 \in M$. Damit muß aber $z_0 \notin M'$ sein: Widerspruch

1.4.3 Prinzip der vollständigen Induktion, zweite Version

Sei $M \subseteq \mathbb{Z}_{\geq r}$, $M \neq \emptyset$. Für alle $z \in \mathbb{Z}_{\geq r}$ gelte:

(i) Ist $z' \in M$ für alle $z' \in \mathbb{Z}_{\geq r}$ mit $z' < z$, so ist auch $z \in M$.

Dann gilt $M = \mathbb{Z}_{\geq r}$ (d.h. wenn für ein beliebiges z alle kleineren Elemente in M liegen und das auch für z selbst gilt, so ist $M = \mathbb{Z}_{\geq r}$).

Beweis: Annahme: $M \neq \mathbb{Z}_{\geq r}$. Mit 1.4.1 gilt: Es existiert $z_0 \in \mathbb{Z}_{\geq r}$ mit $z_0 \notin M$ und $z' \in M$ für alle $z' \in \mathbb{Z}_{\geq r}$ mit $z' < z_0$.

1.4.4 Beispiel

- Behauptung: Sei $n \in \mathbb{Z}_{\geq 3}$. Dann gilt: $n^2 > 2n + 1$.

  Beweis:

  - Sei $M := \{n \in \mathbb{Z}_{\geq 3} | n^2 > 2n + 1\}$.
  - Es ist zu zeigen: $M = \mathbb{Z}_{\geq 3}$.
  - Annahme, $M \neq \mathbb{Z}_{\geq 3}$.
  - Sei z_0 ein minimales Gegenbeispiel, d.h. $z_0^2 \leq 2z_0 + 1$ (1) und $z^2 > 2z + 1$ (2) für alle $z \in \mathbb{Z}_{\geq 3}$ und $z < z_0$.
  - z_0 kann nicht 3 sein ($9 \not\leq 3$), also $z_0 - 1 \in \mathbb{Z}_{\geq 3}$.
  - $z_0^2 \leq 2z_0 + 1$ (aus (1))

  $\Rightarrow$ $((z_0 - 1) + 1)^2 \leq 2z_0 + 1$

$\Rightarrow$ $(z_0 - 1)^2 + 2 \cdot (z_0 - 1) + 1 \leq 2z_0 + 1$ mit (2) links:

$\Rightarrow$ $(2 \cdot (z_0 - 1) + 1) + 2 \cdot (z_0 - 1) + 1 \leq 2z_0 + 1$

$\Rightarrow$ $4z_0 - 2 \leq 2z_0 + 1$

$\Rightarrow$ $z_0 \leq 1,5$

- Widerspruch, da $z > 3$ sein muß!
- Anmerkung: Dieser Beweis liefert gleich ein passendes Gegenbeispiel ($z = 1$), da der Satz tatsächlich für z.B. 1 ungültig ist!

1.5 Gruppen

Sei M eine nichtleere Menge. Sei $\varphi : M \times M \to M$ eine Abbildung (φ heißt innere Verknüpfung auf M) Wir schreiben: $(a, b)\varphi =: ab$ und nennen φ eine Multiplikation auf M, oder wir schreiben $(a, b)\varphi =: a + b$ und nennen φ eine Addition.

Definition: Sei G eine nichtleere Menge und φ eine innere Verknüpfung auf G. Es gelte:

1. Assozivität: $((g_1, g_2)\varphi, g_3)\varphi = (g_1, (g_2, g_3)\varphi)\varphi \; \forall \; g_1, g_2, g_3 \in G$.
2. Existenz des neutralen Elementes: Es existiert genau ein $n \in G$ mit $(g, n)\varphi = g \forall \; g \in G$.
3. Existenz eines inversen Elementes: Zu jedem $g \in G$ existiert genau ein $g' \in G$ mit $(g, g')\varphi = (g', g)\varphi = n \forall \; g, g' \in G$.

Dann heißt (G, φ) bzw. G eine *Gruppe*.

Eine Gruppe G, heißt *abelsch*, falls $(g_1, g_2)\varphi = (g_2, g_1)\varphi \; \forall \; g_1, g_2 \in G$ (Kommutativität).

Bezüglich der Multiplikation schreiben wir 1 als n und g^{-1} als inverses Element; bezüglich der Addition schreiben wir 0 als n und $-g$ als inverses Element. Eine nicht-abelsche Gruppe schreibt man meist multiplikativ, eine abelsche Gruppe meist additiv.

1.5.1 Beispiele

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ sind bezüglich der (»Schul«-)Addition abelsche Gruppen, $\mathbb{N}$ ist keine Gruppe bezüglich der Addidtion.
- $\mathbb{Q}^* := \mathbb{Q} \backslash \{0\}$, $\mathbb{R}^* := \mathbb{R} \backslash \{0\}$ sind bezüglich der (»Schul«-)Multiplikation abelsche Gruppen.

- $G := \{1\}; 1 \cdot 1 := 1$ ist eine abelsche Gruppe.
- $G := \{0, 1\};$ $\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}$
  ist eine abelsche Gruppe.
- Sei Ω eine endliche Menge und $S(\Omega)$ die Menge aller bijektiven Abbildung von Ω in Ω (Permutationen). $S(\Omega)$ ist eine Gruppe beßuglich der Hintereinanderausführung.
  - Assoziativität: siehe 1.3.4
  - Einselement: *id.*; zu zeigen: $g1 = g$. Für alle $\alpha \in \Omega$: $\alpha(g \cdot 1) = (\alpha \cdot g) \cdot 1 = \alpha g$
  - Inverse Elemente: Siehe (1.3.5)
  - Kommutativität: Gegenbeispiel:
    * $\Omega := \{1, 2, 3\}$.
    * $g_1 : 1 \mapsto 2; 2 \mapsto 1; 3 \mapsto 3$
    * $g_2 : 1 \mapsto 1; 2 \mapsto 3; 3 \mapsto 2$
    * $g_1 g_2 : 1 \mapsto 3; 2 \mapsto 1; 3 \mapsto 2$
    * $g_2 g_1 : 1 \mapsto 2; ...$

  $S(\Omega)$ heißt die *Symmetrische Gruppe* auf Ω.

1.5.2 Eindeutige Lösbarkeit von Gleichungen

SATZ: Sei G eine (mult.) Gruppe, und seien $g, h \in G$. Dann existiert genau ein $x \in G$ und genau ein $x' \in G$ mit: $g \cdot x = h$ und $x'g = h$.

BEWEIS: Sei $x := g^{-1} \cdot h$ und $x := h \cdot g^{-1}$. Es gilt: $g(g^{-1} \cdot h) = (g \cdot g^{-1}) \cdot h = 1 \cdot h = h$ und $(h \cdot g^{-1}) \cdot g = h \cdot (g^{-1} \cdot g) = h \cdot 1 = h$.

SATZ: Sei G eine (mult.) Gruppe, und seien $a, b, x, x' \in G$ mit $ax = b$ und $ax' = b$. Dann ist $x = x'$.

BEWEIS: $b = b \Rightarrow ax = ax' \Rightarrow x = 1x = (aa^{-1})x = a^{-1}(ax) = a^{-1}(ax') = (aa^{-1})x' = 1x' = x' \Rightarrow x = x'$.

weiter SÄTZE:

- $(g^{-1})^{-1} = g$
- $(g \cdot h)^{-1} = g^{-1} \cdot h^{-1}$

1.5.3 Untergruppen

Sei G eine Gruppe bezüglich der inneren Verknüpfung φ. Sei T eine nichtleere Teilmenge von G. T heißt *Untergruppe* von G, falls $\varphi|_{T\times T}$ eine innere Verknüpfung auf T ist und $(T, \varphi|_{T\times T})$ eine Gruppe ist.

Sei T eine Untergruppe, sei $t \in T$ Es existiert genau ein inverses Element t' von $t \in T$ und ein inverses Element t'' von $t \in G$. Es existiert ein neutrales Element $n' \in T$ und ein neutrales Element $n'' \in G$.
Daraus folgt:

- $n' \cdot n' = n'$ und $n' \cdot n'' = n'$. Mit 1.5.2 folgt: $n' = n''$.
- $t \cdot t' = n'' = n'$ und $t \cdot t'' = n''$. Mit 1.5.2 folgt: $t' = t''$.

Beispiele:

- $\mathbb{Z} \leqslant \mathbb{Q}$ ist Untergruppe bezüglich der Addition
- $\mathbb{Q} \leqslant \mathbb{R}$ ist Untergruppe bezüglich der Addition
- $\mathbb{Z}^* \leqslant \mathbb{Q}^*$ ist keine Untergruppe bezüglich der Multiplikation
- $\mathbb{Q}^* \leqslant \mathbb{R}^*$ ist Untergruppe bezüglich der Multiplikation
- Sei Ω eine nichtleere Menge. Sei $w \in \Omega$. $A := \{\varphi \in S(\Omega) | \omega\varphi = \omega\}$. Behauptung: A ist eine Untergruppe von $S(\Omega)$. Das heißt, A darf nicht leer sein (i), muß die innere Verknüpfung $\cdot$ (Hintereinanderausführung) haben (ii) und ein neutrales und inverses Element haben (iii).

  Beweis: Wir wissen, daß $id_\Omega \in S(\Omega)$. Es gilt: $\omega id_\Omega = \omega$, also $id_\Omega \in A$ und damit $A \neq \emptyset$ (i). Seien $\varphi, \psi \in A$. Dann ist $\omega(\varphi\psi) = (\omega\varphi)\psi = \omega\psi = \omega$. Daraus folgt: $\varphi\psi \in A$ (ii). id_Ω ist Einselement von A. Sei $\varphi \in A$. Wir zeigen: $\omega\varphi^{-1} = \omega$. $\omega(\varphi\varphi^{-1}) = \omega id_\Omega = \omega$. Daraus folgt: $\omega\varphi^{-1} = \omega$. Also ist $\varphi^{-1} \in A$ (iii).

1.5.4 Untergruppenkriterium

Voraussetzung: Sei G eine Gruppe, T eine nichtleere Teilmenge von G.

Behauptung: Genau dann ist T eine Untergruppe von G, wenn für alle Elemente $a, b \in T$ gilt: $a \cdot b^{-1} \in T$. Das heißt:

1. Wenn T eine Untergruppe ist, dann gilt: $ab^{-1} \in T$ für alle $a, b \in T$.
2. Aus $ab^{-1} \in T$ für alle $a, b \in T$ folgt: T ist eine Untergruppe von G.

Beweis:

1. Seien $a, b \in T$. Daraus folgt: $b^{-1} \in T$, also ist $ab^{-1} \in T$.
2. Sei $a \in T$. Aus der Voraussetzung folgt: $aa^{-1} \in T$, d.h. $1 \in T$, das neutrale Element ist in T. Um zu zeigen, daß zu jedem Element aus T sein inverses Element auch in T ist, nehmen wir $1, a \in T$, also $1a^{-1} \in T$, also liegt zu jedem Element auch das inverse Element in T. Zu zeigen bleibt, daß die Verknüpfung eine innere Verknüpfung ist. Schon gezeigt: $b^{-1} \in T$, daraus folgt: $a(b^{-1})^{-1} \in T$, also $ab \in T$. T ist also eine Gruppe

1.5.5 Bezeichnungen

Sei G eine additive abelsche Gruppe. Sei $z \in \mathbb{Z}$ und $a \in G$.

- $za := 0_G$ für $z = 0_{\mathbb{Z}}$.
- $za := (z-1)a + a$ für $z \geq 1$
- $za := (-z)(-a)$ für $z \leq -1$

Es gelten folgende Rechenregeln für $a, b \in G$ und $m, n \in \mathbb{Z}$:

- $(-n)a = -(na) = n(-a)$
- $(n+m)a = na + ma$
- $n(ma) = (nm)a = m(na)$
- $m(a+b) = ma + mb$

Beweis von $(-n)a = -(na) = n(-a)$:

$n \geq 0$ Nach Voraussetzung ist $(-n) \cdot a = n \cdot (-a)$. Zu zeigen bleibt: $(-n) \cdot a = -(na)$, das ist äquivalent zu: $(-n) \cdot a = inv(na)$.
Beweis mit vollständiger Induktion: $M := \{z \in \mathbb{Z}_{\geq 0} \mid (-z)a = inv(za)\}$; zu zeigen: $M = \mathbb{Z}_{\geq 0}$ mittels Induktion.
Induktionsverankerung: $0 \in \mathbb{Z}_{\geq 0}$: $(-0) \cdot a + 0 \cdot a = 0 \cdot a + 0 \cdot a = 0 + 0 = 0$.
Induktionsannahme: Sei $n \in M$.
Induktionsschluß:

$$\begin{aligned}
(-(n+1)) \cdot a + (n+1) \cdot a &= (n+1) \cdot (-a) + (n+1) \cdot a && (1)\\
&= n \cdot (-a) + (-a) + n \cdot a + a && (2)\\
&= (-n) \cdot a + n \cdot a + (-a) + a && (3)\\
&= 0 + 0 && (4)\\
&= 0 && (5)
\end{aligned}$$

Bei (3) auf (4) wird die Induktionsannahme eingesetzt.

$n < 0$

$$\begin{aligned} -(na) &= -((-n)\cdot(-a)) & (6)\\ &= -((-(-n))(-a)) & (7)\\ &= n\dot{(}-a) & (8)\\ &= (-n)\cdot a & (9) \end{aligned}$$

Sei G eine multiplikative abelsche Gruppe. Sei $z \in \mathbb{Z}$ und $a \in G$.

- $a^z := 1_G$ für $z = 0_{\mathbb{Z}}$.
- $a^z := a^{z-1} \cdot a$ für $z \geq 1$
- $a^z := (a^{-1})^{-z}$ für $z \leq -1$

1.6 Körper

Sei K eine Menge mit mindestens zwei Elementen. Auf K seien zwei inntere Verknüpfungen definiert ($+$ und $\cdot$), und es gelte:

1. K ist bezüglich der Addition eine abelsche Gruppe.
2. $K^* := K \setminus \{0_K\}$ ist eine abelsche Gruppe bezüglich der Multiplikation.
3. K ist bezüglich der beiden Verknüpfungen distributiv, d.h. es gilt: $a \cdot (b + c) = a \cdot b + a \cdot c$.

Dann heißt $(K, +, \cdot)$ *Körper*.

1.7 Beispiele

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Körper.
- $\mathbb{Z}$ ist kein Körper.
- $K := \{0, 1\}; 0 + 0 = 0; 0 + 1 := 1; 1 + 1 := 0;$
  $K^* = \{1\}; 1 \cdot 1 = 1$ ist ein Körper
- Sei p eine Primzahl. Für $a \in \mathbb{Z}$ sei $\overline{a} := \{a+np | n \in \mathbb{Z}\}$. Sei $\mathbb{Z}_p$ die Menge aller $\{\overline{0}, \overline{1}, ..., \overline{p-1}\}$, damit ist $\mathbb{Z}_p$ die Menge aller Äquivalenzklassen der Äquivalenzrelation $A := \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid p|(a - b)\}$.

  Für $\overline{a}, \overline{b} \in \mathbb{Z}_p$ seien $(\overline{a}, \overline{b}) \mapsto \overline{a + b}$ und $(\overline{a}, \overline{b}) \mapsto \overline{ab}$ innere Verknüpfungen auf $\mathbb{Z}_p$. (Beweis, daß dies Abbildungen sind und daß dies eine Gruppe ist, siehe Script).

  Sei $\overline{a} \in \mathbb{Z}_p^*$ fest geählt. Sei $\varphi\overline{x} \mapsto \overline{xa}$. Behauptung:

1. φ ist surjektiv
2. φ ist injektiv

Beweis:

1. (später)
2. Seien $\overline{z}, \overline{z}' \in \mathbb{Z}_p^*$ mit $\overline{z}\varphi = \overline{z'}\varphi$. Dann folgt: $\overline{z}\varphi = \overline{za} = \overline{z'}\varphi = \overline{z'a}$, d.h. $\overline{za} = \overline{z'a}$. p teilt damit $(z - z')a$. Also teilt p entweder a oder $(z - z')$. Falls $p|(z - z')$ gilt, ist die Annahme gezeigt. Andernfalls gilt $p|a$, damit ist aber $\overline{a} = \overline{0}$, das steht im Widerspruch zu $\overline{a} \in \mathbb{Z}_p^*$.

1.8 Charakteristik

1.8.1 Lemma 1

Sei K ein Körper, $a \in K$ und seien $z_1, z_2 \in \mathbb{Z}$. Dann gilt: $(z_1 a)(z_2 a) = (z_1 z_2)a^2$.

1.8.2 Nullteilerfreiheit von Körpern

Sei K ein Körper, $a, b \in K$. Es gelte $ab = 0$. Dann ist $a = 0$ oder $b = 0$. Beweis dafür: Angenommen, $a \neq 0 \wedge b \neq 0$, d.h. $a, b \in K^*$ (also in der multiplikativen Gruppe K^*), aber da die Multiplikation eine innere Verknüpfung auf K^* ist, kann ab nicht 0 sein.

1.8.3 Charakteristik

Sei K ein Körper. Die Charakteristik von K ($char\ K$) sei definiert als:

- $char\ K = 0$, falls $n1 \neq 0$ für alle $n \in \mathbb{N}$
- andernfalls $char\ K = min\{n \in \mathbb{N} \mid n1 = 0\}$

1.8.4 Eigenschaften der Charakteristik

Sei K ein Körper und $p := char\ K$ und $p \neq 0$. Dann gilt:

1. p ist Primzahl
2. Gilt $m1 = 0$ für ein $m \in \mathbb{N}$, so ist p Teiler von m.

Beweis:

1. $1 \in K^*$, d.h. $1 \neq 0$. Daraus folgt: $1 \cdot 1 \neq 0$, d.h. $p > 1$. Dann existieren Primzahlen $q, p' \in \mathbb{N}$ mit $p = qp'$. $p1 = 0$ (wegen *char*). $p1 = (qp')1 = (qp')1^2 = (q1)(q2)$ (mit 1.8.1). Mit 1.8.2 gilt: $q1 = 0$ oder $p'1 = 0$, also ist $p \leq q$ oder $p \leq p'$, damit ist entweder $p' = 1$ oder $q = 1$ und damit $q = p$ oder $q = p$, also ist p Primzahl, q.e.d.

2. Sei $m \in \mathbb{N}$, $m1 = 0$, $m = r + hp$ für $r \in \mathbb{N}_0$ und $h \in \mathbb{Z}$ mit $r < p$. $0 = m1 = (r + hp)1 = r1 + (hp)1 = r1 + h(p1) = r1 + h(0) = r1$. Damit folgt aus der Minimalität von p, daß $r \notin \mathbb{N}$ sein kann, damit ist $r = 0$ und damit $m = hp$.

2 Vektorräume

2.1 Definition und einfache Eigenschaften

Sei K ein Körper und V eine additive abelsche Gruppe und sei $\varphi : K \times V \to V$ eine Abbildung. Wir schreiben $kv := (k, v)\varphi$ und nennen φ Skalarmultiplikation, es gelte $\forall\, k_1, k_2 \in K$:

1. $1_K v = v$
2. $(k_1 k_v)v = k_1(k_2 v)$
3. $(k_1 + k_2)v = k_1 v + k_2 v$
4. $k(v_1 + v_2) = kv_1 + kv_2$

Anmerkung: Gleiche Zeichen haben verschiedene Bedeutungen, es existieren **!**

- $1 \in K$ und $1 \in \mathbb{Z}$
- $0 \in K$, $0 \in V$ und $0 \in \mathbb{Z}$
- $+$ für K und V

Dann heïst V *Vektorraum über* K (kurz: K-*Vektorraum*).

Beispiele: Sei K ein Körper

1. Sei $V := \{0\}$ mit $k0 = 0\ \forall\, k \in K$.
2. $V := K$
3. $K = \mathbb{Q}, V := \mathbb{R}$
4. $V = K^n := \bigotimes_{i=1}^{n} K$ mit komponentenweiser Addition und Skalarmultiplikation
5. Gegeben sei ein lineares Gleichungssystem mit $a_{ij} \in \mathbb{R}$ und der Lösungsmenge $\mathbb{L}$:

$$\begin{array}{cccccc} a_{11}x_1 & +...+ & a_{1n}x_n & = & 0 \\ \vdots & +...+ & \vdots & = & 0 \\ a_{n11}x_1 & +...+ & a_{nn}x_n & = & 0 \end{array}$$

Sei $V := \{(l_1, l_2, ..., l_n) \mid l_i \in \mathbb{R} \text{ und } (l_1, l_2, ..., l_n) \in \mathbb{L}\}$. Dann ist V bezüglich der Addition und Skalarmultiplikation von $\mathbb{R}^n$ ein Vektorraum. Beweis per Unterruppenkriterium (1.5.4):

- $V \neq \emptyset$ gilt, da es mindestens die Lösung $(0, ..., 0)$ gibt
- zz: $a, b \in V \Rightarrow a - b \in V$; sei $a = (l_1, ..., l_n)$ und $b = (h_1, ..., h_n)$

2.1.1 Rechenregeln

Sei $k \in K, v \in V$. Dann gilt:

1. $0v = 0$
2. $k0 = 0$
3. $(-k)v = -(kv) = k(-v)$, insbesondere $(-1)v = -v$

2.1.2 Nullteilerfreiheit der Skalarmultiplikation

Sei $k \in K$ und $v \in V$. Dann gilt:

$$kv = 0 \Rightarrow k = 0 \vee v = 0$$

2.1.3 Bezeichnungen

Seien $v, w \in V$ und $A, B \subseteq V$.

$$\begin{aligned} A + B &:= \{a + b \mid a \in A, b \in B\} \\ a + B &:= \{a\} + B \\ KA &:= \{ka \mid k \in K, a \in A\} \\ Ka &:= K\{a\} \\ \sum_{i=1}^{n} A_i &:= \left\{ \sum_{i=1}^{n} a_i \mid a_i \in A_i \right\} \end{aligned}$$

2.1.4 Unterräume

Eine Teilmenge $U \subseteq V$ heißt *Untervektorraum* von V, wenn U eine Untergruppe der additiven Gruppe V bezüglich der Skalarmultiplikation von V ein Vektorraum ist. Dann schreibt man $U \leq V$

2.1.5 Unterraumkriterium

Sei U eine nichtleere Teilmenge von V.

$$U \leq V \Leftrightarrow KU \subseteq U \wedge U + U \subseteq U$$

Triviale Beispiele: $\emptyset$ und V sind Untervektorräume von V.

2.2 Lineare Unabhängigkeit und Erzeugendensysteme

Sei I eine indexmenge und seien $v_i, i \in I$ Elemente von V. Für jede *endliche* Teilmenge $J \subseteq I$ und $k_j \in K, j \in J$ heißt

$$\sum_{j \in J} k_j v_j$$

Linearkombination der Elemente $v_i, i \in I$. Wir schreiben dafür auch

$$\sum_{i \in I} k_i v_i$$

mit der **Verabredung**, daß nur endlich viele $k_i \neq 0$ sind. Sei $B \subseteq V$. Wir schreiben dann:

$$\sum_{b \in B} k_b b$$

Die Elemente $v_i, i \in I$ heißen *linear abhängig*, falls $k_i \in K, i \in I$ existieren mit:

1. $\sum\limits_{i \in I} k_i v_i = 0$
2. $\exists i \ : \ k_i \neq 0$

Die Elemente $v_i, i \in I$ heißen linear abhängig, falls sie nicht linear abhängig sind, d.h.

$$\sum_{i \in I} k_i v_i = 0 \Rightarrow k_i = 0 \; \forall \; i \in I$$

Sei $B \subseteq V$. B heißt linear (un-)abhängig, wenn die Elemente $b \in B$ linear (un-)abhängig sind. Spezialfälle: Ist $I = \emptyset$, so sind die Elemente $v_i, i \in I$ linear unabhängig. Genauso: $\emptyset$ ist linear unabhängig.

2.2.1 Beispiele

- Sei $v \in V$. Ist $v = 0$, so ist $\{v\}$ linear abhängig: $k \cdot v = 1 \cdot 0 = 0$.
- Sei $v \in V$. Ist $v \neq 0$, so ist $\{v\}$ linear unabhängig: Mit der Nullteilerfreiheit folgt aus $kv = 0 \wedge v \neq 0$, daß $k = 0$ ist.
- Sei $V = \mathbb{R}^3$. dann sind $(1, 0, 0), (0, 1, 0), (0, 0, 1)$ linear unabhängig. Beweis: Seien $k_1, k_2, k_3 \in \mathbb{R}$

$$\begin{aligned} (0,0,0) &= k_1 \cdot (1,0,0) + k_2 \cdot (0,1,0) + k_3 \cdot (0,0,1) \\ &= (k_1,0,0),(0,k_2,0),(0,0,k_3) \\ &= (k_1,k_2,k_3) \end{aligned}$$

  Damit sind alle Koeffizienten gleich 0.

- Sei $V = \mathbb{R}^3$. dann sind $(1,2,3),(2,4,6),(0,1,2)$ linear abhängig. Beispiel: $-2\cdot(1,2,3)+(2,4,6)+0\cdot(0,1,2)=(0,0,0)=0$

- Sei $B \subseteq V$ linear unabhängig. Dann ist jede Teilmenge von B auch linear unabhängig.

- Sei V der Vektorraum der Funktionen von $[0,1] \to R$. Sei P_n mit $n \in \mathbb{N}$ definiert als $P_n(x) = x^n$. Behauptung: Die $P_n, n \in \mathbb{N}$ sind linear unabhängig.
  Beweis: $P_n' = n \cdot P_{n-1}$; $P_n^{(2)} := P_n'' = n\cdot(n-1)\cdot P_{n-2}$ usw. bis $P_n^{(n)} = n! \cdot P_0$. Seien $k_i \in R$ mit $f := \sum\limits_{i\in\mathbb{N}} k_i p_i = 0$. Sei $n \in \mathbb{N}$ das maximale n mit $k_n \neq 0$ (Gibt es so ein n, so wäre f linear abhängig!). Dann ist $f^{(n)} = n! \cdot k_n = 0$, also $k_n = 0$, das widerspricht aber der Annahme, also ist f linear unabhängig.

2.2.2 Satz zur linearen Unabhängigkeit

Seien $v_i, i \in I$ Elemente von V. Dann sind die folgenden Aussagen äquivalent:

(a) Die Elemente $v_i, i \in I$ sind linear unabhängig.

(b) Jedes Element aus V lässt sich auf höchstens eine Weise als Linearkombination der Elemente $v_i, i \in I$ schreiben.

(c) Für alle $i \in I$ ist v_i nicht[1] Linearkombination der Elemente $v_j, j \in I\backslash\{i\}$.

Beweis durch Ringschluß: $(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (a)$.

$(a) \Rightarrow (b)$ Wir setzen voraus, daß (a) gilt, d.h. $v_i, i \in I$ sind linear unabhängig. Sei $v \in V$ und sei $k_i, h_i \in K, i \in I$ mit

$$\begin{aligned}
v &= \sum_{i\in I} k_i v_i = \sum_{i\in I} h_i v_i \\
\Rightarrow 0 &= \sum_{i\in I} k_i v_i - \sum_{i\in I} h_i v_i \\
\Rightarrow 0 &= \sum_{i\in I} (k_i - h_i) v_i \\
\overset{lin.unabh.}{\Rightarrow} k_i - h_i &= 0 \;\forall\, i \in I \\
\Rightarrow k_i &= h_i \;\forall\, i \in I
\end{aligned}$$

D.h. gibt es zwei Linearkombinationen, sind diese gleich, damit gibt es höchstens eine Linearkombination.

[1] „Das Wort heißt »nicht« - was sonst? Welches andere Wort mit fünf Buchstaben kennen denn Sie schon?“

$(b) \Rightarrow (c)$ Wir setzen voraus, daß (b) gilt, d.h. jedes $v \in V$ ist auf höchstens eine Weise Linearkombination von $v_i, i \in I$. Sei $i \in I$. Dann ist $v_i = 1 \cdot v_1$ eine Linearkombination der Elemente $v_j, j \in I$. Diese Linearkombination ist nach Voraussetzung eindeutig, d.h. es kann keine andere Linearkombination geben, die v_i darstellt. Insbesondere kann es also keine Linearkombination der anderen Elemente $v_j, j \in I \setminus \{i\}$ geben.

$(c) \Rightarrow (a)$ Wir setzen voraus, daß (c) gilt, d.h. für alle $j \in I$ ist v_j nicht Linearkombination der Elemente $v_i, i \in I \setminus \{j\}$. Seien $k_i \in K, i \in I$, so daß $\sum_{i \in I} k_i v_i = 0$. Zu zeigen: $k_i = 0$ für alle $i \in I$. Annahme, es existiere ein $j \in I$ mit $k_j \neq 0$.

$$\begin{aligned}
-k_j v_j &= \sum_{i \in I \setminus \{j\}} k_i v_i \\
(-k_j)^{-1}(-k_j) v_j &= \sum_{i \in I \setminus \{j\}} (-k_j)^{-1} k_i v_i \\
v_j &= \sum_{i \in I\ \{j\}} v_i
\end{aligned}$$

Das widerspricht der Voraussetzung !

2.2.3 Austauschsatz

Seien $v_i, i \in I$ linear uabhängig, und seien $k_i \in K, i \in I$ und $v := \sum_{i \in I} k_i v_i$. Es existiere ein $j \in I$ mit $k_j \neq 0$. Dann sind die Elemente v, v_i mit $i \in I \setminus \{j\}$ linear unabhängig.

Beweis: Seien $h, h_i \in K, i \in I \setminus \{j\}$ mit $hv + \sum_{I \setminus \{j\}} h_i v_i = 0$. Zu zeigen: $h = 0$ und $h_i = 0$ für alle $i \in I \setminus \{j\}$.

$$\begin{aligned}
0 &= hv + \sum_{I \setminus \{j\}} h_i v_i \\
0 &= h \sum_{i \in I} k_i v_i + \sum_{I \setminus \{j\}} h_i v_i \\
0 &= h k_j v_j + \sum_{I \setminus \{j\}} [(h k_i + h_i) v_i)]
\end{aligned}$$

Durch die lineare Unabhängigkeit der v_i gilt: $hk_j = 0, hk_i + h_i = 0$ für $i \in I \setminus \{j\}$. Aus $hk_j = 0$ und $k_j = 0$ folgt mit 1.8.2: $h = 0$. Damit ist in $hk_i + h_i = 0$ auch $h_i = 0$.

2.2.4 Erzeugnis

Sei T eine Teilmenge von V. Das *Erzeugnis* von T ist der Durchschnitt aller Unterräume von V, die T enthalten. Das Erzeugnis wird mit $\langle T\rangle$ bezeichnet.

$$\langle T\rangle := \bigcap_{U\leq V;T\subseteq U} U$$

Das Erzeugnis von T ist der kleinste Unterraum von V, der T enthält. Sonderfälle: $\langle\emptyset\rangle = \langle 0\rangle = \{0\}$; $\langle V\rangle = V$.

2.2.5 Struktursatz für Erzeugnisse

Sei T eine Teilmenge von V. Dann gilt: $\langle T\rangle = \{\sum_{v\in T} vk_v \mid k_v \in K\}$ (d.h. das Erzeugnis ist die Menge der Linearkombinationen von T).

Beweis: Sei $D := \{\sum_{v\in T} vk_v \mid k_v \in K\}$. Es gilt: $T \subseteq D$ (jedes Element lässt sich ja als Linearkombination von sich selbst schreiben) und $T \subseteq U \leq V \Rightarrow D \subseteq U$. Wenn wir zeigen, daß D ein Unterraum ist, ist D der kleinste Unterraum, der T enthält. Nach dem Unterraumkriterium (str2.1.3) ist zu zeigen:

1. $D \neq \emptyset$
2. $KD \subseteq D$
3. $D + D \subseteq D$

Beweis:

1. da $T \subseteq D$ ist nur für den Spezialfall $T = \emptyset$ zu zeigen, daß $D \neq \emptyset$ ist. Nach der Definition von D enthält D die „leere Summe“, d.h. also $D = \{0\}$. Damit ist $D \neq \emptyset$.
2. Sei $k \in K$, $\sum_{v\in T} k_v v \in D \Rightarrow k\sum_{v\in T} k_v v \in D = \sum_{v\in T}(kk_v)v \in D$
3. $D + D \subseteq$ ist genauso einfach

2.2.6 Erzeugendensystem, Basis, endlich erzeugt

Sei T Teilmenge von V. T heißt *Erzeugendensystem* von V, falls $\langle T\rangle = V$. T heißt *Basis* von V, falls T Erzeugendensystem von V und linear unabhängig ist. V heißt *endlich erzeugt*[2], falls V ein endliches Erzeugendensystem besitzt.

[2] „...das heißt nicht, daß man sich lange angestrengt hat und V endlich erzeugt hat!“

2.2.7 Eindeutigkeit der Darstellung als Linearkombination

Sei B eine Basis von V. Dann ist jedes Element von V auf genau eine Weise Linearkombination der Elemente aus B.

Beweis: B ist Erzeugendensystem bedeutet: Jedes Element aus V ist Linearkombination der Elemente von B. B ist linear unabhängig, damit folgt mit (2.2.2): Jedes Element läßt sich auf höchstens eine Weise als Linearkombination darstellen. Damit lässt sich jedes Element auf genau eine Weise als Linearkombination vno B darstellen.

2.2.8 Existenz einer Basis

Sei E ein Erzeugendensystem von V und $n \in \mathbb{N}_0$. Wir setzen voraus:

(*) Für jede linear unabhängige Teilmenge $B \subseteq E$ gilt: $|B| \leq n$.

Dann existiert eine Basis von V in E.

Beweis: Wegen (*) existiert bezüglich Inklusion maximale linear unabhängige Teilmenge $B \subseteq E$. Zu zeigen beleibt: $\langle B \rangle = V$ (dann ist B eine Basis).

- Erster Fall $E \subseteq \langle B \rangle$: Dann gilt: $\langle E \rangle \leq \langle B \rangle$ mit $\langle E \rangle = V$, also ist $\langle B \rangle = V$.
- Angenommen, $E \nsubseteq \langle B \rangle$. Dann existiert ein $e \in E \setminus \langle B \rangle$. Sei $E_1 := B \cup \{e\}$. Dann ist E_1 linear abhängig (wegen der Maximalität von B). D.h. es existiert ein $k_v \in K, v \in E_1$ mit $\sum_{v \in E} k_v v = 0$ und nicht alle $k_v = 0$.
  - Der Fall $k_e = 0$: Es folgt: $\sum_{v \in B} k_v v = 0$, mit der linearen unabhängigkeit folgt: $k_v = 0$ für alle $v \in B$, Widerspruch zu eben !
  - Der Fall $k_e \neq 0$: Es folgt: $k_e e = \sum_{v \in B} -k_v v$. Multipliziert mit k_e^{-1}: $e = \sum_{v \in B} -k_e^{-1} k_v v$, das liegt aber nach (2.2.5) in $\langle B \rangle$

2.2.9 Austauschsatz von Steinitz

Sei B eine Basis von V und M eine endliche linear unabhängige Teilmenge von V. Dann existiert ein $B_0 \subseteq B$ mit

1. $|B_0| = |M|$
2. $(B \setminus B_0) \cup M$ ist Basis von V

BEWEIS: Induktion nach $n := |M|$:

- Verankerung für $|M| = 0$. Dann ist $M = \emptyset$, wähle $B_0 = \emptyset$, dann ist auch $(B \setminus \emptyset) \cup \emptyset = B$ eine Basis, trivial
- Induktionsannahme[3]: Es ist $|M| > 0$ und die Behauptung ist richtig für alle linear unabhängigen Teilmengen M' mit $|M'| = n - 1$
- Induktionsschluß: Sei $m \in M$ und $M' = M \setminus \{m\}$. $|M'| = n - 1$ und M' ist linear unabhängig (eine Teilmenge einer linear unabhängigen Menge ist wider linear unabhängig). D.h. es existiert $B_0' \subseteq B$ mit $|B_0'| = n - 1$ und $(B \setminus B_0') \cup M' = B^*$ ist Basis. Daraus folgt: Es existieren $k_v \in K$ mit $m = \sum_{v \in B^*} k_v v$. Angenommen, $k_v = 0$ für alle $B \setminus B_0'$. Dann ist $m = \sum_{v \in M'} k_v v$, Widerspruch zu (2.2.2). Also existier ein $v \in V$ $B_0' mit k_v \neq 0$. Wende (2.2.3) an: $(B^* \setminus \{v\}) \cup \{m\}$ ist Basis von V.

2.2.10 Erzeugnis von Teilmengen

Sei V endlich erzeugt und T Teilmenge von V. Dann existiert eine endliche linear unabhängige Teilmenge $T_0 \subseteq T$ mit $\langle T \rangle = \langle T_0 \rangle$.

BEWEIS: Nach Voraussetzung existiert ein endliches Erzeugendensystem E von V. Sei $n := |E|$. E und n erfüllen (2.2.8). Damit existiert eine Basis $B \subseteq E$ von V und $|B| \leq n$. Mit (2.2.9) folgt: Jede linear unabhängige Teilmenge von V hat höchstens $|B|$ Elemente. Insbesondere erfüllt T die Eigenschaft (*) aus (2.2.8), also existiert eine Basis $T_0 \subseteq T$ von $\langle T \rangle$. Damit ist $|T_0| \leq |B|$.

2.2.11 Vererbung der endlichen Erzeugung

Jeder Unterraum eines endlich erzeugten Vektorraums ist endlich erzeugt.

BEWEIS: Sei V endlich erzeugt und U ein Unterraum von V. Wähle $T := U$. Dann gilt: $\langle T \rangle = U$. Nach (2.2.10) existiert ein endliches T_0 mit $\langle T_0 \rangle = \langle T \rangle = U$.

2.2.12 Gleichmächtigkeit von Basen

Sei V endlich erzeugt. Dann besitzt V eine endliche Basis und alle Basen von V sind gleichmächtig.

BEWEIS: Sei T ein endliches Erzeugendensystem. Mit (2.2.10) existiert ein linear unabhängiges, endliches $T_0 \subseteq T$ mit $\langle T_0 \rangle = \langle T \rangle = V$. Damit ist T_0 eine

[3] „Worte sind Schall und Rauch!“

endliche Basis von V.
Sei B eine Basis von V. Damit ist B insbesondere linear unabhängig. Mit (2.2.8) folgt: $|B| \leq |T_0|$. Wiederum aus (2.2.8) folgt: $|T_0| \leq |B|$.

2.2.13 Gleichmächtigkeit von Basen II

Sei V endlich erzeugt und B Basis. Ist T eine linear unabhängige Teilmenge von V mit $|T| = |B|$, so ist T Basis von V. (im Prinzip die Umkehrung zu (2.2.12)).

Beweis: B ist endlich nach (2.2.12). Mit (2.2.9) angewandt auf T statt M folgt: Es existiert $B_0 \subseteq B$ mit $|B_0| = |T|$ und $(B\ B_0) \cup T = T$ ist Basis von V.

2.2.14 Dimension eines Vektorraums

Sei V endlich erzeugt und B eine Basis von V. Dann ist die Dimension von V definiert als:

$$\dim V := |B|$$

Statt endlich erzeugt sagt man auch *endlich dimensioniert* ($\dim\ V < \infty$). Nicht endlich erzeugte Vektorräume heißen *unendlich dimensional* ($\dim V = \infty$).

Sei V endlich dimensional. Sei $U \leq V$. Mit (2.2.9) und (2.2.11): $\dim\ U \leq \dim V$. Aus (2.2.13) folgt: Falls $\dim U = \dim V$, so ist $U = V$.

2.2.15 Beispiel, kanonische Basis

Sei $V = K^n$. Sei $e_i = (k_1, k_2, ..., k_n)$ mit $k_i = 0$ für alle $i < n$ und $k_n = 1$. Sei $B := \{e_i \mid i \in \{1, 2, ..., n\}\}$ linear unabhängig.

Behauptung: B ist Basis von V.

Beweis: B ist linear unabhängig (schon gezeigt), das $\langle B \rangle$ ist nach dem Struktursatz gleich $\{\sum_{b \in B} k_b b \mid k_b \in K\}$. Es bleibt zu zeigen: $\langle B \rangle = V$. Sei $v \in V$, d.h. es existeren $h_1, ..., h_n \in K$ mit $v = (h_1, h_2, ..., h_n)$. Daraus folgt: $v = \sum_{i=1}^{n} h_i e_i$. B heißt *kanonische Basis* von K^n, $\dim K^n = n$.

2.2.16 Beispiel

- Sei $V = K^3$ und $\{e_1, e_2, e_3\}$ die kanonische Basis. Sei $k \in K \setminus \{0\}$. Sei $v_k = (k, 0, 0)$, also $v_k = ke$. Dann ist $B_k := \{v_k, e_2, e_3\}$ eine Basis von V.

  Beweis: Laut (2.2.13) genügt zu zeigen: B_K linear unabhängig; und dies folgt aus (2.2.3). Damit gibt es automatisch auch unendlich viele Basen, falls K unendlich ist.

- Sei V ein $\mathbb{R}$-Vektorraum der Funktionen von $[0,1]$ in $\mathbb{R}$. Sei $a \in [0,1]$. $f_a : x \mapsto 0$, falls $x \neq a$, andernfalls $f_a : x \mapsto 1$. Sei $B := \{f_x \mid x \in [0,1]\}$. Seien $k_a \in \mathbb{R}, a \in [0,1]$ und nur endlich viele $k_a = 0$. Sei $0 = \sum_{a\in[0,1]} k_a fa =: f$. Für $x \in [0,1]$ ist $f(x) = \sum_{a\in[0,1]} k_a f_a(x) = 0 = k_x f_x(x) = k_x$. Damit ist B linear unabhängig.

  Ist B eine Basis? Kein Beweis: Sei $f \in V$ mit $f(x) = 1$ für alle $x \in [0,1]$. Angenommen, es existieren $k_a \in K$, nur endliche viele ungleich 0, mit $f = \sum_{a\in[0,1]} k_a f_a$. Wähle $b \in [0,1]$ mit der Eigenschaft $k_b = 0$ (es existert ein b, da ja nur endlich viele ungleich 0 sind). $1 = f(b) = \sum_{a\in[0,1]} k_a f_a(b) = k_b f_b(b) = k_b = 0$. Damit ist $0 = 1$. Damit ist f nicht Linearkombination, damit ist B keine Basis von V.

  Damit ist V auch gleich unendlich: B ist unendlich groß und linear unabhängig, in einem endlich dimensionierten Vektorraum könnten jedoch nur $\dim V$ linear unabhängige Elemente existieren.

  Damit ist $\langle B\rangle$ ein Unterraum:

  $$\langle B\rangle = \{f \in V \mid \{x \in [0,1]\ mit\ f(x) \neq 0\} \text{ ist endlich}\}$$

2.2.17 Dimensionssatz

Seien U und W endlich erzeugte Unterräume von V. Dann gilt: $\dim U + \dim W = \dim(U + W) + \dim(U \cap W)$.

Nach (2.2.11) ist $U \cap W$ endlich erzeugt. Sei B_0 eine Basis von $U \cap W$. B_0 ist linear unabhängige Teilmenge von U. Nach (2.2.9) existiert eine Basis B_1 von M mit $B_0 \subseteq B_1$. Genauso existiert eine Basis B_2 von W mit $B_0 \subseteq B_2$. Damit ist $B_0 \subseteq B_1 \cap B_2$ und linear unabhängig in $U \cap W$. Mit (2.2.9) gilt: $B_0 = B_1 \cap B_2$. Damit folgt: $|B_1 \cup B_2| = |B_0| + |B_1 \setminus B_0| + |B_2 \setminus B_0| = |B_1| + |B_2| - |B_0| = \dim U + dimW - dim(U \cap W)$.

Es bleibt zu zeigen: $\dim(U + W) = |B_1 \cup B_2|$, also $B_\cup := B_1 \cup B_2$ ist eine Basis von $U + W$, also linear unabhängig und Erzeugendensystem.

$\langle B_\cup\rangle \leq U + W$ (nach Struktursatz). Andererseits ist $U + B = \langle B_1\rangle + \langle B_2\rangle \leq \langle B_\cup\rangle$, damit ist $\langle B_\cup\rangle = U + W$, also ist $B_\cup$ ein Erzeugendensystem.

Seien $k_b \in K, b \in B_\cup$ und

$$
\begin{aligned}
0 &= \sum_{b \in B_\cup} k_b b \\
&= \sum_{b \in B_1} k_b b + \sum_{b \in B_1 \setminus B_2} k_b b (*) \\
-\sum_{b \in B_1 \setminus B_2} k_b b &= \sum_{b \in B_1} k_b b \\
\sum_{b \in B_1 \setminus B_2} (-k_b) b &= \sum_{b \in B_1} k_b b \\
v &:= \sum_{b \in B_1 \setminus B_2} (-k_b) b \\
&= \sum_{b \in B_1} k_b b \\
v &\in U \cup W
\end{aligned}
$$

v ist Linearkombination der Elemente aus B_0. Mit der Eindeutigkeit der Darstellung als Linearkombination von B_2 folgt: $k_b = 0$ für alle $b \in B_2 \in B_0$. Damit fällt oben der rechte Summand (*) weg, damit ist $0 = \sum_{b \in B_1} k_b b$, mit der Eindeutigkeit der Darstellung als Linearkombination ist $k_b = 0$ für alle $b \in B_1$. Daraus folgt: $k_b = 0$ für alle $b \in B_1 \cup B_2$, damit ist $B_\cup$ linear unabhängig.

2.3 Unendlichedimensionale Vektorräume

2.3.1 geordnete Mengen

- Sei M mit einer Menge, R eine Ordnungsrelation (siehe (1.2)) auf M, dann ist (M, R) eine *geordnete Menge* (notiert wird z.T. $<$ für die Ordnungsrelation, obwohl dies dann die Gleichheit mit einschließt und somit als $\leq$ aufzufassen ist).

- Sei M eine geordnete Menge bezüglich $<$. Sei $a \in M$. a heißt *Minimum von M*, falls $a < x$ für alle $x \in M$.

- Sei M ein *maximales Element von M*, falls für alle $m \in M$ aus $a < m$ schon $a = m$ folgt.

- Die geordnete Menge M ist *wohlgeordnet*, wenn jede nichtleere Teilmenge von M ein Minimum besitzt.

- Sei $X \subseteq M$, $a \in M$. Dann heißt a *obere Schranke* von X, wenn $x < a$ für alle $x \in X$.
- X heißt *Abschnitt*[4] von M, falls aus $x \in X$, $m \in M$ und $m < x$ auch $m \in X$ folgt.
- $X \subseteq M$ heißt *Kette* von M, falls X wohlgeordnet ist.

Beispiele: $(\mathbb{Z}, \leq)$; $(\mathcal{P}(N), \subseteq)$

Eigenschaften:

1. Jede Teilmenge von M ist geordnet.
2. Jeder Abschnitt einer Kette ist eine Kette.
3. Für jede Kette K von M gilt für alle $a, b \in K$: $a < b$ oder $b < a$ (Lineare Ordnung).

2.3.2 Zornsches Lemma

Sei M eine geordnete Mege. Für jede Kette K aus M gelte: (*) K besitzt eine obere Schranke. Dann existiert mindestens ein maximales Element in M.

Beweis: Sei K Kette. Die Menge der oberen Schranken von K sei $\mathcal{S}(K)$. Nach (*) ist $\mathcal{S}(K) \neq \emptyset$.

- Angenommen, es existiert eine Kette K mit $\mathcal{S}(K) \subseteq K$. Wegen der Linearität folgt: $\mathcal{S}(K) = \{x\}$. Behauptung: x ist maximales Element. Sei $m \in M$ und $x < m$. Damit gilt wegen der Transitivität der Ordnungsrelation für alle $k \in K$ mit $k < x$ auch $k < m$, damit ist m obere Schranke, da aber $\mathcal{S}(K)$ nur ein Element enthält, ist $m = x$.
- Angenommen, zu jeder Kette K existiert eine obere Schranke $f(K) \notin K$. Wir führen diesen Fall zum Widerspruch[5].

  Sei K eine Kette. K heißt f-Kette, falls für jeden Abschnitt X von K mit $X \neq K$ gilt: $\min(K \setminus X) = f(X)$.

  (1) Seien K und L f-Ketten, dann ist K ein Abschnitt von L oder L ist Abschnitt von K.

  Beweis: Sei B die Vereinigung aller $X \subseteq K \cap L$ mit (*) X ist

[4] in Analysis *unterer* Abschnitt

[5] „Den Beweis hab' ich von Bender abgeschrieben...“

Abschnitt von K und von L.

Behauptung: B ist Abschnitt von K und von L. Es gilt: $B \subseteq K \cap L$. Sei $b \in B$. Es existiert ein X mit $b \in X$ und X erfüllt (*). Sei $k \in K$ mit $k < b$. Dann folgt: $k \in X \subseteq B$. Damit ist B Abschnitt von K. Analog ist B auch ein Abschnitt von L.

Ist $B = K$ oder $B = L$, so gilt die Aussage (1). Zu betrachten: $B \neq K$ und $B \neq L$ (wird zum Widerspruch geführt). $f(B)$ ist das Minimum von $K \setminus B$ und gleichzeitig das Minimum von $K \setminus L$. Also ist $f(B) \in K \cap L$.

$B \cup \{f(B)\}$ ist Abschnitt von K und von L. Daher muß $B \cup \{f(B)\} \subseteq B$ sein[6] Damit ist $f(B) \in B$, das ist aber ein Widerspruch zur Wahl von $f(B)$

(2) Sei I Indexmenge und K_i mit $i \in I$ f-Ketten von M und $F := \bigcup\limits_{i \in I} K_i$.

Behauptung: Für alle $i \in I$ ist K_i Abschnitt von F.

Beweis: Sei $x \in K_i$ und $y \in F$ mit $y < x$. Zu zeigen: $y \in K_i$. Es existiert $j \in I$ mit $y \in K_j$. Nach (1) gibt es folgende Möglichkeiten:

- K_j ist Abschnitt von K_i, damit liegt y in K_i.
- K_i ist Abschnitt von K_j, damit liegt ebenfalls y in K_i.

(3) Sei I Indexmenge und seien K_i (mit $i \in I$) f-Ketten von M; sei $F := \bigcup\limits_{i \in I} K_i$.

Behauptung: F ist f-Kette. Beweis: Sei X nichtleere Teilmenge von F. Es existiert also ein $i \in I$ mit $X \cup K_i \neq \emptyset$. Sei $u := \min(X \cap K_i)$. Sei $x \in X$, zu zeigen: $u < x$ (dann ist $u = \min X$). Es existiert ein $j \in I$ mit $x \in K_j$. Mit (1) folgt: K_i ist Abschnitt von K_j oder K_j ist Abschnitt von K_i. Aus dem ersten Fall folgt: $u < x$ oder $x < u$, daraus folgt wegen der Eigenschaften eines Abschnittes: $x \in K_i \cap X \Rightarrow u < x \Rightarrow u = x$. Im zweiten Fall folgt: $u < x$ oder $x < u$, daraus folgt $u < x \Rightarrow u = x$.

Sei X Abschitt von F unf $X \neq F$. Sei $x := \min(F \setminus X)$. Zu zeigen: $x = f(X)$. Es existiert ein $i \in I$ mit $x \in K_i$. Mit (2) folgt: K_i ist Abschnitt von F. Daraus folgt: $X \subseteq \{k \in F | k < x\} \subseteq K_i \subseteq F$. K_i ist f-Kete, d.h. $\min(K_i \setminus X) = f(X)$. D.h. $f(X) = x$.

