Skript zur Vorlesung

Lineare Algebra 1 für Lehramtsstudierende (GS/HS/RS)

(Wintersemester 2009/10)

Dieses Geheft enthält in kompakter Form die wesentlichen Inhalte, wie sie in der Vorlesung „Lineare Algebra für Lehramtsstudierende (GS/HS/RS)" vorgestellt werden.

Es ist zum Gebrauch neben der Vorlesung gedacht und erhebt nicht den Anspruch, „in sich selbst verständlich" oder vollständig zu sein.

S. Hilger

Inhaltsverzeichnis

Literatur

Bezüglich der mathematischen Rigorosität gibt es zwei extreme Standpunkte:

- Streng–mathematisch. Auf der Grundlage von Axiomen (nicht weiter hinterfragbaren Grundsätzen) werden Sätze mit Hilfe der Gesetze der Logik deduziert (abgeleitet).
- Es wird einfach an intuitive Vorstellungen (wie sie beispielsweise auch in der Schule präsentiert werden), angeknüpft.

Hier wird versucht, einen vernünftigen Mittelweg zu gehen.

Ein mathematischer Text gliedert sich im wesentlichen in Definitionen, Axiome, Sätze (auch Propositionen, Lemmata, Korollare, Hilfssätze,...), Beweise, Beispiele und zusätzliche Erläuterungen und Bemerkungen.
Hier kann man ebenfalls rigoros oder sehr locker umgehen. Wir gehen auch den Mittelweg.

Zunächst erfolgen viele Definitionen. Sei werden durch Kursivdruck des zu definierenden Objekts kenntlich gemacht.

1 Mengen und Abbildungen

1.1 Mengen

Cantor'sche Auffassung, Naive Mengenlehre

> Unter einer Menge verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens, welche die Elemente von M genannt werden, zu einem Ganzen.
> [Gesammelte Abhandlungen, ed E. Zermelo, Berlin 1932]
>
> **Georg Cantor** (1845 – 1918, Begründer der Mengenlehre)

Elemente von Mengen Zentral wichtig, letztlich aber undefiniert, ist die Beobachtung, dass zwischen zwei mathematischen Objekten a und M die Beziehung

$$a \text{ ist Element der Menge } M, \qquad \text{(symb.)} \quad a \in M$$

bestehen kann.

Innerhalb der Mathematik, wie wir sie kennenlernen werden, ist es für zwei Objekte i.a. prinzipiell klar entscheidbar, ob

$$a \in M \qquad \text{oder} \qquad a \notin M.$$

Schreibweise Eine Menge wird — zunächst — durch Aufzählung aller ihrer Elemente beschrieben.

Bsp.: $M = \Big\{a, b, e, x, y, g, e\Big\}$ oder $M = \Big\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\Big\}$

Dabei:

- In der wissenschaftlichen Mathematik werden zur Trennung Kommata gesetzt, in der Schule Strichpunkte.
- Eine bestimmte Reihenfolge ist mathematisch ohne Belang, manchmal ist sie zweckmäßig.
- Mehrfachnennungen sind möglich.
- Auch Mengen können Elemente sein.

$$M = \Big\{1, 2, 3, \{1, 2\}\Big\}, \qquad \text{Beachte} \quad 2 \neq \{2\}.$$

Die leere Menge Die Menge, die kein Element enthält, wird *leere Menge* genannt.

(Symb.) $\varnothing$ oder $\{\ \ \}$ (Schule)

1.2 Aussagen

Naive Beschreibung:

> Eine *Aussage* ist ein sprachliches Gebilde, das eindeutig als *wahr* (w) oder *falsch* (f) erkannt werden kann.

Ist eine Aussage wahr, so sagt man auch sie *gilt*.

Nicht–Beispiele:

- Bleib hier! (Grammatik)
- Wie geht es Dir? (Grammatik)
- Die Resteverwertung ist bunt. (Sinngehalt)
- ,,Rot" ist eine schöne Farbe. (Wertung, Subjektivität)
- Harald ist rothaarig. (Kontext)
- $x \geq 0$ (Kontext)

Beispiele: ,,Gute" Beispiele erhält man im allgemeinen dadurch, dass man mathematische Objekte als Inhalt wählt. Mit $X = \{1, 2, 3\}$ gilt.

- $1 \in X$. (w)
- $3 \notin X$. (f)
- $5 \in X$.(f)
- 5 ist ungerade. (w)

Andere Beispiele:

- Für $n \geq 3$ hat die Gleichung $x^n + y^n = z^n$ keine ganzzahlige nichttriviale Lösung. (trivial heißt ,,für jeden sofort zu sehen" oft ist es die Null–Lösung). Seit 1992 ist die Wahrheit dieser Aussage bewiesen.

- Es gibt unendlich viele Primzahlzwillinge. (Bis heute nicht entschieden)

Aussagen können zu neuen verknüpft werden, deren Wahrheitswert sich aus denen der vorgegebenen nach bestimmten Regeln, den ,,Gesetzen der Logik", ergibt.

Die Wahrheitswerte der im folgenden zu definierenden Operationen mit Aussagen ergeben sich aus der folgenden Tabelle

		$\mathcal{A}$	w	w	f	f
		$\mathcal{B}$	w	f	w	f
Negation	NICHT $\mathcal{A}$	$\neg\mathcal{A}$	f		w	
Konjunktion	$\mathcal{A}$ UND (ZUGLEICH) $\mathcal{B}$	$\mathcal{A} \wedge \mathcal{B}$	w	f	f	f
Disjunktion	$\mathcal{A}$ ODER $\mathcal{B}$	$\mathcal{A} \vee \mathcal{B}$	w	w	w	f
Disjunktion (ausschl.)	ENTWEDER $\mathcal{A}$ ODER $\mathcal{B}$		f	w	w	f
Implikation	$\mathcal{A}$ IMPLIZIERT $\mathcal{B}$	$\mathcal{A} \Rightarrow \mathcal{B}$	w	w	f	w
Bijunktion	$\mathcal{A}$ ÄQUIVALENT $\mathcal{B}$	$\mathcal{A} \Leftrightarrow \mathcal{B}$	w	f	f	w

Die Negation Beispiel:

- $\mathcal{A}$ Es gibt unendlich viele Primzahlzwillinge.
- $\neg\mathcal{A}$ Es gibt endlich viele Primzahlzwillinge.

Die Konjunktion Beispiel:

- $\mathcal{A}$: n ist eine gerade Zahl.
- $\mathcal{B}$: n ist eine Primzahl.
- $\mathcal{A} \wedge \mathcal{B}$: n ist eine gerade Primzahl (Äquivalent zu $n = 2$).

Die Aussage $\mathcal{A} \wedge \neg\mathcal{A}$ ist falsch für alle Aussagen $\mathcal{A}$.

Die Disjunktion Die ODER–Verknüpfung beinhaltet immer auch die Gültigkeit beider Fälle. Das Vorwort ENTWEDER schließt dies aus.
Beispiele: (g, h Geraden im n–dimensionalen Raum)

- $\mathcal{A}$: g und h sind parallel.
- $\mathcal{B}$: g und h schneiden sich in genau einem Punkt.
- $\mathcal{A} \vee \mathcal{B}$: g und h spannen genau eine Ebene auf.

Die Aussage $\mathcal{A} \vee \neg\mathcal{A}$ ist wahr für alle Aussagen $\mathcal{A}$.

Die Implikation Anstelle von „$\mathcal{A}$ IMPLIZIERT $\mathcal{B}$" spricht man auch:

- Aus $\mathcal{A}$ folgt $\mathcal{B}$.
- Wenn $\mathcal{A}$, dann $\mathcal{B}$.
- $\mathcal{B}$, wenn $\mathcal{A}$.
- $\mathcal{A}$ ist hinreichend für $\mathcal{B}$.
- $\mathcal{B}$ ist notwendig für $\mathcal{A}$.
- (Engl.) If $\mathcal{A}$, then $\mathcal{B}$.

Beispiel:

- $\mathcal{A}$ Heute ist Montag.
- $\mathcal{B}$ Morgen ist Dienstag.

Die Aussage $\mathcal{A} \to \mathcal{B}$ ist wahr, auch wenn Sie dies an einem Donnerstag lesen.

Mathematische Sätze bestehen letztlich aus Aussagen der Form $\mathcal{A} \to \mathcal{B}$. In diesem Zusammenhang heißt $\mathcal{A}$ *Voraussetzung* und $\mathcal{B}$ *Behauptung.*

Oft ist es bei Formulierungen von Sätzen so, dass die Aussage $\mathcal{A}$ unausgesprochen einen Kontext $\mathcal{K}$M(beispielsweise die bisher behandelten Axiome und Sätze) beinhaltet.

Beispiel eines solchen Satzes: Die Lösungen einer quadratischen Gleichung

$$ax^2 + bx + c = 0 \qquad \text{mit } b^2 - 4ac > 0$$

sind gegeben durch

$$x_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \quad \text{und } x_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a}.$$

Der Kontext besteht darin, dass die zugrundeliegende Zahlenmenge die Menge der reellen Zahlen ist mit den zugehörigen Rechengesetzen. (Vgl. Schulpraxis: Die Grundmenge)

Widerspruchsbeweis Der Beweis einer solchen Implikation besteht darin, unter der Annahme, dass $\mathcal{A}$ wahr ist, in kleinen und „von jedem nachvollziehbaren" Schlüssen die Aussage $\mathcal{B}$ abzuleiten.

Da die Äquivalenz

$$(\mathcal{A} \to \mathcal{B}) \quad \Leftrightarrow \quad (\neg\mathcal{B} \Rightarrow \neg\mathcal{A})$$

besteht (Begründung durch Wertetabelle), kann die erste Aussage auch durch den Beweis der zweiten bewiesen werden. Man spricht von einem *Widerspruchsbeweis.*

Ein solches Vorgehen ist typisch beim Beweis dafür, dass etwas **nicht** existiert. Ein Beispiel stellt der Beweis, dass $\sqrt{2} \notin \mathbb{Q}$, dar: Wir nehmen an, dass $\sqrt{2} = \frac{p}{q}$ rational (gekürzt). Dann gilt

$$
\begin{array}{ll}
 & \dfrac{p^2}{q^2} = 2 \quad \Longrightarrow \quad p^2 = 2q^2 \\
\Longrightarrow & 2 \text{ ist Primteiler von } p. \\
\Longrightarrow & 4 \text{ teilt } p^2 \\
\Longrightarrow & 2 \text{ teilt } q^2 \\
\Longrightarrow & 2 \text{ ist Primteiler von } q.
\end{array}
$$

Die Aussagen in der zweiten und letzten Zeile stellen einen Widerspruch zur ,,Gekürztheit” von $\sqrt{2}$ dar.

Die Bijunktion Anstelle von ,,$\mathcal{A}$ ÄQUIVALENT $\mathcal{B}$” sagt man auch:

- $\mathcal{A}$ ist hinreichend und notwendig für $\mathcal{B}$.
- $\mathcal{A}$ genau dann, wenn $\mathcal{B}$.
- (Engl.) $\mathcal{A}$, iff $\mathcal{B}$.

Beispiel (Satz von Thales über Dreieck ΔABC): Ein Kreis mit $[AB]$ als Durchmesser geht genau dann durch C, wenn der Innenwinkel bei C das Maß $90\,^{\circ}$ hat.
Bemerkung: $(\mathcal{A} \Leftrightarrow \mathcal{B}) \quad \Leftrightarrow \quad \Big((\mathcal{A} \Rightarrow \mathcal{B}) \wedge (\mathcal{B} \Rightarrow \mathcal{A})\Big)$. Begründung (Ü) durch Vergleich der Wertetabellen.

Aussagenalgebra

In den Übungen. Ein Beispiel:

$$\mathcal{A} \wedge (\mathcal{B} \vee \mathcal{C}) \quad \Longleftrightarrow \quad (\mathcal{A} \wedge \mathcal{B}) \vee (\mathcal{A} \wedge \mathcal{C})$$

Beweis durch Wahrheitstabelle:

$\mathcal{A}$	w	w	w	w	f	f	f	f
$\mathcal{B}$	w	w	f	f	w	w	f	f
$\mathcal{C}$	w	f	w	f	w	f	w	f
$\mathcal{A} \wedge (\mathcal{B} \vee \mathcal{C})$	w	w	w	f	f	f	f	f
$(\mathcal{A} \wedge \mathcal{B}) \vee (\mathcal{A} \wedge \mathcal{C})$	w	w	w	f	f	f	f	f

1.3 Operieren mit Mengen

Gleichheit Zwei Mengen sind (per definitionem, Cantor) gleich, (genau dann,) wenn sie in ihren Elementen übereinstimmen.

$$X = Y \quad \Longleftrightarrow \quad (a \in X \Longrightarrow a \in Y) \text{ und } (a \in Y \Longrightarrow a \in X).$$

Teilmenge Es seien zwei Mengen X, Y gegeben.

- Y heißt *Teilmenge* von X,

  $$\text{(symb.)} \quad Y \subseteq X,$$

  wenn aus $x \in Y$ folgt: $x \in X$.

- Y heißt *echte Teilmenge* von X, wenn zusätzlich $Y \neq X$ gilt.

Folgerungen:

1. Für jede Menge X gilt:

   $$\emptyset \subseteq X.$$

2. Für zwei Mengen X und Y sind die beiden Aussagen

   $$X = Y, \qquad (X \subseteq Y) \text{ und } (Y \subseteq X)$$

äquivalent. Der Nachweis der Gleichheit zweier Mengen geschieht durch den Nachweis der wechselweisen Teilmengenbeziehung.

Aussagen definieren Teilmengen Es sei X eine Menge. Für jedes $x \in X$ sei eine Aussage $\mathcal{A}(x)$ vorgegeben. Dann kann die Teilmenge

$$Y = \{x \in X \Big| \mathcal{A}(x) \text{ ist wahr } \}$$

gebildet werden.

- Der senkrechte Strich ist als ,,mit der Eigenschaft, dass" zu lesen.
- die Angabe ,,ist wahr" wird weggelassen.

Differenzmenge Für zwei vorgegebene Mengen X, Y heißt

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

die *Differenzmenge*.
(Der Doppelpunkt steht auf der Seite des zu definierenden Objekts.)
Beispiele: Sind

$$X_1 = \{0, 1, 4, 7, 9\}, \qquad Y_1 = \{0, 2, 3, 4, 5\},$$

so gilt:

$$X_1 \setminus Y_1 = \{1, 7, 9\}.$$

Wir haben dabei nicht vorausgesetzt, dass Y eine Teilmenge von X ist. Falls dies der Fall ist, so heißt die Differenzmenge $X \setminus Y$ auch das *Komplement* oder *Komplementärmenge* von Y in X. Beispiel:

$$\{1, 4\} \ \text{ ist das Komplement von } \ \{0, 7, 9\} \ \text{ in } \ X_1.$$

Vereinigungsmenge Für zwei vorgegebene Mengen X, Y heißt

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

die *Vereinigung(-smenge)* von X und Y.
Beispiel:

$$X_1 \cup Y_1 = \{0, 1, 2, 3, 4, 5, 7, 9\}.$$

Schnittmenge Für zwei vorgegebene Mengen X, Y heißt

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

die *Schnittmenge* oder der *Durchschnitt* von X und Y.
Beispiel:

$$X_1 \cap Y_1 = \{0, 4\}.$$

Zwei Mengen X und Y, für die $X \cap Y = \varnothing$ gilt, heißen *disjunkt.*

Graphische Veranschaulichungen durch **Venn–Diagramme**.

