WS 03/04, Universität Augsburg

Mitschrift aus der Vorlesung von Prof. Dr. Pukelsheim

Lineare Algebra I

Tobias Wichtrey, tobias@tarphos.de

24. April 2004

Inhaltsverzeichnis

1 Mengen und Relationen

21. 10. 2003

1.1 Mengen

Die Objekte, die Mathematiker studieren, heißen **„Mengen“**[1] – nur im Spezialfall: Zahlen(mengen) –; die Beziehungen zwischen Mengen heißen **„Relationen“**.

Was „ist“ eine Menge? Solche Seinsfragen gehören in die Philosophie. Wir nehmen den „mathematischen Urknall“ als gegeben.

Es gibt Mengen $X, Y, Z, \ldots$

Eine Menge X enthält Objekte $x, y, z, \ldots$, die **„Elemente“** genannt werden.

Mathematische Konvention für den anständigen Umgang unter Mathematikern

Art. 1: Entweder Unterstreichung[2] oder Anführungsstriche bedeuten Betonung.

Art. 2: Unterstreichung (bzw. Fettdruck, siehe Fußnote 2) und Anführungsstriche bedeuten verpflichtende Sprachregelung.

Art. 3: Großbuchstaben haben **keinen** Aufstrich, Kleinbuchstaben immer **mit** Aufstrich.[3]

Art. 4: Die Aussage „Das Element x ist in der Menge X enthalten“ wird formelmäßig abgekürzt zu „$x \in X$“.
Die Aussage „Das Element x ist in der Menge X nicht enthalten“ wird abgekürzt zu „$x \notin X$“.

Art. 5: Die Aussage „Die Menge Y ist eine Teilmenge der Menge X“ bedeutet, daß jedes Element, das in Y enthalten ist, auch in X enthalten ist, und wird abgekürzt zu „$Y \subseteq X$“.
Die Aussage „Die Menge Y ist nicht eine Teilmenge der Menge X“ bedeutet, daß nicht jedes Element, das in Y enthalten ist, auch in X enthalten ist, und wird abgekürzt durch „$Y \nsubseteq X$“.

Art. 6: Die Aussage „Die Menge Y ist gleich der Menge X“ bedeutet, daß sowohl gilt $Y \subseteq X$ als auch gilt $X \subseteq Y$, und wird abgekürzt zu „$Y = X$“.
Die Aussage „Die Menge Y ist nicht gleich der Menge X“ bedeutet, daß nicht gilt sowohl $Y \subseteq X$ wie auch $X \subseteq Y$, und wird geschrieben als „$Y \neq X$“.

Art. 7: Es gibt eine Menge, die kein Element enthält. Sie heißt „leere Menge“ und wird bezeichnet mit $\emptyset$.

[1] engl. *sets*
[2] Ich werde hier statt Unterstreichung Fettdruck verwenden.
[3] Bitte keine Beschwerden, weil die Kleinbuchstaben in diesem Skript keinen Aufstrich haben. . . ;-)

Ideologie der Mathematik

Wir sagen nie, was die Objekte, die wir betrachten, sind, aber immer präzise, welche Beziehungen wir unter ihnen erlauben. Nur präzise, formelmäßig gefaßte Beziehungen sind erlaubt.

1.1.1 Mengenbeispiele I: Auflistung der Elemente

a)

$$M := \{\overbrace{\underbrace{1,2,3,4,5,6}_{\text{Liste der Elemente}}}^{\text{Menge}}\}$$

Name
„steht für“
Anfang der Menge
Ende der Menge

In Worten: Der Buchstabe M steht für die Menge mit den Elementen $1, 2, 3, 4, 5, 6$.

b) $\mathbb{N}_0 := \{0, 1, 2, 3, \ldots\}$ heißt **„die Menge der natürlichen Zahlen“**.

c) $\mathbb{Z} := \{0, 1, -1, 2, -2, 3, -3, \ldots\}$ heißt **„die Menge der ganzen Zahlen“**.

Bemerkung. Ebenso $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \ldots$

1.1.2 Mengenbeispiele II: Beschreibung der Elemente

a)

$$2\mathbb{Z} := \{\underbrace{z \in \mathbb{Z}}_{\text{Teilmenge}} \mid \overbrace{z \text{ ist gerade}}^{\text{besondere Eigenschaft}}\}$$

Name
„steht für“
mit der Eigenschaft

In Worten: Die Zeichenfolge „$2\mathbb{Z}$“ steht für die Teilmenge derjenigen ganzen Zahlen z, die die Eigenschaft „z ist gerade“ erfüllen.

b) $\mathbb{N}_0 = \{z \in \mathbb{Z} | z \geq 0\}$

Diese Aussage enthält nur Teile, die wir schon kennen. Ob diese Teile so zusammengesetzt sind, daß die Gesamtaussage „richtig“, „mathematisch wahr“, „gültig“ ist, können wir nur durch Nachdenken, Nachprüfen, Beweisen herausfinden:

Links steht die Menge $\mathbb{N}_0$ beschrieben durch Auflistung, rechts steht die Menge $\{z \in \mathbb{Z} | z \geq 0\}$ beschrieben durch ihre Eigenschaften. Also kann das Zeichen „$=$“ in der Mitte nur die Mengengleichheit aus Art. 6 der Konvention sein.

In der Tat: Es gilt $\mathbb{N}_0 \subseteq \{z \in \mathbb{Z} | z \geq 0\}$, denn wenn x eine natürliche Zahl ist ($x \in \mathbb{N}_0$), dann ist X auch eine ganze Zahl ($x \in \mathbb{Z}$) mit der Eigenschaft, daß X nichtnegativ ist ($x \geq 0$). Es gilt auch $\{z \in \mathbb{Z} | z \geq 0\} \subseteq \mathbb{N}_0$, denn wenn z eine ganze Zahl ist ($z \in \mathbb{Z}$) und z nichtnegativ ist, dann muß z eine natürliche Zahl sein ($z \in \mathbb{N}_0$).

1.1.3 Mengenbeispiele III: Berechnung als Teilmenge

Seien X und Y Teilmengen einer gegebenen Menge Z.

a) Durchschnitt[4]

$$X \cap Y := \{z \in Z | z \in X \textbf{ und } z \in Y\}$$

In Worten: Die Zeichenfolge „$X \cap Y$“ steht für die Teilmenge der Elemente $z \in Z$ mit der Eigenschaft, daß z in X enthalten ist und z in Y enthalten ist.

Es gelten die folgenden mathematischen Aussagen: 23. 10. 2003

$$\left.\begin{array}{l} X \cap Y = \{x \in X | x \in Y\} \\ X \cap Y = \{y \in Y | y \in X\} \\ X \cap Y = Y \cap X \\ X \cap Y \subseteq X \\ X \cap Y \subseteq Y \end{array}\right\} \text{ kein Bezug mehr auf die Obermenge } Z$$

b) Differenz[5]

$$X \setminus Y := \{z \in Z | z \in X \textbf{ und } z \notin Y\}$$

Es gelten die folgenden Aussagen:

$$X \setminus Y = \{x \in X | x \notin Y\}$$
$$X \setminus Y \subseteq X$$

c) Vereinigung[6]

$$X \cup Y := \{z \in Z | z \in X \textbf{ oder } z \in Y\}$$

drei Fälle:

$$z \in X \text{ und } z \in Y$$
$$z \in X \text{ und } z \notin Y$$
$$z \notin X \text{ und } z \in Y$$

[4]engl. *intersection*
[5]engl. *difference*
[6]engl. *union*

Es gilt:

$$X \cup Y = Y \cup X$$

Definition.

a) Zwei Mengen X und Y heißen **„disjunkt“** oder **„elementfremd“**, falls $X \cap Y = \emptyset$.

b) Eine Mengendifferenz $X \setminus Y$ heißt **„das Komplement von Y in X“** oder **„die Ergänzungsmenge von Y in X“**, falls $Y \subseteq X$.

c) Eine Mengenvereinigung $X \cup Y$ heißt **„die Mengensumme von X und Y“**, falls $X \cap Y = \emptyset$.

1.2 Relationen (= Beziehungen)

Sei X eine Menge und sei Y eine Menge.

$$X \times Y := \{(x, y) | x \in X \text{ und } y \in Y\}$$

In Worten: Das **„kartesische Produkt von X mit Y“** steht für die Menge aller Paare, deren erste Komponente in X enthalten ist und deren zweite Komponente in Y enthalten ist.

Warnung. Diese Einführung des kartesischen Produkts ist unbefriedigend, denn die Paarmenge wird weder durch Auflistung noch als Teilmenge einer Obermenge eingeführt.

Definition.

a) Eine Menge R heißt **„Relation auf den Mengen X und Y“**, falls $R \subseteq X \times Y$.

b) Eine Menge R heißt **„Relation auf der Menge X“**, falls $R \subseteq X \times X$.

Beispiel. Sei X die Menge der Menschen im Hörsaal.
Mögliche Relationen:

$$\{(x, y) \in X \times X | x \text{ ist blutsverwandt mit } y\}$$
$$\{(x, y) \in X \times X | x \text{ ist verliebt in } y\}$$
$$\{(x, y) \in X \times X | x \text{ zahlt } y \text{ das Mittagessen}\}$$

Definition. Eine Relation R auf der Menge X heißt

a) **„reflexiv“**, falls für jedes Element $x \in X$ gilt: (x, x) ist in R enthalten;

b) **„symmetrisch“**, falls für jedes Element $x \in X$ und für jedes Element $y \in X$ gilt: Wenn (x, y) in R enthalten ist, dann ist (y, x) in R enthalten;

c) **„transitiv“**, falls für jedes Element $x \in X$ und für jedes Element $y \in X$ und für jedes Element $z \in X$ gilt: Wenn (x, y) in R enthalten ist und (y, z) in R enthalten ist, dann ist (x, z) in R enthalten.

Definition. Eine Relation R auf der Menge X heißt **„Äquivalenzrelation“**[7], falls R reflexiv ist und R symmetrisch ist und R transitiv ist.

Beispiel.

a) „$x = y$“ ist Äquivalenzrelation auf $\mathbb{N}_0$ (oder jeder anderen Zahlenmenge).

b) „$X = Y$“ ist Äquivalenzrelation auf dem System aller Teilmengen einer gegebenen Menge Z.

In Anlehnung an das Gleichheitszeichen „=“ schreiben wir für eine Äquivalenzrelation statt $(x, y) \in R$ bevorzugt $x \sim y$. In Worten: x und y sind äquivalent.
Also nochmal:

- Reflexivität: $x \sim x$
- Symmetrie: Wenn $x \sim y$, dann $y \sim x$.
- Transitivität: Wenn $x \sim y$ und $y \sim z$, dann $x \sim z$.

Definition. Sei $\sim$ eine Äquivalenzrelation auf X. Für ein Element $x \in X$ heißt $A(x) := \{y \in X | y \sim x\}$ die **„Äquivalenzklasse von x“**.

Satz (Vorsatz über Äquivalenzklassen). *Für jedes Element $x \in X$ und für jedes Element $y \in X$ gilt: Wenn $x \sim y$, dann $A(x) = A(y)$.*

Beweis. Behauptet wird Mengengleichheit $A(x) = A(y)$, falls $x \sim y$. Gemäß Art. 6 ist zu zeigen, daß (I) $A(x) \subseteq A(y)$ und (II) $A(y) \subseteq A(x)$.

zu (I): Sei $z \in A(x)$. Das bedeutet $z \sim x$. Dem Element y wird ebenfalls Äquivalenz mit x unterstellt: $x \sim y$. Aus der Transitivität folgt $z \sim y$. Das bedeutet $z \in A(y)$ und daher gilt $A(x) \subseteq A(y)$.

zu (II): Ganz analog durch Vertauschung in (I) von x und y.

□

Zusatz. *Entweder $A(x) = A(y)$ oder $A(x) \cap A(y) = \emptyset$.*

Beweis. Sei $x \in X$ und $y \in X$. Wenn $A(x) \cap A(y) \neq \emptyset$, dann gibt es ein Element $z \in X$ mit $z \in A(x)$ und $z \in A(y)$. Daraus folgt $z \sim x$ und $z \sim y$. Symmetrie und Transitivität erzwingen $x \sim y$. Der Vorsatz liefert $A(x) = A(y)$. □

Wegen Reflexivität ist jedes Element $x \in X$ in der Äquivalenzklasse $A(x)$ enthalten.

Satz (Hauptsatz über Äquivalenzrelationen). *Sei X eine Menge und $\sim$ eine Äquivalenzrelation auf X. Das System der Äquivalenzklassen bildet eine „erschöpfende Zerlegung“ („Partition“) von X in dem Sinn, daß jedes Element $x \in X$ in einer Äquivalenzklasse enthalten ist und daß ungleiche Äquivalenzklassen disjunkt sind.*

Definition. Sei X eine Menge. Die Relation $R_= := \{(x, x) | x \in X\}$ heißt **„Elementgleichheit auf X“** und statt $(x, y) \in R_=$ schreibt man $x = y$. 28. 10. 200

Bemerkung. Die Relation $R_=$ heißt **„Diagonale von $X \times X$“**.

Satz. *Sei X eine Menge. Dann gilt:*

i) Elementgleichheit ist eine Äquivalenzrelation.

ii) Für jedes Element $x \in X$ gilt $\{y \in X | x = y\} = \{x\}$.

Bemerkung. Das heißt, Elementgleichheit zerlegt X in das System der Einermengen $\{x\}$ für $x \in X$.

Beweis.

i) Elementgleichheit ist
   - reflexiv: $(x, x) \in R_=$ für jedes Element $x \in X$
   - symmetrisch: Für jedes Element $x \in X$ und jedes Element $y \in X$ gilt: Wenn $(x, y) \in R_=$, dann sind x und y nur verschiedene Namen für dasselbe Element. Also ist das Paar (x, y) dasselbe wie das Paar (y, x), woraus folgt, daß $(y, x) \in R_=$.
   - transitiv: Wenn $(x, y) \in R_=$ und $(y, z) \in R_=$, dann sind x, y und z nur verschiedene Namen für dasselbe Element, woraus folgt, daß $(x, z) \in R_=$.

ii) Wir haben $A(x) := \{y \in X | (x, y) \in R_=\} = \{x\}$, denn $A(x) \subseteq \{x\}$ wegen Definition von $R_=$ und $A(x) \supseteq \{x\}$ wegen Reflexivität.

□

1.3 Abbildungen

Seien X und Y Mengen.

Definition. Eine Relation $G \subseteq X \times Y$ heißt **„Abbildung**(sgraph)“[8], **„Graph“** oder **„Abbildungsrelation“**, falls für jedes Element $x \in X$ genau ein Element $y \in Y$ existiert mit der Eigenschaft $(x, y) \in G$.

Konvention:

a) Das zu $x \in X$ eindeutig bestimmte Element $y \in Y$ bezeichnen wir i. a. mit „$f(x)$“ und lesen „f von x“.

b) Die Abbildung $G \subseteq X \times Y$ bezeichnen wir meist mit $f : X \to Y$ und den zugehörigen Graph bezeichnen wir mit G_f.

[7] engl. *equivalence relation*
[8] engl. *mapping*

c) Man nennt:

X	Definitionsbereich[9]
Y	Wertebereich[10]
f	Zuordnungsvorschrift[11]
x	Argument[12], Variable[13], Urbild[14]
$f(x)$	Wert[15], Bildwert[16]

d) Nützliche sprachliche Vielfalt:

Äquivalenz**klasse**
Definitions**bereich**
Potenz**system**
Abbildungs**graph**
} sind (spezielle) Mengen

Definition. Eine Abbildung $f : X \to Y$ und eine Abbildung $\tilde{f} : \tilde{X} \to \tilde{Y}$ sind **„gleich"**, falls gilt $X = \tilde{X}$ und $Y = \tilde{Y}$ und $G_f = G_{\tilde{f}}$.

1.3.1 Abbildungsbeispiele I: Tabelle der Paare $\big(x, f(x)\big)$

a) $X = \{1, 2, 3, 4, 5, 6\}$ und $Y = \mathbb{N}_0 = \{0, 1, 2, \dots\}$

x	$f(x)$
1	6
2	20
3	999
4	77
5	68
6	0

b) X = Menge der Anwesenden und $Y = \{♀, ♂\}$

x	$f(x)$
Friedrich Pukelsheim	♂
⋮	⋮

c) $X = \{1, 2, 3\} = Y$

[9]engl. *domain of definition*
[10]engl. *range of values*
[11]engl. *assignment rule*
[12]engl. *argument*
[13]engl. *variable*
[14]engl. *preimage*
[15]engl. *value*
[16]engl. *image value*

X	$f(x)$
1	1
2	3
3	2

1.3.2 Abbildungsbeispiele II: Beschreibung der Zuordnungsvorschrift

a) $f_a : \mathbb{Z} \to \mathbb{N}_0$ gegeben durch $f_a(z) := z^2$ für $z \in \mathbb{Z}$. „Quadrieren ganzer Zahlen".

b) $f_b : \mathbb{Z} \to [0, \infty)$ gegeben durch $f_b(z) := z^2$ für $z \in \mathbb{Z}$. Wir haben $f_a \neq f_b$.

c) $f_c : \mathbb{R} \to [0, \infty)$ gegeben durch $f_c(x) := x^2$ für $x \in \mathbb{R}$. „Quadrieren reeller Zahlen".

d) $f_d : \mathbb{R} \to \mathbb{R}$ gegeben durch $f_d(x) := x^2$ für $x \in \mathbb{R}$. Wir haben $f_c \neq f_d$.

e) $f_e : \mathbb{R} \to \mathbb{R}$ gegeben durch $f_e(x) := |x|$ für $x \in \mathbb{R}$. „Betrag reeller Zahlen".

f) $f_f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ gegeben durch $f_f(x, y) := xy$ für $x \in \mathbb{R}$ und $y \in \mathbb{R}$. „Multiplikation zweier reeller Zahlen".

1.3.3 Abbildungsbeispiele III: Berechnung neuer Abbildungen aus alten Abbildungen

Siehe Rest der Vorlesung, denn „Algebra" bedeutet „Rechnen mit Abbildungen".

Definition. Sei X eine Menge. Die Abbildung $f : X \to X$, die gegeben ist durch $f(x) := x$ für jedes Element $x \in X$, heißt **„Identität auf X"** und wird bezeichnet mit id_X.

Es gilt $G_{\mathrm{id}_X} = \{(x, x) | x \in X\} = R_=$ (siehe Seite 10) ist die „Diagonale" in $X \times X$.

Satz. *Seien X, Y und Z Mengen und $f : X \to Y$ eine Abbildung und $g : Y \to Z$ eine Abbildung. Dann gilt: $g \circ f : X \to Z$ mit $\big(g \circ f\big)(x) := g\big(f(x)\big)$ ist eine Abbildung.*

Beweis. Die Relation $R \subseteq X \times Z$, die $g \circ f$ als Abbildung nachweist, ist $R := \{(x, z) \in X \times Z |$ es gibt ein $y \in Y$ mit der Eigenschaft, daß $(x, y) \in G_f$ und $(y, z) \in G_g\}$ mit $x \in X$ und $z \in Z$. □

Definition. „$g \circ f$" heißt **„Komposition von g nach f"**, **„Hintereinanderausführung von g nach f"** oder **„Verkettung von g nach f"** und wird gelesen als „g nach f".

Definition. Eine Abbildung $f : X \to Y$ heißt

a) **„injektiv"**[17], falls für jedes Argument $x \in X$ und für jedes Argument $\tilde{x} \in X$ gilt: Wenn $f(x) = f(\tilde{x})$, dann $x = \tilde{x}$;

b) **„surjektiv"**[18], falls es für jeden Wert $y \in Y$ ein Argument $x \in X$ gibt mit der Eigenschaft $y = f(x)$;

[17]engl. *one-to-one*
[18]engl. *onto*

c) **„bijektiv“**[19], falls f injektiv und surjektiv ist.

In Worten:

- „f ist injektiv“ bedeutet, daß es für jeden Wert $y \in Y$ höchstens ein Argument $x \in X$ gibt mit $y = f(x)$.
- „f ist surjektiv“ bedeutet, daß es für jeden Wert $y \in Y$ mindestens ein Argument $x \in X$ gibt mit $y = f(x)$.
- „f ist bijektiv“ bedeutet, daß es für jeden Wert $y \in Y$ genau ein Argument $x \in X$ gibt mit $y = f(x)$.

Beispiel. 30. 10. 2003

a) $f : \mathbb{R} \to \mathbb{R}$ gegeben durch $f(x) := x^2$ ist weder injektiv (denn $(-2)^2 = 4 = (+2)^2$) noch surjektiv (denn -2 ist kein reelles Quadrat).

b) $f : \mathbb{R} \to [0;\infty)$ gegeben durch $f(x) := x^2$ ist nicht injektiv aber surjektiv.

c) $f : [0;\infty) \to \mathbb{R}$ gegeben durch $f(x) := x^2$ ist injektiv aber nicht surjektiv.

d) $f : [0;\infty) \to [0;\infty)$ gegeben durch $f(x) := x^2$ ist bijektiv.

Satz. *Sei $f : X \to Y$ eine bijektive Abbildung. Dann gilt: Es gibt genau eine Abbildung $g : Y \to X$ mit der Eigenschaft, daß $g \circ f = \mathrm{id}_X$ und $f \circ g = \mathrm{id}_Y$.*

Beweis.

I. (Eindeutigkeit). Sei $g : Y \to X$ eine Abbildung mit $g \circ f = \mathrm{id}_X$ und sei $\tilde{g} : Y \to X$ eine Abbildung mit $\tilde{g} \circ f = \mathrm{id}_X$. Offensichtlich haben g und $\tilde{g}$ denselben Definitionsbereich Y und denselben Wertebereich X. Sei $y \in Y$. Da f surjektiv ist, gibt es ein Argument $x \in X$ mit $y = f(x)$. Daraus folgt: $g(y) = g\big(f(x)\big) = \big(g \circ f\big)(x) = \mathrm{id}_x(x) = \big(\tilde{g} \circ f\big)(x) = \tilde{g}\big(f(x)\big) = \tilde{g}(y)$. Somit sind g und $\tilde{g}$ abbildungsgleich.

II. (Existenz). Wegen der Bijektivität von f gibt es zu jedem Wert $y \in Y$ genau ein Argument $x \in X$, so daß $y = f(x)$ gilt; also setzen wir $g(y) := x$. Die so definierte Abbildung $g : Y \to X$ erfüllt $g \circ f = \mathrm{id}_X$ und $f \circ g = \mathrm{id}_Y$.

□

Definition. Die Abbildung g aus dem Satz heißt **„die inverse Abbildung von f“**, **„die Inverse von f“**, **„die Umkehrabbildung von f“** und wird bezeichnet mit f^{-1}.

Also nochmal: $f^{-1} \circ f = \mathrm{id}$ und $f \circ f^{-1} = \mathrm{id}$.

[19] engl. *one-to-one and onto*

1.4 Mächtigkeit[20] von Mengen

Definition.

a) Zwei Mengen X und Y heißen **„gleichmächtig“** und man schreibt „|X|=|Y|“ oder „$\sharp X = \sharp Y$“, falls eine Abbildung $f : X \to Y$ existiert, so daß f bijektiv ist.

b) Eine Menge X heißt **„unendlich“**[21], falls es eine echte Teilmenge $Y \subseteq X$ und $Y \neq X$ gibt, so daß X und Y gleichmächtig sind.[22]

c) Eine Menge X heißt **„endlich“**[23], falls X nicht unendlich ist.

d) Eine Menge X heißt **„abzählbar“**[24], falls $\mathbb{N}_0$ und X gleichmächtig sind.

Bemerkung.

i) Man kann zeigen, daß X endlich ist, genau dann, wenn es eine natürliche Zahl $n \in \mathbb{N}_0$ gibt, so daß $\{0, 1, \dots, n\}$ und X gleichmächtig sind.

ii) Eigentlich wird die Menge der natürlichen Zahlen $\mathbb{N}_0$ erst zu konstruieren sein (mittels der Idee der Gleichmächtigkeit).

Beispiel.

a) $\mathbb{Z}$ ist abzählbar, denn $\mathbb{N}_0$ und $\mathbb{Z}$ sind gleichmächtig, denn $f : \mathbb{N}_0 \to \mathbb{Z}$ mit $f(n) := \frac{n}{2}$ für $n \in \{0, 2, 4, \dots\}$ („gerade“) und $f(n) := -\frac{n+1}{2}$ für $n \in \{1, 3, 5, \dots\}$ („ungerade“) ist bijektiv.

Anhang: Aussagenlogik

Eine „Aussage“ ist ein sprachliches Gebilde, das grammatisch korrekt ist und das inhaltlich stets entweder „wahr“[25] oder „falsch“[26] ist. Zu jeder Aussage gehört also ein eindeutiger Wahrheitswert. Mehrere Aussagen können zu einer neuen Aussage verknüpft werden, deren Wahrheitswert sich aus den Wahrheitswerten der gegebenen Aussage berechnet. Im folgenden seien zwei Aussagen A und B gegeben.

(N) Die **„Negation“**, „$\neg A$“, **„non A“** hat die folgenden Wahrheitswerte:

A	$\neg A$
w	f
f	w

[20] auch *Kardinalität*, engl. *cardinality*
[21] engl. *infinite*
[22] Diese Defi nition geht zurück auf Richard Dedekind (1831–1916).
[23] engl. *finite*
[24] engl. *countable*
[25] engl. *true*
[26] engl. *false*

(K) Die **„Konjunktion“**, „$A \wedge B$“, **„A und B“** erfüllt:

A \ B	w	f
w	w	f
f	f	f

(D) Die **„Disjunktion“**, „$A \vee B$“[27], **„A oder B“** erfüllt:

A \ B	w	f
w	w	w
f	w	f

(I) Die **„Implikation“**, „$A \Rightarrow B$“, **„aus A folgt B“** erfüllt:

A \ B	w	f
w	w	f
f	w	w

Sprachregelung: A heißt „Prämisse“, „Voraussetzung“. B heißt „Conclusio“, „Behauptung“.

(Ä) Die **„Äquivalenz“**, „$A \Leftrightarrow B$“, **„A genau dann, wenn B“** erfüllt:

A \ B	w	f
w	w	f
f	f	w

A ist wahrheitsgleich zu B.

Satz (Verknüpfung von Aussagen, „Aussagen-Satz, A-Satz“). *Es seien A, B Aussagen. Dann gilt:*

i) $\neg(\neg A) \quad\Leftrightarrow\quad A$

ii) $\neg(A \vee B) \quad\Leftrightarrow\quad (\neg A) \wedge (\neg B)$

iii) $\neg(A \wedge B) \quad\Leftrightarrow\quad (\neg A) \vee (\neg B)$

iv) $\neg(A \Rightarrow B) \quad\Leftrightarrow\quad A \wedge (\neg B)$

v) $\neg(A \Leftrightarrow B) \quad\Leftrightarrow\quad (\neg A) \Leftrightarrow B$

vi) $A \Rightarrow B \quad\Leftrightarrow\quad (\neg B) \Rightarrow (\neg A)$ *„Kontraposition“, „indirekter Beweis“*

vii) $A \Rightarrow B \quad\Leftrightarrow\quad \neg(A \wedge \neg B)$ *„Beweis durch Widerspruch“*

viii) $A \Leftrightarrow B \quad\Leftrightarrow\quad (A \Rightarrow B) \wedge (B \Rightarrow A)$

[27] aus lat. *vel* $\leftrightarrow \vee$

Beweis.

i)

A	$\neg A$	$\neg(\neg A)$
w	f	w
f	w	f

ii)

(A, B)	$A \wedge B$	$\neg(A \wedge B)$	$(\neg A, \neg B)$	$(\neg A) \vee (\neg B)$
(w, w)	w	f	(f, f)	f
(w, f)	f	w	(f, w)	w
(f,w)	f	w	(w, f)	w
(f, f)	f	w	(w, w)	w
		li. S.		re. S.

iii) analog

Die Beweise iv)–viii) werden als Übungsaufgaben gestellt. □

Bemerkung. a) Statt „$A \Rightarrow B$“ schreiben wir oft

Voraussetzung. A

Behauptung. B

b) Negation und Konjunktion würden reichen, um Disjunktion, Implikation, und Äquivalenz auszudrücken, denn aus iii): $A \vee B \;\Leftrightarrow\; \neg\big((\neg A) \wedge (\neg B)\big)$; aus vii): $A \Rightarrow B \;\Leftrightarrow\; \neg\big(A \wedge (\neg B)\big)$; aus viii): $A \Leftrightarrow B \;\Leftrightarrow\; (A \Leftrightarrow B) \wedge (B \Leftrightarrow A)$.

c) Schreibweisen:

- Statt $\neg(A \Rightarrow B)$ bevorzugt $A \not\Rightarrow B$
- Statt $\neg(A \Leftrightarrow B)$ bevorzugt $A \not\Leftrightarrow B$

Sei X eine Menge. Eine **„Eigenschaft auf X“**, **„einstellige Aussageform für die Menge X“** $E(\cdot)$ ist ein sprachliches Gebilde, sodaß durch Einsetzen eines beliebigen Elements $x \in X$ in die „Leerstelle“ eine Aussage $E(x)$ entsteht.