[6] „Ich meine weder, was ich schreibe, noch was ich sage, noch was ich denke.“

Der Widerspruch: Gemäß (3) ist die Vereinigung C aller f-Ketten wieder eine f-Kette. $C \subsetneqq C \cup \{f(C)\}$, da C eine Kette ist; wir zeigen: $C_\cup := C \cup \{f(C)\}$ ist wieder eine f-Kette. Zum einen ist $C_\cup$ wohlgeordnet (da $f(C) > c \; \forall \; c \in C$ ist), zum anderen: Sei X ein Abschnitt von $C_\cup$. Damit ist X ein Abschnitt von C und $f(X) = \min(C \setminus X) = \min(C_\cup \setminus X)$. Damit ist jedoch $C_\cup$ wieder eine f-Kette, damit in C enthalten - Widerspruch![7]

2.3.3 Existenzsatz für Basen

Satz: Jeder Vektorraum besitzt eine Basis.

Beweis: Sei V ein Vektorraum. Sei $\mathcal{M}$ die Menge aller linear unabhängigen Teilmengen von V (trivialerweise nichtleer, $\emptyset \in \mathcal{M}$). Die Menge $\mathcal{M}$ ist geordnet bezüglich Inklusion (da $\mathcal{M} \subseteq \mathcal{P}(V)$). Seien $A, B \in \mathcal{M}$ mit $A < B :\Leftrightarrow A \subseteq B$.

Sei $\mathcal{K}$ eine Kette von $\mathcal{M}$. Sei $Y := \bigcup\limits_{A \in \mathcal{K}} A$. Falls Y linear unabhängig ist, ist Y eine obere Schranke von $\mathcal{K}$ in $\mathcal{M}$.

> Behauptung: Y ist linear unabhängig.
>
> Beweis: Seien $k_y \in K, y \in Y$ mit $\sum_{y \in Y} k_y y = 0$. Zu zeigen: $k_y = 0$ für alle $y \in Y$. Angenommen, es existiert ein $k_j \neq 0$. Seien $y_1, ..., y_k \in Y$, so daß genau die k_{y_1} bis k_{y_n} ungleich 0 sind, damit gilt $\sum_{i=1}^n k_{y_i} y_i = 0$.
>
> Es existieren $A_1, ..., A_n \in \mathcal{K}$ und $y_i \in A_i$. Da $\mathcal{K}$ wohlgeordnet ist, existiert ein j mit $1 \leq j \leq n$ mit $A_i \leq A_j$ für alle $i = 1, ..., n$ (obere Schranke). Dann sind $y_1, ..., y_n \in A_j$ und A_j ist linear unabhängig, damit sind also auch $y_1, ..., y_n$ linear unabhängig.
>
> Es gilt aber: $\sum_{i=1}^n k_{y_i} y_i = 0 \Rightarrow k_{y_i} = 0 \; \forall \; i$, Widerspruch zu oben.Damit gilt: $k_j = 0$, also ist Y linear unabhängig. □

Wende das Zornsche Lemma an: Es existiert ein maximales Element $B \in \mathcal{M}$. Behauptung: B ist Basis von V. Es genügt zu zeigen: $\langle B \rangle = V$.

Beweis: Angenommen, $\langle B \rangle \neq V$. Es existiert also ein $v \in V \setminus \langle B \rangle$. Sei $B^* = B \cup \{v\}$. Damit ist $B \subseteq B^*$, da aber B maximal ist, ist B^* linear abhängig. D.h. es existieren $k_b \in K, b \in B^*$, nicht alle null, so daß $0 = \sum_{b \in B^*} k_b b = k_v v + \sum_{b \in B} k_b b$. Damit ist $-k_v v = \sum_{b \in B} k_b b$ Damit ist $k_v = 0$ (da sonst $-k_v v \in \langle B \rangle$).Damit ist $\sum_{b \in B} k_b b = 0$. Da B linear unabhängig ist, ist $k_b = 0 \; \forall \; b \in B$. Damit ist $k_b = 0 \; \forall \; b \in B^*$, das widerspricht der Annahme!

[7] „Der ganze Beweis war eigentlich nur ein Ornament!“

3 Lineare Abbildungen

3.1 Definitionen

3.1.1 Homomorphismus

Sei K ein Körper, V und W Vektorräume über K. Eine Abbildung $\varphi V \to W$ heißt lineare Abbildung (Homomorphismus) von V in W, falls für alle $v, v' \in V$ und $k \in K$ gilt:

- $(v + v')\varphi = v\varphi + v'\varphi$
- $(kv)\varphi = k(v\varphi)$

3.1.2 Weitere Bezeichnungen

Sei $\varphi : V \to W$ eine lineare Abbildung.

- φ heißt *Monomorphismus*, falls φ injektiv ist.
- φ heißt *Epimorphismus*, falls φ surjektiv ist.
- φ heißt *Isomorphismus*, falls φ bijektiv ist (dann ist V isomorph zu W, schreibe $V \cong W$).
- φ heißt *Endomorphismus*[8], falls $V = W$ ist.
- φ heißt *Automorphismus*, falls $V = W$ und φ bijektiv ist.
- $\text{Kern}\varphi := \{v \in V \mid v\varphi = 0\}$
- $\text{Bild}\varphi := \{v \in V \mid v\varphi \in V\}$
- $A \subseteq V$. $A\varphi := \{a\varphi \mid a \in A\}$ (d.h. $V\varphi = \text{Bild}\varphi$)
- $U \subseteq W$, $U\varphi^{-1} := \{v \in V \mid v\varphi \in U\}$

Bemerkungen:

- φ Monomorphismus $\Leftrightarrow$ $\text{Kern}\varphi = \{0\}$
- φ Epimorphismus $\Leftrightarrow$ $\text{Bild}\varphi = W$

Beweis der ersten Eigenschaft:

[8] „...wie die Namen von Dinosauriern, die haben Sie als Kind bestimmt doch auch gerne auswendig gelernt!“

„⇒“ Seien $v \in \text{Kern}\varphi$, $v\varphi = 0$. Es gilt: $0\varphi = 0$ (siehe (3.3)). Dann ist $v = 0$ wegen der Injektivität von φ.

„⇐“ Sei $\text{Kern}\varphi = \{0\}$. Zu zeigen: Für $v, v' \in V$ und $v\varphi = v'\varphi$ ist $v = v'$. Es gilt: $(-v)\varphi = -(v\varphi)$ (siehe (3.3)). $(v - v')\varphi = (v + (-v'))\varphi = v\varphi + (-v')\varphi = v\varphi + (-(v'\varphi)) = v\varphi - v'\varphi = 0$. Damit: $(v - v')\varphi = 0$, also $v - v' \in \text{Kern}\varphi$. Damit ist $v - v' = 0 \Rightarrow v = v'$.

3.2 Beispiele

- Sei $\varphi : v\varphi = 0 \;\forall\, v \in V$. φ ist eine lineare Abbildung.
- $V = W, \varphi : v\varphi = v \;\forall\, v \in V$. φ heißt *Identität* (identische Abbildung).
- $V = \mathbb{R}^2 = W, \lambda \in [0, 2\pi], \varphi : (x, y) \mapsto (x\cos\lambda - y\sin\lambda, x\sin\lambda + y\cos\lambda)$. φ ist lineare Abbildung (Drehung um λ, Beweis siehe Script).

  $(x, y), (x', y') \in V$.

$$\begin{aligned}
((x, y) + (x', y'))\varphi &= (x + x', y + y')\varphi \\
&= ((x + x')\cos\lambda - (y + y')\sin\lambda, (x + x')\sin\lambda + (y + y')\cos\lambda) \\
&= (x\cos\lambda - y\sin\lambda, x\sin\lambda + y\cos\lambda) \\
&\quad +(x'\cos\lambda - y'\sin\lambda, x'\sin\lambda + y'\cos\lambda) \\
&= (x, y)\varphi + (x', y')\varphi
\end{aligned}$$

- V sei Vektorraum der Funktionen von $[0, 1] \to \mathbb{R}$; sei $p_n : x \mapsto x^n \;\forall\, n \in \mathbb{N}_0$ und $P := \langle p_n | n \in \mathbb{N}_0\rangle$. Sei $\varphi : P \to P$ definiert durch $f \mapsto f'$; $f \in P \Rightarrow f = \sum_{i\in\mathbb{N}_0} k_i p_i$ und $f' = \sum_{i\in\mathbb{N}_0} i k_i p_{i-1}$; dann ist φ eine lineare Abbildung.

3.3 Eigenschaften linearer Abbildungen

Sei im folgenden K ein Körper und U, V, W K-Vektorräume. Sei φ eine lineare Abbildung von V in W und ψ eine lineare Abbildung von W in U. Dann gilt:

1. $0_V = 0_W$
2. $(-v)\varphi = -(v\varphi)$
3. φ ist Monomorphismus $\Leftrightarrow \text{Kern}\varphi = \{0\}$
4. φ ist Isomorphismus $\Rightarrow \varphi^{-1}$ ist Isomorphismus
5. $\varphi\psi$ ist eine lineare Abbildung.

Beweis:

1. $0_V\varphi = (0+0)\varphi = 0\varphi + 0\varphi \Rightarrow 0\varphi = 0_W$
2. $0 = 0\varphi = (v+(-v))\varphi = v\varphi+(-v)\varphi = v\varphi+(-(v\varphi)) \Rightarrow (-v)\varphi = -(v\varphi)$
3. siehe oben
4. φ^{-1} ist leut (1.3.5) bijektiv. Seien $w, w' \in W$. $((w+w')\varphi^{-1})\varphi = w+w' = w\varphi^{-1}\varphi + w'\varphi^{-1}\varphi = (w\varphi^{-1} + w'\varphi^{-1})\varphi$ Mit der Injektivität von φ folgt: $(w+w')\varphi^{-1} = w\varphi^{-1} + w'\varphi^{-1}$

   Sei $k \in K$. $(kw)\varphi^{-1}\varphi)kw = k(w\varphi^{-1})\varphi = (kw\varphi^{-1})\varphi$, wie oben folgt: $(kw)\varphi^{-1} = k(w\varphi^{-1})$.
5. Seien $v, v' \in V$. $(v+v')\varphi\psi = ((v+v')\varphi)\psi(v\varphi + v'\varphi)\psi = v\varphi\psi + v'\varphi\psi$ (analog für die Skalarmultiplikation)

3.4 der Vektorraum Hom(V,W)

Der Vektorraum $\mathrm{Hom}(V,W)$ ist die Menge aller Linearen Abbildungen von V in W. Die Addition sei definiert als $v(\varphi+\psi) := v\varphi + v\psi\ \forall\ \varphi,\psi \in \mathrm{Hom}(V,W); v \in V$. Die Skalarmultiplikation sei definiert als $v(k\varphi) := k(v\varphi)\ \forall\ \varphi \in \mathrm{Hom}(V,W); k \in K; \in V$.

Der Vektorraum ist nicht leer, da er mindestens z.B. die *Nullabbildung* Abbildung enthält, die alle Elemente aus V auf 0_W abbildet.

Zu zeigen[9]:

1. $\varphi+\psi, k\varphi \in \mathrm{Hom}(V,W)$
2. $\mathrm{Hom}(V,W)$ abelsche Gruppe bezüglich $+$
3. Distributivgesetze

Beweis:

1. $(v+v')(\varphi+\psi) = (v+v')\varphi + (v+v')\psi = v\varphi + v'\varphi + v\psi + v'\psi = v(\varphi+\psi) + v'(\varphi+\psi)$

   $(kv)(\varphi+\psi) = (kv)\varphi + (kv)\psi = k(v\varphi + v\psi) = k(v(\varphi+\psi))$
2. Assoziativität ist offensichtlich; Neutrales Element: Nullabbildung ($v \mapsto 0$); Inverses Element $-\varphi$ zu φ: Muß $v(-\varphi) := -(v\varphi)$; es gilt: $v(\varphi + (-\varphi)) = v\varphi + (v(-\varphi)) = v\varphi - v\varphi = 0$.
3. trivial, siehe sonst Script[10]

[9]...man erinnere sich an die Literatur-/Zitate-Prüfung in der Vorlesung :)

[10]da steht auch nur, daß die weiteren Eigenschaften trivial sind...

3.4.1 Eigenschaften der Abbildungen aus Hom(V,W)

Sei $\varphi \in \text{Hom}(V, W)$. Sei $A \leq V, B \leq W$ und $T \subseteq V$. Dann gilt:

1. $A\varphi$ ist ein Unterraum von W
2. $B\varphi^{-1}$ ist ein Unterraum von V
3. $\langle T \rangle \varphi = \langle T\varphi \rangle$
4. Sei φ injektiv. T ist linear unabhängig $\Leftrightarrow$ $T\varphi$ ist linear unabhängig.

Beweis:

1. Wende (2.1.5) an: Wir zeigen: $A\varphi + A\varphi \subseteq A\varphi$ und $KA\varphi \subseteq A\varphi$. Sei $a, b \in A, k \in K$. $a\varphi + b\varphi = (a + b)\varphi \in A\varphi$ da $a + b \in A$. $k(a\varphi) = (ka)\varphi \in A\varphi$ da $ka \in A$.
2. Seien $b, b' \in B$. $b\varphi^{-1} + b\varphi^{-1} = (b + b')\varphi^{-1} \in B\varphi^{-1}$ da $b + b' \in B$. $k(b\varphi^{-1}) = (kb)\varphi^{-1} \in B\varphi^{-1}$ da $kb \in B$.
3. Wende (2.2.5) an, direkt zu zeigen.
4. φ ist injektiv. Sei T linear unabhängig. Seien $k_{t\varphi} \in K$ und $0 = \sum_{t\varphi \in T\varphi} k_{t\varphi} t\varphi$.

$$\begin{aligned} 0 &= \sum_{t\varphi \in T\varphi} k_{t\varphi} t\varphi \\ &\overset{\varphi\ injekt.}{=} \sum_{t \in T} k_{t\varphi} t\varphi \\ &\overset{Linear.}{=} \left(\sum_{t \in T} k_{t\varphi} t \right) \varphi \\ \text{mit (3.3) folgt: } 0 &= \sum_{t \in T} k_{t\varphi} t \\ \Rightarrow 0 &= k_{t\varphi}\ \forall\, t\varphi \in T\varphi \end{aligned}$$

Sei $T\varphi$ linear unabhängig. Seien $k_t \in K$ mit $t \in T$ und $0 = \sum_{t\in T} k_t t$

$$\begin{array}{rcl} 0 & = & 0\varphi \\ & = & \left(\sum\limits_{t\in T} k_t t\right)\varphi \\ & = & \sum\limits_{t\in T} k_t t\varphi \\ & \overset{\varphi \text{ injekt.}}{=} & \sum\limits_{t\varphi\varphi\in T\varphi} k_t t\varphi \\ \overset{T\varphi \text{ lin.unabh.}}{\Longrightarrow} 0 & = & k_t \ \forall\, t \in T \end{array}$$

3.4.2 Eindeutigkeitssatz für lineare Abbildungen

Sei B eine Basis von V und φ^* von B in W. Dann existiert genau eine lineare Abbildung $\varphi \in \mathrm{Hom}(V,W)$ mit $\varphi|_B = \varphi^*$, φ heußt *lineare Fortsetzung* von φ^*. Ist außerdem φ^* injektiv und $B\varphi^*$ linear unabhängig, so ist auch φ injektiv.

Beweis: Existenz von φ: Wende (2.2.6) an: Sei $v \in V$. Dann existiert $k_b \in K$ mit $v = \sum k_b b$ (und diese Darstellung ist eindeutig). Definition von $\varphi : v \mapsto \sum_{b\in B} k_b b\varphi^*$. Dann gilt: $b\varphi = b\varphi^*$. Linearität von φ:

$$\begin{array}{rl} & \left(\sum\limits_{b\in B} k_b b + \sum\limits_{b\in B} h_b b\right)\varphi \\ = & \left(\sum\limits_{b\in B} (k_b + h_b) b\right)\varphi \\ = & \sum\limits_{b\in B} (k_b + h_b) b\varphi^* \\ = & \sum\limits_{b\in B} k_b b\varphi^* + \sum\limits_{b\in B} h_b b\varphi^* \\ = & \left(\sum\limits_{b\in B} k_b b\right)\varphi + \left(\sum\limits_{b\in B} h_b b\right)\varphi \end{array}$$

Eindeutigkeit von φ: Sei $\varphi' \in \mathrm{Hom}(V,W)$ und $\varphi'|B = \varphi^*$.

$$\begin{aligned} & \left(\sum_{b\in B} k_b b\right)\varphi \\ = \; & \sum_{b\in B} k_b b\varphi^* \\ = \; & \sum_{b\in B} k_b b\varphi' \\ = \; & \left(\sum_{b\in B} k_b b\right)\varphi' \\ \Rightarrow \; & \varphi = \varphi' \end{aligned}$$

Damit ist der erste Teil gezeigt. Sei für den Zusatz φ^* injektiv und $B\varphi^*$ linear unabhängig. Es genügt nach (3.3) zu zeigen, daß $\mathrm{Kern}\varphi = \{0\}$. Sei $v \in V$ mit $v\varphi = 0$. Es gilt: $v = \sum_{b\in B} k_b b$ für geeignete $k_b \in K$;

$$\begin{aligned} 0 &= v\varphi \\ &= \left(\sum_{b\in B} k_b b\right)\varphi \\ &= \left(\sum_{b\varphi^*\in B\varphi^*} k_b b\right)\varphi \\ &= \left(\sum_{b\varphi^*\in B\varphi^*} k_b b\right)\varphi \\ &= \sum_{b\varphi^*\in B\varphi^*} k_b b\varphi^* \\ \Rightarrow k_b &= 0 \; \forall\, b \in B \\ \Rightarrow v &= 0 \end{aligned}$$

3.5 Der Isomorphiesatz

3.5.1 Isomorphiesatz

Seien V und W endlich dimensionale K-Vektorräume. Genau dann ist V isomorph zu W, wenn $\mathrm{dim}V = \mathrm{dim}W$ ist.

Beweis:

- Sei $V \cong W$. Sei $\varphi : V \to W$ Isomorphismus, sei B eine Basis von V, d.h. $\dim V = |B|$. Es gilt: $V = \langle B \rangle$. Mit (3.4.1) (3) gilt: $W = V\varphi = \langle B \rangle \varphi = \langle B\varphi \rangle$. Damit ist $B\varphi$ Erzeugendensystem von W. Mit (3.4.1) (4) folgt: $B\varphi$ ist linear unabhängig. Damit ist $B\varphi$ Basis von W, d.h. $\dim W = |B\varphi|$. Die Abbildung $\varphi|_B : B \to B\varphi$ ist bijektiv, also $|B| = |B\varphi|$.

- Sei nun $\dim V = \dim W =: n$. Sei B Basis von V, B' Basis von W, d.h. $|B| = |B'| = n$. Es existiert eine bijektive Abbildung φ^* von B in B'. Nach (3.4.2) existiert ein Homomorphismus $\varphi : V \to W$ und $\varphi|_B = \varphi^*$. injektiv. $V\varphi = \langle B \rangle \varphi \langle B\varphi \rangle = \langle B' \rangle = W$. Also ist φ auch surjektiv und damit bijektiv, also Isomorphismus.

3.5.2 Isomorphie zu K^n

Sei V endlich dimensional und $\dim V = n$. Dann gilt. $v \cong K^n$.

Beweis: Nach (3.5.1) genügt es zu zeigen: $\dim K^n = n$. Siehe dazu das Beispiel (2.2.15).

3.6 Der Homomorphiesatz

3.6.1 Dimensionssatz

Sei V endlich dimensional und $\varphi \in \mathrm{Hom}(V, W)$. Dann ist $\dim V = \dim \mathrm{Bild}\,\varphi + \dim \mathrm{Kern}\,\varphi$

Beweis: Kernφ ist Unterraum. Sei B_0 eine Basis von Kernφ. Mit (2.2.9): Es existiert eine Basis B von V mit $B_0 \subseteq B$. Sei $B_1 := B \setminus B_0$ (somit $B = B_1 \cup B_0$). $V\varphi = \langle B \rangle \varphi = \langle B\varphi \rangle = \langle B_1\varphi \rangle$. $B_1\varphi$ ist Erzeugendensystem von $V\varphi$.

$\varphi|_{B_1}$ ist injektiv, sonst existiert $b, b' \in B_1, b \neq b'$ und $b\varphi = b'\varphi$. Damit folgt: $b\varphi - b'\varphi = 0 \Rightarrow (b - b')\varphi = 0 \Rightarrow u := b - b' \in$Kern$\varphi$. Dies ist ein Widerspruch- zur Eindeutigkeit der Darstellung als Linearkombination (u zum einen als $b - b'$, zum anderen als Linearkombination der Basis B_0 darstellbar)! Also ist $\varphi|_{B_1}$ injektiv.

$\varphi|_{\langle B_1 \rangle} : \langle B_1 \rangle \to V\varphi$ mit B_1 linear unabhängig und $\varphi|_{\langle B_1 \rangle}$ ist injektiv. Mit (3.4.1) folgt: $B_1\varphi$ linear unabhängig. Daher: $B_1\varphi$ ist Basis von $V\varphi$. Also $\dim V\varphi = |B_1\varphi| = |B_1|$. Damit folgt: $\dim V = |B| = |B_1| + |B_0| = \dim V\varphi + \dim \mathrm{Kern}\varphi$.

3.6.2 Nebenklassen

Sei U Unterraum von V, $v \in V$. Dann ist $v + U := \{v + u \mid u \in U\}$ heißt *Nebenklasse* (oder *Restklasse*) von U in V. Die Menge der Nebenklassen ist V/U (sprich V modulo U).

3.6.3 Nebenklassen als Äquivalenzklassen

Sei U Unterraum von V und $R := \{(v, w) \in V \times V \mid v - w \in U\}$. Dann ist R eine Äquivalenzrelation auf V und V/U ist die Menge der Äquivalenzklassen von R.

Beweis: Seien $v, w, z \in V$

- Reflexivität: zu zeigen: $(v, v) \in R$. Dies folgt direkt aus $v - v \in U$, da U Unterraum.
- Symmetrie: zu zeigen: $(v, w) \in R \Rightarrow (w, v) \in R$. Sei $(v, w) \in R$. Dann ist $v - w \in U$. Da U Unterraum, ist auch $-(v - w) \in U$, damit $(w, v) \in R$.
- Transitivität: seien $(v, w), (w, z) \in R$, d.h. $v - w, w - z \in U$, d.h. $v - w + w - z = v - z \in U$, da U Unterraum, d.h. $(v, z) \in R$.

Sei A die Äquivalenzklasse, die v enthält. $A = \{w \in V \mid v - w \in U\} = \{v + u \mid u \in U\} = v + U$

3.6.4 Beispiel, Faktorraum

Wir definieren eine Vektorraum-Struktur auf V/U, die V/U zu einem K-Vektorraum macht.

Für $v + U, w + U \in V/U$ und $k \in K$ definiere:

- Addition: $(v + U) + (w + U) := (v + w) + U$
- Skalarmultiplikation: $k(v + U) = (kv) + U$

Zu prüfen[11]: Sind Addition und Multiplikation Abbildungen?

- D.h. folgt aus $v + U = v' + U$ und $w + U = w' + U$ auch $(v + U) + (w + U) = (v' + U) + (w' + U)$? Zu zeigen: $(v + w) + U = (v' + w') + U$, zu zeigen also, daß die Äquivalenzklassen ein gemeinsames Element haben (dann sind sie gleich). Es gilt: $v + U = v' + U \Rightarrow v - v' \in U$ und $w + U = w' + U \Rightarrow w - w' \in U$. Da U ein Unterraum ist, ist $v - v' + w - w' \in U$. Dies ist gleich $v + w - (v + w') \in U$. Daraus folgt $(v' + w') \in ((v + w) + U) \cap ((v' + w') + U) \Rightarrow (v + w) + U = (v' + w') + U$.

[11] „kurzer Rede, langer Sinn...“

- genauso für Skalarmultiplikation: zu zeigen: $v + U = v' + U \Rightarrow ku + U = kv' + U$. $v - v' \in U$, da U Unterraum ist: $k(v - v') = kv - kv' \in U$.

Zu überprufen sind die Vektorraumaxiome, diese lassen sich aus entsprechenden Axiomen in V herleiten, exemplarisch: neutrales Element bezüglich Addition: $0 + U$; inverses Element zu $v + U$: $(-v) + U$ etc.

V/U heißt *Faktorraum* von V nach U.

Sei $\varphi : V \to V/U$ mit $v \mapsto v + U$. Dann ist φ der *natürliche (kanonische) Homomorphismus* von V in V/U.

Beweis:

- Linearität der Addition: $(v + w)\varphi = (v + w) + U = (v + U) + (w + U) = v\varphi + w\varphi$
- Linearität der Multiplikation: $(kv)\varphi = (kv) + U = k(v + U) = k(v\varphi)$

$\text{Kern}\varphi = \{v \in V \mid v\varphi = 0\} = \{v \in V \mid v + U = 0 + U\} = U$

$\text{Bild}\varphi = V/U$

3.6.5 Homomorphiesatz

Sei $\varphi \in \text{Hom}(V, W)$ surjektiv. Dann gilt $V/\text{Kern}\varphi \cong W$. Zur Erinnerung: $V/\operatorname{Kern}\varphi = \{v + \operatorname{Kern}\varphi \mid v \in V\}$ und $(v + \operatorname{Kern}\varphi) + (w + \operatorname{Kern}\varphi) = (v + w) + \operatorname{Kern}\varphi$ und $k(v \operatorname{Kern}\varphi) := (kv) + \operatorname{Kern}\varphi$

Beweis: Sei $\tilde{\varphi} : V/\operatorname{Kern}\varphi \to W$ definiert durch $v + \operatorname{Kern}\varphi \mapsto v\varphi$ ($\tilde{\varphi}$ heißt der von φ *induzierte Homomorphismus*). Zu zeigen: Ist $\tilde{\varphi}$ eine Abbildung[12] und ist sie linear?

Mit (3.3) gilt: $v\varphi = v'\varphi \Leftrightarrow v - v' \in \operatorname{Kern}\varphi \Leftrightarrow v + \operatorname{Kern}\varphi = v' + \operatorname{Kern}\varphi$, die Abbildung ist also wohldefiniert und injektiv. Die Surjektivität folgt aus der Surjektivität von φ.

Zudem gilt: $((v+\operatorname{Kern}\varphi)+(w+\operatorname{Kern}\varphi))\tilde{\varphi} = ((v+w)+\operatorname{Kern}\varphi)\tilde{\varphi} = (v+w)\varphi = v\varphi + w\varphi = (v + \operatorname{Kern}\varphi)\tilde{\varphi} + (w + \operatorname{Kern}\varphi)\tilde{\varphi}$ Damit ist die Linearität bewiesen.

3.6.6 Folgerungen

Sei $\varphi \in \text{Hom}(V, W)$. Dann ist $V/\operatorname{Kern}\varphi \cong V\varphi$.

Beweis: Betrachte φ als Homomorphismus von V in $\text{Bild}\varphi(= V\varphi)$. Mit (3.6.5) folgt: $V/\operatorname{Kern}\varphi \cong V\varphi$.

[12] wegen der verschiedenen Darstellungsmöglichkeiten der Menge $v + \operatorname{Kern}\varphi$

3.6.7 Dimensionssatz

Sei V endlich dimensional und U Unterraum von V. Dann gilt: $\dim V/U = \dim V - \dim U$.

Beweis: Betrachte die naturliche Abbildung $\varphi : V \to V/U$. φ ist surjektiv und $\operatorname{Kern}\varphi = U$. Mit (3.6.1) folgt: $\dim V = \dim \operatorname{Bild}\varphi + \dim \operatorname{Kern}\varphi$ und $\dim V = \dim V/U + \dim U$.

4 Matrizen

Seien V, W endlich dimensionale Vektorräume über K. Sei $B_1 = \{v_1, ..., v_n\}$ eine Basis von V (mit $n = \dim V$) und $B_2 = \{w_1, ..., w_m\}$ eine Basis von W (mit $m = \dim W$). Sei $\varphi \in \mathrm{Hom}(V, W)$. Mit (3.4.2) gilt: $\varphi|_{B_1}$ legt φ eindeutig fest. Für alle $i \in \{1, ..., n\}$ ist: $v_i\varphi = \sum_{j=1}^{m} a_{ij}w_j$ für geeignete $a_{ij} \in K$.

$$(a_{ij})_{n\times m} := \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix}$$

Die Abbildung φ ist eindeutig bestimmt durch die Matrix $(c_{ij})_{n\times m}$ (bei gegebenen Basen B_1, B_2). Wir schreiben: $M(\varphi, B_1, B_2) := (c_{ij})_{n\times m}$. $\mathcal{M}_{n\times m}(K)$ ist die Menge der $n \times m$-Matrizen mit Koeffizienten aus K (analog $\mathcal{M}_{n\times m}(\mathbb{Z})$ ganz selten mal).

In der n-ten Zeile stehen die Skalare der Linearkombination des n-ten Basisvektors

Beispiele:

- $n = 2, m = 3$, $v_1\varphi = w_1 + w_2 + w_3$ und $v_2\varphi = w_1 + w_2$, dann ist $M(\varphi, B_1, B_2) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$.
- Für $B_1' = \{v_1, v_1 + v_2\}$ ist $M(\varphi, B_1', B_2) = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 1 & 2 \end{pmatrix}$
- Sei $n = m$, $V = W$. Es gilt $v_i\varphi = v_i = \sum_{j=1}^{m} a_{ij}w_j$ für alle $i \in \{1, ..., n\}$. Es gilt aber

  $$M(id, B_1, B_2) = (a_{ij})_{n\times n} := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

  nur dann, wenn „$B_1 = B_2$“[13] ist![14] !
- Für $n = m = 1$ ist $\mathcal{M}_{1\times 1}(K) = \{\, (a)_{1\times 1} \mid a \in K\}$.
- Für $n = 1$ ist $\mathcal{M}_{1\times m}(K) = \{\, (a_{11} \cdots a_{1m})_{1\times m} \mid a_{ij} \in K\}$.[15]

[13] nicht nur gleiche Mengen, sondern auch bezüglich der Indizierung geordnet!
[14] „Wir haben den Boden der Trivialität noch nicht erreicht!“
[15] „Es kommt nicht darauf an, ob wir Kommas dazwischensetzen oder alle Zahlen grün färben!“

- Für $m = 1$ ist $\mathcal{M}_{n\times n}(K) = \left\{ \left(\begin{array}{c} a_{11} \\ \vdots \\ a_{n1} \end{array} \right)_{1\times m} \middle| \; a_{ij} \in K \right\}$.

4.1 Addition und Multiplikation von Matrizen

Gesucht: Summe/Produkt von zwei Matrizen, so daß diese der Matrix zur Summe/zum Produkt der linearen Abbildungen gehört.[16]

Seien V, W endlich dimensionale Vektorräume über K. Sei $B_1 = \{v_1, ..., v_n\}$ eine Basis von V (mit $n = \dim V$) und $B_2 = \{w_1, ..., w_m\}$ eine Basis von W (mit $m = \dim W$).

4.1.1 Abbildung von Hom in $\mathcal{M}$

Die Zuordnung $\varphi \mapsto M(\varphi, B_1, B_2)$ definiert eine bijektive Abbildung ϱ von $\mathrm{Hom}(V, W)$ in $\mathcal{M}_{n\times m}(K)$.

Beweis: Wende (3.4.2) an: $\varphi \mapsto M(\varphi, B_1, B_2)$. $A = (a_{ij})_{n\times m} \; : \; \exists \varphi \in \mathrm{Hom}(V, W)$ mit $A = M(\varphi, B_1, B_2)$. $v_1\varphi := \sum_{j=1}^m a_{ij} w_j$ für alle $i \in \{1, ..., n\}$.

Diese Abbildung ϱ ist bezüglich der folgenden Addition und Skalarmultiplikation auf $\mathcal{M}_{n\times m}(K)$ ein Vektorraum-Isomorphismus (laut Definition bijektiv und lauf der nachfolgenden Definition der Addition und Skalarmultiplikation auch linear).

4.1.2 Addition von Matrizen

Sei $\varphi, \psi \in \mathrm{Hom}(V, W)$. $M(\varphi, B_1, B_2) =: (a_{ij})_{n\times m}$ und $M(\psi, B_1, B_2) =: (b_{ij})_{n\times m}$. Gesucht ist $M(\varphi + \psi, B_1, B_2)$.

Es ist $v(\varphi + \psi) = \sum_{j=1}^m d_{ij} w_j$ für geeignete und eindeutig bestimmte d_{ij}. $v(\varphi + \psi) = v\varphi + v\psi = \sum_{j=1}^m a_{ij} w_j + \sum_{j=1}^m b_{ij} w_j = \sum_{j=1}^m (a_{ij} + b_{ij}) w_j$, daher: $d_{ij} = a_{ij} + b_{ij}$.

$$\begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix} + \begin{pmatrix} b_{11} & \cdots & b_{1m} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nm} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & \cdots & a_{1m} + b_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} + b_{n1} & \cdots & a_{nm} + b_{nm} \end{pmatrix}$$

[16] „Wir stellen uns - wie immer in dieser Vorlesung - dumm, ich sehe, das fällt Ihnen nicht schwer!“

4.1.3 Skalarmultiplikation bei Matrizen

Sei $\varphi \in \mathrm{Hom}(V, W)$ und $k \in K$. $M(\varphi, B_1, B_2) =: (a_{ij})_{n\times m}$.
$v_i(k\varphi) = k(v_i\varphi) = k \sum_{j=1}^{m} a_{ij}w_j = \sum_{j=1}^{m} ka_{ij}w_j \Rightarrow M(k\varphi, B_1, B_2) = (ka_{ij})_{n\times m}$

$$k \cdot \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix} = \begin{pmatrix} ka_{11} & \cdots & ka_{1m} \\ \vdots & \ddots & \vdots \\ ka_{n1} & \cdots & ka_{nm} \end{pmatrix}$$

4.1.4 Multiplikation von Matrizen

Seien die folgenden Bezeichnungen gegeben:

- V, W, U endlich dimensionale Vektorräume über K.
- $B_1 = \{v_1, ..., v_n\}$ eine Basis von V (mit $n = \dim V$)
- $B_2 = \{w_1, ..., w_m\}$ eine Basis von W (mit $m = \dim W$)
- $B_3 = \{u_1, ..., u_r\}$ eine Basis von W (mit $r = \dim U$)
- $\varphi \in \mathrm{Hom}(V, W)$, $\psi \in \mathrm{Hom}(W, U)$, damit auch $\varphi\psi \in \mathrm{Hom}(V, U)$
- $(a_{ij})_{n\times m} := M(\varphi, B_1, B_2)$
- $(b_{ij})_{m\times r} := M(\varphi, B_2, B_3)$
- $(c_{ij})_{n\times r} := M(\varphi, B_1, B_3)$

$$
\begin{aligned}
v_1\varphi\psi &= \left(\sum_{k=1}^{m} a_{ik}w_k\right)\psi \\
&= \sum_{k=1}^{m} a_{ik}(w_k\psi) \\
&= \sum_{k=1}^{m} \left(a_{ik}\sum_{j=1}^{r} b_{kj}u_j\right) \\
&= \sum_{j=1}^{r}\sum_{k=1}^{m} a_{ik}b_{kj}u_j \\
&= \sum_{j=1}^{r}\left(\sum_{k=1}^{m} a_{ik}b_{kj}\right)u_j \\
\Rightarrow c_{ij} &= \sum_{k=1}^{m} a_{ik}b_{kj}
\end{aligned}
$$

Allgemein: Für $(a_{ij})_{n\times m} \in \mathcal{M}_{n\times m}(K)$ und $(b_{ij})_{m\times r} \in \mathcal{M}_{m\times r}(K)$ definieren wir:

$$(c_{ij})_{n\times r} := (a_{ij})_{n\times m} \cdot (b_{ij})_{m\times r} \text{ mit } c_{ij} := \sum_{k=1}^{m} a_{ik}b_{kj}$$

Beispiel[17]:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22} \\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22} \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

4.1.5 Distributivität

Sei[18] $\varphi \in \mathrm{Hom}(V,W), \psi \in \mathrm{Hom}(W,U)$. Dann ist $M(\varphi,\psi,B_1,B_3) = M(\varphi,B_1,B_2)M(\psi,B_2,B_3)$. Ist $U = V = W$ und ϱ wie in (4.1.1), so gilt: $(\varphi\psi)\varrho = (\varphi\varrho)(\psi\varrho)$.

4.1.6 Lineare Abbildungen bei kanonischen Basen

Sei $V = K^n, B_1' = \{e_1, ..., e_n\}$ kanonische Basis und $W = K^m, B_2' = \{f_1, ..., f_m\}$ kanonische Basis [19]. Sei $\varphi \in \mathrm{Hom}(K^n, K^m)$ und $(a_{ij})_{n\times m} := M(\varphi, B_1', B_2')$.

[17] im Prinzip: $c_{ij} = Zeile_i \times Spalte_j$

[18] „Mathematik ist das *Vermeiden* von Rechnen, nicht umgekehrt, wie manche Leute glauben!"

[19] „Über Konventionen sollten Sie sich immer hinwegsetzen!"

$$\begin{aligned}
(k_1, ..., k_n)\varphi &= \left(\sum_{i=1}^{n} k_i e_i\right)\varphi \\
&= \sum_{i=1}^{n} k_i e_i \varphi \\
&= \sum_{i=1}^{n} k_i \left(\sum_{j=1}^{m} a_{ij} f_j\right) \\
&= \sum_{j=1}^{m} \left(\sum_{i=1}^{n} k_i a_{ij}\right) f_j \\
&= \left(\sum_{i=1}^{n} k_i a_{i1}, ..., \sum_{i=1}^{n} k_i a_{im}\right) \\
&\triangleq (k_1 ... k_n)_{1\times n} (a_{ij})_{n\times m}
\end{aligned}$$

Dieser Rechenweg funktioniert nur bezüglich der kanonischen Basis! **!**

4.1.7 Basistransformationssatz

Wie gehabt: $V, B_1, \tilde{B}_1$ weitere Basis; ebenso $W, B_2, \tilde{B}_2$ weitere Basis. Sei $\varphi \in \mathrm{Hom}(V, W)$, und id_V und id_W identische Abbildungen auf V bzw. W.

$$\begin{aligned}
\varphi &= id_V \varphi id_W \\
M(\varphi, \tilde{B}_1, \tilde{B}_2) &= M(id_V(\varphi id_W), \tilde{B}_1, \tilde{B}_2) \\
&= M(id_v, \tilde{B}_1, B_1) \cdot M(\varphi id_W, B_1, \tilde{B}_2) \\
&= M(id_v, \tilde{B}_1, B_1) \cdot M(\varphi, B_1, B_2) \cdot M(id_W, B_2, \tilde{B}_2)
\end{aligned}$$

Satz: Sei $\tilde{B}_1$ eine weitere Basis von V und $\tilde{B}_2$ eine weitere Basis von W. Es gilt:

$$M(\varphi, \tilde{B}_1, \tilde{B}_2) = M(id_v, \tilde{B}_1, B_1) \cdot M(\varphi, B_1, B_2) \cdot M(id_W, B_2, \tilde{B}_2)$$

Beispiel: $n=2, m=3$, $\tilde{B}_1 := \{v_1+v_2, v_2\}$ und $\tilde{B}_2 := \{w_1+w_2, w_2, w_2+w_3\}$; $v_1\varphi := w_1+w_2$, $v_2\varphi := w_2+w_3$. Dann gilt: $(v_1+v_2)\varphi = w_1+2w_2+w_3$.

$$\begin{aligned}
M(\varphi, B_1, B_2) &= \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \\
M(\varphi, \tilde{B}_1, \tilde{B}_2) &= \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \\
M(id_V, \tilde{B}_1, B_1) &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\
M(id_W, B_2, \tilde{B}_2) &= \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix}
\end{aligned}$$

$$\begin{aligned}
M(\varphi, \tilde{B}_1, \tilde{B}_2) &= M(id_V, \tilde{B}_1, B_1) \cdot M(\varphi, B_1, B_2) \cdot M(id_W, B_2, \tilde{B}_2) \\
&= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}
\end{aligned}$$

weiteres Beispiel: Wir wissen: $V \cong K^n$ und $W \cong K^m$. Seien wieder $B_1' = \{e_1, ..., e_n\}$ kanonische Basis von V und $B_2' = \{f_1, ..., f_m\}$ kanonische Basis von W. Sei $\tau_V : v_i \mapsto e_i$ und $\tau_W : w_i \mapsto f_i$ Laut Forsetzungssatz: τ_V, τ_W beschreiben Isomorphismen $V \to K^n$ bzw. $W \to K^n$.

$$\boxed{\begin{array}{ccc} V & \xrightarrow{\varphi} & W \\ \tau_V \downarrow & & \downarrow \tau_W \\ K^n & \overset{M(\varphi,B_1,B_2)}{\dashrightarrow} & K^m \end{array}}$$

Es gilt: $\varphi \cdot \tau_W = \tau_V \cdot M(\varphi, B_1, B_2)$, also:

$$v\varphi = v\tau_V \cdot M(\varphi, B_1, B_2)\tau_W^{-1}$$

Sei $(a_{ij})_{n\times m} := M(\varphi, B_1, B_2)$.

$$\begin{aligned}
v_i\varphi\tau_W &= \left(\sum_{j=1}^{n} a_{ij}w_j\right)\tau_W \\
&= \sum_{j=1}^{n} a_{ij}w_j\tau_W \\
&= \sum_{j=1}^{n} a_{ij}f_j \\
&= (a_{i1}, ..., a_{im}) \\
(v_i\tau_V)\cdot M(\varphi, B_1, B_2) &= e_i \cdot M(\varphi, B_1, B_2) \\
&= (0, ..., 1, ..., 0)_{1\times n}\cdot(a_{ij})_{n\times m} \\
&= (a_{i1}, ..., a_{im})
\end{aligned}$$

Anwendung: Sei $(a_{ij})_{n\times m} := M(\varphi, B_1, B_2)$ gegeben. Was ist das Bild von v unter φ?

$$\sum_{i=1}^{n} k_iv_i = v \overset{\tau_V}{\mapsto} (k_1, ..., k_n) \overset{(a_{ij})_{n\times m}}{\mapsto} (h_1, ..., h_m) \overset{\tau_W^{-1}}{\mapsto} v\varphi = \sum_{i=1}^{m} h_iw_i$$

4.2 Invertierbare Matrizen

4.2.1 Einheitsmatrix

Sei $\delta_{ij} = \begin{cases} 1 & \text{falls } i = j \\ 0 & \text{sonst} \end{cases}$. Sei $I_{n\times n} \in \mathcal{M}_{n\times n}(K)$ mit $I_{n\times n} = (\delta_{ij})_{n\times n}$. Offensichtlich gilt: $AI_{n\times n} = I_{n\times n}A = A$ für alle $A \in \mathcal{M}_{n\times n}(K)$. I heißt die Einheitsmatrix von $\mathcal{M}_{n\times n}(K)$.

4.2.2 inverse Matrix

Die Matrix $A \in \mathcal{M}_{n\times n}(K)$ heißt *invertierbar*, falls ein $X \in \mathcal{M}_{n\times n}(K)$ existiert mit $AX = XA = I_{n\times n}$. Dann ist auch X invertierbar und eindeutig bestimmt. Eindeutigkeit: Sei $AX' = X'A = I_{n\times n}$. Es gilt: $X' = X'I_{n\times n} = X'(AX) = (X'A)X = I_{n\times n}X = X$. X heißt die zu A *inverse Matrix* und wird mit A^{-1} bezeichnet.

4.2.3 invertierbare Matrix $\mapsto$ Isomorphismus

Folgende Aussagen sind äquivalent:

(a) φ ist Isomorphismus

(b) φ ist injektiv und $B_i\varphi$ ist Basis von W

(c) $n = m$, und $M(\varphi, B_1, B_2)$ ist invertierbar

BEWEIS:

$(a) \Rightarrow (b)$ φ Isomorphismus $\Rightarrow \varphi$ injektiv; mit (3.4.1) (d) $\Rightarrow B_1\varphi$ linear unabhängig; mit $W = \langle B_1\varphi\rangle$ folgt: $B_1\varphi$ ist Basis.

$(b) \Rightarrow (c)$ φ injektiv $\Rightarrow |B_1| = |B_1\varphi| \Rightarrow \dim V = |B_1| = |B_1\varphi| = \dim W$, d.h. $n = m$; mit (3.4.1) ist $v\varphi = \langle B_1\varphi\rangle = W \Rightarrow \varphi$ ist Isomorphismus; d.h. es existiert $\varphi^{-1} \in \mathrm{Hom}(W, V)$ mit $\varphi\varphi^{-1} = id_V$ und $\varphi^{-1}\varphi = id_W$; es gilt:

$$\begin{aligned}
I_{n\times n} &= M(\varphi\varphi^{-1}, B_1, B_1)\\
&= M(\varphi, B_1, B_2)M(\varphi^{-1}, B_2, B_1)\\
I_{n\times n} &= M(\varphi^{-1}\varphi, B_2, B_2)\\
&= M(\varphi^{-1}, B_2, B_1)M(\varphi, B_1, B_2)\\
&\Rightarrow M(\varphi, B_1, B_2) \text{ ist invertierbar.}
\end{aligned}$$

$(c) \Rightarrow (a)$ Es existiert $X \in \mathcal{M}_{n\times n}(K)$ mit $XM(\varphi, B_1, B_2) = M(\varphi, B_1, B_2)X = I_{n\times n}$. Mit (4.1.5) folgt: Es existiert $\varphi^* \in \mathrm{Hom}(W, V)$ mit $\varphi^*\varrho = M(\varphi^*, B_1, B_2) = X$.

$$\begin{aligned}
M(\varphi\varphi^*, B_1, B_1 &= M(\varphi, B_1, B_2)M(\varphi^*, B_2, B_1)\\
&= M(\varphi, B_1, B_2)X\\
&= I_{n\times n}\\
&= M(id_V, B_1, B_1)\\
\overset{(ref4.1.2)}{\Longrightarrow} \varphi\varphi^* &= id_V
\end{aligned}$$

Mit der analogen Überlegung für $M(\varphi^*\varphi, B_2, B_2)$ folgt: $\varphi^*\varphi = id_W$.

φ surjektiv: $w \in W : (w\varphi^*)\varphi = wid_w = w$; φ injektiv: $v, v' \in V$ mit $v\varphi = v'\varphi$. $v' = v'\varphi\varphi^* = v\varphi\varphi^* = vid_V = v$

4.2.4 Gruppe der invertierbaren Matritzen

$GL_n(K)$: Menge der invertierbaren Matrizen aus $\mathcal{M}_{n\times n}(K)$; $GL(V)$: Menge der invertierbaren Elemente aus $\mathrm{Hom}(V, V)$

$GL(V)$ und $GL_n(K)$ sind Gruppen bezüglich der Hintereinanderausführung bzw. der Matrizenmultiplikation.

Beweis:

- $id_V \in GL(V)$, also nicht leer
- Sind $\varphi, \psi \in GL(V)$, so ist auch $\varphi\psi \in GL(V)$
- Einselement: id_V
- Inverse zu $\varphi \in GL(V) : \varphi^{-1}$
- $I_{n\times n} \in GL_n(K)$, also nicht leer
- Sind $A, B \in GL_n(K)$, so existieren nach (4.1.5) (mit $B_1 = B_2, V = W$) $\varphi, \psi \in \mathrm{Hom}(V, V)$ mit $\varphi\varrho = A = M(\varphi, B_1, B_1)$ und $\psi\varrho = B = M(\psi, B_1, B_1)$.

  Mit (4.2.3) folgt: $\varphi, \psi \in GL(V) \Rightarrow \varphi\psi \in GL(V)$; $AB = M(\varphi\psi, B_1, B_1)$; damit folgt: AB invertierbar, also $AB \in GL_n(K)$
- Einselement: $I_{n\times n}$
- das Inverse zu $A \in GL_n(K)$ ist A^{-1}

4.2.5 Rang einer Matrix

Sei $A \in \mathcal{M}_{n\times m}(K)$.

$$A := \begin{pmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1m} \\ \vdots & & \vdots & & \vdots \\ a_{i1} & \cdots & a_{ij} & \cdots & a_{im} \\ \vdots & & \vdots & & \vdots \\ a_{n1} & \cdots & a_{nj} & \cdots & a_{nm} \end{pmatrix}$$

Dann sind $(a_{11}, ..., a_{i1}, ..., a_{n1})$ bis $(a_{1m}, ..., a_{im}, ..., a_{nm})$ Spaltenvektoren. Sei Y der von den Zeilenvektoren von A erzeugte Unterraum von K^m. Dann heißt $\dim Y$ der *Rang* von A (geschrieben $\mathrm{rg}\, A$).

Es existiert ein $\varphi \in \mathrm{Hom}(V, W)$ mit $A = M(\varphi, B_1, B_2)$. Mit (4.1.5) folgt:

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & W \\ \tau_V \downarrow & & \downarrow \tau_W \\ K^n & \overset{A}{\dashrightarrow} & K^m \end{array}$$

$K^n A = \langle e_1 A, ..., e_n A\rangle = V\varphi\tau_W$; dann ist der *Rang* $\mathrm{rg}\, A = \dim K^n A = \dim V\varphi$.

4.2.6 Rang einer Abbildung

$\dim \operatorname{Bild} \varphi = \operatorname{rg} M(\varphi, B_1, B_2)$, $\dim \operatorname{Bild} \varphi$ heißt der *Rang* von φ

4.2.7 Invertierbarkeit von $n \times n$-Matrizen

Sei $m = n$ und $A \in \mathcal{M}_{n\times n}(K)$. Genau dann ist A invertierbar, wenn $\operatorname{rg} A = n$.

Beweis: Mit (4.2.3): es existiert $\varphi \in \operatorname{Hom}(V, V)$ mit $A = M(\varphi, B_1, B_1)$, mit (4.2.6) $\operatorname{rg} A = \dim \operatorname{Bild} \varphi$. Nach (3.6.1) $\dim \operatorname{Bild} \varphi = n \Leftrightarrow \operatorname{Kern} \varphi = \{0\} \Leftrightarrow \varphi$ isomorph. Dann folgt mit (4.2.3): A ist invertierbar.

4.2.8 Äquivalenz von Matrizen

Seien $X, Y \in \mathcal{M}_{n\times m}(K)$. X und Y heißen *äquivalent*, falls $\psi \in \operatorname{Hom}(V, W)$ und Basen $B_1, \tilde{B}_1$ von V und $B_2, \tilde{B}_2$ von W existieren mit $X = M(\psi, B_1, B_2)$ und $Y = M(\psi, \tilde{B}_1, \tilde{B}_2)$. D.h. sie heißen äquivalent, wenn sie (unter Beachtung der Verschiedenheit von Basen) die gleiche Abbildung beschreiben.

4.2.9 Matrizen gleichen Ranges

Seien $X, Y \in \mathcal{M}_{n\times m}(K)$. Dann sind folgende Aussagen äquivalent:

(a) X und Y sind äquivalent

(b) $\operatorname{rg} X = \operatorname{rg} Y$

(c) es existieren Matrizen $T \in Gl_n(K), S \in Gl_m(K)$ mit $X = TYS$

Beweis:

(a) $\Rightarrow$ (b) Folgt aus (4.2.6).

(b) $\Rightarrow$ (c) Sei $r := \operatorname{rg} X = \operatorname{rg} Y$. Mit (4.2.3) existiert $\psi \in \operatorname{Hom}(V, W)$ mit $X = M(\psi, B_1, B_2)$. Mit (3.6.1) + (4.2.6)[20] $\dim V = r + \dim \operatorname{Kern} \psi$. Nach (2.2.9) gilt: es exisitert eine Basis $\tilde{B}_1$ von V, $\tilde{B}_1 = \{\tilde{v}_1, ..., \tilde{v}_n\}$ mit $\{\tilde{v}_{r+1}, ..., \tilde{v}_n\}$ Basis von $\operatorname{Kern} \psi$. $U := \langle \tilde{v}_1, ..., \tilde{v}_r \rangle$. Nach (2.2.6) folgt: $U \cap \operatorname{Kern} \psi = \{0\}$. Das heißt: $\psi|_B$ ist injektiv. Mit (3.4.1) folgt: $\tilde{v}_1\psi, ..., \tilde{v}_r\psi$ linear unabhängig. Mit (2.2.9) existiert eine Basis $\tilde{B}_2 = \{\tilde{w}_1, ..., \tilde{w}_m\}$ von W mit $\tilde{w}_i = \tilde{v}_i\psi$ für $i \leq r$.