Potenzmenge Ist eine Menge X gegeben, so heißt die Menge aller Teilmengen von X die *Potenzmenge* von X. Sie wird mit $\mathcal{P}(X)$ bezeichnet.

Es ist $\mathcal{P}(\{1, 2, 3\}) = \Big\{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}, \{1, 3\}, \{1, 2, 3\}\Big\}$.

Mengenalgebra

In den Übungen. Ein Beispiel:

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$$

Beweis: Es sei $a \in X \cup Y \cup Z$. Wir betrachten die drei Aussagen:

$$\mathcal{A} : a \in X, \qquad \mathcal{B} : a \in Y, \qquad \mathcal{C} : a \in Z.$$

Dann gilt

$$\begin{aligned} & a \in X \cap (Y \cup Z) \quad \Longleftrightarrow \quad \mathcal{A} \wedge (\mathcal{B} \vee \mathcal{C}) \\ \Longleftrightarrow \quad & (\mathcal{A} \wedge \mathcal{B}) \vee (\mathcal{A} \wedge \mathcal{C}) \quad \Longleftrightarrow \quad a \in (X \cap Y) \cup (X \cap Z) \end{aligned}$$

1.4 Relationen und Funktionen

Geordnete Paare Für zwei vorgegebene Mengen X, Y und Elemente $x \in X$, $y \in Y$ heißt

$$(x, y) \ := \ \Big\{\{x, y\}, \{x\}\Big\}$$

das durch x und y gebildete *(geordnete) Paar* oder 2–*Tupel*. x und y heißen in diesem Zusammenhang die erste bzw. zweite Koordinate des Paares.

Satz: Sind X, Y zwei Mengen mit $x_1, x_2 \in X$ und $y_1, y_2 \in Y$ so gilt:

$$(x_1, y_1) = (x_2, y_2) \qquad \Longleftrightarrow \qquad x_1 = x_2 \text{ und } y_1 = y_2.$$

Bemerkung: Der Satz wäre mit Mengen anstelle geordneter Paare falsch.

Beweis: Die eine Richtung $\Leftarrow$ ist trivial. Die andere Richtung $\Rightarrow$ muß bewiesen werden.

$$\begin{aligned}
& (x_1, y_1) = (x_2, y_2) \\
\Longrightarrow \quad & \Big\{\{x_1, y_1\}, \{x_1\}\Big\} = \Big\{\{x_2, y_2\}, \{x_2\}\Big\} \\
\Longrightarrow \quad & (\{x_1\} = \{x_2\} \text{ und } \{x_1, y_1\} = \{x_2, y_2\}) \quad \text{ oder} \\
& (\{x_1\} = \{x_2, y_2\} \text{ und } \{x_2\} = \{x_1, y_1\}).
\end{aligned}$$

Wir betrachten die zwei Fälle:
1. Fall:

$$\begin{aligned}
& \{x_1\} = \{x_2\} \text{ und } \{x_1, y_1\} = \{x_2, y_2\} \\
\Longrightarrow \quad & x_1 = x_2 \text{ und } y_1 \in \{x_2, y_2\} \text{ und } y_2 \in \{x_1, y_1\} \\
\Longrightarrow \quad & x_1 = x_2 \text{ und } (y_1 = x_2 = x_1 \text{ oder } y_1 = y_2) \text{ und } (y_2 = x_1 = x_2 \text{ oder } y_2 = y_1) \\
\Longrightarrow \quad & x_1 = x_2 \text{ und } y_1 = y_2.
\end{aligned}$$

2. Fall:

$$\begin{aligned}
& \{x_1\} = \{x_2, y_2\} \text{ und } \{x_2\} = \{x_1, y_1\} \\
\Longrightarrow \quad & x_1 = x_2 = y_2 = y_1.
\end{aligned}$$

Ist der auf der obigen „umständlichen" Definition basierende Satz akzeptiert, so kann diese wieder in den Hintergrund treten.

Das kartesische Produkt Das *Kartesische Produkt* (René Descartes, fr, 1596 – 1650) der Mengen X und Y ist die Menge der geordneten Paare:

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

Relationen Eine *Relation R zwischen X und Y* ist eine beliebige Teilmenge von $X \times Y$. Gut kann man das mit Hilfe eines *Liniendiagramms* oder *Pfeildiagramms* veranschaulichen:

Zwischen einem Element $x \in X$ und einem Element $y \in Y$ wird genau dann eine Linie gezogen, wenn $(x, y) \in R$.

Ist R eine Relation, so heißt

$$R^{-1} := \Big\{ (y, x) \,\Big|\, (x, y) \in R \Big\}$$

die zu R *gespiegelte* Relation oder *Spiegelrelation.*

Eine Relation zwischen X und Y heißt

(♣) links–total,	wenn für jedes	$x \in X$ mindestens ein $y \in Y$
(♠) rechts–eindeutig,		$x \in X$ höchstens ein $y \in Y$
(♡) rechts–total,		$y \in Y$ mindestens ein $x \in X$
(♢) links–eindeutig,		$y \in Y$ höchstens ein $x \in X$

existiert, so dass $(x, y) \in R$.

Im Diagramm veranschaulicht heißt dies:

In	$x \in X$ startet mindestens	ein Pfeil.
	$x \in X$ startet höchstens	
	$y \in Y$ endet mindestens	
	$y \in Y$ endet höchstens	

Funktionen Eine Relation zwischen X und Y heißt *Funktion* oder *Abbildung von X nach Y*, wenn sie links–total (♣) und rechts–eindeutig (♠) ist. In diesem Zusammenhang heißt X *Definitionsmenge* und Y *Wertemenge* der Funktion.

Funktionen werden oft mit kleinen Buchstaben bezeichnet: $f, g, h, \ldots$

Die soeben gegebene Definition des Begriffs ,,Funktion" ist mathematisch befriedigend, für das praktische Arbeiten aber zu umständlich und zu statisch. Eine andere Definition, die nicht in der Mengenlehre verankert ist, unterstreicht den eher dynamischen Charakter einer Funktion:

Es seien zwei Mengen X und Y gegeben. Eine Funktion von X nach Y ist eine Vorschrift, die **jedem** $x \in X$ **genau ein** $y \in Y$ zuordnet. Dies wird auch in einer gänzlich veränderten Notation deutlich:

$$f : \begin{cases} X & \to & Y \\ x & \mapsto & f(x) \end{cases}$$

$f(x)$ ist dabei ein irgendwie gearteter mathematisch sinnvoller Ausdruck (Term, Textdefinition, auch per Fallunterscheidung,...).

Im Diagramm veranschaulicht heißt dies, dass in **jedem** $x \in X$ **genau ein** Pfeil startet.

Geht man von dieser Definition aus, so wird die zugehörige Relation oft als Graph G_f der Funktion bezeichnet:

$$G_f := \left\{ (x, y) \in X \times Y \;\middle|\; y = f(x) \right\}.$$

Auch Teilmengen $X' \subseteq X$ bzw. $Y' \subseteq Y$ werden durch eine Funktion $f : X \to Y$ zugeordnet:

$$\begin{aligned} f(X') &:= \left\{ y \in Y \;\middle|\; \text{Es ex. } x \in X' \text{ mit } f(x) = y \right\} \\ f^{-1}(Y') &:= \left\{ x \in X \;\middle|\; f(x) \in Y' \right\} \end{aligned}$$

Die Menge $f(X)$ heißt *Bild(–menge)* der Funktion f. Unterscheide Bild- und Wertemenge!

	injektiv,		links-eindeutig	
Eine Funktion heißt	*surjektiv*,	wenn sie zusätzlich	rechts-total	ist.
	bijektiv,		links-eindeutig und rechts-total	

Ist X eine Menge, so heißt die Funktion (Begründung)

$$\mathrm{id}_X \;:=\; \Big\{(x,x) \in X \times X \;\Big|\; x \in X\Big\}$$

die *identische Funktion* oder *Identität auf* X. Innerhalb der Zuordnungsauffassung schreibt man oft kurz $x \mapsto x$.
Sind $f : X \to Y$ und $g : Y \to Z$ Funktionen, so heißt die Funktion (Begründung)

$$g \circ f \;:=\; \Big\{(x,z) \in X \times Z \;\Big|\; \text{Es ex. } y \in Y \text{ mit } f(x) = y \text{ und } g(y) = z\Big\}$$

die *Hintereinanderausführung* oder *Komposition* der Funktionen f und g. Da f eine Funktion ist, ist das y in der Definition eindeutig bestimmt.
Innerhalb der Zuordnungsauffassung schreibt man $x \mapsto (g \circ f)(x) = g(f(x))$.

Diagrammveranschaulichung. Achte auf die Schreibrichtung.

Kriterien für Injektivität und Surjektivität

(i) Eine Funktion $f : X \to Y$ ist genau dann injektiv, wenn eine Funktion $g : Y \to X$ existiert, so dass $g \circ f = \mathrm{id}_X$.

(ii) Eine Funktion $f : X \to Y$ ist genau dann surjektiv, wenn eine Funktion $h : Y \to X$ existiert, so dass $f \circ h = \mathrm{id}_Y$.

Beweis (i) $\Longrightarrow$ (ii) Es sei $x_0 \in X$ fest ausgewählt. Definiere die Funktion g durch

$$g(y) \ := \begin{cases} x, & \text{falls } x \text{ (dann eindeutig) exisitert, so dass } f(x) = y \ , \\ x_0, & \text{sonst.} \end{cases}$$

Für alle $x \in X$ gilt dann $g(f(x)) = x$.

$\Leftarrow$ Es seien $x_1, x_2 \in X$ beliebig mit $f(x_1) = f(x_2)$. Dann gilt:

$$x_1 = g(f(x_1)) = g(f(x_2)) = x_2,$$

also ist f injektiv.

(ii) $\Longrightarrow$ (i) Zu jedem $y \in Y$ wähle ein $x \in X$, so dass $f(x) = y$. Es gibt mindestens ein solches x, da f surjektiv. Definiere g durch $g(y) = x$. Dann gilt für alle $y \in Y$: $f(g(y)) = f(x) = y$.

$\Leftarrow$ Sei $y \in Y$. Dan existiert zu jedem $y \in Y$ ein x, nämlich $x = g(y)$, so dass

$$f(x) = f(g(y)) = y.$$

♦

Satz über die Umkehrfunktion Die drei folgenden Aussagen über eine Funktion $f : X \to Y$ sind äquivalent:

(i) f ist bijektiv.

(ii) Die zu f gehörige Spiegelrelation f^{-1} ist eine Funktion.

(iii) Es existiert eine Funktion $g : Y \to X$ mit

$$g \circ f = \mathrm{id}_X \qquad \text{und} \qquad f \circ g = \mathrm{id}_Y.$$

In diesem Fall gilt $g = f^{-1}$. Diese Funktion heißt *Umkehrfunktion* zu f.

Beweis (i) $\Longrightarrow$ (iii) ist fast klar nach dem vorherigen Satz. Wir müssen für (i) $\Longrightarrow$ (iii) nur noch zeigen: Die nach dem letzten Satz existierenden Funktionen $g_1, g_2 : Y \to X$ mit

$$g_1 \circ f = \mathrm{id}_X \qquad \text{und } f \circ g_2 = \mathrm{id}_Y$$

sind identisch:

$$g_1 = g_1 \circ \mathrm{id}_Y = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = \mathrm{id}_X \circ g_2 = g_2$$

Dabei haben wir benutzt, dass für die Hintereinanderausführung von Funktionen das Assoziativgesetz gilt.

(i) $\Longleftrightarrow$ (ii) ist auch ganz einfach:

$$\begin{aligned} f \text{ bijektiv} \quad &\Longleftrightarrow \quad f \text{ links–eindeutig und rechts–total} \\ &\Longleftrightarrow \quad f^{-1} \text{ rechts–eindeutig und links–total} \\ &\Longleftrightarrow \quad f^{-1} \text{ Funktion} \end{aligned}$$

♦

1.5 Die Menge der natürlichen Zahlen

Die Peano–Axiome legen die Eigenschaften der natürlichen Zahlen — ebenfalls in der Sprache und in dem System der Mengenlehre — beschreibend fest.

Deskriptiv statt konstruktiv.

Die Frage der Existenz einer solchen Menge bleibt also unbeantwortet.

Eine Menge $\mathbb{N}$ heißt *Menge der natürlichen Zahlen*, wenn eine Abbildung $\nu : \mathbb{N} \to \mathbb{N}$ (Nachfolger–Abbildung) existiert mit folgenden Eigenschaften:

P1 Es existiert genau eine Zahl — bezeichnet mit 1 — in $\mathbb{N}$ mit $\nu(x) \neq 1$. (Das bedeutet insbesondere, dass ν ist nicht surjektiv ist.)

P2 Die Abbildung ν ist injektiv, das heißt, für alle $x, y \in \mathbb{N}$ mit $x \neq y$ gilt: $\nu(x) \neq \nu(y)$.

P3 Gilt für eine Teilmenge $A' \subseteq \mathbb{N}$

$$1 \in A' \text{ und } \Big(x \in A' \Longrightarrow \nu(x) \in A'\Big),$$

so gilt $A' = \mathbb{N}$.

1.6 Weiterer Aufbau der Zahlenräume

Das weitere Programm für den Mathematiker besteht nun darin, auf der Grundlage dieser Axiome Rechen- und Ordnungsstrukturen auf $\mathbb{N}$ einzuführen und dann diese Zahlenmenge durch größere Zahlenmenge sinnvoll zu erweitern. Wir beschreiben dieses Vorgehen hier nur stichpunktartig. Die im folgenden genannten Begriffe und Gesetze werden anderswo noch in einem allgemeineren Rahmen und genauer behandelt.

1. Addition $+$ auf $\mathbb{N}$ (und ihre Umkehroperation: Subtraktion $-$): Es gilt dann:

   $$\nu(n) = n + 1.$$

2. Multiplikation $\cdot$ auf $\mathbb{N}$ (und ihre Umkehroperation: die Division :),

3. Darstellung der Zahlen von $\mathbb{N}$ im Dezimalsystem.

4. Ordnungsrelation $\mathcal{O} \subseteq \mathbb{N} \times \mathbb{N}$. Statt $(m, n) \in \mathcal{O}$ schreibt man

   $$m < n \quad \text{oder} \quad n > m.$$

   Es wird weiter definiert

   $$\begin{aligned} m \leq n \quad &\overset{\text{def}}{\Longleftrightarrow} \quad (m = n \text{ oder } m < n) \\ m \geq n \quad &\overset{\text{def}}{\Longleftrightarrow} \quad n \leq m. \end{aligned}$$

5. Hinzufügen der Zahl 0 zu der Menge der natürlichen Zahlen:

   $$\mathbb{N}_0 = \mathbb{N} \cup \{0\}$$

   Wir setzen die Rechenregeln für $\mathbb{N}_0$ als bekannt voraus.