Beispiel.

a) „$\cdot$ ist eine gerade Zahl“ ist eine einstellige Aussageform für **Z**. Denn durch Einsetzen einer ganzen Zahl $z \in \mathbb{Z}$ wird „z ist eine gerade Zahl“ zu einer Aussage.

b) „$\cdot$ hat Spaß an der Linearen Algebra“ ist eine Eigenschaft auf der Menge der Hörer im Saal.

Zu diesen elementorientierten Aussagen kommen zwei neue mengenorientierte Aussagen hinzu:

(G) Die **„Generalisierung“** „für jedes Element $x \in X$ gilt $E(x)$“ hat den Wahrheitswert w, falls bei Einsetzen eines beliebigen Elements $x \in X$ die Aussage $E(x)$ wahr ist, und sie hat den Wahrheitswert f, falls es ein Element $x \in X$ gibt, für das die Aussage $E(x)$ falsch ist.

Gleichwertig: Für alle $x \in X$ gilt $E(x)$.
Für alle $x \in X : E(x)$.
$\forall x \in X : E(x)$

Man nennt $\forall$ den „Allquantor“.

(P) Die **„Partikularisierung“** „es existiert ein Element $x \in X$, für das $E(x)$ gilt“ hat den Wahrheitswert w, falls es ein Element $x \in X$ gibt, für das die Aussage E(x) wahr ist, und sie hat den Wahrheitswert f, falls bei Einsetzen eines beliebigen Elements $x \in X$ die Aussage $E(x)$ falsch ist.

Gleichwertig: Es gibt $x \in X$ mit $E(x)$.
Es existiert $x \in X : E(x)$.
$\exists x \in X : E(x)$

Man nennt $\exists$ den „Existenzquantor“.

Satz. *Es sei X eine Menge und $E(\cdot)$ eine einstellige Aussageform auf X. Dann gilt:*

$$\neg\big(\forall x \in X : E(x)\big) \Leftrightarrow \exists x \in X : \neg E(x)$$

Beweis.

I Hinrichtung $\Rightarrow$: aus Festlegung der Wahrheitswerte in (G)

II Rückschritt $\Leftarrow$: durch Kontraposition:
$\forall x \in X : E(x) \Rightarrow \neg\big(\exists x \in X : \neg E(x)\big)$ aus Festlegung der Wahrheitswerte in (P)

□

Bemerkung.

a) Die Aussage „$\forall x \in X : E(x)$“ ist dieselbe wie „$\forall s \in X : E(s)$“. Und die Aussage „$\exists x \in X : E(x)$“ ist dieselbe wie „$\exists t \in X : E(t)$“.

Die Buchstaben x, s, t in diesen Aussagen sind „gebundene Variable“, d. h. sie tragen aus sich selbst heraus keine Bedeutung, sondern erhalten ihre Bedeutung nur durch die Bindung an den Allquantor oder den Existenzquantor.

b) Die Aussage „$\forall x \in \emptyset : E(x)$“ ist **immer** wahr, denn die Verneinung „$\exists x \in \emptyset : \neg E(x)$“ ist falsch. Aus A-Satz i) ergibt sich, daß „$\forall x \in \emptyset : E(x)$“ wahr ist.

c) Die Aussage „$\exists x \in \emptyset : E(x)$“ ist immer falsch.

d) Aus einer einstelligen Aussageform $E(\cdot)$ für X und einer Aussage B können wir neue einstellige Aussageformen konstruieren:

$$\begin{array}{ll} E(\cdot) \wedge B & E(\cdot) \Rightarrow B \\ E(\cdot) \vee B & B \Rightarrow E(\cdot) \end{array}$$

Satz (Satz über Verknüpfung von einstelligen Aussageformen, „Eigenschaften-Satz, E-Satz“). *Es sei X eine Menge, $E(\cdot)$ ein einstellige Aussageform für X und B eine Aussage. Dann gilt:*

i) $\big(\forall x \in X : E(x)\big) \wedge B \quad \Leftrightarrow \quad \forall x \in X : \big(E(x) \wedge B\big)$

ii) $\big(\forall x \in X : E(x)\big) \vee B \quad \Leftrightarrow \quad \forall x \in X : \big(E(x) \vee B\big)$

iii) $\big(\exists x \in X : E(x)\big) \wedge B \quad \Leftrightarrow \quad \exists x \in X : \big(E(x) \wedge B\big)$

iv) $\big(\exists x \in X : E(x)\big) \vee B \quad \Leftrightarrow \quad \exists x \in X : \big(E(x) \vee B\big)$

v) $\big(\forall x \in X : E(x)\big) \Rightarrow B \quad \Leftrightarrow \quad \exists x \in X : \big(E(x) \Rightarrow B\big)$

vi) $\big(\exists x \in X : E(x)\big) \Rightarrow B \quad \Leftrightarrow \quad \forall x \in X : \big(E(x) \Rightarrow B\big)$

vii) $B \Rightarrow \big(\forall x \in X : E(x)\big) \quad \Leftrightarrow \quad \exists x \in X : \big(B \Rightarrow E(x)\big)$

viii) $B \Rightarrow \big(\exists x \in X : E(x)\big) \quad \Leftrightarrow \quad \forall x \in X : \big(B \Rightarrow E(x)\big)$

Beweis.

i) durch Hinsehen

ii) durch Hinsehen

iii) durch Negation von ii)

iv) durch Negation von i)

v)

$$\begin{aligned} \big(\forall x \in X : E(x)\big) \Rightarrow B &\Leftrightarrow \neg\Big(\big[\forall x \in X : E(x)\big] \wedge \neg B\Big) \\ &\Leftrightarrow \Big(\neg\big[\forall x \in X : E(x)\big]\Big) \vee B \\ &\Leftrightarrow \big(\exists x \in X : \neg E(x)\big) \vee B \\ &\Leftrightarrow \exists x \in X : \Big(\big[\neg E(x)\big] \vee B\Big) \\ &\Leftrightarrow \exists x \in X : \big(E(x) \Rightarrow B\big) \end{aligned}$$

vi) analog

vii)

$$\begin{aligned} B \Rightarrow \big(\forall x \in X : E(x)\big) &\Leftrightarrow \neg\Big(B \wedge \neg\big[\forall x \in X : E(x)\big]\Big) \\ &\Leftrightarrow (\neg B) \vee \neg\neg\big[\forall x \in X : E(x)\big] \\ &\Leftrightarrow (\neg B) \vee \forall x \in X : E(x) \\ &\Leftrightarrow \forall x \in X : \big[\neg B \vee E(x)\big] \\ &\Leftrightarrow \forall x \in X : B \Rightarrow E(x) \end{aligned}$$

viii) analog

□

Seien X und Y Mengen. Eine **„zweistellige Aussageform** $E(\cdot,\cdot)$ **für das kartesische Produkt** $X \times Y$**“** ist ein sprachliches Gebilde so, daß durch Einsetzen eines Elements $x \in X$ in die erste Leerstelle eine einstellige Aussageform $E(x,\cdot)$ für Y entsteht und daß durch Einsetzen eines Elements $y \in Y$ in die zweite Leerstelle eine einstellige Aussageform $E(\cdot,y)$ für X entsteht. 6. 11. 2003

Es gilt:

$$\begin{aligned}&\forall x \in X\big[\forall y \in Y : E(x,y)\big]\\ \Leftrightarrow &\forall y \in Y\big[\forall x \in X : E(x,y)\big]\\ \Leftrightarrow &\forall (x,y) \in X \times Y : E(x,y)\end{aligned}$$

In Worten: Zwei Allquantoren sind vertauschbar („kommutierbar“).

$$\begin{aligned}&\exists x \in X\big[\exists y \in Y : E(x,y)\big]\\ \Leftrightarrow &\exists y \in Y\big[\exists x \in X : E(x,y)\big]\\ \Leftrightarrow &\exists (x,y) \in X \times Y : E(x,y)\end{aligned}$$

In Worten: Zwei Existenzquantoren sind vertauschbar.

Aber Existenzquantor und Allquantor sind i. a. nicht vertauschbar:

$$\forall x \in X\big[\exists y \in Y : E(x,y)\big] \not\Leftarrow \exists y \in Y\big[\forall x \in X : E(x,y)\big]$$

Beispiel. Für $\mathbb{R} \times \mathbb{R}$:
$(\forall x \neq 0 \exists y \neq 0 : xy = 1)$ ist wahr.
$(\exists y \neq 0 \forall x \neq 0 : xy = 1)$ ist falsch.

Anwendungen zur Konstruktion von Teilmengen:

a) $\{x \in X | E(x)\}$ ist die Teilmenge derjenigen Elemente $x \in X$, für die $E(x)$ wahr ist.

b) $\{(x,y) \in X \times Y | E(x,y)\}$ ist die Relation derjenigen Paare $(x,y) \in X \times Y$, für die $E(x,y)$ wahr ist.

c) Für alle Teilmengen X, Y einer (Ober-)Menge Z gilt:

$$X \cap Y = \{z \in Z | z \in X \wedge z \in Y\}$$

und

$$X \cup Y = \{z \in Z | z \in X \vee z \in Y\}$$

und

$$X \setminus Y = \{z \in Z | z \in X \wedge \underbrace{\neg z \in Y}_{z \notin Y}\}$$

d) Die Aussage **„Es existiert genau ein Element** $x \in X$ **mit** $E(x)$**“** wird aussagelogisch zu

$$\exists x \in X : E(x) \wedge \big(\forall y \in X : E(y) \Rightarrow x = y\big)$$

und abgekürzt durch $\exists! x \in X : E(x)$.

e) Für alle Graphen $G \subseteq X \times Y$ gilt:

$$G \text{ ist Abbildungsgraph} \quad \Leftrightarrow \quad \forall x \in X \exists! y \in Y : (x,y) \in G$$

f) $\forall R \subseteq X \times X$:

$$\begin{aligned}R \text{ ist Äquivalenzrelation} \quad \Leftrightarrow \quad &\forall x \in X : (x,x) \in R \text{ („Reflexivität“)}\\ &\textbf{und}\\ &\forall x \in X \forall y \in X : (x,y) \in R \Rightarrow (y,x) \in R \text{ („Symmetrie“)}\\ &\textbf{und}\\ &\forall x \in X \forall y \in X \forall z \in X : (x,y) \in R \wedge (y,z) \in R \Rightarrow (x,z) \in R \text{ („Transitivität“)}\end{aligned}$$

Bemerkung.

a) $\forall x \in X \forall y \in X \forall z \in X$ wird oft verkürzt zu $\forall x, y, z \in X$.

b) Diese Formelsprache ist international, die umganssprachlichen Definitionen waren in deutscher Sprache angegeben.

c) Stilregel: Formulieren Sie eine Aussage entweder in der Umgangssprache oder in Formelsprache, aber nicht in einer Mischung aus beiden.

Mathematische Konvention (Fortsetzung)

Art. 8: Für jede Menge X gibt es eine Menge $\mathfrak{P}(X)$, deren Elemente die Teilmengen von X sind; sie heißt **„Potenzsystem von** X**“**, **„Potenzmenge von** X**“**. Kurzform: $Y \in \mathfrak{P}(X) \Leftrightarrow Y \subseteq X$

Beispiel.

a) Sei $X = \{1, 2\}$. Dann ist $\mathfrak{P}(X) = \big\{\emptyset, \{1\}, \{2\}, X\big\}$.

b) Sei $\sharp X = n$ (das soll heißen: X und $\{1, 2, \ldots, n\}$ sind gleichmächtig). Dann gilt: $\sharp\mathfrak{P}(X) = 2^n$ (ohne Beweis). Kurz oft: $\sharp\mathfrak{P}(X) = 2^{\sharp X}$. In Worten: Potenzsysteme sind viel mächtiger als die Ausgangsmengen.

Definition. Sei I eine Menge (genannt „Indexmenge“) und sei X eine Menge. Es heißt $(Y_i)_{i \in I}$ **„eine Familie von Teilmengen von** X**“**, falls gilt: $\forall i \in I : Y_i \subseteq X$.

Bemerkung. Dies ist ganz einfach eine durch Auflistung gegebene Abbildung von I in $\mathfrak{P}(X)$, nämlich mit Abbildungsgraph $\{(i, Y_i) \in I \times \mathfrak{P}(X) | i \in I\}$.

Definition. Sei $(Y_i)_{i\in I}$ eine Familie von Teilmengen einer Menge X. Setze:

$$\bigcap_{i\in I} Y_i := \{x \in X | \forall i \in I : x \in Y_i\}$$
$$\bigcup_{i\in I} Y_i := \{x \in X | \exists i \in I : x \in Y_i\}$$

Im Extremfall haben wir auch $I = \emptyset$ zugelassen:

$$\bigcap_{i\in\emptyset} Y_i = \{x \in X | \underbrace{\forall i \in \emptyset : x \in Y_i}_{\text{richtig}}\} = X$$
$$\bigcup_{i\in\emptyset} Y_i = \{x \in X | \underbrace{\exists i \in \emptyset : x \in Y_i}_{\text{falsch}}\} = \emptyset$$

Blick auf schrumpfende $I \supseteq J$:

$$\bigcap_{i\in I} Y_i = \{x \in X | \forall i \in I : x \in Y_i\} \subseteq \{x \in X | \forall i \in J : x \in Y_i\} = \bigcap_{i\in J} Y_i$$
$$\bigcup_{i\in I} Y_i = \{x \in X | \exists i \in I : x \in Y_i\} \supseteq \{x \in X | \exists i \in J : x \in Y_i\} = \bigcup_{i\in J} Y_i$$

Definition. Sei $f : X \to Y$ eine Abbildung. Dann heißt $f : \mathfrak{P}(X) \to \mathfrak{P}(Y)$ mit $f(A) := \{f(x) \in Y | x \in A\} \in \mathfrak{P}(Y)$ für $A \in \mathfrak{P}(X)$ die **„Bildmengen-Abbildung“** zur gegebenen Abbildung f und $f^{-1} : \mathfrak{P}(Y) \to \mathfrak{P}(X)$ mit $f^{-1}(B) := \{x \in X | f(x) \in B\} \in \mathfrak{P}(X)$ für $B \in \mathfrak{P}(Y)$ die **„Urbildmengen-Abbildung“** zur gegebenen Abbildung f.

Warnung.

a) Das Symbol f wird doppeldeutig verwendet.

b) Die Urbildungen-Abbildung macht immer Sinn, die inverse Abbildung f^{-1} macht nur Sinn, wenn f bijektiv ist.

21. 10. 2003

2 Körper

2.1 Körperaxiome (= definierende Eigenschaften von Körpern)

Definition. Ein **„Körper“**[1] $(K, +, \cdot)$ ist ein Tripel mit den folgenden Eigenschaften:

(Mengen)

(0) K ist eine Menge („Zahlen“, „Skalare“).

$+ : K \times K \to K$ ist eine Abbildung („Addition“).

$\cdot : K \times K \to K$ ist eine Abbildung („Multiplikation“).

(Addition)

(AA) $\forall x, y, z \in K : (x + y) + z = x + (y + z)$ „Assoziativität der Addition“

(NA) $\exists! 0 \in K \forall x \in K : 0 + x = x$ „Existenz und Eindeutigkeit des neutralen Elements der Addition“

(IA) $\forall x \in K \exists! {-x} \in K : x + -x = 0$ „Existenz und Eindeutigkeit inverser Elemente der Addition“

(KA) $\forall x, y \in K : x + y = y + x$ „Kommutativität der Addition“

(Multiplikation)

(AM) $\forall x, y, z \in K : (x \cdot y) \cdot z = x \cdot (y \cdot z)$ „Assoziativität der Multiplikation“

(NM) $\exists! 1 \in K \setminus \{0\} \forall x \in K : 1 \cdot x = x$ „Existenz und Eindeutigkeit des neutralen Elements der Multiplikation“

(IM) $\forall x \in K \setminus \{0\} \exists! x^{-1} \in K : x \cdot x^{-1} = 1$ „Existenz und Eindeutigkeit inverser Elemente der Multiplikation“

(KM) $\forall x, y \in K : x \cdot y = y \cdot x$ „Kommutativität der Multiplikation“

[1] engl. *field*

(Addition und Multiplikation)

(DAM) $\forall x, y, z \in K : x \cdot (y + z) = x \cdot y + x \cdot z$ „Distributivität der Addition und Multiplikation“

Stilregel:

a) Das Additionszeichen $+$ nennt man einen „Operator“ und sollte groß und sichtbar geschrieben werden. Also $x + y$, nicht $x{\scriptstyle +}y$.

b) Das Operatorzeichen $\cdot$ wird meist ganz weggelassen. Also xy, nicht $x \cdot y$.

c) Zur Klammerersparnis gilt die Regel „Punktrechnung vor Strichrechnung“, d. h. Multiplikation vor Addition. Also $xy + xz$ statt $(xy) + (xz)$.

Satz (über die Null). *Sei $(K, +, \cdot)$ ein Körper. Dann gilt:*

(i) $\forall x \in K : 0x = 0$

(ii) $\forall x, y \in K : x \neq 0 \wedge y \neq 0 \Rightarrow xy \neq 0$ *„Nullteilerfreiheit“*

Beweis.

(i) Sei $x \in K$. Dann gilt:

$$0x + 0x \underset{\text{DAM}}{=} (0 + 0)x \underset{\text{NA}}{=} 0x \underset{\text{NA}}{=} 0 + 0x$$

Addition von $\underset{\text{IA}}{-0x}$ ergibt auf der linken Seite:

$$0x + 0x + -0x \underset{\text{AA, IA}}{=} 0x + 0 \underset{\text{KA}}{=} 0 + 0x \underset{\text{NA}}{=} 0x$$

und auf der rechten Seite:

$$0 + 0x + -0x \underset{\text{AA, IA}}{=} 0 + 0 \underset{\text{NA}}{=} 0$$

Also folgt $0x = 0$.

(ii) Seien $x, y \in K$. Wir zeigen (indirekt) $xy = 0 \Rightarrow x = 0 \vee y = 0$. Sei also $xy = 0$. Im Fall $x = 0$ ist die rechte Seite wahr. Im Fall $x \neq 0$ benutzen wir $\underset{\text{IM}}{x^{-1}}$ und erhalten:

$$y \underset{\text{NM}}{=} 1 \cdot y \underset{\text{IM}}{=} (xx^{-1})y \underset{\text{AM}}{=} x(x^{-1}y) \underset{\text{KM}}{=} x(yx^{-1}) \underset{\text{AM}}{=} (xy)x^{-1} \underset{\text{Vor.}}{=} 0x^{-1} \underset{\text{i)}}{=} 0$$

also ist auch hier die rechte Seite wahr.

□

Beispiel.

a) $(\mathbb{R}, +, \cdot)$ ist ein Körper und heißt „Körper der reellen Zahlen“. Siehe Analysis-I-Vorlesung.

b) Der Körper $(\mathbb{Q}, +, \cdot)$.

1. Weg: Sackgasse
$\mathbb{Q} := \{\frac{p}{q} | p \in \mathbb{Z} \wedge q \in \mathbb{N}\}$ mit

$$\frac{p}{q} + \frac{\tilde{p}}{\tilde{q}} := \frac{p\tilde{q} + \tilde{p}q}{q\tilde{q}} \in \mathbb{Q}$$
$$\frac{p}{q} \cdot \frac{\tilde{p}}{\tilde{q}} := \frac{p\tilde{p}}{q\tilde{q}} \in \mathbb{Q}$$

Dabei sei gegeben: $\mathbb{Z}$ mit Rechenregeln. Also Knackpunkt: Was ist der Bruchstrich?

2. Weg: Königsweg zum Erfolg!
Gegeben und bekannt sei $\mathbb{Z}$ mit ihren Rechenregeln und $\mathbb{N} \subseteq \mathbb{Z}$.
Auf der Menge $\mathbb{Z} \times \mathbb{N}$ definieren wir die Relation R durch die Forderung, daß (p, q) und $(\tilde{p}, \tilde{q})$ in Relation stehen, falls gilt:[2]

$$\exists m \in \mathbb{N} : \big[(p = m\tilde{p} \wedge q = m\tilde{q}) \vee (\tilde{p} = mp \wedge \tilde{q} = mq)\big]$$

R ist eine Äquivalenzrelation (Übungsaufgabe).
Sei Q die Menge der Äquivalenzklassen, d. h. $Q := \{A(p, q) | (p, q) \in \mathbb{Z} \times \mathbb{N}\}$. Auf dem Äquivalenzklassensystem Q definieren wie die Addition durch:

$$A(p, q) + A(r, s) := (ps + qr, qs)$$

und die Multiplikation durch

$$A(p, q) \cdot A(r, s) := A(pr, qs)$$

Diese Abbildungen sind wohldefiniert (Übungsaufgabe). $(Q, +, \cdot)$ ist ein Körper (Übungsaufgabe).

Bemerkung.

a) Q enthält die ganzen Zahlen $\mathbb{Z}$ durch Abbildung von p auf $A(p, 1)$, insbesondere von $0 \in \mathbb{Z}$ auf $A(0, 1)$ und von $1 \in \mathbb{Z}$ auf $A(1, 1)$.

b) Q ist enthalten in $\mathbb{R}$ durch Abbildung von $A(p, q)$ auf $\frac{p}{q}$. Der Bruchstrich ist hier die Division in $\mathbb{R}$.

13. 11. 2003

Nachtrag: „Zu einer Gleichung etwas addieren“ oder „Gleichheit und Aussageformen“

Sei X eine Menge und $E(\cdot)$ eine Aussageform für X.
Wir benutzen das **„LEIBNIZ-Ersetzungsaxiom“**:

$$\forall x, y \in X : x = y \Rightarrow \big[E(x) \Leftrightarrow E(y)\big]$$

In Worten: Der Wahrheitswert der Aussage $E(x)$ bleibt unverändert, wenn Gleiches durch Gleiches ersetzt wird.

[2] Im 4. Übungsblatt wurde diese Definition korrigiert zu $\big((p, q), (r, s)\big) \in R :\Leftrightarrow ps = qr$.

Beispiel. Sei $(K, +, \cdot)$ ein Körper und $x, z \in K$.

Betrachte die Aussageform $E(\cdot)$ gegeben durch $x + z = \cdot + z$. Dann ist $E(x)$ wahr (wegen Reflexivität). Sei nun $y \in K$ mit $x = y$. Wegen des LEIBNIZ-Ersetzungsaxioms ist $E(y)$ auch wahr, d. h. es gilt $x + z = y + z$.

Salopper Jargon: Wir haben zur Gleichung $x = y$ auf beiden Seiten z hinzuaddiert.

2.2 Spezielle Körper

2.2.1 Der Körper der komplexen Zahlen $\mathbb{C}$

Gegeben und bekannt sei der Körper der reellen Zahlen $(\mathbb{R}, +, \cdot)$.

- Definition der Grundmenge:

$$\mathbb{C} := \mathbb{R} \times \mathbb{R} = \{(a, b) | a \in \mathbb{R} \wedge b \in \mathbb{R}\}$$

- Definition der Addition. („Komponentenweise“):

$$(a, b) \oplus (\tilde{a}, \tilde{b}) := (a + \tilde{a}, b + \tilde{b}) \in \mathbb{C}$$

komplexe Addition, neu

reelle Addition, bekannt

Zur Unterscheidung jetzt $\oplus$, später nur $+$.

- Definition der Multiplikation. („Kreuzweise“):

$$(a, b) \odot (\tilde{a}, \tilde{b}) := (a\tilde{a} - b\tilde{b}, a\tilde{b} + \tilde{a}b) \in \mathbb{C}$$

Das neutrale Element der (komplexen) Addition ist $(0, 0)$. Wenn es ein neutrales Element der Multiplikation gibt, dann soll es heißen $e := (x, y)$ und es muß erfüllen:

$$(1, 0) \underset{\text{NM}}{=} e \odot (1, 0) = (x, y) \odot (1, 0) \underset{\text{Def.}}{=} (x \cdot 1 - y \cdot 0, x \cdot 0 + y \cdot 1) \underset{\mathbb{R}}{=} (x, y)$$

Das heißt $e = (1, 0)$. In der Tat gilt:

$$\forall (a, b) \in \mathbb{C} : (1, 0) \odot (a, b) \underset{\text{Def.}}{=} (1 \cdot a - 0 \cdot b, 1 \cdot b + 0 \cdot a) \underset{\mathbb{R}}{=} (a, b)$$

Allgemein unterscheiden wir im Paar (a, b) zwischen den Komponenten a (erste Komponente) und b (zweite Komponente). Speziell für die Fälle mit $b = 0$ benutzen wir kürzer, daß $(r, 0)$ identifiziert wird mit r. Damit wird jede reelle Zahl $r \in \mathbb{R}$ auch zu einer komplexen Zahl $(r, 0) \in \mathbb{C}$ („Einbettung“).

Es gilt:

$$\forall r \in \mathbb{R} \forall (a, b) \in \mathbb{C} : r \oplus (a, b) \underset{\text{Ident.}}{=} (r, 0) \oplus (a, b) = (r + a, b)$$
$$r \odot (a, b) \underset{\text{Ident.}}{=} (r, 0) \odot (a, b) \underset{\text{Def.}}{=} (ra - 0 \cdot b, rb + 0 \cdot a) = (ra, rb)$$

Also z. B.

$$\begin{aligned} \forall a \in \mathbb{R} :&\quad a \odot (1, 0) = (a, 0) \\ \forall b \in \mathbb{R} :&\quad b \odot (0, 1) = (0, b) \\ \forall (a, b) \in \mathbb{C} :&\quad a \odot (1, 0) \oplus b \odot (0, 1) = (a, 0) \oplus (0, b) \underset{\text{Def.}}{=} (a, b) \end{aligned}$$

Definition (Leonhard EULER, 1707–1783). Die komplexe Zahl $(0, 1)$ heißt **„imaginäre Einheit“** und wird mit i bezeichnet.

Sie erfüllt $\mathrm{i}^2 \underset{\text{Def.}}{=} (0, 1) \odot (0, 1) \underset{\text{Def.}}{=} (0 - 1, 0) = (-1, 0) = -1$.

Die Addition schreibt sich nun:

$$\begin{array}{ccc} (a, b) \oplus (\tilde{a}, \tilde{b}) & = & (a + \tilde{a}, b + \tilde{b}) \\ \| & & \| \\ (a \oplus b\mathrm{i}) \oplus (\tilde{a} \oplus \tilde{b}\mathrm{i}) & = & (a + \tilde{a}) \oplus (b + \tilde{b})\mathrm{i} \end{array}$$

und lehnt sich optisch an die reelle Addition an.

Die Multiplikation schreibt sich nun:

$$\begin{array}{ccc} (a, b) \odot (\tilde{a}, \tilde{b}) & = & (a\tilde{a} - b\tilde{b}, a\tilde{b} + \tilde{a}b) \\ \| & & \| \\ (a \oplus b\mathrm{i}) \odot (\tilde{a} \oplus \tilde{b}\mathrm{i}) & = & (a\tilde{a} - b\tilde{b}) \oplus (a\tilde{b} + \tilde{a}b)\mathrm{i} \end{array}$$

und lehnt sich optisch an die reelle Rechnung an.