[20] Gilt eigentlich (3.3.1) + (4.2.3) = (7.5.4)?

$$(a_{ij})_{n\times m} = M(\psi, \tilde{B}_1, \tilde{B}_2) = \begin{pmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & \cdots & 0 \\ 0 & 0 & \ddots & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 1 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & \cdots & 0 \end{pmatrix}$$

$$a_ij = \begin{cases} \delta_{ij} & \text{falls } i \leq r \\ 0 & \text{sonst} \end{cases}$$

Mit (4.1.7) + (4.2.3) folgt: $S = M(\mathrm{id}_V, \tilde{B}_1 B_1) \in GL_n(K), T = M(\mathrm{id}_W, B_2, \tilde{B}_2) \in GL_m(K)$, $SXT = M(\psi, \tilde{B}_1, \tilde{B}_2)$. Genauso für Y: Es existiert $\hat{\psi} \in \mathrm{Hom}(V, W)$ und Basen $\hat{B}_1, \hat{B}_2$ von V bzw. W und $\hat{S} \in GL_n(K), \hat{T} \in GL_m(K)$ mit $M(\hat{\psi}, \hat{B}_1, \hat{B}_2) = (a_{ij})_{n\times m} = M(\psi, \tilde{B}_1, \tilde{B}_2)$

$$\begin{aligned} \hat{S}Y\hat{T} &= M(\hat{\psi}, \hat{B}_1, \hat{B}_2) \\ \Rightarrow \hat{S}Y\hat{T} &= SXT \\ \Rightarrow S^{-1}\hat{S}Y\hat{T}T^{-1} &= S^{-1}SXTT^{-1} \\ \Rightarrow (S^{-1}\hat{S})Y(\hat{T}T^{-1}) &= X \end{aligned}$$

(c) $\Rightarrow$ (a) Mit (4.2.3) existiert $\lambda \in \mathrm{Hom}(V, V)$ mit $M(\lambda, B_1, B_1) = T$. Aus (4.2.6) folgt: λ ist invertierbar, d.h. $B_1\lambda$ ist Basis von V. $M(\mathrm{id}_V, B_1\lambda, B_1) = T$. Genauso: Ex existiert $\mu \in \mathrm{Hom}(W, W)$ und $M(\mu, B_2, B_2) = S^{-1}$ und $M(id_W, B_2\mu, B_2) = S^{-1}$. $M(id_W, B_2\mu, B_2)M(\mathrm{id}_W, B_2, B_2\mu) = I_{m\times m}$. Aus (4.2.4) folgt: $M(\mathrm{id}_W, B_2, B_2\mu) = S$. Sei $Y = M(\psi, B_1, B_2)$. Zudem: $X = TYS = M(id_V, B_1\lambda, B_2)M(\psi, B_1, B_2)M(id_W, B_2, B_2\mu) = M(\psi, B_1\lambda, B_2\mu)$. Damit: X und Y sind äquivalent.

4.2.10 transponierte Matrix

Sei $A = (a_{ij})_{n\times m} \in \mathcal{M}_{n\times m}(K)$. Definiere $A^t := (a'_{ij})_{n\times m}$ und $a'_{ij} = a_{ji}$. Dann heißt A^t die zu A *transponierte Matrix*.

$$\begin{pmatrix} 1 & 3 \\ 4 & 5 \\ 7 & 9 \end{pmatrix}^t = \begin{pmatrix} 1 & 4 & 7 \\ 3 & 5 & 9 \end{pmatrix}$$

4.2.11 Rechenregeln für transponierte Matrizen

Seien $A, B \in \mathcal{M}_{n\times m}(K), C \in \mathcal{M}_{m\times r}(K)$ und $k \in K$.

1. $(A^t)^t = A$
2. $(kA)^t = kA^t$
3. $(A+B)^t = A^t + B^t$
4. $(AC)^t = C^t A^t$
5. $(A^t)^{-1} = (A^{-1})^t$

4.2.12 Gleichrangigkeit transponierter Matrizen

Sei[21] $A \in \mathcal{M}_{n\times m}(K)$. Dann ist $\operatorname{rg} A = \operatorname{rg} A^t$

4.3 Lineare Gleichungssysteme

In diesem Abschnitt ist $A := (a_{ij})_{n\times m} \in \mathcal{M}_{n\times m}(K); b := (b_1, ..., b_m) \in K^m$. Wir interessieren uns für Lösungen des Linearen Gleichungssystems $(LG) \times A = b$, d.h. für Elemente $x \in K^n$, für die $xA = b$ gilt.

Ist $b = 0$, so heißt (LG) *homogenes Gleichungssystem*, andernfalls *inhomogen*. $(LG)_h$ ist das zu (LG) gehörende homogene Gleichungssystem (d.h. A ist gleich, aber $b = 0$).

erste Interpreation: Sei $x = (x_1, ..., x_n)$ Lösung von (LG).

$$\begin{aligned}(b_1, ..., b_n) &= (x_1, ..., x_n)(a_{ij})_{n\times m}\\ &= (\sum_{i=1}^n x_i a_{i1}, \sum_{i=1}^n x_i a_{i2}, ..., \sum_{i=1}^n x_i a_{in})\\ b_j &= \sum_{i=1}^n x_i a_{ij}\end{aligned}$$

$$\begin{array}{ccccccccc} \sum_1^n x_i a_{i1} & = & b_1 & a_{11}x_1 & + & ... & + & a_{n1}x_n \\ \sum_1^n x_i a_{i2} & = & b_1 & a_{12}x_1 & + & ... & + & a_{n2}x_n \\ \vdots & = & \vdots & \vdots & + & ... & + & \vdots \\ \sum_1^n x_i a_{im} & = & b_1 & a_{1m}x_1 & + & ... & + & a_{nm}x_n \end{array}$$

Seien B_1 und B_2 die natürlichen Basen von K^n bzw. K^m, d.h. $B_1 = \{e_1, ..., e_n\}$. Es existiert ein $\varphi \in \operatorname{Hom}(K^n, K^m)$ mit $M(\varphi, B_1, B_2) = A$. Für $v \in K^n : v\varphi = vA$.

[21] „Die fünf Minuten wollte ich Ihnen zu Weihnachten schenken, klatschen Sie doch nicht jetzt schon, sollte doch 'ne Überraschung werden!"

Die Lösungsmenge (LG) ist die Menge aller $v \in K^n$, die unter φ auf b abgebildet werden.

4.3.1 Lösungsmenge für homogene Gleichungssysteme

Die Menge der Lösungen von $(LG)_h$ ist ein Unterraum von K^n der Dimension $n - \operatorname{rg} A$.

Beweis: Sei U die Lösungsmenge von $(LG)_h$. Es ist $U = \operatorname{Kern} \varphi$, also ist es ein Unterraum von K^n. Laut Dimensionssatz (3.6.1) gilt: $n = \dim K^n = \dim \operatorname{Bild} \varphi + \dim \operatorname{Kern} \varphi$. Damit folgt: $\dim U = n - \dim \operatorname{Bild} \varphi = n - \dim \langle e_1 A, ..., e_n A \rangle = n - \operatorname{rg} A$ (nach (4.2.5))

4.3.2 Lösungsmenge für inhomogene Gleichungssysteme

Sei U der Lösungsraum von $(LG)_h$ und x eine Lösung von (LG). Dann ist $x + U$ die Menge der Lösungen von (LG).

Beweis[22]: Sei v Lösung von (LG). $(v - x)\varphi = v\varphi - x\varphi = b - b = 0 \Rightarrow$ v - x ist Lösung von $(LG)_h$. Damit ist $v - x \in U \Rightarrow v + U = x + U$, d.h. $v \in x + U$.

Sei $u \in U$. $(x + u)\varphi = x\varphi + u\varphi = b + 0 = b$, d.h. $x + u$ ist eine Lösung von (LG). Damit ist $x + U$ die Lösungsmenge von (LG).

4.3.3 Lösbarkeit von Gleichungssystemen

Sei $A^* = (a^*_{ij})_{(n+1)\times m} \in \mathcal{M}_{(n+1)\times m}(K)$ mit $a^*_{(n+1)i} = b_i$ für $i = 1, ..., m$, sonstige $a^*_{ij} = a_{ij}$.

$$A^* = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \cdots & \ddots & \cdots \\ a_{n1} & \cdots & a_{nm} \\ b_1 & \cdots & b_m \end{pmatrix}$$

Genau dann hat (LG) eine Lösung, wenn $\operatorname{rg} A = \operatorname{rg} A^*$.

Beweis:

„$\Rightarrow$“ Sei Y das Erzeugnis der Zeilenvektoren von A_j, d.h. $\operatorname{rg} A = \dim Y$, $\operatorname{Bild} \varphi = Y$. Sei $\operatorname{rg} A = \operatorname{rg} A^*$, dann folgt: $\dim Y = \operatorname{rg} A = \operatorname{rg} A^* = \dim \langle Y, b \rangle \Rightarrow Y = \langle Y, b \rangle \Rightarrow b \in Y \Rightarrow b \in \operatorname{Bild} \varphi$. Damit existiert ein $x \in K^n$ mit $x\varphi = b$, also ist x Lösung von (LG).

[22] „Der schwierigste Teil des Beweises ist, die Tafel zu wischen.“

„$\Leftarrow$“ Sei x Lösung von (LG). D.h. $x\varphi = b \Rightarrow b \in \operatorname{Bild}\varphi = Y$. $\dim Y = \dim \langle Y, b\rangle \Rightarrow \operatorname{rg} A = \operatorname{rg} A^*$.

4.3.4 Anzahl der Lösungen einen LGS

1. Ist $\operatorname{rg} A = m$, so besitzt (LG) eine Lösung.
2. Ist $\operatorname{rg} A = n$, so besitzt (LG) höchstens eine Lösung.
3. Ist $\operatorname{rg} A = n = m$, so besitzt (LG) genau eine Lösung.

Beweis:

1. folgt aus (4.3.3)
2. Sei U Lösungsunterraum von $(LG)_h$. Mit (4.3.1) folgt: $\dim U = n - \operatorname{rg} A = 0 \Rightarrow U = \{0\}$. Rest mit (4.3.2).[23]

Beispiele:

$$\begin{aligned}
(LG) &: xA = b \\
b &= (0,0,1) \\
A &= \begin{pmatrix} 3 & 4 & -7 \\ 0 & 6 & -2 \\ 3 & 10 & -9 \end{pmatrix} \\
e_3A - e_1A &= (0,6,-2) = e_2A \\
\Rightarrow \operatorname{rg} A &\leq 2 \\
\operatorname{Bild}\varphi &= \langle e_1A, e_3A\rangle
\end{aligned}$$

Das (LG) hat genau dann Lösung, wenn $(0,0,1) \in \langle (3,4,-7),(3,10,-9)\rangle$ gilt. Angenommen, $b \in \langle e_1A, e_3A\rangle$, dann existieren k_1 und k_2 mit:

$$\begin{aligned}
(0,0,1) &= k_1(3,4,-7) + k_2(3,10,-9) \\
\Rightarrow 0 &= 3k_1 + 3k_2 \\
\wedge 0 &= 4k_1 + 10k_2 \\
\wedge 1 &= -7k_1 - 9k_2
\end{aligned}$$

[23]„Ich hab' mir die Rechnerei bis zum Ende aufgehoben, dann können Sie sich amüsieren, und wenn ich nciht mehr weiterkomme, hören wir auf!“

Fallunterscheidung: Erster Fall: Gelte $\operatorname{char} K = 3$:

$$\begin{aligned} \Rightarrow 0 &= 0k_1 + 0k_2 \\ \wedge 0 &= k_1 + k_2 \\ \wedge 1 &= -k_1 \\ \Rightarrow k_1 = -1 & \\ \wedge k_2 = 1 & \end{aligned}$$

Man findet also eine Lösung. Zweiter Fall: $\operatorname{char} K \neq 3$:

$$\begin{aligned} \Rightarrow k_1 &= -k_2 \\ \wedge 6k_2 &= 0 \\ \wedge 1 &= -2k_2 \end{aligned}$$

Widerspruch zwischen den letzten beiden Zeilen: Aus der letzten Zeile folgt: $\operatorname{char} K \neq 2$ und $k_2 \neq 0$, die zweite Zeile darf jetzt durch 6 geteilt werden, dann folgt $k_2 = 0$, Widerspruchzur dritten Zeile.

Es existiert also eien Lösung bei $\operatorname{char} K = 3$, andernfall nicht.

4.3.5 Multiplikation von Gleichungssystem mit Matrix

Sei (LG) gegeben als $xA = b$ mit $A \in \mathcal{M}_{n\times m}(K)$ und $b \in K^m$. Sei $T \in \mathcal{M}_{m\times m}(K)$ invertierbar. Genau dann ist x eine Lösung von (LG), wenn x Lösung von $xAT = bT$ ist.

Beweis: x Lösung von (LG) bedeutet: $xA = b$, beide Seiten sind Element aus K^m, die Multiplikation mit T liefert $xAT = bT$. Andere Richtung: Sei x Lösung von $xAT = bT$, multipliziere mit T^{-1} und erhalte $xA = xATT^{-1} = bTT^{-1} = b$.

4.3.6 Dreiecksmatrix, Matrizen $P_{rs}^{(m)}$ und $E_{rs}^{(m)}(k)$

Sei im folgenden $n = m$, $(d_{ij})_{n\times n} := D \in \mathcal{M}_{n\times n}(K)$ heißt untere Dreiecksmatrix, falls $d_{ij} = 0$ für alle $i < j$.

$$D \hat{=} \begin{pmatrix} x & 0 & \cdots & 0 \\ x & x & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ x & x & \cdots & x \end{pmatrix}$$

Sei $P_{rs}^{(m)} := (p_{ij})_{m \times m}$ (für $1 \leq r \neq s \leq m$) definiert durch

$$p_{ij} := \begin{cases} \delta_{ij} & \text{falls} \quad j \notin \{r, s\} \\ \delta_{ir} & \text{falls} \quad j = s \\ \delta_{is} & \text{falls} \quad j = r \end{cases}$$

Die Matrix sieht folgendermaßen aus:

$$\left(\begin{array}{ccc|c|ccc|c|ccc}
1 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\
0 & \ddots & 0 & \vdots & \vdots & 0 & \vdots & \vdots & \vdots & 0 & \vdots \\
0 & 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\
\hline
0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\
\hline
0 & \cdots & 0 & 0 & 1 & 0 & 0 & 0 & 0 & \cdots & \cdots \\
\vdots & 0 & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & 0 & 0 \\
0 & \cdots & 0 & 0 & 0 & 0 & 1 & 0 & 0 & \cdots & \cdots \\
\hline
0 & \cdots & 0 & 1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\
\hline
0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 1 & \cdots & 0 \\
\vdots & 0 & \vdots & \vdots & \vdots & 0 & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 1
\end{array}\right)$$

Sei $E_{rs}^{(m)}(k) := (e_{ij})_{m \times m}$ (für $k \in K, 1 \leq r \neq s \leq m$) definiert durch

$$e_{ij} := \begin{cases} \delta_{ij} & \text{falls} \quad (i, j) \neq (r, s) \\ k & \text{sonst} \end{cases}$$

D.h. die Einheitsmatrix, bei der an der Stelle (r, s) das Element k steht.

Sei $A := (a_{ij})_{n \times m} \in M_{n \times m}(K)$. Für $C = AP^{(}_{rs}m) = (c_{ij})_{n \times m}$ gilt:

$$c_{ij} = \begin{cases} \sum_k a_{ik}\delta_{kj} & \text{falls} \quad j \notin \{r, s\} \\ \sum_k a_{ik}\delta_{kr} & \text{falls} \quad j = s \\ \sum_k a_{ik}\delta_{ks} & \text{falls} \quad j = r \end{cases} = \begin{cases} a_{ij} & \text{falls} \quad j \notin \{r, s\} \\ a_{ir} & \text{falls} \quad j = s \\ a_{is} & \text{falls} \quad j = r \end{cases}$$

Zudem ist $C' = AE_{rs}^{m}(k) = (c_{ij})_{n \times m}$ folgendes:

$$c'_{ij} = \sum_k a_{ik} e_{kj} = \begin{cases} a_{ij} & \text{falls} \quad j \neq s \\ a_{is} + k a_{ir} & \text{falls} \quad j = s \end{cases}$$

Die Matrix C' geht also aus A hervor, indem das k-fache der r-ten Spalte zur s-ten Spalte hinzugezählt.

4.3.7 Gauß'sches Eliminationsverfahren

Sei $xA = b$, $A \in \mathcal{M}_{n\times n}(K)$ ein lineares Gleichungssystem. Dann existiert eine Folge $T_1, ..., T_l$ von Matrizen der Form $P_{rs}^{(}m)$ und $E_{rs}^{(m)}(k)$, so daß $xaT_1 \cdots T_l = bT_1 \cdots T_l$ ein Lineares Gleichungssystem mit unterer Dreiecksmatrix $AT_1 \cdots T_l$ ist.

Beweis: Induktion nach n.

IV $n = 1$ nichts zu zeigen.

IA $n > 1$ und Behauptung richtig für alle (LG) mit Matrix aus $\mathcal{M}_{m\times m}(K)$ für $m < n$.

IS Wende geeignete $P_{rs}^{(m)}$ an, so daß $AP_{rs}^{(m)} = (a_{ij}^{(1)})_{ij}$ mit $a_{11}^{(1)} \neq 0$, falls nicht schon alle $a_{ij} = 0$ sind für alle j.

- Durch Anwendung geeigenter $E_{rs}^{(m)}(K)$ erhält man $a_{ij} = 0$ für $1 < j$.
- Erhalte $\tilde{A} \in \mathcal{M}_{(m-1)\times(m-1)}(K)$ durch Streichen der ersten Zeile und Spalte von A.
- Es existiert nach Induktion eine Folge $T_1', ..., T_l'$ von $(m-1) \times (m-1)$-Matrizen der Form P oder E mit $\tilde{A} = T_1' \cdots T_l'$ mit Dreiecksmatrix.
- Ist $T_i' = P_{rs}^{(m-1)}$, definiere $T_i := P_{(r+1)(s+1)}^{(m)}$.
- $\tilde{A}T_1 \cdots T_h$ untere Dreiecksmatrix.[24]

[24] „Für Informatiker ist $\frac{n(n-1)}{2}$ ja gleich n^2, genauer rechnen Informatiker ja nie."

4.3.8 Beispiel

$$
\begin{aligned}
A &= \begin{pmatrix} 1 & 1 & 2 \\ 1 & -3 & 1 \\ 1 & -3 & 2 \end{pmatrix} \\
\text{mit } E_{13}(-2) &\rightarrow \begin{pmatrix} 1 & 1 & 0 \\ 1 & -3 & -1 \\ 1 & -3 & 0 \end{pmatrix} \\
\text{mit } E_{12}(-1) &\rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 1 & -4 & -1 \\ 1 & -4 & 0 \end{pmatrix} \\
\text{mit } E_{23}(-\frac{1}{4}) &\rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 1 & -4 & 0 \\ 1 & -4 & 1 \end{pmatrix} \\
b &= (1,2,1) \\
\text{mit } E_{13}(-2) &\rightarrow (1,2,1) \\
\text{mit } E_{12}(-1) &\rightarrow (1,1,1) \\
\text{mit } E_{23}(-\frac{1}{4}) &\rightarrow (1,1,\frac{3}{4}) \\
\Rightarrow x \cdot \begin{pmatrix} 1 & 0 & 0 \\ 1 & -4 & 0 \\ 1 & -4 & 1 \end{pmatrix} &= (1,1,\frac{3}{4}) \\
x_3 &= \frac{3}{4} \\
x_2 &= -1? \\
x_1 &= ...
\end{aligned}
$$

5 Determinanten

5.1 Die Symmetrische Gruppe vom Grad n

Sei $\Omega = \{1, ..., n\}$. Die Symmetrische Gruppe (siehe (1.5.1), Menge der bijektiven Abbildungen bzw. Permutationen) auf Ω heißt Symmetrische Gruppe vom Grad n und wird mit Σ_n bezeichnet. Sei $x \in \Sigma_n$, x heißt *k-Zyklus*, falls k verschiedene $a_1, ..., a_k \in \Omega$ existieren mit der folgenden Eigenschaft:

1. $a_i x = a_{i+1}$ für $1 \leq i < k$
2. $a_k x = a_1$
3. $ax = a$ für alle $a \in \Omega \setminus \{a_1, ..., a_k\}$

Wir schreiben $x =: (a_1 \cdots a_k)$. k heißt die Ordnung des k-Zyklus. Alle 2-Zyklen heißen *Transpositionen*.

Zwei Zyklen $(a_1 \cdots a_k)$ und $(b_1 \cdots b_r)$ heißen *elementfremd*, wenn $\{a_1, ..., a_k\} \cap \{b_1, ..., b_r\} = \emptyset$.

Bemerkungen:

1. Die Identität ist der einzige 1-Zyklus, d.h. $1 = (1) = (3) = (n)$
2. Sei $x = (a_1 \cdots a_k) \in \Sigma_n$. Dann ist $x = (a_i \cdots a_k a_i \cdots a_{i-1})$ für alle $1 < i \leq k$[25]
3. $x^{-1} = (a_k a_{k-1} \cdots a_1)$
4. $x^k = 1$
5. Sei t Transposition von Σ_n. Dann gilt $t^2 = 1$ und $t^{-1} = t$
6. Es existiert in Σ_n kein k-Zyklus für $k > n$
7. Zu jedem $x \in \Sigma_n$ existiert ein $m \in \mathbb{N}$ mit $x^m = 1$

5.1.1 Eigenschaften von Zyklen & Transpositionen

Sei $x \in \Sigma_n$. Dann gilt:

1. Ist $x \neq 1$, so ist x Produkt von paarweise elementfremder Zyklen der Ordnung > 1.
2. x ist Produkt von Transpositionen

[25] „Wenn man das mit dem Finger macht, geht das sehr viel schneller!“

3. Sei $y = (a_1 \cdots a_k) \in \Sigma_n$. Dann ist $x^{-1}yx = (a_1x \cdots a_kx)$
4. Sind x und y elementfremde Zyklen, so gilt $yz = zy$
5. Sind t, t' Transpositionen aus aus Σ_n, so gilt $tt' = t't$ und $(tt')^2 = 1$ oder $tt't = t'tt'$ und $(tt')^3 = 1$

Beweis:

1. $F(x) := \{a \in \Omega \mid ax = a\}$, $x \neq 1$, d.h. $F(x) \neq \Sigma$. $m(x) := n - |F(x)| > 0$. Beweis durch Induktion nach $m(x)$. Induktionsverankerung: Es ist $m(x) \geq 2$. Es ist $\Omega = \{i, j\} \cup F(x)$ und $x = (ij)$. Induktionsannahme: Die Behauptung ist richtig für alle $g \neq 1$ mit $m(g) < m(x)$.

   Induktionsschluß: Sei $a \in \Omega \setminus F(x)$. Definiere $a_1 := a$ und $a_i := a_{i-1}x$ für $i > 1$ (d.h. $a_i = a_1x^{i-1}$ für $i > 1$). Es existiert $m \in \mathbb{N}$ mit $x^{m+1} = 1$, d.h. $a_1x^{m+1} = a_1$.

   Wähle $k \in \mathbb{N}$ minimal mit $a_{k+1} = a_1$. Setze $y := x(a_1 \cdots a_k)^{-1} = x(a_k \cdots a_1)$. Dann ist für $1 \leq i < k$: $a_iy = a_{i+1}(a_k \cdots a_i) = a_i$, $a_ky = a_1(a_k \cdots a_1) = a_k$, $b \in F(x), by = b(a_k \cdots a_1) = b$.

   Daraus folgt: $\{a_1, ..., a_k\} \cup F(x) \subset F(y) \Rightarrow m(y) < m(x) \Rightarrow y = x_1 \cdot x_2 \cdots x_r$ für paarweise elementfremde Zyklen $x_1, ..., x_r$. Alle Elemente aus Ω in dem Zyklus x_i sind nicht in $F(y)$.

   Damit folgt: x_i ist teilerfremd zu $(a_1 \ldots a_k)$. Es gilt $y = x(a_1 \cdots a_k)^{-1} = x_1 \cdot x_2 \cdots x_r \Rightarrow x = x_1 \cdot x_2 \cdots x_r(a_1 \cdots a_k) \Rightarrow x$ erfüllt die Eigenschaft.

2. Der Fall $x = 1$: x ist das „leere Produkt“ von Transpositionen. Der Fall $x \neq 1$: Nach (1) genügt es, (2) für einen k-Zyklus $x = (a_1 \cdots a_k)$ (mit $k \geq 2$) zu zeigen.

$$
\begin{aligned}
x &= (a_1a_2)(a_1a_3) \cdots (a_1a_k) \\
a_i((a_1a_2) \cdots (a_1a_i) \cdots (a_1a_k)) &= a_1(a_1a_{i+1}) \cdots (a_1a_k) \\
&= a_{i+1}(a_1a_{i+2}) \cdots (a_1a_k) \\
&= a_{i+1} \\
a_k((a_1a_2) \cdots (a_1a_k)) &= a_1
\end{aligned}
$$

3. x ist bijektiv. Gleichwertig also: $\Omega = \{1x, ..., nx\}$. Sei $ax \in \Omega$. Wende $x^{-1}yx$ an: $ax(x^{-1}yx) = ayx = \begin{cases} a_{i+1}x & \text{falls} \quad a = a_i, i < k \\ a_ix & \text{sonst} \end{cases} \quad a = a_kaxa \notin \{a_1, ..., a_k\}$.
   Damit folgt: $x^{-1}yx = ((a_1x)(a_2x)(a_kx))$

4. $y = (a_1 \cdots a_k), z = (b_1 \cdots b_r)$ mit $\{a_1, ..., a_k\} \cap \{b_1, ..., b_r\} = \emptyset$.
$a_i(yz) = \begin{cases} a_{i+1}z = a_{i+1} & \text{falls} \quad i < k \\ a_1 z = a_1 & \text{falls} \quad i = k \end{cases}, b_i(yz) = b_j z = \begin{cases} b_{i+1} & \text{falls} \quad j < r \\ b_1 & \text{falls} \quad j = r \end{cases},$
$c(yz) = c$ für alle $c \in \Omega \setminus \{a_1, ..., a_k, b_1, ..., b_r\}$.
$a_i(zy) = a_i y = \begin{cases} a_{i+1} & \text{falls} \quad i < k \\ a_1 & \text{falls} \quad i = k \end{cases}, b_i(zy) = \begin{cases} b_{j+1}y = b_{j+1} & \text{falls} \quad j < r \\ b_1 y = b_1 & \text{falls} \quad j = r \end{cases},$
$c(yz) = c$.

5. zu Hause oder so

5.1.2 gerade/ungerade Transpositionsdarstellungen

Sei $x \in \Sigma_n$ und seien $\tilde{t}_1, ..., \tilde{t}_k$ und $t'_1, ..., , t'_l$ Transpositionen mit $x = \tilde{t}_1 \cdots \tilde{t}_k = t'_1 \cdots t'_l$. Dann ist $k + l$ gerade (d.h. zwei verschiedene Transpositionen sind *beide* gerade oder ungerade).

Beweis: Für Transpositionen t gilt: $t^2 = 1$, damit folgt: $t = t^{-1}$.

$$\begin{aligned} \tilde{t}_1 \cdots \tilde{t}_k &= t'_1 \cdots t'_l \\ 1 &= \tilde{t}_1 \cdots \tilde{t}_k \cdot t'_1 \cdots t'_l \end{aligned}$$

Es genügt zu zeigen: 1 ist nicht Produkt von ungerade vielen Transpositionen. Widerspruchsbeweis: Angenommen, es exisiteren m (m ungerade) Transpositionen $t_1, ..., t_m$ mit $1 = t_1 \cdots t_m$ $(*)$ mit $t_i = (a_i b_i)$; $a_i, b_i \in \{1, ..., n\}$ und $a_i \neq b_i$. Wähle m minimal mit $(*)$.

Angenommen, es existiert $i \neq j \leq m$ mit $t_i = t_j$ (O.B.d.A. $i < j$).

$$\begin{aligned} 1 &= t_1 t_2 \cdots t_{i-1} \cdot t_i \cdot t_{i+1} \cdot t_{i+2} \cdots t_{j-1} \cdot t_j \cdot t_{j+1} \cdots t_m \\ &= t_1 t_2 \cdots t_{i-1} \cdot t_i \cdot t_{i+1} \cdot (t_i \cdot t_i) \cdot t_{i+2} \cdot (t_i t_i) \cdots (t_i t_i) \cdot t_{j-1} \cdot t_j \cdot t_{j+1} \cdots t_m \\ &= t_1 t_2 \cdots t_{i-1} \cdot (t_i \cdot t_{i+1} \cdot t_i) \cdot (t_i \cdot t_{i+2} \cdot t_i) \cdot t_i \cdots t_i \cdot (t_i \cdot t_{j-1} t_i) \cdot t_{j+1} \cdots t_m \end{aligned}$$

Nach (5.1.1) sind alle Klammern wieder Transpositionen. Zählt man die Transpositionen dann durch (und zählt die Klammern jeweils als eine Transposition), ist ein neues m' gefunden, das wie m ebenfalls ungerade ist[26], aber damit ist m nicht minimal.

Damit sind alle $t_1, ..., t_m$ sind verschieden $(**)$. Sei $r \leq m$ und $a_1 = a_i$ für alle $i \leq r$ und $a_1 \neq a_{r+1}$. Unter allen $t_1, ..., t_m$ mit $(*)$ und m minimal wählen wir die $t_1, ..., t_m$ noch so aus, daß r maximal wird.

[26]Hier wird die Voraussetzung benutzt, daß m ungerade ist - nur dann ist es ein Widerspruch, andernfalls ist 1 gleich der leeren Menge von Transpositionen.

Wegen $(**)$ gilt $a_1(t_1 \cdots t_r) = b_1 \neq a_1 \Rightarrow r < m$. Es ist $a_1(t_1 \cdots t_r) \neq a_1$, aber $a_1(t_1 \cdots t_m) = a_1$, also exisitert $j > r$ mit $a_1 = a_j$ oder $a_1 = b_j$.

$$\begin{aligned} 1 &= t_1 \cdots t_r \cdot t_{r+1} \cdots t_{j-1} \cdot t_j \cdots t_m \\ &= t_1 \cdots t_r \cdot (t_j \cdot t_j) \cdot t_{r+1} \cdot (t_j \cdot t_j) \cdots (t_j \cdot t_j) \cdot t_{j-1} \cdot t_j \cdots t_m \\ &= t_1 \cdots t_r \cdot t_j \cdot (t_j \cdot t_{r+1} \cdot t_j) \cdot t_j \cdots t_j \cdot (t_j \cdot t_{j-1} \cdot t_j) \cdots t_m \end{aligned}$$

mit $t_j = (a_1 b)$ mit $b = \begin{cases} b_j & \text{falls} \quad a_1 = a_j \\ a_j & \text{falls} \quad a_1 = b_j \end{cases}$.

Durch das Umsortieren kann ein neues $r' = r + 1$ gewählt werden, das widerspricht der Wahl von r als maximal.

5.1.3 Multiplikativität des Signums

Definition: Sei[27] $x \in \Sigma_n$. Sei

$$\operatorname{sgn}(x) = \begin{cases} 1 & \text{falls} \quad x \text{ Produkt von gerade vielen Transpositionen} \\ -1 & \text{falls} \quad x \text{ Produkt von ungerade vielen Transpositionen} \end{cases}$$

Signum ist wohldefiniert wegen (5.1.2). Seien $x, y \in \Sigma_n$. Dann gilt: $\operatorname{sgn}(xy) = \operatorname{sgn}(x) \cdot \operatorname{sgn}(y)$ und $\operatorname{sgn}(x^{-1}) = \operatorname{sgn}(x)$ (folgt direkt aus der Definition von Signum).

5.1.4 alternierende Untergruppe

Definition: Sei $A_n := \{x \in \Sigma_n \mid \operatorname{sgn}(x) = 1\}$ (trivial: $1 \in A_n \neq \emptyset$). Wegen (1.5.4) ist A_n eine Untergruppe. Dann heißt A_n die *Alternierende Gruppe von Grad n*.

Sei t eine Transposition aus Σ_n. Dann ist $\Sigma_n = A_n \cup t \cdot A_n$.

Beweis:

„$\subseteq$“: Sei $x \in \Sigma_n$. Mit (5.1.3) folgt: $\operatorname{sgn}(x) = 1$ ($\Rightarrow x \in A_n$) oder $\operatorname{sgn}(tx) = 1$ ($\Rightarrow tx \in A_n \Rightarrow x = t(tx) \in tA_n$).

„$\supseteq$“: trivial[28]

[27] „Mathematik ist die Wissenschaft des Leidens - aber das kennen Sie ja inzwischen ganz gut.“

[28] „Sie haben jetzt alles gelernt, was Sie schon immer über symmetrische Gruppen wissen wollten, aber sich nie zu fragen trauten!“

5.2 Determinantenfunktionen (Volumenfunktionen)

In diesem Abschnitt ist K Körper, V ein n-dimensionaler endlichdimensionaler Vektorraum über K mit $n \geq 1$. Eine Abbildung $f : V^n \to K$ heißt *Determinantenfunktion auf* V, falls gilt:

1. f ist in jeder Komponente linear, d.h. $f(v_1, ..., v_i - 1, v_i + kw_i, ..., v_n) = f(v_1, ..., v_n) + kf(v_1, ..., v_{i-1}, w_i, v_{i+1}, ..., v_n)$ für alle $1 \leq i \leq n$, $k \in K$ und $v_1, ..., v_n, w_n \in V$.

2. $f(v_1, ..., v_n) = 0$, falls $v_1, ..., v_n$ linear abhängig sind in V.

3. Es existiert eine Basis $v_1, ..., v_n$ von V mit $f(v_1, .., v_n) \neq 0$.

5.2.1 Eigenschaften von Determinantenfunktionen

Sei f eine Determinantenfunktion[29] auf V und seien $v_1, ..., v_n \in V$ und $k \in K$. Dann gilt:

1. $f(v_1, ..., v_{i-1}, v_i + kv_j, v_{i+1}, ..., v_n) = f(v_1, ..., v_n)$ für alle $i \neq j$.

2. $f(v_{1x}, ..., v_{nx}) = \text{sgn}(x) f(v_1, ..., v_n)$ für alle $x \in \Sigma_n$

3. Seien $a_{ij} \in K$ für $1 \leq i, j \leq n$ und $w_i = \sum_{j=1}^{n} a_{ij} v_j$ für $i \in \{1, ..., n\}$. Dann:

$$f(w_1, ..., w_n) = \sum_{x \in \Sigma_n} \text{sgn}(x) a_{11x} \cdots a_{nnx} \ f(v_1, ..., v_n)$$

.

BEWEIS:

1. Es gilt:

$$\begin{aligned} & f(v_1, ..., v_{i-1}, v_i + kv_j, v_{i+1}, ..., v_n) \\ = \ & f(v_1, ..., v_i, ..., v_n) + kf(v_1, ..., v_{i-1}, v_j, ..., v_{j-1}, v_j, ..., v_n) \\ = \ & f(v_1, ..., v_i, ..., v_n) + k0 \\ = \ & f(v_1, ..., v_i, ..., v_n) \end{aligned}$$

wegen des doppelten Auftauchens von v_j sind die Argumente im rechten Summanden linear abhängig und damit $kf(...) = 0$.

[29] Existenz noch nicht bewiesen...

2. Für $n = 1$ trivial[30], sei $n > 2$. Sei $t = (ij)$ Transposition mit $i < j$ und $1 \leq i, j \leq n$.

$$\begin{aligned}
& f(v_1, ..., v_n) \\
= \;& f(v_1, ..., v_{i-1}, v_i + v_j, ..., v_n) \\
= \;& f(v_1, ..., v_{i-1}, v_i + v_j, ..., v_{j-1}, v_j - (v_i + v_j), ..., v_n) \\
= \;& f(v_1, ..., v_i + v_j, ..., -v_i, ..., v_n) \\
= \;& f(v_1, ..., v_j, ..., -v_i, ..., v_n) \\
= \;& -1 \cdot f(v_1, ..., v_j, ..., v_i, ..., v_n) \\
= \;& \operatorname{sgn}(t) \cdot f(v_{1t}, ..., v_{it}, ..., v_{jt}, ..., v_{nt})
\end{aligned}$$

Sei $x \in \Sigma_n$ und $x \neq 1$. Nach (5.1.1) ist $x = t_1 \cdots t_r$ für Transpositionen $t_1, ..., t_r \in \Sigma_n$. Beweis durch Induktion nach r.

Induktionsverankerung: $r = 1$ schon gezeigt.

Induktionsannahme: $r > 1$ und die Behauptung ist für das Produkt von $r - 1$ Transpositionen richtig.

Induktionsschluß: $x' := t_1 \cdots t_{r-1}$, es gilt: $f(v_{1x'}, ..., v_{nx'}) = \operatorname{sgn}(x') f(v_1, ..., v_n)$, dann folgt:

$$\begin{aligned}
& & f(v_{1x}, ..., v_{nx}) \\
& = & f(v_{1x't_r}, ..., v_{nx't_r}) \\
& = & \operatorname{sgn}(t_r) \cdot f(v_{1x'}, ..., v_{nx'}) \\
& = & \operatorname{sgn}(t_r) \cdot \operatorname{sgn}(x') \cdot f(v_1, ..., v_n) \\
\xrightarrow{(5.1.3)} & = & \operatorname{sgn}(x) \cdot f(v_1, ..., v_n)
\end{aligned}$$

3. $w_i = \sum_{j=i}^{n} a_{ij} v_j$, $i = 1, ..., n$,

$$\begin{aligned}
f(w_1, ..., w_n) &= f(\sum_{j_1=1}^{n} a_{ij_1} v_{ij_1}, ..., \sum_{j_n=1}^{n} a_{ij_n} v_{ij_n}) \\
&= \sum_{j_1=1}^{n} \cdots \sum_{j_n=1}^{n} (a_{1j} \cdots a_{nj} \cdot f(v_{j_1}, ... v_{j_n})) \\
&= \sum_{j_1, ..., j_n} (a_{1j_1} \cdots a_{nj_n} \cdot f(v_{j_1}, ... v_{j_n}))
\end{aligned}$$

- Der Fall $\{j_1, ..., j_n\} < \{1, ..., n\}$: D.h. $\exists\, l, k \;:\; l < k$ mit $j_l = j_k$; damit $f(v_1, ..., v_{l-1}, v_l, ..., v_{k-1}, v_l, ..., v_n) = 0$.

[30] „Hm, $v_j - (v_i + v_j)$ - das ist ja so einfach, das kann sogar ich! Da kommt $-v_j$ raus!"

$\Rightarrow$ Damit ist der Summand null, falls $\{j_1, ..., j_n\} \neq \{1, ..., n\}$. Betrachte $s \mapsto j_s$, diese Abbildung ist in diesem Fall nicht bijektiv.

- Der Fall $\{j_1, ..., j_n\} = \{1, ..., n\}$: Dann ist $s \mapsto j_s$ bijektiv. Umgekehrt liefert jede bijektive Abbildung $x \in \Sigma_n$ ein n-Tupel $(1x, ..., nx)$ mit $\{1x, ..., nx\} = \{1, ..., n\}$.[31] Also ist

$$\begin{aligned} f(w_1, ..., w_n) &= \sum_{x \in \Sigma_n} (a_{11x} \cdots a_{nnx} f(v_{1x}, ..., v_{nx}) \\ &= \sum_{x \in \Sigma_n} (a_{11x} \cdots a_{nnx} f(v_1, ..., v_n) \cdot \operatorname{sgn}(x) \end{aligned}$$

5.2.2 Kriterium für Basen

Sei f eine Determinantenfunktion auf V_1 und seien $w_1, ..., w_n \in V$. Genau dann ist $w_1, ..., w_n$ eine Basis von V, wenn $f(w_1, ..., w_n) \neq 0$.

Beweis: Sei $f(w_1, ..., w_n) \neq 0$. Nach Definition sind $w_1, ..., w_n$ linear unabhängig. Mit $n = \dim V$ folgt: $w_1, ..., w_n$ ist eine Basis.

Sei nun $w_1, ..., w_n$ Basis. Nach Definition der Determinantenfunktion existiert eine Basis $v_1, ..., v_n$ mit $f(v_1, ..., v_n) \neq 0$. Dann existiert $a_{ij} \in K$ mit $v_i = \sum_{j=1}^n a_{ij} w_j$ und $i = 1, ..., n$.

Mit (5.1.1) folgt: $0 \neq f(v_1, ..., v_n) = \sum_{x \in \Sigma_n} \operatorname{sgn}(x) \cdot (a_{11x} \cdots a_{nnx} f(v_1, ..., v_n) \Rightarrow f(w_1, ..., w_n) \neq 0$.

5.2.3 Determinantenfunktion f_φ

Sei $\varphi \in \operatorname{Hom}(V, V)$ und f Determinantenfunktion auf V. Definiere $f_\varphi : V^n \to K$ durch $f_\varphi(v_1, ..., v_n) := f(v_1\varphi, ..., v_n\varphi)$.

Satz: Sei f Determinantenfunktion auf V und $\varphi \in \operatorname{Hom}(V, V)$. Ist φ bijektiv, so ist f_φ eine Determinantenfunktion auf V. Ist φ nicht bijektiv, so ist f_φ die Nullabbildung.

Beweis: f_φ ist linear in jeder Komponente (trivial). φ bildet Familien linear abhängiger Vektoren auf Familien linear abhängiger Vektoren ab, d.h. f_φ erfüllt die ersten beiden Eigenschaften aus der Definition der Determinantenfunktion.

- Sei φ bijektiv und $v_1, ..., v_n$ eine Basis von V. Damit folgt: $v_1\varphi, ..., v_n\varphi$ ist Basis. Mit (5.2.2) folgt: $f(v_1\varphi, ..., v_n\varphi) = f(v_1, ..., v_n) \neq 0$.

- Sei φ bijektiv und seien $w_1, ..., w_n \in V$. Dann ist $w_1\varphi, ..., w_n\varphi$ linear abhängig. Mit der Definition der Determinantenfunktion folgt: $0 = f(w_1\varphi, ..., w_n\varphi) = f_\varphi(w_1, ..., w_n)$. Damit ist $f_\varphi = 0$.

[31] „Ja aber das ist schön!“

5.2.4 Zusammenhang zwischen Determinantenfunktionen

Seien f_1, f_2 zwei Determinantenfunktionen auf V. Dann existiert ein $c \in K^*$ mit $f_1 = cf_2$.

Beweis: Sei $w_1, ..., w_n$ Basis von V und $c = f_1(w_1, ..., w_n)f_2(w_1, ..., w_n)^{-1}$ (beachte (5.2.2)!). Sei $u_1, ..., u_n \in V$. Dann existieren $a_{ij} \in K$ mit $\sum_{j=1}^{n} a_{ij}w_j = u_i$ für alle $i \in \{1, ..., n\}$.

$$\begin{aligned}
f(u_1, ..., u_n) &= \sum_{x \in \Sigma_n} \operatorname{sgn}(x) \cdot (a_{11x} \cdots a_{nnx} f_1(w_1, ..., w_n) \\
&= \sum_{x \in \Sigma_n} \operatorname{sgn}(x) \cdot (a_{11x} \cdots a_{nnx} c \cdot f_2(w_1, ..., w_n) \\
&= c \cdot \left(\sum_{x \in \Sigma_n} \operatorname{sgn}(x) \cdot (a_{11x} \cdots a_{nnx} f_2(w_1, ..., w_n) \right) \\
&= c \cdot f_2(u_1, ..., u_n)
\end{aligned}$$

5.2.5 Existenz von Determinantenfunktionen

Sei $v_1, .., v_n$ eine Basis von V und $\hat{f} : V^n \to K$ definiert durch

$$\hat{f}(w_1, ..., w_n) = \sum_{x \in \Sigma_n} \operatorname{sgn}(x) a_{11x} \cdots a_{nnx} \text{ für } w_i = \sum_{j=1}^{n} a_{ij} v_j,\ i \in \{1, ..., n\}$$

Dann ist $\hat{f}$ eine Determinantenfunktion auf V mit $\hat{f}(v_1, ..., v_n) = 1$ (insbesondere existieren damit Determinantenfunktionen auf V!).

Beweis: Offensichtlich ist $\hat{f}(v_1, ..., v_n) = 1$, die Linerität von $\hat{f}$ ist einfach nachzurechnen.
Seien $w_1, ..., w_n$ linear abhängig. Dann existiert i mit $w_i = \sum_{i \neq j} k_j w_j$.

$$\hat{f}(w_1, ..., w_n) = \sum_{j \neq i} k_j \hat{f}(w_1, ..., w_{i-1}, w_j, ..., w_{j-1}, w_j, ..., w_n)$$

Es genügt $\hat{f}(w_1, ..., w_{i-1}, w_j, ..., w_{j-1}, w_j, ..., w_n) = 0$ zu zeigen.

$$f(w_1, ..., w_{i-1}, w_j, ..., w_{j-1}, w_j, ..., w_n) = \sum_{x \in \Sigma_n} \operatorname{sgn}(x) a_{11x} \cdots a_{jix} \cdots a_{jjx} \cdots a_{nnx}$$

Sei $t := (ij), y \in A_n$. Es folgt:

$$\begin{array}{rl} & \operatorname{sgn}(y) \cdot a_{11x} \cdots a_{jix} \cdots a_{jjx} \cdots a_{nnx} + \operatorname{sgn}(ty) \cdot a_{11(ty)} \cdots a_{ji(ty)} \cdots a_{jj(ty)} \cdots a_{nn(ty)} \\ = & \operatorname{sgn}(y) \cdot a_{11x} \cdots a_{jix} \cdots a_{jjx} \cdots a_{nnx} + \operatorname{sgn}(ty) \cdot a_{11y} \cdots a_{jjy} \cdots a_{jiy} \cdots a_{nny} \\ = & 1 \cdot a_{11x} \cdots a_{jix} \cdots a_{jjx} \cdots a_{nnx} + (-1) \cdot a_{11y} \cdots a_{jjy} \cdots a_{jiy} \cdots a_{nny} \\ = & 0 \end{array}$$

Wende (5.1.4) an: $\Sigma_n = A_n \cup tA_n$. Damit ist die Summe oben 0.

5.2.6 Determinanten

Sei[32] $\phi \in \operatorname{Hom}(V, V)$, f Determinantenfunktion, nach (5.2.3) ist f_ϕ Determinantenfunktion. Nach (5.2.4) exisitert $0 \neq c \in K$ mit $f_\phi = cf$.

$$\det_f \phi = \begin{cases} c & \text{falls} \quad \phi \; bijektiv \; f_\phi = cf \\ 0 & \text{sonst} \end{cases}$$

Satz: Sei $\phi \in \operatorname{Hom}(V, V)$, f, f' Determinantenfunktionen, dann gilt: $\det_f \phi = \det_{f'} \phi$.

Beweis: mit (5.2.4) gilt: $f' = df$ für ein $0 \neq d \in K$. Damit gilt: $f'_\phi = df_\phi \Rightarrow \det_f \phi = \det_{f'} \phi$.

Definition: Da die Determinante unabhängig von der Funktion ist, sei $\det \phi := \det_f \phi$. $\det \phi$ heißt *Determinante*.

Sei $(a_{ij})_{n\times n} := A \in \mathcal{M}_{n\times n}(K)$. Dann sei $\det A := \sum_{x\in\Sigma_n} \operatorname{sgn}(x)(a_{11x} \cdots a_{nnx})$.

Beispiele:

- $n = 2$, $\Sigma_n = \{id, (12)\}$, dann ist $\det A = a_{11}a_{22} - a_{12}a_{21}$
- $n = 3$, $\Sigma_n = \{id, (12), (13), (23), (123), (132)\}$, dann ist $\det A = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31} - a_{11}a_{32}a_{23}$ (Merkregeln von Sarrus für $n = 3$).
- falls $a_{ij} = 0$ für alle $i < j$ gilt: $\det A = a_{11} \cdots a_{nn}$

5.2.7 Determinanten von Lin.Abb./Matrix

Sei $\phi \in \operatorname{Hom}(V, V)$, B Basis von V. Dann ist $\det \phi = \det M(\phi, B, B)$. Beweis: siehe (5.2.1).

[32] ab hier ist die Vertretung am Werk...

5.3 Eigenschaften von Determinanten

5.3 Sei K Körper, V endlichdimensionaler Vektorraum über K und $\phi \in \mathrm{Hom}(V, V)$.

5.3.1 Determinanten injektiver Abbildungen

ϕ injektiv $\Leftrightarrow \det \phi \neq 0$.

Beweis: Sei f Determinantenfunktion, $\{v_1, ..., v_n\}$ Basis von V. ϕ invertierbar $\Leftrightarrow \{v_1\phi, ..., v_n\phi\}$ Basis von $V \Leftrightarrow f(v_1, .., v_n) \neq 0 \Leftrightarrow f_\phi(v_1, ..., v_n) \neq 0$.

5.3.2 Multiplikativität der Determinante

Seien $\phi, \psi \in \mathrm{Hom}(V, V)$. Dann gilt: $\det(\psi\phi) = (\det \psi)(\det \phi)$.

Beweis:

- einer nicht bijektiv: ϕ nicht bijektiv $\Rightarrow \mathrm{Kern}\, \phi \neq 0 \Rightarrow \mathrm{Kern}\, \phi\psi \neq 0 \Rightarrow \det \phi\psi = 0 = \det \phi = (\det \phi)(\det \psi)$
- Seien ϕ, ψ bijektiv. $\det \phi\psi = \frac{f(v_1\phi\psi, ..., v_n\phi\psi)}{f(v_1, ..., v_n)} = \frac{f(v_1\phi\psi, ..., v_n\phi\psi)}{f(v_1, ..., v_n)} \cdot \frac{f(v_1\phi, ..., v_n\phi)}{f(v_1, ..., v_n)} = \det \psi \cdot \det \phi = \det \phi \cdot \det \psi$

Folgerung: $\det AB = \det A \cdot \det B$, $\det A^{-1} = \frac{1}{\det A}$

5.3.3 Determinanten der Transposition

Sei $A \in \mathcal{M}_{n\times n}(K)$. Dann gilt: $\det A = \det A^t$. Beweis: $\det A = \sum_{x\in\Sigma_n} \mathrm{sgn}(x) a_{11x} \dots a_{nnx}$. Für $x \in \Sigma_n$:

$$\begin{aligned}
\det A &= \sum_{x\in\Sigma_n} \mathrm{sgn}(x) a_{11x} \dots a_{nnx} \\
&= \sum_{x\in\Sigma_n} \mathrm{sgn}(x^{-1})(a_{1x^{-1}1} \cdots a_{nx^{-1}n}) \\
&= \sum_{x\in\Sigma_n} \mathrm{sgn}(x^{-1})(a_{1x^{-1}1x^{-1}x} \cdots a_{nx^{-1}nx^{-1}x}) \\
&= \sum_{x^{-1}\in\Sigma_n} \mathrm{sgn}(x^{-1})(a_{1x^{-1}1} \cdots a_{nx^{-1}n}) \\
&= \sum_{y\in\Sigma_n} \mathrm{sgn}(y)(a_{1y1} \cdots a_{nyn}) \\
&= \det A^t
\end{aligned}$$

5.3.4 Rechenregeln für Determinanten

Sei $(a_{ij})_{n\times n} := A \in \mathcal{M}_{n\times n}(K)$, $c \in K$. Für $E^n_{ij}(c)$ und $P^{(n)}_{ij}$ siehe (4.3). Dann gilt:

1. $c \cdot \det A = \det(AE^{(n)}_{rr}(c))$ (multipliziert man eine Spalte der Matrix mit c, wird auch der Wert der Determinanten mit c multipliziert)

2. $\det A = \det AE^{(n)}_{ij}(c)$ für $i \neq j$ (addiert man das c-fache einer Spalte zu einer anderen, so ändert sich der Wert der Matrix nicht)

3. $\det AP^{(n)}_{ij} = -\det A$ für $i \neq j$ (das Vertauschen von Spalten ändert das Vorzeichen der Matrix)

4. Sind zwei Zeilen oder Spalten von A gleich, so ist $\det A = 0$

Beweis:

1-3. folgt aus (5.3.2)

4. $B = \{v_1, ..., v_n\}$, $\hat{f}$ die in (5.2.5) definierte Determinantenfunktion, $\hat{f}(v_1, ..., v_n) = 1$. $\phi \in \mathrm{Hom}(V,V), A = M(\phi, B, B)$ $\det A = \det \phi = \hat{f}(v_1\phi, ..., v_n\phi) = 0$

5.3.5 Vandermondesche Determinante

$$A := \begin{pmatrix} 1 & b_1 & b_1^2 & \cdots & b_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & b_n & b_n^2 & \cdots & b_n^{n-1} \end{pmatrix} \quad a_{ij} = b_i^{j-1}$$

Dann ist $\det A = \prod\limits_{i<j}(b_i - b_j)$.