6. Erweiterung der Menge $\mathbb{N}_0$ zur Menge der ganzen Zahlen $\mathbb{Z}$

$$\begin{aligned}
\mathbb{Z}^+ &:= \mathbb{N} \qquad \text{(positive ganze Zahlen)} \\
\mathbb{Z}^- &:= \left\{ -n \,\middle|\, n \in \mathbb{N} \right\} \qquad \text{(negative ganze Zahlen)} \\
\mathbb{Z} &= \mathbb{Z}^+ \cup \{0\} \cup \mathbb{Z}^-
\end{aligned}$$

Definiere weiter die Betragsfunktion

$$\text{abs} \begin{cases} \mathbb{Z} & \to & \mathbb{N}_0 \\ m & \mapsto & |m| \end{cases} \qquad \text{durch} \qquad |m| := \begin{cases} m, & \text{falls } m \text{ nicht–negativ,} \\ n, & \text{falls } m = -n \text{ negativ.} \end{cases}$$

Die ,,Mathematik" von $\mathbb{Z}$ ist durch die folgenden Regeln definiert:

$$m + n \quad := \quad \begin{cases} m+n, & \text{falls } m \text{ und } n \text{ nicht–negativ,} \\ -(|m|+|n|), & \text{falls } m \text{ und } n \text{ negativ,} \\ |m|-|n|, & \text{falls } m \text{ nicht–negativ, } n \text{ negativ und } |m| > |n|, \\ -(|n|-m), & \text{falls } m \text{ nicht–negativ, } n \text{ negativ und } |n| > |m|, \\ |n|-|m|, & \text{falls } n \text{ nicht–negativ, } m \text{ negativ und } |n| > |m|, \\ -(|m|-n), & \text{falls } n \text{ nicht–negativ, } m \text{ negativ und } |m| > |n|. \end{cases}$$

$$m \cdot n \quad := \quad \begin{cases} |m| \cdot |n|, & \text{falls beide nicht–negativ oder beide negativ ,} \\ -(|m| \cdot |n|), & \text{anderenfalls.} \end{cases}$$

$$m < n \quad \overset{\text{def}}{\Longleftrightarrow} \quad n - m \text{ ist positiv.}$$

7. Erweiterung der Menge $\mathbb{Z}$ der ganzen Zahlen zu der Menge $\mathbb{Q}$ der *rationalen Zahlen (Bruchzahlen)*

$$\mathbb{Q} = \left\{ \frac{m}{n} \,\middle|\, m \in \mathbb{Z}, n \in \mathbb{Z} \setminus \{0\} \right\}.$$

Die ,,Mathematik" von $\mathbb{Q}$ ist durch die folgenden Regeln definiert:

$$\begin{aligned}
\frac{m}{n} = \frac{p}{q} \quad &\overset{\text{def}}{\Longleftrightarrow} \quad m \cdot q = p \cdot n \\
\frac{m}{n} \pm \frac{p}{q} \quad &:= \quad \frac{mq + pn}{nq} \\
\frac{m}{n} \cdot \frac{p}{q} \quad &:= \quad \frac{mp}{nq} \\
\frac{m}{n} : \frac{p}{q} \quad &:= \quad \frac{mq}{pn} \\
\frac{m}{n} < \frac{p}{q} \quad &\overset{\text{def}}{\Longleftrightarrow} \quad m \cdot q < p \cdot n, \qquad \text{wobei } n \cdot q > 0.
\end{aligned}$$

Das entscheidende Axiom P3 äußert sich mehr konkret in der zwei fundamentalen mathematischen Verfahren:

Rekursive Definition (Fassen Sie diese Aussage als Axiom auf (Nebulös))
Mathematische Objekte M_n können für $n \in \mathbb{N}$ dadurch definiert werden, dass

1. das Objekt M_1 definiert wird und
2. für jedes $n \in \mathbb{N}$ angegeben wird, wie das Objekt M_{n+1} bei bekanntem M_n definiert ist.

Eine ,,Begründung" besteht darin, dass man das Axiom P3 auf die Teilmenge

$$A' = \{n \in \mathbb{N} | M_n \text{ ist definiert } \}$$

anwendet.

Beispiel: Wir definieren rekursiv höhere n–*Tupel*. Es sei für jedes $n \in \mathbb{N}$ eine Menge X_n und ein Element $x_n \in X_n$ gegeben. Definiere rekursiv

- $(x_1) = x_1$
- $(x_1, x_2, \ldots, x_n, x_{n+1}) = ((x_1, x_2, \ldots, x_n), x_{n+1})$.

Prinzip der vollständigen Induktion Es sei $\mathcal{A}(n)$ für jedes $n \in \mathbb{N}$ eine Aussage. Gilt

- $\mathcal{A}(1)$ und
- $\mathcal{A}(n) \implies \mathcal{A}(n+1)$,

so ist $\mathcal{A}(n)$ wahr für alle $n \in \mathbb{N}$.

Die Aussage in der ersten Zeile heißt in diesem Zusammenhang auch *Induktionsanfang*. Die Aussage $\mathcal{A}(n)$ in der zweiten Zeile heißt *Induktionsvoraussetzung* oder *Induktionsannahme*. Die Implikation in der zweiten Zeile wird als *Induktionsschritt* oder *Induktionsschluss* bezeichnet.

Beweis: Man wende das Axiom P3 auf die Teilmenge

$$A' = \{n \in \mathbb{N} | \mathcal{A}(n) \text{ ist wahr } \}$$

an.

Entscheidend an diesen beiden Prinzipien ist die Tatsache, dass unendlich viele Aussagen durch endlich viele (zwei) (Definitions– bzw. Beweis–)Schritte ,,mathematisch dingfest" gemacht sind.

Bemerkung: Die beiden Prinzipien können – entsprechend modifiziert — auch bei Zugrundelegung anderer Teilmengen von $\mathbb{Z}$ angewandt werden. Beispiele:

$$\mathbb{N}_0,$$
$$\{n \in \mathbb{Z} | n \geq N\} \text{ für ein fest gewähltes } N \in Z,$$
$$\{n \in \mathbb{Z} | n \leq N\} \text{ für ein fest gewähltes } N \in Z,$$
$$2\mathbb{N} = \{n \in \mathbb{N} | n \text{ ist gerade } \}.$$

Wir definieren durch Rekursion einige spezielle Funktionen auf Zahlenmengen:

- Die Summenschreibweise: Es sei für jedes $k \in \{1, \ldots, n\}$ eine Zahl a_k gegeben. Dann ist durch

  $$S_1 = a_1, \qquad S_{k+1} = a_{k+1} + S_k$$

  die zugehörige Summenfolge definiert. Um den Aufwand in der Definition geringer zu halten, schreibt man kürzer und suggestiver:

  $$S_n = a_n + a_{n-1} + \cdots + a_1 \quad \text{oder} \quad S_n = \sum_{k=1}^{n} a_k.$$

- Wir definieren $s_0 = 0, \qquad s_{k+1} = (k+1) + s_k$ für $k \in \mathbb{N}_0$, das heißt also

  $$s_n = n + (n-1) + \cdots + 1 = \sum_{k=0}^{n} k.$$

  Wir zeigen durch Induktion:

  $$s_n = \frac{n \cdot (n+1)}{2}.$$

  Induktionsanfang: $s_0 = 0 = \frac{0 \cdot 1}{2}$
  Induktionsschluss: Wir nehmen an, dass die Behauptung für $n \geq 2$ gezeigt ist. Dann gilt:

  $$\begin{aligned} s_{n+1} &\overset{\text{def}}{=} (n+1) + s_n \overset{\text{IndV}}{=} (n+1) + \frac{n \cdot (n+1)}{2} = \\ &= \frac{2(n+1) + n \cdot (n+1)}{2} = \frac{(n+2) \cdot (n+1)}{2} = \frac{(n+1) \cdot (n+2)}{2}. \end{aligned}$$

  Also gilt die Behauptung auch für $n + 1$.

  Nach dem Induktionsprinzip ist die Aussage für alle $n \in \mathbb{N}_0$ richtig.

- Sätzchen (Geometrische Summe): Für ein beliebiges $q \in \mathbb{Q} \setminus \{1\}$ gilt:

  $$\begin{aligned} \sum_{k=0}^{n} q^k &= 1 + q + q^2 + \ldots q^n = \frac{1 - q^{n+1}}{1 - q}, \\ \sum_{k=1}^{n} q^k &= q + q^2 + \ldots q^n = \frac{q - q^{n+1}}{1 - q}. \end{aligned}$$

  Beweis durch Induktion über n:
  Induktionsanfang:

  $$\sum_{k=0}^{0} q^k = q^0 = 1 = \frac{1 - q^{0+1}}{1 - q}$$

Induktionsschritt: Wir nehmen an, dass die Aussage für n gezeigt ist.

$$\sum_{k=0}^{n+1} q^k = \sum_{k=0}^{n} q^k + q^{n+1} \stackrel{\text{IndV}}{=} \frac{1-q^{n+1}}{1-q} + q^{n+1} =$$
$$\frac{1-q^{n+1}+(1-q)q^{n+1}}{1-q} = \frac{1-q^{n+2}}{1-q}.$$

Die zweite Formel folgt ganz leicht aus der ersten:

$$\sum_{k=1}^{n} q^k = \sum_{k=0}^{n} q^k - 1 = \frac{q-q^{n+1}}{1-q} - 1 = \frac{1-q^{n+1}}{1-q} - \frac{1-q}{1-q} = \frac{q-q^{n+1}}{1-q}.$$

- Die Produktschreibweise: Es sei für jedes $k \in \{1, \dots, n\}$ eine Zahl a_k gegeben. Dann ist durch

  $$P_1 = a_1, \qquad P_{k+1} = a_{k+1} \cdot P_k$$

  die zugehörige Produktfolge rekursiv definiert.

- Potenzfunktion: Für festes $n \in \mathbb{Z}$ ist die Potenzfunktion

  $$\left\{ \begin{array}{ccc} \mathbb{Q} & \to & \mathbb{Q} \\ a & \mapsto & a^n \end{array} \right. \qquad \text{durch } a^0 = 1, \qquad a^{n+1} = a \cdot a^n, \qquad a^{n-1} = \frac{1}{a} \cdot a^n$$

  rekursiv definiert. Man kann diese Definition auch suggestiver schreiben als

  $$a^n = \underbrace{a \cdot a \cdot \ldots \cdot a}_{n \text{ Faktoren}}, \quad n \in \mathbb{N}, \qquad a^n = \frac{1}{\underbrace{a \cdot a \cdot \ldots \cdot a}_{|n| \text{ Faktoren}}}, \quad n \in -\mathbb{N},$$

  Es gilt dann für $m, n \in \mathbb{Z}$:

  $$a^m \cdot a^n = a^{m+n}, \qquad (a^m)^n = a^{m \cdot n}.$$

- Ähnlich wie bei Summen kann man mittels rekursiver Definition auch Produkte definieren:

  $$\prod_{k=1}^{n} a_k = a_1 \cdot a_2 \cdot \ldots \cdot a_k.$$

- Fakultäts–Funktion:

  $$\left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{N} \\ n & \mapsto & n! \end{array} \right. \qquad \text{durch } 1! = 1, \qquad (n+1)! = (n+1) \cdot n! \text{ für alle } n \geq 1.$$

  Suggestiver:

  $$n! = n \cdot (n-1) \cdot \ldots \cdot 1 = \prod_{k=1}^{n} k.$$

1.7 Mächtigkeit von Mengen

- Zwei Mengen X, Y heißen *gleichmächtig*, wenn eine bijektive Abbildung $X \to Y$ existiert.

- Es sei $n \in \mathbb{N}$. Besteht zwischen einer Menge X und der Menge $\{1, 2, 3, \ldots, n\}$ eine bijektive Abbildung, so sagt man, dass die Menge X die *Mächtigkeit* n hat oder, dass die *Anzahl* ihrer Elemente n ist. Symbolisch: $|X| = n$.

- Die leere Menge hat die *Mächtigkeit* 0.

- Eine Menge der Mächtigkeit n, $n \in \mathbb{N}_0$, heißt *endlich*. Falls X und Y endlich sind, gilt (ohne Beweis)

$$
\begin{aligned}
&X \cap Y = \varnothing \quad \Longrightarrow \quad |X \cup Y| = |X| + |Y| \\
&Y \subseteq X \quad \Longrightarrow \quad |X \setminus Y| = |X| - |Y| \\
&|X \cup Y| + |X \cap Y| = |X| + |Y| \\
&|X \times Y| = |X| \cdot |Y| \qquad \text{(Daher der Name Produkt)} \\
&|X| = n \quad \Longrightarrow \quad |\mathcal{P}(X)| = 2^n \qquad \text{(Induktionsbeweis Übung)}
\end{aligned}
$$

- Eine Menge, die nicht endlich ist, heißt *unendlich*.

- Besteht zwischen einer Menge X und der Menge $\mathbb{N}$ eine bijektive Abbildung, so sagt man, dass die Menge X *abzählbar unendlich* ist.

- Eine Menge heißt *(höchstens) abzählbar*, wenn sie endlich oder abzählbar unendlich ist.

- Eine Menge, die nicht (höchstens) abzählbar ist, heißt *überabzählbar*.

  Beispiel: $\mathbb{Q}$ ist abzählbar, $\mathbb{R}$ ist überabzählbar.

2 Gruppen und Körper

2.1 Verknüpfungen

Definition: Es sei X eine beliebige Menge. Eine Abbildung

$$v : \begin{cases} X \times X & \to & X \\ (a,b) & \mapsto & v(a,b) \end{cases}$$

heißt *Verknüpfung auf* X. Um die ,,Binarität" der Verknüpfung zu betonen, schreibt man meist

$$v(a,b) = a \star b.$$

Anstelle des Zeichens $\star$ werden vielfältige Symbole benutzt.

Beispiele:

- Auf der Menge $X = \mathbb{N}$:
  - Addition $(a,b) \mapsto a + b$,
  - Multiplikation $(a,b) \mapsto a \cdot b = ab$,
  - Potenz $(a,b) \mapsto a^b$,
  - Größter gemeinsamer Teiler $(a,b) \mapsto a \sqcap b = \mathrm{ggT}(a,b)$,
  - Kleinstes gemeinsames Vielfaches $(a,b) \mapsto a \sqcup b = \mathrm{kgV}(a,b)$,
  - Minimum $\quad \min : (a,b) \mapsto \begin{cases} a, & \text{falls } a \le b, \\ b, & \text{falls } a > b, \end{cases}$
  - $(a,b) \mapsto 3a + 2b$.
- Auf der Menge $X = \mathbb{Q}$:
  - Addition, Subtraktion, Multiplikation, Minimum,
  - Arithmetisches Mittel $(a,b) \mapsto a \perp b \ := \frac{a+b}{2}$.
- Auf der Menge $X = \mathcal{P}(Y)$, wobei Y eine Menge:
  - Vereinigung, Durchschnitt, Differenz, Symmetrische Differenz.