Salopp: Rechne „reell“, aber bedenke $\mathrm{i}^2 = -1$.

Definition. Für eine gegebene komplexe Zahl $(a, b) = a + b\mathrm{i} \in \mathbb{C}$ heißt „a“ ihr **„Realteil“** und „b“ ihr **„Imaginärteil“**.

Insgesamt:

- Das neutrale Element der Addition ist $(0, 0) = 0$.
- Das zu (a, b) inverse Element der Addition ist $-(a, b) = (-a, -b)$.
- Die Addition ist assoziativ und kommutativ.
- Das neutrale Element der Multiplikation ist $(1, 0) = 1$.
- Das zu (a, b) inverse Element der Multiplikation ist $(a, b)^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$, denn $(a, b) \odot (a, b)^{-1} = \left(a \cdot \frac{a}{a^2+b^2} - b \cdot \frac{-b}{a^2+b^2}, a \cdot \frac{-b}{a^2+b^2} + b \cdot \frac{a}{a^2+b^2}\right) = (1, 0)$.
  Beachte:

$$\begin{aligned} (a, b) \neq 0 &\Leftrightarrow \neg[(a, b) = (0, 0)] \\ &\Leftrightarrow \neg[a = 0 \wedge b = 0] \\ &\Leftrightarrow a \neq 0 \vee b \neq 0 \\ &\Leftrightarrow a^2 + b^2 > 0 \end{aligned}$$

- Die Multiplikation ist assoziativ und kommutativ.
- Die Distributivität von Addition und Multiplikation gilt.

2.2.2 Der Quaternionenschiefkörper

Auch für 4-Tupel $(a, b, c, d) \in \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ kann man eine Addition (und Subtraktion) und Multiplikation (und Division) definieren. Allerdings ist die Multiplikation nicht kommutativ, so daß nicht die volle Körperstruktur erreicht wird, sondern „nur“ die Struktur eines „Schiefkörpers“ $\mathbb{H}$ (nach W. R. HAMILTON, 1805–1895).

Und für 8-Tupel $(a, b, c, d, e, f, g, h) \in \mathbb{R} \times \cdots \times \mathbb{R}$ gibt es ähnliches (Oktaven $\mathbb{O}$ nach A. CAYLEY, 1821–1895). Dann ist Schluß mit der Multipliaktion und ihren Eigenschaften.

Siehe H.-D. EBBINGHAUS u. a.: „Zahlen“, 3. Aufl.

Kap. 7: $\mathbb{H}$

Kap. 9: $\mathbb{O}$

Kap. 11: Multiplikation und Division nur möglich für 2-, 4- und 8-Tupel

Kap. 14: Von Mengen zu Zahlen

2.2.3 Endliche Körper

Es gibt auch endliche Körper, z. B.:
$\mathbb{F}_2 := \{0, 1\}$
mit Additions-Tafel

$+$	0	1
0	0	1
1	1	0

und Multiplikations-Tafel

$\cdot$	0	1
0	0	0
1	0	1

ist ein Körper.

Satz. *Sei $n \in \mathbb{N}$. Dann gilt:* 18. 11. 2003

$$\forall a \in \mathbb{Z} \exists! q \in \mathbb{Z} \exists! r \in \{0, \dots, n-1\} : a = qn + r$$

(ohne Beweis).
In Worten: Jede ganze Zahl a ist ganzzahliges Vielfaches von n plus einem Rest in $\{0, \dots, n-1\}$.

Beispiel. für $n = 3$:

$$\begin{aligned} a = 13 = 4 \cdot 3 + 1 &\quad \rightsquigarrow \quad q = 4,\ r = 1 \\ a = -13 = (-5) \cdot 3 + 2 &\quad \rightsquigarrow \quad q = -5,\ r = 2 \end{aligned}$$

Definition. $a \mod n$ (lies „a modulo n“) steht für den Rest r nach Division durch n im Sinne des vorstehenden Satzes.

Beispiel.

$$\begin{aligned} 13 \quad &\mod 3 = 1 \\ (-13) \quad &\mod 3 = 2 \end{aligned}$$

Definition. Zwei ganze Zahlen $a, b \in \mathbb{Z}$ heißen **„restkongruent bzgl. n“**, **„restgleich bzgl. n“** oder **„kongruent modulo n“**, falls $(a \mod n) = (b \mod n)$. In diesem Fall schreiben wir $a \equiv b \,(\mathrm{mod}\, n)$.

Bemerkung.

a) Die Relation $\equiv$ ist eine Äquivalenzrelation auf $\mathbb{Z}$; die zugehörigen Äquivalenzklassen sind die n „Restklassen“ $A(r) := \{a \in \mathbb{Z} | (a \mod n) = r\}$ für „Reste“ $r \in \{0, \dots, n-1\} =: \mathbb{Z}_n$

b) Mit den Resten läßt sich rechnen.

$$\begin{aligned} \forall r, s \in \mathbb{Z}_n : \quad & r \oplus s := (r + s) \mod n \\ & r \odot s := (rs) \mod n \end{aligned}$$

Beispiel. $\mathbb{Z}_3 = \{0, 1, 2\}$ hat die Additions-Tafel

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

und die Multiplikations-Tafel

$\odot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

z. B.

$$\begin{aligned} -1 &= 2 \qquad\qquad 2^{-1} = 2 \\ -2 &= 1 \end{aligned}$$

Satz (Fastkörpersatz). *Sei $n \in \mathbb{N}$. Dann erfüllt $(\mathbb{Z}_n, \oplus, \odot)$ außer IM alle übrigen Körpereigenschaften: (0), AA, NA, IA, KA, AM, NM, KM, DAM.*[3]

Beweis. (angedeutet)

(0) $\mathbb{Z}_n$ ist Menge und $\oplus, \odot$ sind Abbildungen von $\mathbb{Z}_n \times \mathbb{Z}_n$ nach Z_n.

(AA) Die Addition $\oplus$ ist assoziativ.

[3]Zu den Kürzeln siehe Seite 22.

(NA) Vermutung: Das neutrale Element ist 0, denn $\forall r \in \mathbb{Z}_n : r \oplus 0 = \big[(r+0) \mod n\big] = (r \mod n) = r$.

(IA) Das zu r inverse Element der $\oplus$-Addition ist $n-r$, denn $r \oplus (n-r) = \big[(r+n-r) \mod n\big] = 0$.

(KA) Die Addition $\oplus$ ist kommutativ.

(AM) Die Multiplikation $\odot$ ist assoziativ.

(NM) Vermutung: Das neutrale Element ist 1, denn $\forall r \in \mathbb{Z}_n : 1 \odot r = \big[(1 \cdot r) \mod n\big] = (r \mod n) = r$.

(KM) Die Multiplikation $\odot$ ist kommutativ.

(DAM) Das Distributivgesetz gilt.

□

Satz (Nichtexistenz-Satz). *Sei $a, b \in \{2, 3, \dots\}$. Dann ist $(\mathbb{Z}_{ab}, \oplus, \odot)$ **kein** Körper.*

Beweis. Es ist $a, b \in \mathbb{Z}_{ab} \setminus \{0\}$ und $a \odot b = \big[(ab) \mod ab\big] = 0$. Also hat 0 die Teiler a und b, was in Körpern unmörlich ist (wegen Satz über die Null auf Seite 23). □

Satz (Existenz-Satz). *Sei $p \in \mathbb{N}$ prim. Dann ist $(\mathbb{Z}_p, \oplus, \odot)$ ein Körper. Name: der Restklassenkörper zur Primzahl p.*

Beweis. Noch zu zeigen ist IM. Sei dazu $a \in \mathbb{Z}_p$ und $a \neq 0$.

I. Von den Produkten $0 \odot a, 1 \odot a, 2 \odot a, \dots, (p-1) \odot a$ sind keine zwei gleich, denn:

   Indirekt nehmen wir an, daß gilt: $h \odot a = k \odot a$ mit $h \neq k$. Dann haben wir $ha = qp + r$ und $ka = \tilde{q}p + r$. Daraus folgt $(h-k)a = (q-\tilde{q})p$, was durch p teilbar ist. Da p kein Teiler von a ist, muß $h-k$ von p geteilt werden. Aber $h-k \in \{-(p-1), \dots, -1, 0, 1, \dots, p-1\}$ und dort wird nur 0 von p geteilt. Also gilt zwangsläufig $h-k=0$, d. h. $h = k$ ↯.

II. $\mathbb{Z}_p \setminus \{0\} = \{h \odot a | h = 1, \dots, p-1\}$, denn: „$\supseteq$“ gilt per Definition von $\odot$. Zudem hat die linke Seite $p-1$ Elemente und die rechte Seite auch (wegen I). Also müssen die beiden Mengen gleich sein.

III. Somit gilt: $\exists! h \in \{1, \dots, p-1\} : h \odot a = 1$. Das heißt $h = a^{-1}$.

□

Bemerkung. Allgemein gilt: Es gibt einen Körper F_q endlicher Mächtigkeit q genau dann, wenn $\exists p$ prim $\exists m \in \mathbb{N} : q = p^m$. Speziell für $m = 1$ erhalten wir die Restklassenkörper $(\mathbb{Z}_p, \oplus, \odot)$.

2.3 Körperautomorphismen

Homomorphismus: strukturerhaltende Abbildung von einer Struktur auf eine Struktur

Isomorphismus: bijektiver Homomorphismus

Automorphismus: Isomorphismus von einer Struktur auf sich selbst

Seien $(K, +, \cdot)$ und $(L, +, \cdot)$ Körper.

Definition. $f : K \to L$ heißt ein „(Körper-)**Homomorphismus**“, falls gilt:

$$\forall x, y \in K : \quad f(x+y) = f(x) + f(y)$$

und

$$f(x \cdot y) = f(x) \cdot f(y)$$

In Worten: Das Bild einer Summe ist gleich der Summe der Bilder und das Bild eines Produkts ist gleich dem Produkt der Bilder.

20. 11. 2003 **Satz.** *Seien K, L Körper und $f : K \to L$ ein Homomorphismus. Dann gilt:*

(i) $f(0) = 0$ ***und*** $\forall x \in K : f(-x) = -f(x)$

(ii) $f(1) \neq 0 \quad \Leftrightarrow \quad f^{-1}\big(\{0\}\big) = \{0\} \quad \Leftrightarrow \quad f$ *injektiv*

(iii) $f(1) \neq 0 \quad \Leftrightarrow \quad f(1) = 1$ ***und*** $\forall x \in K\{0\} : f\big(x^{-1}\big) = \big(f(x)\big)^{-1}$

Beweis.

(i) (I) Einerseits gilt

$$f(0) = f(0+0) \underset{\text{Homom.}}{=} f(0) + f(0)$$

Andererseits haben wir

$$f(0) = f(0) + 0 = f(0) + f(0) + -f(0)$$

Zusammen ergibt das

$$f(0) = \big(f(0) + f(0)\big) + -f(0) = f(0) + -f(0) = 0$$

(II) Für $x \in K$ setze $z := f(-x)$. Aus

$$f(x) + z = f(x) + f(-x) \underset{\text{Homom.}}{=} f(x + -x) = f(0) \underset{\text{(I)}}{=} 0$$

folgt $z = -f(x)$.

(ii) Wir beweisen $A \Leftrightarrow B \Leftrightarrow C$ durch den „Ringschluß“ $A \Rightarrow B$ **und** $B \Rightarrow C$ **und** $C \Rightarrow A$.

(I) Zu zeigen ist $A \Rightarrow B$. Es gelte $f(1) \neq 0$. Wegen (i) ist nur noch zu zeigen, daß $\forall x \in K : f(x) = 0 \quad \Rightarrow \quad x = 0$. Dies ergibt sich indirekt: Wenn $x \neq 0$, dann folgt $0 \neq f(1) = f\big(xx^{-1}\big) \underset{\text{Homom.}}{=} f(x)f\big(x^{-1}\big)$. Aus dem Satz über die Null auf Seite 23 folgt $f(x) \neq 0$.

(II) Es gelte $\forall x \in K : f(x) = 0 \quad \Rightarrow \quad x = 0$. Zu zeigen ist die Injektivität von f. Seien $x, y \in K$ mit $f(x) = f(y)$ gegeben. Dann gilt:

$$f(x-y) \underset{\text{Homom.}}{=} f(x) + f(-y) \underset{\text{(i)}}{=} f(x) + -f(y) = f(y) + -f(y) = 0$$

Die Voraussetzung erzwingt $x + -y = 0$, d. h. $x = y$.

(III) Zu zeigen ist f injektiv $\quad \Rightarrow \quad f(1) \neq 0$. Das folgt indirekt: $f(1) = 0 \underset{1 \neq 0}{\Rightarrow} \neg(f \text{ injektiv})$

(iii) Zur Hinrichtung gelte $f(1) \neq 0$. Einerseits haben wir

$$f(1) = f(1 \cdot 1) = f(1) \cdot f(1),$$

andererseits

$$1 = f(1) \cdot \big(f(1)\big)^{-1}.$$

Zusammen ergibt das

$$f(1) = f(1)f(1)\big(f(1)\big)^{-1} = f(1)\big(f(1)\big)^{-1} = 1$$

Und für $x \in K \setminus \{0\}$ setze $z := f\big(x^{-1}\big)$. Aus

$$f(x) \cdot z = f(x) \cdot f\big(x^{-1}\big) \underset{\text{Homom.}}{=} f\big(x \cdot x^{-1}\big) = f(1) = 1$$

folgt $z = \big(f(x)\big)^{-1}$.

Der Rückschritt ist trivial wegen $1 = f(1) \neq 0$.

□

Satz (über die Starrheit von $\mathbb{Q}$). $\forall f : \mathbb{Q} \to \mathbb{Q} : f$ *Automorphismus* $\quad \Leftrightarrow \quad f = \mathrm{id}_{\mathbb{Q}}$

Beweis.

(I)

$$\begin{aligned} \forall n \in \mathbb{N} : \quad f(n) &= f(n-1+1) \underset{\text{Homom.}}{=} f(n-1) + f(1) \\ &= f(n-1) + 1 \underset{\text{vollst. Ind.}}{=} (n-1) + 1 = n \end{aligned}$$

(II) Ebenso $f(-n) = -n$.

(III) Für $q = \frac{z}{n} \in \mathbb{Q}$ folgt daraus

$$\begin{aligned} f(q) &= f\left(\frac{z}{n}\right) = f\big(z \cdot n^{-1}\big) \underset{\text{Homom.}}{=} f(z) \cdot \big(f(n)\big)^{-1} \\ &= zn^{-1} = \frac{z}{n} = q \end{aligned}$$

□

Satz (über die Starrheit von $\mathbb{R}$). $\forall f : \mathbb{R} \to \mathbb{R} : f$ *Automorphismus* $\quad \Leftrightarrow \quad f = \mathrm{id}_{\mathbb{R}}$

Beweis.

(I) Wie vorher folgt $f(n) = n$, $f(z) = z$ und $f(q) = q$, sodaß sicherlich alle rationalen Zahlen Fixpunkte sind.

(II) f muß „isoton“ sein, d. h. es gilt:

$$\forall a, b \in \mathbb{R} : a < b \quad \Rightarrow \quad f(a) < f(b),$$

denn: Sei $c := b - a > 0$. Setze $r := \sqrt{c} > 0$. Dann

$$f(b) - f(a) \underset{\text{Homom.}}{=} f(b-a) = f\big(r^2\big) \underset{\text{Homom.}}{=} \big(f(r)\big)^2 > 0$$

(III) Intervallschachtelung.

□

Definition. Für $z = a + bi \in \mathbb{C}$ heißt $\overline{z} := a - bi$ **„die zu z konjugiert-komplexe Zahl“**.

Satz (über die Konjugation als nichttrivialer Automorphismus von $\mathbb{C}$). *Die Abbildung* $\overline{} : \mathbb{C} \to \mathbb{C}$, $z \mapsto \overline{z}$ *ist ein Automorphismus.*

Beweis.

(I) Sei $(a, b), \big(\tilde{a}, \tilde{b}\big) \in \mathbb{C}$. Es gilt:

$$\begin{aligned} \overline{(a,b) + \big(\tilde{a}, \tilde{b}\big)} &= \overline{a + \tilde{a}, b + \tilde{b}} = \big(a + \tilde{a}, -b - \tilde{b}\big) \\ &= (a, -b) + \big(\tilde{a}, -\tilde{b}\big) = \overline{(a,b)} + \overline{\big(\tilde{a}, \tilde{b}\big)} \end{aligned}$$

Ebenso für die Multiplikation.

(II) $\overline{(1,0)} = (1,0)$
$\rightsquigarrow$ Konjugation ist injektiv.
Konjugation ist surjektiv.

□

3 Vektorräume (= lineare Räume)

Problem bei Körpern: Addition und Multiplikation als Abbildungen $K \times K \to K$ sind nicht des Rätsels Lösung. Stattdessen $K \times V \to V$.

3.1 Definition

Definition. Ein K-Vektorraum[1] $(V, +, \cdot)$ besteht aus einem Körper $(K, +, \cdot)$ und dem angegebenen Tripel mit den folgenden Eigenschaften:

Grundeigenschaften

V ist eine Menge („Vektoren").

$+ : V \times V \to V$ ist Abbildung („Vektoraddition").

$\cdot : V \times V \to V$ ist Abbildung („Skalarmultiplikation").

Eigenschaften der Vektoraddition

(AV) $\forall u, v, w \in V : (u + v) + w = u + (v + w)$

(NV) $\exists 0 \in V \forall v \in V : 0 + v = v$

(IV) $\forall v \in V \exists - v \in V : v + -v = 0$

(KV) $\forall u, v \in V : u + v = v + u$

Eigenschaften der Skalarmultiplikation

(S1) $\forall v \in V : 1 \cdot v = v$

(S2) $\forall k, h \in K \forall v \in V : (k + h) \cdot v = k \cdot v + h \cdot v$

(S3) $\forall k, h \in K \forall v \in V : (k \cdot h) \cdot v = k \cdot (h \cdot v)$

(S4) $\forall k \in K \forall u, v \in V : k \cdot (u + v) = k \cdot u + k \cdot v$

Satz (Eindeutigkeit). *Sei $(V, +, \cdot)$ ein K-Vektorraum. Dann gilt:*

(i) $\forall u \in V : (\forall v \in V : u + v = v) \quad \Rightarrow \quad u = 0$

[1]engl. *vector space, linear space*

(ii) $\forall v \in V \forall w \in V : v + w = 0 \quad \Rightarrow \quad w = -v$

Beweis.

(i) Sei $u \in V$ so, daß gilt: $\forall v \in V : u + v = v$. Dann folgt

$$u \underset{\text{(NV)}}{=} 0 + u \underset{\text{(KV)}}{=} u + 0 \underset{\text{Vor.}}{=} 0$$

(ii) Seien $v, w \in V$ mit $v + w = 0$. Dann folgt:

$$w \underset{\text{(NV)}}{=} w + 0 \underset{\text{(IV)}}{=} w + v + -v \underset{\text{(AV), (KV)}}{=} v + w - v \underset{\text{Vor.}}{=} 0 + -v \underset{\text{(NV)}}{=} -v$$

□

25. 11. 2003

3.2 Vektorraum-Beispiele

3.2.1 Zeichenebene mit Koordinatenpunkten (x, y) als Vektoren

$V = \mathbb{R}^2 = \{(x, y) | x, y \in \mathbb{R}\}$

Der Vektor (x, y) wird als Pfeil (d. h. als gerichtete Strecke) vom gegebenen Ursprung $(0, 0)$ zu (x, y) dargestellt.

Die Vektoraddition ist die Verkettung von Pfeilen, d. h. die komponentenweise Addition der Koordinaten: $(3, 1) + (1, 1) = (4, 2)$

Die Skalarmultiplikation ist die Skalierung (Stauchung, Streckung) um einen Faktor $k \in \mathbb{R}$, d. h. die komponentenweise Skalierung der Koordinaten: $2 \cdot (1, 1) = (2, 2)$

Dies ist ein $\mathbb{R}$-Vektorraum.

3.2.2 Raum der n-Tupel über K

$V = K^n = \{(x_1, \ldots, x_n) | x_1 \in K, \ldots, x_n \in K\}$ für festes, beliebiges $n \in \mathbb{N}$ mit Vektoraddition

$$\forall (x_1, \ldots, x_n), (y_1, \ldots, y_n) \in K^n : \quad (x_1, \ldots, x_n) + (y_1, \ldots, y_n) := (x_1 + y_1, \ldots, x_n + y_n)$$

und Skalarmultiplikation

$$\forall k \in K \forall (x_1, \ldots, x_n) \in K : k(x_1, \ldots, x_n) := (kx_1, \ldots, kx_n)$$

ist ein K-Vektorraum.

Spezialfälle:

$\mathbb{R}^2$: Zeichenebene, (x, y)

$\mathbb{R}^3$: Die Welt, in der wir leben, (x, y, z)

$\mathbb{R}^4$: Raum-Zeit-Komtinuum, (x, y, z, t)

$\mathbb{R}^n$: Listen von Zahlen, $(x_1, \dots, x_n)$

Der Gewinn der Linearen Algebra besteht darin, sich nicht von den (vielen) Komponenten irritieren zu lassen, sondern das durch sie bestimmte Objekt zu betrachten. In diesem Sinn bevorzugen wir die Schreibweise $x = (x_1, \dots, x_n)$ und $x + y$.

3.2.3 Raum der $p \times q$-Matrizen

$$V = K^{p\times q} = \left\{ \left. \begin{pmatrix} a_{11} & \dots & a_{1q} \\ a_{21} & \dots & a_{2q} \\ \dots & \dots & \dots \\ a_{p1} & \dots & a_{pq} \end{pmatrix} \right| a_{11}, \dots, a_{1q}, \dots, a_{p1}, \dots, a_{pq} \in K \right\}$$

p Zeilen, q Spalten.

Mit Vektoraddition

$$\begin{pmatrix} a_{11} & \dots & a_{1q} \\ \dots & \dots & \dots \\ a_{p1} & \dots & a_{pq} \end{pmatrix} + \begin{pmatrix} b_{11} & \dots & b_{1q} \\ \dots & \dots & \dots \\ b_{p1} & \dots & b_{pq} \end{pmatrix} := \begin{pmatrix} a_{11}+b_{11} & \dots & a_{1q}+b_{1q} \\ \dots & \dots & \dots \\ a_{p1}+b_{p1} & \dots & a_{pq}+b_{pq} \end{pmatrix}$$

und Skalarmultiplikation

$$k \begin{pmatrix} a_{11} & \dots & a_{1q} \\ \dots & \dots & \dots \\ a_{p1} & \dots & a_{pq} \end{pmatrix} := \begin{pmatrix} ka_{11} & \dots & ka_{1q} \\ \dots & \dots & \dots \\ ka_{p1} & \dots & ka_{pq} \end{pmatrix}$$

Oft abgekürzt als

$$A = \begin{pmatrix} a_{11} & \dots & a_{1q} \\ \dots & \dots & \dots \\ a_{p1} & \dots & a_{pq} \end{pmatrix} = (a_{ij})_{\substack{i=1,\dots,p \\ j=1,\dots,q}}$$

Damit $A + B$ und kA.

Dies ist ein K-Vektorraum.

Beispiel. Im Matrizenraum $\mathbb{F}^{2\times 4}$ gilt:

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

3.2.4 Raum der Folgen

$V = K^{\mathbb{N}} =: \{(a_1, a_2, \dots) \in K\} =: a$ („Folge von Zahlen aus K") mit Vektoraddition $a+b := (a_1 + b_1, a_2 + b_2, \dots)$ und Skalarmultiplikation $ka := (ka_1, ka_2, \dots)$ ist ein K-Vektorraum.

3.2.5 Raum der finitären Folgen

Definition. Eine Folge $b = (b_1, b_2, \dots) \in K^{\mathbb{N}}$ heißt **„finitär"**, falls gilt $\exists l \in \mathbb{N} \forall n > l : b_n = 0$.

Beispiel. $(1, 2, 3, 0, 0, \dots)$ hat $l = 3$.
$(1, 2, 3, 4, 5, 0, 0, \dots)$ hat $l = 5$.

$V := K^{\mathbb{N}}_{\text{finitär}}$ ist ein K-Vektorraum mit Vektoraddition und Skalarmultiplikation wie in 3.2.4.

3.2.6 Raum der $\mathbb{R}$-wertigen Funktionen auf $\mathbb{R}$

$V = \mathbb{R}^{\mathbb{R}} := \{f : \mathbb{R} \to \mathbb{R} | f \text{ Abbildung}\}$ mit Vektor-Addition $\big(f + g\big)(x) := f(x) + g(x)$ und Skalarmultiplikation $\big(kf\big)(x) := k \cdot f(x)$ ist ein $\mathbb{R}$-Vektorraum.

3.2.7 Zusammenfassung

	Name der Vektoren	Name des Vektorraums	Symbol
3.2.1	Punkte	Zeichenebene	$\mathbb{R}^2$
3.2.2	n-Tupel, Zeilenlisten	Raum der n-Tupel über K	K^n
3.2.3	Matrizen	Raum der $p \times q$-Matrizen	$K^{p\times q}$
3.2.4	K-wertige Folgen	Raum der Folgen	$K^{\mathbb{N}}$
3.2.5	finitäre Folgen	Raum der finitären Folgen	$K^{\mathbb{N}}_{\text{finitär}}$
3.2.6	reelle Abbildungen auf $\mathbb{R}$	Raum der $\mathbb{R}$-wertigen Funktionen auf $\mathbb{R}$	$\mathbb{R}^{\mathbb{R}}$

Bemerkung.

a) Das selbe Objekt kann verschiedene Strukturen erlauben:

- $\mathbb{R}^2$ als reelle Ebene ist ein Vektorraum.
- $\mathbb{R}^2$ als Körper $\mathbb{C}$ ist ein Körper.

b) K ist ein Körper. K ist auch ein Vektorraum.

Satz. Jeder Körper K ist auch ein K-Vektorraum.

c) Interessanter ist, daß K^2, K^n u. ä. Vektorräume aber i. a. keine Körper sind.

3.3 Lineare Kombinationen und lineare Abbildungen: Spann und Basis

Gegeben sei ein Körper K und ein K-Vektorraum V.

3.3.1 Lineare Kombinationen

Sei $M \subseteq V$ eine beliebige Teilmenge in V. Ein Vektor $u \in V$ der Form $u := k_1 v_1 + \dots + k_n v_n$ heißt **„eine lineare Kombination von Vektoren in M“**, falls gilt:

$$\begin{aligned} n \in \mathbb{N} \quad &\textbf{und} \quad v_1, \dots, v_n \in M \\ &\textbf{und} \quad k_1, \dots, k_n \in K \end{aligned}$$

Wegen (KV) spielt die Reihenfolge der Summanden keine Rolle, z. B. gilt $u = k_1 v_1 + k_n v_n + k_{n-1} v_{n-1} + \dots$. Wegen (AV) dürfen die Vektoren $v_1, \dots, v_n$ als paarweise verschieden angenommen werden, denn wenn etwa $v_1 = v_2$ gilt, dann ergibt sich $u = (k_1 + k_2) v_1 + k_3 v_3 + \dots + k_n v_n$. Zur Erzeugung linearer Kombinationen bedarf es keiner (geordneten) n-Tupel $(v_1, \dots, v_n) \in M^n$ sondern nur einer ungeordneten endlichen Teilmenge $F := \{v_1, \dots, v_n\} \subseteq M$.

Definition. $\mathcal{F}(M) := \{F \subseteq M | F \text{ endlich}\}$ ist „das System der endlichen Teilmengen von M“.

Zu jedem Vektor $v \in F$ gehört ein Skalar $k(v)$, d. h. wir brauchen eine Abbildung $k : F \to K$.

Definition. $K^F := \{k : F \to K | k \text{ Abbildung}\}$ ist „die Menge der Koeffizientenabbildungen auf F“.