Beweis:

- Addiere das $-b_1$-fache der $(n-1)$-ten Spalte zur n-ten Spalte
- Addiere das $-b_2$-fache der $(n-2)$-ten Spalte zur $(n-1)$-ten Spalte
- ...
- Addiere das $-b_n$-fache der ersten Spalte zur zweiten Spalte

... und sonst siehe Script.

5.3.6

Sei $(a_{ij})_{n\times n} := A \in \mathcal{M}_{n\times n}(K)$. Sei weiter

$$A_{ij} = (b_{rs})_{n\times n}; b_{rs} = \begin{cases} a_{rs} & \text{falls} \quad i \neq r, j \neq s \\ 0 & \text{falls} \quad i = r, j \neq s \\ 0 & \text{falls} \quad i \neq r, j = s \\ 1 & \text{falls} \quad i = r, j = s \end{cases}$$

d.h. bei A_{ij} steht in der i-te Zeile und in der j-ten Spalte überall eine 0, nur an der Position (i, j) eine 1.[33] Definiere zudem A'_{ij} durch Streichen der i-ten Zeile und der j-ten Spalte. Beispiel:

$$A := \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \Rightarrow A_{22} = \begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 0 \\ 7 & 0 & 9 \end{pmatrix} \Rightarrow A'_{22} := \begin{pmatrix} 1 & 3 \\ 7 & 9 \end{pmatrix}$$

Satz: Sei $(a_{ij})_{n\times n} := A \in \mathcal{M}_{n\times n}(K)$. Dann gilt: $\det A_{ij} = (-1)^{i+j} \cdot \det A'_{ij}$.

Beweis: Sei $(a'_{ij})_{(n-1)\times(n-1)} := A' \in \mathcal{M}_{(n-1)\times(n-1)}(K)$ Sei $C = (c_{rs})_{n\times n}$ mit

$$c_{rs} := \begin{cases} a'_{rs} & \text{falls} \quad r < n \wedge s < n \\ \delta_{rs} & \text{falls} \quad r = n \wedge s = n \end{cases}$$

Wende (5.3.4) an, es gilt:

$$\begin{aligned} \det A_{ij} &= (-1)^{(n-j)+(n-i)} \cdot \det C \\ &= (-1)^{2n-(i+j)} \cdot \det C \\ &= (-1)^{i+j} \cdot \det C \\ &= (-1)^{i+j} \cdot \sum_{x\in\Sigma_n} \operatorname{sgn} x c_{11x} \cdots c_{nnx} \\ c_{nnx} &= \begin{cases} 0 & \text{falls} \quad n \neq nx \\ 1 & \text{falls} \quad n = nx \end{cases} \\ \det A_{ij} &= (-1)^{i+j} \cdot \sum_{x\in\Sigma_n \mid n=nx} \operatorname{sgn} x c_{11x} \cdots c_{(n-1)(n-1)x} \\ &= (-1)^{i+j} \cdot \sum_{x\in\Sigma_n \mid n=nx} \operatorname{sgn} x a'_{11x} \cdots a'_{(n-1)(n-1)x} \\ &= (-1)^{i+j} \cdot \sum_{x\in\Sigma_{n-1}} \operatorname{sgn} x a'_{11x} \cdots a'_{(n-1)(n-1)x} \\ &= \det A'_{ij} \end{aligned}$$

[33] Original wieder da, Vertretung wieder wech...

5.3.7 Entwicklungssatz

Sei $(a_{ij})_{n\times n} := A \in \mathcal{M}_{n\times n}(K)$.

Die Entwicklung nach der i-ten Zeile für ein festes i:

$$\begin{aligned}\det A &= \sum_{j=1}^{n} a_{ij} \det A_{ij} \\ &= \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det A'_{ij}\end{aligned}$$

Die Entwicklung nach der j-ten Spalte für ein festes j:

$$\begin{aligned}\det A &= \sum_{i=1}^{n} a_{ij} \det A_{ij} \\ &= \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det A'_{ij}\end{aligned}$$

Beispiel: Entwicklung nach der 2. Zeile[34]:

$$\begin{aligned}A &:= \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \\ \det A &= a_{21} \det A_{21} + a_{22} \det A_{22} + a_{23} \det A_{23} \\ &= -a_{21} \det A'_{21} + a_{22} \det A'_{22} - a_{23} \det A'_{23} \\ &= -4 \cdot \begin{pmatrix} 2 & 3 \\ 8 & 9 \end{pmatrix} + 5 \cdot \begin{pmatrix} 1 & 3 \\ 7 & 9 \end{pmatrix} - 6 \cdot \begin{pmatrix} 1 & 2 \\ 7 & 8 \end{pmatrix} \\ &= -4 \cdot (-6) + 5 \cdot (-12) - 6 \cdot (-6) \\ &= 0\end{aligned}$$

Beweis: Sei $V = K^n$, $B = \{e_1, ..., e_n\}$ die kanonische Basis und sei $\hat{f}$ bezüglich V und B wie in (5.2.4), d.h. $z_i = \sum_{j=1}^{n} z_{ij} e_j$;

$$\hat{f}(z_1, ..., z_n) = \sum_{x\in\Sigma_n} \operatorname{sgn}(x) \cdot z_{11x} \cdots z_{nnx}$$

Dann ist $\det A = \hat{f}(a_1, ..., a_n)$, wobei a_i der i-te Zeilenvektor von A ist $(a_i \sum_{j=1}^{n} a_{ij} e_j)$.

[34] „$5 \times (-12)$ ist schon schwer, so knapp 60...“

$$\begin{aligned}
\det A &= \hat{f}(a_1, ..., a_n) \\
&= \hat{f}(a_1, ..., a_{i-1}, \sum_{j=1}^{n} a_{ij} e_j, ..., a_n) \\
&= \sum_{j=1}^{n} a_{ij} \hat{f}(a_1, ..., a_{i-1}, e_j, ..., a_n) \\
&= \sum_{j=1}^{n} a_{ij} \det A^*_{ij} \\
&= \sum_{j=1} n a_{ij} \det A'_{ij}
\end{aligned}$$

... mit A^*_{ij} als alte Version von A_{ij}, die Determinanten sind gleich, siehe Übungsaufgabe[35]. Die zweite Gleichung (Entwicklung nach Spalten) folgt wegen $\det A = \det A^t$ sofort.

5.3.8 Berechnung der inversen Matrix

Sei $(a_{ij})_{n\times n} := A \in \mathcal{M}_{n\times n}(K)$ und $(\tilde{a}_{ij})_{n\times n} := \tilde{A}$ durch $\tilde{a}_{ij} := \det A_{ji}$. Dann gilt:

1. $A\tilde{A} = (\det A) I_{n\times n} = \tilde{A}A$
2. Ist $\det A \neq 0$, so ist $A^{-1} = (\det A)^{-1}\tilde{A}$

[35] „Was man nicht kann, stellt man als Übungsaufgabe - Sie sind schließlich jünger und intelligenter!“

Beispiel:

$$\begin{aligned}
A &:= \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 2 & 0 & 3 \end{pmatrix} \\
\det A &= 6-4=2 \\
\det A_{11} &= (-1)^2 \cdot 6 \\
\det A_{12} &= (-1)^3 \cdot 0 \\
\det A_{13} &= (-1)^4 \cdot (-4) \\
\det A_{21} &= (-1)^3 \cdot 0 \\
\det A_{22} &= (-1)^4 \cdot 1 \\
\det A_{23} &= (-1)^5 \cdot 0 \\
\det A_{31} &= (-1)^4 \cdot (-2) \\
\det A_{32} &= (-1)^5 \cdot 0 \\
\det A_{33} &= (-1)^6 \cdot 2 \\
\tilde{A} &= \begin{pmatrix} 6 & 0 & -2 \\ 0 & 1 & 0 \\ -4 & 0 & 2 \end{pmatrix} \\
A^{-1} &= 2^{-1} \cdot \tilde{A} \\
&= \begin{pmatrix} 3 & 0 & -1 \\ 0 & 0,5 & 0 \\ -2 & 0 & 1 \end{pmatrix}
\end{aligned}$$

Beweis:

1. Wir benutzen wie im Beweis von (5.3.7) die Determinantenfunktion $\hat{f}$ auf K^n. Sei $(b_{ij}) := A\tilde{A}$.

$$\begin{aligned}
b_{ij} &= \sum_{k=1}^{n} a_{ik}\tilde{a}_{kj} \\
&= \sum_{k=1}^{n} a_{ik} \det A_{jk} \\
&= \sum_{k=1}^{n} a_{ik}\hat{f}(a_1, ..., a_{j-1}, e_k, a_{j+1}, ..., a_n)
\end{aligned}$$

wobei $a_1, ..., a_n$ die Zeilenvektoren von A sind.

$$\begin{aligned} b_{ij} &= \hat{f}(a_1, ..., a_{j-1}, \sum_{k=1}^{n} a_{ik}e_k, a_{j+1}, ..., a_n) \\ &= \hat{f}(a_1, ..., a_{j-1}, a_i, a_{j+1}, ..., a_n) \\ &= \begin{cases} 0 & \text{falls} \quad i \neq j \\ \det A & \text{falls} \quad i = j \end{cases} \\ \Rightarrow A\tilde{A} &= \begin{pmatrix} \det A & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \det A \end{pmatrix} \end{aligned}$$

Zweite Gleichung zeigt man mittels Übergang zur Transposition $(\tilde{A}A)^t = A^t\tilde{A}^t = \det A \cdot I_{n\times n}$ Nun rechne wie oben.

2. folgt direkt, denn $A(\det A)^{-1} = I_{n\times n} = (\det A)^{-1}A$.

5.3.9 Cramersche Regel

VORAUSSETZUNG: Sei $xA = b$ ein lineare Gleichungssystem mit $b = (b_1, ..., b_n) \in K^n$ und $A \in \mathcal{M}_{n\times n}(K)$ mit $\det A \neq 0$.

BEHAUPTUNG: $Y = (y_1, ..., y_n) \in K^n$ mit $y_i = (\det A)^{-1} \sum_{k=1}^{n} b_k \cdot \det A_{ik}$ für $i \in \{1, ..., n\}$ die eindeutig bestimmte Lösung dieses linearen Gleichungssystems.

BEWEIS: $\det A \neq 0 \Leftrightarrow A$ invertierbar $\Leftrightarrow \operatorname{rg} A = n \Rightarrow$ eindeutig lösbar , es bleibt zu zeigen: $(y_1, ..., y_n)$ ist Lösung.

Angenommen, $yA \overset{!}{=} b$. Dann ist $\sum_i y_i a_{ij} \overset{!}{=} b_j$, wobei $A = (a_{ij})_{n\times n}$. Für jedes j gilt:

$$\begin{aligned} \sum_i y_i a_{ij} &= \sum_i \left((\det A)^{-1} \sum_k b_k \det A_{ik} a_{ij} \right) \\ &= (\det A)^{-1} \cdot \sum_k \left(b_k \sum_i \tilde{a}_{ki} a_{ij} \right) \\ &= (\det A)^{-1} \cdot \sum_k \left(b_k \sum_i \det A_{ik} a_{ij} \right) \\ &= (\det A)^{-1} \cdot b_j \det A \\ &= b_j \end{aligned}$$

Zur 3. Zeile: An der Stelle (k,j) der Matrix $\tilde{A}A$ steht $\sum_i \det A_{ik} a_{ij}$.

BEISPIEL:

$$\begin{aligned} xA &= b \\ A &:= \begin{pmatrix} 1 & 2 & 0 \\ 2 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix} \\ b &:= (1,1,1) \\ \det A &= 1-4-4=-7 \end{aligned}$$

$$\begin{array}{rcr|rcr|rcr} \det A_{11} & = & -3 & -\det A_{12} & = & -2 & \det A_{13} & = & 4 \\ -\det A_{21} & = & -2 & \det A_{22} & = & 1 & -\det A_{23} & = & -2 \\ \det A_{31} & = & 4 & -\det A_{32} & = & -2 & \det A_{33} & = & -3 \end{array}$$

$$\begin{aligned} y_1 &= -\frac{1}{7}(-3-2+4) = \frac{1}{7} \\ y_2 &= -\frac{1}{7}(-2+1-2) = \frac{3}{7} \\ y_3 &= -\frac{1}{7}(4-2-3) = \frac{1}{7} \\ Y &= \left(\frac{1}{7}, \frac{3}{7}, \frac{1}{7}\right) \end{aligned}$$

6 Polynomringe

6.1 Definitionen für Ringe

Sei R eine nichtleere Menge mit zwei inneren Verknüpfungen $+, \cdot$. R heißt *Ring*, falls gilt:

1. $(R, +)$ ist eine abelsche Gruppe
2. $\cdot$ ist assoziativ und bezüglich $+$ distributiv d.h. $(ab)c = a(bc)$ und $(a+b)c = ac + bc$ sowie $a(b+c) = ab + ac$ für alle $a, b, c \in R$.

Ist $\cdot$ zusätzlich kommutativ, so heißt R ein *kommutativer Ring*. Existiert $1 \in R$ mit $1x = x1 = x$ für $x \in R$, so heißt R *Ring mit Eins* und 1 das *Einselement*.

Beispiel:

- $\mathbb{Z}$ ist ein kommutativer Ring mit 1.
- $n\mathbb{Z}$ ist ein kommutativer Ring.

Eine nichtleere Teilmenge von R heißt *Teilring*, falls sie bezüglich der Addition und Multiplikation von R ein Ring ist.

Seien R und $\tilde{R}$ Ringe und $\varphi : R \to \tilde{R}$ eine Abbildung. Dann heißt φ *Ringhomomorphismus*, falls

$$(a+b)\varphi = a\varphi + b\varphi \;\wedge\; (ab)\varphi = a\varphi b\varphi \;\forall\, a, b \in R$$

Sei im folgenden K ein Körper. Sei F die Menge aller Folgen $(f_0, ..., f_1)$ mit $f_i \in K$ und $(*)$ nur endlich viele der f_i sind ungleich null (d.h. die Menge der endlichen Folgen in K).

Setze $0 := (0, 0, ...)$ und $1 := (1, 0, 0, ...)$.

Für $0 \neq f = (f_0, ..., f_i, ...) \in F$ sei $\operatorname{grad} f := \max\{ i \mid f_i \neq 0\}$, $f_{\operatorname{grad} f}$ heißt *Leitkoeffizient* von f.

Wir definieren für $f = (f_0, ..., f_i, ...)$ und $g = (g_0, ..., g_i, ...)$:

- $f + g := (f_0 + g_0, ..., f_i + g_i, ...)$
- $f \cdot g := (c_0, ..., c_n, ...)$ mit $c_n = \sum_{i+j=n} f_i g_j$

Seien $f, g \in F \setminus \{0\}$. Dann gilt (Gradgleichung):

- $\operatorname{grad} f + g \leq \max\{\operatorname{grad} g, \operatorname{grad} f\}$
- $\operatorname{grad} fg = \operatorname{grad} f + \operatorname{grad} g$

Bezeichnung: Für $n = 0, ..., 1$ und $k \in K$ setze $x^n := (0, ..., 0, 1_{n.\,\text{Stelle}}, 0, ...)$ (also $x_0 = 1$). Bezeichne zudem $k := (k, 0, 0, ...)$ (Damit: „$K \subseteq F$“).

6.2 Polynomring

Sei $f \in F$, $f = (k_0, ..., k_n, ...,)$. Dann ist $f = \sum_{i=0}^{m} k_i x^i$, wobei $m \geq n = \operatorname{grad} f$.

$(F, +, \cdot)$ ist ein kommutativer Ring mit 1, der *Polynomring* über K, bezeichnet mit $K[x]$.

Anteil vom Beweis: 0 ist neutrales Element, (1, 0, 0, ...) ist Einselement, zu $f(f_0, ...) \in F$ ist $(-f_0, ...)$ das inverse Element, ...

6.3 Nullteilerfreiheit

Satz: Seien $f, g \in K[x]$. Dann gilt: $fg = 0 \Leftrightarrow (f = 0) \vee (g = 0)$.

Beweis: mit der Gradgleichung

6.4 Euklidischer Algorithmus

Satz: Seien $f, g \in K[X]$ und $g \neq 0$. Dann existieren $p, q \in K[x]$ mit $f = pg + q$, wobei $q = 0$ oder $\operatorname{grad} q < \operatorname{grad} g$.

Beweis:

- Spezialfall $f = 0$, dann existieren $p = q = 0$ mit $f = pg + q$
- Spezialfall $f \neq 0$ und $\operatorname{grad} f < \operatorname{grad} g$: Wähle $p = 0$ und $q = f$.
- Sei im folgenden $f \neq 0$ und $\operatorname{grad} f \geq \operatorname{grad} g$. Beweis[36] durch Induktion nach $\operatorname{grad} f$. Setze $n := \operatorname{grad} f$, $m := \operatorname{grad} g$. Sei a_n der Leitkoeffizient von f und b_m der Leitkoeffizient von g.

  Induktionsverankerung: Für $n = 0$ ist $\operatorname{grad} g = 0$ und $g \in K^*$. Setze $p = fg^{-1}$ und $q = 0$, dann ist $pg + q = f$.

  Induktionsannahme: $n > 0$ und Behauptung richtig für alle Polynome vom Grad n.

  Induktionsschluß: Sei $b := a_n b_m^{-1}$. Definiere $\tilde{f} := f - bx^{n-m}g$. Dann ist $\operatorname{grad} \tilde{f} < \operatorname{grad} f$. Mit der Induktionsannahme folgt: $\tilde{f} = \tilde{p}g + \tilde{q}$, wobei $\tilde{q} = 0$ oder $\operatorname{grad} \tilde{q} < \operatorname{grad} g$. Daraus folgt: $f = \tilde{f} + bx^{n-m}g = (\tilde{p} + bx^{n-m})g + \tilde{q}$. Wähle $p := \tilde{p} + bx^{n-m}$ und $q := \tilde{q}$.

[36] „Zu Hause, wenn es keiner sieht, können Sie ja sogar arrogant sein!“

6.5 (Haupt)Ideale

Sei R ein kommutativer Ring mit 1. Eine nichtleere Teilmenge I heißt *Ideal* von R, falls gilt:

1. $(I, +)$ ist eine Untergruppe von $(R, +)$
2. $RI = \{ri \mid r \in R, i \in I\} = I$

Ein Ideal von R heißt *Hauptideal*, falls ein $r \in I \subseteq R$ existiert mit $rR = I$. Ist jedes Ideal von R Hauptideal, so heißt R Hauptidealring. Beispiel:

1. $\{0\}, R$ sind Ideale
2. Sind I, J Ideale, so sind auch $I \cap J$ und $I + J$ Ideale.
3. In $\mathbb{Z}$ sind $z\mathbb{Z}$ Ideale ($z \in \mathbb{Z}$)
4. Allgemein: $a \in R$, aR ist Ideal.

6.6 Hauptidealeigenschaften von $K[x]$

Satz: $K[x]$ ist Hauptidealring.

Beweis: Sei I ein Ideal von $K[x]$. Zu zeigen: Es exisitiert ein $g \in K[x]$ mit $I = K[x]g$.

Ist $I = \{0\}$, so ist $I = K[x]0$. Sei nun $I \neq \{0\}$. Sei $n := \min\{\operatorname{grad} i \mid i \in I \setminus \{0\}\}$. Sei $g \in I$ mit $\operatorname{grad} g = n$. Zu zeigen: $I = K[x]g$.

Sei $f \in I$. Mit (6.4): es existieren $p, q \in K[x]$ mit $f = pg + q$ und $(q = 0) \vee (\operatorname{grad} q < n)$. Es genügt zu zeigen: $q \in I$, dann folgt: $q = 0 \Rightarrow f = pg$.

$q = f - pg$ mit $f \in I$ und $pg \in I$, da I Gruppe: $q \in I$.

6.7 Faktorringe

Sei R ein kommutativer Ring mit 1, I Ideal von R und $R/I = \{r + I \mid r \in R\}$. Dann werden durch

- $(r + I) + (r' + I) := (r + r') + I$
- $(r + I)(r' + I) := rr' + I$

innere Verknüpfungen auf R/I definiert und R/I ist bezüglich dieser Verknüpfungen ein Ring mit Einselement $(1+I)$.

Die Abbildung $\varphi : R \to R/I$ mit $r \mapsto r+I$ ist ein surjektiver Ringhomomorphismus und heißt *natürliche (kanonische) Homomorphismus*.

BEWEIS: Benutze das Argument aus (3.6.3): R/I ist die Menge der Äquivalenzklassen bezüglich der Äquivalenzrelation

$$\{(a,b) \in R \times R \mid a-b \in I\}$$

Seien $r, r', h, h' \in R$ und $r+I = h+I$ und $r'+I = h'+I$. Damit folgt: $r-h, r'-h' \in I$. Dann folgt:

$$\begin{aligned}
(r+r')+I &= (h+h')+I \\
rr'-hh' &= rr'+rh'-r'h-hh' \\
&= (r-h)r'+h(r'-h') \\
\Rightarrow rr'-hh' &\in I \\
\Rightarrow rr'+I &= hh'+I
\end{aligned}$$

6.8 irreduzibel, neue Körper

BEZEICHNUNG[37]: Seien $f, g, h \in K[x]$ und $\operatorname{grad} f \geq 1$. f heißt *irreduzibel*, falls aus $f = gh$ folgt, daß $\operatorname{grad} g = 0$ oder $\operatorname{grad} h = 0$.

SATZ: Sei f irreduzibel und $I = K[x]f$. Dann ist $K[x]/I$ ein Körper.

BEISPIEL:

$$\begin{aligned}
K &= \{0,1\} = \mathbb{Z}_2 \\
\{p \in K[x] \mid \operatorname{grad} p = 1\} &= \{x, x+1\} \\
\{p \in K[x] \mid \operatorname{grad} p = 2\} &= \{x^2, x^2+x, x^2+x+1, x^2+1\} \\
\text{davon nicht irreduzibel:}\quad & \ \{x^2, x^2+x, x^2+1\} \\
g &= x^2+x+1 \text{ (irreduzibel)} \\
K[x]/K[x]g &= \{h + K[x]g \mid (h=0) \vee (\operatorname{grad} h \leq 2)\}
\end{aligned}$$

BEWEIS: Sei $g \in K[x]$ mit $g+I \neq 0+I$. Es ist zu zeigen: $g+I$ besitzt ein Inverses. Gesucht ist $h \in K[x]$ mit $(g+I)(h+I) = 1+I$. Setze $J = K[x]g+I$. J ist Ideal von $K[x]$ mit $f \in I \subseteq J \Rightarrow J \neq \{0\}$. Mit (6.6) folgt: es existiert $\tilde{f} \in K[x]$ mit $J = K[x]\tilde{f} \Rightarrow\ \exists\, w \in K[x]$ mit $f = w\tilde{f}$. Da f irreduzibel:

[37] man erinnere sich hier an den Vorschlag an die Politik zur Translation des Semesters

- Angenommen: $\operatorname{grad} w = 0 \Rightarrow w \in K, w \neq 0 \Rightarrow \tilde{f} = w^{-1}f \in I \Rightarrow K[x]\tilde{f} \subseteq I \Rightarrow J \subseteq I \Rightarrow g \in J \subseteq I \Rightarrow g + I = 0 + I$
- Also gilt: $\operatorname{grad} \tilde{f} = 0 \Rightarrow \tilde{f} \in K, f \neq 0 \Rightarrow J = K[x]$ und $K[x]/I = J/I \Rightarrow 1 + I \in J/I \Rightarrow \ \exists\, v \in K[x]$ mit $1 + I = vg + I = (v + I)(g + I) = (g + I)(v + I)$, wähle $h := v$

6.9 Eindeutige Primfaktorzerlegung

VORAUSSETZUNG: Sei $f \in K[x]$, $\operatorname{grad} f \geq 1$.

SATZ: Es existieren irreduzible Polynome $f_1, ..., f_r \in K[x]$ mit $f = f_1 \cdot f_2 \cdots f_r$, und diese Polynome sind bis auf die Reihenfolge und Muliplikation mit Körperelementen eindeutig bestimmt. BEWEIS:

1. Existenz: Induktion nach dem Grad von f.

   Induktionsverankerung für $n = 1$: folgt aus der Gradgleichung

   Induktionsannahme: $n > 1$ und die Behauptung ist richtig für alle h mit $1 \leq \operatorname{grad} h < n$.

   Induktionsschluß: f irreduzibel $\Rightarrow$ Behauptung. Angenommen, f sei nicht irreduzibel. $\Rightarrow\ \exists\, g, h \in K[x]$ mit $\operatorname{grad} g \geq 1, \operatorname{grad} h \geq 1$ und $f = gh$. Aus der Gradgleichung folgt: $\operatorname{grad} f = n = \operatorname{grad} g + \operatorname{grad} h$. Dann folgt: $1 \leq \operatorname{grad} g < n$ und $1 \leq \operatorname{grad} h < n$, mit der Induktionsannahme folgt: es existieren irreduzible $g_1, ..., g_s, h_1, ..., h_t \in K[x]$, so daß $g = g_1 \cdots g_s$ und $h = h_1 \cdots h_t$. Damit: $f = gh = g_1 \cdots g_s h_1 \cdots h_t$.

2. Eindeutigkeit[38]: Sei $f = f_1 \cdots f_r = f'_1 \cdots f'_s$ wobei die f_i, f'_i irreduzibel. Sei $I_k := K[x]f_k$ für $k = 1, ..., r$; sei $F_k := K[x]/I_K$. Sei $\varphi_k : K[x] \to F_k$ kanonischer Homomorphismus.

$$\begin{aligned} f\varphi_k &= f_1\varphi_k \cdots f_r\varphi_k \\ &= f'_1\varphi_k \cdots f'_s\varphi_k \\ f_k\varphi_k &= f_K + I \\ &= 0 + I_k, \text{ da } f_k \in I \\ \Rightarrow f_1\varphi_k \cdots f_s\varphi_k &= 0 \end{aligned}$$

[38] „...soll ja keine Drohung sein, sondern soll Sie neugierig machen...“

F_k ist Körper nach (6.8), F_k ist nullteilerfrei, d.h. $\exists\, j \in \{1, ..., s\}$ mit $f_j' \varphi_k = 0$.

$$\begin{aligned} \Rightarrow f_j'\varphi_k &= f_j' + I_k = 0 + I_k \\ \Rightarrow f_j' &\in I_k \\ \Rightarrow \exists\, g &\in K[x] \text{ mit } f_j' = g f_k \end{aligned}$$

Da f_j' irreduzibel: Enweder $\operatorname{grad} f_k = 0$ oder $\operatorname{grad} g = 0$, da f_k aber irreduzibel ist, ist $\operatorname{grad} g = 0$. Damit: $g \in K$

Wir haben gezeigt: Zu jedem $k \in \{1, ..., r\}$ existiert $j_k \in \{1, ..., s\}$ mit $f_{j_k}' = a_k f_k, a_k \in K$. Wir können also annehmen:

$$\begin{aligned} f &= k \prod_{i=1}^{t} f_i^{e_i} \\ &= \prod_{i=1}^{t} f_i^{e_i'} \end{aligned}$$

wobei $f_1, ..., f_t$ die Eigenschaft haben:

$$f_j \notin K[x] f_i \text{ für } i \neq j$$

Es bleibt zu zeigen: $e_i = e_i'$ für $i = 1, .., t$.

Angenommen, es existiert $k \in \{1, ..., t\}$ mit $e_k \neq e'_k$, o.B.d.A $e_k > e'_k$

$$\begin{aligned}
0 &= \left(k \prod_{i=1}^{t} f_i^{e_i}\right) - \left(\prod_{i=1}^{t} f_i^{e'_i}\right) \\
&= f_k^{e'_k} \cdot \left(\left(k f_k^{e_k - e'_k} \prod_{i \neq k}^{t} f_i^{e_i}\right) - \left(\prod_{i \neq k}^{t} f_i^{e'_i}\right)\right) \\
\overset{(6.3)}{\Rightarrow} 0 &= \left(k f_k^{e_k - e'_k} \prod_{i \neq k}^{t} f_i^{e_i}\right) - \left(\prod_{i \neq k}^{t} f_i^{e'_i}\right) \\
k f_k^{e_k - e'_k} \prod_{i \neq k}^{t} f_i^{e_i} &= \prod_{i \neq k}^{t} f_i^{e'_i} \\
k f_k^{e_k - e'_k} \prod_{i \neq k}^{t} f_i^{e_i} &\in \in K[x] f_k =: I_k \\
\Rightarrow \prod_{i \neq k}^{t} f_i^{e'_i} &\in \in K[x] f_k \\
\text{mit } \varphi_k : K[x] &\to K[x]/I_K \\
\Rightarrow 0 &= \left(\prod_{i \neq k}^{t} f_i^{e'_i}\right) \varphi_k \\
&= \prod_{i \neq k}^{t} (f_i \varphi_k)^{e'_i}
\end{aligned}$$

Aufgrund der Nullteilerfreiheit existiert ein j mit $j \neq k$ und $f_j \varphi_K = 0$. Daraus folgt: $f_j \in I_K = K[x] f_k$, das ist ein Widerspruchzu $j \neq k$.

6.10 Einsetzhomomorphismus, Nullstellen

Sei $a \in K$. Sei zudem der folgende *Einsetzhomomorphismus* definiert:

$$\varphi_a : K[x] \to K \text{ mit } f := \sum_{i=0}^{n} k_i x^i \mapsto f(a) := \sum_{i=0}^{n} k_i a^i$$

Seien $\sum_{i=0}^{n} k_i x^i, \sum_{i=0}^{n} h_i x^i \in K[x]$.

$$\begin{aligned}
& \left(\sum_{i=0}^{n} k_i x^i + \sum_{i=0}^{n} h_i x^i\right) \varphi_a \\
= & \left(\sum_{i=0}^{n} (k_i + h_i) x^i\right) \varphi_a \\
= & \sum_{i=0}^{n} (k_i + h_i) a^i \\
= & \sum_{i=0}^{n} k_i a^i + \sum_{i=0}^{n} h_i a^i \\
= & \left(\sum_{i=0}^{n} k_i a^i\right) \varphi_a + \left(\sum_{i=0}^{n} h_i a^i\right) \varphi
\end{aligned}$$

Für Multiplikation genauso. Sei $f \in K[x]$ und $a \in K$. a heißt Nullstelle von f, falls $f(a) = 0$

6.11 Zerlegung in Linearfaktoren, Vielfachheit

DEFINITION: Sei a Nullstelle von f, dann heißt $x - a$ Linearfaktor von f.

SATZ: Sei $0 \neq f \in K[x]$, und seien $a_1, ..., a_n$ paarweise verschiedene Nullstellen von f. Dann gilt $n \leq \operatorname{grad} f$, und es existiert $h \in K[x]$ mit $f = h \prod_{i=1}^{n} (x - a_i)$

BEWEIS: Sei $g := x - a_n$. Euklidischer Algorithmus: es existiert $p \in K[x]$ und $q \in K[x]$ mit $q = 0$ oder $\operatorname{grad} q < \operatorname{grad} g = 1$ mit $f = pg + q$, d.h. in diesem Fall $q = 0$ oder $\operatorname{grad} q = 0$.

Angenommen, $q \neq 0$. $f(a_n) = p(a_n)g(a_n) + q(a_n)$. Da $g(a_n) = f(a_n) = 0$ ist, folgt: $q(a_n) = 0 \Rightarrow q = 0$Damit ist $q = 0$, also: $f = pg$.

Sei $a_j \neq a_n$, dann folgt: $g(a_j) = a_j - a_n \neq 0$. Es ist also a_j keine Nulstelle von g für $j \neq n$. Da aber $f(a_j) = 0$ ist, muß $p(a_j) = 0$ sein für alle $j < n$, d.h. $a_1, ..., a_{n-1}$ sind Nullstellen von p.

Durch Induktion nach dem Grad von f folgt: $p = h \prod_{i=1}^{n-1} (x - a_i)$, also $f = h \prod_{i=1}^{n} (x - a_i)$.

Sei $r_a := \max\{m \in \mathbb{N} \mid (x - a)^m \text{ ist Faktor von } f\}$. Dann heißt r_a die Vielfachheit der Nullstelle a.

6.12 Körper der rationalen Funktionen

Zur Erinnerung ans Verfahren: $(a,b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ mit $(a,b) \sim (a',b') :\Leftrightarrow ab' = ba'$; dann ist $\sim$ eine Äquivalenzrelation, die Äquivalenzklassen $\frac{a}{b} := \overline{(a,b)}$ mit $\overline{(a,b)} + \overline{(c,d)} := \overline{(ad+cb,bd)}$ und $\overline{(a,b)} \cdot \overline{(c,d)} := \overline{(ac,bd)}$ definieren die rationalen Zahlen.

Definition: $(f,g) \in K[x] \times (K[x] \setminus \{0\})$ mit $(f,g) \sim (f',g') :\Leftrightarrow fg' = gf'$; dann ist $\sim$ eine Äquivalenzrelation, die Äquivalenzklasse von (f,g) ist $\overline{(f,g)}$, die Menge der Äquivalenzklassen ist $K(x)$; definiere Verknüpfungen $\overline{(f,g)} + \overline{(h,l)} := \overline{(fl+hg,gl)}$ und $\overline{(f,g)} \cdot \overline{(h,l)} := \overline{(fh,gl)}$.

Behauptung: die Verknüpfungen sind wohldefiniert.

Beweis: Seien $\overline{(f,g)} = \overline{(f',g')}$ und $\overline{(h,l)} = \overline{(h',l')}$, d.h. $fg' = gf'$ und $hl' = lh'$.

$$\begin{aligned}
\overline{(f,g)} + \overline{(h,l)} &= \overline{(fl+hg,gl)} \\
\overline{(f',g')} + \overline{(h',l')} &= \overline{(f'l'+h'g',g'l')} \\
\text{zu zeigen: } \overline{(fl+hg,gl)} &\sim \overline{(f'l'+h'g',g'l')} \\
(fl+hg)g'l' &= flg'l' + hgg'l' \\
&= (fg')(ll') + (hl')(gg') \\
&= (gf')(ll') + (lh')(gg') \\
&= (f'l'+h'g')gl
\end{aligned}$$

Damit ist $(K(x),+)$ eine abelsche Gruppe mit Nullelement $\overline{(0,1)}$ und inversem Element $\overline{(-f,g)}$, da

$$\overline{(f,g)} \cdot \overline{(-f,g)} = \overline{(fg-fg,gg)} = \overline{(0,1)}$$

Weitere Eigenschaften analog, somit ist $(K(x),+,\cdot)$ der Körper der rationalen Funktionen über K. Zudem soll gelten: $K[x] \subseteq K(x)$ mittels $f := \overline{(f,1)}$ für $f \in K[x]$

7 Das Minimalpolynom einer linearen Abbildung

Sei K ein Körper, V ein endlich dimensionaler Vektorraum über K und $\varphi \in \operatorname{Hom}(V,V)$. $\operatorname{Hom}(V,V)$ ist ein Vektorraum über K, $\operatorname{Hom}(V,V)$ ist zudem ein Ring mit 1[39].

- Addition: $v(\alpha+\beta) := v\alpha + v\beta$ (mit $v \in V$ und $\alpha, \beta \in \operatorname{Hom}(V,V)$)
- Skalarmultiplikation: $v(k\alpha) := k(v\alpha)$ (mit $k \in K, v \in \operatorname{Hom}(V,V)$)
- Multiplikation: $v(\alpha\beta) := (v\alpha)\beta$

$K[x]$ ist Polynomring über K, also kommutativ mit 1, nullteilerfrei und Hauptideal. $\sum_{i=0}^{n} k_i\varphi^i \in \operatorname{Hom}(V,V)$ (mit $k_i \in K$; beachte: $\varphi^0 := \mathrm{id}$).

$$\mu_\varphi : K[x] \to \operatorname{Hom}(V,V)$$

$$\mu_\varphi : \sum_{i=0}^{n} k_i x^i \mapsto \sum_{i=0}^{n} k_i \varphi^i$$

Die Abbildung μ_φ ist sowohl Vektorraum-Homomorphismus wie auch Ringhomomorphismus.

Bezeichnung: $K[\varphi] := \operatorname{Bild} \mu_\varphi$; Insbesondere ist $K[\varphi]$ ein kommutativer Ring.

7.1 Elementare Eigenschaft von Ringhomomorphismen

Seien $R, \tilde{R}$ Ringe und $\mu : R \to \tilde{R}$ ein Ringhomomorphismus.

- Ist I ein Ideal von R, so ist das Bild $I\varphi$ ein Ideal von $R\varphi$.
- Ist $\tilde{I}$ ein Ideal von $\tilde{R}$, so ist das Urbild $\tilde{I}\mu^{-1}$ ein Ideal von R[40].

Wiederholung Idealeigenschaften: I ist Ideal von R, wenn $I + I \subseteq I$ und $RI \subseteq I$ (und $IR \subseteq I$, falls R nicht kommutativ).

Beweis:

- Seien $a, b \in I$. Zu zeigen: $a\mu + b\mu \in I\mu$. Es gilt: $a\mu + b\mu = (a+b)\mu$ Da $(a+b) \in I$, ist $(a+b)\mu \in I\mu$.

  Seien nun $a \in I, r \in R$. Zu zeigen: $(r\mu)(a\mu) \in I\mu$. Es gilt: $(r\mu)(a\mu) = (ra)\mu$. Da $ra \in I$, ist $(ra)\mu \in I\mu$ (andere Richtung analog).

[39] Strukturen, die gleichzeitig Vektorraum und Ring sind, heißen *Algebra*.

[40] $\tilde{I}\mu^{-1} := \left\{ a \in R \mid a\mu \in \tilde{I} \right\}$

- Seien $a, b \in \tilde{I}\mu^{-1}$, d.h. $\exists\, \tilde{a} \in \tilde{I}$ und $\tilde{b} \in \tilde{I}$ mit $a\mu = \tilde{a}$ und $b\mu = \tilde{b}$. Es gilt: $(a+b)\mu = a\mu + b\mu = \tilde{a} + \tilde{b} \in \tilde{I}$, damit ist $(a+b) \in \tilde{I}\mu^{-1}$.

  Seien nun $a \in \tilde{I}\mu^{-1}, r \in R$. Es gilt: $(ra)\mu = (r\mu)(a\mu)$, weiterhin $r\mu \in \tilde{R}$ und $a\mu \in \tilde{I}$, damit $(r\mu)(a\mu) \in \tilde{I}$ (andere Richtung analog). □

7.2 Annulatoren

Sei $\emptyset \neq U \subseteq V$. Sei $I_U := \{\alpha \in K[\varphi] \mid U\alpha = \{0\}\}$. I_U ist Ideal von $K[\varphi]$. Also ist $I_U\mu^{-1}$ Ideal von $K[x]$, das Urbild heißt *Annulatorideal* von U (bezüglich φ), geschrieben $\mathrm{Ann}_\varphi(U)$.

Gilt $U \subseteq U' \subseteq V$, so ist $\mathrm{Ann}_\varphi(U') \subseteq \mathrm{Ann}_\varphi(U)$.

$K[x]$ ist *Hauptidealring*: Es existiert $m_\varphi(U) \in \mathrm{Ann}_\varphi(U)$ mit $\mathrm{Ann}_\varphi(U) = K[x]m_\varphi(U)$. Eindeutig ist $m_\varphi(U)$ bestimmt, wenn wir verlangen, daß es entweder 0 ist oder Leitkoeffizient 1 hat. Dann nennen wir $m_\varphi(U)$ den *φ-Annulator* von U.

Für $U = V$ heißt $m_\varphi := m_\varphi(V)$ das *Minimalpolynom* von φ.

Einfache Beispiele:

1. $V = \{0\}$; damit ist $\mathrm{Hom}(V, V) = \{0\}$; $\mathrm{Ann}_\varphi(V) = K[x]$; $m_\varphi = 1 \cdot x^0 = 1$; $\mathrm{grad}\, m_\varphi = 0$.

2. $\mathrm{Ann}_\varphi(V) = K[x]$; also $m_\varphi = 1$; damit $m_\varphi(\varphi) = \mathrm{id}$, also $V = \{0\}$

   Es gilt also: $\mathrm{grad}\, m_\varphi = 0 \Leftrightarrow V = \{0\}$.

3. Sei $V \neq \{0\}$ und $\varphi = 0$; $\mathrm{Ann}_\varphi(V) = K[x]x$; $m_\varphi = x$; $m_\varphi(\varphi) = \varphi$.

4. Sei $V \neq \{0\}$ und $\varphi = \mathrm{id}$; d.h. $\varphi - \mathrm{id} = 0$, also $(x-1) \in \mathrm{Ann}_\varphi(V)$ und $m_\varphi = x - 1$

5. Sei $V \neq \{0\}$ und $v\varphi = kv$ für ein $0 \neq v \in V$ und ein $k \in K$; die 1 ist nicht in $\mathrm{Ann}_\varphi(v)$. Es gilt: $v\varphi - kv = 0 = v\varphi - v(k\varphi^0) = v(\varphi - k\varphi^0)$, also ist $x - k \in \mathrm{Ann}_\varphi(v)$. Damit ist auch schon $m_\varphi(v) = x - k$.

7.3 Eigenwerte, Eigenvektoren, Eigenräume

7.3.1 Existenz/Erzeugung von Annulatoren

Sei $\emptyset \neq U \subseteq V$. Dann ist $\mathrm{Ann}_\varphi(U) \neq \{0\}$. Insbesondere ist $\mathrm{Ann}_\varphi(V) \neq \{0\}$.

Beweis: Es gilt: $\mathrm{Ann}_\varphi(V) \subseteq \mathrm{Ann}_\varphi(U)$; es genügt also zu zeigen: $\mathrm{Ann}_\varphi(V) \neq \{0\}$ zu zeigen.

- Ist $V = \{0\}$, dann ist $\mathrm{Ann}_\varphi(V) = K[x] \neq \{0\}$.
- Sei $V \neq \{0\}$ und $0 \neq v \in V$, und sei $n := \dim V (\geq 1)$. Die Elemente $v\varphi^0, ..., v\varphi^n$ ($n+1$ Stück) sind linear abhängig. Es existieren $k_0, ..., k_n \in K$, nicht alle null, mit $\sum_{i=0}^n k_i v\varphi^i = 0$.

  D.h. $v\left(\sum_{i=0}^n k_i\varphi^i\right) = 0$. Damit: $\sum_{i=0}^n k_i x^i \in \mathrm{Ann}_\varphi(v)$.

VORAUSSETZUNG: Sei $v_1, ..., v_n$ eine Basis von V. Eben gesehen: $\mathrm{Ann}_\varphi(v_i) \neq \{0\}$. Seien $m_\varphi(v_i) =: m_i$ die entsprechenden Annullatoren. Sei $m := \prod_{i=1}^n m_i \neq 0$ (Nullteilerfreiheit).

BEHAUPTUNG: $m \in \mathrm{Ann}_\varphi(V)$

BEWEIS: Es genügt zu zeigen: $v_i m(\varphi) = 0 \; \forall \; i = 1, ..., n$. Es gilt:

$$\begin{aligned} v_i m(\varphi) &= v_i \prod_{j=1}^n m_j(\varphi) \\ &= v_i m_i(\varphi) \prod_{j\neq i} m_j(\varphi) \\ &= 0 \prod_{j\neq i} m_j(\varphi) = 0 \end{aligned}$$

Damit ist $m \in \mathrm{Ann}_\varphi(V)$ und somit $\mathrm{Ann}_\varphi(V) \neq \{0\}$. □

7.3.2 Definition von Eigenwert, -vektor und -räumen

Sei $k \in K$. Dann sind äquivalent:

1. k ist Nullstelle von m_φ
2. Es existiert $0 \neq v \in V$ mit $v\varphi = kv$.

BEWEIS:

„$\Rightarrow$“ k ist also Nullstelle von m_φ. Damit ist[41] $m_\varphi = (x-k)h$ für ein $h \in K[x]$ mit $\operatorname{grad} h < \operatorname{grad} m_\varphi$. Wegen $\operatorname{grad} h < \operatorname{grad} m_\varphi$ gilt: $h \notin \mathrm{Ann}_\varphi(V)$, d.h. $\exists\, 0 \neq w \in V$ mit $wh(\varphi) \neq 0$. Setze $v := wh(\varphi)$.

$$\begin{aligned} 0 &= wm_\varphi(\varphi) \\ &= wh(\varphi)(\varphi - k \cdot \mathrm{id}) \\ &= v(\varphi - k\cdot \mathrm{id}) \\ &= v\varphi - v(k \cdot \mathrm{id}) \\ \Rightarrow v\varphi &= kv \end{aligned}$$

[41] offiziell 6.7/bei mir 6.11

„$\Leftarrow$" Es existiert $0 \neq v \in V$ mit $v\varphi = kv$. $m_\varphi, (x-k) \in \mathrm{Ann}_\varphi(v)$ und $x-k = m_{\varphi,v}$ (siehe Beispiel). Damit existiert $h \in K[x]$ mit $m_\varphi = (x-k)h$ (Hauptidealeigenschaften). Damit ist k eine Nullstelle von m_φ. □

DEFINITION:

- $k \in K$ heißt *Eigenwert* von φ, falls eine der gerade als äquivalenten bewiesenen Aussagen für k gilt.
- Ist k Eigenwert von φ, so heißt ein $v \in V$ mit $v \neq 0$ und $v\varphi = kv$ *Eigenvektor* von φ zum Eigenwert k.
- $V(k) = \{v \in V \mid v\varphi = kv\}$ heißt *Eigenraum* von φ zum Eigenwert k.

Beachte: $V(k)$ ist Unterraum von V, und es gilt: $V(k)\varphi \subseteq V(k)$ (da für $w \in V(k)$ gilt: $(w\varphi)\varphi = (kw)\varphi = k(w\varphi)$).

BEISPIELE für $V \neq \{0\}$:

- $\varphi = \mathrm{id}$: Eigenwert ist 1, denn $v\varphi = v = 1v$; dies ist auch der einzige Eigenwert von φ. Der Eigenraum: $V(1) = V$.
- $\varphi = 0$: der einzige Eigenwert ist 0, $V(0) = V$.[42]
- $\varphi = k \cdot \mathrm{id}$: der einzige Eigenwert ist k, $V(k) = V$.
- $\det \varphi = 0$: Eigenwert 0, Eigenraum: $V(0) = \mathrm{Kern}\,\varphi \neq \{0\}$.
- Sei 0 Eigenwert von φ. Dann folgt: $\mathrm{Kern}\,\varphi \neq \{0\} \Rightarrow \det \varphi = 0$.
- $K = \mathbb{C}$, Basis v_1, v_2 von V und $v_1\varphi = v_2$ sowie $v_2\varphi = -v_1$. Seien $k, k_1, k_2 \in K$ mit $(k_1v_1 + k_2v_2)\varphi = k(k_1v_1 + k_2v_2)$.

$$\begin{aligned}
(k_1v_1 + k_2v_2)\varphi &= (k_1v_1)\varphi + (k_2v_2)\varphi \\
&= k_1v_2 - k_2v_1 \\
&= kk_1v_1 + kk_2v_2) \\
\Rightarrow k_1 &= kk_2 \\
\wedge - k_2 &= kk_1 \\
\Rightarrow -k_2 &= k^2k_2
\end{aligned}$$

Daraus folgt entweder $k_2 = 0$ und damit auch $k_1 = 0$, also $k_1v_1 + k_2v_2 = 0$, oder $k = \pm i$, dann ist $k_1 = \pm ik_2$.

- $V(i) = \{h(v_i - iv_2) \mid h \in K\}$
- $V(-i) = \{h(v_i + iv_2) \mid h \in K\}$

[42]„Ein Physiker würde sagen: super, klappt immer, es gibt immer nur einen Eigenwert und der Eigenraum ist immer gleich V"

7.3.3 Unabhängigkeit von Eigenvektoren, Anzahl der Eigenwerte

Seien $a_1, ..., a_n$ paarweise verschiedene Eigenwerte von φ und $v_1, ..., v_n$ entsprechende Eigenvektoren. Dann sind $v_1, ..., v_n$ linear unabhängig. Insbesondere existieren höchstens $\dim V$ verschiedene Eigenwerte von φ.

Beweis: Angenommen, v_1 bis v_n sind linear abhängig, d.h. es existieren $k_1, ..., k_n \in K$, nicht alle gleich null, mit $\sum_{i=1}^{n} k_i v_i = 0$.

Seien $k_1, ..., k_r \in K$ $(r \leq n)$ nicht alle Null mit $\sum_{i=1}^{r} k_i v_i = 0$ und r minimal mit dieser Eigenschaft. Damit ist $k_r \neq 0$ und $r \geq 2$.

$$\begin{aligned}
0 &= a_r \sum_{i=1}^{r} k_i v_i - \left(\sum_{i=1}^{r} k_i v_i\right)\varphi \\
&= \sum_{i=1}^{r} a_r k_i v_i - \left(\sum_{i=1}^{r} k_i a_i v_i\right) \\
&= \sum_{i=1}^{r} (a_r - a_i) k_i v_i \\
&= (a_r - a_r) k_r v_r + \sum_{i=1}^{r-1} (a_r - a_i) k_i v_i \\
&= \sum_{i=1}^{r-1} (a_r - a_i) k_i v_i
\end{aligned}$$

Mit der Minimalität von r: $(a_r - a_i)k_i = 0$ für ein $i = 1, ..., r-1$; zudem $a_r - a_i \neq 0$ (da $a_r \neq a_i$), also ist $k_i = 0$ für $i = 1, ..., r-1$. Also ist $k_r = 0$ im Widerspruch zur Wahl der k_i. □

7.4 Direkte Summen und Diagonalisierbarkeit

7.4.1 Direkte Summe

Seien $V_1, ..., V_n$ Unterräume von V. Gilt

1. $V = \sum_{i=1}^{n} V_i$ und
2. $V_i \cap \sum_{j \neq i} V_j = \{0\}$

Dann heißt V die *direkte Summe* der Unterräume $V_1, ..., V_n$. In Zeichen:

$$V = V_1 \oplus ... \oplus V_n = \bigoplus_{i=1}^{n} V_i$$

7.4.2 Kriterien für direkte Summen

Seien $V_1, ..., V_n$ Unterräume von V und $V = \sum_{i=1}^n V_i$. Dann sind äquivalent:

(a) $V = \bigoplus\limits_{i=1}^{n} V_i$

(b) Zu jedem $v \in V$ und $i \in \{1, ..., n\}$ existiert genau ein $v_i \in V_i$ mit $v = \sum_{i=1}^n v_i$

(c) Seien $0 \neq v_i \in V_i$ für $i = 1, ..., n$. Dann sind die Elemente $v_1, ..., v_n$ linear unabhängig.