2.2 Gruppen

Definition: Eine Menge G zusammen mit einer Verknüpfung $\star$ heißt *Gruppe*, symbolisch $(G, \star)$, wenn folgende Gesetze erfüllt sind:

AG (Assoziativgesetz) Für beliebige $a, b, c \in G$ gilt:

$$(a \star b) \star c = a \star (b \star c)$$

NE (Existenz und Eindeutigkeit des neutralen Elements) Es existiert genau ein Element $e \in G$, so dass für alle $a \in G$ gilt

$$a \star e = a \qquad \text{und} \qquad e \star a = a$$

IE (Existenz und Eindeutigkeit der inversen Elemente) Zu jedem $a \in G$ existiert genau ein Element $b \in G$, so dass für alle $a \in G$

$$b \star a = e \qquad \text{und} \qquad a \star b = e.$$

Beispiele:

- Addition auf $\mathbb{Z}$, Addition auf $\mathbb{Q}$,
- Multiplikation auf $\mathbb{Q} \setminus \{0\}$.
- Symmetrische Differenz auf $\mathcal{P}(Y)$.
- Die sogenannte *triviale Gruppe* besteht aus einem einzigen Element: $G = \{e\}$.
- Definiere auf der Menge $\{g, u\}$ die Verknüpfung

$\oplus$	g	u
g	g	u
u	u	g

Es handelt sich um eine Gruppe mit zwei Elementen, sie wird meist mit $\mathbb{Z}_2$ bezeichnet.

Betrachte für eine Verknüpfung die beiden Rechengesetze:

NE' (Existenz eines links–neutralen Elements) Es existiert ein Element $e \in G$, so dass für alle $a \in G$ gilt

$$e \star a = a$$

IE' (Existenz eines links–inversen Elemente) Zu jedem $a \in G$ existiert ein Element $b \in G$, so dass

$$b \star a = e,$$

wobei e ein links–neutrales Element ist.

Satz 1: Für eine assoziative Verknüpfung $\star$ auf einer Menge X sind die beiden folgenden Aussagen äquivalent:

(i) Es gelten die Gesetze (NE) und (IE).

(ii) Es gelten die Gesetze (NE') und (IE').

Beweis: Die Implikation (i) $\Longrightarrow$ (ii) ist trivial. Für (ii) $\Longrightarrow$ (i) braucht man mehrere Schritte:

1. Sei $a \in X$ und b links–invers zu a, so dass $b \star a = e$ für ein links–neutrales $e \in X$. Wir zeigen, dass b auch rechts–invers ist. (Übung 11). Es sei $c \in X$ links–invers zu b, so dass $c \star b = e$. Jetzt gilt:

$$a \star b = e \star (a \star b) = (c \star b) \star (a \star b) = c \star (b \star a) \star b = c \star e \star b = c \star b = e.$$

2. Umgekehrt ist es so, dass ein beliebiges rechts–inverses Element auch links–invers ist. Also braucht man nur über inverse Elemente zu sprechen.

3. Dann zeigen wir, dass ein links–neutrales Element e auch rechts–neutral ist: Es sei $a \in X$ beliebig mit inversem Element b. Dann gilt:

$$a \star e = a \star (b \star a) = (a \star b) \star a = e \star a = a.$$

4. Umgekehrt gilt, dass ein beliebiges rechts–neutrales Element auch links–neutral ist. Also braucht man nur über neutrale Elemente zu sprechen.

5. Das neutrale Element ist eindeutig. Sind e, e' zwei neutrale Elemente, so gilt:

$$e' = e \star e' = e.$$

6. Das zu einem beliebiges $a \in G$ inverse Element ist eindeutig. Sind b, b' zwei inverse Elemente so gilt:

$$b = b \star e = b \star (a \star b') = (b \star a) \star b' = e \star b' = b'.$$

Bemerkung: Da das inverse Element zu einem beliebiges $a \in G$ eindeutig ist, kann es symbolisch auf a bezogen werden: Man schreibt — je nach verwendetem — Verknüpfungssymbol:

$$a^{-1}, \qquad \frac{1}{a}, \qquad -a, \qquad \ominus a.$$

Satz 2 (Existenz und Eindeutigkeit der Lösung):
Ist $(G, \star)$ eine Gruppe, so gibt es zu $a, b \in G$ genau ein $c \in G$, so dass $a \star c = b$.
Anders ausgedrückt: Die Gleichung $a \star x = b$ hat genau eine Lösung. Entsprechendes gilt natürlich für eine „Rechts–Lösung".

Beweis Existenz: Für gegebene $a, b \in G$ setze $c := a^{-1} \star b$. Dann gilt tatsächlich

$$a \star (a^{-1} \star b) \stackrel{\text{AG}}{=} (a \star a^{-1}) \star b \stackrel{\text{IE}}{=} e \star b \stackrel{\text{NE}}{=} b.$$

Eindeutigkeit: Es seien $c_1, c_2 \in G$, so dass

$$a \star c_1 = b \qquad \text{und} \qquad a \star c_2 = b.$$

Dann folgt:

$$a \star c_1 = a \star c_2.$$

Wir multiplizieren diese Gleichung mit a^{-1}

$$a^{-1} \star a \star c_1 = a^{-1} \star a \star c_2.$$

Daraus folgt mit (IE) und (NE) $c_1 = c_2$. ♦

Definition: Eine Gruppe $(G, \star)$ heißt *abelsch* oder *kommutativ*, wenn die folgende Eigenschaft vorliegt:

KG Für alle $a, b \in G$ gilt:

$$a \star b = b \star a.$$

Alle bisher behandelten Beispiele sind kommutative Gruppen. Gibt es auch nicht–kommutative Gruppen? Ja, natürlich: Beispielsweise Permutationsgruppen: Später!

2.3 Körper

Definition: Eine Menge $\mathbb{K}$, auf der zwei Verknüpfungen

$$\oplus : \begin{cases} \mathbb{K} \times \mathbb{K} & \to & \mathbb{K} \\ (a,b) & \mapsto & a \oplus b \end{cases} \qquad \text{und} \qquad \otimes : \begin{cases} \mathbb{K} \times \mathbb{K} & \to & \mathbb{K} \\ (a,b) & \mapsto & a \otimes b \end{cases}$$

(Addition und Multiplikation) definiert sind, heißt *(kommutativer) Körper* $(\mathbb{K}, \oplus, \otimes)$, wenn folgendes gilt:

(1) $(\mathbb{K}, \oplus)$ ist eine abelsche Gruppe (mit neutralem Element 0).

(2) $(\mathbb{K} \setminus \{0\}, \otimes)$ ist eine abelsche Gruppe.

(3) Für alle $a, b, c \in \mathbb{K}$ gilt das Distributivgesetz:

$$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c).$$

Bemerkungen:

- Addition:
  - Das neutrale Element der Addition heißt *Null(–element)*, es wird mit 0 bezeichnet.
  - Das zu $a \in \mathbb{K}$ additiv inverse Element wird mit $\ominus a$ bezeichnet.
  - Die Addition eines inversen Elements (von rechts) wird als *Subtraktion* bezeichnet. Man schreibt
- Multiplikation:
  - Das neutrale Element der Multiplikation heißt *Eins(–element)*, es wird mit 1 bezeichnet.
  - Das zu $a \in \mathbb{K} \setminus \{0\}$ multiplikativ inverse Element wird mit a^{-1} bezeichnet. Die Multiplikation (von rechts) mit einem inversen Element wird als *Division* bezeichnet.
  - Das Verknüpfungssymbol $\otimes$ wird oft weggelassen. Man schreibt kürzer:

$$a \otimes b = a\, b.$$

- Es wird die Konvention „Punkt vor Strich" benutzt. Das Distributivgesetz kann dann so geschrieben werden:

$$a(b \oplus c) = a \otimes (b \oplus c) = a \otimes b \oplus a \otimes c = ab \oplus ac.$$

Beispiele:

- $(\mathbb{Q}, +, \cdot)$ ist ein Körper.
- Information aus der Analysis: Der Körper $\mathbb{R}$ der *reellen Zahlen* umfasst den Körper $\mathbb{Q}$:

  $$\mathbb{Q} \subseteq \mathbb{R}$$

  Die Zahlen in $\mathbb{R} \setminus \mathbb{Q}$ heißen *irrational*. Der genaue Unterschied zwischen $\mathbb{R}$ und $\mathbb{Q}$ wird in der Analysis geklärt. Wesentlich ist, dass man in $\mathbb{R}$ beliebige Wurzeln von positiven reellen Zahlen ziehen kann und dass $\mathbb{R}$ fundamentale Konstanten der Mathematik enthält:

  $$\sqrt[n]{a} \in \mathbb{R} \text{ für beliebige } n \in \mathbb{N}, a \in \mathbb{R}^+, \qquad \pi \in \mathbb{R}, \qquad e \in \mathbb{R}.$$

- Der Körper

  $$\mathbb{C} \ := \ \{a + bi | a, b \in \mathbb{R}\}$$

  der komplexen Zahlen.
- Wir definieren auf der Menge $\{g, u\}$ die Verknüpfungen

$\oplus$	g	u
g	g	u
u	u	g

$\otimes$	g	u
g	g	g
u	g	u

  Der Beweis, dass dies ein Körper ist, besteht darin, alle Körpergesetze für alle Einsetzungen von g, u für die in diesen Gesetzen auftretenden Variablen zu testen (vgl. Ü 14).

  Das Null–Element ist $0 = g$. Das Eins–Element ist $1 = u$.

  Dieser Körper wird mit $GF(2)$ (Galois–Feld) bezeichnet. Oft wird diese Körperstruktur auf der Menge $\{0, 1\}$ definiert. Wir werden ihm vermutlich nicht weiter begegnen.

Eine erste wesentliche Folgerung aus den Körperaxiomen ist der folgende Satz:

Satz 1 *(Nullteilerfreiheit): Für zwei beliebige Elemente $a, b \in \mathbb{K}$ gilt:*

$$a = 0 \text{ oder } b = 0 \qquad \Longleftrightarrow \qquad a \otimes b = 0.$$

Beachte, dass die Folgerung

$$a \oplus a \oplus \cdots \oplus a = 0 \qquad \Longrightarrow \qquad a = 0$$

im allgemeinen nicht gilt.

Die zweite Aussage verdeutlichen wir an einem (Gegen–)Beispiel: In dem Körper $\{g, u\}$ gilt $u \oplus u = 0$, u ist aber nicht das neutrale Element bzgl. der Addition.

Beweis „$\Longrightarrow$" (Ü 15): Es gilt für ein beliebiges $a \in \mathbb{K}$:

$$a \otimes 0 = a \otimes (0 \oplus 0) = a \otimes 0 \oplus a \otimes 0.$$

Das heißt aber, dass $a \otimes 0$ das additiv neutrales Element ist. Also ist $a \otimes 0 = 0$.
„$\Longleftarrow$": Es seien $a, b \in \mathbb{K}$ gewählt mit

$$a \otimes b = 0 \quad \text{und} \quad a \neq 0.$$

Wir müssen beweisen, dass $b = 0$. Es sei a^{-1} das zu a multiplikativ inverse Element. Dann gilt:

$$b = e \otimes b = a^{-1} \otimes a \otimes b = a^{-1} \otimes 0 = 0.$$

♦

2.4 Der Körper der komplexen Zahlen

2.4.1 Definition

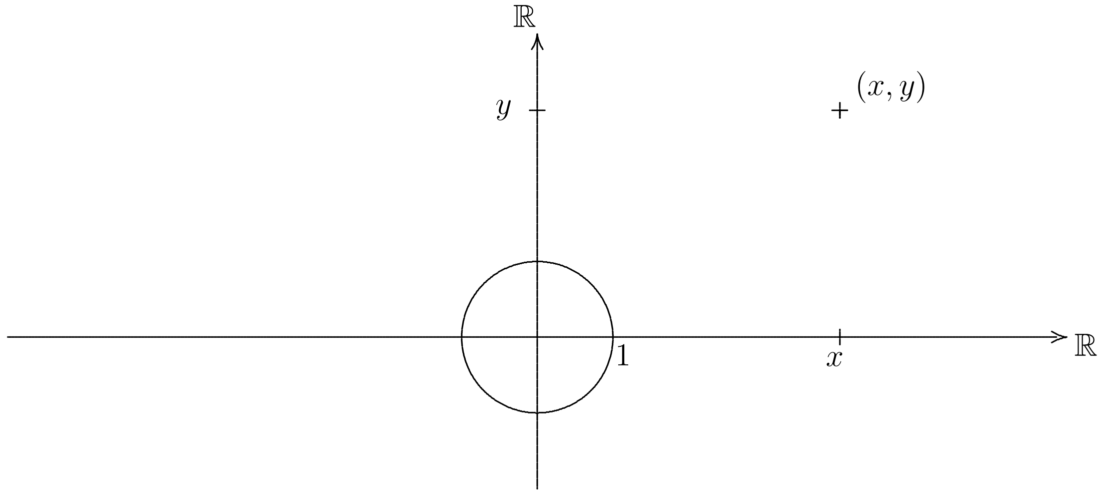
Wir betrachten die Menge der reellen Zahlenpaare

$$\mathbb{C} \ := \ \mathbb{R} \times \mathbb{R} \ := \ \Big\{(x,y) \ \Big| \ x,y \in \mathbb{R}\Big\}.$$

In dem nun zu entwickelnden Kontext heißen die Zahlenpaare *komplexe Zahlen*. Im allgemeinen verwendet man die Buchstaben

$$z = (x,y) \qquad \text{oder} \qquad w = (u,v).$$

Wir stellen uns diese Menge als eine Ebene vor.



Bei Zugrundelegung dieser Auffassung heißt die Ebene auch *Gauß'sche Zahlenebene* oder *komplexe Zahlenebene*.

Wir stellen uns die Aufgabe, dieser Menge der Zahlenpaaren die ,,Grundrechenarten" so einführen, dass die Körperaxiome erfüllt sind. Ein erster Versuch könnte darin bestehen, die Verknüpfungen komponentenweise durchzuführen:

$$\begin{aligned} (x,y) + (u,v) \quad &:= \quad (x+u, y+v) \\ (x,y) \cdot (u,v) \quad &:= \quad (xu, yv) \end{aligned}$$

Tatsächlich ist dann $(\mathbb{R} \times \mathbb{R}, +)$ eine abelsche Gruppe mit dem neutralen Element $(0,0)$. Leider ist aber $(\mathbb{R} \times \mathbb{R} \setminus \{(0,0)\}, \cdot)$ keine Gruppe, da Elemente der Form $(a,0)$ oder $(0,b)$ keine Inversen besitzen. Anderes Argument: Es gilt auch

$$(a,0) \cdot (0,b) = (0,0).$$

Wir wissen aber, dass Körper keine Nullteiler besitzen. SACKGASSE!