Für $F = \{1, \dots, n\}$ erhalten wir

$$\begin{aligned} K^{\{1,\dots,n\}} &= \{k : \{1, \dots, n\} \to K | k \text{ Abbildung}\} \\ &= \{(k(1), \dots, k(n)) \mid k(1) \in K, \dots, k(n) \in K\} \\ &= \{(x_1, \dots, x_n) \mid x_1 \in K, \dots, x_n \in K\} \\ &= K^n \text{ aus 3.2.2} \end{aligned}$$

In Worten: Die Menge der n-Tupel K^n ist dasselbe wie die Menge der Koeffizientenabbildungen auf $\{1, \dots, n\}$.

Definition. Für $F \in \mathcal{F}(M)$ und $k \in K^F$ setze: 27. 11. 2003

$$\sum_{v \in F} k(v)v := \begin{cases} 0 & \text{für } F = \emptyset \\ k(v_0)v_0 + \sum\limits_{v \in F \setminus \{v_0\}} k(v)v & \text{für } F \neq \emptyset \text{ und } v_0 \in F \end{cases}$$

Bemerkung. Vollständige Induktion nach der Mächtigkeit von F. Also:

(0) Die Summe über die leere Menge ist der Nullvektor (per Definition).

(1) Die Summe über eine einelementige Menge $F = \{v_1\}$ ist

$$\sum_{v \in F} k(v)v = k(v_1)v_1 + \underbrace{\sum_{v \in \emptyset} k(v)v}_{=0} = k(v_1)v_1.$$

(2) Die Summe über eine zweielementie Menge $F = \{v_1, v_2\}$ ist

$$\sum_{v \in F} k(v)v = k(v_1)v_1 + \underbrace{\sum_{v \in F \setminus \{v_1\}} k(v)v}_{=k(v_2 v_2)} = k(v_1)v_1 + k(v_2)v_2 = k(v_2)v_2 + \sum_{v \in F \setminus \{v_2\}} k(v)v.$$

In Worten: $\sum\limits_{v \in F} k(v)v$ ist „wohldefiniert“, d. h. hängt nicht ab von der Wahl von v_0 und ist gleich $k(v_1)v_1 + k(v_2)v_2$.

(3) Die Summe über eine dreielementige Menge $F = \{v_1, v_2, v_3\}$ ist analog

$$\sum_{v \in F} k(v)v = k(v_1)v_1 + k(v_2)v_2 + k(v_3)v_3.$$

(n) Dies motiviert die Schreibweise für n-elementige Mengen $F = \{v_1, \dots, v_n\}$ als

$$k(v_1)v_1 + \dots + k(v_n)v_n := \sum_{v \in F} k(v)v.$$

Dies erst gibt der Ellipse $\cdots$ eine präzise mathematische Bedeutung.

Definition. Sei $M \subseteq V$.

(i) Man nennt einen Vektor $u \in V$ **„eine lineare Kombination von Vektoren in M“**, falls gilt:

$$\exists F \in \mathcal{F}(M) \exists k \in K^F : u = \sum_{v \in F} k(v)v$$

In Worten: u ist eine „endliche Summe von skalierten Vektoren in M“.

(ii) Die Menge $\operatorname{span} M := \left\{ \sum\limits_{v \in F} k(v)v \,\middle|\, F \in \mathcal{F}(M) \textbf{ und } k \in K^F \right\}$ heißt **„das Erzeugnis von M“, „der Spann von M“.**

Bemerkung.

a) Beutelspacher schreibt $\langle M \rangle$ für $\operatorname{span} M$.

b) Wenn $M = \emptyset$, dann $\operatorname{span} \emptyset = \{0\}$.

c) Wenn M selber schon endlich ist, dann vereinfacht sich (i) zu $\exists k \in K^M : u = \sum\limits_{v \in M} k(v)v$ und (ii) zu $\operatorname{span} M = \left\{ \sum\limits_{v \in M} k(v)v \,\middle|\, k \in K^M \right\}$.

Definition. Sei $U \subseteq V$. Dann heißt U ein **„Untervektorraum von V“**, falls gilt:

$$\begin{aligned} &\oplus : U \times U \to U \text{ mit } x \oplus y := x + y \text{ ist wohldefiniert} \\ \text{und } &\odot : K \times U \to U \text{ mit } k \odot x := k \cdot x \text{ ist wohldefiniert} \\ \text{und } &(U, \oplus, \odot) \text{ ist ein Vektorraum.} \end{aligned}$$

In Worten: U zusammen mit den von V ererbten Rechenoperationen ist selber ein Vektorraum.

Satz (Untervektorraum-Kriterium). *Sei $U \subseteq V$. Dann gilt:*

$$\begin{array}{rl} U \textit{ Untervektorraum} \Leftrightarrow & 0 \in U \\ \textbf{\textit{und}} & \forall u, \tilde{u} \in U : u - \tilde{u} \in U \\ \textbf{\textit{und}} & \forall h \in K \forall u \in U : hu \in U \end{array}$$

Beweis.
„$\Rightarrow$“ ✓
„$\Leftarrow$“
Aus $0 \in U$ und $u - \tilde{u} \in U$ folgt (mit $u = 0$):$-\tilde{u} \in U$. Somit auch $u + \tilde{u} = u - \underbrace{(-\tilde{u})}_{\in U} \in U$. Und es gelten alle Vektorraum-Eigenschaften (ohne Beweis). □

Satz. $\forall M \subseteq V : \operatorname{span} M$ *ist ein Untervektorraum von* V.

Beweis.

I. Offenbar ist $0 = \sum_{v \in \emptyset} k(v)v \in \operatorname{span} M$.

II. Sei $u = \sum_{v \in F} k(v)v$ (mit $F \in \mathcal{F}(M)$ und $k \in K^F$) und $\tilde{u} = \sum_{v \in \tilde{F}} \tilde{k}(v)v$ (mit $\tilde{F} \in \mathcal{F}(M)$ und $\tilde{k} \in K^{\tilde{F}}$). Dann ist $G := F \cup \tilde{F}$ endlich und zerfällt in die disjunkten Teilmengen $F \setminus \tilde{F}, F \cap \tilde{F}, \tilde{F} \setminus F$. Definiere $h \in K^G$ durch

$$h(v) := \begin{cases} k(v) & \text{für } v \in F \setminus \tilde{F} \\ k(v) - \tilde{k}(v) & \text{für } v \in F \cap \tilde{F} \\ -\tilde{k}(v) & \text{für } v \in \tilde{F} \setminus F \end{cases}$$

Dann gilt: $u - \tilde{u} = \left(\sum_{v \in F} k(v)v\right) - \left(\sum_{v \in \tilde{F}} \tilde{k}(v)v\right) = \sum_{v \in G} h(v)v \in \operatorname{span} M$.

III. Für $h \in K$ und $u = \sum_{v \in F} k(v)v$ gilt $hu = \sum_{v \in F} \big(hk(v)\big)v \in \operatorname{span} M$.

□

Definition. Sei $M \subseteq V$.

(i) Man nennt M **„linear unabhängig“**, falls gilt:

$$\forall F \in \mathcal{F}(M) \forall k \in K^F : \sum_{v \in F} k(v)v = 0 \Rightarrow \forall v \in F : k(v) = 0$$

In Worten: Die einzige lineare Kombination für den Nullvektor ist die, bei der alle Koeffizienten verschwinden.

(ii) Man nennt M **„linear abhängig“**, falls gilt: $\neg(M$ linear unabhängig$)$. Das heißt:

$$\begin{aligned} M \text{ linear abhängig} &\Leftrightarrow \exists F \in \mathcal{F}(M) \exists k \in K^F : \sum_{v \in F} k(v)v = 0 \wedge \big(\exists v \in F : k(v) \neq 0\big) \\ &\Leftrightarrow \exists F \in \mathcal{F}(M) \exists k \in K^F \exists v_0 \in F : \sum_{v \in F} k(v)v = 0 \wedge k(v_0) \neq 0 \end{aligned}$$

In Worten: Es gibt eine lineare Kombination für den Nullvektor, bei der einer der Koeffizienten **nicht** verschwindet.

Bemerkung.

a) Was macht der Fall $M = \emptyset$? Die leere Menge ist linear **un**abhängig, denn die Aussage $\forall v \in \emptyset : E(v)$ ist immer wahr.

b) Wenn die Menge M selber schon endlich ist, dann einfacher in (i)

$$\forall k \in K^M : \sum_{v \in M} k(v)v = 0 \Rightarrow \forall v \in M : k(v) = 0$$

und in (ii)

$$\exists k \in K^M : \sum_{v \in M} k(v)v = 0 \wedge \exists v_0 \in M : k(v_0) \neq 0.$$

Satz (Charakterisierung der linearen Abhängigkeit). *Sei $M \subseteq V$, $M \neq \emptyset$. Dann gilt:*

$$M \textit{ linear abhängig} \quad \Leftrightarrow \quad \exists v_0 \in M : v_0 \in \operatorname{span}(M \setminus \{v_0\})$$

In Worten: Es existiert ein Vektor in M, der eine lineare Kombination der „anderen“ Vektoren in M ist.

Beweis.
„$\Rightarrow$“
Es existiert $F \in \mathcal{F}(M)$ und $k \in K^F$ und $v_0 \in F$ mit $0 = \sum_{v \in F} k(v)v$ und $k(v_0) \neq 0$. Wegen $\sum_{v \in F} k(v)v = k(v_0)v_0 + \sum_{v \in F \setminus \{v_0\}} k(v)v = 0$ erhält man $v_0 = -k(v_0)^{-1} \sum_{v \in F \setminus \{v_0\}} k(v)v \in \operatorname{span}(M \setminus \{v_0\})$
„$\Leftarrow$“
Es existiert $F \in \mathcal{F}(M \setminus \{v_0\})$ und $k \in K^F$ mit $v_0 = \sum_{v \in F} k(v)v$. Dann gilt $0 = v_0 + \sum_{v \in F} \big(-k(v)\big)$, wobei v_0 den Koeffizienten $1 \neq 0$ hat. □

2. 12. 2003 *Beispiel.*

a) Zeichenebene $V = \mathbb{R}^2$.
$\forall v = (x, y) \neq 0 : \operatorname{span}\{v\} = \{kv | k \in \mathbb{R}\} =$ die durch v erzeugte Gerade

$$\forall u \in \mathbb{R}^2 : \quad u \in \operatorname{span}\{v\} \Leftrightarrow \exists k \in \mathbb{R} : u = kv$$
$$\underset{\text{Schule}}{\Leftrightarrow} u, v \text{ kollinear}$$
$$\underset{\text{Uni}}{\Leftrightarrow} \{u, v\} \text{ linear abhängig}$$

Somit durch Übergang zur Negation:

$$\{u, v\} \text{ linear unabhängig} \Leftrightarrow u \notin \operatorname{span}\{v\}$$

b) Welt-Raum $V = \mathbb{R}^3$.
$\forall v = (x, y, z) \neq 0 : \operatorname{span}\{v\} = \{kv | k \in \mathbb{R}\} =$ die durch v bestimmte Gerade

$\forall v_1, v_2 \in \mathbb{R}^3 : \{v_1, v_2\}$ linear unabhängig
$\Rightarrow \operatorname{span}\{v_1, v_2\} = \{k_1 v_1 + k_2 v_2 | k_1, k_2 \in \mathbb{R}\} =$ die von v_1 und v_2 bestimmte Ebene

$$\forall u \in \mathbb{R}^3 : \quad u \in \operatorname{span}\{v_1, v_2\} \Leftrightarrow \exists k_1, k_2 \in \mathbb{R} : u = k_1 v_1 + k_2 v_2$$
$$\underset{\text{Schule}}{\Leftrightarrow} u, v_1, v_2 \text{ komplanar}$$
$$\underset{\text{Uni}}{\Leftrightarrow} \{u, v_1, v_2\} \text{ linear abhängig}$$

Durch Negation:

$$\{u, v_1, v_2\} \text{ linear unabhängig} \Leftrightarrow u \notin \operatorname{span}\{v_1, v_2\} \textbf{ und } \{v_1, v_2\} \text{ linear unabhängig}$$

Satz (über Koeffizientenvergleich). *Sei $M \subseteq V$ linear unabhängig und $u \in \operatorname{span} M$. Dann gilt:*

(i)

$$\forall F, \tilde{F} \in \mathcal{F}(M) \forall k \in (K \setminus \{0\})^F \forall \tilde{k} \in (K \setminus \{0\})^{\tilde{F}} :$$
$$\left(u = \sum_{v \in F} k(v) v \wedge u = \sum_{v \in \tilde{F}} \tilde{k}(v) v \right) \Rightarrow F = \tilde{F} \wedge \forall v \in F : k(v) = \tilde{k}(v)$$

(ii) Sei M endlich. Dann gilt:

$$\forall k, \tilde{k} \in K^F : \left(u = \sum_{v \in M} k(v) v \wedge u = \sum_{v \in M} \tilde{k}(v) v \right) \Rightarrow \forall v \in M : k(v) = \tilde{k}(v)$$

In Worten: Jeder Vektor $u \in \operatorname{span} M$ hat eine eindeutige Darstellung als lineare Kombination von Vektoren in M, wenn man verschwindende Koeffi zienten nicht beachtet.

Beweis.

(ii) Aus $0 = u - u = \sum_{v \in M} \big(k(v) - \tilde{k}(v)\big) v$ und der linearen Unabhängigkeit von M folgt:

$$\forall v \in M : k(v) - \tilde{k}(v) = 0,$$

d. h. $k(v) = \tilde{k}(v)$.

(i) Unter den gegebenen Umständen haben wir:

$$0 = u - u = \sum_{v \in F \setminus \tilde{F}} k(v) v + \sum_{v \in F \cap \tilde{F}} \big(k(v) - \tilde{k}(v)\big) v - \sum_{v \in \tilde{F} \setminus F} \tilde{k}(v) v$$

Wegen der linearen Unabhängigkeit müssen alle Koeffizienten verschwinden, insbesondere für die mittlere Summe:
$$\forall v \in F \cap \tilde{F} : k(v) = \tilde{k}(v)$$

Wenn $F \setminus \tilde{F} \neq \emptyset$, dann folgt für $v \in F \setminus \tilde{F}$, daß gilt: $k(v) = 0$; dies steht im Widerspruch zur Annahme $k \in (K \setminus \{0\})^F$; also notgedrungen

$$F \setminus \tilde{F} = \emptyset, \text{ d. h. } F \subseteq \tilde{F}.$$

Ebenso
$$\tilde{F} \setminus F = \emptyset, \text{ d. h. } \tilde{F} \subseteq F.$$

Zusammen ergibt sich $F = \tilde{F}$, wie behauptet.

□

Definition. Sei $M \subseteq V$.

(i) Man nennt M einen **„Erzeuger von V“**, falls gilt:

$$\operatorname{span} M = V.$$

(ii) Man nennt M eine **„Basis von V“**, falls gilt:

$$M \text{ ist ein Erzeuger von } V \textbf{ und } M \text{ ist linear unabhängig.}$$

Beispiel.

a) Im n-Tupel-Raum K^n setze $e_i := (\underbrace{0,\dots,0}_{i-1 \text{ Nullen}}, 1, \underbrace{0,\dots,0}_{n-i \text{ Nullen}})$. Zum Beispiel:

$$e_1 = (1, 0, \dots, 0)$$
$$e_2 = (0, 1, 0, \dots, 0)$$
$$e_3 = (0, 0, 1, 0, \dots, 0)$$

Dann ist $\{e_1, e_2 \dots, e_n\}$ eine Basis von K^n, denn:

$$\forall x \in K^n : x = (x_1, \dots, x_n) = \sum_{i=1}^{n} x_i e_i \in \operatorname{span}\{e_1, e_2 \dots, e_n\}$$

und

$$0 = \sum_{i=1}^{n} k_i e_i = (k_1, k_2, \dots, k_n) \Rightarrow \forall i = 1, \dots, n : k_i = 0$$

b) Der „triviale“ Vektorraum $\{0\}$ hat die Basis $\emptyset$, denn $\operatorname{span}\emptyset = \{0\}$ und $\emptyset$ linear abhängig.

Satz (Basis-Satz über Eindeutigkeit von Darstellungen mittels linearer Kombinationen). *Sei $M \subseteq V$. Dann gilt:*

(i)
$$M \textit{ Basis} \Leftrightarrow \forall u \in V \exists! F \in \mathcal{F}(M) \exists! k \in (K \setminus \{0\})^F : u = \sum_{v \in F} k(v)v$$

(ii) Sei M endlich. Dann gilt:

$$M \textit{ Basis} \Leftrightarrow \forall u \in V \exists! k \in K^M : u = \sum_{v \in M} k(v)v$$

Beweis.

(i) „$\Rightarrow$“
Sei $u \in V$. Da M ein Erzeuger von V ist, gilt $u \in \operatorname{span} M$. Teil (i) des Satzes zum Koeffizientenvergleich auf Seite 41) ergibt die Behauptung.

„$\Leftarrow$“
Offenbar ist $V \subseteq \operatorname{span} M$, also sogar $V = \operatorname{span} M$, d. h. M ist ein Erzeuger. Speziell für $u = 0$ erhält man die definierende Eigenschaft der linearen Unabhängigkeit.

(ii) Analog mit Teil (ii) des Satzes über Koeffizientenvergleich.

$\square$

Satz (Basis-Ergänzungssatz). *Sei $M \subseteq V$. Dann gilt:*

$$M \textit{ Basis} \Leftrightarrow M \textit{ linear unabhängig } \wedge \forall v_0 \in V \setminus M : M \cup \{v_0\} \textit{ linear abhängig}$$

In Worten: M ist eine maximale (=größtmögliche) linear unabhängige Menge.

Beweis. „$\Rightarrow$“

I. lineare Unabhängigkeit ✓

II. Sei $v_0 \in V \setminus M$. Da M ein Erzeuger ist, gilt $v_0 \in \operatorname{span} M$. Also existiert $F \in \mathcal{F}(M)$ und $k \in K^F$ mit $v_0 = \sum_{v \in F} k(v)v$. Daraus folgt: $0 = 1 \cdot v_0 - \sum_{v \in F} k(v)v \in \operatorname{span} M \cup \{v_0\}$, wobei der Koeffizient von v_0 ungleich 0 ist. Somit ist $M \cup \{v_0\}$ linear abhängig.

„$\Leftarrow$“

I. M linear unabhängig ✓

II. Sei $v_0 \in V \setminus M$. Da $M \cup \{v_0\}$ linear abhängig ist, existiert $F \in \mathcal{F}(M)$ und $k \in K^F$ mit $0 = k(v_0)v_0 + \sum_{v \in F} k(v)v$ mit nicht nur verschwindenden Koeffizienten.

Fall $k(v_0) = 0$. Dann bleibt $0 = \sum_{v \in F} k(v)v$, was wegen der linearen Unabhängigkeit von M unmöglich ist.

Fall $k(v_0) \neq 0$. Dann folgt

$$v_0 = \sum_{v \in F} \big(-k(v_0)^{-1} k(v)\big) v \in \operatorname{span} M.$$

$\square$

4. 12. 2003 **Satz (Basis-Auswahlsatz).** *Sei $M \subseteq V$. Dann gilt:*

$$M \textit{ Basis} \Leftrightarrow M \textit{ Erzeuger von } V \wedge \forall v_0 \in M : M \setminus \{v_0\} \textit{ kein Erzeuger}$$

In Worten: M ist ein kleinstmöglicher (minimaler) Erzeuger.

Beweis. „$\Rightarrow$“

I. M Erzeuger. ✓

II. $\forall v_0 \in M : M$ linear unabhängig $\Rightarrow v_0 \notin \operatorname{span} M \setminus \{v_0\}$

„$\Leftarrow$“

I. M Erzeuger. ✓

II.
$$\forall F \in \mathcal{F}(M) \forall k \in K^F : 0 = \sum_{v \in F} k(v)v \Rightarrow \forall v \in F : k(v) = 0$$

Also ist m linear unabhängig.

□

Definition. V heißt **„endlichdimensional"**[2], falls gilt:

$$\exists M \subseteq V : M \text{ endlich } \wedge \operatorname{span} M = V$$

In Worten: V ist „endlich erzeugt".

Behauptung (Basis-Existenzsatz). *Sei V endlichdimensional. Dann gilt:*

$$\exists B \subseteq V : B \textit{ endlich } \wedge B \textit{ Basis}$$

Beweis. Sei $M \subseteq V$ gegeben mit M endlich und $\operatorname{span} M = V$.

I. Entweder M kleinstmöglicher Erzeuger, dann setze $B = M$ (wegen Basis-Auswahlsatz). Oder $\exists v_1 \in M : M \setminus \{v_1\}$ Erzeuger; dann weiter

II. Entweder $M \setminus \{v_1\}$ kleinstmöglicher Erzeuger, dann setze $B = M \setminus \{v_1\}$. Oder $\exists v_2 \in M \setminus \{v_1\} : M \setminus \{v_1, v_2\}$ Erzeuger; dann weiter

III. ...

Da M endlich, kommt man mit diesem Ausdünnungsprozeß nach endlich vielen Schritten zu einer Basis. □

3.3.2 Basen in endlichdimensionalen Vektorräumen

Sei zusätzlich unser gegebener K-Vektorraum V auch endlichdimensional.
Ziel: Alle Basen von V sind gleichmächtig.
Weg: Ernst STEINITZ 1871–1928.

Satz (Vorsatz). *Sei B eine endliche Basis für V. Dann gilt:*

$$\forall w \in V \setminus \{0\} \exists v_1 \in B : \tilde{B} := \{w\} \cup (B \setminus \{v_1\}) \textit{ ist Basis}$$

In Worten: Für jeden Vektor $w \neq 0$ existiert ein Opfer $v_1 \in B$, sodaß v_1 gegen w ausgetauscht werden kann, ohne die Basis-Eigenschaft zu verlieren.

Beweis. Sei $w \neq 0$ gegeben.

I. B endlicher Erzeuger $\Rightarrow \exists k \in K^B : w = \sum_{v \in B} k(v)v$

II. $w \neq 0 \Rightarrow \exists v_1 \in B : k(v_1) \neq 0$

III. Es ist $\tilde{B}$ (wie oben definiert) ein Erzeuger von V, denn aus

$$v_1 \underset{\text{(I.)}}{=} k(v_1)^{-1} w - \sum_{v \in B \setminus \{v_1\}} \big(k(v_1)^{-1} k(v)\big) v \in \operatorname{span} \tilde{B}$$

und $\forall v \in B \setminus \{v_1\} : v \in \tilde{B}$ (per Konstruktion) folgt: $B \subseteq \operatorname{span} \tilde{B}$ und $V = \operatorname{span} B \subseteq \operatorname{span} \tilde{B} \subseteq V$. Also ist $\tilde{B}$ Erzeuger.

[2] engl. *of finite dimension*

IV. B linear unabhängig $\Rightarrow \tilde{B}$ linear unabhängig, denn (indirekt):

$$\tilde{B} \text{ linear abhängig } \Rightarrow \exists h \in K^{\tilde{B}} : 0 = \sum_{v \in \tilde{B}} h(v)v \wedge \exists v_0 \in \tilde{B} : h(v_0) \neq 0$$

IV.A Im Fall $h(w) = 0$ ist B wegen $0 = \sum_{v \in B \setminus \{v_1\}} h(v)v$ mit $h(v_0) \neq 0$ offenbar linear abhängig. (Fertig.)

IV.B Im Fall $h(w) \neq 0$ erhält man:

$$0 = w + \sum_{v \in B \setminus \{v_1\}} \big(h(w)^{-1} h(v)\big) v \underset{\text{(I.)}}{=} k(v_1) v_1 + \sum_{v \in B \setminus \{v_1\}} \big(k(v) + h(w)^{-1} h(v)\big) v$$

Wegen $k(v_1) \neq 0$ (II.) ist also B linear abhängig. (Fertig.)

□

Beispiel. Welt-Raum $V = \mathbb{R}^3$
$B = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}$ ist Basis für $\mathbb{R}^3$.
Für $w = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}$ gilt: $w = e_1 - e_2 = \sum_{i=1}^{3} k_i e_i$ mit $k_1 = 1, k_2 = -1, k_3 = 0$. ✓
Also kann e_1 gegen w ausgetauscht werden, oder e_2, nicht aber e_3 (denn in der Tat, $\{e_1, e_2, w\}$ sind komplanar).

Satz (Austauschsatz von STEINITZ). *Sei B Basis von V, $n := \sharp B \in \mathbb{N}$ (d. h. B endlich). Dann gilt:*

$$\forall C \subseteq V : C \textit{ linear unabhängig } \Rightarrow \exists D \subseteq B : C \cup D \textit{ Basis } \wedge \sharp D = n - \sharp C$$

(insbesondere $\sharp C \leq n$, d. h. wenn die Basis aus n Vektoren besteht, enthält jede linear unabhängige Menge höchstens n Vektoren).

Beweis. Durch vollständige Induktion nach $l := \sharp C$.
Induktionsanfang. $l = 0$: Dann $C = \emptyset$ und $D = B$. ✓
Induktionsschritt. $l \geq 0$ und $l < n$ und die Behauptung ist wahr für alle linear unabhängigen Mengen $\tilde{C} \subseteq V$ mit $\sharp C = l$.
Sei nun $C \subseteq V$ linear unabhängig mit $\sharp C = l + 1$. Sei $w \in C$, setze $\tilde{C} := C \setminus \{w\}$. Wegen $\sharp \tilde{C} = l$ existiert $\tilde{D} \subseteq B$ mit $\sharp \tilde{D} = n - l$, sodaß $\tilde{C} \cup \tilde{D}$ Basis ist.
Ziel ist, einen Vektor $v_1 \in \tilde{D}$ gegen w auszutauschen. Dazu schreiben wir w als lineare Kombination von Vektoren in $\tilde{C} \cup \tilde{D}$:

$$w = \sum_{v \in \tilde{C} \cup \tilde{D}} k(v)v$$

Im Fall, daß für alle $v \in \tilde{D}$ gilt $k(v) = 0$, folgt $0 = w - \sum_{v \in \tilde{C}} k(v)v$, was wegen der linearen Unabhängigkeit von C unmöglich ist.

Im gegenteiligen Fall existiert $v_1 \in \tilde{D}$ mit $k(v_1) \neq 0$. Aus dem Beweis des Vorsatzes auf Seite 45 ergibt sich, daß v_1 ausgetauscht werden kann gegen w. Mit $D := \tilde{D} \setminus \{v_1\}$ folgt die Induktionsbehauptung, d. h. $C \cup D$ Basis und $\sharp D = n - (l+1)$.

Zuletzt ergibt sich für $l = n-1$ die Behauptung auch für $l+1 = n$, d. h. für $\sharp C = n$ ergibt sich $D = \emptyset$. Es gilt also C linear unabhängig $\wedge \sharp C = n \Rightarrow C$ Basis.

Das macht die Fälle $\sharp C > n$ unmöglich, denn sonst existiert eine Teilmenge $\tilde{C} \subseteq C$ mit $\sharp C = n$ und $\tilde{C}$ Basis. Dies steht im Widerspruch zum Basisergänzungssatz auf Seite 43 und kann also nicht eintreten. □

Korollar 1 (Mächtigkeit linear unabhängiger Mengen). *Sei $B \subseteq V$ Basis von V mit $\sharp B =: n < \infty$. Dann gilt:* 9. 12. 2003

$$\forall C \subseteq V : [C \text{ linear unabhängig} \Rightarrow \sharp C \leq n]$$

Beweis. Sei $C \subseteq V$ linear unabhängig. Nach Steinitz gibt es $D \subseteq B$, so daß $C \cup D$ Basis von V und $\sharp D = n - \sharp C$. Insbesondere folgt $\sharp C = n - \underbrace{\sharp D}_{\geq 0} \leq n$. □

Korollar 2 (Gleichmächtigkeit von Basen). *Seien K ein Körper, V ein endlichdimensionaler K-Vektorraum und $B_1, B_2 \subseteq V$ zwei Basen von V mit $n_1 := \sharp B_1$ und $n_2 := \sharp B_2$. Dann gilt:*

$$n_1 = n_2 < \infty$$

In Worten: Je zwei Basen haben dieselbe endliche Mächtigkeit.