(d) $\dim V = \sum_{i=1}^n \dim V_i$

Beweis:

(a) $\Rightarrow$ (b) Sei $v \in V$, seien $v_i, v_i' \in V_i$ und $v = \sum_{i=1}^n v_i = \sum_{i=1}^n v_i'$. Zu zeigen: $v_i = v_i' \; \forall \, i$. Es gilt:

$$V_i \ni v_i - v_i' = \sum_{i \neq j} v_j' - v_j \in \sum_{i \neq j} V_j$$

Damit ist nach Definition der direkten Summe: $v_i - v_i' \in V_i \cap \sum_{j \neq i} V_j = \{0\}$, also $v_i = v_i'$.

(b) $\Rightarrow$ (c) Seien $0 \neq v_i \in V_i$, $i = 1, ..., n$. Seien $k_1, ..., k_n \in K$ mit $\sum_{i=1}^n k_i v_i = 0$. Zu zeigen: $k_1 = ... = k_n = 0$. Es gilt: $k_i v_i \in V_i$. Nach Voraussetzung ist $0 \in V$ nur auf eine Weise als Kombination der Elemente aller V_i darstellbar, also $0_V = 0_{V_1} + ... + 0_{V_n}$, damit $k_i v_i = 0$ für alle i.

(c) $\Rightarrow$ (d) Wähle B_i als Basis von V_i für alle $i = 1, ..., n$. Setze $B := \bigcup\limits_{i=1}^{n} B_i$. Dann ist

$$B_i \cap \bigcup_{j \neq i} B_i = \emptyset \Rightarrow |B| = \sum_{i=1}^{n} |B_i| = \sum_{i=1}^{n} \dim V_i$$

Es genügt zu zeigen: B ist Basis von V. $\langle B \rangle \geq \langle B_i \rangle$ für alle $i = 1, ..., n$. Damit gilt: $V = \sum_{i=1} nV_i \leq \langle B \rangle \leq V$.

Sei $k_b \in K$, $b \in B$ und $\sum_{b \in B} k_b b = 0$. Dann ist

$$0 = \underbrace{\sum_{b \in B_1} k_b b}_{\in V_1} + ... + \underbrace{\sum_{b \in B_n} k_b b}_{\in V_n}$$

Nach Voraussetzung ist $\sum_{b \in B_i} k_b = 0 \; \forall \, i$. B_i ist Basis von V_i, also linear unabhängig. Also ist $k_b = 0 \; \forall \, b \in B_i \; \forall \, i$

(d) $\Rightarrow$ (a) Es ist zu zeigen: $V_i \cap \sum_{j \neq i} V_j = \{0\}$. Es ist $V = V_j + \sum_{i \neq j} V_j$. Mit Dimensionsformel folgt:

$$\begin{aligned}
\dim V &= \dim V_i + \dim\left(\sum_{j \neq i} V_j\right) - \dim\left(V_i \cap \sum_{j \neq i} V_j\right) \\
&\leq \dim V_i + \sum_{j \neq i} V_j - \dim\left(V_i \cap \sum_{j \neq i} V_j\right) \\
&= \dim V - \dim\left(V_i \cap \sum_{j \neq i} V_j\right) \\
\Rightarrow 0 &= \dim\left(V_i \cap \sum_{j \neq i} V_j\right)
\end{aligned}$$

7.4.3 Direkte Summe der Eigenräume

Seien $a_1, ..., a_n$ paarweise verschiedene Eigenwerte von φ. Dann gilt:

$$\sum_{i=1}^{n} V(a_i) = V(a_1) \oplus ... \oplus V(a_n)$$

Beweis: Wende (7.3.3) und (7.4.2) (c) $\Rightarrow$ (a) an.

7.4.4 Teiler, teilerfremd

$g, h \in K[x]$. Wir sagen g *teilt* h, falls ein $u \in K[x]$ existiert mit $h = gu$ (in Zeichen $g|h$). Seien $g, h \in K[x] \setminus K$. Dann heißen g und h *teilerfremd*, falls kein $u \in K[x] \setminus K$ existiert mit $u|g$ und $u|h$.

7.4.5 Kern von zwei Teilern von Polynomen auf Abbildungen

Seien $g_1, g_2 \in K[x] \setminus K$ teilerfremd und $f := g_1 g_2$. Dann gilt:

$$\operatorname{Kern} f(\varphi) = \operatorname{Kern} g_i(\varphi) \oplus \operatorname{Kern} g_2(\varphi)$$

Beweis: Setze $W := \operatorname{Kern} f(\varphi)$ und $W_i := \operatorname{Kern} g_i(\varphi)$. Sei $w \in W_1 \cap W_2$. Sei $h = m_\varphi(W)$.

- Beachte: $W_i \varphi \leq W_i$, denn $\varphi g_i(\varphi) = g_i(\varphi)\varphi$. Insbesondere $W_i g_j(\varphi) \leq W_i$.

- $g_1, g_2 \in K[x] \cdot h$; es gilt: $0 = wh(\varphi)$, $h|g_1$ und $h|g_2$. Mit der Teilerfremdheit von g_1, g_2 folgt: $h \in K$. Damit: $0 = wh(\varphi) = hw$. Da $h \neq 0$ folgt: $w = 0$. Damit ist $W_1 \cap W_2 = \{0\}$.

- Es bleibt zu zeigen: $W = W_1 + W_2$. Doppelte Inklusion:

  „$\subseteq$" Sei $v \in W$. Setze $v_1 := vg_2(\varphi)$ und $v_2 := vg_1(\varphi)$. Dann gilt:

  $$v_1 g_i(\varphi) = vg_2(\varphi g_1(\varphi) = vf(\varphi) = 0$$

  Damit ist $v_1 \in W_1$, genauso $v_2 \in W_2$. $g_i(\varphi) : W_j \to W_j$ ist für $i \neq j$ eine injektive lineare Abbildung, denn $\operatorname{Kern} g_i(\varphi) \cap W_j = W_i \cap W_j = \{0\}$. Da W_j endlich dimensional ist, ist $g_i(\varphi)$ auch surjektiv (damit bijektiv).

  Also existiert ein $v'_j \in W_j$ mit $v'_j g_i(\varphi) = v_j$. Sei $u := v - v'_1 - v'_2$. Dann ist

  $$\begin{aligned} ug_1(\varphi) &= \underbrace{vg_1(\varphi)}_{=v_2} - \underbrace{v'_1 g_1(\varphi)}_{=0} - \underbrace{v'_2 g_1(\varphi)}_{=v_2} = 0 \\ ug_2(\varphi) &= \underbrace{vg_2(\varphi)}_{=v_1} - \underbrace{v'_1 g_2(\varphi)}_{=v_1} - \underbrace{v'_2 g_2(\varphi)}_{=0} = 0 \end{aligned}$$

  Damit folgt: $u \in \operatorname{Kern} g_1(\varphi) \cap \operatorname{Kern} g_2(\varphi) = \{0\}$, also $u = 0$. Damit ist $v = v'_1 + v'_2 \Rightarrow v \in W_1 + W_2$, also $W \subseteq W_1 + W_2$.

  „$\supseteq$" $W_i f(\varphi) = W_i g_1(\varphi) g_2(\varphi) = \{0\}$, damit $W_i \subseteq W$

7.4.6 Kern von mehreren Teilern von Polynomen auf Abbildungen

Seien $g_1, ..., g_n$ paarweise teilerfremde Polynome aus $K[x]$ und $f = g_1 \cdot ... \cdot g_n$. Dann gilt:

$$\operatorname{Kern} f(\varphi) = \bigoplus_{i=1}^{n} \operatorname{Kern} g_i(\varphi)$$

Beweis: Induktion nach n:

- Verankerung: trivial für $n = 1$, für $n = 2$ gerade gezeigt.

- Annahme: Sei $n \geq 3$ und die Behauptung richtig für $n - 1$.

- Schluß: Setze $h_i = \prod\limits_{j \neq i} g_j$. Nach [6.6] sind h_i und g_i teilerfremd. Dann ist $\operatorname{Kern} f(\varphi) = \operatorname{Kern} g_i(\varphi) \oplus \operatorname{Kern} h_1(\varphi)$. Mit der Induktionsannahme ist $\operatorname{Kern} h_i(\varphi) = \bigoplus\limits_{j \neq i} \operatorname{Kern} g_j(\varphi)$. Damit ist $\operatorname{Kern} f(\varphi) = \bigoplus_{i=1}^{n} \operatorname{Kern} g_i(\varphi)$.

7.4.7 Diagonalisierbarkeit

φ heiß *diagonalisierbar*, falls eine Basis B von V existiert, so daß $M(\varphi, B, B)$ eine Diagonalmatrix ist (d.h. nur in der Diagonalen stehen Koeffizienten ungleich 0).[43] Damit gilt für $b_i \in B$: $b_i\varphi = a_{ii}b_i$. Damit ist φ genau dann diagonalisierbar, wenn V eine Basis von Eigenvektoren von φ besitzt.

7.4.8 Diagonalisierbarkeitskriterium

φ ist genau dann diagonalisierbar, wenn es paarweise verschiedene Eigenwerte $a_1, ..., a_r$ von φ gibt mit

$$m_\varphi = \prod_{i=i} r(x - a_i)$$

Beweis:

„$\Rightarrow$" Sei φ diagonalisierbar. Dann existiert eine Basis von Eigenvektoren. Sei a_i der Eigenwert zu v_i für $i = 1, ..., n$. Sei die Numerierung[44] und r so gewählt, daß $a_1, ..., a_r$ paarweise verschieden und $\{a_1, .., a_r\} = \{a_1, ..., a_n\}$. Es gilt $V(a_i) = \text{Kern}(\varphi - a_i \cdot id)$ wegen

$$w \in \text{Kern}(\varphi - a_i \cdot \text{id}) \Leftrightarrow w(\varphi - a_i \cdot \text{id}) = 0 \Leftrightarrow w\varphi = a_i \cdot w \Leftrightarrow w \in V(a_i)$$

Sei $g := \prod_{i=1}^{r}(x - a_i)$. Dann gilt (mit j so gewählt, daß v_l Eigenvektor zu a_j):

$$v_l g(\varphi) = v_l(\varphi - a_j \cdot \text{id}) \prod_{i \neq j}(\varphi - a_i \cdot \text{id}) = 0$$

Damit ist Kern $g(\varphi) = V$. Wir haben gezeigt: $g \in K[x]m_\varphi$, d.h. $m_\varphi | g$. Nach (6.7) und Definition von Eigenwert gilt auch $g | m_\varphi$. Insbesondere: $\text{grad}\, g = \text{grad}\, m_\varphi$, beide haben Leitkoeffizient 1, also $g = m_\varphi$.

Noch mal ausführlicher: $g = hm_\varphi$ und $m_\varphi = h'g$ für je ein $h, h' \in K[x]$, mit Gradgleichung: $h, h' \in K$, da beide Leitkoeffizient 1 haben: $h = h' = 1$.

„$\Leftarrow$" Sei $m_\varphi = \prod_{i=1}^{r}(x - a_i)$ und $a_1, ..., a_r$ paarweise verschieden. Beachte: $(x - a_1), ..., (x - a_r)$ sind paarweise teilerfremd. Nach (7.4.6) ist

$$\begin{aligned} V &= \text{Kern}\, m_\varphi(\varphi) \\ &= \text{Kern}(\varphi - a_i \cdot \text{id}) \oplus ... \oplus \text{Kern}(\varphi - a_r \cdot \text{id}) \\ &= V(a_1) \oplus ... \oplus V(a_r) \end{aligned}$$

[43] „Zweites Semester sind sie jetzt... ich ja auch."

[44] „Wie wird heutzutage *Num(m)erierung* geschrieben? Mit zwei *m*? Ach, das ist mir egal!"

Sei B_i Basis von $V(a_i)$ für $i = 1, ..., r$, damit ist $\bigcup B_i =: B$ Menge von Eigenvektoren und $\langle B \rangle = V$. Mit (7.4.2) ist B linear unabhängig.

7.5 Das charakteristische Polynom

Sei $n := \dim V \geq 1$. Es ist $K \subseteq K[x] \subseteq K(x)$ (Körper der rationalen Funktionen)[45]. Sei B Basis von V und $A := M(\varphi, B, B)$. Dann ist

$$\begin{pmatrix} x - a_{11} & \cdots & -a_{1n} \\ \vdots & \ddots & \vdots \\ -a_{n1} & \cdots & x - a_{nn} \end{pmatrix} = x \cdot I_{n\times n} - A \in \mathcal{M}_{n\times n}(K(x))$$

DEFINITION:

$$f_\varphi := \det(xI_{n\times n} - A) \in K(x)$$

Sei B' eine weitere Basis, dann gilt:

$$\begin{aligned}
U &:= M(\mathrm{id}, B', B) \\
U^{-1} &= M(\mathrm{id}, B, B') \\
UU^{-1} &= I_{n\times n} \\
M(\varphi, B', B') &= U \cdot M(\varphi, B', B') \cdot U^{-1} \\
\det(xI_{n\times n} - UAU^{-1}) &= \det U(xI_{n\times n} - A)U^{-1} \\
&= \det U \cdot \det(xI_{n\times n} - A) \cdot \det U^{-1} \\
&= \det U \cdot \det U^{-1} \cdot \det(xI_{n\times n} - A) \\
&= \det I_{n\times n} \cdot \det(xI_{n\times n} - A) \\
&= 1 \cdot \det(xI_{n\times n} - A) \\
&= \det(xI_{n\times n} - A) \\
&= f_\varphi
\end{aligned}$$

Damit ist f_φ unabhängig von der Basis, f_φ heißt das *charakteristische Polynom*.

[45] „Wenn sie das erstmal haben, haben sie mehr zum Spielen - wie im Sandkasten!“

Sei $xI_{n\times n} - A =: B = (b_{ij})_{n\times n}$. Dann ist

$$\begin{aligned}
\det B &= \sum_{\sigma\in S_n} (\operatorname{sgn}\sigma)\left(\prod_{i=1}^{n} b_{ij}\sigma\right)\\
&= \prod_{i=1}^{n} b_{ii} + \sum_{1\neq\sigma\in S_n} (\operatorname{sgn}\sigma)\left(\prod_{i=1}^{n} b_{ij}\sigma\right)\\
&= \underbrace{\prod_{i=1}^{n}(x-a_{ii})}_{grad\ n} + \underbrace{\sum_{1\neq\sigma\in S_n} (\operatorname{sgn}\sigma)\left(\prod_{i=1}^{n} b_{ij}\sigma\right)}_{grad<n}
\end{aligned}$$

Beachte: $b_{ij} = -a_{ij}$ für $i \neq j$ und $b_{ii} = x - a_{ii}$. Damit ist $\det B \in K[x]$, grad $f_\varphi = n$, Leitkoeffizient 1!

Beispiel:

1.

$$\begin{aligned}
A := M(\varphi, B, B) &= \begin{pmatrix} 0 & 0 & 1 & 1\\ 0 & 1 & 0 & 0\\ 0 & -1 & 0 & -1\\ 0 & 1 & 1 & 2 \end{pmatrix}\\
xI_{n\times n} - A &= \begin{pmatrix} x & 0 & -1 & -1\\ 0 & x-1 & 0 & 0\\ 0 & 1 & x & 1\\ 0 & -1 & -1 & x-2 \end{pmatrix}\\
\det xI_{n\times n} - A &= (x-1)\cdot\det\begin{pmatrix} x & -1 & -1\\ 0 & x & 1\\ 0 & -1 & x-2 \end{pmatrix}\\
&= (x-1)\cdot x\cdot\det\begin{pmatrix} x & 1\\ -1 & x-2 \end{pmatrix}\\
&= (x-1)\cdot x\cdot(x^2-2x+1)\\
&= x\cdot(x-1)^3
\end{aligned}$$

2.

$$
\begin{aligned}
A &:= \begin{pmatrix} 4 & -6 & -15 \\ 0 & 1 & 0 \\ 1 & -2 & -4 \end{pmatrix} \\
xI_{n\times n} - A &= \begin{pmatrix} x-4 & 6 & 15 \\ 0 & x-1 & 0 \\ -1 & 2 & x+4 \end{pmatrix} \\
\det xI_{n\times n} - A &= (x-1)\cdot\det\begin{pmatrix} x-4 & 15 \\ -1 & x+4 \end{pmatrix} \\
&= (x-1)(x^2-1) \\
&= (x-1)^2(x+1)
\end{aligned}
$$

7.5.1 Nullstellen des charakteristischen Polynoms

Sei $a \in K$. a ist genau dann Eigenwert von φ, wenn a Nullstelle des Charakteristischen Polynoms f_φ.

Beweis: Sei $k \in K$. Dann ist

$$
\begin{aligned}
f_\varphi(k) &= \det(k \cdot I_{n\times n} - M(\varphi, B, B)) \\
&= \det(M(k \cdot \mathrm{id}, B, B) - M(\varphi, B, B)) \\
&= \det(k \cdot \mathrm{id} - \varphi) \\
f_\varphi(a) &= 0 = \det(a \cdot \mathrm{id} - \varphi)
\end{aligned}
$$

Damit ist $(a \cdot \mathrm{id} - \varphi)$ nicht invertierbar, damit ist $\mathrm{Kern}(a \cdot \mathrm{id} - \varphi) \neq \{0\}$, also existiert von $0 \neq v \in V$ mit $v(a \cdot \mathrm{id} - \varphi) = 0$. Damit existiert ein $0 \neq v \in V$ mit $va = v\varphi$, also ist a Eigenwert. Alle Schritte des Beweises sind äquivalent.

7.5.2 Char. Polynom im invarianten Unter- und Faktorraum

Sei $U \leq V$ Unterraum. U heißt *φ-invariant*, falls $U\varphi \subseteq U$.

Sei U ein φ-invarianter Unterraum. Sei $\varphi|_U$ die Einschränkung von φ auf U. Dann ist $\varphi|_{V/U}$ die auf V/U induzierte lineare Abbildung:

$$\varphi|_{V/U} : v + U \mapsto v\varphi + U$$

Es gilt:

$$f_\varphi = f_{\varphi|_U} \cdot f_{\varphi|_{V/U}} \text{ und } m_{\varphi|_U} \cdot m_{\varphi|_{V/U}} \in K[x]m_\varphi$$

Beweis: Für $U = \{0\}$ offensichtlich. Sei $\dim U =: r \geq 1$.

Sei $B := \{b_1, ..., b_r, b_{r+1}, ..., b_n\}$ eine Basis von V (mit $n := \dim V$), wobei

$B_1 := \{b_1, ..., b_r\}$ eine Basis von U ist. Sei $\overline{B_1} = (B \setminus B_1) + U = \{b_{r-1} + U, ..., b_n + U\}$.

$$\begin{aligned}
M(\varphi, B, B) &= \begin{pmatrix} A & 0 \\ C & D \end{pmatrix} \in \mathcal{M}_{n\times n}(K) \\
A &= M(\varphi|_U, B_1, B_1) \in \mathcal{M}_{r\times r}(K) \\
D &= M(\varphi|_{V/U}, \overline{B_1}, \overline{B_1}) \in \mathcal{M}_{n-r\times n-r}(K) \\
xI_{n\times n} - M(\varphi, B, B) &= \begin{pmatrix} A' & 0 \\ C' & D' \end{pmatrix} \\
f_{\varphi|_U} &= \det(\underbrace{xI_{r\times r} - A}_{A'}) \\
f_{\varphi|_{V/U}} &= \det(\underbrace{xI_{n-r\times n-r} - D}_{D'}) \\
{}_{\text{Entwicklungssatz}}\ f_\varphi &= \det A' \cdot \det D' \\
&= f_{\varphi|_U} \cdot f_{\varphi|_{V/U}} \\
(m_{\varphi|_U} \cdot m_{\varphi|_{V/U}})(\varphi) &= m_{\varphi|_{V/U}}(\varphi) \cdot m_{\varphi|_U}(\varphi) \\
\underbrace{vm_{\varphi|_{V/U}}(\varphi)}_{\in U} m_{\varphi|_U}(\varphi) &= 0
\end{aligned}$$

7.5.3 Matrix mit Minimalpolynom = char. Pol

Sei $\dim V \geq 1$, $r := \operatorname{grad} m_\varphi$ und $m_\varphi = \sum_{i=0}^r a_i x^i$. Es existiert ein $v \in V$ mit $V = \langle v\varphi^i | i \in \mathbb{N}\rangle$. Dann ist $\dim V = r$ und $B = \{v\varphi^0, ..., v\varphi^{r-1}\}$ eine Basis von V und es gilt:

$$M(\varphi, B, B) = \begin{pmatrix}
0 & 1 & 0 & 0 & \cdots & 0 \\
0 & 0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 0 & 1 & \ddots & 0 \\
\vdots & \vdots & \vdots & \ddots & \ddots & 0 \\
0 & 0 & 0 & 0 & 0 & 1 \\
-a_0 & -a_1 & -a_2 & -a_3 & \cdots & -a_{n-1}
\end{pmatrix}$$

Beweis: Beachte $r \geq 1$. Es gilt: $m_{\varphi,v}(v) = \varphi^k m_{\varphi,v}(\varphi)$, d.h.

$$0 = \underbrace{vm_{\varphi,v}(\varphi)}_{0} \varphi^k = (v\varphi^k) m_{\varphi,v}(\varphi)$$

Damit ist $m_{\varphi,v} \in K[x]m_\varphi$, also $m_\varphi | m_{\varphi,v}$. Andererseits: $m_\varphi \in K[x]m_{\varphi,v}$, d.h. $m_{\varphi,v} | m_\varphi$. Damit gilt: $m_\varphi = m_{\varphi,v}$

Als nächstes zeigen wir: $v\varphi^0, ..., v\varphi^{r-1}$ sind linear unabhängig. Seien $w = \sum_{i=0}^{r-1} k_i(v\varphi^i)$ eine Linearkombination mit $k_i \in K$. Sei $g := \sum_{i=0}^{r-1} k_i x^i$. Dann ist $w = vg(\varphi)$.

Genau dann ist $w = 0$, wenn $g \in \mathrm{Ann}_\varphi(v) = K[x]m_{\varphi,v} = K[x]m_\varphi$. Damit ist $g = 0$ oder $r = \operatorname{grad} m_\varphi \leq \operatorname{grad} g = r - 1$, der zweite Fall kann nicht sein. Damit ist $g = 0$, also $k_0 = ... = k_{r-1} = 0$, also $v\varphi^0, ..., \varphi^{r-1}$ linear unabhängig.

Angenommen, $V > W := \langle v\varphi^0, ..., v\varphi^{r-1}\rangle$. Es existiert ein $v\varphi^k \in V \setminus W$, sei zusätzlich k minimal mit dieser Eigenschaft. Es ist $k \geq r$. Das Element $v\varphi^{r-1}$ liegt wegen der Minimalität von k in W. Damit existiert eine Linearkombination:

$$\begin{aligned}
v\varphi^{k-1} &= \sum_{i=0}^{r-1} h_i v\varphi^i \\
(v\varphi^{k-1})\varphi &= \left(\sum_{i=0}^{r-1} h_i v\varphi^i\right)\varphi \\
&= \sum_{i=1}^{r} h_{i-1} v\varphi^i \\
&= \underbrace{.....}_{\in W} + h_{r-1} v\varphi^r \\
\Rightarrow \underbrace{h_{r-1}}_{\neq 0} v\varphi^r &\notin W \\
\Rightarrow v\varphi^r &\notin W
\end{aligned}$$

Da k minimal ist, ist $k = r$.

$$\begin{aligned}
0 &= vm_\varphi(\varphi) \\
&= \sum_{i=0}^{r-1} a_i v\varphi^i + \underbrace{a_r}_{=1} v\varphi^r \\
v\varphi^r &= -\sum_{i=0}^{r-1} a_i v\varphi^i \in W
\end{aligned}$$

Damit ist $v\varphi^r \in W$, Widerspruch, also ist es eine Basis.

Wir haben gezeigt: $B = \{v\varphi^0, ..., v\varphi^{r-1}\}$ ist eine Basis von V. Die Matrix ist direkt zu berechnen. Das charakteristische Polynom:

$$
\begin{aligned}
f_\varphi &= \det(xI_{r\times t} - M(\varphi, B, B)) \\
&= \det \begin{pmatrix} x & -1 & 0 & 0 & \cdots & 0 \\ 0 & x & -1 & 0 & \cdots & 0 \\ 0 & 0 & x & -1 & \ddots & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & 0 & 0 & x & -1 \\ a_0 & a_1 & a_2 & a_3 & \cdots & x + a_{r-1} \end{pmatrix} \\
&= \underbrace{(-1)^{r+1} a_0 \cdot \det \begin{pmatrix} -1 & 0 & 0 & \cdots & 0 \\ x & -1 & 0 & \cdots & 0 \\ 0 & x & -1 & \ddots & 0 \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & 0 & x & -1 \end{pmatrix}}_{a_0} + \underbrace{(-1)^{r+2} a_1 \cdot \det(...)}_{a_1 x^1} ... \\
&= a_0 + a_1 x + ... + a_{r-1} x^{r-1} + x^r
\end{aligned}
$$

7.5.4 Satz von Cayley-Hamilton

Das charakteristische Polynom liegt im von Minimalpolynom erzeugten Hauptideal des Polynomrings

$$f_\varphi \in K[x] m_\varphi, \text{d.h.} f_\varphi(\varphi) = 0$$

BEWEIS: Induktion nach $\dim V$:

- Induktionsanfang: $\dim V = 1$, dann $V = \langle v \rangle$, zudem $v\varphi = kv$ für ein $k \in K$, d.h. k ist Eigenwert von φ; $f_\varphi = x - k = m_\varphi$
- Induktionsannahme: Sei $\dim V \geq 2$ und die Behauptung richtig für alle Vektorräume der Dimension kleiner $\dim V$.
- Induktionsschluß: Es existiert $v \in V$ mit $V = \langle v\varphi^i | i \in \mathbb{N} \rangle$, so folgt $m_\varphi = f_\varphi$ aus (7.5.3). Also können wir annehmen: Für $0 \neq v \in V$ ist $U := \langle v\varphi^i | i \in \mathbb{N} \rangle$ ein echter Unterraum von V, der φ-invariant ist. Da U ein echter Unterraum ist, gilt nach Induktionsannahme: $F_{\varphi|_U} \in K[x] m_{\varphi|_U}$. Dimensionssatz: $\dim V/U < \dim V$. Wieder mit Induktionsannahme: $f_{\varphi_{V/U}} \in K[x] m_{\varphi_{V/U}}$.

$$f_\varphi = f_{\varphi|_U} \cdot f_{\varphi_{V/U}} \in K[x] \cdot \underbrace{m_{\varphi|_U} \cdot m_{\varphi_{V/U}}}_{\in K[x] m_\varphi} \subseteq K[x] \cdot m_\varphi$$

7.6 Bemerkung über unendlichdimensionale Vektorräume

Z.B. $V := K[x]$ ist ein unendlichdimensionaler Vektorraum über K.

BEWEIS: Annahme, V sei endlich. Sei $f_1, ..., f_n$ endliche Basis, dann hat ein Polynom $g = \sum_{i=1}^{n} k_i f_i$ den Grad $\leq \max\{\text{grad}\, f_i\}$, damit kann $g \cdot x$ nicht existieren.

Sei $g \notin K$ fest gewählt aus $K[x]$. Dann gilt: $(f_1+f_2)g = f_1g+f_2g$ und $(kf_1)g = k(f_1g)$. Beachte daher die lineare Abbildung $\varphi_g : f \mapsto fg$ (Rechtsmultiplikation). Was ist m_{φ_g}? Suche Annulatorideal $Ann_{\varphi_g}(V) = \{ f \in K[x] \mid f(\varphi_g) = 0\}$

Sei $f = \sum_{i=0}^{n} k_i x^i$, $h \in K[x]$, dann ist

$$\begin{aligned} hf(\varphi_g) &= h\left(\sum_{i=0}^{n} k_i \varphi_g^i\right) \\ &= \sum_{i=0}^{n} k_i h \varphi_g^i \\ &= \sum_{i=0}^{n} k_i h g^i \end{aligned}$$

Daraus folgt: $f = 0$, also $\text{Ann}_{\varphi_g}(V) = \{0\}$, also $m_\varphi = 0$.

Daraus ergibt sich folgende allgemeingültige Definition (also für endlich- und unendlichdimensionale Vektorräume) für Eigenwerte: k heißt Eigenwert von φ falls $v \neq 0 \in V$ existiert mit $v\varphi = kv$.

8 Normalform linearer Abbildungen

Sei K Körper, V endlichdimenstionaler Vektorraum und $\varphi \in \mathrm{Hom}(V,V)$.

8.1 invariant, zyklisch, unzerlegbar

Sei U ein φ-invarianter Unterraum von V. U heißt *φ-zyklisch*, falls $v \in U$ mit $U = \langle v\varphi^i | i \in \mathbb{N}\rangle$. Zudem heißt U *φ-unzerlegbar*[46], falls U nicht direkte Summe von echten (d.h. $\neq U$) φ-invarianten Unterräumen ist.

Sei U ein φ-zyklischer Unterraum, W ein φ-invarianter Unterraum von U. Dann folgt: $U/W = \langle v\varphi^i + W | i \in \mathbb{N}\rangle$ ist $\varphi_{U/W}$-zyklisch.

Sei $\psi \in \mathrm{Hom}(V,V)$ mit φ vertauschbar, d.h. $\varphi\psi = \psi\varphi$ (z.B. wenn $\psi = g(\varphi)$ für ein $k \in K[x]$). Dann ist

$$\begin{aligned} U\psi &= \left\langle v\varphi^i\psi | i \in \mathbb{N}\right\rangle \\ &= \left\langle (v\psi)\varphi^i | i \in \mathbb{N}\right\rangle \end{aligned}$$

Damit ist $U\psi$ wieder φ-zyklisch. Beispiele:

- Der Vektorraum $(\mathbb{Z}/2\mathbb{Z})^2$ (kanonische Basis $\{e_1, e_2\}$) ist für $e_1\varphi = e_1$ und $e_2\varphi = e_1 + e_2$ φ-unzerlegbar und φ-zyklisch.
- Der Vektorraum $(\mathbb{Z}/3\mathbb{Z})^2$ (kanonische Basis $\{e_1, e_2\}$) ist für $e_1\varphi = e_1$ und $e_2\varphi = -e_2$ nicht φ-unzerlegbar, aber φ-zyklisch.

8.2 Zerlegung in φ-zyklische Unterräume

8.2.1 direkte Summe φ-unzerlegbarer Unterräume

V ist direkte Summe φ-unzerlegbarer Unterräume.

Beweis: Induktion nach $\dim V$. Ist V φ-unzerlegbar, so gilt die Behauptung. Sei V nicht φ-unzerlegbar. D.h. $V = A_1 \oplus A_2$ für zwei φ-invariante echte Unterräume A_1, A_2. Also: $\dim A_i < \dim V$. Nach Induktion ist $A_1 = B_1 \oplus \ldots \oplus B_s$ und $A_2 = C_1 \oplus \ldots \oplus C_t$, wobei C_i und B_i φ-unzerlegbar sind. Damit ist $V = (B_1 \oplus \ldots \oplus B_s) \oplus (C_1 \oplus \ldots \oplus C_t)$, Klammern können nach (7.4.2) weggelassen werden, denn $\dim V \overset{(7.4.2)}{=} \dim A_1 + \dim A_2 \overset{(7.4.2)}{=} \sum_{i=1}^{s} \dim B_i + \sum_{i=1}^{t} \dim C_i$

[46] „Hm, ich seh' schon, das ist gar kein Gegenbeispiel - OK, dann ist es halt ein Beispiel.“

8.2.2 Minimalpolynom unzerlegbarer Vektorräume

Sei $V \neq \{0\}$ ein φ-unzerlegbarer Vektorraum. Dann ist $m_\varphi = f^e$ für ein irreduzibles Polynom von $f \in K[x]$ und ein $e \in \mathbb{N}$.

Beweis: folgt aus (6.6) und (7.4.6): $m_\varphi = \prod_{i=1}^r f_i^{e_i}$, zudem $f_1, ..., f_r$ sind paarweise telerfremde irreduzible Polynome. Angenommen, $r > 1$ und $h = \prod_{i=2}^r f_i^{e_i}$. Dann ist $g = f_1^{e_1}$, d.h. $m_\varphi = gh$ und g, h sind teilerfremd. Mit (7.4.6) ist $V = \text{Kern}\, g(\varphi) \oplus \text{Kern}\, h(\varphi)$, das ist ein Widerspruch zur φ-Unzerlegbarkeit.

8.2.3 Bild/Kern von Faktoren des Minimalpolynoms

Sei V φ-zyklisch und $m_\varphi = gh$ mit $g, h \in K[x]$. Dann ist Bild $g(\varphi) =$ Kern $h(\varphi)$ und $f_{\varphi|_{Kern\, h(\varphi)}} = ch$ für ein $c \in K$. Außerdem hat jeder Eigenraum von φ Dimension 1.

Beweis: Es existiert $v \in V$ mit $V = \langle v\varphi^i | i \in \mathbb{N} \rangle$. Sei $U := \text{Bild}\, g(\varphi)$. Die Räume V/U und U sind wieder φ-zyklisch. Mit (7.5.3) angewandt auf $V, U, V/U$ gilt:

1. $m_\varphi = f_\varphi$, $m_{\varphi|_U} = f_{\varphi|_U}$, $m_{\varphi_{V/U}} = f_{\varphi_{V/U}}$
2. Mit (7.5.2) $gh = m_\varphi = f_\varphi = f_{\varphi|_U} f_{\varphi_{V/U}} = m_{\varphi|_U} m_{\varphi_{V/U}}$

3.

$$\begin{aligned}
V/U g(\varphi_{V/U}) &= \left\{ \underbrace{vg(\varphi)}_{\in U} + U \;\middle|\; v \in V \right\} \\
&= \{0\} \\
U h(\varphi) &= \{vg(\varphi)h(\varphi) \mid v \in V\} \\
&= \{vm_\varphi(\varphi) \mid v \in V\} \\
&= \{0\} \\
\Rightarrow g &\in K[x] m_{\varphi_{V/U}} \\
\wedge h &\in K[x] m_{\varphi|_U} \\
\Rightarrow \operatorname{grad} g &\geq \operatorname{grad} m_{\varphi_{V/U}} \\
\wedge \operatorname{grad} h &\geq \operatorname{grad} m_{\varphi|_U} \\
\operatorname{grad} gh &= \operatorname{grad} g + \operatorname{grad} h \\
&= \operatorname{grad} m_\varphi \\
&= \operatorname{grad} m_{\varphi_{V/U}} + \operatorname{grad} m_{\varphi|_U} \\
\Rightarrow \operatorname{grad} g &= \operatorname{grad} m_{\varphi_{V/U}} \\
\wedge \operatorname{grad} h &= \operatorname{grad} m_{\varphi|_U}
\end{aligned}$$

Insbesondere ist $h = cm_{\varphi|_U}$ für ein $c \in K$. Es ist

$$\operatorname{grad} h = \operatorname{grad} m_{\varphi|_U} \stackrel{(7.5.3)}{=} \dim U$$

Genauso ist (mit g und h vertauscht)

$$\operatorname{grad} g = \dim \operatorname{Bild} h(\varphi)$$

$$\begin{aligned}
\dim V &\stackrel{(7.5.3)}{=} \operatorname{grad} m_\varphi \\
&= \operatorname{grad} g + \operatorname{grad} h \\
&= \dim \operatorname{Bild} h(\varphi) + \dim \operatorname{Kern} h(\varphi) \\
\Rightarrow \operatorname{grad} h &= \dim \operatorname{Kern} h(\varphi) \\
&= \dim U
\end{aligned}$$

Aus (3) folgt: $U \leq \operatorname{Kern} h(\varphi)$, also $U = \operatorname{Kern} h(\varphi)$.

Zu zeigen bleibt: Jeder Eigenraum von φ hat die Dimension 1. Sei a

Eigenwert von φ (damit ist $V \neq \{0\}$). Dann ist $m_\varphi = (x-a)h'$ für ein $h' \in K[x]$. Setze $g' = (x-a)$. Dann ist wie eben gesehen:

$$\begin{aligned}
\operatorname{Kern} h'(\varphi) &= \operatorname{Bild} g'(\varphi)\\
\text{und } \dim \operatorname{Kern} h'(\varphi) &= \dim \operatorname{Bild} g'(\varphi)\\
&= \operatorname{grad} f_{\varphi|_{\operatorname{Kern} h'(\varphi)}} - \operatorname{grad} h'\\
&= \operatorname{grad} m_\varphi - 1\\
&\overset{(7.4.5)}{=} \dim V - 1\\
\dim V &= \dim \operatorname{Kern} g'(\varphi) + \underbrace{\dim \operatorname{Bild} g'(\varphi)}_{=\dim V - 1}\\
\Rightarrow \dim \operatorname{Kern} g'(\varphi) &= 1\\
\operatorname{Kern} g'(\varphi) &= \operatorname{Kern}(\varphi - a \cdot \mathrm{id})\\
&= \{v \in V \mid v(\varphi - a\cdot \mathrm{id}) = 0\}\\
&= V(a)\\
\Rightarrow \dim V(a) &= 1
\end{aligned}$$

8.2.4 invarianter Unterraum $\oplus$ zyklischer Unterraum

Sei $m_\varphi = f^e$, $f \in K[x]$ irreduzibel und $e \in \mathbb{N}$, und sei U ein φ-zyklischer Unterraum maximaler Dimension von V. Dann existiert ein φ-invarianter Unterraum $W \leq V$ mit $V = U \oplus W$.

Beweis: Induktion nach $\dim V$:

- Induktionsanfang: $\dim V \leq 1$ offensichtlich, da V selbst φ-zyklisch ist.
- Induktionsannahme: $\dim V \geq 2$ und die Behauptung ist richtig für alle Vektorräume der Dimension kleiner $\dim V$.
- Sei $\tilde{U}$ ein φ-invarianter Unterraum. Dann ist $m_\varphi \in K[x]m_{\varphi|_{\tilde{U}}}$ und $m_\varphi \in K[x]m_{\varphi|_{V/\tilde{U}}}$. Mit (6.6) folgt:

  $$m_{\varphi|_{\tilde{U}}} = f^{e'} \text{ und } m_{\varphi_{V/\tilde{U}}} = f^{e''}$$

  Das heißst $\tilde{U}$ und $V/\tilde{U}$ erfüllen die Voraussetzungen bezüglich $\varphi|_{\tilde{U}}$ bzw. $\varphi_{V/\tilde{U}}$. Sei nun $\tilde{U}$ auch φ-zyklisch. Mit (7.4.5) folgt:

  $$\begin{aligned}
  \dim \tilde{U} &= \operatorname{grad} m_{\varphi|_{\tilde{U}}} = e' \operatorname{grad} f\\
  \dim \tilde{U} \text{ maximal} &\Leftrightarrow e' \text{ maximal}
  \end{aligned}$$

Sei nun zusätzlich e' maximal gewählt und $U := \tilde{U}$. Für alle φ-zyklischen Unterräume $\hat{U}$ gilt:

$$\hat{U}f^{\hat{e}'} = \hat{U}f^{e'} = \{0\} \Rightarrow f^{e'} \in K[x]m_\varphi = K[x]f^e \Rightarrow e = e' \Rightarrow m_\varphi = m_{\varphi|_U}$$

Betrachte zwei Fälle:

1. V/U ist nicht φ-unzerlegbar. Es existieren φ-invariante[47] $A_1, A_2 \leq V$ mit $U \subseteq A_1 \cap A_2$, $A_1 \neq V \neq A_2$ und $V/U = A_1/U \oplus A_2/U$. Insbesondere gilt: $\dim A_i < \dim V$ und $m_{\varphi,A_i} = m_\varphi$ für $i = 1, 2$, denn $m_{\varphi,A_i} \in K[x]m_{\varphi|_U} = K[x]m_\varphi$ und $m_\varphi \in K[x]m_{\varphi|_{A_i}}$.

   Mit Induktion gilt: $A_i = U \oplus A_i^*$, wobei A_1^* φ-invariant ist für $i = 1, 2$. Setze $W := A_1^* + A_2^*$. Es ist

   $$U + W = U + A_1^* + A_2^* + U = A_1 + A_2 = V$$

   Es bleibt zu zeigen: $U \cap W = \{0\}$. Dann ist[48]

   $$A_i/U = (A_i + U^*)/U \simeq A_i^*/(A_i^* \cap U) \simeq A_i^*$$

   $$\begin{aligned} \dim V - \dim U + \dim U \cap W &= \dim W \\ &\leq \dim A_1^* + \dim A_2^* \\ &= dim A_1/U + \dim A_2/U \\ &= \dim V/U \\ &= \dim V - \dim U \\ \Rightarrow U \cup W &= \{0\} \end{aligned}$$

2. V/U ist φ-unzerlegbar. Induktion nach $\dim V$ sagt uns: Ist U_1 ein $\varphi_{V/U}$-zuyklischer Unterraum maximaler Dimension, so existiert ein $\varphi_{V/U}$-invarianter Unterraum W_1 mit $V/U = U_1 \oplus W_1$.

   Mit der Unzerlegbarkeit folgt: $W_1 = \{0\}$ und V/U ist φ-zyklisch. D.h. es existiert $v \in V$ mit $V/U = \langle v\varphi^i + U | i \in \mathbb{N}\rangle$. Damit ist $\overline{m} := m_{\varphi_{V/U}}$ ein Teiler von m_φ. Also ist $\overline{m} = f^k$ für ein $k \leq e$. Sei

[47] „Ich habe Ihnen ja schon immer gesagt - Sie sollen mein Script lesen und nicht mir zuhören!"

[48] „Deutschland - das Land der Dichter und Denker! Stellen Sie doch mal die Sinnfrage!"

$r = e - k$.

$$\begin{aligned} vf^k(\varphi)f^r(\varphi) &= f^{k+r}(\varphi) = vf^e(\varphi) \\ &= vm_\varphi(\varphi) = 0 \\ vf^k(\varphi) &= v\overline{m}(\varphi) \in \operatorname{Kern} f^r(\varphi) \\ (v+U)\overline{m}(\varphi_{V/U}) &= 0 + U \\ &= v\overline{m}(\varphi) + U \\ U \cap \operatorname{Kern} f^r(\varphi) &= \operatorname{Kern} f^r(\varphi|_U) \\ &= \operatorname{Bild} f^k(\varphi|_U \\ &= Uf^k(\varphi) \end{aligned}$$

Also existiert $u_v \in U$ mit $u_v f^k(\varphi) = vf^k(\varphi)$. Setze $v' = v - u_v$ unt $W := \langle v'\varphi^i | i \in \mathbb{N}\rangle$. Dann ist

$$v'f^k(\varphi) = (v - u_v)f^k(\varphi) = 0$$

Mit (7.5.3) folgt:

$$\dim W \leq \operatorname{grad} f^k = \operatorname{grad} \overline{m} = \dim V/U$$

Dann ist $v\varphi^i \in W + U = V$. Mit Dimensionssätzen folgt:

$$\begin{aligned} \dim V + \dim W - \dim U \cup W &= \dim V \\ &= \dim V/U + \dim U \\ &\geq \dim W + \dim U \\ \Rightarrow U \cap W &= \{0\} \\ \Rightarrow V &= U \oplus W \end{aligned}$$

8.2.5 unzerlegbar $\Rightarrow$ zyklisch

Ist V φ-unzerlegbar, so ist V φ-zyklisch.

Beweis: Mit (8.2.2): $m_\varphi = f^e$, f irreduzibel; also nach (8.2.4): V ist φ-zyklisch.

8.2.6 Bedingung für zyklisch $\Rightarrow$ unzerlegbar

Sei $m_\varphi = f^e$, $f \in K[x]$ irreduzibel. Genau dann ist V φ-zyklisch, wenn V φ-unzerlegbar ist.

Beweis: Wege (8.2.5) bleibt nur eine Richtung zu zeigen. Angenommen,

$V = V_1 \oplus V_2$ und V_1, V_2 verschiedene φ-invariable Unterräume ungleich $\{0\}$. Sei $m_{\varphi|_{V_i}} = f^{e_i}$ mit $e_i \leq e$. Sei o.B.d.A $e_1 \leq e_2 \leq e$.

$$\begin{aligned} V f^{e_2}(\varphi) &= V_1 f^{e_2}(\varphi) + V_2 f^{e_2}(\varphi) \\ &= \{0\} \\ \Rightarrow e_2 &= e \end{aligned}$$

Mit (7.5.3) und (7.5.4) gilt:

$$\operatorname{grad} m_{\varphi|_{V_2}} \leq \operatorname{grad} f_{\varphi|_{V_2}} = \dim V_2 \leq \dim V = \operatorname{grad} m_\varphi$$

$$\begin{aligned} \operatorname{grad} m_{\varphi|_{V_2}} &\leq \operatorname{grad} f_{\varphi|_{V_2}} \\ &= \dim V_2 \leq \dim V \\ &= \operatorname{grad} m_\varphi \\ &= \operatorname{grad} m_{\varphi|_{V_2}} \\ \Rightarrow \dim V &= \dim V_2 \\ \Rightarrow V &= \{0\} \end{aligned}$$

Dies ist ein Widerspruch zur Wahl von V_1.

8.2.7 direkte Summe zyklischer und unzerlegbarer Unterräume

V ist direkte Summe φ-zyklischer φ-unzerlegbarer Unterräume.

Beweis: Induktion nach $\dim V$:

- Verankerung: für $\dim V \leq 1$
- Annahme: Sei $\dim V \geq 2$, und die Behauptung richtig für alle Vektorräume kleinerer Dimension.
- Schluß: Laut (6.6) gilt: $m_\varphi = f_1^{e_1} \cdot \ldots \cdot f_r^{e_r}$, wobei f_i paarweise teilerfremde irreduzible Polynome aus $K[x]$ sind.

  Mit (7.4.6). $V = W_1 \oplus \ldots \oplus W_r$, wobei $W_i := \operatorname{Kern} f_i^{e_i}(\varphi)$.

  - Angenommen, $r > 1$. Mit (7.4.2) gilt: $\dim V = \dim W_1 + \ldots + \dim W_r$, also $\dim W_i < \dim V$. W_i ist φ-invariant, mit der Induktionsannahme gilt: $W_i = W_{i1} \oplus \ldots \oplus W_{in_i}$

    Dann sind W_{ij} jeweils $\varphi|_{W_i}$-zyklisch und $\varphi|_{W_i}$-unzerlegbar, also auch φ-zyklisch und φ-unzerlegbar. Dann ist

    $$V = W_{11} \oplus \ldots \oplus W_{1n_1} \oplus \ldots \oplus W_{r1} \oplus \ldots \oplus W_{rn_r}$$

– Sei nun $r = 1$ Sei U ein φ-zyklischer Unterraum maximaler Dimension, insbesondere $U \neq \{0\}$. Mit (8.2.4) existiert $W \leq V$ φ-invariant mit $V = U \oplus W$, es ist $\dim W < \dim V$, mit Induktionsannahme: $W = W_2 \oplus ... \oplus W_r$, damit ist W_i φ-zyklisch und φ-unzerlegbar.

$$V = U \oplus W_2 \oplus ... \oplus W_r$$

ist die gesuchte Zerlegung wegen (8.2.6) angewandt auf U (beachte $m_{\varphi|_U} | m_\varphi$)

8.2.8 Zerlegungssatz

Sei $V = V_1 \oplus ... \oplus V_r$ und $V = W_1 \oplus ... \oplus W_s$ zwei Zerlegungen in φ-zyklische, φ-unzerlegbarer Unterräume. Dann ist $r = s$ und es existiert $\pi \in S_r$, so daß $V_i \simeq W_{i\pi}$ und eine invertierbare lineare Abbildung (Isomorphismus) $\varrho \in \mathrm{Hom}(V, V)$ existiert mit

$$V_i\varrho = W_{i\pi} \text{ und } \varrho\varphi = \varphi\varrho$$

Beweis: siehe Script

8.3 Die allgemeine Normalform

Voraussetzung: Sei φ lineare Abbildung auf endlichdimensionalem Vektorraum V.

8.3.1 Satz über die allgemeine Normalform

Es existieren linear unabhängige Teilmengen $B_1, ..., B_r$ von V, so daß für $B; = \bigcup_{i=1}^r B_i$ gilt:

1. $\langle B_i \rangle$ ist φ-zyklisch und φ-unzerlegbar

2. $V = \langle B_1 \rangle \oplus ... \oplus \langle B_r \rangle$

3. B ist Basis von V und

$$M(\varphi, B, B) = \begin{pmatrix} A_1 & 0 & 0 \\ \vdots & \ddots & \vdots \\ 0 & 0 & A_r \end{pmatrix}$$

$$A_i = M(\varphi|_{\langle B_i \rangle}, B_i, B_i) = \begin{pmatrix} 0 & 1 & ... & 0 \\ \vdots & 0 & 1 & \vdots \\ 0 & ... & 0 & 1 \\ -a_0 & -a_1 & ... & -a_{n_i - 1} \end{pmatrix}$$

$$m_{\varphi|_{\langle B_i \rangle}} = \sum_{i=0}^{n_i - 1} a_i x^i$$

Beweis: Nach (8.2.7) existiert eine Zerlegung $V = V_1 \oplus ... \oplus V_r$ mit V_i φ-zyklisch und φ-unzerlegbar. Nach (7.5.3) existiert eine Basis B_i von V_i mit $M(\varphi|_{\langle B_i \rangle}, B_i, B_i = A_i$ wie in (3). Nach (7.4.2) ist B eine Basis von V mit der gewünschten Eigenschaft.

8.3.2 Beispiele

1. Sei $\dim V = 4$, B Basis,

$$A := M(\varphi, B, B) = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 2 & 0 & 0 \\ -1 & 1 & 2 & 1 \\ -1 & 1 & 0 & 3 \end{pmatrix}$$

   Gesucht: „die“ allgemeine Normalform von φ. Das charakteristische Polynom berechnet sich als $f_\varphi = \det(xI - A) = (x-2)^4$. Das Minimalpolynom folgt daraus (nach ein bißchen Matrizenrechnung) als $m_\varphi = (x-2)^2 = x^2 - 4x + 4$. Denkbar sind dann die Matrizen

$$\begin{pmatrix} \begin{pmatrix} 0 & 1 \\ -4 & 4 \end{pmatrix} & \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} \\ \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} & \begin{pmatrix} 0 & 1 \\ -4 & 4 \end{pmatrix} \end{pmatrix} \text{ und } \begin{pmatrix} \begin{pmatrix} 0 & -1 \\ -4 & 4 \end{pmatrix} & \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} \\ \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} & \begin{matrix} (2) & 0 \\ 0 & (2) \end{matrix} \end{pmatrix}$$

   Da das Minimalpolynom Potenz eines irreduziblen Polynoms ist, muß es einen Eigenraum geben, der das gleiche Minimalpolynom hat (und damit $\dim \geq 2$).

$$\dim \operatorname{Bild}(\varphi - 2\mathrm{id}) = \operatorname{rg} C = 1 \Rightarrow \dim \operatorname{Kern}(\varphi - 2\mathrm{id}) = 3 = \dim V(2)$$

2. kommt noch

8.4 Die Jordansche Normalform

In diesem Abschnitt sei $\dim V \geq 1$ und sei K ein *algebraisch abgeschlossener Körper*, d.h. jedes irreduzible Polynom aus $K[x]$ hat Grad 1, äquivalent dazu: jedes Polynom vom Grad ≥ 1 in $K[x]$ hat eine Nullstelle in K. Insbesondere ist $\mathbb{C}$ algebraisch abgeschlossen (Hauptsatz der Algebra).

8.4.1 Satz über die Jordansche Normalform

Sei K algebraisch abgeschlossen[49]. Dann existieren linear unabhängige Teilmengen B_i mit $i = 1, ..., r$, so daß für $B = \bigcup\limits_{i=1}^{r} B_i$ gilt:

1. $\langle B_i \rangle$ ist φ-zyklisch und unzerlegbar für $i = 1, ..., r$
2. $V = \langle B_1 \rangle \oplus ... \oplus \langle B_r \rangle$
3. $$M(\varphi, B, B) = \begin{pmatrix} A_1 & 0 & 0 & 0 \\ 0 & A_2 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & A_r \end{pmatrix}$$

   wobei

   $$A_i = M(\varphi|_{\langle B_i \rangle}, B_i, B_i) = \begin{pmatrix} c_i & 1 & 0 & \cdots & 0 \\ 0 & c_i & 1 & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & c_i & 1 \\ 0 & \cdots & 0 & 0 & c_i \end{pmatrix}$$

   und $\{c_1, ..., c_r\}$ die Menge der Eigenwerte von φ ist.