Es gibt aber eine Lösung unserer Aufgabe. Wir definieren auf der Menge $\mathbb{C}$ zwei Verknüpfungen wie folgt:

$$\begin{aligned} (x,y) + (u,v) \quad &:= \quad (x+u, y+v) \\ (x,y) \cdot (u,v) \quad &:= \quad (xu - yv, xv + yu) \end{aligned}$$

Es werden die gleichen Verknüpfungssymbole wie in $\mathbb{R}$ benutzt. Dies wird, wie wir sehen werden, nicht irgendwelche Probleme bereiten.

Wir probieren diese Verknüpfungen an verschiedenen Beispielen aus.

- Die Addition ist einfach die aus der Schule bekannte Addition von Vektoren in der Zeichenebene.

- Wir betrachten die Verknüpfung für Zahlenpaare, deren zweite Koordinate 0 ist.

  $$(x, 0) + (u, 0) = (x + u, 0), \qquad (x, 0) \cdot (u, 0) = (x \cdot u, 0).$$

  Das bedeutet, dass mit diesen Zahlen genauso gerechnet wird wie mit den reellen Zahlen. Auf diese Weise kann die Menge der reellen Zahlen als Teilmenge der komplexen Zahlen aufgefasst werden. Man sagt auch, dass die Zahlen $(a, 0)$ reell sind.

- Aus der Schule ist Ihnen bekannt, dass Vektoren auch vervielfacht werden können (Skalar–Multiplikation). Wir multiplizieren eine reelle Zahl mit einer beliebigen komplexen Zahl:

  $$(x, 0) \cdot (u, v) = (xu, xv).$$

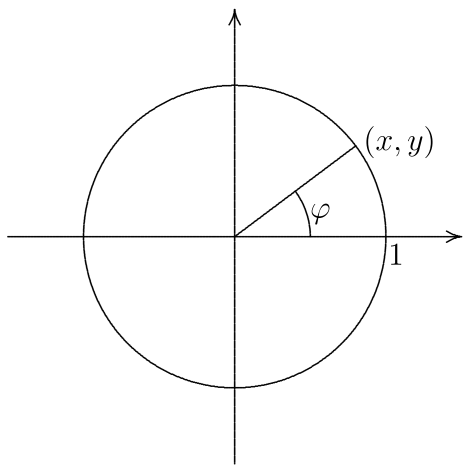
  Dies ist tatsächlich die Vektorvervielfachung.

- Wir betrachten jetzt Zahlen, die auf dem Einheitskreis der komplexen Zahlenebene liegen:

  $$E = \{(x, y) \in \mathbb{C} | x^2 + y^2 = 1\} \subseteq \mathbb{C}$$

  Aus der Analysis weiß man, dass es zu $(x, y) \in E$ eine Zahl $\varphi \in \mathbb{R}$ (Bogenmass) gibt, so dass

  $$(x, y) = (\cos \varphi, \sin \varphi).$$

  Entsprechend gibt es zu einer anderen Zahl $(u, v) \in E$ eine Zahl $\psi \in \mathbb{R}$, so dass $(u, v) = (\cos \psi, \sin \psi)$.

Wir multiplizieren zwei solche Zahlen:

$$
\begin{aligned}
&(u,v)\cdot(x,y) = (\cos\psi,\sin\psi)\cdot(\cos\varphi,\sin\varphi) = \\
&(\cos\psi\cdot\cos\varphi - \sin\psi\cdot\sin\varphi, \cos\psi\cdot\sin\varphi + \cos\varphi\cdot\sin\psi) = \\
&\qquad \text{(Additionstheoreme)} \\
&(\cos(\psi+\varphi),\sin(\psi+\varphi)).
\end{aligned}
$$

Das heißt, die Multiplikation zweier komplexer Zahlen auf dem Einheitskreis bedeutet die Addition der zugehörigen Winkel.

- Spezialfall: Das Quadrat von $(0,1)$.

  $$(0,1)^2 = (0,1)\cdot(0,1) = (-1,0).$$

  Wir haben also eine Wurzel von $-1 \in \mathbb{R}$ gefunden.

- Dies ist Anlaß für eine eingängigere Schreibweise: Wir kürzen ab (definieren):

  $$
  \begin{aligned}
  x &:= (x,0) \quad \text{für alle } x \in \mathbb{R} \\
  i &:= (0,1) \quad\quad (\textit{Imaginäre Einheit})
  \end{aligned}
  $$

  Dann kann eine beliebige komplexe Zahl z ein–eindeutig geschrieben werden als:

  $$z = (x,y) = (x,0) + (0,y) = (x,0) + (0,1)\cdot(y,0) = x + iy$$

  mit $x, y \in \mathbb{R}$. Die reelle Zahl x heißt *Realteil* und y *Imaginärteil* der komplexen Zahl $z = (x,y)$. Man schreibt:

  $$x = \operatorname{Re} z \qquad \text{und} \qquad y = \operatorname{Im} z$$

  Die Multiplikation zweier komplexer Zahlen geht dann wie folgt:

  $$(x+iy)\cdot(u+iv) \overset{DG}{=} xu + xiv + iyu + iyiv = (xu - yv) + i(xv + yu).$$

  Dabei haben wir die Gültigkeit des DG vorweggenommen. Man sieht, dass diese Multiplikation in Übereinstimmung mit der Definition am Anfang ist.

- Polarkoordinaten

  Aus der Analysis ist weiter bekannt, dass sich jede komplexe Zahl wie folgt als Produkt einer nicht–negativen reellen Zahl und einer Zahl auf dem Einheitskreis schreiben lässt:

  $$x + iy = \sqrt{x^2+y^2}\cdot\left(\frac{x}{\sqrt{x^2+y^2}} + i\frac{y}{\sqrt{x^2+y^2}}\right) \;=:\; r\cdot(\cos\varphi + i\sin\varphi).$$

  Man nennt die Darstellung von komplexen Zahlen mit Hilfe von *Betrag* r und *Argument (Phasenwinkel)* φ die *Darstellung in Polarkoordinaten (PKD)*. Es gilt

  $$(r_1\cos\varphi_1, r_1\sin\varphi_1)\cdot(r_2\cos\varphi_2, r_2\sin\varphi_2) = (r_1r_2\cos(\varphi_1+\varphi_2), r_1r_2\sin(\varphi_1+\varphi_2)),$$

  das heißt die Multiplikation zweier komplexer Zahlen manifestiert sich bei Benutzung von Polarkoordinaten als Multiplikation der Beträge und Addition der Phasenwinkel.

Satz 2 $(\mathbb{C}, +, \cdot)$ *ist ein Körper.*

Beweis

- Assoziativgesetz: Vgl. Übung 16.

$$(p \cdot q) \cdot z = p \cdot (q \cdot z).$$

- Das neutrale Element bzgl. der Addition ist $0 = (0, 0)$. Das additive inverse zu einer Zahl $z = (x, y)$ ist $-z = (-x, -y)$.

- Das neutrale Element bzgl. der Multiplikation ist $1 = (1, 0)$. Das zu einem Element $z = (x, y)$ multiplikativ inverse ist gegeben durch $\frac{1}{z} = (\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2})$. In der Tat gilt

$$(x, y) \cdot \Big(\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2}\Big) = \Big(\frac{x^2}{x^2 + y^2} + \frac{y^2}{x^2 + y^2}, \frac{xy}{x^2 + y^2} - \frac{yx}{x^2 + y^2}\Big) = (1, 0).$$

oder — in anderer Schreibweise:

$$\begin{aligned}
&(x + iy) \cdot \Big(\frac{x}{x^2 + y^2} - i\frac{y}{x^2 + y^2}\Big) = \\
&\Big(\frac{x^2}{x^2 + y^2} + \frac{y^2}{x^2 + y^2}\Big) + i\Big(\frac{xy}{x^2 + y^2} - \frac{yx}{x^2 + y^2}\Big) = 1.
\end{aligned}$$

(Wie bei rationalen oder reellen Zahlen wird bei der Division zweier komplexer Zahlen die Bruchschreibweise verwendet.)

- Es bleibt noch, das DG zu zeigen. Wir berechnen getrennt die linke und die rechte Seite:

$$\begin{aligned}
&(x, y) \cdot [(u, v) + (p, q)] = (x, y) \cdot (u + p, v + q) = \\
&\big(x(u + p) - y(v + q), y(u + p) + x(v + q)\big) = \\
&(xu + xp - yv - yq, yu + yp + xv + xq)
\end{aligned}$$

$$\begin{aligned}
&(x, y) \cdot (u, v) + (x, y) \cdot (p, q) = \\
&(xu - yv, yu + xv, xp - yq, xq + yp) = \\
&(xu + xp - yv - yq, yu + yp + xv + xq)
\end{aligned}$$

Nach weiteren Umformungen mit Hilfe der Kommutativgesetze stimmen die beiden Ausdrücke überein. qed.

♦

2.4.2 Absolutbetrag und Konjugation

Wir definieren für komplexe Zahlen $z = x + iy$:

- den *Absolutbetrag*: $|z| \ := \ \sqrt{x^2 + y^2} \in \mathbb{R}_0^+$.
- die *konjugiert–komplexe* Zahl: $\overline{z} \ := \ x - iy$.

Es gilt dann für beliebige $z, w \in \mathbb{C}$:

- $|z| = 0 \quad \Longleftrightarrow \quad z = 0$.
- $|z|^2 = z \cdot \overline{z} \in \mathbb{R}_0^+$.
- $z = \overline{z} \quad \Longleftrightarrow \quad z \in \mathbb{R}$.
- $\overline{z+w} = \overline{z} + \overline{w}, \qquad \overline{z-w} = \overline{z} - \overline{w}, \qquad \overline{z \cdot w} = \overline{z} \cdot \overline{w}, \qquad \overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}$, $w \neq 0$.
- $\overline{\overline{z}} = z$
- $$z^{-1} = \frac{1}{z} = \frac{\overline{z}}{\overline{z} \cdot z} = \frac{\overline{z}}{|z|^2} = \frac{x - iy}{x^2 + y^2}.$$
- $$\operatorname{Re} z = \frac{z + \overline{z}}{2}, \qquad \operatorname{Im} z = \frac{z - \overline{z}}{2i}.$$

3 Vektorräume

Da wir es fast immer mit den konkreten Beispielen $\mathbb{Q}, \mathbb{R}$ oder $\mathbb{C}$ von Körpern zu tun haben werden, benutzen wir ab jetzt generell die Zeichen $+$ und $\cdot$ für die Addition bzw. Multiplikation in einem Körper.

3.1 Definition

Sie werden vermutlich beim Begriff Vektor an Pfeile oder Klassen parallelgleicher Pfeile denken. Tatsächlich sind Pfeile als eine mögliche Veranschaulichung von Vektoren geeignet, man muss aber darauf achten, dass diese Veranschaulichung zu eng oder gar irreführend sein kann. Ganz knapp und nicht ganz exakt kann man sagen, dass Vektoren mathematische Objekte sind, die man addieren und vervielfachen, i.a. aber nicht miteinander multiplizieren kann. Wir wollen dies ganz exakt aufschreiben:

Definition: Es sei ein Körper $\mathbb{K}$ vorgegeben. Eine Menge V heißt $\mathbb{K}$–*Vektorraum* oder *Vektorraum über* $\mathbb{K}$, wenn auf ihr eine Addition

$$\oplus : \begin{cases} V \times V & \to & V \\ (v, w) & \mapsto & v \oplus w \end{cases}$$

und eine *skalare Multiplikation*

$$\odot : \begin{cases} \mathbb{K} \times V & \to & V \\ (\alpha, v) & \mapsto & \alpha \odot v \end{cases}$$

festgelegt sind, so dass folgendes gilt:

- V ist bezüglich der Addition $\oplus$ eine abelsche Gruppe.
- (AG/sM) Für $\alpha, \beta \in \mathbb{K}$ und $v \in V$ gilt:

  $$(\alpha \cdot \beta) \odot v = \alpha \odot (\beta \odot v)$$

- (NE/sM) Für $v \in V$ gilt:

  $$1 \odot v = v.$$

- (DGa/sM) Für $\alpha, \beta \in \mathbb{K}$ und $v \in V$ gilt:

  $$(\alpha + \beta) \odot v = \alpha \odot v \oplus \beta \odot v.$$

- (DGb/sM) Für $\alpha \in \mathbb{K}$ und $v, w \in V$ gilt:

  $$\alpha \odot (v \oplus w) = \alpha \odot v \ \oplus \ \alpha \odot w.$$

Bemerkungen:

1. Die Elemente eines Vektorraums heißen *Vektoren*. Im Zusammenhang mit Vektorräumen heißen die Elemente des Körpers *Skalare*.

2. Sie werden vielleicht aus der Schule die Konvention kennen, dass Vektoren durch kleine Rechtspfeile oberhalb des Symbols gekennzeichnet werden, beispielsweise durch $\vec{v}$, $\vec{w}$ oder ähnlich. Dies ist auch in der wissenschaftlichen Mathematik möglich, aber eher unüblich.

3. Sie werden sich im Laufe des Kurses davon überzeugen können, dass es keine großen Probleme bedeutet, wenn wie für die beiden Vektorraumoperationen $\oplus$ und $\odot$ auch nur die einfachen Symbole $+$ bzw. $\cdot$ benutzen. Oft wird auch der Punkt weggelassen. Man sollte sich aber immer vergegenwärtigen, innerhalb welcher Menge diese Operationen gerade ausgeführt werden.

4. Das (eindeutige) neutrale Element bzgl. der Addition heißt *Nullvektor*. Er wird mit $\vec{0}$, später, wenn keine Verwechslungen auftreten, auch nur mit 0 bezeichnet.

5. Der zu einem Vektor v bezüglich der Addition inverse Vektor heißt der zu v negative Vektor, er wird mit $-v$ bezeichnet.

6. Ein $\mathbb{R}$–Vektorraum wird auch einfach reeller Vektorraum genannt. Entsprechend gibt es komplexe oder rationale Vektorräume.

7. Die Vektorraum–Axiome enthalten keinerlei Aussagen über Basen, lineare Unabhängigkeit oder Dimension.

8. Beachte, dass noch nicht die Rede ist von Länge von Vektoren oder Winkel zwischen Vektoren.

9. Wie oben bei der Formulierung der Distributivgesetze schon zu sehen war, gilt auch in Vektorräumen die Punkt–vor–Stich–Konvention.

Satz 3 *(VR 1): Für $\alpha \in \mathbb{K}$ und $v \in V$ gilt die folgende Äquivalenz*

$$\alpha \cdot v = \vec{0} \qquad \Longleftrightarrow \qquad \alpha = 0 \ \text{oder} \ v = \vec{0}.$$

Beweis Der Beweis besteht aus drei Schritten:

(1) Wir beweisen zuerst die Implikation $\alpha = 0 \Longrightarrow \alpha \cdot v = \vec{0}$.
Für $v \in V$ gilt

$$0 \cdot v = (0 + 0) \cdot v = 0 \cdot v + 0 \cdot v.$$

Deshalb ist $0 \cdot v$ das neutrale Element der Addition, also $0 \cdot v = \vec{0}$.

