Lineare Algebra 1

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:* $\bigcup_{i \in I} := \{x | x \in M_i \text{ für ein } i \in I\} = M_1 \cup M_2 \cup \ldots$
  - *Durchschnitt:* $\bigcap_{i \in I} := \{x | x \in M_i \text{ für alle } i \in I\} = M_1 \cap M_2 \cap \ldots$
  - *kartes. Produkt:* $\bigotimes_{i \in I} := \{(x_1, \ldots, x_r) | x_i \in M_i, i \in I\} = M_1 \times M_2 \times \ldots$
  - *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: $\overline{N} := M \setminus N$
    * $M \setminus \bigcap_{N \in \mathcal{N}} N = \bigcup_{N \in \mathcal{N}} (M \setminus N) \Leftrightarrow \overline{\bigcap_{N \in \mathcal{N}} N} = \bigcup_{N \in \mathcal{N}} \overline{N}$
    * $M \setminus \bigcup_{N \in \mathcal{N}} N = \bigcap_{N \in \mathcal{N}} (M \setminus N) \Leftrightarrow \overline{\bigcup_{N \in \mathcal{N}} N} = \bigcap_{N \in \mathcal{N}} \overline{N}$
    * $A \subseteq B \Rightarrow \overline{B} \subseteq \overline{A}$

- Eine (Klasseneinteilung) ist eine vollständige Aufteilung einer Menge in Teilmengen ohne Schnittmengen. Wenn für $\mathcal{N} \subseteq \mathcal{P}(M)$ gilt: $\bigcup_{N \in \mathcal{N}} N = M \wedge \bigcap_{N \in \mathcal{N}} N = \emptyset$, 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) $\tilde{x} = \tilde{y} \vee \tilde{x} \cap \tilde{y} = \emptyset$

Beweise:

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

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

(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 $A = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} | xteilty\}$ 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 $\varphi : M \rightarrow N$.

- 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 $\varphi : M \rightarrow Bild\varphi$ 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: $\tilde{\varphi} : M/\backsim \rightarrow N$, 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 $\phi : M \rightarrow N$ und $\psi : N \rightarrow R$. Dann ist $\phi\psi : M \rightarrow R$ 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

$\phi : M \rightarrow N; \psi : N \rightarrow P; \mu : P \rightarrow S \Rightarrow (\phi\psi)\mu = \phi(\psi\mu)$ 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 ϕ^** 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. $V = K^n := \bigotimes\limits_{i=1}^{n} K$ 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, $E \not\subseteq \langle B \rangle$. 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. $\square$

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 $\varphi \in \mathrm{Hom}(V, W)$. 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 $0 = \sum_{t\in T} k_t t$

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

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:

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

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 $\dim V = \dim W$ 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$V\varphi$+dimKernφ.

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

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: $c_{ij} = \mathit{Zeile}_i \times \mathit{Spalte}_j$

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

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

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

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:

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

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 $E^{(m)}_{rs}(k)$, 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 $P^{(m)}_{rs}$ an, so daß $AP^{(m)}_{rs} = (a^{(1)}_{ij})_{ij}$ mit $a^{(1)}_{11} \neq 0$, falls nicht schon alle $a_{ij} = 0$ sind für alle j.

- Durch Anwendung geeigenter $E^{(m)}_{rs}(K)$ 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 $T'_i = P^{(m-1)}_{rs}$, definiere $T_i := P^{(m)}_{(r+1)(s+1)}$.
- $\tilde{A}T_1 \cdots T_h$ 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: $ax(x^{-1}yx) = ayx = \begin{cases} a_{i+1}x & \text{falls} \quad a = a_i, i < k \\ a_ix & \text{sonst} \end{cases}$ $a = a_kaxa \notin \{a_1, ..., a_k\}$.
   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:

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

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:

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

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, $yA \stackrel{!}{=} b$. Dann ist $\sum_i y_i a_{ij} \stackrel{!}{=} b_j$, 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 $e_k > e'_k$

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

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:

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

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 $f \in K[x]$

Index