Beweis. Weil V endlichdimensional, gibt es eine Basis B von V mit $\sharp B =: n \in \mathbb{N}_0$ (Basis-Existenzsatz auf Seite 45). Für $i = 1, 2$ gilt: B_i ist als Basis linear unabhängig, also $n_i \leq n < \infty$ nach Korollar 1. Außerdem:

$$B_1 \text{ linear unabhängig} \wedge B_2 \text{ Basis von } V \underset{\text{Kor. 1}}{\Rightarrow} n_1 = \sharp B_1 \leq \sharp B_2 = n_2$$
$$B_2 \text{ linear unabhängig} \wedge B_1 \text{ Basis von } V \underset{\text{Kor. 1}}{\Rightarrow} n_2 = \sharp B_2 \leq \sharp B_1 = n_1$$

Zusammen: $n_1 = n_2$. □

Dies rechtfertigt folgende

Definition. Seien K Körper, V endlichdimensionaler K-Vektorraum, $B \subseteq V$ *irgendeine* Basis von V. Dann heißt $\sharp B \in \mathbb{N}_0$ die **„Dimension von V"**. Schreibweise: $\dim V := \sharp B$.

Bemerkung. Nachträglich rechtfertigt das die Bezeichnung „endlichdimensional".

Korollar 3 (Basis-Kriterium). *Sei K Körper, V K-Vektorraum mit $\dim V < \infty$. Dann gilt:*

$$\forall B \subseteq V : [B \text{ ist Basis von } V \Leftrightarrow B \text{ linear unabhängig} \wedge \sharp B = \dim V]$$

Beweis.
„$\Rightarrow$"
Klar nach Definition der Basis und Korollar 2.
„$\Leftarrow$"
Sei B linear unabhängig und $\sharp B = \dim V$. Nach Steinitz können wir aus einer gegebenen Basis $\tilde{B}$ von V (also $\sharp \tilde{B} = \dim V$) eine Teilmenge $D \subseteq \tilde{B}$ auswählen, so daß $B \cup D$ eine Basis von V ist und daß $\sharp D = \dim V - \sharp B \underset{\text{Vor.}}{=} \dim V - \dim V = 0$. Dies erzwingt $D = \emptyset$. Also ist $B \cup \emptyset = B$ eine Basis von V. □

Beispiel.

(i) $K = \mathbb{R}$, $V = \mathbb{R}^3$

Schon gesehen: $B = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}$ ist Basis von $\mathbb{R}^3$.

Daher $\dim \mathbb{R}^3 = \sharp B = 3$.

(ii) Allgemeiner: Für beliebige Körper K und $n \in \mathbb{N}$ sieht man leicht:

$$B = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \right\} \subseteq K^n \text{ ist eine Basis von } K^n.$$

Lineare Unabhängigkeit: siehe Übungsaufgabe 28.
$\operatorname{span} B = K^n$, denn

$$\forall x_1, \ldots x_n \in K : \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = x_1 \cdot \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \cdots + x_n \cdot \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

Damit: $\dim K^n = \sharp B = n$.

(iii) Aus Übungsaufgabe 21 (i): $K = \mathbb{F}_2$, $V = \mathfrak{P}(X)$ (X beliebig) mit Vektoraddition $\triangle$ und Skalarmultiplikation $\cdot$.

Hier z. B. $X = \{1, 2, 3\}$.

Probiere $B := \{\{1\}, \{2\}, \{3\}\}$. Durch Probieren aller Linearkombinationen von B (beachte $\sharp \left(\mathbb{F}_2^B\right) = 8$) sieht man: $\operatorname{span} B = \mathfrak{P}(X)$ und B ist linear unabhängig. Also ist B Basis von $\mathfrak{P}(X)$. Insbesondere $\dim \mathfrak{P}(X) = \sharp B = 3$.

Basis und Dimension von Untervektorräumen

Erinnerung: $U \subseteq V$ heißt Untervektorraum von V, falls U mit den auf U eingeschränkten, von V ererbten Verknüpfungen ein K-Vektorraum ist. Daher können wir auch von Basis und Dimension eines Untervektorraums sprechen.

Korollar 4 (Verschachtelte Untervektorräume). *Seien K ein Körper, V ein K-Vektorraum mit $\dim V < \infty$ und U_1, U_2 Untervektorräume von V mit $U_1 \subseteq U_2$. Dann gilt:*

(i) $\dim U_1 \leq \dim U_2$

(ii) $\forall B_1 \subseteq U_1 : [B_1$ *Basis von* $U_1 \Rightarrow \exists D \subseteq U_2 \setminus U_1 : B_1 \cup D$ *ist Basis von* $U_2 \wedge \sharp D = \dim U_2 - \dim U_1]$
In Worten: Jede Basis von U_1 kann zu einer Basis von U_2 ergänzt werden.

(iii) $U_1 = U_2 \Leftrightarrow \dim U_1 = \dim U_2$

Beweis. Sei B_2 Basis von U_2, also B_2 linear unabhängig. Mit Korollar 1: $\sharp B_2 \leq \dim V < \infty$. Also ist U_2 endlichdimensional.

(i), (ii) Sei B_1 Basis von U_1, also B_1 linear unabhängig. Wegen $U_1 \subseteq U_2$ gilt $\sharp B_1 \leq \dim U_2$ nach Korollar 1, d. h. $\dim U_1 \leq \dim U_2$

Nach STEINITZ (angewandt auf den Vektorraum U_2 mit Basis B_2) gibt es $D \subseteq B_2$, so daß $B_1 \cup D$ Basis von U_2 und $\sharp D = \sharp B_2 - \sharp B_1 = \dim U_2 - \dim U_1$.

Dabei gilt $D \cap U_1 = \emptyset$, denn sonst gibt es $v \in D \cap U_1 = D \cap \operatorname{span} B_1$, also $B_1 \cup D$ linear abhängig. $\lightning$ zur Basis-Eigenschaft von $B_1 \cup D$.

Also gilt $D \subseteq B_2 \setminus U_1 \subseteq U_2 \setminus U_1$.

(iii) „$\Rightarrow$“
klar.
„$\Leftarrow$“
Sei $\dim U_1 = \dim U_2$. Nach (ii) gibt es $D \subseteq B_2$, so daß $B_1 \cup D$ Basis von U_2 und $\sharp D = \dim U_2 - \dim U_2 \underset{\text{Vor.}}{=} 0$. Dies erzwingt $D = \emptyset$, so daß B_1 Basis von U_2 ist. Damit: $U_1 = \operatorname{span} B_1 = U_2$

□

Korollar 5 (Spezialfall $U_2 = V$). *Sei K Körper V K-Vektorraum mit $\dim V < \infty$, U Untervektorraum von V. Dann gilt:*

(i) $\dim U \leq \dim V$

(ii) $\forall B \subseteq U : [B$ *Basis von* $U \Rightarrow \exists D \subseteq V \setminus U : B \cup D$ *ist Basis von* $V \wedge \sharp D = \dim V - \dim U]$

(iii) $U = V \Leftrightarrow \dim U = \dim V$

Beweis. Setze $U_1 = U$ und $U_2 = V$ in Korollar 4. □

Überlegung Sei wie in Korollar 5 ein Untervektorraum U von V gegeben. Sei B Basis von U (insbesondere $\operatorname{span} B = U$). Nach Korollar 5 (ii) gibt es $D \subseteq V \setminus U$, so daß $B \cup D$ Basis von V und $\sharp D = \dim V - \dim U$.

Sei $W := \operatorname{span} D$, also W Untervektorraum von V. Für die Untervektorräume U, W von V gilt:

(i) $U \cap W = \{0\}$, denn:
„$\supseteq$“ klar. Zum Beweis von „$\subseteq$“ sei $x \in U \cap W = \operatorname{span} B \cap \operatorname{span} D$, d. h. es gibt $F \in \mathcal{F}(B)$, $k \in K^F$ und $G \in \mathcal{F}(D)$, $l \in K^G$ mit $x = \sum_{v \in F} k(v)v = \sum_{v \in G} l(v)v$, also $0 = x - x = \sum_{v \in F} k(v)v - \sum_{v \in G} l(v)v$ mit $F \cup G \in \mathcal{F}(B \cup D)$, d. h. wir haben hier eine Darstellung von 0 als Linearkombination von $B \cup D$.

Da $B \cup D$ linear unabhängig, folgt[3]: $k(v) = 0$ für alle $v \in F$, $l(v) = 0$ für alle $v \in G$. Insbesondere $x = \sum_{v \in F} k(v)v = 0$.

Dies zeigt: $U \cap W = \{0\}$. (Der Schnitt von U, W ist minimal.)

(ii) $\operatorname{span}(U \cup W) = V$ (mit Schreibweise aus Übungsaufgabe 27 (ii): $U + W = V$).

Wegen $B \subseteq U$ und $D \subseteq W$ gilt $B \cup D \subseteq U \cup W$ und daher: $V = \operatorname{span}(B \cup D) \subseteq \operatorname{span}(U \cup W) \subseteq V$, also $\operatorname{span}(U \cup W) = V$.

(Das heißt, die „Summe“ von U, W ist maximal).

Definition. Seien K Körper, V K-Vektorraum, $U_1, U_2 \subseteq V$ zwei Untervektorräume von V. Dann heißen U_1, U_2 **„zueinander komplementär in V“**, falls gilt:

$$U_1 \cap U_2 = \{0\} \qquad \text{und} \qquad \operatorname{span}(U_1 \cup U_2) = V$$

11. 12. 2003 **Satz (Existenz).** *Sei K Körper, V K-Vektorraum, U Untervektorraum von V. Dann gilt: $\exists W \subseteq V : W$ Untervektorraum und U, W zueinander komplementär.*

Beweis. Siehe Überlegung auf dieser Seite. □

Beispiel. Zeichenebene $V = \mathbb{R}^2$ als $\mathbb{R}$-Vektorraum, $U = \operatorname{span}\left\{\binom{2}{1}\right\}$. Setze $W_1 := \operatorname{span}\left\{\binom{3}{1}\right\}$ und $W_2 := \operatorname{span}\left\{\binom{-1}{1}\right\}$.

Dafür gilt:

(i) $U \cap W_i = \{0\}$

(ii) $U + W_i = \mathbb{R}^2$, denn $\left\{\binom{2}{1}, \binom{3}{1}\right\}$ linear unabhängig und daher Basis, $\left\{\binom{2}{1}, \binom{-1}{1}\right\}$ ebenso.

Damit: U, W_1 zueinander komplementär in $\mathbb{R}^2$. U, W_2 ebenso.

[3] beachte: $\left.\begin{array}{l} D \subseteq V \setminus U \\ B \subseteq U \end{array}\right\} \Rightarrow F \cap G = \emptyset$

Satz (Eindeutige Vektorzerlegung durch zueinander komplementäre Untervektorräume). *Seien U_1, U_2 zueinander komplementäre Untervektorräume in V. Dann gilt:*

$$\forall v \in V \exists! u_1 \in U_1 \exists! u_2 \in U_2 : v = u_1 + u_2$$

Beweis. Sei $v \in V$.

I. (Existenz). Nach Voraussetzung gilt $V = \operatorname{span}(U_1 \cup U_2)$. Also gibt es $F \in \mathcal{F}(U_1 \cup U_2)$ und $k \in K^F$ mit $v = \sum_{w \in F} k(w)w$. Setze $F_1 := F \cap U_1 \in \mathcal{F}(U_1)$ und $F_2 := F \setminus F_1 \in \mathcal{F}(U_2)$. Dann $F_1 \cap F_2 = \emptyset$ und $F_1 \cup F_2 = F$ und

$$v = \sum_{w \in F} k(w)w = \underbrace{\sum_{w \in F_1} k(w)w}_{=:u_1 \in U_1} + \underbrace{\sum_{w \in F_2} k(w)w}_{=:u_2 \in U_2} = u_1 + u_2.$$

II. (Eindeutigkeit). Seien $u_1, \tilde{u}_1 \in U_1$ und $u_2, \tilde{u}_2 \in U_2$ mit $v = u_1 + u_2 = \tilde{u}_1 + \tilde{u}_2$. Daraus folgt

$$\underbrace{u_1 - \tilde{u}_1}_{\in U_1} = \underbrace{u_2 - \tilde{u}_2}_{\in U_2} \in U_1 \cap U_2 = \{0\}$$

und $u_1 = \tilde{u}_1$ und $u_2 = \tilde{u}_2$.

□

3.3.3 Der Dimensionssatz für zwei Untervektorräume

Sei K Körper und V ein endlichdimensionaler K-Vektorraum.

Vorüberlegung mit zwei Teilmengen Y_1, Y_2 einer endlichen Menge X:

$$\sharp(Y_1 \cup Y_2) = \sharp Y_1 + \sharp Y_2 - \sharp(Y_1 \cap Y_2)$$

Satz (Dimensionssatz für beliebige Untervektorräume). *Seien U_1, U_2 Untervektorräume von V. Dann gilt:*

$$\dim(U_1 + U_2) = \dim U_1 + \dim U_2 - \dim(U_1 \cap U_2)$$

Bemerkung. Dies ist eine Gleichung zwischen natürlichen Zahlen.

Beweis.

I. Der Basis-Existenzsatz auf Seite 45 gibt drei Basen:

C Basis für $U_1 \cap U_2$

B_1 Basis für U_1

B_2 Basis für U_2

II. Der Austauschsatz von STEINITZ auf Seite 46 liefert einerseits

$$\exists D_1 \subseteq B_1 : \tilde{B}_1 := C \cup D_1 \text{ Basis von } U_1$$

und andererseits

$$\exists D_2 \subseteq B_2 : \tilde{B}_2 := C \cup D_2 \text{ Basis von } U_2.$$

III. Für $B := \tilde{B}_1 \cup \tilde{B}_2$ gilt gemäß Vorüberlegung:

$$\sharp B = \underset{\underset{\dim U_1}{\|}}{\sharp \tilde{B}_1} + \underset{\underset{\dim U_2}{\|}}{\sharp \tilde{B}_2} - \sharp(\tilde{B}_1 \cap \tilde{B}_2)$$

IV. $\tilde{B}_1 \cap \tilde{B}_2 = C$, denn:
Per Konstruktion gilt $C \subseteq \tilde{B}_1 \cap \tilde{B}_2$. Die andere Inklusion $\tilde{B}_1 \cap \tilde{B}_2 \subseteq C$ folgt indirekt:

Wenn es einen Vektor $d \notin C$ gibt mit $d \in \tilde{B}_1 \cap \tilde{B}_2$, dann o. B. d. A. $d \in D_1$. Dann auch $d \in D_2$, also auch $d \in D_1 \cap D_2 \subseteq U_1 \cap U_2$. Es ist $C \cup \{d\}$ linear unabhängig in $U_1 \cap U_2$, was wegen der Basis-Eigenschaft von C nicht geht.

Also gilt: $\tilde{B}_1 \cap \tilde{B}_2 = C$ und $\sharp C = \dim(U_1 \cap U_2)$.

V. B ist ein Erzeuger von $U_1 + U_2$, denn:
$u_1 \in U_1$ ist darstellbar gemäß $u_1 = \sum_{v \in \tilde{B}_1} k(v)v$ und $u_2 \in U_2$ ist darstellbar gemäß $u_2 = \sum_{v \in \tilde{B}_2} h(v)v$.
Zusammen:

$$u_1 + u_2 = \sum_{v \in C} \big(k(v) + h(v)\big) + \sum_{v \in D_1} k(v)v + \sum_{v \in D_2} h(v)v \in \operatorname{span} B$$

Somit:

$$U_1 + U_2 \subseteq \operatorname{span} B \subseteq \operatorname{span}(U_1 \cup U_2) = U_1 + U_2$$

VI. B linear unabhängig, denn:
Mit $k \in K^B$ sei

$$0 = \sum_{v \in B} k(v)v = \sum_{v \in C} k(v)v + \sum_{v \in D_1} k(v)v + \sum_{v \in D_2} k(v)v. \tag{3.1}$$

Dann folgt

$$\underbrace{\sum_{v \in C} k(v)v + \sum_{v \in D_1} k(v)v}_{\in U_1} = \underbrace{-\sum_{v \in D_2} k(v)v}_{\in U_2} \in U_1 \cap U_2$$
$$= \sum_{v \in C} h(v)v \text{ mit geeigneten Koeffizienten } h \in K^C.$$

Eingesetzt in (3.1) erhalten wir

$$0=\sum_{v\in C}h(v)v+\sum_{v\in D_2}k(v)v.$$

Da $\tilde{B}_2=C\cup D_2$ linear unabhängig ist, folgt $k(v)=0$ für alle $v\in D_2$. Damit wird (3.1) zu:

$$0=\sum_{v\in C}k(v)v+\sum_{v\in D_1}k(v)v.$$

Da $\tilde{B}_1=C\cup D_1$ linear unabhängig ist, folgt $k(v)=0$ für alle $v\in\tilde{B}_1=C\cup D_1$. Somit $k(v)=0$ für alle Vektoren $v\in B=C\cup D_1\cup D_2$.

Finale: Wegen V und VI ist B Basis von U_1+U_2 und wegen III erhalten wir die Behauptung.

□

Korollar 1 (Dimensions-Satz für direkte Summen).

$$U_1\cap U_2=\{0\}\Rightarrow\dim(U_1+U_2)=\dim U_1+\dim U_2$$

Beweis. ✓ □

Bemerkung.

a) Allgemein heißt $U_1+U_2=\operatorname{span}(U_1\cup U_2)$ die Summe von U_1 und U_2.

b) Speziell heißt $U_1+U_2=\operatorname{span}(U_1\cup U_2)$ „direkte Summe“, wenn zusätzlich gilt $U_1\cap U_2=\{0\}$.

Korollar 2 (Dimensionssatz für zueinander komplementäre Untervektorräume).

$$U_1,U_2\text{ *zueinander komplementär* }\Rightarrow\dim U_1+\dim U_2=\dim V$$

Beweis. ✓ □

Korollar 3 (Dimensionssatz für Hyperebenen).

$$[U_1\not\subseteq U_2\text{ und }\dim U_2=\dim V-1]\Rightarrow\dim(U_1\cap U_2)=\dim U_1-1$$

Beweis.

I. $U_1+U_2=V$, denn:
Sei B_2 Basis von U_2. Dann $\sharp B_2=n-1$, wobei $n:=\dim V$. Wähle $u\in U_1\setminus U_2$ und setze $B:=B_2\cup\{u\}$. Dann ist $\sharp B=(n-1)+1=n$.

Zudem ist B linear unabhängig: Sei

$$0=\sum_{v\in B}k(v)v=\left(\sum_{v\in B_2}k(v)v\right)+k(u)u.$$

Im Fall $k(u)\neq 0$ ist

$$u=\sum_{v\in B_2}\big(-k(u)^{-1}k(v)\big)v\in U_2\ \lightning.$$

Also muß eintreten: $k(u)=0$. Wegen der linearen Unabhängigkeit von B_2 erzwingt die verbleibende Darstellung $0=\sum_{v\in B_2}k(v)v$, daß gilt $k(v)=0$ für alle $v\in B_2$.

Zusammen: B Basis von V und $V=\operatorname{span}B\subseteq\operatorname{span}(U_1\cup U_2)=U_1+U_2\subseteq V$. Also $U_1+U_2=V$.

II. Nun aus Dimensions-Satz:

$$n=\dim U_1+(n-1)-\dim(U_1\cap U_2)$$

Hieraus folgt die Behauptung.

□

16. 12. 2003

3.3.4 Faktorraum

Sei K Körper, V endlichdimensionaler K-Vektorraum, U Untervektorraum von V.
Definiere eine Relation auf V durch

$$R:=\{(x,y)\in V\times V|x-y\in U\}$$

Gemäß Übungsaufgabe 29 ist R Äquivalenzrelation mit Äquivalenzklasse

$$A(x)=\{x+u|u\in U\}=:x+U,$$

genannt **„Nebenklasse von x modulo U“**, **„der um den Vektor x verschobene (translatierte) Untervektorraum U“**, **„die zu U parallele Menge durch x“**.

Warnung. Aus $x\neq y$ folgt nicht immer, daß $x+U\neq y+U$.

Entwarnung. Es gilt $\forall x,y\in V$:

(i) $x+U=y+U\Leftrightarrow A(x)=A(y)\Leftrightarrow(x,y)\in R\Leftrightarrow x-y\in U$

(ii) $x+U\neq y+U\Leftrightarrow x-y\notin U$

Definition. $V/U:=\{x+U|x\in V\}\subseteq\mathfrak{P}(V)$ heißt **„Faktorraum von V modulo U“**, **„System aller Nebenklassen von U“**.

Bemerkung. Dies kann wieder zu einem K-Vektorraum gemacht werden (siehe Übungsaufgabe 32).

4 Anwendungen von Vektorräumen

4.1 Affine Geometrien

Definition. Ein **„affiner Raum“** (P, G, I) ist ein Tripel mit den folgenden Eigenschaften:

(0) P ist eine Menge („Punkte“)
G ist eine Menge („Geraden“)
$I \subseteq P \times G$ („Inzidenzrelation“)

Interpretation: $(A, g) \in I$ bedeutet anschaulich, daß der Punkt A auf der Geraden g liegt.

(VA) Verbindungsaxiom:

$$\forall A, B \in P : A \neq B \Rightarrow [\exists! g \in G : (A, g) \in I \wedge (B, g) \in I]$$

Bemerkung. Diese eindeutig bestimmte Gerade wird mit AB bezeichnet.

(PA) Parallelenaxiom: Es gibt eine Äquivalenzrelation $\parallel$ („parallel“) auf G so, daß gilt:

$$\forall g \in G \forall A \in P \exists! h \in G : g \parallel h \wedge (A, h) \in I$$

Bemerkung. h heißt „die Parallele zu g durch A“.

(DA) Dreiecksaxiom: Seien $A, B, C \in P$ Punkte, die *nicht* auf einer gemeinsamen Geraden liegen und seien $\tilde{A}, \tilde{B} \in P$ Punkte mit $\tilde{A}\tilde{B} \parallel AB$. Dann treffen sich die Parallele zu AC durch $\tilde{A}$ und die Parallele zu BC durch $\tilde{B}$ in einem Punkt $\tilde{C}$.

Hauptbeispiel. Sei K Körper und V ein K-Vektorraum.

$$\begin{aligned} \text{Setze} \quad P &:= V \\ \mathcal{U}_1(V) &:= \{U \subseteq V | U \text{ Untervektorraum } \textbf{und } \dim U = 1\} \\ G &:= \{x + U | x \in V \textbf{ und } U \in \mathcal{U}_1(V)\} \\ I &:= \{(v, g) \in P \times G | v \in g\} \end{aligned}$$

Dann ist $A(V) := (P, G, I)$ ein affiner Raum. Für den allgemeinen Fall siehe Beutelspacher S. 89f. Hier speziell für Zeichenebene $V = \mathbb{R}^2$.

I. Sei $m \in \mathbb{R}$ und $b \in \mathbb{R}$. Die „Gerade mit Steigung m und Achsenabschnitt b“ ist die Menge der Lösungen (x, y) der „Geradengleichung“ $y = mx + b$:

$$\begin{aligned} g &= \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \middle| x \in \mathbb{R} \textbf{ und } y = mx + b \right\} \\ &= \left\{ \begin{pmatrix} x \\ mx + b \end{pmatrix} \middle| x \in \mathbb{R} \right\} \\ &= \begin{pmatrix} 0 \\ b \end{pmatrix} + \left\{ x \begin{pmatrix} 1 \\ m \end{pmatrix} \middle| x \in \mathbb{R} \right\} \\ &= \begin{pmatrix} 0 \\ b \end{pmatrix} + \operatorname{span} \begin{pmatrix} 1 \\ m \end{pmatrix} \end{aligned}$$

Diese Geraden sind die Nebenklassen von $\operatorname{span} \binom{1}{m}$.

Bemerkung. Im Fall $m = 0$ ist $\operatorname{span} \binom{1}{m}$ die „x-Achse“.
Im Fall $m \neq 0$ gilt $\operatorname{span} \binom{1}{m} = \operatorname{span} \binom{m^{-1}}{1}$ („geneigte Gerade“).
Dies legt den Zusatzfall $m \to \infty$ nahe: $\operatorname{span} \binom{0}{1}$, die „$y$-Achse“. Die Nebenklassen der y-Achse sind ebenfalls Geraden des affinen Raumes: $g = \binom{a}{0} + \operatorname{span} \binom{0}{1}$.

Alle diese Geraden sind von der Form $g = v + \operatorname{span} u$ mit $u, v \in \mathbb{R}^2, u \neq 0$.

II. Umgekehrt sei $v + \operatorname{span} u$ gegeben mit $u \neq 0$.

Im Fall $u_1 \neq 0$ setze $m := \frac{u_2}{u_1}$ und $b := v_2 - mv_1$. Dann:

$$\begin{aligned} \operatorname{span} \begin{pmatrix} 1 \\ m \end{pmatrix} &= \left\{ x \begin{pmatrix} 1 \\ m \end{pmatrix} \middle| x \in \mathbb{R} \right\} \underset{\tilde{x} := u_1 \cdot x}{=} \left\{ \begin{pmatrix} \tilde{x} \cdot 1 \\ \tilde{x} \cdot m \end{pmatrix} \middle| \tilde{x} \in \mathbb{R} \right\} \\ &= \operatorname{span} \begin{pmatrix} u_1 \\ u_2 \end{pmatrix} = \operatorname{span} u \end{aligned}$$

und

$$v - \begin{pmatrix} 0 \\ b \end{pmatrix} = \begin{pmatrix} v_1 \\ v_2 - v_2 + mv_1 \end{pmatrix} = v_1 \begin{pmatrix} 1 \\ m \end{pmatrix} \in \operatorname{span} u$$

also $v + \operatorname{span} u = \binom{0}{b} + \operatorname{span} \binom{1}{m}$.

Im Fall $u_1 = 0$ folgt $v + \operatorname{span} u = \binom{v_1}{0} + \operatorname{span} \binom{0}{1}$.

I und II zusammen: Die Geraden der Schule sind genau die Nebenklassen $v + \operatorname{span} u$ (mit $u, v \in \mathbb{R}^2$ und $u \neq 0$) der linearen Algebra.

Zu VA: Gegeben seien $v, w \in \mathbb{R}^2$ mit $v \neq w$.

Gesucht ist ein eindimensionaler Untervektorraum U mit $v + U = w + U$. Dann muß gelten: $v - w \in \mathbb{U}$; wegen $\dim U = 1$ folgt $U = \operatorname{span}(v - w)$.

In Worten: Die Gerade durch v und w ist $w + \operatorname{span}(v - w)$.

Zu PA: Die „Parallelenrelation“ auf G sei definiert durch

$$x + U \parallel \tilde{x} + \tilde{U}, \text{ falls } U = \tilde{U}$$

Bei gegebenem Punkt $v \in P$ und Gerade $x + U \in G$ ist $v + U \parallel x + U$ und $v \in v + U$. Wenn zusätzlich $v \in y + U$, dann $\{v\} \in (v + U) \cap (y + U)$ und der nichtleere Durchschnitt erzwingt $v + U = y + U$, d. h. Eindeutigkeit.

Zu DA: Die Punkte $A, B, C, \tilde{A}, \tilde{B}$ seien gegeben durch die Vektoren $u, v, w, \tilde{u}, \tilde{v}$.

Aus $\tilde{A}\tilde{B} \parallel AB$ und $AB = u + \operatorname{span}(v - u)$ folgt $\tilde{A}\tilde{B} = \tilde{u} + \operatorname{span}(v - u)$.

Wegen $\tilde{B} \in \tilde{A}\tilde{B}$ existiert $k \in K$ mit $\tilde{B} = \tilde{u} + k(v - u)$. Die Parallele zu AC durch $\tilde{A}$ ist $\tilde{u} + \operatorname{span}(w - u)$. Die Parallele zu BC durch $\tilde{B}$ ist $\tilde{u} + k(v - u) \operatorname{span}(w - v)$. Der Punkt $\tilde{C} := \tilde{u} + k(w - u) = \tilde{u} + k(v - u) + k(w - v)$ liegt offenbar auf beiden Geraden.