(2) Wir beweisen dann die Implikation $v = \vec{0} \Longrightarrow \alpha \cdot v = \vec{0}$.
Für $\alpha \in \mathbb{K}$ ist hier

$$\alpha \cdot \vec{0} = \alpha \cdot (\vec{0} + \vec{0}) = \alpha \cdot \vec{0} + \alpha \cdot \vec{0}.$$

Wieder ist $\alpha \cdot \vec{0}$ neutrales Element der Addition, somit $\alpha \cdot \vec{0} = \vec{0}$.

(3) Es bleibt noch der $\Longrightarrow$ Anteil der Behauptung zu zeigen.
Ist $\alpha \in \mathbb{K} \setminus \{0\}$ und $v \in V$ mit $\alpha \cdot v = \vec{0}$, so gilt

$$v = 1 \cdot v = \frac{1}{\alpha} \cdot \alpha \cdot v = \frac{1}{\alpha} \cdot \vec{0} = \vec{0}.$$

Das war's. ♦

3.2 Beispiele

1. Der Vektorraum $\mathbb{K}^n$ der n–Tupel ist gegeben durch

$$\mathbb{K}^n \ := \ \left\{ \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \ \Big| \ v_1, v_2, \ldots, v_n \in \mathbb{K} \right\}$$

   Wir schreiben also n–Tupel von Zahlen aus $\mathbb{K}$ als *Spaltenvektoren*.

   Die Addition und die skalare Multiplikation sind *koordinatenweise* definiert:

$$\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} + \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix} := \begin{pmatrix} v_1 + w_1 \\ v_2 + w_2 \\ \vdots \\ v_n + w_n \end{pmatrix}, \qquad \alpha \cdot \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} := \begin{pmatrix} \alpha \cdot v_1 \\ \alpha \cdot v_2 \\ \vdots \\ \alpha \cdot v_n \end{pmatrix}$$

   Man überzeuge sich (mündlich) davon, dass die Vektorraumaxiome erfüllt sind.

2. • $\mathbb{R}$ ist ein $\mathbb{Q}$–Vektorraum.
   • $\mathbb{C}$ ist ein $\mathbb{Q}$–Vektorraum.
   • $\mathbb{C}$ ist ein $\mathbb{R}$–Vektorraum.

3. Für $n = 1$ kann die Menge $\mathbb{K}^1$ als identisch mit der Menge $\mathbb{K}$ angesehen werden. Die Vektoraddition in $\mathbb{K}^1$ entspricht der Addition in $\mathbb{K}$, die skalare Multiplikation entspricht der Multiplikation in $\mathbb{K}$. Also:

   Sätzchen: Ein Körper kann immer als Vektorraum über sich selbst angesehen werden.

4. Mehr schulisch als mathematisch orientiert sind die Anschauungsräume, die ,,Zeichenebene" und der ,,uns umgebende dreidimensionale Raum". Die Äquivalenzklassen parallelgleicher Pfeile sind die Vektoren. Wie man dies Vektoren addiert bzw. skalar multipliziert, ist aus der Schule bekannt bzw. anschaulich klar.

5. Eine Menge mit genau einem Element kann für jeden Körper $\mathbb{K}$ als $\mathbb{K}$–Vektorraum aufgefasst werden, indem man das einzige Element als Null–Vektor $\vec{0}$ ansieht:

$$\mathbb{K}^0 \ := \ \{\vec{0}\}.$$

   Die Vektoraddition und die skalare Multiplikation sind durch

$$\vec{0} + \vec{0} = \vec{0} \qquad \text{bzw.} \qquad \alpha \cdot \vec{0} = \vec{0} \quad \text{für alle } \alpha \in \mathbb{K}$$

   festgelegt.

6. Definition: Für eine beliebige Menge X heißt eine Abbildung $a : \mathbb{N} \to X$ eine *Folge* in X. Das Bildelemente in X heißen auch *Glieder* der Folge. Sie werden — anders als bei allgemeinen Funktionen üblich — geschrieben als

$$a_n = a(n).$$

Für die gesamte Folge gibt es verschiedene Notationen

$$a = (a_n)_{n \in \mathbb{N}} = (a_n)_n = (a_n) = (a_1, a_2, a_3 \ldots).$$

Beispiele: Durch $a(n) = n^2$ ist die Folge der Quadratzahlen gegeben. Man schreibt

$$a = (n^2)_{n \in \mathbb{N}} = (1, 4, 9, \ldots)$$

Durch $b(n) = 3n + 1$ ist ebenfalls eine Folge festgelegt:

$$b = (3n + 1)_{n \in \mathbb{N}} = (4, 7, 10, \ldots).$$

Wir können zwei Folgen a und b addieren. Die Summenfolge $a + b$ ist definiert als Abbildung $\mathbb{N} \to \mathbb{K}$ durch die Vorschrift

$$(a + b)_n \ := \ a_n + b_n.$$

Wir können auch eine Folge b skalar multiplizieren. Für $\alpha \in \mathbb{K}$ ist die Folge $\alpha \cdot b$ definiert durch

$$(\alpha \cdot b)_n \ := \ \alpha \cdot b_n.$$

Satz: Durch diese *gliedweise* Addition und skalare Multiplikation wird die Menge aller Folgen in $\mathbb{K}$ zu einem $\mathbb{K}$–Vektorraum. Er wird mit $\mathbb{K}^{\mathbb{N}}$ bezeichnet.

In den Beispielen oben:

$$\begin{aligned} a + b &= (5, 11, 19, \ldots) = (n^2 + 3n + 1)_{n \in \mathbb{N}} \\ -\frac{1}{2} \cdot a &= (-\frac{1}{2}, -2, -\frac{9}{2}, \ldots) = (-\frac{n^2}{2})_{n \in \mathbb{N}}. \end{aligned}$$

7. Eine Folge a heißt *finit*, wenn es ein $n \in \mathbb{N}$ gibt, so dass

$$a_m = a(m) = 0 \qquad \text{für alle } m > n.$$

Anders ausgedrückt: Die Folge enthält nur endlich viele Glieder ungleich Null.

Die Menge der finiten Folgen in einem Körper $\mathbb{K}$ bildet unter gliedweiser Addition und skalarer Multiplikation einen Vektorraum. Wir bezeichnen ihn mit $\mathbb{K}_0^{\mathbb{N}}$.

3.3 Grundlagen der Vektorraum–Theorie

Nochmal: Ein $\mathbb{K}$–Vektorraum ist eine Menge von mathematischen Objekten, die sinnvoll addiert und mit Faktoren aus $\mathbb{K}$ vervielfacht werden können. Dass diese beiden Operationen im Mittelpunkt stehen, wird auch an den folgenden wichtigen Definitionen deutlich:

Definitionen: Es sei ein $\mathbb{K}$–Vektorraum V und eine nichtleere Teilmenge $W \subseteq V$ gegeben.

1. Ein Vektor $v \in V$ heißt *Linearkombination* von (Vektoren aus) W, wenn es **endlich viele** Vektoren $w_1, \ldots, w_n \in W$ und Skalare $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ gibt, so dass

   $$v = \alpha_1 w_1 + \cdots + \alpha_n w_n.$$

   Wichtig: Zwei Linearkombinationen sollen als gleich angesehen werden, wenn sie

   - sich nur in der Reihenfolge der Summanden unterscheiden, im Beispiel

     $$3w_1 + 4w_2 - 7w_3 = 4w_2 - 7w_3 + 3w_1$$

     oder
   - mehrere Summanden zum gleichen Vektor $w_k \in W$ auftreten, sich diese zu einem Summanden zusammenfassen lassen, dieser eine Summand dann übereinstimmt, im Beispiel

     $$3w_1 + w_2 - 7w_3 + 3w_2 = 5w_2 + 3w_1 - w_2 - 7w_3.$$

2. Die Menge der Linearkombinationen von W heißt das *Erzeugnis* oder der *Span* von W:

   $$\operatorname{span} W = \langle W \rangle \ := \Big\{ \alpha_1 w_1 + \cdots + \alpha_n w_n \ \Big| \ n \in \mathbb{N}, \alpha_i \in \mathbb{K}, w_k \in W \text{ für alle } k = 1, \ldots, n \Big\}$$

   Ist die Menge $W = \{w_1, \ldots, w_n\}$ endlich, so schreibt man auch

   $$\langle W \rangle = \langle w_1, \ldots, w_n \rangle.$$

   (Man definiert zusätzlich: $\operatorname{span} \varnothing = \langle \varnothing \rangle = \{\vec{0}\}$.)

3. Die Menge W heißt *linear unabhängig* (ℓ.u.) (man sagt auch: die Vektoren aus W sind *linear unabhängig*), wenn jeder Vektor $v \in V$ auf **höchstens** eine Weise als Linearkombination von W dargestellt werden kann.

4. Die Menge W heißt *Erzeugendensystem* von V, wenn jeder Vektor $v \in V$ auf **mindestens** eine Weise als Linearkombination von W dargestellt werden kann.

5. Die Menge W heißt eine *Basis* von V, wenn jeder Vektor $v \in V$ auf **genau** eine Weise als Linearkombination von W dargestellt werden kann.

6. Ist die Menge W nicht linear unabhängig, so heißt sie *linear abhängig.* (Man sagt auch, die Vektoren aus W sind *linear abhängig*).

In Bezug auf den Nullvektor gilt folgendes:

- Für beliebiges W gilt: $\vec{0} \in \langle W \rangle$.

  Begründung: Mit $w \in W$ beliebig gilt $\vec{0} = 0 \cdot w$, also ist $\vec{0}$ als Linearkombination von W darstellbar.

- Enthält eine Menge W den Nullvektor $\vec{0}$, so ist sie linear abhängig.

  Begründung: Der Nullvektor $\vec{0} \in V$ ist auf mehrere verschiedene Arten als Linearkombination von $\vec{0}$ darstellbar, beispielsweise wie folgt:

$$\vec{0} = 0 \cdot \vec{0} = 1 \cdot \vec{0}.$$

Beispiele:

- Die Menge W enthalte genau einen Vektor $w \neq \vec{0}$. Dann gilt:

$$\langle w \rangle = \{\alpha \cdot w | \alpha \in \mathbb{K}\}.$$

  W ist linear unabhängig, da jeder Vektor auf höchstens eine Weise als Linearkombination von W darstellbar ist. Begründung:

  1. Fall: Ist $v \in \langle w \rangle$ und gilt mit $\alpha, \beta \in \mathbb{K}$:

$$v = \alpha \cdot w \quad \text{und} \quad v = \beta \cdot w,$$

  so folgt:

$$(\alpha - \beta) \cdot w = \alpha \cdot w - \beta \cdot w = v - v = \vec{0}.$$

  Wegen $w \neq \vec{0}$ folgt daraus mit dem Satz über die Nullteilerfreiheit in Vektorräumen $\alpha - \beta = 0$ und damit $\alpha = \beta$. Also gibt es genau eine Darstellung als Linearkombination von W.

  2. Fall: Ist $v \notin \langle w \rangle$, so kann v gar nicht als Linearkombination dargestellt werden.

- Wir betrachten den $\mathbb{R}^2$.

  - Die beiden Vektoren $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ und $\begin{pmatrix} 2 \\ 1 \end{pmatrix}$ sind linear unabhängig.

    Gilt nämlich für einen Vektor $v \in \mathbb{R}^2$

$$v = \alpha_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \alpha_2 \begin{pmatrix} 2 \\ 1 \end{pmatrix} \qquad \text{und} \qquad v = \beta_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta_2 \begin{pmatrix} 2 \\ 1 \end{pmatrix},$$

    so folgt $\alpha_1 = \beta_1$ und $\alpha_2 = \beta_2$.

  - Die beiden Vektoren bilden eine Basis von $\mathbb{R}^2$, da jeder Vektor $v = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$ als Linearkombination dargestellt werden kann:

$$v = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = (v_1 - 2v_2) \begin{pmatrix} 1 \\ 0 \end{pmatrix} + v_2 \begin{pmatrix} 2 \\ 1 \end{pmatrix}.$$

– Die beiden Vektoren $\begin{pmatrix} -2 \\ 3 \end{pmatrix}$ und $\begin{pmatrix} 6 \\ -9 \end{pmatrix}$ sind linear abhängig, da (beispielsweise) der Vektor $\begin{pmatrix} 2 \\ -3 \end{pmatrix}$ geschrieben werden kann als

$$\begin{pmatrix} 2 \\ -3 \end{pmatrix} = (-1) \cdot \begin{pmatrix} -2 \\ 3 \end{pmatrix} + 0 \cdot \begin{pmatrix} 6 \\ -9 \end{pmatrix} = 0 \cdot \begin{pmatrix} -2 \\ 3 \end{pmatrix} + \frac{1}{3} \cdot \begin{pmatrix} 6 \\ -9 \end{pmatrix}.$$

Die in dem Beispiel auftretenden Schlussweisen muten umständlich an. Die beiden folgenden Sätze stellen einfachere Kriterien für den Nachweis der Linearen (Un–)Abhängigkeit bereit.

Satz 4 *(VR 2, Charakterisierung der linearen Abhängigkeit)*
Die folgenden Aussagen über eine nichtleere Teilmenge $W \subseteq V$ sind äquivalent:

(i) *W ist linear abhängig.*

(ii) *Es gibt $n \in \mathbb{N}$, paarweise verschiedene Vektoren $w_1, \ldots, w_n \in W$ und Skalare $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ mit $\alpha_k \neq 0$ für mindestens ein $k \in \{1, \ldots, n\}$, so dass*

$$\vec{0} = \alpha_1 w_1 + \cdots + \alpha_n w_n,$$

d.h. der Nullvektor kann als nichttriviale Linearkombination von W geschrieben werden.

Oder: ,,Mit Hilfe" der Vektoren aus W kann eine geschlossene Vektorkette gebildet werden.

(iii) *Es gibt einen Vektor $w \in W$, $n \in \mathbb{N}$, $w_1, \ldots, w_n \in W \setminus \{w\}$ und $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$, so dass*

$$w = \alpha_1 w_1 + \cdots + \alpha_n w_n,$$

d.h. mindestens ein Vektor in W kann als Linearkombination der anderen Vektoren von W geschrieben werden.

Beachte:

Im Satz wird nicht behauptet, dass die Zahlen $n \in \mathbb{N}$, Vektoren $w_1, \ldots, w_n \in W$, Zahlen $\alpha_1, \ldots, \alpha_n \in W$, wie sie in (ii) und (iii) beschrieben werden, jeweils übereinstimmen.

In (iii) wird nicht behauptet, dass jeder Vektor aus W als Linearkombination von anderen Vektoren aus W dargestellt werden kann.

Beweis Wir zeigen die Äquivalenz $(i) \iff (ii) \iff (iii)$ durch einen Ringschluss $(i) \Longrightarrow (ii) \Longrightarrow (iii) \Longrightarrow (i)$.