Beweis: Wie in (8.3.1) zerlegt man V in „eine“ direkte Summe von φ-unzerlegbaren, φ-zyklischen Unterräumen. Also $V = V_1 \oplus ... \oplus V_r$. Es bleibt zu zeigen: in V_i existiert eine Basis B_i, so daß $A_i = M(\varphi|_{V_i}, B_i, B_i)$ die gewünschte Gestalt hat.

Sei $m_i := m_{\varphi|_{V_i}}$, K algebraisch abgeschlossen, V_i φ-unzerlegbar. Mit (8.2.2) folgt: $m_i = (x - c_i)^{n_i}$. Mit (7.5.3) gilt: Es existiere $v \in V_i$, so daß $v\varphi^0, ..., v\varphi^{n_i-1}$ Basis von V_i ist und $\dim V_i = n_i$.

Setze $\psi := \varphi - c_i \cdot \mathrm{id}$ und $v_i := v\psi^i$ für $0 \leq i \leq n_i - 1$. Dann ist V_i ψ-invariant, damit: $\underbrace{\langle v_0, ..., v_{n_i-1} \rangle}_{\varphi-\text{invariant}} \subseteq V_i$, daraus folgt: $V_i \leq \langle v_0, ..., v_{n_i-1} \rangle \leq V_i$, also ist $\{v_0, ..., v_{n_i-1}\}$ eine Basis von V_i.

Betrachte $A_i := M(\varphi|_{V_i}, B_i, B_i)$. Für $0 \leq j \leq n_i - 2$ gilt: $v_j\varphi = v\psi^j\varphi =$

[49] Nicht unbedingt notwendig, notwendig ist nur: Das Minimalpolynom zerfällt in Linearfaktoren.

$v\psi^j(\psi + c_i \cdot \mathrm{id}) = v\psi^{j+1} + c_i v\psi^j$. Damit steht in der Matrix A_i an Position (j,j) gerade c_i und 1 an $(j, j+1)$. Noch zu betrachten:

$$v_{n-i-1}\varphi = v\psi n_i - 1^(\psi + c_i \cdot \mathrm{id}) = v\psi^{n_i} + \underbrace{c_i v\psi^{n_i - 1}}_{=v_{n_i - 1}}$$

und $v\psi^{n_i} = (\varphi - c_i \cdot \mathrm{id})^{n_i} = vm_i(\varphi) = 0$.

8.4.2 Beispiele

1. Sei $\dim V = 4$, B Basis,

$$M(\varphi, B, B) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 4 & -6 & 4 \end{pmatrix}$$

   Damit ist $m_\varphi = f_\varphi = 1 - 4x + 6x^2 - 4x^3 + x^4 = (x-1)^4$, damit ist die Jordansche Normalform:

$$M(\varphi, B', B') = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

2. (wird noch korrigiert)

9 Alpha-Bilinearform

Sei im Folgenden K ein Körper.

9.1 Körperautomorphismen

Eine Abbildung α heißt Körperautomorphismus (von K), falls sie bijektiv von K nach K ist und gilt:

$$(k_1 + k_2)\alpha = k_1\alpha + k_2\alpha \text{ und } (k_1k_2)\alpha = k_1\alpha k_2\alpha \;\forall\; k_1, k_2 \in K$$

Beispiel:

1. Sei $K = \mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$ (Körper der komplexen Zahlen). Sei

   $$\alpha : \mathbb{C} \to \mathbb{C} \text{ mit } a + ib \mapsto a - ib$$

   Dann ist α ein Körperautomorphismus von $\mathbb{C}$, zudem $\alpha^2 = \mathrm{id} \neq \alpha$. α heißt die *Komplexkonjugation*.

2. Sei K Körper mit $\operatorname{char} K = 2$. Dann ist

   $$\alpha : K \to K \text{ mit } k \mapsto k^2$$

   ein Körperautomorphismus: Für alle $k_1, k_2 \in K$ gilt

   $$(k_1 + k_2)\alpha = (k_1 + k_2)^2 = k_1^2 + \underbrace{2k_1k_2}_{=0} + k_2^2 = k_1\alpha + k_2\alpha$$

   $$(k_1k_2)\alpha = (k_1k_2)^2 = k_1^2k_2^2 = k_1\alpha k_2\alpha$$

9.2 Eigenschaften der Bilinearform

Sei in diesem Abschnitt α Automorphismus von K und V ein Vektorraum über K.

Definition: Eine Abbildung $f : V \times V \to K$ heißt *α-Bilinearform*, falls gilt:

1. $f(v_1, v_2 + v_3) = f(v_1, v_2) + f(v_1, v_3)$
   $f(v_1 + v_2, v_3) = f(v_1, v_3) + f(v_2, v_3)$

2. $f(kv_1, v_2) = kf(v_1, v_2)$
   $f(v_1, kv_2) = (k\alpha) \cdot f(v_1, v_2)$

Ist $\alpha = \mathrm{id}$, so heißt f *Bilinearform.*

BEISPIEL:

1. $\alpha = \mathrm{id}$, $V = \mathbb{R}^n$. Sei

$$f((a_1, ..., a_n), (b_1, ..., b_n)) := \sum_{i=1}^{n} a_i b_i$$

   Dann ist f Bilinearform und heißt das *Skalarprodukt* auf $\mathbb{R}^n$.

2. α Komplexkonjugation, $V = \mathbb{C}^n$. Sei

$$f((a_1, ..., a_n), (b_1, ..., b_n)) := \sum_{i=1}^{n} a_i (b_i \alpha)$$

   Dann ist f α-Bilinearform und heißt das *Skalarprodukt* auf $\mathbb{C}^n$.

3. $\alpha = \mathrm{id}$, $V = \mathbb{R}^4$. Sei $0 \neq c \in \mathbb{R}$ fest gewählt. Sei

$$f((a_1, ..., a_4), (b_1, ..., b_4)) := a_1 b_1 + a_2 b_2 + a_3 b_3 - c^2 a_4 b_4$$

   Dann ist f Bilinearform und (V, f) ist der *Minkowski-Raum* (wichtig z.B. in der Relativitätstheorie)

- Eigenschaften beider Sklarmultiplikationen, jedoch nicht im Minkowski-Raum:

$$f(v, v) \geq 0 \text{ und } f(v, v) = 0 \Leftrightarrow v = 0$$

9.2.1 Gram'sche Matrix

Im Folgenden sei V ein endlichdimensionaler Vektorraum und f eine α-Bilinearform auf V. Sei zudem $n := \dim V$ und $B = \{v_1, ..., v_n\}$ eine Basis von V. Definiere die *Gram'sche Matrix*:

$$G_B(f) := (f(v_i, v_j))_{n \times n} = \begin{pmatrix} f(v_1, v_1) & \cdots & f(v_1, v_n) \\ \vdots & \ddots & \vdots \\ f(v_n, v_1) & \cdots & f(v_n, v_n) \end{pmatrix}$$

Sei $v = \sum_{i=1}^{n} k_i v_i$, $w = \sum_{i=1}^{n} h_i w_i$, dann

$$f(v, w) = \sum_{i=1}^{n} \sum_{j=1}^{n} f(v_i, v_j)(k_i (h_j \alpha))$$

9.2.2 reguläre Bilinearform

DEFINITION: f (und V bezüglich f) heißt *regulär* (oder *nicht ausgeartet*), falls gilt:

$$f(v,w) = 0 \;\forall\; w \in V \Rightarrow v = 0$$

SATZ: Die folgenden Aussagen sind äquivalent:

(a) f ist regulär

(b) $\det G_b(f) \neq 0$

(c) $f(w,v) = 0 \;\forall\; w \in V \Rightarrow v = 0$

BEWEIS:

$(a) \Rightarrow (b)$ Betrachte das LGS $(*)$ der Gestalt $xG_B(f) = 0$. Wir wissen: $(0,...,0)$ ist einzige Lösung von $(*)$ in K^n genau dann, wenn $\det G_B(f) \neq 0 \Leftrightarrow \det G_B(f)^t \neq 0$. Sei $(k_1,...,k_n) \in K^n$ Lösung von $(*)$. Damit folgt:

$$\sum_{i=1}^{n} k_i f(v_i, v_j) = 0 \;\forall\; j = 1,...,n$$

Für $v := \sum_{i=1}^{n} k_i v_i$ gilt somit: $f(v, v_j) = 0 \;\forall\; j = 1,...,n$. Sei $w := \sum_{t=1}^{n} h_t v_t \in V$. Dann ist

$$f(v,w) = \sum_{t=1}^{n} h_t \alpha \underbrace{f(v, v_t)}_{=0} = 0$$

Da f regulär ist, ist $v = 0$, damit folgt: $k_i = 0$ für alle $i = 1,...,n$; damit ist $\det G_B(f) \neq 0$.

$(b) \Rightarrow (a)$ Aus $\det G_B(f) \neq 0$ folgt: $(0,...,0)$ ist einzige Lösung von $(*)$. Sei $v := \sum_{i=1}^{n} k_i v_i$. Dann ist

$$f(v, v_j) = 0 \Rightarrow \sum_{i=1}^{n} k_i f(v_i, v_j) = 0 \;\forall\; j = 1,...,n$$

Damit folgt: $(k_1,...,k_n)$ ist Lösung von $(*)$, damit ist $(k_1,...,k_n) = (0,...,0)$, also $v = 0$, damit ist f regulär.

$(b) \Leftrightarrow (c)$ Betrachte das LGS $(**)$ der Gestalt $xG_B(f)^t = 0$. Wir wissen: $(0,...,0)$ ist einzige Lösung von $(**)$ in K^n genau dann, wenn $\det G_B(f) \neq 0 \Leftrightarrow \det G_B(f)^t \neq 0$. Sei $(k_1,...,k_n) \in K^n$ Lösung von $(**)$. Äquivalent:

$$\sum_{i=1}^{n} k_i f(v_j, v_i) = 0 \;\forall\; j = 1,...,n$$

Für $v := \sum_{i=1}^n k_i\alpha^{-1}v_i$ gilt somit: $(k_1, ..., k_n)$ ist Lösung von $(**)$ genau dannn, wenn $f(w, v) = 0$ für alle $w \in V$ (beachte $\sum_{i=1}^n k_i f(v_j, v_i) = f(v_j, v))$. Nun folgt Äquivalenz wie in „(a) $\Leftrightarrow$ (b)“ wenn man berücksichtigt: $k_1\alpha^{-1} = ... = k_n\alpha^{-1} = 0 \Rightarrow k_1 = ... = k_n = 0$.

9.2.3 Gram'sche Matrizen verschiedener Basen

Seien B, B' Basen von V und sei $(a_{ij}) := A := M(\mathrm{id}, B', B)$. Dann gilt:

$$G_{B'}(f) = AG_B(f)(A\alpha)^t \text{ mit } A\alpha := (a_{ij}\alpha)$$

Insbesondere gilt für die Determinanten:

$$\det G_{B'}(f) = \det G_B(f) \cdot \det A \cdot \det A\alpha$$

Beweis: Sei $n := \dim V$, $B = \{v_1, ..., v_n\}$ und $B' = \{w_1, ..., w_n\}$, sei $A = (a_{ij})_{n\times n}$

$$\begin{aligned}
w_i &= \sum_{j=1}^n a_{ij}v_j \;\forall\, i \\
f(w_i, w_j) &= f\left(\sum_{k=1}^n a_{ik}v_k, \sum_{t=1}^n a_{jt}v_t\right) \\
&= \sum_{k=1}^n \sum_{t=1}^n a_{ik}a_{jt}\alpha f(v_k, v_t) \\
&= \sum_{k=1}^n \sum_{t=1}^n a_{ik}f(v_k, v_t)a_{jt}\alpha \\
&= ij\text{-Element der Matrix } A \cdot G_B(t) \cdot (A\alpha)^t
\end{aligned}$$

9.2.4 Vektorraum der α-Biliearformen

Sei α fest vorgegeben und $B_\alpha(V)$ die Menge der α-Biliearformen auf V. Durch

$$(f + g)(v, w) := f(v, w) + g(v, w) \text{ und } (kf)(v, w) := kf(v, w)$$

für $f, g \in B_\alpha(V)$ und $k \in K$ sowie $v, w \in V$ wird $B_\alpha(V)$ zu einem Vektorraum.

Auch $\mathcal{M}_{n\times n}(K)$ ist ein Vektorraum über K. Sei B eine Basis von V. Dann ist die folgende Abbildung ein Vektorraumisomorphismus[50]:

$$\mu : B_\alpha(V) \to \mathcal{M}_{n\times n}(K)\mu : f \mapsto G_B(f)$$

[50] „Das sagt ihnen genauer: Es gibt Bilinearformen wie Sand am Meer, und V ist das Meer...“

Sei $A = (a_{ij}) \in \mathcal{M}_{n\times n}(K)$. Dann existiert $f \in B_\alpha(V)$ mit $f\mu = A$, d.h. $a_{ij} = f(v_i, v_j)$ wobei $B = \{v_1, ..., v_n\}$ ist[51].

9.3 Der duale Vektorraum

Sei V ein Vektorraum über dem Körper K. Dann ist $\mathrm{Hom}(V, K)$ ein Vektorraum, der zu V *duale Vektorraum*. Im folgenden setzen wir $V^* := \mathrm{Hom}(V, K)$. Die Elemente von V^* heißen *Linearfunktionen* (oder lineare Funktionale).

9.3.1 Isomorphiesatz

Sei V endlichdimensional und B die Basis von V. Für $b \in B$ sie $b^* \in V^*$ definiert mittels:

$$b'b^* := \begin{cases} 0 & \text{falls} \quad b' \neq b \\ 1 & \text{falls} \quad b' = b \end{cases} \quad b' \in B$$

Dann ist $B^* := \{b^* \mid b \in B\}$ eine Basis von V^* und es gilt: $V \simeq V^*$.

Beweis: Offensichtlich ist die Abbildung $B \to B^*$ mit $b \mapsto b^*$ bijektiv: die Surjektivität ergibt sich aus der Definition von B^*, die Injektivität: $b^* = b'*$ (mit $b, b' \in B$). Damit: $bb'^* = bb^* = 1 \Rightarrow b = b'$. Es genügt zu zeigen: B^* ist Basis.

Sei $\beta \in V^*$, definiere $k_b := b\beta \in K$. Setze $\beta' = \sum_{b\in B} k_b b^*$. Dann ist für $e \in B$:

$$\begin{aligned} e\beta' &= \sum_{b\in B} k_b(eb^*) \\ &= k_e(ee^*) = k_e \\ e\beta &= k_e \end{aligned}$$

Damit ist $\beta = \beta'$ und $\beta \in \langle B^* \rangle$, d.h. B^* ist Erzeugendensystem von V^*.

Sei $k_{b^*} \in K$ und $\sum_{b^*\in B^*} k_{b^*} b^* = 0$. Sei $e \in B$. Dann gilt:

$$\begin{aligned} 0 &= e \cdot 0 \\ &= e \cdot \sum_{b^*\in B^*} k_{b^*} b^* \\ &= \sum_{b^*\in B^*} k_{b^*} eb^* \\ &= k_{e^*} \\ \Rightarrow k_{e^*} &= 0 \ \forall\, e \in B \\ \Rightarrow k_{e^*} &= 0 \ \forall\, e^* \in B^* \end{aligned}$$

[51] „Wir hätten aufhören können mit der Linearen Algebra, viele hätten sich gefreut...“

Die Basis B^* heißt die zu B *duale Basis*.

BEISPIEL:

1. Sei $V = K[x]$ und $B = \{x^i \mid i \in \mathbb{N}\}$ ist eine Basis von V. Sei B^* wie in (9.3.1) definiert.

   Es gilt $\langle B^*\rangle \neq V^*$. Sei $\delta \in V^*$ mit $x^i\delta = 1$ für alle $i \in \mathbb{N}$. Angenommen, $\delta \in \langle B^*\rangle$. Es existiert eine endliche Teilmenge $B_0^* \subseteq B^*$ und $k_{b^*} \in K$ für $b^* \in B_0^*$ mit $\delta = \sum_{b^*\in B_0^*} k_{b^*}b^*$.

   Es existiert x^i mit $x^i \notin B_0^*$. Dann ist

$$\begin{aligned} 1 &= x^i\delta \\ &= \sum_{b^*\in B_0^*} k_{b^*} \underbrace{x^i b^*}_{=0} \\ &= 0 \end{aligned}$$

   Widerspruch!

9.3.2 Dimensionssatz

Bezeichnung: Sei $U \leq V$, $H \leq V^*$. Definiere

$$\begin{aligned} U^\perp &:= \{\beta \in V^* \mid u\beta = 0 \,\forall\, u \in U\} \\ H^\top &:= \{v \in V \mid v\beta = 0 \,\forall\, \beta \in H\} \end{aligned}$$

Offensichtlich ist $U^\perp$ ein UR von V^* und $H^\top$ UR von V. Betrachte $U^{\perp\top\perp\dots}$

SATZ: Sei V endlichdimensional und U ein Unterraum von V. Dann gilt:

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

BEWEIS: Sei B_0 Basis von U, B Basis von V mit $B_0 \subseteq B$. Sei $B^* = \{b^* \mid b \in B\}$ wie in (9.3.1).

Zur Erinnerung: $b^* \in V^*$, $b'b^* = \begin{cases} 0 & \text{falls} \quad b' = b \\ 1 & \text{falls} \quad b' \in B \setminus \{b^*\} \end{cases}$).

Sei $B_0^* = \{b^* \mid b \in B_0\}$; $B_1 = B^* \setminus B_0^*$. Dann ist

$$\begin{aligned} \dim V &= \dim V^* = |B^*| \\ &= |B_0^*| + |B_1^*| \\ &= |B_0| + |B_1^*| \\ &= \dim U + |B_1^*| \end{aligned}$$

Es genügt zu zeigen: $|B_1^*| = \dim U^\perp$. Sei $W := |B_1^*| \subseteq V^*$, es ist $\dim W = |B_1^*|$. Sei $b_0 \in B_0$ und $b_1^* \in B_1^*$. Dann ist

$$b_0 b_1^* = \begin{cases} 1 & \text{falls} \quad b_0 \neq b_1 \\ 0 & \text{sonst} \end{cases}$$

Angenommen, $b_0 = b_1$, dann ist $b_0^* = b_1^* \in B_0^* \cap B_1^*$, Widerspruch, da $B_0^* \cap B_1^* = \emptyset$.

Wir haben gezeigt: $b_i^* \in \langle B_0 \rangle^\perp = U^\perp$, damit $W \leq U^\perp$.

Sei $\beta \in U^\perp$. Seien $k_{b^*} \in K$ mit $\beta = \sum_{b^* \in B^*} k_{b^*} b^*$. Für $b_0 \in B_0 \subseteq U$ ist

$$\begin{aligned} 0 &= b_0 \beta \\ &= b_0 \sum_{b^* \in B^*} k_{b^*} b^* \\ &= \sum_{b^* \in B^*} k_{b^*} b_0 b^* \\ &= \sum_{b^* \in B^*} k_{b^*} b_0 b^* \\ &= k_{b_0^*} \\ \Rightarrow \beta &= \sum_{b^* \in B_1^*} k_{b^*} b^* \in W \\ \Rightarrow U^\perp &\leq W \\ \Rightarrow W &= U^\perp \\ \Rightarrow |B_1^*| &= \dim U^\perp \end{aligned}$$

9.3.3 der $(\mathbf{Raum}^*)^*$

Sei V endlichdimensional. Dann ist

$$\varphi : V \to (V^*)^* \text{ mit } \beta(v\varphi) := v\beta \; \forall \, v \in V, \beta \in V^*$$

ein Isomorphismus, insbesondere gilt $H^\top \simeq H^\perp$ für alle $H \leq V^*$.

BEWEIS: Seien $v, w \in V$, $k \in K$, $\beta \in V^*$.

$$\begin{aligned}
\beta(v+w)\varphi &= (v+w)\varphi \\
&= v\beta + w\beta \\
&= \beta(v\varphi) + \beta(w\varphi) \\
&= \beta(v\varphi + w\varphi) \\
\beta(kv)\varphi &= (kv)\beta \\
&= k(v\beta) \\
&= k(\beta(v\varphi)) \\
&= \beta(k(v\varphi))
\end{aligned}$$

Sei $v \in V$ und $v\varphi = 0$. Dann ist $\beta(v\varphi) = v\beta = 0$ für alle $\beta \in V^*$. Aus (9.3.1) folgt $v = 0$, sonst existiert $v^* \in V^*$ mit $vv^* = 1 = v^*(v\varphi) = 0$. Damit ist φ injektive lineare Abbildung von V in $(V^*)^*$. Mit (9.3.1) ist $\dim V = \dim V^* = \dim(V^*)^*$, also ist φ bijektiv.

Sei $H \leq V^*$. Dann gilt:

$$\begin{aligned}
H^\top &= \{v \in V \mid v\beta = 0 \;\forall\, \beta \in H\} \\
&= \{v \in V \mid \beta(v\varphi) = 0 \;\forall\, \beta \in H\} \\
&= H^\perp \varphi^{-1} \\
\Rightarrow H^\top &\simeq H^\perp
\end{aligned}$$

9.3.4 Dualitätssatz

Sei V endlichdimensional. Dann gilt:

1. $(U^\perp)^\top = U$ und $(H^\top)^\perp = H$ für alle Unterräume $U \leq V$ und $H \leq V^*$
2. $(U_1 \cap U_2)^\perp = U_1^\perp + U_2^\perp$ und $(U_1 + U_2)^\perp = U_1^\perp \cap U_2^\perp$ für alle Unterräume $U_1, U_2 \leq V$
3. $(H_1 \cap H_2)^\top = H_1^\top + H_2^\top$ und $(H_1 + H_2)^\top = H_1^\top \cap H_2^\top$ für alle Unterräume $H_1, H_2 \leq V^*$

BEWEIS:

1. Offensichtlich gilt $U \leq (U^\perp)^\top$. Es genügt, $\dim U = \dim(U^\perp)^\top$ zu zeigen.

$$\begin{aligned}
\dim V &\overset{(9.3.2)}{=} \dim U + \dim U^\perp \\
&\overset{(9.3.1)}{=} \dim V^* \\
&\overset{(9.3.2)}{=} \dim U^\perp + \dim \underbrace{(U^\perp)^\perp}_{\leq V^{**}} \\
\Rightarrow \dim U &= \dim(U^\perp)^\perp \\
&\overset{(9.3.3)}{=} \dim(U^\perp)^\top
\end{aligned}$$

2. Offensichtlich gilt: $(U_1 + U_2)^\perp = U_1^\perp \cap U_2^\perp$ und $U_1^\perp + U_2^\perp \leq (U_1 \cap U_2)^\perp$.
Zu zeigen bleibt: $\dim(U_1^\perp + U_2^\perp) = \dim(U_1 \cap U_2)^\perp$

$$\begin{aligned}
\dim(U_1^\perp + U_2^\perp) &\overset{[2.2.11]}{=} \dim U_1^\perp + \dim U_2^\perp - \dim(\underbrace{U_1^\perp \cap U_2^\perp}_{=(U_1+U_2)^\perp}) \\
&\overset{(9.3.2)}{=} 2 \cdot \dim V - \dim U_1 - \dim U_2 - \dim(U_1 + U_2)^\perp \\
&\overset{(9.3.2)}{=} \dim V - \dim U_1 - \dim U_2 + \dim(U_1 + U_2) \\
&\overset{[2.2.11]}{=} \dim V - \dim(U_1 \cap U_2) \\
&\overset{(9.3.2)}{=} \dim(U_1 \cap U_2)^\perp
\end{aligned}$$

3. analog

9.3.5 Abbildungen ϱ_w und ${}_w\varrho$

Sei V endlichdimensional, f α-Bilinearform auf V. Für $w \in V$ definiere:

$$\varrho_w : V \to K \text{ mit } \varrho_w : v \mapsto f(v, w)$$

$${}_w\varrho : V \to K \text{ mit } {}_w\varrho : v \mapsto f(w, v)\alpha^{-1}$$

Dann gilt: Für alle $w \in V$ sind ϱ_w und ${}_w\varrho$ Elemente aus V^*.

BEWEIS: Einfaches Nachrechnen der Linearitätseigenschaften:

$$\begin{aligned}
(v+u)\varrho_w &= f(v+u,w) \\
&= f(v,w)+f(u,w) \\
&= v\varrho_w + u\varrho_w \\
(kv)\varrho_w &= f(kv,w) \\
&= kf(v,w) \\
&= kf(v\varrho_w) \\
(kv)\,{}_w\varrho &= f(w,kv)\alpha^{-1} \\
&= ((k\alpha)\cdot f(w,v))\alpha^{-1} \\
&= (k\alpha)\alpha^{-1}(f(w,v)\alpha^{-1}) \\
&= k(v\,{}_w\varrho)
\end{aligned}$$

9.3.6 Abbildung $V \to V^*$

Seien $\varphi, \varphi' : V \to V^*$ mit $w\varphi = \varrho_w$ bzw. $w\varphi' = {}_w\varrho$ sowie $K := \{w \in V \mid w\varphi = 0\}$ und $K' := \{w \in V \mid w\varphi' = 0\}$. Dann gilt:

1. K und K' sind Unterräume von V
2. Ist U ein Unterraum von V mit $U \cap K = \{0\}$, so erhält $\varphi|_U$ die lineare Unabhängigkeit von Elementen von U.
3. Aussage b gilt entsprechend für φ' und K'.
4. Ist f regulär, so sind φ und φ' bijektiv. Ist zusätzlich $\alpha = \mathrm{id}$, so sind φ und φ' Isomorphismen.

BEWEIS:

1. Einfaches Nachrechnen
2. Seien $v_1, ..., v_n$ linear unabhängig in U. Sezte $\beta_i := v_i\varphi$. Seien $k_1, ..., k_n \in K$ mit $\sum_{i=1}^n k_i\beta_i = 0$.

Es gilt für alle $v \in V$:

$$\begin{aligned}
0 &= v \cdot 0_{V^*} \\
&= v \cdot \sum_{i=1}^{n} k_i \beta_i \\
&= \sum_{i=1}^{n} k_i (v \beta_i) \\
&= \sum_{i=1}^{n} k_i f(v, v_i) \\
&= f\left(v, \sum_{i=1}^{n} k_i \alpha^{-1} v_i\right) \\
\Rightarrow f(v,w) &= 0 \;\forall\, v \in V
\end{aligned}$$

Damit ist $\varrho_w = 0 \in V^*$, zudem $w\varphi = \varrho_w \Rightarrow w \in U \cap K = \{0\}$, damit folgt:

$$w = 0 = \sum_{i=1}^{n} k_i \alpha^{-1} v_i$$

Daraus folgt $k_1 \alpha^{-1} = ... = k_n \alpha^{-1} = 0$, nach Multiplikation mit α: $\beta_1, ..., \beta_n$ sind linear unabhängig.

3. analog

4. Seien $v_1, ..., v_n$ Basis von V und $\beta_i := v_i \varphi$. Wie eben gezeigt folgt: $\beta_1, ..., \beta_n$ sind linear unabhängig in V^*. Mit (9.3.1) gilt: $\dim V = \dim V^*$. Damit ist $\beta_1, ..., \beta_n$ eine Basis von V^*.

   Sei $\beta \in V^*$. Dann existieren $h_1, ..., h_n \in K$ mit $\beta = \sum_{i=1}^{n} h_i \beta_i$. Es ist

$$\begin{aligned}
v\beta &= \sum h_i v \beta_i \\
&= \sum h_i f(v, v_i) \\
&= f\left(v, \sum h_i \alpha^{-1} v_i\right) \\
\Rightarrow \beta &= \sum h_i \alpha^{-1} v_i
\end{aligned}$$

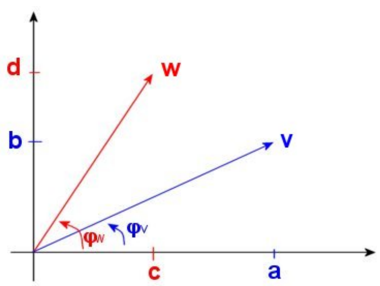
   und φ ist surjektiv. Seien $w, w' \in V$ mit $w\varphi = w'\varphi$. Dann folgt: $f(v,w) = v(w\varphi) = v(w'\varphi) = f(v,w') \;\forall\, v \in V$, damit folgt: $f(v,w) - f(v,w') = 0 = f(v, w - w') \;\forall\, v \in V$. Da f regulär ist, ist $w - w' = 0$.

9.4 Orthosymmetrische Alpha-Bilinearform

9.4.1 Definitionen

In diesem Abschnitt ist V ein Vektorraum über K und f eine α-Bilinearform auf V.

- f heißt *orthosymmetrisch*, falls für alle $v, w \in V$ gilt: $f(v,w) = 0 \Leftrightarrow f(w,v) = 0$.
- Sei f orthosymmetrisch, $v, w \in V$. Dann heißt v *orthogonal* zu w (oder: v *steht senkrecht* auf w), falls $f(v,w) = 0$; wir schreiben $v \perp w$, falls $f(v,w) = 0$.
- Für $A, B \subseteq V$ ist A orthogonal zu B, falls $a \perp b$ für alle $a \in A$, $b \in B$ (und damit $A \perp B$).
- Definiere weiter $A^\perp := \{v \in V \mid v \perp a \; \forall \, a \in A\}$
- Das *Radikal* von V ist definiert als: $\operatorname{rad} V := V^\perp$
- V ist regulär genau dann, wenn $\operatorname{rad} V = \{0\}$.
- Für einen Unterraum $U \leq V$ gilt: U heißt *regulär*, falls $U \cap U^\perp = \{0\}$.
- U ist regulär genau dann, wenn $f|_{U \times U}$ regulär ist.
- Seien $V_1, ..., V_n$ Unterräume von V und $V = V_1 \oplus ... \oplus V_n$. Gilt $V_i \leq V_j^\perp \; \forall \, i \neq j$, so schreiben wir $V = V_1 \perp ... \perp V_n$ und nennen es *orthogonale Summe* (oder *orthogonale Zerlegung*)[52]
- Sei B eine Basis von V. B heißt *Orthogonalbasis* von V (bezüglich f), falls $f(b, b') = 0 \; \forall \, b, b' \in B$ mit $b \neq b'$.
- Die Basis heißt *Orthonormalbasis*, falls zusätzlich $f(b,b) = 1$ für alle $b \in B$.
- Beispiel:



[52] d.h. spezielle direkte Summe, wobei alle Summanden aufeinander senkrecht stehen

Im R^2, f das Skalarprodukt[53]; $v = (a, b)$ und $w = (c, d)$; Länge von v: $|v| = \sqrt{a^2 + b^2} = \sqrt{f(v, v)}$. Zudem:

$$\cos\varphi_v = \frac{a}{|v|} \qquad \cos\varphi_w = \frac{c}{|w|} \qquad \sin\varphi_v = \frac{b}{|v|} \qquad \sin\varphi_w = \frac{d}{|w|}$$

$$\begin{aligned} f(v,w) &= ac + bd \\ &= |v|\cos\varphi_v \cdot |w| \cdot \cos\varphi_w + |v|\sin\varphi_v \cdot |w| \cdot \sin\varphi_w \\ &= |v|\,|w|\,(\cos\varphi_v\cos\varphi_w + \sin\varphi_v\sin\varphi_w) \\ &= |v|\,|w|\cos(\varphi_w - \varphi_v) \end{aligned}$$

Wann ist $f(v, w) = 0$ für $v \neq 0$ und $w \neq 0$? Wenn $\cos(\varphi_w - \varphi_v) = 0 \Leftrightarrow \varphi_w - \varphi_v = (2k + 1)\frac{\pi}{2}$ gilt.

Im folgenden sei f eine orthosymmatrische α-Bilinearform auf V.

9.4.2 Senkrechträume sind Unterräume („Jippie!!!“)

Ist $A \subseteq V$, so ist $A^\perp$ ein Unterraum.

Beweis: Seien $v, w \in A^\perp$, $k \in K$. Es gilt: $f(u, v) = 0 \;\forall\, u \in A$, damit folgt:

$$f(u, kv) = k\alpha f(u, v) = 0 \;\forall\, u \in V \Rightarrow kv \in A^\perp$$

$$\text{und } f(u, v + w) = f(u, v) + f(u, w) = 0 + 0 = 0 \;\forall\, u \in V \Rightarrow u + w \in A^\perp$$

9.4.3 Dimensionssatz

Sei V endlichdimensional und U Unterraum von V mit $U \cap \operatorname{rad} V = \{0\}$. Dann gilt:

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

Nach (9.3.2) genügt zu zeigen:

$$\dim U^{\perp_{(9.3)}} = \dim U^{\perp_{(9.4)}}$$

Sei U_* das in (9.3) definiert $U^\perp$. Sei $U_* = \{B \in V^* \mid U_\beta = 0\}$. Mit (9.3.5): Zu $v \in V$ existiert $f_v \in V^*$ mit $wf_v := f(w, v)$.

Es ist $\operatorname{rad} V = \{v \in V \mid f_v = 0\}$. Wähle Basis B von U, definiere $H := \langle f_b | b \in B\rangle \leq V^*$. Es gilt nach Voraussetzung: $U \cap \operatorname{rad} V = \{0\}$

Mit (9.3.6) folgt: Die Abbildung $u \mapsto f_u$ erhält lineare Unabhängigkeit, damit

[53] „Es gibt Vektoren der Länge null, die nicht null sind. Das ist halt Ihr Problem.“

sind $f_b, b \in B$ linear unabhängig und damit ist $f_b, b \in B$ Basis von H. Damit ist $\dim U = \dim H$. Es gilt[54]:

$$\begin{array}{rcl}
\dim V & \overset{(9.3.2)}{=} & \dim U + \dim U_* \\
\dim V & \overset{(9.3.1)}{=} & \dim V^* \\
& = & \dim H + \dim H^{\perp} \overset{(9.3)}{=} \\
& \overset{(9.3.3)}{=} & \dim H + \dim H^{\top} \\
& = & \dim U + \dim H^{\top}
\end{array}$$

Noch zu zeigen: $\dim H^{\top} = \dim U^{\perp}$, es gilt sogar: $H^{\top} = U^{\perp}$, denn:

$$\begin{array}{rcl}
H^{\top} & = & \{v \in V \mid v\beta = 0 \;\forall\, b \in H\} \\
& = & \{v \in V \mid vf_b = 0 \;\forall\, b \in B\} \\
& = & \{v \in V \mid f(v,b) = 0 \;\forall\, b \in B\} \\
& = & \{v \in V \mid f(v,b) = 0 \;\forall\, b \in B\} \\
& = & \{v \in V \mid f(v,u) = 0 \;\forall\, u \in U\} \\
& = & U^{\perp}
\end{array}$$

9.4.4 der $(\text{Raum}^{\perp})^{\perp}$

Sei V endlichdimensional und U ein Unterraum von V. Dann gilt:

1. Ist V regulär, so ist $U^{\perp\perp} = U$
2. Ist U regulär, so ist $V = U \perp U^{\perp}$

Beweis:

1. offensichtlich: $U \leq U^{\perp\perp}$, zu zeigen bleibt: $\dim U = \dim U^{\perp\perp}$. Nach (9.4.3) ist

$$\begin{array}{rcl}
\dim V & = & \dim U + \dim U^{\perp} \\
& = & \dim U^{\perp} + \dim U^{\perp\perp} \\
\Rightarrow \dim U & = & \dim U^{\perp\perp}
\end{array}$$

2. U regulär heißt: $U \cup U^{\perp} = \{0\}$. Damit ist $U + U^{\perp} = U \oplus U^{\perp}$. Nach (7.4.2) ist $\dim(U + U^{\perp}) = \dim U + \dim U^{\perp}$.

   Da U regulär ist, ist $U \cap \operatorname{rad} V = \{0\}$. Mit (9.4.3) ist $\dim V = \dim U + \dim U^{\perp}$, also ist

$$V = U + U^{\perp} = U \oplus U^{\perp} = U \perp U^{\perp}$$

[54] „Wir wären fertig, wenn wir zeugen könnten...“

9.4.5 Klassen von Bilinearformen

1. Sei $\alpha = \mathrm{id}$, f heißt *symmetrisch*, falls $f(v,w) = f(w,v)\ \forall\ v,w \in V$. f heißt *schiefsymmetrisch*, falls $f(v,w) = -f(w,v)\ \forall\ v,w \in V$. Das Skalarprodukt auf $\mathbb{R}^n$ ist eine symmetrsiche Bilinearform.

   Offensichtlich gilt für $G_B(f)$: $G_B(f) = G_B(f)^t$, falls f symmetrisch[55], und $G_B(f) = -G_B(f)$, falls f schiefsymmetrisch[56].

2. Sei $\alpha = \mathrm{id}$. f heißt *symplektisch*, falls $f(v,v) = 0$ für alle $v \in V$. Beispiel: $V = \mathbb{R}^4$, B kanonische Basis,

$$G_B(f) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$$

   Es gilt:

$$\begin{aligned} & f(k_1e_1 + k_2e_2 + k_3e_3 + k_4e_4, k_1e_1 + k_2e_2 + k_3e_3 + k_4e_4) \\ = \ & k_1k_1 \underbrace{f(e_1,e_1)}_{0} + k_1k_2 \underbrace{f(e_1,e_2)}_{1} + k_1k_3 \underbrace{f(e_1,e_3)}_{0} + k_1k_4 \underbrace{f(e_1,e_4)}_{0} + \dots \\ = \ & k_1k_2 \underbrace{f(e_1,e_2)}_{1} + k_1k_2 \underbrace{f(e_2,e_1)}_{-1} + k_3k_4 \underbrace{f(e_3,e_4)}_{1} + k_3k_4 \underbrace{f(e_4,e_3)}_{-1} \\ = \ & 0_{\text{töfftöff}} \end{aligned}$$

$\Rightarrow$ Sei f symplektisch. Für $v,w \in V$ gilt:

$$0 = f(v+w, v+w) = \underbrace{f(v,v)}_{0} + f(v,w) + f(w,v) + \underbrace{f(w,w)}_{0}$$

   Damit folgt:

$$f(v,w) = -f(w,v)$$

   Ist $\operatorname{char} K \neq 2$ und f schiefsymmetrisch, so ist f symplektisch.

3. Ist $\alpha = \mathrm{id}$, $\operatorname{char} K \neq 2$ und f symmetrisch, so heißt f *orthogonal*.

4. Ist $\alpha^2 = \mathrm{id} \neq \alpha$ und $f(v,w) = f(w,v)\alpha$, so heißt f *unitär* (oder *hermitesch*) (Beispiel: Das Skalarprodukt auf $\mathbb{C}^n$)

[55] „... ob Sie lineare Abbildungen lieben oder ob Sie Matrizen lieben... Mathematiker lieben Abbildungen, Nicht-Mathematiker lieben Matrizen..."

[56] Analogien auch zu (schief)symmetrischen Matrizen etc.

9.4.6 Automorphismus und inverses Element

Sei α ein Automorphismus von K und $\alpha^2 = \mathrm{id} \neq \alpha$, und sei $0 \neq a \in K$. Genau dann ist $a(a\alpha) = 1$, wenn ein $b \in k$ existiert mit $a = b(b^{-1}\alpha)$.

BEWEIS:

„$\Leftarrow$“ Sei $a = b(b^{-1}\alpha)$. Dann gilt:

$$\begin{aligned}
a\alpha &= b(b^{-1}\alpha)\alpha \\
&= b\alpha(b^{-1}\alpha)\alpha \\
&= b\alpha b^{-1}\alpha^2 \\
&= b\alpha b^{-1} \\
a(a\alpha) &= b(b^{-1}\alpha)(b\alpha)b^{-1} \\
&= (b^{-1}\alpha)(b\alpha) \\
&= (b\alpha)^{-1}(b\alpha) \\
&= 1
\end{aligned}$$

$b^{-1}\alpha = (b\alpha)^{-1}$

„$\Rightarrow$“ Für $c \in K$ setze $b(c) := c + a(c\alpha)$. Dann ist

$$\begin{aligned}
b(c)\alpha &= (c + a(c\alpha))\alpha \\
&= c\alpha + a\alpha(c\alpha^2) \\
&= c\alpha + a^{-1}c \\
&= a^{-1}(a(c\alpha) + c) \\
&= a^{-1}b(c)
\end{aligned}$$

Angenommen, $b(c) \neq 0$. Dann:

$$\begin{aligned}
a &= b(c)(b(c)\alpha)^{-1} \\
&= b(c)((b(c)^{-1})\alpha)
\end{aligned}$$

Es genügt also, $c \in K$ zu finden mit $b(c) \neq 0$.

- Ist $a \neq -1$, dann ist $b(1) = 1 + a \neq 0$.
- Ist $a = -1$, dann ist $b(c) = c - c\alpha \neq 0$ für alle $c \neq c\alpha$, weden $\alpha \neq \mathrm{id}$ existiert so ein c.

9.4.7 Äquivalenz zwischen Bilinearformen

Seien f_1, f_2 zwei α-Bilinearformen auf V. Wir sagen: f_1 ist *äquivalent* zu f_2, falls $a \in K \setminus \{0\}$ existiert mit $f_1 = af_2$, d.h.

$$f_1(v,w) = af_2(v,w)\ \forall\ v,w \in V$$

9.4.8 Klassifikationssatz für orthosym. Alpha-Bilinearf.

Sei V endlichdimensional und regulär bezüglich f und $\dim V \geq 2$. Dann gilt einer der folgenden Fälle:

1. $\alpha = \mathrm{id}$ und f ist symmetrisch oder schiefsymmetrisch
2. $\alpha^2 = \mathrm{id} \neq \alpha$ und f ist äquivalent zu einer unitären Form

Beweis: Sei $n := \dim V$ und seien φ und φ' wie in (9.3.6) (also $v \mapsto \varrho_v$ oder ${}_v\varrho$). Wähle $0 \neq v_0 \in V$. Setze $\beta := v_0\varphi$, $\beta' := v_0\varphi'$, d.h.

$$w\beta = f(w,v_0) \text{ und } w\beta' = f(v_0,w)\alpha^{-1}\ \forall\ w \in V$$

f orthosymmetrisch, $\mathrm{Kern}\,\beta = \mathrm{Kern}\,\beta' =: W$. Mit Dimensionssatz folgt: $\dim V = \dim W + \dim \mathrm{Bild}\,\beta$, da V regulär ist, gilt: $\mathrm{Bild}\,\beta = K$, damit ist $\dim W = n-1$.

Sei $v_1 \in V \setminus W$. Dann ist $V = W \oplus \langle v_1 \rangle$. Setze $a(v_0) := v_1\beta(v_1\beta')^{-1}$ und $\mu := a(v_0)\beta'$. Für alle $k \in K$ und $w \in W$ ist dann

$$\begin{aligned}
(kv_1+w)\mu &= a(v_0)(kv_1+w)\beta' \\
&= a(v_0)(kv_1\beta'+0) \\
&= (v_1\beta)\cdot(v_1\beta')^{-1}\cdot k\cdot(v_1\beta') \\
&= k\cdot(v_1\beta) \\
&= (kv_1)\beta \\
(kv_1+w)\beta &= (kv_1)\beta+0 \\
&= (kv_1)\beta \\
\Rightarrow \beta &= \mu
\end{aligned}$$

Wir zeigen: $a(v_0) = a(v_0')\ \forall\ v_0' \in V\setminus\{0\}$. Sei $v_0' \in V \setminus \{0\}$.

- Sei zunächst v_0, v_0' linear unabhängig. Insbesondere $v_0 + v_0' \neq 0$. Für alle $w \in V$ gilt:

$$\begin{array}{rcl} f(w, v_0 + v_0') & = & a(v_0 + v_0')f(v_0 + v_0', w)\alpha^{-1} \\ & = & f(a(v_0 + v_0')\alpha(v_0 + v_0'), w)\alpha^{-1} \\ f(w, v_0 + v_0') & = & f(w, v_0) + f(w, v_0') \\ & = & a(v_0)f(v_0, w)\alpha^{-1} + a(v_0')f(v_0', w)\alpha^{-1} \\ & = & f(a(v_0)\alpha v_0, w)\alpha^{-1} + f(a(v_0')\alpha v_0', w)\alpha^{-1} \\ & = & (f(a(v_0)\alpha v_0, w) + f(a(v_0)'\alpha v_0', w))\alpha^{-1} \end{array}$$

Damit gilt für alle $w \in V$:

$$\begin{array}{rcl} f(a(v_0 + v_0')\alpha(v_0 + v_0'), w) & = & f(a(v_0)\alpha v_0, w) + f(a(v_0)'\alpha v_0', w) \\ & = & f(a(v_0)\alpha v_0 + a(v_0)'\alpha v_0', w) \end{array}$$

Und es folgt:

$$f(\underbrace{a(v_0 + v_0')\alpha(v_0 + v_0') - a(v_0)\alpha v_0 - a(v_0')\alpha v_0'}_{\in \operatorname{rad} V \text{ (und } \operatorname{rad} V = \{0\} \text{ wg. Regularität)}}, w) = 0 \;\forall\; w$$

Damit gilt:

$$\begin{array}{rrcl} & 0 & = & a(v_0 + v_0')\alpha(v_0 + v_0') - a(v_0)\alpha v_0 - a(v_0')\alpha v_0' \\ \Rightarrow & a(v_0 + v_0')\alpha(v_0 + v_0') & = & [a(v_0)\alpha]\, v_0 + [a(v_0')\alpha]\, v_0' \\ & & = & [a(v_0 + v_0')\alpha]\, v_0 + [a(v_0 + v_0')\alpha]\, v_0' \\ \Rightarrow & a(v_0 + v_0') & = & a(v_0) = a(v_0') \end{array}$$

- Sei nun v_0, v_0' linear abhängig. Da $\dim V \geq 2$, damit existiert $v_1 \in V \setminus \langle v_0 \rangle$ und v_1, v_0 sind linear unabhängig, wie auch v_0', v_1. Wie oben gesehen: $a(v_1) = a(v_0)$ und $a(v_1) = a(v_0')$.

Damit gilt allgemein:

$$a(v_0) = a(v_0') \;\forall\; v_0 \in V \setminus \{0\}$$

Setze $a := a(v_0)$. Dann gilt für alle $v, w \in V$:

$$\begin{array}{rcl} f(v, w) & = & af(w, v)\alpha^{-1} \\ & = & a(af(v, w)\alpha^{-1})\alpha^{-1} \\ & = & a(a\alpha^{-1})f(v, w)\alpha^{-2} \end{array}$$

Da V regulär ist, existieren $v, w \in V$ mit $k := f(v, w) \neq 0$. Dann ist $f(k^{-1}v, w) = k^{-1}f(v, w) = 1$, es existiert also $u \in V$ mit $f(u, w) = 1$

(Normierung).

Da α ein Automorphismus ist und daher $1\alpha = 1$ ist, gilt:

$$\begin{aligned} 1 &= f(u,w) \\ &= \big(a \cdot (a\alpha^{-1})\big)\, f(u,w)\alpha^{-2} \\ &= \big(a \cdot (a\alpha^{-1})\big)\, 1\alpha^{-2} \\ &= a \cdot (a\alpha^{-1}) \end{aligned}$$

Es ist also $a \cdot (a\alpha^{-1}) = 1$, also gilt für alle $v, w \in V$:

$$\begin{array}{rrcl} & f(v,w) &=& f(v,w)\alpha^{-2} \\ \Rightarrow & K &=& \{ f(v,w) \mid v,w \in V\} \\ \Rightarrow & \alpha^{-2} &=& \mathrm{id} \\ \Rightarrow & \alpha^2 &=& \mathrm{id} \end{array}$$

Unterscheidung in zwei Fälle:

1. Der Fall $\alpha = \mathrm{id}$: Damit folgt aus $a(a\alpha^{-1}) = 1$, daß $a^2 = 1$ ist. Damit ist a Nullstelle von $x^2 - 1 \in K[x]$, damit ist $a = 1$ oder $a = -1$.
   - $a = 1$, dann: $f(v,w) = f(w,v)$
   - $a = -1$, dann: $f(v,w) = -f(w,v)$
2. Der Fall $\alpha^2 = \mathrm{id} \neq \alpha$. Es gilt: $\alpha = \alpha^{-1}$. Mit (9.4.6) gilt: es existiert $b \in K \setminus \{0\}$ mit $b(b^{-1}\alpha) = a \Rightarrow b^{-1}\alpha = b^{-1}a$. Definiere $g := b^{-1}f$. Seien $v, w \in V$, dann gilt:

$$\begin{aligned} g(v,w) &= b^{-1}f(v,w) \\ &= b^{-1}af(w,v)\alpha \\ &= b^{-1}\alpha f(w,v)\alpha \\ &= (b^{-1}f(w,v))\alpha \\ &= g(w,v)\alpha \end{aligned}$$

   Damit: g ist unitär, damit ist f äquivalent zu einer unitären Form.

10 Isometrien

VORAUSSETZUNG: In diesem Kapitel ist V ein endlichdimensionaler Vektorraum über K und f eine α-Bilinearform auf V.

10.1 Orthogonale Zerlegungen

In diesem Abschnitt betrachten wir unitäre, symplektische und orthosymmetrische α-Bilinearform.

10.1.1 unitär/orthogonal folgt (V = rad V gdw. symplektisch)

Sei f unitär und orthogonal und $V \neq \operatorname{rad} V$. Dann existiert ein $v \in V$ mit $f(v,v) \neq 0$.

BEWEIS: Sei $v' \in V \setminus \operatorname{rad} V$. Es existiert $w \in V$ mit $k := f(v', w) \neq 0$. Sei $v := k^{-1}v^{-1}$.

Annahme: (V, f) ist ein Gegenbeispiel, d.h. $f(x,x) = 0 \;\forall\; x \in V$. Für alle $k_1, k_2 \in K$ gilt:

$$\begin{aligned}
0 &= f(k_1 v + k_2 w, k_1 v + k_2 w) \\
&= k_1(k_1\alpha)\underbrace{f(v,v)}_{=0} + k_1(k_2\alpha)f(v,w) + k_2(k_1\alpha)f(w,v) + k_2(k_2\alpha)\underbrace{f(w,w)}_{=0} \\
f(v,w) &= f(k^{-1}v', w) = k^{-1}f(v', w) \\
&= k^{-1}k = 1
\end{aligned}$$

Damit ist auch[57] $f(w,v) = 1$ (da f unitär oder orthogonal ist). Damit ist

$$0 = k_1 k_2 \alpha + k_2 k_1 \alpha \;\forall\; k_1, k_2 \in K$$

Damit folgt: $(*)$ $k_1 = k_2 = 1 \Rightarrow 0 = 11\alpha + 11\alpha = 2$, Widerspruch falls $\operatorname{char} K \neq 2$!Sei $k_1 = 1$, dann folgt aus $(*)$: $k_2\alpha + k_2 = 0$, also $-k_2 = k_2\alpha = k_2$ für alle $k_2 \in K$. Damit ist $\alpha = \mathrm{id}$, also ist f ist orthogonal[58] und $\operatorname{char} K \neq 2$, Widerspruch![59]

BEISPIEL: Sei $\alpha = \mathrm{id}$ und $\operatorname{char} K = 2$, $\dim V = 2$, Basis $B := \{v_1, v_2\}$ von

[57] zu einer falschen Antwort: „Da werd' ich ja zum Terroristen!"