4.2 Lineare Gleichungssysteme

8. 1. 2004

Sei K ein Körper.

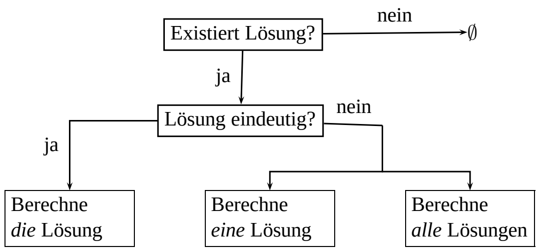
4.2.1 Problemstellung

Sei $m, n \in \mathbb{N}$. Für $i = 1, \ldots, m$ und $j = 1, \ldots, n$ sei $a_{ij} \in K$. Sei $b_1, \ldots, b_m \in K$.

Problem: Existieren Skalare $x_1, \ldots, x_n \in K$ mit

$$\begin{aligned}
a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\
a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\
\vdots \qquad\qquad\qquad & \quad \vdots \\
a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m \qquad ?
\end{aligned}$$

Programm:



Was hat dieses Problem mit K-Vektorräumen zu tun? Offenbar

$$b := \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in K^m \qquad \text{„Vektor der rechten Seiten“}$$

$$\text{und} \quad x := \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^n \qquad \text{„Lösungsvektor“.}$$

Die **„Koeffizienten“** a_{ij} werden zu einer Matrix A (siehe 3.2.3 auf Seite 35) zusammengefaßt und das Gleichungssystem kurz geschrieben als $Ax = b$ mittels Matrizenmultiplikation:

4.2.2 Matrizenmultiplikation

Gegeben $A = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix} \in K^{m \times n}$.

$K^{m \times n}$ ist ein K-Vektorraum, besitzt also eine Matrizenaddition und eine Skalarmultiplikation. Zusätzlich gibt es eine Matrizenmultiplikation. Sei dazu

$$B = \begin{pmatrix} b_{11} & \ldots & b_{1s} \\ \ldots & \ldots & \ldots \\ b_{r1} & \ldots & b_{rs} \end{pmatrix} \in K^{r \times s}.$$

Definition. Falls $n = r$, so ist das **„Matrizenprodukt“** $C := AB \in K^{m \times s}$ definiert durch

$$\boxed{c_{iv} := \sum_{j=1}^{n} a_{ij} b_{jv} \quad \text{für} \quad \begin{matrix} i = 1, \ldots, m \\ v = 1, \ldots, s \end{matrix}}$$

also durch die Summe aller gemischten Produkte der i-ten Zeile von A und der v-ten Spalte von B.

Beispiel. (für $K = \mathbb{R}$)

a) $\begin{pmatrix} 1 & 0 & 5 \\ 3 & 2 & 7 \end{pmatrix} \begin{pmatrix} 2 \\ 4 \\ -1 \end{pmatrix} = \begin{pmatrix} -3 \\ 7 \end{pmatrix}$

b) $\begin{pmatrix} 1 & 0 & 6 & 6 \end{pmatrix} \begin{pmatrix} 1 \\ 7 \\ 8 \\ 9 \end{pmatrix} = (103) = 103$ (skalar: Sonderfall)

c) $\begin{pmatrix} 1 \\ 7 \\ 8 \\ 9 \end{pmatrix} \begin{pmatrix} 1 & 0 & 6 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 6 & 6 \\ 7 & 0 & 42 & 42 \\ 8 & 0 & 48 & 48 \\ 9 & 0 & 54 & 54 \end{pmatrix}$

Offenbar impliziert die Existenz beider Produkte AB und BA nur $n = r$ und $s = m$. Also ist $AB \in \mathbb{R}^{m\times m}$ und $BA \in \mathbb{R}^{n\times n}$.

d) Selbst im Fall $m = n = r = s$ kann gelten $AB \neq BA$. Zum Beispiel
$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.
Matrizenmultiplikation ist i. a. *nicht* kommutativ.

e) $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$
Matrizenmultiplikation ist i. a. *nicht* nullteilerfrei.

Zurück zum Thema: $Ax \in K^m$ ist wohldefiniert.
Da wir x (noch) nicht kennen, betrachten wir Ax als Abbildung mit A fest und x variabel:

$$A: \quad \begin{aligned} K^n &\to K^m \\ x &\mapsto Ax \end{aligned}$$

Satz (über Matrizenmultiplikation als lineare Abbildung). *Sei $A \in K^{m\times n}$. Dann gilt:*

(i) $\forall x \in K^n \forall k \in K : A(kx) = k(Ax)$

(ii) $\forall x, y \in K^n : A(x + y) = (Ax) + (Ay)$

(iii) $\forall F \in \mathcal{F}(K^n)\, \forall k \in K^F : A\left(\sum_{x\in F} k(x)x\right) = \sum_{x\in F} k(x)(Ax)$
In Worten: Das Bild einer linearen Kombination ist gleich der linearen Kombination der Bilder.

Beweis.

(i) Sei $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ und $k \in K$ gegeben.

Dann $kx = \begin{pmatrix} kx_1 \\ \vdots \\ kx_n \end{pmatrix}$ und $A(kx) = \begin{pmatrix} \sum_{j=1}^n a_{1j}kx_j \\ \vdots \\ \sum_{j=1}^n a_{mj}kx_j \end{pmatrix} \underset{(*)}{=} k \begin{pmatrix} \sum_{j=1}^n a_{1j}x_j \\ \vdots \\ \sum_{j=1}^n a_{mj}x_j \end{pmatrix} = k(Ax)$.

Die Gleichheit (*) gilt wegen $a_{ij}kx_j \underset{\text{(KM)}}{=} ka_{ij}x_j$ und wegen DAM und der Definition der Skalarmultiplikation.

(ii) Sei $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ und $x = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ gegeben. 13. 1. 2004

Dann $x + y = x = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}$ und

$$A(x+y) = \begin{pmatrix} \sum_{j=1}^n a_{1j}(x_j + y_j) \\ \vdots \\ \sum_{j=1}^n a_{mj}(x_j + y_j) \end{pmatrix} \underset{\text{DAM, KA}}{=} \begin{pmatrix} \left(\sum_{j=1}^n a_{1j}x_j\right) + \left(\sum_{j=1}^n a_{1j}y_j\right) \\ \vdots \\ \left(\sum_{j=1}^n a_{mj}x_j\right) + \left(\sum_{j=1}^n a_{mj}y_j\right) \end{pmatrix} = Ax + Ay.$$

(iii) Die Behauptung folgt aus (i) und (ii).

□

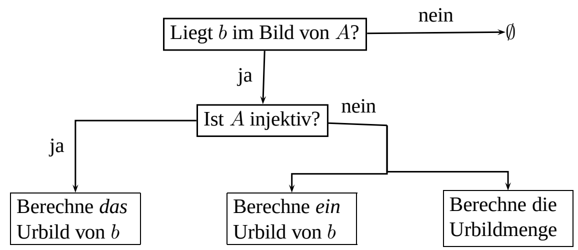
Bemerkung.

1. Die Abbildung $x \mapsto Ax$ ist also ein Vektorraumhomomorphismus von K^n ins K^m.

2. Vektorraumhomomorphismen heißen auch **„lineare Abbildungen“**, weil sie mit linearen Kombinationen so harmonieren wie in (iii).

3. Um die Interpretation von Ax als Abbildung zu betonen, müßte man schreiben $A(x)$, tut man aber nicht.

4. Das Programm zum Studium der Gleichung $Ax = b$ aus Kapitel 4.2.1 auf Seite 57 läßt sich jetzt so präzisieren:



4.2.3 Lösbarkeit

oder: Liegt die rechte Seite b im Bild von A?
Dazu betrachte die Lösungsmenge:

Definition.

(i) $L(A, b) := \{x \in K^n | Ax = b\}$ **„Lösungsmenge“**

(ii) Man nennt ein lineares Gleichungssystem $Ax = b$ **„homogen“**, falls $b = 0$ und **„inhomogen“**, falls $b \neq 0$.

Bemerkung. Zukünftig oft „lineare Gleichung“ statt „lineares Gleichunsgssystem“.

Satz (Struktursatz). *Sei $A \in K^{m \times n}$, $b \in K^m$, $b \neq 0$. Dann gilt:*

(i) $L(A, 0)$ *ist Untervektorraum von* K^n.

(ii) $L(A, b) \neq \emptyset \Rightarrow \forall x \in L(A, b) : L(A, b) = x + L(A, 0)$

Bemerkung.

a) Es gilt immer $L(A, 0) \neq \emptyset$. Aber $L(A, b) = \emptyset$ ist möglich.

b) (ii) in Worten: Alle Lösungen der inhomogenen Gleichung erhält man als eine spezielle Lösung plus allen Lösungen der homogenen Gleichung.

Beweis.

(i) Mit Untervektorraum-Kriterium aus Kapitel 3.3.1 auf Seite 39:

- $0 \in L(A, 0)$, denn $A0 = 0$
- $\forall x, \tilde{x} \in L(A, 0) : x - \tilde{x} \in L(A, 0)$, denn $A(x - \tilde{x}) = (Ax) - (A\tilde{x}) = 0 - 0 = 0$
- $\forall k \in K \forall x \in L(A, 0) : kx \in L(A, 0)$, denn $A(kx) = k \cdot 0 = 0$

(ii) Sei $x \in L(A, b)$. Dann einerseits $L(A, b) \subseteq x + L(A, 0)$, denn für $\tilde{x} \in L(A, b)$ ergibt sich $\tilde{x} = x + (\tilde{x} - x) \in x + L(A, 0)$, denn $A(x - \tilde{x}) = (Ax) - (A\tilde{x}) = b - b = 0$.

Andererseits gilt $x + L(A, 0) \subseteq L(A, b)$, denn für $\tilde{x} \in L(A, 0)$ gilt $A(x + \tilde{x}) = (Ax) + (A\tilde{x}) = b + 0 = b$.

□

Zur Motivation der Definition des „Rangs“ betrachte:

$$Ax \underset{\text{Def.}}{=} \begin{pmatrix} \sum_{j=1}^n a_{1j} x_j \\ \vdots \\ \sum_{j=1}^n a_{mj} x_j \end{pmatrix}$$

Dies betont die Zeilen von A.

Alternativ sei $v_j := \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}$ die j-te Spalte von A (für $j = 1, \dots, n$). Damit folgt:

$$\sum_{j=1}^n x_j v_j = \begin{pmatrix} \sum_{j=1}^n x_j a_{1j} \\ \vdots \\ \sum_{j=1}^n x_j a_{mj} \end{pmatrix} = Ax$$

Das heißt, Ax ist die lineare Kombination der Spalten von A mit Koeffizienten gegeben durch x.

Die Schreibweise $A = v_1 | \dots | v_n$ bedeutet, daß A die Spalten v_j besitzt.

Satz. $\operatorname{Bild}(A) = \operatorname{span}\{v_1, \dots, v_n\}$

Beweis.

$$\begin{aligned} \operatorname{Bild}(A) = A(K^n) = \{Ax | x \in K^n\} &= \left\{ \sum_{j=1}^n x_j v_j \,\middle|\, x_1, \dots, x_n \in K \right\} \\ &= \operatorname{span}\{v_1, \dots, v_n\} \end{aligned}$$

□

Definition. $\forall A \in K^{m \times n} : \operatorname{Rang}(A) := \dim\big(\operatorname{Bild}(A)\big) = \dim\big(\operatorname{span}\{v_1, \dots, v_n\}\big)$

Beispiel.

a) $\operatorname{Rang}(0) = 0$

b) $\operatorname{Rang}(v) = \begin{cases} 1 \\ 0 \end{cases}$ für $v \begin{cases} \neq 0 \\ = 0 \end{cases} \quad \forall v \in K^m$

c) Sei $e_i := \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \\ 0 \end{pmatrix} \in K^n$ mit der 1 an i-ter Stelle.

Die Matrix $E_n := e_1 | e_2 | \dots | e_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix}$ heißt **„Einheitsmatrix“** oder **„Identität“**. Es gilt $\operatorname{Rang}(E_n) = n$. (Siehe 3.3.1 auf Seite 37)

d) $\operatorname{Rang}\begin{pmatrix} 2 & 0 & 3 \\ 0 & 1 & 6 \\ 8 & -4 & 17 \end{pmatrix} = 3$ (ohne Beweis)

15. 1. 2004 Es bezeichne $A|b \in K^{m \times (n+1)}$ die um die rechte Seite b „erweiterte“ Matrix.

Satz (Existenz). *Sei $A \in K^{m \times n}$ und $b \in K^m$. Dann gilt:*

$$L(A, b) \neq \emptyset \Leftrightarrow \operatorname{Rang}(A) = \operatorname{Rang}(A|b)$$

Beweis. Immer gilt $\operatorname{Bild}(A) \subseteq \operatorname{Bild}(A|b)$.

„⇒“
Wegen $L(A,b) \neq \emptyset$ existiert $x \in K^n$ mit $Ax = b$. Daher $b = Ax \in \operatorname{Bild}(A)$ und $\operatorname{Bild}(A|b) \subseteq \operatorname{Bild}(A)$. Zusammen folgt $\operatorname{Bild}(A) = \operatorname{Bild}(A|b)$ und $\operatorname{Rang}(A) = \operatorname{Rang}(A|b)$.

„⇐“
Aus der Vorbemerkung folgt bei Gleichheit der Ränge auch die Gleichheit der Untervektorräume, also $\operatorname{Bild}(A) = \operatorname{Bild}(A|b)$. Also $b \in \operatorname{Bild}(A) = \{Ax | x \in K^n\}$; das bedeutet: es existiert ein Vektor $x \in K^n$ mit $b = Ax$. Also $L(A,b) \neq \emptyset$. □

Satz (Eindeutigkeit). *Sei $A \in K^{m\times n}$. Dann gilt:*

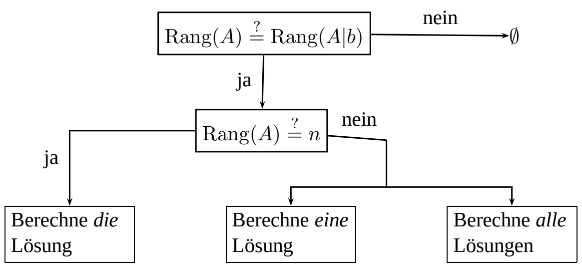
$$A \text{ (als Abbildung } K^n \to K^m\text{) injektiv} \Leftrightarrow \operatorname{Rang}(A) = n$$

Beweis.

$$\begin{aligned}
&A \text{ (als Abbildung } K^n \to K^m\text{) injektiv}\\
&\Leftrightarrow \forall b \in \operatorname{Bild}(A) \exists! x \in K^n : Ax = b\\
&\Leftrightarrow L(A,b) = x + L(A,0)\\
\exists! y \in K^n : 0 = Ay = \sum_{j=1}^{n} y_j v_j \quad &\text{(nämlich } y = 0\text{)}\\
&\Leftrightarrow \{v_1, \ldots, v_n\} \text{ linear unabhängig}\\
&\Leftrightarrow \operatorname{Rang}(A) = n
\end{aligned}$$

□

Das Programm zum Studium von $Ax = b$ sieht jetzt so aus:



4.2.4 Numerische lineare Algebra

Jede Matrix $A \in K^{m\times n}$ kann man natürlich auch nach ihren Zeilen $z_1, \ldots, z_n$ unterteilen:

$$A = \underbrace{v_1|\ldots|v_n}_{\substack{\text{Spaltenvektoren}\\ \in K^m}} = \underbrace{\begin{array}{c} z_1 \\ \hline \vdots \\ \hline z_m \end{array}}_{\substack{\text{Zeilenvektoren}\\ \in K^{1\times n} = K^n}}$$

Satz (Rangsatz I). $\operatorname{Rang}(A) = \dim(\operatorname{span} z_1, \ldots, z_m)$
In Worten: (Spalten-)Rang ist gleich Zeilenrang.

Beweis.

I. Wenn die letzte Spalte eine lineare Kombination der anderen Spalten ist: $v_n = \sum_{j=1}^{n-1} \tilde{k}_j v_j$, dann ist der Zeilenrang mit und ohne letzte Spalte derselbe. Das heißt in

$$v_1|\ldots|v_{n-1}|\sum_{j<n} \tilde{k}_j v_j = \begin{array}{c} z_1|v_{n1} \\ \hline \vdots \\ \hline \underbrace{z_m}_{\in K^{n-1}}|v_{nm} \end{array}$$

gilt $\forall k_1, \ldots, k_m \in K$:

$$\sum_{i=1}^{m} k_i (z_i | v_{ni}) = 0 \Leftrightarrow \sum_{i=1}^{m} k_i z_i = 0.$$

Denn „⇒“ ✓ und „⇐“:

$$\sum_{i=1}^{m} k_i v_{ni} = \sum_{i=1}^{m} k_i \sum_{j<n} \tilde{k}_j \underbrace{v_{ji}}_{=z_{ij}} = \sum_{j<n} \tilde{k}_j \underbrace{\left(\sum_{i=1}^{m} k_i z_{ij}\right)}_{=0 \text{ nach Vor.}} = 0$$

II. Durch Entfernen von Spalten, die lineare Kombinationen der anderen Spalten sind und durch Entfernen von Zeilen, die lineare Kombinationen der anderen Zeilen sind, entsteht dann eine neue Matrix $B \in K^{r\times c}$ mit $\operatorname{Rang}(A) = \operatorname{Rang}(B) = c$ und $c \geq r$, sowie $\operatorname{Zeilenrang}(A) = \operatorname{Zeilenrang}(B) = r$ und $r \geq c$. Somit folgt $\operatorname{Rang}(A) = c = r = \operatorname{Zeilenrang}(A)$.

□

Satz (Rangsatz II). *A vererbt seinen Rang an $T(A)$, wenn $T(A)$ durch eine der folgenden Transformationen aus A hervorgeht:*

- *Vertauschung zweier Zeilen (bzw. Spalten)*

- *Skalierung einer Zeile (bzw. Spalte) mit $k \neq 0$*
- *Addition einer skalierten Zeile (bzw. Spalte) zu einer anderen Zeile (bzw. Spalte)*

„elementare Zeilen-/Spaltenumformungen“

Beweis. Klar. □

Gaußscher Algorithmus siehe Beutelspacher, S. 102ff

5 Lineare Abbildungen

5.1 Grundlagen

Wir haben eine Matrix $A \in K^{m \times n}$ auch als Abbildung aufgefaßt von K^n in K^m. Neben den sehr speziellen Vektorräumen vom Typ K^n gibt es noch viele andere Vektorräume (siehe 3.2 auf Seite 34). Dafür allgemein:

Sei K Körper. Seien V und W K-Vektorräume.

Definition. Eine Abbildung $f : V \to W$ heißt **„linear“**, **„Vektorraum-Homomorphismus“**, falls

(i) $\forall k \in K \forall v \in V : f(kv) = k \cdot f(v)$

(ii) $\forall v, \tilde{v} \in V : f(v + \tilde{v}) = f(v) + f(\tilde{v})$.

20. 1. 2004 **Satz.** *Sei $f : V \to W$ linear. Dann gilt:*

$$\forall F \in \mathcal{F}(V) \forall k \in K^F : f\left(\sum_{v \in F} k(v)v\right) = \sum_{v \in F} k(v)f(v)$$

Beweis. ✓ □

Satz. *Sei $f : V \to W$ linear. Dann ist $\mathrm{Bild}(f) := f(V) = \{f(v) | v \in V\}$ Untervektorraum von W.*

Beweis.

$$\begin{aligned} 0 = f(0) &\in \mathrm{Bild}(f) ✓ \\ kf(v) = f(kv) &\in \mathrm{Bild}(f) ✓ \\ f(v) - f(\tilde{v}) = f(v - \tilde{v}) &\,\mathrm{Bild}(f) ✓ \end{aligned}$$

□

Beispiel.

a) Die „Nullabbildung“ $f : V \to W$ mit $\forall v \in V : f(v) = 0$ ist linear. Sie ist die einzige lineare Abbildung (von V nach W), die konstant ist.

b) Die „Identität“ $f : V \to V$ mit $\forall v \in V : f(v) = v$ ist linear.

c) Sei $k_0 \in K$ fest vorgegeben. Die „Skalierung“ $f : V \to W$ mit $\forall v \in V : f(v) = k_0 v$ ist linear. Für $K = \mathbb{R}$ spricht man auch von Streckung ($k_0 > 1$), bzw. von Stauchung ($k_0 \in (0, 1)$).

d) Seien U_1 und U_2 zueinander komplementäre Untervektorräume von V. Die **„Projektion** (auf U_1 entlang U_2)**“** $f : V \to V$ mit $\forall v \in V : v = \underbrace{u_1}_{\in U_1} + \underbrace{u_2}_{\in U_2} \Rightarrow f(v) = u_1$ ist linear.

Beweis.

I. kv hat Zerlegung $ku_1 + ku_2$, daher ist $f(kv) = ku_1 = kf(v)$.

II. Für zwei Vektoren $v, \tilde{v}$ mit Zerlegungen $v = u_1 + u_2$, $\tilde{v} = \tilde{u}_1 + \tilde{u}_2$ ist $v + \tilde{v} = (u_1 + \tilde{u}_1) + (u_2 + \tilde{u}_2)$ und damit $f(v + \tilde{v}) = u_1 + \tilde{u}_1 = f(v) + f(\tilde{v})$

□

Dabei gilt $\mathrm{Bild}(f) = U_1$.

Warnung. Es ist auch möglich, die Abbildung $g : V \to U_1$ mit $\forall v \in V : g(v) = u_1$ als Projektion zu bezeichnen.

Beispielsweise ist $f : \mathbb{R}^3 \to \mathbb{R}^3$ mit $f\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix} = \begin{pmatrix}x_1\\x_2\\0\end{pmatrix}$ eine Projektion.

Alternativ $g : \mathbb{R}^3 \to \mathbb{R}^2$ mit $g\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix} = \begin{pmatrix}x_1\\x_2\end{pmatrix}$.

e) Vorgriff: Sei $K = \mathbb{R}$ und $v_0 \in V$ fest.

Das **„Differential“**, die **„Ableitung“** ist linear, $D_{v_0}(f) \equiv$ Ableitung in v_0 von f, denn:

$$\begin{array}{lll} & kf \text{ ist differenzierbar} & \text{und } D_{v_0}(kf) = kD_{v_0}(f) \\ \text{und} & \underbrace{f + \tilde{f} \text{ ist differenzierbar}}_{\substack{\text{Vektorraumstruktur der Menge aller}\\ \text{differenzierbaren Funktionen } f : V \to \mathbb{R}}} & \text{und } \underbrace{D_{v_0}(f + \tilde{f}) = D_{v_0}(f) + D_{v_0}(\tilde{f})}_{\text{Linearität der Ableitung in } v_0} \end{array}$$

f) Vorgriff: Sei $K = \mathbb{R}$ und $M \subseteq V$ fest.

Das **„Integral“** $\int_M f \mathrm{d}v$ ist linear, denn:

$$\begin{array}{lll} & kf \text{ ist integrierbar} & \text{und } \displaystyle\int_M (kf)\mathrm{d}v = k\int_M f\mathrm{d}v \\ \text{und} & \underbrace{f + \tilde{f} \text{ ist integrierbar}}_{\substack{\text{Vektorraumstruktur der Menge aller}\\ \text{integrierbaren Funktionen } f : V \to \mathbb{R}}} & \text{und } \underbrace{\displaystyle\int_M (f + \tilde{f})\mathrm{d}v = \int_M f\mathrm{d}v + \int_M \tilde{f}\mathrm{d}v}_{\text{Linearität der Integration über die Menge } M} \end{array}$$

Definition.

(i) $\mathrm{Hom}_K(V, W) := \{f :\to W | f \text{ linear}\}$ **„Vektorraum-Homomorphismen“**

(ii) $\mathrm{Iso}_K(V, W) := \{f \in \mathrm{Hom}_K(V, W) | f \text{ bijektiv}\}$ **„Vektorraum-Isomorphismen“**

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

(iv) $\mathrm{Aut}_K(V) := \mathrm{Iso}_K(V, V)$ **„Vektorraum-Automorphismen“**

Bemerkung. $\mathrm{Hom}_K(V, W)$ ist selber ein K-Vektorraum, denn kf ist die Abbildung $\big(kf\big)(v) = kf(v)$ und somit linear: $kf \in \mathrm{Hom}_K(V, W)$. Interessiert später…

Jetzt Studium einer einzelnen linearen Abbildung f.

Satz (Festlegung durch Basisbilder). *Sei $\{v_1, \ldots, v_n\}$ eine Basis von V. Dann gilt:*

$$\forall w_1, \ldots, w_n \in W \exists! f \in \mathrm{Hom}_K(V, W) : \forall i = 1, \ldots, n : f(v_i) = w_i$$

In Worten: Durch die Bilder einer Basis wird die lineare Abbildung f festgelegt.

Beweis. Sei $w_1, \ldots, w_n$ fest vorgegeben.

I. *Existenz.* Sei $u \in V$ und $u = \sum_{j=1}^n k_j v_j$ die *eindeutige* (siehe Kapitel 3.3.1 auf Seite 37) lineare Kombination von u. Setze $f(u) := \sum_{j=1}^n k_j w_j$. Diese Abbildung ist linear, denn:

$$ku = \sum_{j=1}^n kk_j v_j \qquad \Rightarrow f(ku) = \sum_{j=1}^n kk_j w_j = kf(u)$$

$$u + \tilde{u} = \sum_{j=1}^n k_j v_j + \sum_{j=1}^n \tilde{k}_j v_j \qquad \Rightarrow f(u + \tilde{u}) = \cdots = f(u) + f(\tilde{u})$$

II. *Eindeutigkeit.* Sei $g \in \mathrm{Hom}_K(V, W)$ mit $g(v_j) = w_j$. Dann $\forall u \in V$:

$$f(u) = \sum_{j=1}^n k_j w_j = \sum_{j=1}^n k_j g(v_j) = g(u).$$

□

22. 1. 2004 **Satz (Eigenschaften der Basisbilder).** *Sei $f \in \mathrm{Hom}_K(V, W)$, $\{v_1, \ldots, v_n\}$ eine Basis von V und $B := \{f(v_1), \ldots, f(v_n)\} \subseteq W$. Dann gilt:*

(i) f injektiv $\Leftrightarrow$ B linear unabhängig in W

(ii) f surjektiv $\Leftrightarrow$ B Erzeuger von W

(iii) f bijektiv $\Leftrightarrow$ B Basis von W

Beweis.

(i) „$\Rightarrow$“
Sei f injektiv. Sei $0 = \sum k_j f(v_j)$ gegeben. Da f linear ist, gilt $0 = f\left(\sum k_j v_j\right)$. Daher $\sum k_j v_j = 0$ und $k_1 = \cdots = k_n = 0$. Also B linear unabhängig.

„$\Leftarrow$“
$f(v) = f(u)$ und $v = \sum k_j v_j$ und $u = \sum \tilde{k}_j v_j$.
$\Rightarrow 0 = f(v - u) = \sum (k_j - \tilde{k}_j) f(v_j)$
$\Rightarrow k_1 = \tilde{k}_1, \ldots, k_n = \tilde{k}_n$
$\Rightarrow v = u$

(ii) „$\Rightarrow$“

$$\forall w \in W : w \underset{\boxed{\exists v}}{=} f(v) \underset{\boxed{\exists k_j}}{=} \sum_{j=1}^{n} k_j f(v_j) \in \operatorname{span} B$$

„$\Leftarrow$“

$$\forall w \in W : w = \sum_{j=1}^{n} k_j f(v_j) \underset{\boxed{f \text{ linear}}}{=} f\left(\sum k_j v_j\right) \in \operatorname{Bild}(f)$$

(iii) folgt aus (i) und (ii).

□

Satz (Isomorphiesatz). *Seien V, W endlichdimensionale K-Vektorräume. Dann gilt:*

$$\begin{aligned}\dim V = \dim W &\Leftrightarrow \exists f \in \operatorname{Hom}_K(V,W) : f \textit{ injektiv}\\ &\Leftrightarrow \operatorname{Iso}_K(V,W) \neq \emptyset\end{aligned}$$

In Worten: Je zwei Vektorräume derselben Dimension sind isomorph.