Es gelte (i), d.h. die Menge W sei linear abhängig. Dann existiert ein Vektor $v \in V$, der auf zwei verschiedene Weisen als Linearkombination von W dargestellt werden kann. Es seien $w_1, w_2, \ldots, w_n$ alle Vektoren aus W, die in der einen oder in der anderen dieser beiden Linearkombinationen vorkommen. Sie seien paarweise verschieden. Es gelte also

$$v = \alpha_1 w_1 + \cdots + \alpha_n w_n \qquad \text{und} \qquad v = \beta_1 w_1 + \cdots + \beta_n w_n.$$

Dabei ist $\alpha_k \neq \beta_k$ für mindestens ein $k \in \{1, \ldots, n\}$. Daraus folgt aber

$$\vec{0} = v - v = (\alpha_1 - \beta_1) w_1 + \cdots + (\alpha_n - \beta_n) w_n$$

mit $\alpha_k - \beta_k \neq 0$. Also ist (ii) — mit $\alpha_k - \beta_k$ anstelle von α_k — bewiesen.

Es gelte jetzt (ii). Das heißt, der Nullvektor kann als nichttriviale Linearkombination dargestellt werden:

$$\vec{0} = \alpha_1 w_1 + \cdots + \alpha_n w_n = \sum_{j=1}^{n} \alpha_j w_j, \qquad \text{mindestens ein } \alpha_j \neq 0.$$

Wir wählen ein k aus, so dass $\alpha_k \neq 0$. Dann folgt aber:

$$\alpha_k w_k = - \sum_{j=1, j\neq k}^{n} \alpha_j w_j$$

und dann

$$w_k = - \sum_{j=1, j\neq k}^{n} \frac{\alpha_j}{\alpha_k} w_j.$$

Das ist aber die Aussage (iii).

Es gelte jetzt (iii). $w \in W$ lasse sich als Linearkombination von anderen Vektoren aus W darstellen. Ist $w = \vec{0}$, so gilt (i). Wir brauchen also nur den Fall $w \neq \vec{0}$ studieren.

$$w = \sum_{j=1}^{n} \alpha_j w_j, \quad w_j \neq w \text{ für alle } j \in \{1, \dots, n\}.$$

In dieser Gleichung stehen aber zwei verschiedene Linearkombinationen aus W, die den Vektor w darstellen. Also ist W linear abhängig. ♦

Satz 5 *(VR 3, Charakterisierung der linearen Unabhängigkeit)*
Die folgenden Aussagen über eine nichtleere Teilmenge $W \subseteq V$ sind äquivalent:

(i) *W ist linear unabhängig.*

(ii) *(Koeffizientenvergleich) Gilt mit $n \in \mathbb{N}$, paarweise verschiedenen $w_k \in W$, $\alpha_k, \beta_k \in \mathbb{K}$ die Gleichung*

$$\alpha_1 w_1 + \cdots + \alpha_n w_n = \beta_1 w_1 + \cdots + \beta_n w_n \qquad (*)$$

so folgt:

$$\alpha_k = \beta_k \quad \text{für alle} \quad k \in \{1, \ldots, n\}.$$

(iii) *Der Nullvektor kann* ***nur*** *als triviale Linearkombination von W geschrieben werden. Strenger mathematisch:*

Wenn $\vec{0} = \alpha_1 w_1 + \cdots + \alpha_n w_n$ gilt mit paarweise verschiedenen $w_1, w_2, \ldots, w_n \in W$, so folgt $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$.

Beweis Die Aussage (ii) ist einfach eine Umformulierung der Definition der linearen Unabhängigkeit. Die Äquivalenz $(i) \iff (iii)$ ist einfach die logische Umkehrung der Äquivalenz $(i) \iff (ii)$ aus Satz VR 1. ♦

Beispiel: Es seien die Vektoren

$$v = \begin{pmatrix} 0 \\ 2 \\ -1 \end{pmatrix}, \quad w = \begin{pmatrix} 1 \\ 0 \\ 3 \end{pmatrix}, \quad p = \begin{pmatrix} 0 \\ 3 \\ 0 \end{pmatrix}, \quad q = \begin{pmatrix} 0 \\ 0 \\ 2 \end{pmatrix}$$

im $\mathbb{R}^3$ gegeben.

- Ist $\{v, w, p\}$ linear unabhängig? JA. Wir setzen

$$\vec{0} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = \alpha_1 v + \alpha_2 w + \alpha_3 p = \alpha_1 \begin{pmatrix} 0 \\ 2 \\ -1 \end{pmatrix} + \alpha_2 \begin{pmatrix} 1 \\ 0 \\ 3 \end{pmatrix} + \alpha_3 \begin{pmatrix} 0 \\ 3 \\ 0 \end{pmatrix}.$$

  Dann folgt (sukzessive): $\alpha_2 = 0$, $\alpha_1 = 0$, $\alpha_3 = 0$.

- Ist $\{v, p, q\}$ linear unabhängig? NEIN. Wir können nämlich den Nullvektor als nichttriviale Linearkombination dieser Menge schreiben:

$$\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = -6 \begin{pmatrix} 0 \\ 2 \\ -1 \end{pmatrix} + 4 \begin{pmatrix} 0 \\ 3 \\ 0 \end{pmatrix} + 3 \begin{pmatrix} 0 \\ 0 \\ 2 \end{pmatrix}$$

3.4 Basen und Dimension eines Vektorraums

Grundlegende Frage: Gibt es in jedem Vektorraum eine Basis?
Beispiele:

- Im $\mathbb{K}^n$ definieren wir die Vektoren

$$e_j = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \qquad \text{mit der 1 in der } j\text{–ten Zeile.}$$

  Die Menge

$$E = \{e_j | j = 1, \dots, n\}$$

  ist eine Basis des $\mathbb{K}^n$. Sie heißt die *kanonische Basis* oder *Standardbasis* von $\mathbb{K}^n$.

  Begründung: Jeder Vektor $v \in \mathbb{K}^n$ läßt sich in dieser Basis darstellen:

$$v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = v_1 e_1 + \cdots + v_n e_n.$$

  Es ist offensichtlich, dass diese Darstellung eindeutig ist.

- Der $\mathbb{R}$–Vektorraum $\mathbb{C}$ besitzt die Menge $\{1, i\}$ als Basis. Jede komplexe Zahl z läßt sich nämlich schreiben als $z = x + iy$. Außerdem sind die reellen Zahlen x, y durch z eindeutig bestimmt.

- Im Vektorraum $\mathbb{K}^{\mathbb{N}}$ der Folgen definieren wir ähnlich wie oben die Folge

$$e_j = (0, \dots, 0, 1, 0, \dots) \qquad \text{mit genau einer 1 an der } j\text{–ten Stelle.}$$

  Die Menge

$$E = \{e_j | j \in \mathbb{N}\}$$

  ist linear unabhängig.

  Begründung: Gilt für ein $n \in \mathbb{N}$ und $\alpha_1, \dots, \alpha_n \in \mathbb{K}$

$$\vec{0} = \sum_{j=1}^{n} \alpha_j e_j,$$

  so folgt $\alpha_j = 0$ für alle $j \in \{1, \dots, n\}$.

  Die Menge E ist aber keine Basis von $\mathbb{K}^{\mathbb{N}}$, da sich beispielsweise die Konstant–1–Folge $(1, 1, 1, \dots)$ nicht als Linearkombination (endlich viele Summanden!) von E darstellen läßt.

- Die Menge E ist aber eine Basis des Vektorraums $\mathbb{K}_0^{\mathbb{N}}$ der finiten Folgen. Für jede finite Folge gibt es nämlich eine Darstellung

$$a = a_1 e_1 + \cdots + a_m e_m,$$

wobei m die größte Zahl ist, für die die Folge $(a_n)_{n\in\mathbb{N}}$ an der Stelle m ein Glied ungleich Null hat.

Satz 6 *(VR 4: Ergänzung, Herausnahme und Austausch von Vektoren) Es sei W eine Teilmenge des $\mathbb{K}$–Vektorraums V. Dann gilt:*

(i) Ist W linear unabhängig, aber kein Erzeugendensystem, so gibt es einen Vektor $w \in V \setminus W$, so dass $W \cup \{w\}$ immer noch linear unabhängig ist.

(ii) Ist W ein Erzeugendensystem, aber nicht linear unabhängig, so gibt es einen Vektor $w \in W$, so dass $W \setminus \{w\}$ immer noch ein Erzeugendensystem ist.

(iii) (Austauschlemma) Ist W eine Basis, so gibt es zu jedem Vektor $v \in V \setminus \{\vec{0}\}$ einen Vektor $w \in W$, so dass

$$W' \;:=\; (W \setminus \{w\}) \cup \{v\}$$

ebenfalls eine Basis ist.

Genauer: Hat der Vektor v die Darstellung

$$v = \sum_{j=1}^{n} \alpha_j w_j$$

als Linearkombination von W, so kann er gegen jeden Vektor $w_k \in W$, für den $\alpha_k \neq 0$ in dieser Darstellung gilt, ausgetauscht werden.

Bemerkung: Ein Lemma ist ein Hilfssatz, der zum Beweis eines anderen Satzes gebraucht wird.

Beweis (Zum Teil in Ü 29). Zu (i) Da W kein Erzeugendensystem ist, gibt es einen Vektor $w \in V$, der nicht als Linearkombination von W darstellbar ist. Es gilt $w \notin W$. Wir zeigen jetzt, dass $W \cup \{w\}$ linear unabhängig ist. Dazu betrachten wir eine beliebige Linearkombination von $W \cup \{w\}$, die den Nullvektor darstellt:

$$\vec{0} = \alpha \cdot w + \sum_{j=1}^{n} \alpha_j w_j.$$

1. Fall: $\alpha = 0$. Dann sind wegen der linearen Unabhängigkeit von W auch die Zahlen $\alpha_j = 0$.
2. Fall: $\alpha \neq 0$. Daraus folgt, dass w als Linearkombination von W darstellbar ist. Widerspruch, vgl. Satz VR 3(iii).

Zu (ii): W ist linear abhängig, also gibt es nach Satz VR 2(iii) einen Vektor $w \in W$, der als Linearkombination von n anderen Vektoren $w_j \in W \setminus \{w\}$ dargestellt werden kann:

$$w = \sum_{j=1}^{n} \alpha_j w_j.$$

Ein beliebiger Vektor $v \in V$ ist nach Voraussetzung als Linearkombination von w und m anderen Vektoren $p_j \in W \setminus \{w\}$ darstellbar:

$$v = \beta w + \sum_{j=1}^{m} \beta_j p_j.$$

Daraus folgt aber:

$$v = \beta \cdot \big(\sum_{j=1}^{n} \alpha_j w_j \big) + \sum_{j=1}^{m} \beta_j p_j = \sum_{j=1}^{n} \beta \alpha_j w_j + \sum_{j=1}^{m} \beta_j p_j.$$

Also ist v auch als Linearkombination von $W \setminus \{w\}$ darstellbar.

Zu (iii) v ist als Linearkombination von W darstellbar:

$$v = \sum_{j=1}^{n} \alpha_j w_j. \qquad (*)$$

Wegen $v \neq \vec{0}$ gibt es ein $k \in \{1, \ldots, n\}$, so dass

$$\alpha_k \neq 0.$$

Wir beweisen, dass die Menge $W' := (W \setminus \{w_k\}) \cup \{v\}$ linear unabhängig und ein Erzeugendensystem ist.

1. W' ist ein Erzeugendensystem. Ist $p \in V$ ein beliebiger Vektor, so ist er als Linearkombination von W, das heißt evtl. von w_k und m anderen Vektoren w'_j aus W, darstellbar:

   $$p = \beta w_k + \sum_{j=1}^{m} \beta_j w'_j.$$

   Wegen $(*)$ ist

   $$w_k = \frac{1}{\alpha_k} \cdot \Big(v - \sum_{j=1, j\neq k}^{n} \alpha_j w_j \Big).$$

   Daraus folgt aber:

   $$\begin{aligned} p &= \beta \cdot \Big[\frac{1}{\alpha_k} \cdot \Big(v - \sum_{j=1, j\neq k}^{n} \alpha_j w_j \Big) \Big] + \sum_{j=1}^{m} \beta_j w'_j = \\ &= \frac{\beta}{\alpha_k} v - \sum_{j=1, j\neq k}^{n} \frac{\beta\, \alpha_j}{\alpha_1} w_j + \sum_{j=1, j\neq k}^{m} \beta_j w'_j. \end{aligned}$$

   Also ist p als Linearkombination von W' darstellbar.

2. W' ist linear unabhängig. Es sei

$$\vec{0} = \gamma v + \sum_{j=1}^{\ell} \gamma_j w'_j \qquad \text{mit} \qquad w'_j \in W$$

eine Darstellung des Nullvektors als Linearkombination von W'.

1. Fall: Ist $\gamma = 0$, so ist

$$\vec{0} = \sum_{j=1}^{\ell} \gamma_j w'_j.$$

eine Linearkombination von W. Da W linear unabhängig ist, folgt $\gamma_j = 0$ für alle $j = 1, \ldots, \ell$. Es folgt, dass W' linear unabhängig ist.

2. Fall: Ist $\gamma \neq 0$, so gilt

$$\vec{0} \overset{(*)}{=} \gamma \Big(\sum_{j=1}^{n} \alpha_j w_j \Big) + \sum_{j=1}^{\ell} \gamma_j w'_j = \gamma\alpha_k\, w_k + \sum_{j=1, j\neq k}^{n} \gamma\alpha_j w_j + \sum_{j=1}^{\ell} \gamma_j w'_j.$$

Aufgrund von $\gamma\alpha_k \neq 0$ kann aber dann w_k als Linearkombination von anderen Vektoren aus W dargestellt werden im Widerspruch dazu, dass W linear unabhängig ist (vgl. Satz VR 2(iii)).

♦

Satz 7 *(VR 5) Jeder Vektorraum besitzt eine Basis.*

Beweis Wir können diesen Satz nur für einen (für uns wichtigen) Spezialfall vollständig beweisen. Beobachtungen:

- Direkt aus der Definition folgt, dass eine Menge $W \subseteq V$ genau dann eine Basis ist, wenn sie linear unabhängig ist und ein Erzeugendensystem ist.
- Die Menge $\{w\}$ mit $w \neq 0$ ist immer linear unabhängig, im allgemeinen aber kein Erzeugendensystem.
- Der gesamte Vektorraum V ist immer ein Erzeugendensystem, aber nicht linear unabhängig.

Beim Beweis des Satzes geht es darum, durch geeignetes ,,Vergrößern" von $\{w\}$ oder ,,Verkleinern" von V eine Basis zu finden.

- Wir können beweisen: Besitzt V ein endliches Erzeugendensystem, so besitzt V auch eine (endliche) Basis.