[58] „Das ist für Leute, die aus Hessen kommen, nicht so leicht, die können kein r und kein *ch* aussprechen. Eigentlich können sie fast gar nichts aussprechen"

[59] „Lassen Sie sich diese Lämmer auf der Zunge zergehen!" ;-)

V mit $G_B(f) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Dann gilt für $k_1, k_2 \in K$:

$$\begin{aligned} 0 &= f(k_1 v + k_2 w, k_1 v + k_2 w) \\ &= k_1^2 \underbrace{f(v,v)}_{=0} + k_1 k_2 \underbrace{f(v,w)}_{=1} + k_2 k_1 \underbrace{f(w,v)}_{=1} + k_2^2 \underbrace{f(w,w)}_{=0} \\ &= 2k_1 k_2 \\ &= 0 \end{aligned}$$

10.1.2 unitär/orthogonal $\Rightarrow$ Orthogonalbasis und Diagonalmatrix

Sei f unitär oder orthogonal. Dann existiert eine Orthogonalbasis von V, damit ist die Gramsche Matrix eine Diagonalmatrix.

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

- Induktionsverankerung: Mangels Elementen in der Basis offensichtlich f"ur$n \leq 1$.
- Induktionsannahme: $n \geq 2$ und Behauptung richtig für Räume der Dimension $< n$.
- Induktionsschritt: Ist $V = \operatorname{rad} V$, so ist jede Basis Orthogonalbasis. Sei $V \neq \operatorname{rad} V$, nach (10.1.1) existiert $v \in V$ mit $f(v,v) \neq 0$. Mit (9.4.4)b gilt: $\langle v \rangle \perp \langle v \rangle^\perp$. Es ist $\dim \langle v \rangle^\perp < \dim V$. Mit Induktionsvoraussetzung existiert eine Orthogonalbasis von $\langle v \rangle^\perp$ (bezüglich $f_{\langle v \rangle^\perp \times \langle v \rangle^\perp}$).

  Siehe (7.4.2), Basis von V ist $B_0 \cup \{v\}$, und zwar eine Orthogonalbasis. dumdidum...

10.1.3 (an)isotrop, hyperbolisch

Sei $v \in V$. v heißt *isotrop*, falls $f(v,v) = 0$. Ein Unterraum $U \leq V$ heißt *isotrop*, falls $f|_{U \times U}$ die Nullform ist. U heißt *anisotrop*, falls 0 das einzige isotrope Element von U ist. Ein Paar $(v,w) \in V \times V$ heißt *hyperbolisches Paar*, falls v, w isotrop sind und $f(v,w) = 1$ gilt. !

Sei v, w hyperbolisches Paar, $H := \langle v, w \rangle$, dann ist $\dim H = 2$,

$$G_{\{v,w\}}(f_{H \times H}) = \begin{pmatrix} 0 & 1 \\ f(w,v) & 0 \end{pmatrix}$$

Ein zweidimensionaler Unterraum von V heißt *hyperbolische Ebene*, wenn er von einem hyperbolischen Paar erzeugt wird.

10.1.4 Isotropie

Sei f orthogonal oder unitär (also nicht symplektisch). Genau dann ist U isotrop, wenn jedes Elemente aus U isotrop ist.

BEWEIS: U isotrop heißt: $U = \operatorname{rad} U = U \cap U^{\perp}$.

„$\Rightarrow$" Aus U isotrop folgt: jedes Element aus U ist isotrop.

„$\Leftarrow$" Jedes Element aus U sei also isotrop. Angenommen, $U \neq \operatorname{rad} U$, dann folgt mit (10.1.1): es existiert $u \in U$ mit $f(u,u) \neq 0$, also ist u nicht isotrop, Widerspruch!

10.1.5 Körperlemma

Sei $\alpha^2 = \mathrm{id} \neq \alpha$ und $a \in K$ mit $a\alpha = a$. Dann existiert $b \in K$ mit $b + b\alpha = a$.

BEWEIS: Fallunterscheidung:

- Der Fall $k + k\alpha = 0\ \forall\ k \in K$, dann folgt: $1 + 1\alpha = 1 + 1 = 0$, also $\operatorname{char} K = 2$, daraus folgt: $k\alpha = -k = k\ \forall\ k \in K$, also ist $\alpha = \mathrm{id}$, Widerspruch zu Wahl von α!

- Der Fall: es existiert $k_0 \in K$ mit $k_0 + k_0\alpha \neq 0$. Sei $k_1 := k_0 + k_0\alpha$, setze $b := k_0 k_1^{-1} a$. Es gilt:

  $$k_1\alpha = (k_0 + k_0\alpha) = k_0\alpha + k_0\alpha^2 = k_0\alpha + k_0 = k_1 \Rightarrow k_1^{-1}\alpha = k_1^{-1}$$

  Damit gilt:

  $$\begin{aligned} b + b\alpha &= k_0 k_1^{-1} a + (k_0 k_1^{-1} a)\alpha \\ &= k_0 k_1^{-1} a + k_0\alpha \underbrace{(k_1^{-1}\alpha)}_{k_1^{-1}} \underbrace{(a\alpha)}_{a} \\ &= a k_1^{-1} \underbrace{(k_0 + k_0\alpha)}_{k_1} \\ &= a \end{aligned}$$

10.1.6 Existenz eine hyperbolischen Paares

VORAUSSETZUNG: Sei f symplektisch, orthogonal oder unitär. Es existiere ein isotropes Element $v \in V \setminus \operatorname{rad} V$.

SATZ: Es existiert ein $w \in V$, so daß (v, w) ein hyperbolischs Paar ist.

BEWEIS: Es existiert $w' \in V$ mit $f(v, w') \neq 0$. Sei $k' = (f(v,w)^{-1})\alpha^{-1}$. Dann gilt:

$$f(v, k'w') = k'\alpha f(v, w') = f(v, w')^{-1} f(v, w) = 1$$

Wir können damit w' so wählen, daß $f(v, w') = 1$. Zu zeigen bleibt: w' ist isotrop oder ein anderer von w' abgeleiteter Vektor w, für den gilt: $f(v, w) = 0$

- Falls f symplektisch, ist jeder Vektor isotrop.
- Falls f nicht symplektisch, für $k \in K$ gilt:

$$f(v, kv + w') = f(v, kv) + f(v, w') = k\alpha \underbrace{f(v, v)}_{=0} + f(v, w') = 1$$

  - Falls f orthogonal: Setze $k_0 := -2^{-1} f(w', w')$ und $w := k_0 v + w'$. Dann gilt:

$$\begin{aligned} f(w, w) &= f(k_0 v + w', k_0 v + w') \\ &= \underbrace{f(k_0 v, k_0 v)}_{=0} + f(k_0 v, w') + f(w', k_0 v) + f(w', w') \\ &= 2k_0 \underbrace{f(v, w')}_{=1} + f(w', w') \\ &= -\frac{2}{2} f(w', w') + f(w', w') = 0 \end{aligned}$$

    Damit ist w isotrop.

  - Falls f unitär: Es ist $f(w', w') = f(w', w')\alpha$, also auch $-f(w', w') = (-f(w', w'))\alpha$. Wende (10.1.5) an, damit existiert ein $k_0 \in K$ mit $k_0 + k_0\alpha = -f(w', w')$. Setze $w = k_0 v + w'$.

$$\begin{aligned} f(w, w) &= f(k_0 v + w', k_0 v + w') \\ &= \underbrace{f(k_0 v, k_0 v)}_{=0} + f(k_0 v, w') + f(w', k_0 v) + f(w', w') \\ &= k_0 \underbrace{f(v, w')}_{=1} + k_0\alpha \underbrace{f(v, w')\alpha}_{=1} + f(w', w') \\ &= k_0 + k_0\alpha + f(w', w') \\ &= -f(w', w') + f(w', w') = 0 \end{aligned}$$

    Damit ist w isotrop.

Damit ist (v, w) ein hyperbolisches Paar.

BEISPIEL: Sei $\operatorname{char} K = 2$ und $\alpha = \mathrm{id}$, sei $\dim V = 2$. Sei $B := \{v_1, v_2\}$ Basis von V. Sei $G_B(f) := \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. Dann ist f symmetrisch und regulär, d.h.

$\operatorname{rad} V = \{0\}$. Offensichtlich ist v_1 isotrop. Sei $w = k_1 v_1 + k_2 v_2$.

$$\begin{aligned} f(w,w) &= f(k_1v_1 + k_2v_2, k_1v_1 + k_2v_2) \\ &= k_1^2 \underbrace{f(v_1,v_1)}_{=0} + k_1k_2 f(v_1,v_2) + k_1k_2 f(v_w,v_1) + k_2^2 f(v_1,v_2) \\ &= \underbrace{2 \cdot k_1k_2}_{=0} + k_2^2 = k_2^2 \end{aligned}$$

Damit gilt:

$$f(w,w) = 0 \Leftrightarrow k_2^2 = 0 \Leftrightarrow k_2 = 0 \Leftrightarrow w = k_1 v$$

Damit ist w linear abhängig von v; somit existiert kein hyperbolisches Paar (v,w) in $V \times V$.

10.1.7 Unterraum durch hyperbolische Paare „aufblasen“

Voraussetzung: Sei f symplektisch, orthogonal oder unitär und V regulär bezüglich f. Sei U ein Unterraum von V mit $U = \operatorname{rad} U \perp U_0$, sei $m := \dim \operatorname{rad} U$.

Satz: Für jede Basis $\{u_1, ..., u_m\}$ von $\operatorname{rad} U$ gilt:

1. Es existieren $v_1, ..., v_m \in V$ mit

   $$U + \langle v_1, ..., v_m \rangle = U_0 \perp \langle u_1, v_1 \rangle \perp ... \perp \langle u_m, v_m \rangle$$

   wobei die (u_i, v_i) hyperbolische Paare sind.

2. Ist U isotrop, so ist $\dim U \leq \frac{1}{2} \cdot \dim V$

Beweis:

1. durch Induktion nach m:

   - Induktionsanfang: $m = 0$ ist trivialerweise erfüllt.
   - Induktionsannahme: $m \geq 1$ und Behauptung richtig für $m - 1$.
   - Induktionsschritt: Sei

     $$U^* = U_0 \perp \langle u_1, ..., u_{m-1} \rangle \text{ wobei } \langle u_1, ..., u_{m-1} \rangle \leq \operatorname{rad} U^*$$

     Zudem ist $\operatorname{rad} U^* \leq \operatorname{rad} U$, damit folgt: $\operatorname{rad} U^* = \langle u_1, ..., u_{m-1} \rangle$. Mit (9.4.4) ist $U^{*\perp\perp} = U^*$, also

     $$\operatorname{rad} U^{*\perp} = U^{*\perp} \cap U^{*\perp\perp} = U^{*\perp} \cap U^* = \operatorname{rad} U^*$$

Damit folgt: $\operatorname{rad} U^* = \operatorname{rad} U^{*\perp} = \langle u_1, ..., u_{m-1}\rangle$. Damit ist $u_m \in U^{*\perp}$ und nicht in $\operatorname{rad} U^{*\perp}$. Mit (10.1.6) (angewand auf $U^{*\perp}$ und u_m) gilt: es existiert $v_m \in U^{*\perp}$, so daß (u_m, v_m) ein hyperbolisches Paar ist.

Sei $H := \langle u_m, v_m\rangle$ hyperbolische Ebene, H ist regulär. Mit (9.4.4) folgt:

$$V = H \perp H^\perp \text{ und } U^* \leq H^\perp$$

Da $H^\perp$, H und V alle regulär sind, erfüllen $H^\perp$ und U^* die Voraussetzungen für $m-1$. Nach Induktionsvoraussetzung existieren $v_1, ..., v_{m-1} \in H^\perp$, so daß (u_i, v_i) für $i = 1, ..., m-1$ hyperbolische Paare sind und

$$\begin{aligned} U^* + \langle v_1, ..., v_{m-1}\rangle &= U_0 \perp \langle u_1, v_1\rangle \perp ... \perp \langle u_{m-1}, v_{m-1}\rangle \\ U^* + \langle v_1, ..., v_m\rangle &= U_0 \perp \langle u_1, v_1\rangle \perp ... \perp \langle u_{m-1}, v_{m-1}\rangle \perp H \end{aligned}$$

2. Sei U isotrop, d.h. $U = \operatorname{rad} U$, also $U_0 = \{0\}$. Dann folgt aus eben gezeigtem 1.:

$$U \leq \underbrace{\langle u_1, v_1\rangle \perp ... \perp \langle u_m, v_m\rangle}_{\text{hyperbolische Ebenen}} \leq V$$

Damit ist $\dim U \leq 2 \dim U \leq \dim V$.

10.1.8 Zerlegung eines Raumes in hyperbolische Ebenen

Voraussetzung: Sei f und V wie in (10.1.7), und sei U ein bezüglich Inklusion maximaler isotroper Unterraum von V. Sei $\dim U = m$ und $\{u_1, ..., u_m\}$ Basis von U.

Behauptung: Es existieren $v_1, ..., v_m \in V$, so daß:

$$V = \langle u_1, v_1\rangle \perp \langle u_m, v_m\rangle \perp V_0$$

wobei (u_i, v_i) hyperbolische Paare und V_0 anisotrop.

Beweis: Wende (10.1.7) an, dann existieren $v_1, ..., v_m$, so daß

$$U \leq \tilde{U} := \langle u_1, v_1\rangle \perp ... \perp \langle u_1, v_1\rangle$$

wobei (u_i, v_i) hyperbolische Paare sind. Sei $B := \{u_1, v_1, ..., u_m, v_m\}$, dann ist

$$G_B(f) = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Damit ist $\tilde{U}$ regulär, also nach (9.4.4) ist $\tilde{U} \perp \tilde{U}^{\perp}$. Setze $V_0 := \tilde{U}^{\perp}$.

10.1.9 Vektorräume gerader Dimension

Sei V regulär und f symplektisch. Dann gilt:

1. $V = H_1 \perp ... \perp H_n$ mit H_i hyperbolische Ebenen für $i = 1, ..., n$
2. $\dim V$ ist gerade.

10.2 Isometrien

10.2.1 Definition

- Sei K Körper und α fest gewählter Automorphismus von K. V und W sind K-Vektorräume mit α-Bilinearform f bzw. g. Ein Homomorphismus $\varphi : V \to W$ heißt *Isometrie*, falls gilt:

$$f(v, w) = g(v\varphi, w\varphi) \; \forall \; v, w \in V$$

- Ist zusätzlich φ bijektiv, so heißen (V, f) und (W, g) *isometrisch*.
- Sei $\varphi \in \operatorname{Hom}(V, W)$, sei B Basis von V. Genau dann ist φ Isometrie, wenn $f(b, b') = g(b\varphi, b'\varphi)$ ist für alle Basiselemente b, b'. Sind B und B' Basen von V bzw. W und ist $\varphi : B \to B'$ eine Bijektion mit der Eigenschaft $f(b, b') = g(b\varphi, b'\varphi)$ für alle $b, b' \in B$, so sind (V, f) und (W, g) isometrisch.
- Sei V Vektorraum mit α-Bilinearform f. Dann heißt $\varphi \in \operatorname{Hom}(V, V)$ f-Isometrie, falls $f(v, w) = f(v\varphi, w\varphi) \; \forall \; v, w \in V$.
- Sei $I_f(V)$ die Menge aller f-Isometrien auf V.

10.2.2 Gruppe der Isomorphismen

Voraussetzung: Sei f orthosymmetrisch. Sei V regulär.

Behauptung: Alle Elemente aus $I_f(V)$ sind Isomorphismen, und $I_f(V)$ ist eine Untergruppe von $GL(V)$.

Beweis: Sei $\varphi \in I_f(V)$.

- Wir zeigen: $\operatorname{Kern} \varphi = \{0\}$, dann ist φ bijektiv. Sei $v \in \operatorname{Kern} \varphi$. Für alle $w \in V$ gilt:
$$f(v, w) = f(v\varphi, w\varphi) = f(0, w\varphi) = 0$$
Damit ist $v \in \operatorname{rad} V = \{0\}$ wegen der Regularität. Also $\operatorname{Kern} \varphi = \{0\}$, und damit ist φ Isomorphismus.

- Zu zeigen bleibt: Untergruppenkriterium $x, y \in I_f(V) \Rightarrow xy^{-1} \in I_f(V)$. Sei $\varphi \in I_f(V)$, dann gilt:

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

  Damit ist $\varphi^{-1} \in I_f(V)$. Seien $\varphi, \psi \in I_f(V)$. Dann gilt:

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

  Damit ist $\varphi\psi^{-1} \in I_f(V)$.

10.2.3 Kriterium für Isometrie

VORAUSSETZUNG: Sei B Basis von V und $\varphi \in \mathrm{Hom}(V,V)$ bijektiv, und seien f und g α-Bilinearformen auf V.

BEHAUPTUNG: Genau dann ist φ eine Isometrie von (V,f) auf (W,g), falls

$$(*) \quad G_B(f) = M(\varphi, B, B) \cdot G_B(g) \cdot (M(\varphi, B, B)\alpha)^t$$

BEWEIS:

„$\Rightarrow$“ Sei φ Isometrie. Dann ist $G_B(f) = G_{B\varphi}(g)$. Mit (9.2.3) gilt:

$$\begin{aligned}(**) \quad G_B(f) = G_{B\varphi}(g) &= M(\mathrm{id}, B\varphi, B) G_B(g) (M(\mathrm{id}, B, B\varphi)\alpha)^t \\ &= M(\varphi, B, B) \cdot G_B(g) \cdot (M(\varphi, B, B)\alpha)^t\end{aligned}$$

„$\Leftarrow$“ Gelte $(*)$. Dann gilt auch $(**)$ (siehe (9.2.3)), also ist $G_{B\varphi}(G) = G_B(f)$.

10.2.4 Beispiele

- Sei μ eine Isomor.[60] von V auf W und f α-Bilinearform auf V. Für $u, w \in W$ sei $g(u,w) := f(u\mu^{-1}, w\mu^{-1})$. Dann ist g eine α-Bilinearform auf W, und (V,g) und (W,g) sind isometrisch.

$$f(v,v') \stackrel{?}{=} g(v\mu, v'\mu) = f(v\mu\mu^{-1}, v'\mu\mu^{-1}) = f(v,v')$$

  Seien (V,f) und (W,h) gegeben, und es existiere ein Isomorphismus $\mu : V \to W$. Genau dann sind (V,f) und (W,h) isometrische, wenn (W,h) und (W,g) (wobei g wie oben definiert) isometrisch sind.

[60] „klingt männlicher...“

- Sei f orthogonal, $w \in V$ mit $f(w,w) \neq 0$. Sei

  $$s_w : V \to V \text{ mit } vs_w := v - 2f(v,w) \cdot f(w,w)^{-1} w \;\forall\, v \in V$$

  Dann ist s_w eine Isometrie auf (V,f) und heißt *Spiegelung* zu w an $\langle w \rangle^\perp$:

  - s_w ist lineare Abbildung: einfafches Nachrechnen.
  - Seien $u, v \in V$. Dann ist

    $$\begin{aligned} f(us_w, vs_w) &= f\left(u - 2\frac{f(u,w)}{f(w,w)}w, v - 2\frac{f(v,w)}{f(w,w)}w\right) \\ &= f(u,v) - 2\frac{f(u,w)}{f(w,w)}f(w,v) - 2\frac{f(v,w)}{f(w,w)}f(u,w) \\ &\quad +4\frac{f(u,w)f(v,w)}{f(w,w)f(w,w)}f(w,w) \\ &= f(u,v) - 4\frac{f(u,w)f(v,w)}{f(w,w)} + 4\frac{f(u,w)f(v,w)}{f(w,w)} \\ &= f(u,v) \end{aligned}$$

  - Veranschaulichung: $V = \mathbb{R}^2$, f Skalarprodukt; $f(v,w) = |v|\,|w| \cos\alpha$; $w_0 := (|v|\,|w|^{-1} \cos\alpha)w$; $x = v - w_0$; $v - 2w_0 = v - 2\frac{|v|}{|w|}\cos\alpha w = v - 2\frac{f(v,w)}{f(w,w)}w = vs_w$

- Sei f symplektisch, $0 \neq w \in V$. Für alle $c \in K^*$ ist $vt_w := v + cf(v,w)w$ eine Isometrie auf V, dabei heißt t_w *Transvektion* zu w (bezüglich c).

  $$\begin{aligned} & f(vt_w, v't_w) \\ =\; & f(v + cf(v,w)w, v' + cf(v',w)w) \\ =\; & f(v,v') + cf(v,w) \cdot \underbrace{(f(v',w) + f(w,v'))}_{=0} + \underbrace{c^2 f(v,w)f(v',w)f(w,w)}_{=0} \\ =\; & f(v,v') \end{aligned}$$

  t_w ist linear (einfaches Nachrechnen), Beachte: $f(w,w) = 0$, d.h. $w \in \langle w \rangle^\perp$.

  t_w ist bijektiv: Sei $u \in \langle w \rangle^\perp$, dann: $ut_w = u$. Entweder ist $V = \langle w \rangle^\perp \Rightarrow t_w = \mathrm{id}$, oder $V \neq \langle w \rangle^\perp$, d.h. $\dim \langle w \rangle^\perp = \dim V - 1$. Sei $w_0 \in V \setminus \langle w \rangle^\perp$ und B_0 Basis von $\langle w \rangle^\perp$. Dann ist $B = \{w_0\} \cup B_0$. Dann ist

  $$M(t_w, B, B) = \left(\begin{array}{c|ccc} 1 & * & * & * \\ \hline 0 & 1 & \cdots & 0 \\ 0 & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & 1 \end{array}\right)$$

Damit ist $\det M = 1$

10.2.5 Klassifikationssatz für symplektische Räume

SATZ: Zwei endlich-dimensionale reguläre symplektische Räume über K sind genau dann isometrisch, wenn sie gleiche Dimension haben.

BEWEIS:

„$\Rightarrow$" Seien (V, f) und (W, G) endlichdimensionale reguläre symplektische Räume. Ist (V, f) isometrisch zu (W, g), so sind insbesondere V und W isomorph, also $\dim V = \dim W$.

„$\Leftarrow$" Sei $\dim V = \dim W$. Nach (10.1.9) existieren hyperbolische Paare $(v_1, w_1), ..., (v_n, w_n)$ von V und $(v'_1, w'_1), ..., (v'_n, w'_n)$ von W mit

$$V = \langle v_1, w_1 \rangle \perp ... \perp \langle v_n, w_n \rangle \text{ und } W = \langle v'_1, w'_1 \rangle \perp ... \perp \langle v'_n, w'_n \rangle$$

Insbesondere ist $\{v_1, w_1, ..., v_n, w_n\}$ Basis von V und $\{v'_1, w'_1, ..., v'_n, w'_n\}$ Basis von W. Definiere

$$\mu : V \to W \text{ mit } v_i\mu = v'_i \text{ und } w_i\mu = w'_i$$

Es gilt: $f(v_i, v_j) = 0 = g(v_i\mu, v_j\mu)$ und

$$f(v_i, w_j) = \begin{cases} 1 & \text{falls} \quad i = j \\ 0 & \text{sonst} \end{cases} = g(v_i\mu, w_j\mu)$$

Damit ist μ eine bijektive Isometrie.

10.2.6 Körperlemma

VORAUSSETZUNG: Sei K ein endlicher Körper und $K^2 := \{k^2 \mid k \in K\}$.

BEHAUPTUNG:

1. • bei $\operatorname{char} K = 2$: $K = K^2$
   • bei $\operatorname{char} K \neq 2$: $|K^*| = 2 \cdot ((K^2) - 1)$
2. Für alle $a, b \in K^*$ gilt: $K = aK^2 + bK^2$

BEWEIS:

1. Sei $k \in K$. Dann hat $x^2 - k^2 \in K[x]$ in K die Nullstellen $\pm k$. Sei $\beta : K \to K^2$ mit $k \mapsto k^2$. Sei $k^2 \in K^2 \cap K^*$.

- Falls $\operatorname{char} K = 2$, so hat k^2 genau ein Urbild. Damit ist β injektiv, K endlich, also β auch bijektiv, also $K = K^2$.
- Falls $\operatorname{char} K \neq 2$ ist, so hat k^2 genau zwei Urbilder. $|K^*| = 2\,|K^2 \cap K^*| = 2(|K^2| - 1)$

2. Ist $\operatorname{char} K = 2$, so ist wie gesehen $K = K^2$, damit folgt:

$$k = a \cdot (ka^{-1}) + b \cdot 0 \;\forall\; k \in K^*$$

Sei also $\operatorname{char} K \neq 2$ und $K_2 := K^2 \cap K^*$. Wie oben gesehen ist

$$2\left|K^2\right| = 2(|K_2| + 1) = 2\,|K_2| + 2 = |K^*| + 2 = |K| + 1$$

Damit enthält K^2 mehr als die Hälfte der Elemente von K. Die Mengen

$$-K^2 \text{ und } -b^{-1}k + (ab^{-1})K^2 = \left\{ -b^{-1} + (ab^{-1})h^2 \;\middle|\; h \in K \right\}$$

mit $k \in K$ haben jeweils $|K^2|$ Elemente und sind damit nicht disjunkt. Es existieren also $t, h \in K$ mit

$$-t^2 = -b^{-1}k + (ab^{-1})h^2 \Rightarrow k = bt^2 + ah^2$$

10.2.7 Klassifikation von anisotropen Vektorräumen

Sei K endlich, f orthogonal und $c \in K \setminus K^2$ und sei V anisotrop bezüglich f. Dann gilt einer der folgenden Fälle:

(a) $\dim V = 0$

(b) $\dim V = 1$ und es existiert $v \in V$ mit $f(v,v) = 1$

(c) $\dim V = 1$ und es existiert $v \in V$ mit $f(v,v) = c$

(d) $\dim V = 2$ und es existiert eine Basis v_1, v_2 von V mit

$$f(v_1, v_1) = 1 \quad \wedge \quad f(v_1, v_2) = 0 \quad \wedge \quad f(v_2, v_2) = -c$$

Keine zwei der in (a) bis (d) angegebenen Räume sind isometrisch.

Beweis:

- Wir können annehmen: $n := \dim V \geq 1$.

- Wir zeigen: $n \leq 2$. Mit (10.1.2) gilt: Es existiert eine Orthogonalbasis $v_1, ..., v_n$ von V. Setze $a_i := f(v_i, v_i)$. Da V anisotrop ist, ist $a_i \neq 0$. Angenommen, $n \geq 3$. Dann folgt mit (10.2.6): $K = a_1 K^2 + a_2 K^2$. Es existieren $k_1, k_2 \in K$ mit $a_1 k_1^2 + a_2 k_2^2 = -a_3$.

  $$f(k_1 v_1 + k_2 v_2 + v_3, k_1 v_1 + k_2 v_2 + v_3) = k_1^2 a_1 + k_2^2 a_2 + a_3 = 0$$

  Da V anisotrop ist, ist $k_1 v_1 + k_2 v_2 + v_3 = 0$. Damit sind die Basiselemente nicht mehr linear unabhängig, Widerspruch!

- Sei nun $\dim V = 1$. Sei $K_2 := K^2 \cap K^*$, dann ist K_2 eine Untergruppe von K^*. Für $a, b \in K^*$ sei $a \sim b :\Leftrightarrow ab^{-1} \in K_2$, dann ist $\sim$ eine Äquivalenzrelation auf K^* mit den Äquivalenzklassen aK_2 für $a \in K^*$

  - Angenommen: $a_1 \in K_2$. Dann existiert $q \in K^*$ mit $q^2 = a_1$. Setze $v := q^{-1} v_1$. Dann:

    $$\begin{aligned} f(v, v) &= f(q^{-1} v_1, q^{-1} v_1) \\ &= (q^{-1})^2 f(v_1, v_1) \\ &= (q^{-1})^2 a_1 = (q^{-1})^2 q^2 = 1 \end{aligned}$$

    Dies ist Fall (b).

  - Angenommen, $a_1 \notin K_2$. Nach (10.2.6) ist $|K_2| = \frac{1}{2} |K^*|$, außerdem (mit der Bijektion $x \mapsto cx$) $|K_2| = |cK_2|$, also ist wegen der oben genannten Äquivalenzklassen $K^* = K_2 \uplus cK_2$. Damit ist $a_i \in cK_2$, dann folgt $a_1 \in cK_2$, damit existieren $k^2 \in K_2$ mit $a_1 = ck^2$. Sei $v := k^{-1} v_1$, dann ist

    $$f(v, v) = f(k^{-1} v_1, k^{-1} v_1) = k^{-2} a_1 = c$$

    Dies ist Fall (c).

- Wir zeigen: Die Räume aus (b) und (c) sind nicht isometrisch. Sei (V, f) wie in (b) und (V, f') wie in (c). Angenommen, es existiert eine bijektive Isometrie φ von (V, f) auf (V, f'). Wende (10.2.3) an, dann:

  $$G_{\{v_1\}}(f) = G_{\{v_1 \varphi\}}(f') \overset{(10.2.3)}{=} \{ (\mid \varphi\}, \{v_1\}, \{v_1\}) \cdot G_{\{v_1\}}(f') \cdot M(\varphi, \{v_1\}, \{v_1\})^t$$

  Betrachte Determinanten:

  $$1 = (\det M(\varphi, \{v_1\}, \{v_1\}))^2 c$$

  Damit liegt $c^{-1} \in K_2$ und damit $c \in K_2$, Widerspruch! Damit existiert keine Isometrie.

- Sei nun $\dim V = 2$. Nach (10.2.6) ist $a_1K^2 + a_2K^2 = K$. Also existieren $k_1, k_2 \in K^*$ mit $a_1k_1^2 + a_kk_2^2 = 1$. Setze $w_1 := k_1v_1 + k_2v_2$, dann ist[61]

  $$f(w_1, w_1) = k_1a_1 + k_2a_2 = 1$$

  Zudem ist $\langle w_1\rangle^\perp \perp \langle w_1\rangle = V$, damit existiert w_2' mit $\langle w_1\rangle^\perp = \langle w_2'\rangle$. Sei $b := f(w_2', w_2')$. Dann gilt für alle $k \in K^*$:

  $$f(kw_1 + w_2', kw_1 + w_2') = k^2 f(w_1, w_1) + b = k^2 + b$$

  Da V anisotrop ist, gilt: $k^2 + b \neq 0$ für alle $k \in K^*$, damit ist $-b \notin K_2$. Damit ist $-b \in cK_2$, dann existiert $h \in K^*$ mit $-b = ch^2$. Setze $w_2 = h^{-1}w_2'$. Dann gilt:

  $$f(w_2, w_2) = f(h^{-1}w_2', h^{-1}, w_2') = h^{-2}b = -c$$

  Zudem ist w_2 ein skalares Vielfaches von w_2', und $w_2' \perp w_1$, damit ist

  $$f(w_1, w_2) = 0$$

  Damit ergibt sich die Gram'sche Matrix als

  $$\begin{pmatrix} 1 & 0 \\ 0 & -c \end{pmatrix}$$

10.2.8 Klassifikation von Vektorräumen (f orthogonal)

Sei K endlich, $c \in K^* \setminus K^2$ und f orthogonal, und sei V regulär bezüglich f und $\dim V \geq 1$. Dann ist $n \in \mathbb{N}_0$ und es existieren hyperbolische Ebenen $H_1, ..., H_n$ in V, und es gilt einer der folgenden Fälle:

(a) $\dim V = 2n + 1$ und $V = H_1 \perp ... \perp H_n \perp \langle v_0\rangle$ mit $f(v_0, v_0) = 1$.

(b) $\dim V = 2n + 1$ und $V = H_1 \perp ... \perp H_n \perp \langle v_0\rangle$ mit $f(v_0, v_0) = c$.

(c) $\dim V = 2n$ und $V = H_1 \perp ... \perp H_n$.

(c) $\dim V = 2n$ und $V = H_1 \perp ... \perp H_{n-1} \perp V_0$ mit V_0 wie in (10.2.7)(d)

Keine zwei der in (a) bis (d) angegebenen Räume sind isometrisch.

Beweis: Wende (10.1.8) an: V läßt sich zerlegen in hyperbolische Ebenen und anisotropes V_0:

$$V = H_1 \perp ... \perp H_n \perp V_0$$

[61] Zu einem Kommentar zu einem Schreibfehler an der Tafel: „Erschrecken Sie mich doch nicht so! Sie müssen auf mein Alter Rücksicht nehmen!“

Mit (10.2.7) ist V_0 bekannt, nämlich einer der vier Fälle. Sei (v_i, w_i) hyperbolisches Paar H_i. Dann ist $B = \{v_1, w_1, ..., v_n, w_n, v_0\}$ Basis von V in den Fällen (a) und (b); sei $B = \{v_1, w_1, ..., v_n, w_n\}$ Basis im Fall (c) und $B = \{v_1, w_1, ..., v_{n-1}, w_{n-1}, v, w\}$ Basis im Fall (d).

Im Fall (a):

$$G_B(f) = \begin{pmatrix} 0 & 1 & \cdots & 0 & 0 & 0 \\ 1 & 0 & \ddots & 0 & 0 & 0 \\ \vdots & \ddots & \ddots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \Rightarrow \det G_B(f) = (-1)^n$$

Im Fall (b):

$$G_B(f) = \begin{pmatrix} 0 & 1 & \cdots & 0 & 0 & 0 \\ 1 & 0 & \ddots & 0 & 0 & 0 \\ \vdots & \ddots & \ddots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & c \end{pmatrix} \Rightarrow \det G_B(f) = (-1)^n c$$

Im Fall (c):

$$G_B(f) = \begin{pmatrix} 0 & 1 & \cdots & 0 & 0 \\ 1 & 0 & \ddots & 0 & 0 \\ \vdots & \ddots & \ddots & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \Rightarrow \det G_B(f) = (-1)^n$$

Im Fall (d):

$$G_B(f) = \begin{pmatrix} 0 & 1 & \cdots & 0 & 0 & 0 & 0 \\ 1 & 0 & \ddots & 0 & 0 & 0 & 0 \\ \vdots & \ddots & \ddots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -c \end{pmatrix} \Rightarrow \det G_B(f) = (-1)^n c$$

Damit sind (a) und (b) sowie (c) und (d) nicht isotrop.

10.2.9 Klassifikation von Vektorräumen (f unitär)

Sei K endlich, f unitär und V regulär bezüglich f mit $\dim V \geq 1$. Dann gilt einer der folgenden Fälle:

(a) $\dim V = 2n$ und $V = H_1 \perp ... \perp H_n$ mit H_i hyperbolische Ebenen.

(b) $\dim V = 2n + 1$ und $V = H_1 \perp ... \perp H_n \perp \langle v_0 \rangle$ mit H_i hyperbolische Ebenen und $f(v_0, v_0) = 1$.

In beiden Fällen existiert eine Orthonormalbasis von V.

10.2.10 Trägheitssatz von Sylvester

Definition: Der *Index* einer Bilinearform ist definiert als

$$\operatorname{Ind} f := \max \left\{ \dim U \mid U \leq V \wedge \underset{\text{Orth.Basis}}{\exists\ B} \text{ bezüglich } f|_{U \times U} \right\}$$

Voraussetzung: Sei entweder

(i) $K = \mathbb{R}$ und f orthogonal

(ii) $K = \mathbb{C}$ und f unitär, wobei α die Komplexkonjugation ist.

Behauptung: Dann existiert eine Orthogonalbasis B von V mit

$$f(b, b) \in \{0, 1, -1\}\ \forall\, b \in B \tag{*}$$

Für jede Basis, die $(*)$ erfüllt, ist $\operatorname{Ind} f$ die Anzahl der $b \in B$ mit $f(b, b) = 1$.

Beweis: Nach (10.1.2) existiert eine Orthogonalbasis B' von V. Sei $b \in B'$ und $k_b := f(b, b)$. Dann ist

$$k_b = \begin{cases} k_b \in \mathbb{R} & \text{falls} \quad K = \mathbb{R} \\ \overline{k_b} \in \mathbb{R} & \text{falls} \quad K = \mathbb{C} \end{cases}$$

Falls $k_b > 0$: Es existiert $q_b \in \mathbb{R}$ mit $q_b^2 = k_b$; analog: falls $k_b < 0$: Es existiert $q_b \in \mathbb{R}$ dumdidummit $q_b^2 = -k_b$. Durch Ersetzen der $b \in B'$ mit $k_b \neq 0$ durch $q_b^{-1} b$ erhalten wir eine Basis B. Dann gilt:

$$f(q_b^{-1} b, q_b^{-1} b) = \begin{cases} q_b^{-2} f(b, b) = q_b^{-2} k_b & \text{falls} \quad K = \mathbb{R} \\ q_b^{-1} \overline{q_b^{-1}} f(b, b) = q_b^{-2} k_b & \text{falls} \quad K = \mathbb{C} \end{cases}$$

Dabei ist

$$q_b^{-2} k_b = \begin{cases} k_b^{-1} k_b = 1 & \text{falls} \quad k_b > 0 \\ -k_b^{-1} k_b = -1 & \text{falls} \quad k_b < 0 \end{cases}$$

Damit ist $f(b,b) \in \{0,1,-1\}\ \forall\, b \in B$.

Sei $U \leq V$ mit Orthonormalbasis E und $\dim U = \operatorname{Ind} f$. Sei $B_1 = \{b \in B \mid f(b,b) = 1\}$ und $B^* = B \setminus B_1$. Zu zeigen: $\dim U = |B_1|$.

Angenommen, $|B_1| \neq \dim U$, also $|B_1| < \dim U$ (der Fall $|B_1| > \dim U$ geht nicht, da $\dim U$ maximal gewählt wurde). Dann ist

$$\dim U + \dim \langle B^* \rangle = \dim U + |B^*| > |B_1| + |B^*| = |B| = \dim V$$

Nach Dimensionssatz ist aber

$$\dim V = \dim U + \dim \langle B^* \rangle - \dim(U \cap \langle B^* \rangle)$$

Damit ist $U \cap \langle B^* \rangle \neq \{0\}$. Sei also $w \in U \cap \langle B^* \rangle$ mit $w \neq 0$ Dann existieren $h_e, l_b \in K$ mit

$$w = \sum_{e \in E} h_e e = \sum_{b \in B^*} l_b b$$

Dann ist

$$\begin{aligned}
f(w,w) &= f\left(\sum_{e \in E} h_e e, \sum_{e \in E} h_e e\right) \\
&= \sum_{e \in E} \begin{cases} h_e^2 f(e,e) = h_e^2 & \text{falls } K = \mathbb{R} \\ h_e \overline{h_e} f(e,e) & \text{falls } K = \mathbb{C} \end{cases} \\
f(w,w) &= f\left(\sum_{b \in B^*} l_b b, \sum_{b \in B^*} l_b b\right) \\
&= \sum_{b \in B^*} \begin{cases} l_b^2 f(b,b) & \text{falls } K = \mathbb{R} \\ l_b \overline{l_b} f(e,e) & \text{falls } K = \mathbb{C} \end{cases}
\end{aligned}$$

Damit ist

(i) bei $K = \mathbb{R}$:

$$\underbrace{\sum_{e \in E} h_e^2}_{>0} = \underbrace{\sum_{b \in B^*} l_b^2 \underbrace{f(b,b)}_{=0 \vee = -1}}_{\leq 0}$$

(ii) bei $K = \mathbb{C}$:

$$\underbrace{\sum_{e \in E} h_e \overline{h_e}}_{>0} = \underbrace{\sum_{b \in B^*} l_b \overline{l_b} \underbrace{f(b,b)}_{=0 \vee = -1}}_{\leq 0}$$

10.2.11 Klassifikationssatz für orthogonale und unitäre Räume

Satz: Zwei endlichdimensionale reguläre Vektorräume, die beide (i) oder beide (ii) aus (10.2.10) erfüllen, sind genau dann isometrisch, wenn sie gleiche Dimension und gleichen Index haben. Beweis: Sei (V, f) und (V', f') endlichdimensional, regulär mit (i) bzw. (ii) aus (10.2.10).

„$\Leftarrow$" Angenommen, $\dim V = \dim V'$ und $\operatorname{Ind} f = \operatorname{Ind} f'$. Wende (10.2.10) an: Es existieren Basen $B = \{b_1, ..., b_n\}$ von V und $B' = \{b'_1, ..., b'_n\}$ von V'. Sei $n = \dim V$.

$$\begin{aligned} f(b_i, b_i) &= f'(b'_i, b'_i) = 1 \; \forall \; i = 1, ..., \operatorname{Ind} f \\ f(b_j, b_j) &= f'(b'_j, b'_j) = -1 \; \forall \; i = \operatorname{Ind} f + 1, ..., n \end{aligned}$$

Sei $\varphi : V \to V'$ die lineare Fortsetzung der Abbildung $b_i \mapsto b'_i \; \forall \; i = 1, ..., n$. Dann gilt: $f(b_i, b_j) = f'(b'_i\varphi, b'_j\varphi)$ und φ ist bijektive Isometrie.

„$\Rightarrow$" Seien (V, f) und (V', f') isometrisch, sei φ bijektive Isometrie. Damit sind die Raume isomorph, also $n := \dim V = \dim V'$. Zu zeigen: $\operatorname{Ind} f = \operatorname{Ind} f'$. Seien B, B' wie oben Basen, also $f(b_i, b_i) = 1$ für $i \leq \operatorname{Ind} f$. Dann ist $B\varphi = \{b_1\varphi, ..., v_n\varphi\}$ Basis von V' und $f(b_1, b_i) = f'(b_i\varphi, b_i\varphi) \in \{0, 1, -1\}$ für alle i.

Die Anzahl der $b_i\varphi \in B\varphi$ mit $f(b_i\varphi, b_i\varphi) = 1$ ist $\operatorname{Ind} f$. Nach (10.2.10) ist diese Anzahl auch $\operatorname{Ind} f'$, also $\operatorname{Ind} f = \operatorname{Ind} f'$.

10.2.12 Satz von Witt

Satz: Sei f orthogonal, symplektisch oder unitär und V regulär bezüglich f. Seien U_1 und U_2 Unterräume von V. Es existiere eine biejktive Isometrie φ von $(U_1, f|_{U_1 \times U_1})$ auf $(U_2, f|_{U_2 \times U_2})$. Dann existiert $\varphi^* \in I_f(V)$ mit $\varphi^*|_{U_1} = \varphi$.

Beweis: Induktion nach $\dim V$.

- Induktionsverankerung: Bei $\dim V = 0$ ist nichts zu zeigen.
- Induktionsannahme: Sei $n := \dim V > 0$ und die Behauptung richtig für Vektorräume kleinerer Dimension.
- Induktionsschritt: Fallunterscheidung:

  (A) U_1 ist nicht isotrop, und es existiert ein regulärer Unterraum $\{0\} \neq H \leq U_1 \cap U_2$ mit $\varphi|_H = \mathrm{id}$.

  (B) U_1 ist nicht isotrop.

(B_1) f ist symplektisch.

(B_2) Es existiert $v_1 \in U_1$ mit $f(v_1, v_1) \neq 0$ und $H = \langle v_1, v_1\varphi\rangle$ ist regulär.

(B_3) Es existiert $v_1 \in U_1$ mit $f(v_1, v_1) \neq 0$ und $H = \langle v_1, v_1\varphi\rangle$ ist nicht regulär.

(C) U_1 ist isotrop.

(A) Sei $V_0 := H^\perp$. Nach (9.4.4)(b) angewandt auf V, U und U_2 gilt:

$$V = H \perp V_0 \quad U_2 = H \perp (V_0 \cap U_2) \quad U_1 = H \cap (V_0 \cap U_1)$$

Da $\varphi|_H = \mathrm{id}$ ist, ist $(V_0 \cap U_1)\varphi = V_0 \cap U_2$, damit ist $\varphi|_{V_0 \cap U_1}$ eine bijektive Isometrie. Außerdem gilt wegen $H \neq \{0\}$: $\dim V_0 < \dim V$. Da V regulär ist, ist auch V_0 regulär (aus $V = H \perp V_0$). Nach Induktion existiert $\mu \in I_{f|_{V_0 \times V_0}}(V_0)$ mit $\mu|_{U_1 \cap V_0} = \varphi|_{U_1 \cap V_0}$.

Sei $k := \dim H$ und $\{v_1, ..., v_k\}$ Basis von H sowie $\{v_{k+1}, ..., v_n\}$ Basis von V_0. Dann ist $B = \{v_1, ..., v_n\}$ Basis von V.

Sei φ^* die lineare Fortsetzung der Abbildung

$$\varphi^* : v_i \mapsto \begin{cases} v_i & \text{falls} \quad i \leq k \\ v_i\mu & \text{falls} \quad i > k \end{cases}$$

Dann ist φ^* bijektiv, und $f(v_i, v_j) = f(v_i\varphi^*, v_j\varphi^*)$ für alle i, j. Also ist $\varphi^* \in I_f(V)$. Sei $u_1 \in U_1$. Dann ist $u_1 = h + v_0$ mit $h \in U$ und $v_0 \in U_1 \cap V_0$. Dann ist

$$u_1\varphi^* = h\varphi^* + v_0\varphi^* = h\mathrm{id} = v_0\mathrm{id} = (h + v_0)\varphi = u_1\varphi$$

(B) Nach (10.1.2) ist f symplektisch, oder es existiert $v_i \in U_1$ mit $f(v_1, v_1) \neq 0$.

(B_1) Nach (10.1.6) existiert eine hyperbolische Ebene H_1 in U_1. Definiere $H_1' := H_1\varphi$, seien $V_0 := H_1^\perp$ und $V_0' := H_1'^{\perp}$. Mit (9.4.4)(b) ist

$$V = H_1 \perp V_0 = H_1' \perp V_0'$$

und V_0 und V_0' sind reguläre symplektische Raume bezüglich $f|_{V_0 \times V_0}$ bzw. $f|_{V_0' \times V_0'}$ der Dimension $\dim V - 2$. Nach (10.1.9) existieren hyperbolische Ebenen $H_2, ..., H_r$ in V_0 und $H_2', ..., H_r'$ in V_0', so daß

$$V = H_1 \perp ... \perp H_r = H_1' \perp ... \perp H_r'$$

Seien v_i, w_i hyperbolische Paare von H_i bzw. v_i', w_i' von H_i', wobei $v_1' = v_1\varphi$ und $w_1' = w_1\varphi$. Sei ψ die lineare Fortsetzung der Abbildung $v_i \mapsto v_i'$ bzw. $w_i \mapsto w_i'$. Dann ist ψ eine bijektive Isometrie, d.h. $\psi \in I_f(V)$.

Definiere $\varphi' := \psi^{-1}\varphi|_{U_1\psi}$, dann ist φ' ein bijektiver Isomorphismus von $U\psi$ auf U_2.

Betrachte $\varphi'|_{H_1'}$, dies ist gleich der Identität, da $v_1'\psi' = v_i\psi\psi^{-1}\varphi = v_i\varphi$ (analog für w_1).

Nach Fall (A) existiert ein $\nu \in I_f(V)$ mit

$$\nu|_{U_1\psi} = \varphi' = \psi^{-1}\varphi|_{U_1\psi} \Rightarrow \psi\nu|_{U_1} = \varphi$$

Setze $\varphi^* = \psi\nu$.

(B_2) Sei $k := \dim H$, d.h. $k = 1$ oder $k = 2$. Mit (9.4.4) ist $V = H \perp H^\perp$. Nach (10.1.2) existieren in H Orthogonalbasen $\{v_1, v_k\}$ und $\{v_1', v_k'\}$ mit $v_1' = v_1\varphi$. Sei $v_{k+1}, ..., v_n$ Orthogonalbasis von $H^\perp$. Dann sind

$$B = \{v_1, v_k, v_{k+1}, ..., v_n\} \text{ und } B = \{v_1', v_k', v_{k+1}, ..., v_n\}$$

Orthogonalbasen von V.

- Sei $k = 1$. Dann ist die lineare Fortsetzung ψ der Abbildung $v_1 \mapsto v_1'$ und $v_i \mapsto v_i$ für $i > 1$ aus $I_f(V)$, denn $f(v_1, v_1) = f(v_1\varphi, v_1\varphi) = f(v_1', v_1')$.

  Es gilt: $H = \langle v_1 \rangle = \langle v_1\varphi \rangle \leq U_1\psi \cap U_2$, zudem ist H regulär. Setze $\varphi' := \psi^{-1}\varphi$, dann ist $\varphi'|_H = \mathrm{id}$. Nach Fall (A) existiert $\nu \in I_f(V)$ mit

  $$\nu|_{U_1\psi} = \varphi' = \psi^{-1}\varphi|_{U_1\psi} \Rightarrow \psi\nu|_{U_1} = \varphi$$

  Setze $\varphi^* = \psi\nu$.
- Sei $k = 2$. Dann ist

$$\begin{aligned}
\det G_B(f) &= f(v_1, v_1)f(v_2, v_2)\prod_{i\geq 3} f(v_i, v_i) \\
\det G_{B'}(f) &= f(v_1', v_1')f(v_2', v_2')\prod_{i\geq 3} f(v_i, v_i) \\
&= \underbrace{f(v_1\varphi, v_1\varphi)}_{f(v_1, v_1)} f(v_2', v_2')\prod_{i\geq 3} f(v_i, v_i)
\end{aligned}$$

Nach (9.2.3) ist für ein $h \in K^*$

$$\det G_B(f) = \det G_B(f) \cdot h \cdot h\alpha \Rightarrow f(v_2, v_2) = hh\alpha f(v_2', v_2')$$

Ersetze in der Basis B' das Element v_2' durch hv_2'. Dann ist

$$f(hv_2', hv_2') = hh\alpha f(v_2', v_2') = f(v_2, v_2)$$

Wir können auch annehmen: $f(v_2, v_2) = f(v_2', v_2')$. Sei ψ die lineare Fortsetzung der Abbildung $v_i \mapsto v_i'$ für $i = 1, 2$ und $v_i \mapsto v_i$ für $i \geq 3$. Dann ist $\psi \in I_f(V)$ und für $\varphi' = \psi^{-1}\varphi$ gilt. Dann ist $\psi^{-1}\varphi : U_1\psi \to U_2$ Isometrie und

$$\langle v_1\varphi \rangle = \langle v_1' \rangle = \langle v_1\psi \rangle \in U_1\psi \cap U_2$$

und $\langle v_1\varphi \rangle$ ist regulär, und $\varphi'|_{\langle v_1' \rangle} = \mathrm{id}$. Nach Fall (A) existiert wieder ν wie oben, setze $\varphi^* = \psi\nu$.

(B_3) Da H nicht regulär ist, ist $\dim H = 2$ (da $0 < \dim \operatorname{rad} V < \dim H$). Zudem existiert $0 \neq v_0 \in \operatorname{rad} H$ und

$$H = \langle v_0 \rangle \perp \langle v_1 \rangle = \langle v_0 \rangle \perp \langle v_1\varphi \rangle$$

Mit (10.1.6) existiert $w_0 \in \langle v_1 \rangle^\perp$ so, daß (v_0, w_0) ein hyperbolisches Paar ist. Sei

$$H_0 := \langle v_1, v_0, w_0 \rangle = \langle v_1 \rangle \perp \langle v_0, w_0 \rangle$$

Wir zeigen: H_0 ist regulär. Die Gramsche Matrix bezüglich $\{v_1, v_0, w_0\}$ ist

$$\det G_{\{v_1,v_0,w_0\}}(f) = \det \begin{pmatrix} f(v_1, v_1) & 0 & 0 \\ 0 & 0 & 1 \\ 0 & \pm 1 & 0 \end{pmatrix} = \pm f(v_1, v_1) \neq 0$$

Satz (10.1.6) angewandt auf H_0 besagt: Es existiert $w_0' \in \langle v_1\varphi \rangle^\perp \cap H_0$, so daß (v_0, w_0') ein hyperbolisches Paar ist. Dann ist $H_0 = \left\langle v_1^\perp \right\rangle \perp \langle v_0, w_0' \rangle$. Dann sind B_0 und B_0' Basen von H_0:

$$B_0 := \{v_1, v_0, w_0\} \text{ und } B_0' = \{v_1\varphi, v_0, w_0'\}$$

Es ist $V = H_0 \perp H_0^\perp$, ergänze daher die Basen B_0 und B_0' zu Basen B und B' durch Hinzufügen einer Basis B_1 von $H_0^\perp$.