Beweis. $f(v_j) = w_j$, wobei v_j eine Basis von V und w_j eine Basis von W ist. □

Speziell $V = W$:

Satz (Basistransformation). *Sei V ein endlichdimensionaler K-Vektorraum. Dann gilt:*

$$\forall \textit{ Basen } B, \tilde{B} \subseteq V \exists f \in \operatorname{Aut}_K(V) : f(B) = \tilde{B}$$

Beweis. Spezialfall des vorigen Satzes. □

5.2 Matrizendarstellungen linearer Abbildungen

Sei V ein n-dimensionaler K-Vektorraum mit Basis $\{v_1, \dots, v_n\}$ und W ein m-dimensionaler K-Vektorraum mit Basis $\{w_1, \dots, w_m\}$.

Für jede lineare Abbildung $f : V \to W$ (d. h. $f \in \operatorname{Hom}_K(V,W)$) gilt:

$$\forall j = 1, \dots, n \exists! a_{1j}, \dots, a_{mj} \in K : f(v_j) = \sum_{i=1}^{m} a_{ij} w_i$$

Setze $M(f) := \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \in K^{m \times n}$.

Beispiel. $M(\mathrm{id}_V) = \begin{pmatrix} 1 & \dots & 0 \\ 0 & 1 & \dots \\ \dots & \ddots & \dots \\ 0 & \dots & 1 \end{pmatrix} = E_n$

Satz (Darstellungssatz). *Die Abbildung $M : \operatorname{Hom}_K(V,W) \to K^{m \times n}$ ist ein Vektorraum-Isomorphismus.*

Beweis.

I. Sei $k \in K$ und $f \in \operatorname{Hom}_K(V,W)$. Wegen $(kf)(v_j) = k(f(v_j)) = \sum_i k a_{ij} w_i$ gilt $M(kf) = \begin{pmatrix} ka_{11} & \dots & ka_{1n} \\ \dots & \dots & \dots \\ ka_{m1} & \dots & ka_{mn} \end{pmatrix} = kM(f)$

II. Sei $f, \tilde{f} \in \operatorname{Hom}_K(V,W)$. Wegen $(f + \tilde{f})(v_j) = f(v_j) + \tilde{f}(v_j)$ folgt $M(f + \tilde{f}) = M(f) + M(\tilde{f})$.

Also ist M linear.

III. M ist injektiv, denn $f, \tilde{f} \in \operatorname{Hom}_K(V,W)$ mit $M(f) = M(\tilde{f})$ impliziert

$$f(v_j) = \sum_i a_{ij} w_i = \sum_i \tilde{a}_{ij} w_i = \tilde{f}(v_j)$$

für alle $j = 1, \dots, n$. Somit $f = \tilde{f}$ und M ist injektiv.

IV. M ist surjektiv. Denn sei $A \in K^{m \times n}$ gegeben. Dann existiert (genau) eine lineare Abbildung f mit $f(v_j) \sum_{i=1}^{m} a_{ij} w_i$. Also $M(f) = A$.

□

Bemerkung.

a) Ebenso ist die Abbildung

$$c_n := V \to K^n \text{ mit } c_n(u) = \begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix} \text{ falls } u = \sum_{j=1}^{n} k_j v_j$$

ein Vektorraum-Isomorphismus.

b) Wegen

$$f(u) = \sum_j k_j f(v_j) = \sum_j k_j \sum_i a_{ij} w_i = \sum_i \left(\sum_j a_{ij} k_j\right) w_i$$

gilt

$$c_m(f(u)) = \begin{pmatrix} \sum_j a_{1j} k_j \\ \vdots \\ \sum_j a_{mj} k_j \end{pmatrix} = A c_n(u) = M(f) \cdot c_n(u)$$

In Worten: Den Koeffizientenvektor des Bildes $f(u)$ (bzgl. der Basis C) erhält man als Produkt der Matrix $M(f)$ mit dem Koeffizientenvektor von u (bzgl. der Basis B).

Definition. $\operatorname{Rang}(f) := \dim\big(\operatorname{Bild}(f)\big)$

Satz (über den Rang einer linearen Abbildung).

$$\operatorname{Rang}(f) = \operatorname{Rang}\big(M(f)\big)$$

Beweis.

$$\operatorname{Bild}(f) = \{f(u) | u \in V\} = \left\{ \sum k_j f(v_j) \middle| k_1, \dots, k_n \in K \right\} = \operatorname{span}\{f(v_1), \dots, f(v_n)\}$$

ist isomorph zu

$$\operatorname{span}\big\{c_m\big(f(v_1)\big), \dots, c_m\big(f(v_n)\big)\big\} = \operatorname{span}\left\{ \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix}, \dots, \begin{pmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix} \right\}.$$

Also sind die Dimensionen gleich:

$$\operatorname{Rang}(f) = \operatorname{Rang}\big(M(f)\big)$$

$\square$

Satz (Isomorphismen und quadratische Matrizen von vollem Rang). *Sei $n = m$, d. h. $\dim V = \dim W$. Dann gilt:*

$$\forall f \in \operatorname{Hom}_K(V,W) : \underbrace{f \text{ bijektiv}}_{\Leftrightarrow f \in \operatorname{Iso}(V,W)} \Leftrightarrow \operatorname{Rang}\big(\underbrace{M(f)}_{\in K^{n\times n}}\big) = n$$

Beweis.

$$\begin{aligned} f \text{ bijektiv} &\Leftrightarrow \{f(v_1), \dots, f(v_n)\} \text{ Basis von } W \\ &\Leftrightarrow \big\{c_n\big(f(v_1)\big), \dots, c_n\big(f(v_n)\big)\big\} \text{ Basis in } K^n \\ &\Leftrightarrow \operatorname{Rang}\big(M(f)\big) = n \end{aligned}$$

$\square$

Definition. $\operatorname{GL}_k(n) := \{A \in K^{n\times n} | \operatorname{Rang}(A) = n\}$ heißt **„generelle lineare Gruppe** (in $K^{n\times n}$)**“**.

Bemerkung.

a) $\forall A, B \in \operatorname{GL}_K(n) : AB \in \operatorname{GL}_K(n)$, denn

$$\operatorname{Bild}(AB) = \{ABx | x \in K^n\} \underset{\boxed{\operatorname{Rang}(B)=n}}{=} \{Ay | y \in K^n\} \underset{\boxed{\operatorname{Rang}(A)=n}}{=} K^n$$

und somit $\operatorname{Rang}(AB) = n$.

b) $\forall A \in \operatorname{GL}_K(n) : E_n A = A = A E_n$.

In Worten: E_n ist sowohl linksneutral als auch rechtsneutral. Salopp: E_n ist das Einselement der Matrizenmultiplikation.

c) Für $i = 1, 2, 3$ seien V_i K-Vektorräume der Dimension n_i mit Basis B_i. Für die linearen Abbildungen $f_{21} \in \operatorname{Hom}_K(V_1, V_2)$ und $f_{32} \in \operatorname{Hom}_K(V_2, V_3)$ gilt

$$f_{32} \circ f_{21} \in \operatorname{Hom}_K(V_1, V_3)$$

und

$$M_{31}(f_{32} \circ f_{21}) = M_{32}(f_{32}) \cdot M_{21} f(21).$$

d) Sei weiter $V_3 = V_1$. Sei f_{21} bijektiv und speziell dann $f_{12} := f_{21}^{-1}$. Dann gilt:

$$M_{12}\big(f_{21}^{-1}\big) \cdot M_{21}(f_{21}) = M_{11}\big(f_{21}^{-1} \circ f_{21}\big) = M_{11}(\operatorname{id}_{V_1}) = E_{n_1}$$

27. 1. 2004 Das heißt, zu $A := M_{21}(f_{21})$ existiert eine **„inverse Matrix“** B, nämlich $B = M_{12}(f_{21}^{-1})$, mit der Eigenschaft $BA = E_{n_1}$.

Satz. *Sei $A \in \operatorname{GL}_K(n)$. Dann gilt:*

(i) $\forall B \in \operatorname{GL}_K(n) : BA = E_n \Rightarrow AB = E_n$
In Worten: Jede linksinverse Matrix zu A ist auch rechtsinvers.

(ii) $\forall B, C \in \operatorname{GL}_K(n) : (BA = E_n$ ***und*** $CA = E_n) \Rightarrow C = B$
In Worten: Es gibt nur genau eine inverse Matrix zu A.

Beweis.

(i) Sei B gegeben mit $BA = E_n$. Sei D eine (links)inverse Matrix zu B, also $DB = E_n$. Damit gilt:

$$AB = E_n AB = D(BA)B = DE_n B = DB = E_n$$

(ii) $C = CE_n \underset{\text{(i)}}{=} CAB = E_n B = B$

$\square$

Definition. Eine Matrix $A \in K^{n\times n}$ heißt **„invertierbar“**, **„umkehrbar“**, **„regulär“**, **„nichtsingulär“**, falls eine Matrix $A^{-1} \in K^{n\times n}$ existiert mit $A^{-1}A = E_n$.

Bemerkung. A^{-1} heißt „**die** Inverse“ zu A und ist auch rechtsinvers.

Satz. $\forall A \in K^{n\times n}$: *A invertierbar* $\Leftrightarrow A \in \operatorname{GL}_K(n)$

Beweis.

„$\Rightarrow$“
A invertierbar $\Rightarrow \operatorname{Rang}(A^{-1}A) = \operatorname{Rang}(E_n) = n \underset{\text{Ü 43}}{\Rightarrow} \operatorname{Rang}(A) = n \Rightarrow A \in \operatorname{GL}_K(n)$

„$\Leftarrow$“
$A \in \operatorname{GL}_K(n)$ **und** $A = M_{21}(f_{21}) \Rightarrow A^{-1} := M_{12}(f_{21}^{-1})$ erfüllt $A^{-1}A = M(\operatorname{id}) = E_n$ $\square$

In Worten: Die generelle lineare Gruppe $\mathrm{GL}_K(n)$ besteht genau aus den invertierbaren $n \times n$-Matrizen.

Bemerkung.

a) Zur numerischen Berechnung von $A^{-1} = v_1|v_2|\ldots|v_n$:
Die Gleichung $AA^{-1} = E_n$ ist dasselbe wie die n Gleichungen $Av_j = e_j$ für $j = 1,\ldots,n$. Letzteres wird mit GAUSS-Algorithmus gelöst, indem $A|e_j$ transformiert wird zu $E_n|v_j$. Für alle n Gleichungen ergibt sich zusammen: $A|e_1|e_2|\ldots|e_n$ wird transformiert zu

$$E_n|v_1|\ldots|v_n = E_n|A^{-1}.$$

Kurz:

$$A|E_n \text{ wird transformiert zu } E_n|A^{-1}$$

Vergleiche Übung 44.

Wichtig: Die (multiplikative) Inverse A^{-1} wird im GAUSS-Algorithmus nur mittels Skalarmultiplikation und Vektoraddition berechnet.

b) Zusammenfassung zur Matrizenmultiplikation im $K^{n\times n}$:

- assoziativ: $(AB)C = A(BC)$ (i. a. nicht kommutativ, $AB \neq BA$ möglich).
- neutrales Element ist E_n: $E_nA = A$.
- **Aber:** Invertierbare Matrizen gibt es nur in $\mathrm{GL}_K(n) \subsetneq K^{n\times n}$.

Spätere Terminologie:
Die Matrizenmultiplikation macht den Vektorraum $K^{n\times n}$ zu einer (assoziativen und unitären) **„Algebra“**; die Matrizenmultiplikation macht $\mathrm{GL}_K(n)$ zu einer **„Gruppe“**.

5.3 Der Homomorphiesatz

Sei $f : V \to W$ linear. Dann ist $\mathrm{Bild}(f)$ ein Untervektorraum in W.

Definition. $\mathrm{Kern}(f) := \{v \in V | f(v) = 0\}$ heißt **„Kern**[1] (von f)**“**, **„Nullraum“**[2].

Bemerkung.

a) $\mathrm{Kern}(f) = f^{-1}(\{0\})$

b) $\mathrm{Kern}(f)$ ist der Lösungsraum der homogenen Gleichung $f(v) = 0$, d. h. $L(f, 0) = \{v \in V | f(v) = 0\} = \mathrm{Kern}(f)$.

c) $\mathrm{Kern}(f)$ ist Untervektorraum in V.

Satz. $\mathrm{Kern}(f) = \{0\} \Rightarrow f$ *injektiv*

[1] engl. *kernel*
[2] engl. *nullspace*

Beweis.
„$\Rightarrow$“

$$\begin{aligned} f(v) = f(\tilde v) \underset{\text{lin.}}{\Rightarrow} f(v-\tilde v) = 0 \Rightarrow v - \tilde v \in \mathrm{Kern}(f) \\ \underset{\text{Vor.}}{\Rightarrow} v - \tilde v = 0 \Rightarrow v = \tilde v \Rightarrow f \text{ injektiv} \end{aligned}$$

„$\Leftarrow$“

$$v \in \mathrm{Kern}(f) \Rightarrow f(v) = 0 = f(0) \underset{\text{Vor.}}{\Rightarrow} v = 0 \Rightarrow \mathrm{Kern}(f) = \{0\}$$

□

Erinnerung: Der Quotientenraum $V/\mathrm{Kern}(f)$ ist definiert als die Menge der Nebenklassen $\{v + \mathrm{Kern}(f) | v \in V\}$, betrachtet als K-Vektorraum (siehe Übung 32).

Satz (Homomorphiesatz). *Sei* $f \in \mathrm{Hom}_K(V,W)$. *Dann gilt:*

$$\dim\big(V/\mathrm{Kern}(f)\big) = \dim\big(\mathrm{Bild}(f)\big)$$

Beweis.

I. Durch $\phi : V/\mathrm{Kern}(f) \to \mathrm{Bild}(f)$ mit $\phi\big(v + \mathrm{Kern}(f)\big) := f(v)$ wird eine Abbildung definiert, denn wenn $v+\mathrm{Kern}(f) = \tilde v+\mathrm{Kern}(f)$, dann $v-\tilde v \in \mathrm{Kern}(f)$ und $f(v-\tilde v) = 0$ und $f(v) = f(\tilde v)$.

II. ϕ ist linear, denn

$$\phi\Big(k\big(v + \mathrm{Kern}(f)\big)\Big) = \phi\big(kv + \mathrm{Kern}(f)\big) = f(kv) = kf(v) = k\phi\big(v + \mathrm{Kern}(f)\big)$$

und

$$\begin{aligned} \phi\Big(\big(v + \mathrm{Kern}(f)\big) + \big(\tilde v + \mathrm{Kern}(f)\big)\Big) &= \phi\big((v+\tilde v) + \mathrm{Kern}(f)\big) = f(v+\tilde v) \\ &= f(v) + f(\tilde v) = \phi\big(v + \mathrm{Kern}(f)\big) + \phi\big(\tilde v + \mathrm{Kern}(f)\big). \end{aligned}$$

III. ϕ surjektiv: klar.

IV. ϕ injektiv, denn wenn für $v + \mathrm{Kern}(f)$ und $\tilde v + \mathrm{Kern}(f)$ gilt $f(v) = f(\tilde v)$, dann $v - \tilde v \in \mathrm{Kern}(f)$ und $v + \mathrm{Kern}(f) = \tilde v + \mathrm{Kern}(f)$.

V. Es ist also ϕ ein Isomorphismus von $V/\mathrm{Kern}(f)$ auf $\mathrm{Bild}(f)$. Der Isomorphiesatz aus Kapitel 5.1 auf Seite 69 ergibt Gleichheit der Dimensionen.

□

29. 1. 2004 *Beispiel.* $f : \mathbb{R}^2 \to \mathbb{R}$ mit $f\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = x_1 + x_2$

$$\operatorname{Kern}(f) = \left\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \middle| x_1 + x_2 = 0 \right\} = \left\{ \begin{pmatrix} x_1 \\ -x_1 \end{pmatrix} \middle| x_1 \in \mathbb{R} \right\} = \left\{ x_1 \begin{pmatrix} 1 \\ -1 \end{pmatrix} \middle| x_1 \in \mathbb{R} \right\}$$
$$= \operatorname{span}\left\{ \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}$$

Korollar 1. *Sei $f \in \operatorname{Hom}_K(V, W)$. Dann gilt:*

$$\underbrace{\dim\bigl(\operatorname{Kern}(f)\bigr)}_{=:\text{nullity}(f)} + \underbrace{\dim\bigl(\operatorname{Bild}(f)\bigr)}_{=\operatorname{Rang}(f)} = \dim V$$

Beweis.
$$\dim\bigl(\operatorname{Bild}(f)\bigr) = \dim\bigl(V/\operatorname{Kern}(f)\bigr) \underset{\text{Ü. 32(v)}}{=} \dim V - \dim\bigl(\operatorname{Kern}(f)\bigr)$$

□

Korollar 2. *Sei $A \in K^{m \times n}$. Dann gilt:*

$$\dim\bigl(L(A, 0)\bigr) = n - \operatorname{Rang}(A)$$

Beweis. Offenbar $L(A, 0) = \operatorname{Kern}(A)$ und $V = K^n$ und $\dim(K^n) = n$ und $\dim\bigl(\operatorname{Bild}(A)\bigr) = \operatorname{Rang}(A)$. □

Korollar 3. *Sei $\dim V = \dim W =: n$. Dann gilt:*

$$\forall f \in \operatorname{Hom}_K(V, W) : f \textit{ injektiv } \Leftrightarrow f \textit{ surjektiv}$$

Beweis.

$$f \text{ injektiv} \Leftrightarrow \operatorname{Kern}(f) = \{0\} \Leftrightarrow \dim\bigl(\operatorname{Bild}(f)\bigr) = n \Leftrightarrow \operatorname{Bild}(f) = W \Leftrightarrow f \text{ surjektiv}$$

□

5.4 Der Dualraum V^*

Sei V ein n-dimensionaler K-Vektorraum. Wir betrachten $V^* := \operatorname{Hom}_K(V, K)$. Eine Abbildung $f \in V^*$ heißt **„Linearform** (auf V)**“**, d. h. $f : V \to K$ ist linear.

Beispiel.

a) Die Abbildung $f : K^n \to K$ mit $f\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} := x_1 + \cdots + x_n$ ist eine Linearform, die **„Quersumme“**.

b) Sei $B = \{v_1, \ldots, v_n\}$ eine Basis von V. Die Abbildung $f_i : V \to K$, die $u = \sum_{i=1}^n k_i v_i$ auf k_i abbildet, ist eine Linearform, die **„i-te Koeffizientenabbildung“**. Offenbar gilt: $u = \sum_{i=1}^n k_i v_i = \sum_{i=1}^n f_i(u) v_i$.

Satz (Kern einer Linearform). *Sei $f \in V^*$ und $f \neq 0$. Dann gilt:*

$$\dim\bigl(\operatorname{Kern}(f)\bigr) = n - 1$$

Beweis. Sei $u \in V$ mit $f(u) \neq 0$. Dann einerseits $\dim\bigl(\operatorname{Bild}(f)\bigr) = \dim\bigl(\operatorname{span}\{f(v) | v \in V\}\bigr) \geq \dim\bigl(\operatorname{span}\{f(u)\}\bigr) = \dim K = 1$ und andererseits $\dim\bigl(\operatorname{Bild}(f)\bigr) \leq \dim K = 1$. □

Satz (vom Dualraum). *Sei $\dim V = n$ und $\dim W = m$. Dann gilt:*

(i) $\dim\bigl(\operatorname{Hom}_K(V, W)\bigr) = n \cdot m$

(ii) $\dim(V^*) = n$

(iii) *V und V^* sind isomorph.*

Beweis.

(i) Nach dem Darstellungssatz (Kapitel 5.2 auf Seite 70) sind $\operatorname{Hom}_K(V, W)$ und $K^{m \times n}$ isomorph. Aus Isomorphiesatz (Kapitel 5.1 auf Seite 69) folgt $\dim\bigl(\operatorname{Hom}_K(V, W)\bigr) = \dim(K^{m \times n}) = m \cdot n$

(ii) Klar wegen $V^* = \operatorname{Hom}_K(V, K)$ und $m = 1$.

(iii) aus Isomorphiesatz

□

Ansicht der Isomorphie zwischen V und V^* durch „schöne“ Basis von V^* Sei eine Basis $B = \{v_1, \ldots, v_n\}$ in V gegeben. Betrachte die Koeffizientenabbildungen: für alle $i = 1, \ldots, n$: $v_i^* := f_i : V \to K$ mit $v_i^*(u) = k_i$, falls $u = \sum_{i=1}^n k_i v_i$. Wie auch sonst ist v_i^* bestimmt durch ihre Basisbilder:

$$\forall j = 1, \ldots, n : v_i^*(v_j) = \begin{cases} 1 & \text{falls } i = j \\ 0 & \text{falls } i \neq j \end{cases} =: \delta_{ij} \qquad \text{„Kronecker}^3\text{-Delta“}$$

In der Tat ist $B^* := \{v_1^*, \ldots, v_n^*\}$ eine Basis für V^*; sie heißt **„die duale Basis** (zu B)**“**.

Beweis.

I. B^* ist linear unabhängig. Denn sei $\sum_{i=1}^n k_i v_i^* = 0$. Dann $\forall j = 1, \ldots, n$:

$$0 = \underbrace{\left(\sum_{i=1}^n k_i v_i^* \right)}_{\in V^*}(v_j) = \underbrace{\sum_{i=1}^n k_i\bigl(v_i^*(v_j)\bigr)}_{\in K} = \sum_{i=1}^n k_i \delta_{ij} = k_j$$

[3] Leopold Kronecker, 1823–1891

II. B^* ist Erzeuger von V^*. Denn sei $f \in V^*$. Setze $a_i := f(v_i)$ für $i = 1, \ldots, n$ und konstruiere die lineare Abbildung $\sum_{i=1}^n a_i v_i^* : V \to K$. Es gilt $\forall u \in K$:

$$\left(\sum_{i=1}^n a_i v_i^*\right)(u) = \sum_{i=1}^n a_i\big(v_i^*(u)\big) = \sum_{i=1}^n f(v_i)v_i^*(u) = f\left(\sum_{i=1}^n v_i^*(u)v_i\right) = f(u)$$

Also gilt $f \in \operatorname{span} B^*$

□

6 Ringe

Motivation: $\mathbb{Z}$ ist kein Körper wegen fehlender Divisionsmöglichkeit, aber ein Ring.

Definition. Ein Tripel $(R, +, \cdot)$ heißt **„Ring“**, falls

- R Menge, $+ : R \times R \to R$ „Addition“, $\cdot : R \times R \to R$ „Multiplikation“
- und die Addition assoziativ und kommutativ ist, ein Nullelement hat und inverse Elemente
- und die Multiplikation assoziativ ist
- und die Distributivgesetze gelten.

Beispiel.

a) Sei K Körper. Für $n \in \mathbb{N}$ ist $K^{n\times n}$ ein Ring (in Wirklichkeit sogar eine Algebra).

3. 2. 2004 b) Funktionenringe: Gegeben sei Menge X und ein Ring R. R^X ist ein Ring mit der üblichen Addition und Multiplikation für Funktionen:

- $\big(f+g\big)(x) := f(x) + g(x) \quad \forall x \in X$
- $\big(fg\big)(x) := f(x)g(x) \quad \forall x \in X$
- mit Nullelement $n(x) := 0 \quad \forall x \in X$

Insbesondere auch für Körper K ist K^X ein Funktionenring, aber hier sogar mehr: eine Funktionenalgebra[1].

c) Sei R ein kommutativer Ring. Dann definiere **„Potenzfunktionen“** durch $f_j(x) := x^j : R \to R$ durch $x^0 := 1$, $x^j := x \cdot x^{j-1} = x^{j-1} \cdot x$. Eine lineare Kombination von Potenzen heißt „ein Polynom“, d. h. $\exists n \in \mathbb{N} \exists k_0, \ldots, k_n \in R \forall x \in R : f(x) = \sum_{j=0}^n k_j x^j$. Dann ist $R[x] := \operatorname{span}\{x^j | j \in \mathbb{N}_0\}$ ein Ring, genannt der **„Polynomring** (über $\mathbb{R}$)**“**.

Insbesondere für Körper K ist $K[x]$ ein Ring, hier sogar eine Algebra.

[1] Algebra = Vektorraum mit Multiplikation

7 Determinanten

Für Körper K und $n \in \mathbb{N}$ betrachte $K^{n\times n}$.

7.1 Determinantenformen

Gesucht sind Abbildungen $f : K^{n\times n} \to K$ mit drei Eigenschaften:

(ML) $\forall j = 1, \ldots, n \forall z_1, \ldots, z_{j-1}, z_{j+1}, \ldots, z_n \in K^n$:

$$f_{j|z_1,\ldots,z_{j-1},z_{j+1},\ldots,z_n} : K^n \to K$$
$$z_j \mapsto f \begin{pmatrix} — z_1 — \\ \vdots \\ — z_{j-1} — \\ — z_j — \\ — z_{j+1} — \\ \vdots \\ — z_n — \end{pmatrix}$$

ist linear. In Worten: Die Abbildung f ist **„multilinear“** in dem Sinne, daß die „partiellen Abbildungen“ $z_j \mapsto f \begin{pmatrix} — z_1 — \\ \vdots \\ — z_n — \end{pmatrix}$ bei festen Zeilen $i \neq j$ linear sind in z_j.

(GL) $\forall A \in K^{n\times n} \setminus \mathrm{GL}_K(n) : f(A) = 0$

(NB) $f(E_n) = 1$ („Normierungsbedingung“)

Bemerkung.

a) Eine solche Abbildung – falls sie existiert – heißt eine Determinantenform.

b) Die Abbildungen kf mit $k \neq 1$ erfüllen auch (ML) und (GL) aber nicht (NB).

Beispiel. $n = 2$. Auf $K^{2\times 2}$ definiere g durch $g \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} := a_{11}a_{22} - a_{12}a_{21}$. Dann ist g eine Determinantenform, denn

(ML) Mit a_{21}, a_{22} fest, gilt

$$g \begin{pmatrix} ka_{11} & ka_{12} \\ a_{21} & a_{22} \end{pmatrix} = ka_{11}a_{22} - ka_{12}a_{21} = kg \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

und

$$\begin{aligned} g \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ a_{21} & a_{22} \end{pmatrix} &= (a_{11}+b_{11})a_{22} - (a_{12}+b_{12})a_{21} \\ &= g \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + g \begin{pmatrix} b_{11} & b_{12} \\ a_{21} & a_{22} \end{pmatrix}. \end{aligned}$$

$\rightsquigarrow g_{1|a_{21},a_{22}}$ linear. Ebenso folgt, daß g_2 linear.

(GL) $\mathrm{Rang}(A) = 0 \Rightarrow A = 0 \Rightarrow g(0) = 0$
$\mathrm{Rang}(A) = 1 \Rightarrow A = \begin{pmatrix} a_{11} & a_{12} \\ ka_{11} & ka_{12} \end{pmatrix} \Rightarrow g(A) = a_{11}ka_{12} - ka_{11}a_{12} = 0$

(NB) $g \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1 - 0 = 1$

Satz (Determinantenformen und elementare Zeilenumformungen).

Sei $f : K^{n\times n} \to K$ *eine Determinantenform,* $A = \begin{pmatrix} — z_1 — \\ \vdots \\ — z_n — \end{pmatrix} \in K^{n\times n}$, $j \in \{1, \ldots, n\}$ *fest,* $\check{A}_j(v) := \begin{pmatrix} — z_1 — \\ \vdots \\ — z_{j-1} — \\ — v — \\ — z_{j+1} — \\ \vdots \\ — z_n — \end{pmatrix}$. *Dann gilt:*

(i) $\forall k \in K : f\big(\check{A}_j(kz_j)\big) = kf(A)$ ✓

(ii) $\forall k \in K \forall l \neq j : f\big(\check{A}_j(z_j + kz_l)\big) = f\big(\check{A}_j(z_j)\big) + \underbrace{kf\big(\check{A}_j(z_l)\big)}_{=0} = f(A)$ ✓

(iii) $\forall l \neq j$:

$$B := \begin{pmatrix} — z_1 — \\ \vdots \\ — z_{j-1} — \\ — z_l — \\ — z_{j+1} — \\ \vdots \\ — z_{l-1} — \\ — z_j — \\ — z_{l+1} — \\ \vdots \\ — z_n — \end{pmatrix} \Rightarrow f(B) = -f(A)$$

Beweis. (iii)

$$0 = f\begin{pmatrix} \vdots \\ j\text{-te Zeile: } — z_j + z_l — \\ \vdots \\ l\text{-te Zeile: } — z_l + z_j — \\ \vdots \end{pmatrix} = f\begin{pmatrix} \vdots \\ — z_j + z_l — \\ \vdots \\ — z_l — \\ \vdots \end{pmatrix} + f\begin{pmatrix} \vdots \\ — z_j + z_l — \\ \vdots \\ — z_j — \\ \vdots \end{pmatrix}$$

$$= f(A) + 0 + 0 + f(B)$$

□

Satz (Eindeutigkeit). *Seien $f, g : K^{n\times n} \to K$. Dann gilt:* 5. 2. 2004

$$f \text{ Determinantenform } \textbf{und } g \text{ Determinantenform} \Rightarrow f = g$$

Bemerkung. Die damit eindeutig bestimmte Determinantenform heißt „die Determinante“ und wird mit $f =: \det$ bezeichnet.

Beweis.

I. $\forall A \in K^{n\times n} \setminus \mathrm{GL}_K(n) : f(A) \underset{\text{(GL)}}{=} 0 = g(A)$

II. $\forall A \in \mathrm{GL}_K(n)$: Der GAUSS-Algorithmus macht aus $A^{-1}|E_n$ mittels elementarer Zeilenumformungen $E_n|A$. Es gibt also eine Abfolge $B_1 := E_n, B_2, \dots, B_{l-1}, B_l := A$ so, daß B_j aus B_{j-1} durch eine elementare Zeilentransformation hervorgeht. Entlang dieser Abfolge gilt für f und g:

$$f(B_1) = f(E_n) = 1 = g(E_n) = g(B_1) \quad \text{und}$$

(i) Skalarmultiplikation mit $k \neq 0$: $f(B_j) = kf(B_{j-1}) \neq 0$

(ii) Vektoraddition einer skalierten Zeile zu einer anderen: $f(B_j) = f(B_{j-1}) \neq 0$

(iii) Vertauschung zweier Zeilen: $f(B_j) = -f(B_{j-1}) \neq 0$

Also $f(B_2) = \left\{\begin{matrix} k \\ +1 \\ -1 \end{matrix}\right\} f(B_1) = \left\{\begin{matrix} k \\ +1 \\ -1 \end{matrix}\right\} g(B_1) = g(B_2)$

u. s. w. bis $f(A) = \left\{\begin{matrix} k \\ +1 \\ -1 \end{matrix}\right\} f(B_{l-1}) = \left\{\begin{matrix} k \\ +1 \\ -1 \end{matrix}\right\} g(B_{l-1}) = g(A)$.

□

Korollar. $\forall A \in K^{n\times n} : A \in \mathrm{GL}_K(n) \Leftrightarrow \det A \neq 0$

Beweis.

„$\Rightarrow$“

Aus Rückschau auf Beweis oben.

„$\Leftarrow$“

Indirekt: $A \notin \mathrm{GL}_K(n) \underset{\text{(GL)}}{\Rightarrow} \det A = 0$. □

7.2 Permutationen

Sei $n \in \mathbb{N}$ und die Menge $\{1, \dots, n\}$ gegeben.

Definition. Die Menge aller bijektiven Abbildungen von $\{1, \dots, n\}$ auf sich selbst heißt **„symmetrische Gruppe S_n“**. Diese Abbildungen nemmt man **„Permutationen“**.

Also $S_n := \big\{\pi : \{1, \dots, n\} \to \{1, \dots, n\} \bigm| \pi \text{ bijektiv}\big\}$.

Satz (Abzählsatz). $\sharp S_n = n! := 1 \cdot 2 \cdot 3 \dots (n-2)(n-1)n$
($n!$: „n Fakultät“[1])

Beweis. Für die Werte von $\pi(1)$ gibt es n mögliche Werte $j_1 \in \{1, \dots, n\}$. Für $\pi(2)$ gibt es $(n-1)$ mögliche Werte $j_2 \in \{1, \dots, n\} \setminus \{j_1\}$. Danach sind für $\pi(3)$ die Werte $j_3 \in \{1, \dots, n\} \setminus \{j_1, j_2\}$ möglich. Und so weiter… □

Beschreibung einer Permutation mittels Wertetabelle:

n	$\pi(n)$
1	$3 = \pi(1)$
2	$2 = \pi(2)$
3	$4 = \pi(3)$
4	$1 = \pi(4)$

oder

n	1	2	3	4
$\psi(n)$	3	2	1	4

ψ hat „Fixpunkte“ 2 und 4, d. h. $\mathrm{Fix}(\psi) = \{2, 4\}$. Analog $\mathrm{Fix}(\pi) = \{2\}$.

Komposition $\pi \circ \psi$:

n	1	2	3	4
$\pi \circ \psi(n)$	3	2	1	4

mit $\mathrm{Fix}(\pi \circ \psi) = \{2, 3\}$.

Alternative Notation mit „Zyklen“ ist effizienter:

$\pi \leftrightarrow \begin{pmatrix}1 & 3 & 4\end{pmatrix}$ **„3-Zyklus“**, lies: $\pi(1) = 3, \pi(3) = 4, \pi(4) = 1$

$\psi \leftrightarrow \begin{pmatrix}1 & 3\end{pmatrix}$ **„2-Zyklus“** $\equiv$ **„Transposition“**.

$\pi \circ \psi \leftrightarrow \begin{pmatrix}1 & 4\end{pmatrix} = \begin{pmatrix}1 & 3 & 4\end{pmatrix} \circ \begin{pmatrix}1 & 3\end{pmatrix}$, denn für $x = 1, 2, 3, 4$ erhält man

$$\begin{array}{ll} \text{links } \begin{pmatrix}1 & 4\end{pmatrix}(1) = 4 & \text{rechts } \begin{pmatrix}1 & 3 & 4\end{pmatrix} \circ \begin{pmatrix}1 & 3\end{pmatrix}(1) = 4 \\ \text{links } \begin{pmatrix}1 & 4\end{pmatrix}(2) = 2 & \text{rechts } \begin{pmatrix}1 & 3 & 4\end{pmatrix} \circ \begin{pmatrix}1 & 3\end{pmatrix}(2) = 2 \\ \text{links } \begin{pmatrix}1 & 4\end{pmatrix}(3) = 3 & \text{rechts } \begin{pmatrix}1 & 3 & 4\end{pmatrix} \circ \begin{pmatrix}1 & 3\end{pmatrix}(3) = 3 \\ \text{links } \begin{pmatrix}1 & 4\end{pmatrix}(4) = 1 & \text{rechts } \begin{pmatrix}1 & 3 & 4\end{pmatrix} \circ \begin{pmatrix}1 & 3\end{pmatrix}(4) = 1. \end{array}$$

Zyklen brauchen nur $n - \sharp\,\mathrm{Fix}(\pi)$ Speicherplätze.

Speziell für Transpositionen:

$j \neq l$, hat Zyklus $\begin{pmatrix}j & l\end{pmatrix}$

n	$1 \;\dots\; j-1$	j	$j+1 \;\dots\; l-1$	l	$l+1 \;\dots\; n$
$\pi(n)$	fix	l	fix	j	fix

Offenbar gilt $\begin{pmatrix}j & l\end{pmatrix}\begin{pmatrix}j & l\end{pmatrix} = \text{Identität} := \epsilon$, d. h. $\begin{pmatrix}j & l\end{pmatrix}^{-1} = \begin{pmatrix}j & l\end{pmatrix}$.

Satz. *Jeder k-Zyklus ($k > 2$) ist Komposition von Transpositionen.*

[1] engl. *n factorial*

Beispiel. $\begin{pmatrix}1 & 3 & 4\end{pmatrix} = \begin{pmatrix}1 & 3\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix}$

Allgemein:

$$\begin{pmatrix}x_1 & x_2 & x_3 & \dots & x_{l-2} & x_{l-1} & x_l\end{pmatrix} = \begin{pmatrix}x_1 & x_2\end{pmatrix} \circ \begin{pmatrix}x_2 & x_3\end{pmatrix} \circ \dots \circ \begin{pmatrix}x_{l-2} & x_{l-1}\end{pmatrix} \circ \begin{pmatrix}x_{l-1} & x_l\end{pmatrix}$$

Man kann 2-Zyklus expandieren in Nachbartranspositionen.

Beispiel. $\begin{pmatrix}1 & 4\end{pmatrix} = \begin{pmatrix}1 & 3 & 4\end{pmatrix} \circ \begin{pmatrix}1 & 3\end{pmatrix} = \begin{pmatrix}1 & 3\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix} \circ \begin{pmatrix}1 & 3\end{pmatrix}$
weiter $\begin{pmatrix}1 & 3\end{pmatrix} = \begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}2 & 3\end{pmatrix} \circ \begin{pmatrix}1 & 2\end{pmatrix}$
ergibt zusammen $\begin{pmatrix}1 & 4\end{pmatrix} = \begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}2 & 3\end{pmatrix} \circ \begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix} \circ \begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}2 & 3\end{pmatrix} \circ \begin{pmatrix}1 & 2\end{pmatrix}$

Satz. *Jede Transposition ist Komposition einer ungeraden Anzahl von Nachbartranspositionen.*

Beweis.

$$\begin{aligned}\begin{pmatrix}j & l\end{pmatrix} = \begin{pmatrix}j & j+1\end{pmatrix}\begin{pmatrix}j+1 & j+2\end{pmatrix} \cdots \begin{pmatrix}l-2 & l-1\end{pmatrix}\begin{pmatrix}l-1 & l\end{pmatrix}&\\ \begin{pmatrix}l-2 & l-1\end{pmatrix} \cdots \begin{pmatrix}j+1 & j+2\end{pmatrix}\begin{pmatrix}j & j+1\end{pmatrix}&\end{aligned}$$

besteht aus $1 + 2(l - 1 - j)$ Nachbartranspositionen. □

Speziell für Nachbartranspositionen:
$\begin{pmatrix}j & j+1\end{pmatrix}$ hat $1 + 2(j + 1 - 1 - j) = 1$.
Interpretation der Zahl $1 + 2(l - 1 - j)$:

Definition. Sei $\pi \in S_n$.

(i) Ein Paar $\begin{pmatrix}j & l\end{pmatrix} \in \{1, \dots, n\}^2$ heißt **„Fehlstand** (von π)**“**, falls $j < l$ und $\pi(j) > \pi(l)$.

(ii) $f(\pi) := \sharp\left\{\begin{pmatrix}j & l\end{pmatrix} \,\middle|\, \begin{pmatrix}j & l\end{pmatrix} \text{ ist Fehlstand von } \pi\right\}$

Beispiel.

a) $f\left(\begin{pmatrix}j & j+1\end{pmatrix}\right) = 1$, denn

n	$1 \;\dots\; j-1$	j	$j+1$	$\dots\; n$
$\begin{pmatrix}j & j+1\end{pmatrix}$	fix	$j+1$	j	fix

b) $f\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 2 & 4 & 1\end{pmatrix} = 4$, denn $(1,2), \cancel{(1,3)}, (1,4), \cancel{(2,3)}, (2,4), (3,4)$

c) Eine Transposition $\begin{pmatrix}j & l\end{pmatrix}$ mit $j < l$ hat $f\left(\begin{pmatrix}j & l\end{pmatrix}\right) = 1 + 2(l - 1 - j)$.

Im folgenden bezeichne $\tau \in S_n$ stets eine Transposition und $\nu \in S_n$ eine Nachbartransposition. 10. 2. 2004

Definition (Signum-Funktion). $\operatorname{sig} : S_n \to \{-1, +1\}$ ist definiert durch

$$\operatorname{sig}(\pi) := \begin{cases} +1, & \text{falls } f(\pi) \in 2\mathbb{N}_0 \text{ (gerade)} \\ -1, & \text{falls } f(\pi) \in 2\mathbb{N}_0 + 1 \text{ (ungerade)} \end{cases}.$$

Bemerkung.

a) Kurz spricht man von „geraden“ Permutationen, falls $\operatorname{sig}(\pi) = +1$, und von „ungeraden“ Permutationen, falls $\operatorname{sig}(\pi) = -1$.

b) Jede Transposition ist ungerade, d. h. $\operatorname{sig}(\tau) = -1$.

c) Die Identität ϵ ist gerade, d. h. $\operatorname{sig}(\epsilon) = 1$.

Satz. *Seien* $\pi, \sigma \in S_n$ *und* $\pi = \underbrace{\tau_T \circ \dots \circ \tau_1}_{\text{Komposition von Transpositionen}} = \underbrace{\nu_N \circ \dots \circ \nu_1}_{\text{Komposition von Nachbartranspositionen}}$. *Dann gilt:*

(i) $\operatorname{sig}(\pi \circ \sigma) = \operatorname{sig}(\pi) \cdot \operatorname{sig}(\sigma)$

(ii) $\operatorname{sig}(\pi) = (-1)^T = (-1)^N$

(iii) π *gerade* $\Leftrightarrow$ T *gerade* $\Leftrightarrow$ N *gerade*

(iv) π *ungerade* $\Leftrightarrow$ T *ungerade* $\Leftrightarrow$ N *ungerade*

Beweis. (i) und (ii): Sei $\nu = \begin{pmatrix}j & j+1\end{pmatrix}$. Dann gilt:

$$\begin{aligned}(j, j+1) \text{ Fehlstand von } \sigma &\Rightarrow f(\nu \circ \sigma) = f(\sigma) - 1\\ (j, j+1) \text{ kein Fehlstand von } \sigma &\Rightarrow f(\nu \circ \sigma) = f(\sigma) + 1\end{aligned}$$

Zusammen folgt: $\operatorname{sig}(\nu \circ \sigma) = -\operatorname{sig}(\sigma) = \operatorname{sig}(\nu) \cdot \operatorname{sig}(\sigma)$. Daraus für $\tau = \begin{pmatrix}j & l\end{pmatrix}$:

$$\operatorname{sig}(\tau \circ \sigma) \underset{j<l}{=} (-1)^{1+2(l-1-j)} \cdot \operatorname{sig}(\sigma = (-1)\operatorname{sig}(\sigma) = \operatorname{sig}(\tau) \cdot \operatorname{sig}(\sigma)$$

Insbesondere $\operatorname{sig}(\pi) = (-1)^T = (-1)^N$ und $\operatorname{sig}(\pi \circ \sigma) = \operatorname{sig}(\tau_T \circ \dots \circ \tau_1 \circ \sigma) = (-1)^T \operatorname{sig}(\sigma) = \operatorname{sig}(\pi)\operatorname{sig}(\sigma)$.
(iii) und (iv) klar. □

7.3 Leibnizsche Determinantenformel

Satz. *Sei* $n \in \mathbb{N}$ *und* K *ein Körper. Dann ist die Abbildung* $\det : K^{n \times n} \to K$ *mit*

$$\det(A) := \sum_{\pi \in S_n} \operatorname{sig}(\pi) \prod_{i=1}^{n} a_{i\pi(i)}$$

die Determinantenform auf $K^{n \times n}$.

Beispiel. $n = 1$: $S_1 = \{\epsilon\}$, $\det(a) = \operatorname{sig}(\epsilon) \cdot a = a$

$n = 2$: $2! = 2$, $S_2 = \left\{\epsilon, \begin{pmatrix}1 & 2\end{pmatrix}\right\}$,

$$\det\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix} = \operatorname{sig}(\epsilon)a_{11}a_{22} + \operatorname{sig}\begin{pmatrix}1 & 2\end{pmatrix} a_{12}a_{21} = a_{11}a_{22} - a_{12}a_{21}$$

$n=3$: $3! = 6$, $S_3 = \left\{ \underset{+}{\epsilon}, \underset{+}{\begin{pmatrix}1 & 2 & 3\end{pmatrix}}, \underset{+}{\begin{pmatrix}1 & 3 & 2\end{pmatrix}}, \underset{-}{\begin{pmatrix}2 & 3\end{pmatrix}}, \underset{-}{\begin{pmatrix}1 & 3\end{pmatrix}}, \underset{-}{\begin{pmatrix}1 & 2\end{pmatrix}} \right\}$,

$$\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32}$$
$$- a_{11}a_{23}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33}$$

Beweis.

I. Für (ML) ist zu zeigen, daß $\det(A)$ als Funktion der j-ten Zeile $z_j := (a_{j1}, \ldots, a_{jn})$ linear ist. Dazu seien $P_j(h) := \{\pi \in S_n | \pi(j) = h\}$ die Permutationen, die j auf h abbilden. Deren (disjunkte) Vereinigung für $h = 1, \ldots, n$ ergibt S_n, d. h.

$$S_n = \sum_{h=1}^{n} P_j(h).$$

Daraus folgt

$$\det(A) = \sum_{\pi \in S_n} \operatorname{sig}(\pi) \prod_{i=1}^{n} a_{i\pi(i)} = \sum_{h=1}^{n} \underbrace{\sum_{\pi \in P_j(h)} \left[\operatorname{sig}(\pi) \prod_{\substack{i=1 \\ i \neq j}}^{n} a_{i\pi(i)} \right]}_{=: c_h} a_{jh}$$
$$= \sum_{h=1}^{n} c_h a_{jh},$$

was offensichtlich linear ist in z_j.

II. a) Für (GL) ist zu zeigen, daß $\det(A)$ verschwindet, wenn $z_j = \sum_{i \neq j} k_i z_i$ lineare Kombination der anderen Zeile ist. Nach I gilt:

$$\det \begin{pmatrix} - z_1 - \\ \vdots \\ - z_{j-1} - \\ - z_j - \\ - z_{j+1} - \\ \vdots \\ - z_n - \end{pmatrix} = \sum_{i \neq j} k_i \det \underbrace{\begin{pmatrix} - z_1 - \\ \vdots \\ - z_{j-1} - \\ - z_i - \\ - z_{j+1} - \\ \vdots \\ - z_n - \end{pmatrix}}_{\text{Matrix mit 2 gleichen Zeilen}}$$

b) Sei A Matrix mit zwei gleichen Zeilen i und j, d. h. $a_{il} = a_{jl}$ für $l = 1, \ldots, n$. Dazu seien $P_{ij}(l,h) := \{\pi \in S_n | \pi(i) = l, \pi(j) = h\}$ (i $\neq$ j) die Permutationen die i auf l

und j auf h abbilden. Deren (disjunkte) Vereinigung ist

$$S_n = \sum_{l=1}^{n} \sum_{h=1}^{n} P_{ij}(l,h) = \sum_{l=1}^{n-1} \sum_{h=l+1}^{n} \left(P_{ij}(l,h) + \{\pi \circ \tau | \pi \in P_{ij}(l,h)\} \right),$$

wobei $\tau = \begin{pmatrix} i & j \end{pmatrix}$. Daraus

$$\begin{aligned} \det(A) &= \sum_{\pi \in S_n} \operatorname{sig}(\pi) \prod_{i=1}^{n} a_{i\pi(i)} \\ &= \sum_{l=1}^{n-1} \sum_{h=l+1}^{n} \sum_{\pi \in P_{ij}(l,h)} \left[\operatorname{sig}(\pi) \prod_{r=1}^{n} a_{r\pi(r)} + \operatorname{sig}(\pi \circ \tau) \prod_{r=1}^{n} a_{r\pi\circ\tau(r)} \right] \\ &\underset{(*)}{=} \sum_{l=1}^{n-1} \sum_{h=l+1}^{n} \sum_{\pi \in P_{ij}(l,h)} \underbrace{[\operatorname{sig}(\pi) - \operatorname{sig}(\pi)]}_{=0} \prod_{r=1}^{n} a_{r\pi(r)} = 0 \end{aligned}$$

(*) gilt wegen

$$\begin{aligned} r \neq i, j &\Rightarrow a_{r\pi\circ\tau(r)} = a_{r\pi(r)} \\ r = i &\Rightarrow a_{i\pi\circ\tau(i)} = a_{i\pi(j)} = a_{j\pi(j)} \\ r = j &\Rightarrow a_{j\pi\circ\tau(j)} = a_{j\pi(i)} = a_{i\pi(i)} \\ \text{Somit } \prod_{r=1}^{n} a_{r\pi(r)} &= \prod_{r=1}^{n} a_{r\pi\circ\tau(r)}. \end{aligned}$$

III. Für (NB) ist zu zeigen, daß $\det(E_n) = 1$. Dazu $\det(E_n) = \operatorname{sig}(\epsilon) \cdot 1 \cdots 1 + 0 = 1$.

□

12. 2. 2004 **Definition.** Die zu $A = (a_{ij})_{\substack{i=1,\ldots,n \\ j=1,\ldots,n}} \in K^{m \times n}$ **„transponierte Matrix“** A^T ist definiert durch $A^T := (a_{ji})_{\substack{j=1,\ldots,n \\ i=1,\ldots,m}}$.[2]

Beispiel.

a) $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \in \mathbb{R}^{2\times 3}$

$\Rightarrow A^T = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix} \in \mathbb{R}^{3\times 2}$

b) $A = \begin{pmatrix} 7 & 8 \\ 9 & 0 \end{pmatrix} \in \mathbb{R}^{2\times 2}$

$\Rightarrow A^T = \begin{pmatrix} 7 & 9 \\ 8 & 0 \end{pmatrix} \in \mathbb{R}^{2\times 2}$

[2] Andere Schreibweisen: A^t, ${}^tA$, A'

Satz (Invarianz der Determinante unter Transposition).

$$\forall A \in K^{n\times n} : \det(A) = \det\big(A^T\big)$$

Beweis.

$$\det(A) = \sum_{\pi\in S_n} \operatorname{sig}(\pi) \prod_{i=1}^{n} a_{i\pi(i)} \underset{\boxed{\substack{j:=\pi(i)\\ i=\pi^{-1}(j)}}}{=} \sum_{\pi^{-1}\in S_n} \operatorname{sig}\left(\pi^{-1}\right) \prod_{j=1}^{n} a_{\pi^{-1}(j)j}$$

$$\underset{\boxed{\sigma:=\pi^{-1}}}{=} \sum_{\sigma\in S_n} \operatorname{sig}(\sigma) \prod_{j=1}^{n} a_{\sigma(j)j} = \det\big(A^T\big)$$

□

Satz (Multiplikationssatz für Determinanten).

$$\forall A, B \in K^{n\times n} : \det(AB) = \det(A)\det(B)$$

Beweis. Sei B fest.

I. Sei A die Matrix, die in B die Zeilen j und l vertauscht, d. h.

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

mit $a_{jj} = a_{ll} = 0$ und $a_{jl} = a_{lj} = 1$ und 1 auf der restlichen Hauptdiagonalen und 0 sonst. Tatsächlich gilt:

$$A \underbrace{\begin{pmatrix} — z_1 — \\ \vdots \\ — z_j — \\ \vdots \\ — z_l — \\ \vdots \\ — z_n — \end{pmatrix}}_{\equiv B} = \underbrace{\begin{pmatrix} — z_1 — \\ \vdots \\ — z_l — \\ \vdots \\ — z_j — \\ \vdots \\ — z_n — \end{pmatrix}}_{=:\tilde{B}}$$

Es gilt $\det(A) = -1$ und $\det(AB) = \det(\tilde{B}) = -\det(B) = \det(A)\det(B)$.

II. Sei A die Matrix, die die Zeile j in B mit $k \neq 0$ skaliert, d. h.

$$A := \begin{pmatrix} 1 & \cdots & \cdots & \cdots & \cdots \\ \cdots & \ddots & \cdots & 0 & \cdots \\ \cdots & 1 & \cdots & \cdots & \cdots \\ \cdots & \cdots & k & \cdots & \cdots \\ \cdots & \cdots & \cdots & 1 & \cdots \\ \cdots & 0 & \cdots & \ddots & \cdots \\ \cdots & \cdots & \cdots & \cdots & 1 \end{pmatrix}$$

mit $a_{jj} = k$ und 1 auf der restlichen Hauptdiagonalen und 0 sonst. Tatsächlich gilt:

$$A \underbrace{\begin{pmatrix} — z_1 — \\ \vdots \\ — z_j — \\ \vdots \\ — z_n — \end{pmatrix}}_{\equiv B} = \underbrace{\begin{pmatrix} — z_1 — \\ \vdots \\ — kz_j — \\ \vdots \\ — z_n — \end{pmatrix}}_{=:\tilde{B}}$$

Es gilt $\det(A) = k$ und $\det(AB) = \det(\tilde{B}) = k\det(B) = \det(A)\det(B)$.

III. Sei A die Matrix, die in B zur Zeile j das k-fache der Zeile l hinzuaddiert, d. h.

$$A := \begin{pmatrix} 1 & \cdots & \cdots & \cdots & \cdots \\ \cdots & \ddots & \cdots & k & \cdots \\ \cdots & \cdots & \ddots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \ddots & \cdots \\ \cdots & \cdots & \cdots & \cdots & 1 \end{pmatrix}$$

mit 1 auf der Hauptdiagonalen und $a_{jl} = k$ und 0 sonst. Tatsächlich gilt:

$$A \underbrace{\begin{pmatrix} — z_1 — \\ \vdots \\ — z_j — \\ \vdots \\ — z_l — \\ \vdots \\ — z_n — \end{pmatrix}}_{\equiv B} = \underbrace{\begin{pmatrix} — z_1 — \\ \vdots \\ — z_j + kz_l — \\ \vdots \\ — z_l — \\ \vdots \\ — z_n — \end{pmatrix}}_{=:\tilde{B}}$$

Es gilt $\det(A) = 1$ und $\det(AB) = \det(\tilde{B}) = \det(B) = \det(A)\det(B)$.

IV. Sei nun A beliebig, aber mit $\operatorname{Rang}(A) = n$. Dann können wir A^{-1} mit endlich vielen elementaren Zeilentransformationen $T_1, \ldots, T_m$ zu E_n transformieren, denn mit GAUSS-Algorithmus:

$$A^{-1}|E_n \xrightarrow[T_{1,\ldots,m}]{\text{Gauss}} E_n|A$$

Das heißt $\left[\prod_{r=1}^m T_r\right] A^{-1} = E_n$. Multiplikation von rechts mit A liefert $A = \prod_{r=1}^m T_r$. Insbesondere folgt

$$\begin{aligned}\det(A) &= \det\left(\prod_{r=1}^m T_r\right) = \det\left(T_1 \prod_{r=2}^m T_r\right) \underset{\text{I, II, III}}{=} \det(T_1)\det\left(T_2 \prod_{r=3}^m T_r\right) \\ &= \cdots = \prod_{r=1}^m \det(T_r)\end{aligned}$$

und

$$\begin{aligned}\det(AB) &= \det\left(\left[\prod_{r=1}^m T_r\right] B\right) = \det\left(T_1 \left[\prod_{r=2}^m T_r\right] B\right) \\ &\underset{\text{I, II, III}}{=} \det(T_1)\det\left(T_2 \left[\prod_{r=3}^m T_r\right] B\right) = \cdots = \left[\prod_{r=1}^m \det(T_r)\right]\det(B) \\ &= \det(A)\det(B)\end{aligned}$$

V. Sei nun A beliebig mit $\operatorname{Rang}(A) < n$. Es gilt $\det(A) = 0$ und $\operatorname{Rang}(AB) \underset{\text{Ü 43}}{\leq} \operatorname{Rang}(A) < n$ und damit $\det(AB) = 0 = \det(A)\det(B)$.

□

Korollar.

(i) $\forall A, B \in K^{n\times n} : \det(AB) = \det(BA)$

(ii) $\forall A \in \mathrm{GL}_K(n) : \det(A^{-1}) = \frac{1}{\det(A)}$