Sei ψ die lineare Forsetzung der Abbildung

$$v_1 \mapsto v_1\varphi \qquad v_0 \mapsto v_0 \qquad w_0 \mapsto w_0' \qquad b \mapsto b \,\forall\, b \in B_1$$

Die Abbildung ψ ist bijektiv und Isometrie.

Es ist $v_1\psi = v_1\varphi \in U_1\psi \cap U_2$ und $\langle v_1\varphi\rangle$ ist regulär. Sei $\varphi' := \psi^{-1}\varphi|_{U_1\psi}$. Dann ist $(v_1\varphi)\varphi' = v_1\varphi$, also ist $\varphi'|_{\langle v_1\varphi\rangle} = \mathrm{id}$. Dann ist φ' bijektive Isometrie mit $\varphi' : U_1\psi \to U_2$. Nach Fall (A) existiert wieder ν wie oben.

(C) U_1 ist isotrop. Dann ist auch $U_2 = U_1\varphi$ isotrop. Sei $k := \dim U_1$. Sei $\{u_1, ..., u_k\}$ Basis von U_1 (dann ist $\{u'_1, ..., u'_k\}$ Basis von U_2, wobei $u'_i = u_i\varphi$). Mit (10.1.7) existiert eine Basis $v_1, ..., v_k, v'_1, ..., v'_k$ in V, so daß (u_i, v_i) und (u'_i, v'_i) hyperbolische Paare sind. Sei

$$W_1 := \langle u_1, v_1\rangle \perp ... \perp \langle u_k, v_k\rangle \text{ und } W_2 := \langle u'_1, v'_1\rangle \perp ... \perp \langle u'_k, v'_k\rangle$$

W_1 und W_2 sind reguläre Unterräume der Dimension $2k$, also nicht isotrop. Definiere

$$\varphi' : W_1 \to W_2 \text{ mit } \varphi' : u_i \mapsto u'_i (= u_i\varphi) \text{ und } \varphi' : v_i \mapsto v'_i$$

φ' ist bijektive Isometrie von W_1 auf W_2, W_1 ist nicht isotrop. Nach Fall B existiert $\varphi^* \in I_f(V)$ mit $\varphi^*|_{W_1} = \varphi'$. Es gilt also $\varphi^*|_{U_1} = \varphi'|_{U_1} = \varphi$.

11 Skalarprodukte

In diesem Kapitel ist V ein Vektorraum Über K und $K = \mathbb{R}$ oder $K = \mathbb{C}$.

11.1 Grundlagen

11.1.1 Definition

Eine α-Bilinearform auf V heißt Skalarprodukt auf V, falls für alle $v \in V$ gilt:

1. $f(v, v) \in \mathbb{R}_{\geq 0}$ (*positiv definit*)
2. $f(v, v) = 0 \Leftrightarrow v = 0$
3.
   - falls $K = \mathbb{R}$: $\alpha = \mathrm{id}$ und f orthogonal
   - falls $K = \mathbb{C}$: α ist die Komplexkonjugation, und f ist unitär

Beispiel: V der Vektorraum der komplexwertigen stetigen Funktionen auf $[0, 1]$. Definiere

$$f(h, g) = \int_0^1 h(x)\overline{g(x)}\, dx \;\forall\, g, h \in V$$

Eigenschaften:

1. $\int_0^1 h(x)\overline{h(x)}\, dx = \int_0^1 |f(x)|^2\, dx \geq 0$
2. $\int_0^1 |f(x)|^2\, dx = 0 \Leftrightarrow h = 0$
3. f ist unitär

11.1.2 Orthogonaliesierungsverfahren nach E. Schmidt

Sei V Vektorraum mit Skalarprodukt f, sei $n := \dim V$ und $\{b_1, ..., b_n\}$ Basis von V. Sei $b_1^* = b_1$. Rekursives Verfahren: Sei $r \in \mathbb{N}$ mit $1 \leq r < n$. Seien $b_1^*, ..., b_r^*$ so definiert, daß sie orthogonal sind und $W_r := \langle b_1, ..., b_r\rangle = \langle b_1^*, ..., b_r^*\rangle$. Beachte: $b_{r+1} \notin W_r$, d.h. $b_1^*, ..., b_r^*, b_{r+1} + v$ sind linear unabhängig für alle $v \in W_r$. Sei $v := \sum_{j=1}^r k_i b_i^*$

$$\begin{aligned}
f(b_i^*, b_{r+1} + v) &= f(b_i^*, b_{r+1}) + f(b_i^*, v) \\
&= f(b_i^*, b_{r+1}) + \sum_{j=1}^r \overline{k_j} f(b_i^*, b_j^*) \\
&= f(b_i^*, b_{r+1}) + \overline{k_i} f(b_i^*, b_i^*)
\end{aligned}$$

Setze

$$-\overline{k_i} = f(b_i^*, b_{r+1}) f(b_i^*, b_i^*)^{-1} \; \forall\, i = 1, ..., r \text{ und } b_{r+1}^* := b_{r+1} + v$$

Dann ist $\{b_1^*, ..., b_{r+1}^*\}$ Orthogonalbasis. Rekursiv angewendet ergibt sich $\{b_1^*, ..., b_n^*\}$ als Orthogonalbasis von V. Für $b_i^{**} := f(b_i^*, b_i^*)^{-\frac{1}{2}} b_i^*$ ist $b_1^{**}, ..., b_n^{**}$ eine Orthonormalbasis von V.[62]

11.1.3 Schwarzsche Ungleichung

Seien $v, w \in V$. Dann gilt:

$$|f(v,w)|^2 \leq f(v,v) f(w,w)$$

Außerdem gilt die Gleichheit genau dann, wenn v und w linear abhängig sind.
Beweis: Für $v = 0 = w$ gilt die (Un)Gleichung. Sei nun O.B.d.A. $w \neq 0$, sei $a := -f(v,w) f(w,w)^{-1}$. Dann gilt

$$\begin{aligned}
0 \leq f(v+aw, v+aw) &= f(v,v) + \overline{a} f(v,w) + a f(w,v) + a\overline{a} f(w,w) \\
&= f(v,v) + \overline{a} f(v,w) + a \overline{f(v,w)} + a\overline{a} f(w,w) \\
\overset{\text{Multiplikation}}{\underset{\text{mit } f(w,w)}{\Longrightarrow}} 0 &\leq f(w,w) f(v,v) \\
&\quad -\overline{f(v,w)} f(w,w)^{-1} f(v,w) f(w,w) \\
&\quad -f(v,w) f(w,w)^{-1} \overline{f(v,w)} f(w,w) \\
&\quad +f(v,w)\overline{f(v,w)} f(w,w)^{-1} f(w,w)^{-1} f(w,w) f(w,w) \\
&= f(v,v) f(w,w) - f(v,w)\overline{f(v,w)} \\
&= f(v,v) f(w,w) - |f(v,w)|^2
\end{aligned}$$

Sei $w = kv$. Dann folgt:

$$|f(v,kv)|^2 = \left|\overline{k}\right|^2 |f(v,v)|^2 \text{ und } |k|^2 f(v,v)^2 = f(v,v) f(kv,kv)$$

11.1.4 (induzierte) Normen

Definition: Sei $\|\cdot\|$ eine Abbildung von V in $\mathbb{R}$, so daß für alle $v, w \in V$, $k \in K$ gilt:

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

[62] „Wir haben noch fünf Minuten, vielleicht gebe ich Ihnen dann die fünf Minuten, um sich warmzulaufen, sie werden's brauchen!“

2. $\|kv\| = |k| \|v\| \ \forall\, k \in K$

3. $\|v + w\| \leq \|v\| + \|w\|$ (Dreiecksungleichung)

Dann heißt $\|\cdot\|$ *Norm* auf V.

Durch

$$\|\cdot\| : V \to \mathbb{R} \text{ mit } \|v\| := \sqrt{f(v, v)}$$

wird die von f auf V *induzierte Norm* definiert. BEWEIS:

3. Betrachte nur Quadrate[63]:

$$\begin{aligned}
f(v, w) + \overline{f(v, w)} &= 2\Re(f(v, w)) \\
&\leq |f(v, w)| \\
&\overset{(11.1.3)}{\leq} 2 \|v\| \|w\| \\
\|v + w\|^2 &= f(v + w, v + w) \\
&= f(v, v) + f(w, w) + f(v, w) + \overline{f(v, w)} \\
&\leq \|v\|^2 + \|w\|^2 + 2 \|v\| \|w\| \\
&= (\|v\| + \|w\|)^2
\end{aligned}$$

11.2 Normierte Vektorräume

Ein Vektorraum V heißt normiert, falls auf V eine Norm existiert.

BEISPIELE:

1. Sei $n := \dim V$, $\{b_1, ..., b_n\}$ Basis von V. Dann ist folgendes die 1-Norm:

$$\left\| \sum_{i=1}^{n} k_i b_i \right\| := \sum_{i=1}^{n} |k_i|$$

2. Sei V der Vektorraum der reellwertigen stetigen Funktionen auf $[0, 1]$, $f \in V$. Dann sind folgende Abbildungen Normen:

$$\|f\| := \max\{\, |f(x)| \mid x \in [0, 1]\} \text{ und } \|f\| = \int_0^1 |f(x)|\, dx$$

[63] „... mit der Wurzel aus der Schwarzschen Ungleichung folgt ...“

11.2.1 Stetigkeit linearer Abbildungen mit Norm

Sei V endlichdimensional, $n := \dim V$, $\{b_1, ..., b_n\}$ Basis. Sei $\|\cdot\|$ die 1-Norm auf V. Sei W ein weiterer normierter Vektorraum und $\varphi \in \mathrm{Hom}(V, W)$. Dann ist die folgende Abbildung stetig:

$$\psi : V \to \mathbb{R} \text{ mit } \psi : v \mapsto \|v\varphi\|$$

Beweis: Sei $M := \max\{\|b_i\varphi\| \mid i = 1, ..., n\}$. Sei $v = \sum_{i=1}^{n} k_i b_i \in V$. Dann ist

$$\|v\varphi\| = \left\|\sum_{i=1}^{n} k_i b_i \varphi\right\| \leq \sum_{i=1}^{n} |k_i| \|b_i\varphi\| \leq M \cdot \sum_{i=1}^{n} |k_i| = M \|v\|$$

Sei $\varepsilon > 0$. Wähle $\delta = \frac{\varepsilon}{M+1}$. Seien nun $v, v' \in V$ mit $\|v - v'\| < \delta$. Dann folgt:

$$\|v\varphi - v'\varphi\| = \|(v - v')\varphi\| \leq M \|v - v'\| \leq \frac{M}{M+1}\varepsilon < \varepsilon$$

11.2.2 Äquivalente Normen

Sei V endlichdimensionaler $\mathbb{R}$-Raum[64] und seien $\|\cdot\|_1$ und $\|\cdot\|_2$ Normen auf V. Dann existiere $c_1, c_2 \in \mathbb{R}_{>0}$ mit

$$c_1 \|v\|_1 \leq \|v\|_2 \leq c_2 \|v\|_1 \ \forall\, v \in V$$

Beweis: Sei $n := \dim V$ und $\{b_1, ..., b_n\}$ Basis von V. Sei $V' = \mathbb{R}^n$ und $\|\|_0$ die 1-Norm bezüglich der kanonischen Basis von V'. Sei

$$\varphi : V' \to V \text{ mit } \varphi : (k_1, ..., k_n) \mapsto \sum_{i=1}^{n} k_i b_i$$

Dann ist $\varphi \in \mathrm{Hom}(V', V)$. Sei $\|\cdot\|$ eine Norm auf V. Die Abbildung $\psi : (k_1, ..., k_n) \mapsto \|(k_1, ..., k_n)\varphi\|$ ist stetig nach (11.2.1). Sei

$$B := \{(k_1, ..., k_n) \in \mathbb{R} \mid \|(k_1, ..., k_n)\|_0 = 1\}$$

B ist kompakt. ψ hat auf B ein Minimum. Sei

$$m_{\|\cdot\|} = \min\{\|(k_1, ..., k_n)\varphi\| \mid (k_1, ..., k_n) \in B\}$$

Für $0 \neq w \in V'$ ist $\|w\|_0^{-1} w \in B$. Damit ist

$$\|w\|_0^{-1} \|w\varphi\| = \left\|\|w\|_0^{-1} w\varphi\right\| \geq m_{\|\cdot\|}$$

[64] siehe genauer Stellmachers Script

Dann folgt mit $M_{\|\cdot\|} = \max\{\|b_i\| \mid i = 1, ..., n\}$:

$$m_{\|\cdot\|}\,\|w_0\| \leq \|w\varphi\| \leq M_{\|\cdot\|}\,\|w\|_0$$

Dann ist

$$\frac{1}{M_{\|\cdot\|}}\,\|w\varphi\| \leq \|w\|_0 \leq \frac{1}{m_{\|\cdot\|}}\,\|w\varphi\|$$

Für verschiedene Normen folgt mit $\frac{1}{M_{\|\cdot\|_1}}\,\|w\varphi\| \leq \|w\|_0 \leq \frac{1}{m_{\|\cdot\|_2}}\,\|w\varphi\|$, daß:

$$\frac{m_{\|\cdot\|_2}}{M_{\|\cdot\|_1}}\,\|w\varphi\|_1 \leq \|w\varphi\|_2 \leq \frac{m_{\|\cdot\|_1}}{M_{\|\cdot\|_2}}$$

11.2.3 Stetigkeit linearer Abbildungen

Seien V und W endlichdimensionale normierte Vektorräume. Sei $\varphi \in \mathrm{Hom}(V, W)$. Dann ist φ stetig.

Beweis: Sei $n := \dim V$, Basis $\{b_1, ..., b_n\}$ von V und $M := \max\{\|b_i\varphi\| \mid i = 1, ..., n\}$. Sei $\|\cdot\|_1$ die 1-Norm. Mit (11.2.2) existiert $c \in \mathbb{R}_{>0}$ mit $\|\cdot\|_1 \leq c\,\|\cdot\|$. Sei $\varepsilon > 0$. Wähle $\delta := \frac{\varepsilon}{c(M+1)}$. Seien $v, v' \in V$ mit $\|v - v'\| < \delta$. Seien $k_i, k_i' \in K$ mit $v = \sum_{i=1}^n k_i b_i$ und $v' = \sum_{i=1}^n k_i' b_i$. Dann ist

$$\begin{aligned}
\|v\varphi - v'\varphi\| &= \left\|\sum_{i=1}^n (k_i - k_i')b\varphi\right\| \\
&\leq \sum_{i=1}^n |k_i - k_i'|\,\|b_i\varphi\| \leq M \cdot \sum_{i=1}^n |k_i - k_i'| \\
&= M\,\|v - v'\|_1 \leq Mc\,\|v - v'\| < Mc\delta = \frac{M}{M+1}\varepsilon < \varepsilon
\end{aligned}$$

11.3 Adjungierte Abbildungen

In diesem Abschnitt sind V und W endlichdimensionale Vektorräume über K ($= \mathbb{R}$ oder $= \mathbb{C}$) mit Skalarprodukt f bzw. g. V^* ist der Dualraum von V.

11.3.1

Sei $h \in V^*$. Dann existiert genau ein $w \in V$ mit $vh = f(v, w)$ für alle $v \in V$.

Beweis: Sei $w \in V$. Nach (9.3.5): $vh_w := f(v, w)$ definert ein Element aus V^*. Sei B Basis von V. Sei $B' = \{h_b \mid b \in B\} \subseteq V^*$, wir zeigen: B' ist Basis von V^*.

Nach (9.3.1) gilt $\dim V = \dim V^*$, es genügt zu zeigen: Alle h_b sind linear unabhängig. Seien $k_b \in K$ mit $\sum_{b\ inB} k_b h_b = 0$. Dann ist für alle $v \in V$:

$$\begin{aligned} 0 &= v \sum_B k_b h_b \\ &= \sum_B k_b v h_b \\ &= \sum_B k_b f(v, b) \\ &= f\left(v, \sum_B \overline{k_b} b\right) \end{aligned}$$

Da f regulär ist, ist $\sum_B \overline{k_b} b = 0$, da B Basis ist, also sind alle $\overline{k_b} = 0 = k_b$. Damit sind alle h_b linear unabhängig. Schreibe h als Linearkombination von B', dann existieren $l_b \in K$ mit $h = \sum_B l_b h_b$. Setze dann

$$w := \sum_{b \in B} \overline{l_b} b$$

Dann ist für $v \in V$:

$$\begin{aligned} vh &= \sum_{b \in B} l_b v h_b \\ &= \sum_{b \in B} l_b f(v, b) \\ &= f\left(v, \sum_{b \in B} \overline{l_b} b\right) = f(v, w) \end{aligned}$$

Die Eindeutigkeit von w folgt aus der Regularität von V.

11.3.2 Existenz der adjungierten Abbildung

Sei $\varphi \in \mathrm{Hom}(V, W)$. Dann existiert genau ein $\varphi^{\mathrm{ad}} \in \mathrm{Hom}(W, V)$ mit

$$g(v\varphi, w) = f(v, w\varphi^{\mathrm{ad}})\ \forall\ v \in V, w \in W$$

Nenne die Abbildung φ^{ad} die zu φ *adjungierte* Abbildung. Beweis: Aus der Regularität von V folgt die Eindeutigkeit, es bleibt die Existenz zu zeigen. Sei $w \in W$, folgendes ist dann eine lineare Abbildung aus V^*:

$$h'_w : V \to K \text{ mit } vh'_w := g(v\varphi, w)$$

Mit (11.3.1): Es existiert $v_w \in V$ mit $vh'_w = f(v, v_w) \; \forall \, v \in V$. Definiere nun

$$\varrho : W \to V \text{ mit } \varrho : w \mapsto v_w$$

Es gilt für $k \in K$:

$$\begin{aligned} f(v, (kw)\varrho) &= f(v, v_{kw}) = vh'_{kw} = g(v\varphi, kw) \\ &= \overline{k}g(v\varphi, w) = \overline{k}vh'_w = \overline{k}f(v, v_w) = f(v, kv_w) \\ &= f(v, k(w\varrho)) \end{aligned}$$

Damit für alle $v \in V$: $f(v, (kw)\varrho - k(w\varrho)) = 0$, mit der Regularität: $(kw)\varrho = k(w\varrho)$. Ähnlich zeigt man, daß ϱ linear bezüglich der Addition ist, damit ist ϱ eine lineare Abbildung.

Definiere nun $\varphi^{\text{ad}} := \varrho$, dann ist $g(v\varphi, w) = f(v, w\varphi^{\text{ad}})$.

Beispiel: Zur Erinnerung: Sei $B := \{e_1, ..., e_n\}$ Orthonormalbasis von V; $w = \sum_{i=1}^n k_i e_i$ Linearkombination. Dann ist

$$f(w, e_i) = f\left(\sum_{j=1}^n k_j e_j, e_i\right) = \sum_{j=1}^n k_j f(e_j, e_i) = k_j$$

Für alle $v \in V$ gilt also:

$$v = f(v, e_1)e_1 + ... + f(v, e_n)e_n$$

Sei $V = \mathbb{C}^2$ und

$$\varphi \text{ mit } M(\varphi, B, B) = \begin{pmatrix} i & 0 \\ 2 & 1 \end{pmatrix}$$

Was ist $M(\varphi^{\text{ad}}, B, B)$?

$$M(\varphi^{\text{ad}}, B, B) = \begin{pmatrix} f(e_1\varphi^{\text{ad}}, e_1) & f(e_1\varphi^{\text{ad}}, e_2) \\ f(e_2\varphi^{\text{ad}}, e_1) & f(e_2\varphi^{\text{ad}}, e_2) \end{pmatrix} = \begin{pmatrix} -i & 2 \\ 0 & 1 \end{pmatrix}$$

da

$$\begin{aligned} f(e_1\varphi^{\text{ad}}, e_1) &= \overline{f(e_1, e_1\varphi^{\text{ad}})} = \overline{f(e_1\varphi, e_1)} = \overline{i} = -i \\ f(e_1\varphi^{\text{ad}}, e_2) &= \overline{f(e_1, e_2\varphi^{\text{ad}})} = \overline{f(e_2\varphi, e_1)} = \overline{2} = 2 \\ f(e_2\varphi^{\text{ad}}, e_1) &= 0 \\ f(e_2\varphi^{\text{ad}}, e_2) &= 1 \end{aligned}$$

11.3.3 Eigenschaften der adjungierten Abbildung

Seien $\varphi, \psi \in \mathrm{Hom}(V, W)$ und $\mu \in \mathrm{Hom}(W, T)$, wobei T ein weiterer endlich-dimensionaler Vektorraum und Skalarprodukt h ist. Dann gilt:

1. $(\varphi + \psi)^{\mathrm{ad}} = \varphi^{\mathrm{ad}} + \psi^{\mathrm{ad}}$
2. $(k\varphi)^{\mathrm{ad}} = \overline{k}\varphi^{\mathrm{ad}}$
3. $(\varphi\mu)^{\mathrm{ad}} = \mu^{\mathrm{ad}}\varphi^{\mathrm{ad}}$
4. $(\varphi^{\mathrm{ad}})^{\mathrm{ad}} = \varphi$
5. $\mathrm{Kern}\,\varphi = (\mathrm{Bild}\,\varphi^{\mathrm{ad}})^{\perp}$, φ injektiv genau dann, wenn φ^{ad} surjektiv
6. $\mathrm{Bild}\,\varphi^{\mathrm{ad}} = (\mathrm{Kern}\,\varphi)^{\perp}$, φ surjektiv genau dann, wenn φ^{ad} injektiv
7. Ist φ bijektiv, so ist $(\varphi^{-1})^{\mathrm{ad}} = (\varphi^{\mathrm{ad}})^{-1}$.

Beweis:

1.-4. einfaches Nachrechnen

5. Sei $v \in \mathrm{Kern}\,\varphi$, dann ist $0 = g(v\varphi, w) = f(v, w\varphi^{\mathrm{ad}})$, damit ist v senkrecht auf $\mathrm{Bild}\,\varphi^{\mathrm{ad}}$. Mit $v \in (\mathrm{Bild}\,\varphi^{\mathrm{ad}})^{\perp}$, $w \in W$ ist $f(v, w\varphi^{\mathrm{ad}}) = 0 = g(v\varphi, w)$, damit ist $v\varphi \in \mathrm{rad}\,W$ also $v \in \mathrm{Kern}\,\varphi$.

   Zusatz folgt wegen $V = U \perp U^{\perp}$ für alle $U \leq V$ angewandt auf $U = \mathrm{Bild}\,\varphi^{\mathrm{ad}}$.

6. $(\mathrm{Kern}\,\varphi)^{\perp} = (\mathrm{Bild}\,\varphi^{\mathrm{ad}})^{\perp\perp} \overset{(9.4.4)}{=} \mathrm{Bild}\,\varphi^{\mathrm{ad}}$

7. Folgt aus 3. wegen $\varphi^{\mathrm{ad}}(\varphi^{-1})^{\mathrm{ad}} = (\varphi\varphi^{-1})^{\mathrm{ad}} = \mathrm{id}_V^{\mathrm{ad}} = \mathrm{id}_V$.

11.3.4 adjungierte Matrix

Seien $B = \{v_1, ..., v_n\}$ und $B' = \{v'_1, ..., v'_m\}$ Basen von V bzw. W und $\varphi \in \mathrm{Hom}(V, W)$. Dann gilt:

$$M(\varphi, B, B')G_{B'}(g) = G_B(f)\overline{M(\varphi^{\mathrm{ad}}, B', B)}^t$$

Sind B und B' Orthogonalbasen, so gilt:

$$M(\varphi, B, B') = \overline{M(\varphi^{\mathrm{ad}}, B', B)}^t$$

Beweis: Sei $n := \dim V$ und $m := \dim W$. Seien

$$\begin{array}{ll} (a_{ij})_{n\times m} := M(\varphi, B, B') & (f_{ij})_{n\times n} := G_B(f) \\ (a'_{ij})_{m\times n} := M(\varphi^{\text{ad}}, B', B) & (g_{ij})_{m\times m} := G_{B'}(g) \end{array}$$

Dann ist

$$\begin{aligned} M(\varphi, B, B') \cdot G_{B'}(g) &= \left(\sum_{k=1}^{m} a_{ik} g_{kj}\right)_{n\times m} \\ \sum_{k=1}^{m} a_{ik} g_{kj} &= \sum_{k=1}^{m} a_{ik} g(v'_k, v'_j) \\ &= g\left(\sum_{k=1}^{m} a_{ik} v'_k, v'_j\right) \\ &= g(v_i\varphi, v'_j) \\ &= f(v_i, v'_j\varphi^{\text{ad}}) \\ &= f\left(v_i, \sum_{l=1}^{n} a'_{jl} v_l\right) \\ &= \sum_{l=1}^{n} \overline{a'_{jl}} f\left(v_i, v_l\right) \\ &= \sum_{l=1}^{n} f_{il} \overline{a'_{jl}} \\ G_B(f) \cdot \overline{M(\varphi^{\text{ad}}, B', B)}^t &= \left(\sum_{l=1}^{n} f_{il} \overline{a'_{jl}}\right)_{n\times m} \end{aligned}$$

Bei Orthonormalbasen sind die Gram'schen Matrizen jeweils gleich der entsprechenden Einheitsmatrix, damit folgt die Behauptung.

Bezeichnung: Sei $A \in \mathcal{M}_{n\times m}(K)$. Dann heißt $\overline{A}^t \in \mathcal{M}_{m\times n}(K)$ die zu A *adjungierte Matrix*

11.3.5 Determinante, Eigenwerte

Sei $\varphi \in \text{Hom}(V, V)$. Dann gilt:

1. $\det \varphi = \overline{\det \varphi^{\text{ad}}}$
2. $a \in K$ ist genau dann Eigenwert von φ, wenn $\overline{a}$ Eigenwert von φ^{ad} ist.

Beweis:

1. Folgt aus (11.3.4) mit Orthonormalbasis.

2. „⇒“ Sei a Eigenwert von φ zum Eigenvektor w. Dann ist für alle $v \in V$:

$$f(w, v\varphi^{\mathrm{ad}}) = f(w\varphi, v) = f(aw, v) = af(w, v) = f(w, \overline{a}v)$$

Daraus folgt für alle v:

$$f(w, v\varphi^{\mathrm{ad}} - \overline{a}v) = 0 = f(w, v(\varphi^{\mathrm{ad}} - \overline{a}\mathrm{id}))$$

Damit steht w senkrecht auf $V(\varphi^{\mathrm{ad}} - \overline{a}\mathrm{id})$. Da w Eigenvektor ist, ist $w \neq 0$. V ist regulär, damit ist $V(\varphi^{\mathrm{ad}} - \overline{a}\mathrm{id}) \neq V$ Somit ist die Abbildung $(\varphi^{\mathrm{ad}} - \overline{a}\mathrm{id})$ nicht surjektiv. Mit Dimensionsformel ist

$$\mathrm{Kern}(\varphi^{\mathrm{ad}} - \overline{a}\mathrm{id}) \neq \{0\}$$

Sei $0 \neq v \in \mathrm{Kern}(\varphi^{\mathrm{ad}} - \overline{a}\mathrm{id})$, dann ist v Eigenvektor zum Eigenwert $\overline{a}$.

„⇐“ Sei $\overline{a}$ Eigenwert von φ^{ad}. Wie eben gezeigt, ist $a = \overline{\overline{a}}$ Eigenwert zu $(\varphi^{\mathrm{ad}})^{\mathrm{ad}} \overset{(11.3.3)}{=} \varphi$.

11.3.6 Isomorphismus lin. Abbildungen/Bilinearformen

Sei $B_\alpha(V)$ die Menge der α-Bilinearformen und α die Komplexkonjugation. Die folgende Abbildung ist ein Vektorraum-Isomorphismus:

$$\psi : \mathrm{Hom}(V, V) \to B_\alpha(V) \text{ mit } \varphi \mapsto f(v, w\varphi^{\mathrm{ad}}) \ \forall\, v, w \in V$$

Beweis: Sei $f_\varphi := \varphi\psi$. Einfach nachzurechnen: $f_\varphi \in B_\alpha(V)$. Linearität von ψ:

- zu zeigen: $f_{k\varphi} = kf_\varphi$

$$\begin{aligned} f_{k\varphi}(v, w) &= f(v, w(k\varphi)^{\mathrm{ad}}) \overset{(11.3.3)}{=} f(v, \overline{k}w\varphi^{\mathrm{ad}}) \\ &= kf(v, w\varphi^{\mathrm{ad}}) = kf_\varphi(v, w) \end{aligned}$$

- analog: $f_{\varphi+\varphi'} = f_\varphi + f_{\varphi'}$

Sei $f_\varphi(v, w) = 0 \ \forall\, v, w \in V$. Zu zeigen. $\varphi = 0$, d.h. ψ ist injektiv.

$$\begin{aligned} 0 &= f_\varphi(v, w) = f(v, w\varphi^{\mathrm{ad}}) = f(v\varphi, w) \ \forall\, v, w \\ \Rightarrow 0 &= v\varphi \ \forall\, v \in V \\ \Rightarrow 0 &= \varphi \end{aligned}$$

Nach (4.1.2) und (9.2.4) ist

$$\dim \mathrm{Hom}(V, V) = \dim \mathcal{M}_{n\times n}(K) = \dim B_\alpha(V)$$

11.4 Normale Abbildungen

11.4.1 Definitionen

In diesem Abschnitt ist V endlichdimensionaler Vektorraum über $\mathbb{R}$ oder $\mathbb{C}$ mit Skalarprodukt f. Sei $\varphi \in \mathrm{Hom}(V, V)$. Dann heißt φ

- *normal*, falls $\varphi\varphi^{\mathrm{ad}} = \varphi^{\mathrm{ad}}\varphi$
- *selbstadjungiert* (oder *hermitesch*), falls $\varphi = \varphi^{\mathrm{ad}}$
- *unitär*, falls φ bijektiv und $\varphi^{-1} = \varphi^{\mathrm{ad}}$

Es gilt:

- Die unitären Abbildungen sind genau die f-Isometrien auf V, da

$$f(v, w\varphi\varphi^{\mathrm{ad}}) = f(v\varphi, w\varphi) = f(v, w)\ \forall\, v, w \Rightarrow w = w\varphi\varphi^{\mathrm{ad}}\ \forall\, w \in V$$

- $H_f(V)$ ist der $\mathbb{R}$-Vektorraum der selbstadjungierten Abbildungen aus $\mathrm{Hom}(V, V)$, aber kein Vektorraum über $\mathbb{C}$. Mit $k \in \mathbb{C}, \varphi \in H_f(\mathbb{C})$ ist $(k\varphi)^{\mathrm{ad}} \overset{(11.3.3)}{=} \overline{k}\varphi^{\mathrm{ad}} = \overline{k}\varphi$

Matrizen heißen normal, selbstadjungiert bzw. unitär, wenn sie bezüglich einer Orthonormalbasis eine normale, selbstadjungierte bzw. unitäre Abbildung beschreiben.

11.4.2 Kriterium für normale Abbildungen

Sei $\varphi \in \mathrm{Hom}(V, V)$. Dann ist φ normal genau dann, wenn

$$f(v\varphi, w\varphi) = f(v\varphi^{\mathrm{ad}}, w\varphi^{\mathrm{ad}})\ \forall\, v, w \in V$$

Beweis:

„⇒“

$$f(v\varphi, w\varphi) = f(v, w\varphi\varphi^{\mathrm{ad}}) = f(v, w\varphi^{\mathrm{ad}}\varphi) = f(v\varphi^{\mathrm{ad}}, w\varphi^{\mathrm{ad}})$$

„⇐“ Sei $v, w \in V$. Dann gilt:

$$\begin{aligned} f(v(\varphi\varphi^{\mathrm{ad}} - \varphi^{\mathrm{ad}}\varphi), w) &= f(v\varphi\varphi^{\mathrm{ad}}, w) - f(v\varphi^{\mathrm{ad}}\varphi, w) \\ &= f(v\varphi, w\varphi) - f(v\varphi^{\mathrm{ad}}, w\varphi^{\mathrm{ad}}) = 0 \end{aligned}$$

Wegen der Regularität ist $v(\varphi\varphi^{\mathrm{ad}} - \varphi^{\mathrm{ad}}\varphi) = 0$, also $\varphi\varphi^{\mathrm{ad}} = \varphi^{\mathrm{ad}}\varphi$.

11.4.3 normale, selbstadjungierte, unitäre Matrizen

Sei $n := \dim V$, $\varphi \in \mathrm{Hom}(V, V)$, B Orthogonalbasis von V, $A = (a_{ij}) = M(\varphi, B, B)$

1. φ ist normal genau dann, wenn A normal ist, genau dann, wenn

$$\sum_{k=1}^{n} a_{ik}\overline{a_{jk}} = \sum_{k=1}^{n} \overline{a_{ik}}a_{jk} \;\forall\; i, j$$

2. φ ist selbstadjungiert genau dann, wenn A selbstadjungiert ist, genau dann, wenn

$$a_{ij} = \overline{a_{ji}} \;\forall\; i, j$$

3. φ ist unitär genau dann, wenn A unitär ist, genau dann, wenn

$$\sum_{k=1}^{n} a_{ik}\overline{a_{jk}} = \delta_{ij} \;\forall\; i, j$$

11.4.4 Räume der orthogonalen/unitären Bilinearformen

Sei φ der in (11.3.6) definierte Vektorraum-Isomorphismus von $\mathrm{Hom}(V, V)$ in $B_\alpha(V)$.

- $K = \mathbb{R}$: $H_f(V)\psi$ ist der Unterraum der orthogonalen Bilinearformen.
- $K = \mathbb{C}$: $H_f(V)\psi$ ist der Unterraum der unitären Bilinearformen.

11.4.5 Eigenwerte der adjungierten Abbildung

Sei $\varphi \in \mathrm{Hom}(V, V)$ eine normale Abbildung, v ein Eigenvektor von φ zum Eigenwert k. Dann ist v Eignevektor von φ^{ad} zum Eigenwert $\overline{k}$. Insbesondere sind die Eigenwerte von selbstadjungierten Abbildungen reell.

Beweis: Es ist

$$\begin{aligned}
& f(v(\varphi^{\mathrm{ad}} - \overline{k} \cdot \mathrm{id}), v(\varphi^{\mathrm{ad}} - \overline{k} \cdot \mathrm{id})) \\
= \;& f(v\varphi^{\mathrm{ad}} - \overline{k}v, v\varphi^{\mathrm{ad}} - \overline{k}v) \\
= \;& f(v\varphi^{\mathrm{ad}}, v\varphi^{\mathrm{ad}}) - kf(v\varphi^{\mathrm{ad}}, v) - \overline{k}f(v, v\varphi^{\mathrm{ad}}) + k^2 f(v, v) \\
\overset{(11.4.2)}{=} \;& f(v\varphi, v\varphi) - kf(v, v\varphi) - \overline{k}f(v\varphi, v) + k\overline{k}f(v, v) \\
= \;& k\overline{k}f(v, v) - k\overline{k}f(v, v) - k\overline{k}f(v, v) + k\overline{k}f(v, v) \\
= \;& 0 \Rightarrow v\varphi^{\mathrm{ad}} = \overline{k}v
\end{aligned}$$

11.4.6 invariante Unterräume

Sei $K = \mathbb{C}$ und φ eine normale Abbildung aus $\mathrm{Hom}(V, V)$. Sei U ein φ-invarianter Unterraum (d.h. $U\varphi \subseteq U$). Dann ist U auch φ^{ad}-invariant und es gilt: $U^\perp\varphi \subseteq U^\perp$.

Beweis: Annahme: $U\varphi^{\mathrm{ad}} \subseteq U$. Sei $v \in U^\perp$, $u \in U$. Dann ist

$$f(u, v\varphi) = f(u\varphi^{\mathrm{ad}}, v) = 0 \Rightarrow U^\perp\varphi \leq U^\perp$$

Es ist also nur noch der erste Teil zu zeigen. Beweis per Induktion nach $\dim U$.

- Induktionsverankerung: Für $\dim U = 0$ ist nichts zu zeigen, bei $U = \langle u \rangle$ ist u Eigenvektor von φ und damit nach (11.4.5) auch von φ^{ad}.
- Induktionsannahme: Die Behauptung gelte für alle φ-invarianten Unterräume kleinerer Dimension.
- Induktionsschritt: Wende (8.4.1) an: Es existiert eine Basis $B = \{u_1, ..., u_m\}$ mit $M(\varphi|_U, B, B)$ ist in Jordan-Normalform. Für $U_0 := \langle u_2, ..., u_m \rangle$ ist $U_0\varphi \subseteq U_0$. Nach Induktion: $U_0\varphi^{\mathrm{ad}} \subseteq U_0$, also auch $U_0^\perp\varphi \subseteq U_0^\perp$. Mit (9.4.3) und (9.4.4) gilt:

  $$V = U_0 \perp U_0^\perp \text{ mit } \dim U_0^\perp = \dim V - \dim U_0$$

  Mit Dimensionssatz: $\dim U \cap U_0^\perp = 1$, zudem $U = U_0 \perp (U \cap U_0)^\perp$, außerdem

  $$(U \cap U_0^\perp)\varphi = \underbrace{U\varphi}_{\leq U} \cap \underbrace{U_0^\perp\varphi}_{U_0^\perp} = U \cap U_0^\perp$$

  Nach Induktion:

  $$\begin{array}{rcl} (U \cap U_0^\perp)\varphi^{\mathrm{ad}} & \subseteq & U \cap U_0^\perp \\ U\varphi^{\mathrm{ad}} & = & (U_0 + (U \cap U_0^\perp))\varphi^{\mathrm{ad}} \\ & = & U_0\varphi^{\mathrm{ad}} + (U \cap U_0^\perp)\varphi^{\mathrm{ad}} \\ & \leq & U_0 + (U \cap U_0^\perp) = U \end{array}$$

11.4.7 Orthogonalbasis aus Eigenvektoren

Sei $\varphi \in H_f(V)$. Dann existiert eine Orthonormalbasis von V, die aus Eigenvektoren von φ besteht. Insbesondere ist φ diagonalisierbar.

Beweis: Sei B eine Orthonormalbasis von V und $A = M(\varphi, B, B)$. Nach (11.4.3) gilt: $A = \overline{A}^t$. Wir betrachten $\mathbb{C}^n$ mit dem natürlichen Skalarprodukt und der natürlichen Basis B^*. Wähle $\varphi^* \in \mathrm{Hom}(\mathbb{C}^n, \mathbb{C}^n)$ so, daß

$M(\varphi^*, B^*, B^*) = A$ ist.

Nach (11.4.3) ist φ^* selbstadjungiert. $\mathbb{C}$ ist algebraisch abgeschlossen, also besitzt φ^* einen Eigenwert k. Mit (11.4.5) gilt: k ist reell. Also ist k auch ein Eigenwert von φ. Sei v ein Eigenvektor zu k in V.

Es ist $f(v,v) > 0$, nach $v_1 = \sqrt{f(v,v)}^{-1}$ können wir annehmen: $f(v_1, v_1) = 1$. Nach (11.4.6) ist $\langle v\rangle^{\perp}\varphi \subseteq \langle v\rangle^{\perp} =: U$. Dann ist $\varphi|_U$ selbstadjungiert auf U (bezüglich $f|_{U\times U}$).

Nach Induktion können wir annehmen: Es existiert Orthonormalbasis $\{v_2, ..., v_n\}$ von U, die aus Eigenvektoren von φ besteht. Damit gilt:

$$V = \langle v\rangle \perp \langle v\rangle^{\perp} = \underbrace{\langle v_1, v_2, ..., v_n\rangle}_{\text{Orthonormalbasis}}$$

11.4.8 Hauptachsentransformation

Sei $K = \mathbb{R}$ und g eine orthogonale Bilinearform auf V (zusätzlich zu f). Dann existiert eine Basis von V, die Orthonormalbasis bezüglich f und Orthogonalbasis bezüglich g ist.

Beweis: Nach (11.3.6) und (11.3.3):

$$\exists\, \varphi \in \operatorname{Hom}(V,V) \text{ mit } g(v,w) = f(v, w\varphi^{\text{ad}})\ \forall\, v,w \in V$$

und nach (11.4.4) ist φ selbstadjungiert. (11.4.7) Es existiert eine Orthonormalbasis B von V die aus Eigenvektoren von φ besteht. Seien $b, b' \in B$. Dann gilt:

$$g(b,b') = f(b, b'\varphi) = f(b, k_{b'}b') = \overline{k_{b'}}f(b,b') = \begin{cases} 0 & \text{falls} \quad b \neq b' \\ \overline{k_{b'}} & \text{falls} \quad b = b' \end{cases}$$

11.4.9 Charakterisierung der normalen Abbildungen über $\mathbb{C}$

Sei $K = \mathbb{C}$, $\dim V \geq 1$ und $\varphi \in \operatorname{Hom}(V,V)$. Dann sind äquivalent:

(a) φ ist normal

(b) Es existiert eine Orthonormalbasis von V, die aus Eigenvektoren von φ besteht, insbesondere ist φ diagonalisierbar.

(c) Für alle $v \in V$ gilt: $f(v\varphi, v\varphi) = f(v\varphi^{\text{ad}}, v\varphi^{\text{ad}})$

Beweis:

(a) $\Rightarrow$ (b) Da $\mathbb{C}$ algebraisch abgeschlossen ist, besitzt φ einen Eigenwert a. Sei v ein EIgenvektor zu diesem Eigenwert und $W := \langle v \rangle^\perp$. Nach (9.4.4) ist $V = \langle v \rangle \perp W$, und nach (11.4.6) ist $W\varphi \leq W$. Mit Induktion nach $\dim V$ können wir annehmen, daß eine Orthonormalbasis von W existiert, die aus Eigenvektoren von φ besteht. Nimmt man $\sqrt{f(v,v)}^{-1} \cdot v$ zu dieser Basis hinzu, erhält man (b).

(b) $\Rightarrow$ (c) Sei B eine Orthonormalbasis von V, die aus Eigenwerten von φ besteht, und seien $k_b \in K$, $b \in B$ und $v = \sum_{b \in B} k_b b$. Dann ist

$$f(v\varphi, v\varphi) = \sum_{b \in B} k_b \overline{k_b} a_b \overline{a_b} \qquad (*)$$

wobei a_b der Eigenwert zum Eigenvektor b ist. Als nächstes zeigen wir, daß $b \in B$ auch Eigenvektor von φ^{ad} zum Eigenwert $\overline{a_b}$ ist. Man beachte, daß

$$f(b, b'\varphi^{\text{ad}}) = f(b\varphi, b') = a_b f(b, b') \;\forall\, b, b' \in B$$

Sei wieder $v = \sum_{b \in B} k_b b$. Dann gilt:

$$f(v, b'\varphi^{\text{ad}}) = \sum_{b \in B} k_b f(b, b'\varphi^{\text{ad}}) = k_{b'} a_{b'} = f(v, \overline{a_{b'}} b')$$

und aus der Regularität von V folgt $b'\varphi^{\text{ad}} = \overline{a_{b'}} b'$, d.h. b' ist Eigenvektor von φ^{ad} für alle $b' \in B$. Aus ($*$) folgt nun:

$$f(v\varphi, v\varphi) = \sum_{b \in B} k_b \overline{k_b} a_b \overline{a_b} = f(v\varphi^{\text{ad}}, v\varphi^{\text{ad}}) \;\forall\, v \in V$$

(c) $\Rightarrow$ (a) Seien $v, w \in V$. Dann gilt:

$$f((v+w)\varphi, (v+w)\varphi) = f(v\varphi, v\varphi) + f(v\varphi, w\varphi) + f(w\varphi, v\varphi) + f(w\varphi, w\varphi)$$

und

$$f((v+w)\varphi^{\text{ad}}, (v+w)\varphi^{\text{ad}}) = f(v\varphi^{\text{ad}}, v\varphi^{\text{ad}}) + f(v\varphi^{\text{ad}}, w\varphi^{\text{ad}}) + f(w\varphi^{\text{ad}}, v\varphi^{\text{ad}}) + f(w\varphi^{\text{ad}}, w\varphi^{\text{ad}})$$

also

$$\begin{aligned} f(v\varphi, w\varphi) + f(w\varphi, v\varphi) &= f(v\varphi^{\text{ad}}, w\varphi^{\text{ad}}) + f(w\varphi^{\text{ad}}, v\varphi^{\text{ad}}) \\ &= f(v\varphi, w\varphi) + \overline{f(v\varphi, w\varphi)} \\ &= f(v\varphi^{\text{ad}}, w\varphi^{\text{ad}}) + \overline{f(v\varphi^{\text{ad}}, w\varphi^{\text{ad}})} \\ &= 2\Re(f(v\varphi, w\varphi)) = 2\Re(f(v\varphi^{\text{ad}}, w\varphi^{\text{ad}})) \end{aligned}$$

Mit $v + iw$ an Stelle von $v + w$ erhalten wir mit dem gleichen Argument

$$2\Im(f(v\varphi, w\varphi)) = 2\Im(f(v\varphi^{\text{ad}}, v\varphi^{\text{ad}}))$$

Daraus folgt $f(v\varphi, w\varphi) = f(v\varphi^{\text{ad}}, w\varphi^{\text{ad}})$ und mit (11.4.2) folgt (a).

11.4.10 Charakterisierung der selbstadjungierten Abbildungen über $\mathbb{C}$

Sei $K = \mathbb{C}$ und $\varphi \in \mathrm{Hom}(V, V)$. Dann sind äquivalent:

(a) φ ist selbstadjungiert

(b) φ ist normal, und alle Eigenwerte von φ sind reell.

(c) Für alle $v \in V$ gilt: $f(v\varphi, v) \in \mathbb{R}$

BEWEIS:

(a) $\Rightarrow$ (b) Folgt aus (11.4.5)

(b) $\Rightarrow$ (c) Nach (11.4.9) existiert eine Orthonormalbasis B von V, die aus Eigenvektoren von φ besteht. Sei $v \in V$ und a_b der Eigenwert zu $b \in B$. Es existieren $k_b \in K$, $b \in B$ mit $v = \sum_{b\in B} k_b b$. Daraus folgt

$$f(v\varphi, v) = f\left(\sum_{b\in B} k_b b\varphi, \sum_{b\in B} k_b b\right) = \sum_{b\in B} a_b k_b \overline{k_b} \in \mathbb{R}$$

(c) $\Rightarrow$ (a) Seien $v, w \in V$. Dann ist

$$f((v+w)\varphi, v+w) = f(v\varphi, v) + f(w\varphi, w) + f(v\varphi, w) + f(w\varphi, v)$$

und aus $f((v+w)\varphi, v+w)$, $f(v\varphi, v)$, $f(w\varphi, w) \in \mathbb{R}$ folgt:

$$f(v\varphi, w) + f(w\varphi, v) \in \mathbb{R} \tag{*}$$

Aus ($*$), angewandt auf v und iw, folgt $i(-f(v\varphi, w) + f(w\varphi, v)) \in \mathbb{R}$. Deshalb ist

$$\Im(f(v\varphi, w)) = -\Im(f(w\varphi, v)) \text{ und } \Re(f(v\varphi, w)) = \Re(f(w\varphi, v))$$

Also ist $f(v\varphi, w) = \overline{f(w\varphi, v)}$. Insbesondere ist nun

$$f(v\varphi, w) = \overline{f(w\varphi, v)} = f(v, w\varphi) = f(v\varphi^{\mathrm{ad}}, w)$$

Aus der Regularität von V folgt $\varphi = \varphi^{\mathrm{ad}}$.

11.4.11 Charakterisierung der unitären Abbildungen über $\mathbb{C}$

Sei $K = \mathbb{C}$ und $\varphi \in \mathrm{Hom}(V, V)$. Dann sind äquivalent:

(a) φ ist unitär

(b) φ ist normal, und für jeden Eigenwert a von φ gilt: $a\overline{a} = 1$.

(c) Für alle $v \in V$ gilt: $f(v\varphi, v\varphi) = f(v, v)$

Beweis:

(a) $\Rightarrow$ (b) Sei a Eigenwert von φ zum Eigenvektor v. Dann gilt wegen (11.4.5):

$$\overline{a}v = v\varphi^{\mathrm{ad}} = v\varphi^{-1} = a^{-1}v \Rightarrow a\overline{a} = 1$$

(b) $\Rightarrow$ (c) Nach (11.4.9) existiert eine Orthonormalbasis B von V, die aus Eigenvektoren von φ besteht. Sei $v \in V$ und a_b der Eigenwert von $b \in B$. Es existieren $k_b \in K, b \in B$ mit $v = \sum_{b\in B} k_b b$. Deshalb gilt:

$$f(v\varphi, v\varphi) = f\left(\sum_{b\in B} k_b k\varphi, \sum_{b\in B} k_b k\varphi\right) = \sum_{b\in B} k_b\overline{k_b}a_b\overline{a_b} = \sum_{b\in B} k_b\overline{k_b b} = f(v, v)$$

(c) $\Rightarrow$ (a) Seien $v, w \in V$. Dann folgt aus $f((v+w)\varphi, (v+w)\varphi) = f(v+w, v+w)$:

$$f(v\varphi, w\varphi) + f(w\varphi, v\varphi) = f(v, w) + f(w, v) \qquad (*)$$

Aus ($*$), angewandt auf v, iw folgt außerdem:

$$-f(v\varphi, w\varphi) + f(w\varphi, v\varphi) = -f(v, w) + f(w, v)$$

Wir erhalten also:

$$\begin{aligned} f(v\varphi, w\varphi) + \overline{f(v\varphi, w\varphi)} &= f(v, w) + \overline{f(v, w)} \\ \text{und } -f(v\varphi, w\varphi) + \overline{f(v\varphi, w\varphi)} &= -f(v, w) + \overline{f(v, w)} \end{aligned}$$

und damit

$$\Re(f(v\varphi, w\varphi)) = \Re(f(v, w)) \text{ und } \Im(f(v\varphi, w\varphi)) = \Im(f(v, w))$$

Damit $f(v\varphi, w\varphi) = f(v, w) = f(v\varphi\varphi^{\mathrm{ad}}, w)$. Aus der Regularität von V folgt: $\varphi^{-1} = \varphi^{\mathrm{ad}}$.

11.4.12 Quadratische Gleichungen mit mehreren Variablen

- allgemein: $ax^2 + bxy + cy^2 + dx + ey + f = 0$ bzw.

$$xAx^T + xb^T + c_0 = 0$$

- Ellipse/Kreis: $x^2 + a^2y^2 = 1$
- Hyperbel: $x^2 - y^2 = 1$
- Parabel: $y^2 = x$
- zwei Geraden: $x^2 - a^2y^2 = 0$
- Koordinatentransformation: $x' = xC$ mit $C \in O_n(K)$, dann

$$x'CAC^tx' + x'Cb^T + c_0 = 0$$

$q_A : V \to K$ mit $x \mapsto xAx^T$ (wobei $A \in \mathcal{M}_{n\times n}(K)$), dann (mit f Bilinearform):

$$q_A(v + w) = q_A(v) + q_A(w) + f(v, w)$$

$g(u, v) = uAv^T$, mit (11.4.8) existiert B, welche bezüglich f Orthonormalbasis, bezüglich g Orthogonalbasis ist.

Satz: Jede quadratische Gleichung mit n Unbestimmten ist zu einer quadratischen Gleichung der Form

$$\sum a_ix_i^2 + \sum x_ib_i + c_0 = 0$$

äquivalent. Insbesondere kann $b_i = 0$ gewählt werden, falls $a_i \neq 0$.

Bei $n = 2$:

- $a_1x^2 + a_2y^2 + c_0 = 0$ Ellipse, Hyperbeln, Punktspiegelung, Geradenpaare, $\emptyset$
- $a_1x^2 + b_2y + c_0 = 0$ Parabeln
- ($b_1x + b_2y + c_0 = 0$ Gerade)

Bei $n = 3$: $\nabla := \left(\frac{\partial}{\partial x_1}, \frac{\partial}{\partial x_2}, \ldots, \frac{\partial}{\partial x_n}\right)$

$$\sum_{i,j} a_{ij}\frac{\partial^2}{\partial x_i \partial y_i} = \nabla A \nabla^T$$

Index