  Begründung (Herausnahmeverfahren): Wir nehmen gemäß (ii) des letzten Satzes sukzessive Vektoren aus dem gegebenen endlichen Erzeugendensystem heraus, bis wir nach endlich vielen Schritten genau bei einer linear unabhängigen Menge angekommen sind, die dann auch ein Erzeugendensystem, also auch eine Basis, ist.
- Besitzt der Vektorraum V kein endliches Erzeugendensystem, so könnte man das obige ,,Herausnahmeverfahren" mit dem Erzeugendensystem V starten. Es wäre aber i.a. nicht in endlich vielen Schritten durchführbar. Durch ein Axiom der Mengenlehre, das sogenannte *Auswahlaxiom* oder das dazu äquivalente *Zorn'sche Lemma* wird sichergestellt, dass auch in diesem Fall irgendwo zwischen $\{w\}$ und V eine Basis existiert.

♦

Satz 8 *(VR 6: Steinitz'scher Austauschsatz) Es sei B eine Basis des $\mathbb{K}$–Vektorraums V und $W = \{w_1, \ldots, w_n\}$ eine linear unabhängige Teilmenge von V.*

(i) Dann gibt es n verschiedene Vektoren $v_1, \ldots, v_n$ in B, so dass

$$B' := (B \setminus \{v_1, \ldots, v_n\}) \cup \{w_1, \ldots, w_n\}$$

ebenfalls eine Basis von V ist.

(ii) Die linear unabhängige Teilmenge $W = \{w_1, \ldots, w_n\}$ kann durch Vektoren aus B zu einer Basis ergänzt werden.

(iii) Es gilt: $|B| \geq n$.

Beweis *(ii) und (iii) sind direkte Folgerungen von (i). Wir beweisen den Teil (i) durch Induktion über die Anzahl $n \in \mathbb{N}$ der auszutauschenden Vektoren.*
Der Fall $n = 1$ ist bereits durch das Austauschlemma abgedeckt.
Wir nehmen jetzt als Induktionsvoraussetzung an, dass der Satz für $n - 1$ richtig ist. Wir wissen also bereits, dass $n - 1$ Vektoren $v_1, \ldots, v_{n-1} \in B$ existieren, so dass

$$B'' := (B \setminus \{v_1, \ldots, v_{n-1}\}) \cup \{w_1, \ldots, w_{n-1}\}$$

eine Basis ist. Dann besitzt der noch einzufügende Vektor w_n eine Darstellung

$$w_n = \sum_{j=1}^{m} \beta_j p_j + \sum_{j=1}^{n-1} \alpha_j w_j$$

mit Vektoren aus B''. Angenommen, alle β_j wären Null. Dann wäre aber

$$w_n = \sum_{j=1}^{n-1} \alpha_j w_j$$

im Widerspruch zur linearen Unabhängigkeit von $\{w_1, \ldots, w_n\}$. Es existiert also ein $\beta_j \neq 0$, sagen wir, es ist β_k. Dann kann aber nach dem Austauschlemma $v_n := p_k$ durch w_n ersetzt werden. Die Menge

$$B' := (B'' \setminus \{p_k\}) \cup \{w_n\} = (B' \setminus \{v_1, \ldots, v_{n-1}, v_n\}) \cup \{w_1, \ldots, w_{n-1}, w_n\}$$

ist also die gewünschte neue Basis. ♦

Folgerung 9 *(VR 7) Es sei $B' = \{b_1, \ldots, b_n\}$ eine Basis des Vektorraums V und B eine weitere Basis. Dann enthält auch B genau n Elemente.*

Beweis Da B' linear unabhängig ist, enthält nach dem Austauschsatz von Steinitz, Teil (iii), (mit $W = B'$), auch B mindestens n Elemente.

Wir nehmen jetzt an, B enthält eine Teilmenge B'' mit $n + 1$ Elementen. Da B linear unabhängig ist, ist auch B'' linear unabhängig. Nach dem Austauschsatz von Steinitz, Teil (iii), (mit $W = B''$), enthält dann aber B' mindestens $n+1$ Elemente. Widerspruch. ♦

Wir setzen ab jetzt für diese Vorlesung voraus: Alle vorkommenden Vektorräume haben eine **endliche Basis**.

Da jede dieser endlichen Basen gleich viele Elemente enthält, können wir definieren:

Definition: Die Mächtigkeit einer Basis B eines $\mathbb{K}$–Vektorraums V (mit endlicher Basis) heißt die *Dimension* des Vektorraums V. Man schreibt dafür

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

Ein Vektorraum mit endlicher Basis heißt auch *endlich–dimensional.*

Bei der Festlegung der Dimension eines Vektorraums kommt es darauf an, über welchem Körper er betrachtet wird. Um dies genauer zu betonen, müsste man eigentlich von der $\mathbb{K}$–*Dimension* sprechen und die Schreibweise $\dim_{\mathbb{K}} V$ benutzen.

Beispiele:

- Der Vektorraum $\mathbb{K}^n$ hat die Dimension n. Wir kennen bereits zwei Basen der Mächtigkeit n.
- Der $\mathbb{R}$–Vektorraum $\mathbb{C}$ hat die Dimension $\dim_{\mathbb{R}} \mathbb{C} = 2$. Als $\mathbb{C}$–Vektorraum hat $\mathbb{C}$ die Dimension $\dim_{\mathbb{C}} \mathbb{C} = 1$.

Folgerung 10 *(VR 8) Der $\mathbb{K}$–Vektorraums V habe die Dimension n.*

(i) Es sei W eine beliebige linear unabhängige Teilmenge von V. Dann gilt:

$$|W| \leq n$$

$$|W| = n \qquad \Longleftrightarrow \qquad W \text{ ist eine Basis von } V$$

(ii) Es sei W ein beliebiges Erzeugendensystem von V. Dann gilt:

$$|W| \geq n$$

$$|W| = n \qquad \Longleftrightarrow \qquad W \text{ ist eine Basis von } V$$

Beweis *Zu (i): Die erste Aussage ist bereits in Satz VR 5 enthalten. Die $\Leftarrow$ Richtung des zweiten Teils ist ebenfalls schon bewiesen. Für die $\Rightarrow$ Richtung wende man Satz VR 5 (i) auf eine beliebige Basis $B = \{v_1, \ldots, v_n\}$ an. Durch Auswechseln aller Vektoren von B gegen die Vektoren aus W folgt, dass*

$$B' = (B \setminus B) \cup W = W$$

eine Basis ist.

(ii) Angenommen, es existiert ein Erzeugendensystem W mit $m < n$ Elementen. Die Menge W kann nicht linear unabhängig sein, da sie sonst eine Basis mit $m < n$ Elementen wäre. Nach Satz VR 3 (ii) kann W sukzessive verkleinert werden, bis ein linear unabhängiges Erzeugendensystem, d.h. eine Basis, entsteht. Diese hätte aber weniger als n Elemente. Widerspruch.

Wäre ein Erzeugendensystem W mit n Elementen keine Basis, so könnte man diese Menge nach Satz VR 3 (ii) zu einer Basis verkleinern. Diese Basis hätte dann aber weniger als n Elemente. ♦

3.5 Unterräume von Vektorräumen

Definition: Eine Teilmenge $U \subseteq V$ eines $\mathbb{K}$–Vektorraums heißt *Unterraum* von V, wenn U bzgl. der von V her gegebenen Verknüpfungen selbst ein Vektorraum ist.

Satz 11 (UR 1, Charakterisierung von Unterräumen)
Die folgenden Aussagen über eine Teilmenge U des Vektorraums V sind äquivalent:

(A) U ist ein Unterraum.

(B) Für alle $u_1, u_2 \in U$ gilt $u_1 + u_2 \in U$ und für alle $\alpha \in \mathbb{K}$, $u \in U$ gilt $\alpha u \in U$.

(C) Für alle $\alpha_1, \alpha_2 \in \mathbb{K}, u_1, u_2 \in U$ gilt

$$\alpha_1 u_1 + \alpha_2 u_2 \in U.$$

Beweis (i) $\iff$ (ii) ist lediglich eine Präzisierung der obigen Definition. (iii) ist eine Zusammenfassung der beiden Aussagen von (ii). ♦
Beispiele:

- Jeder Vektorraum V besitzt die sogenannten *trivialen* Unterräume V und $\{\vec{0}\}$.
- Es sei W eine Teilmenge von V. Dann ist das Erzeugnis $\operatorname{span} W = \langle W \rangle$ ein Unterraum von V.

  Begründung: Es seien $u_1, u_2 \in \operatorname{span} W$, $\alpha_1, \alpha_2 \in \mathbb{K}$. Die beiden Vektoren sind Linearkombinationen von W:

  $$u_1 = \sum_{j=1}^{n} \beta_j w_j \qquad \text{und} \qquad u_2 = \sum_{j=1}^{m} \gamma_j w'_j$$

  Für beliebige $\alpha_1, \alpha_2 \in \mathbb{K}$ gilt dann

  $$\alpha_1 u_1 + \alpha_2 u_2 = \sum_{j=1}^{n} \alpha_1 \beta_j w_j + \sum_{j=1}^{m} \alpha_2 \gamma_j w'_j.$$

  Dieser Vektor ist ebenfalls eine Linearkombination von W, also enthalten in $\operatorname{span} W$. qed.
- Im ,,Anschauungsraum" bilden Geraden oder Ebenen durch den Ursprung Unterräume.

Da ein Unterraum ein „selbstständiger" Vektorraum ist, hat er Basen und eine Dimension.

Satz 12 (UR 2) *Es seien U ein Unterraum von V.*

(i) Es ist: $\dim U \leq \dim V$.

(ii) $\dim U = \dim V \quad \Longleftrightarrow \quad U = V$.

Beweis (i) Es sei B' eine Basis von U.

Ist v ein beliebiger Vektor aus V, so lässt er sich

- im Fall $v \in U$ auf genau eine Weise,
- im Fall $v \notin U$ auf keine Weise,
- im allgemeinen also auf höchstens eine Weise

als Linearkombination von B' darstellen. Das aber bedeutet, dass B' eine linear unabhängige Teilmenge von V ist, die zu einer Basis B von V ergänzt werden kann.

Daraus folgt aber $|B'| \leq |B|$ und das ist genau die Aussage von (i).

(ii) Die $\Leftarrow$ Richtung ist trivial. Nach Satz VR 5(i) können wir eine Basis B' von U zu einer Basis B von V ergänzen. Wegen $\dim U = \dim V$ muss dann aber $B = B'$ gelten. Da jeder Vektor $v \in V$ als Linearkombination von B dargestellt werden kann, kann er auch als Linearkombination von B' dargestellt werden. Damit gilt $v \in U$ für jeden beliebigen Vektor $v \in V$, also $V = U$. ♦

Auf der „Menge aller Unterräume" kann man Verknüpfungen definieren:

Satz 13 (und Definition UR 3) *Es seien U_1, U_2 Unterräume des Vektorraums V.*
(i) Die Menge $U_1 \cap U_2$ ist ein Unterraum von V, der sogenannte Schnittraum.
(ii) Der von U_1 und U_2 erzeugte Raum

$$U_1 + U_2 \; := \; \langle U_1 \cup U_2 \rangle = \{u_1 + u_2 | u_1 \in U_1, u_2 \in U_2\}$$

ist ein Unterraum von V.
(iii) Beachte, dass $U_1 \cup U_2$ im allgemeinen kein Unterraum ist.

Beweis Übung! ♦

Satz 14 (UR 4) *Sind U_1, U_2 Unterräume des Vektorraums V, so gilt*

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

Machen Sie sich diese Gleichung anhand verschiedener Beispiele (Geraden, Ebenen im 3–dimensionalen Anschauungsraum) klar.

Beweis (0) Der Beweis lässt sich durchsichtiger ausführen, wenn wir die Bezeichnungen ändern. Wir setzen

$$U \; := \; U_1 \cap U_2, \quad W \; := \; U_1 + U_2, \quad P \; := \; U_1, \quad Q \; := \; U_2$$

und wollen zeigen, dass

$$\dim P + \dim Q = \dim U + \dim W.$$

(1) Eine Basis $B_U = \{u_1, \ldots, u_n\}$ von U kann sowohl zu einer Basis $B_P = \{u_1, \ldots, u_n, p_1, \ldots, p_m\}$ von P als auch zu einer Basis $B_Q = \{u_1, \ldots, u_n, q_1, \ldots, q_\ell\}$ von Q ergänzt werden. Wir zeigen jetzt, dass

$$B_W := \{u_1, \ldots, u_n, p_1, \ldots, p_m, q_1, \ldots, q_\ell\}$$

eine Basis von W ist.

(2) Zunächst ist klar, dass B_W ein Erzeugendensystem für W ist, denn es kann jeder Vektor aus $\langle P \cup Q \rangle$ als Linearkombination von Vektoren aus P und Vektoren aus Q, damit als Linearkombination der Basen B_P und B_Q, damit als Linearkombination von B_W geschrieben werden.

(3) Um die lineare Unabhängigkeit von B_W zu zeigen, setzen wir den Nullvektor als Linearkombination an:

$$\vec{0} = \underbrace{\sum_{j=1}^{n} \alpha_j u_j}_{=:\, u} + \underbrace{\sum_{j=1}^{m} \beta_j p_j}_{=:\, p} + \underbrace{\sum_{j=1}^{\ell} \gamma_j q_j}_{=:\, q} . \qquad (*)$$

Daraus folgt aber, dass der Vektor $q \in Q$ wegen

$$q = -u - p \in P$$

in $U = P \cap Q$ enthalten ist, deshalb als Linearkombination von B_U geschrieben werden kann:

$$\sum_{j=1}^{\ell} \gamma_j q_j = q = \sum_{j=1}^{k} \delta_j u_j$$

Diese Gleichung stellt q als Linearkombinationen von zwei disjunkten Teilmengen von B_Q dar, was nur im Fall $q = 0$ möglich ist.

Völlig analog zeigt man, dass $p = 0$ ist, es folgt mit $(*)$, dass $u = \vec{0}$.

Die lineare Unabhängigkeit B_U, B_P, B_Q impliziert nun, dass alle Koeffizienten in $(*)$ Null sein müssen.

(4) Jetzt kann man leicht nachrechnen:

$$\begin{aligned} \dim P + \dim Q &= (n+m) + (n+\ell) = n + (n+m+\ell) \\ &= \dim(P \cap Q) + \dim(P + Q). \end{aligned}$$

♦

4 Lineare Abbildungen

4.1 Definition und erste Eigenschaften

Definition: Es sei $\mathbb{K}$ ein Körper und V, W seien zwei $\mathbb{K}$–Vektorräume. Eine Abbildung $f : V \to W$ heißt $\mathbb{K}$–*linear*, meist einfach nur *linear*, wenn sie die Eigenschaft

$$f(\alpha_1 \cdot v_1 + \alpha_2 \cdot v_2) = \alpha_1 \cdot f(v_1) + \alpha_2 \cdot f(v_2) \qquad \text{für alle } v_1, v_2 \in V,\ \alpha_1, \alpha_2 \in \mathbb{K}$$

hat. Beispiele:

- Es sei $\alpha \in \mathbb{K}$ ein beliebiger Skalar. Die Abbildung

  $$m_\alpha : \begin{cases} V & \to & V \\ v & \mapsto & \alpha \cdot v, \end{cases}$$

  die jedem Vektor das α–fache zuordnet, heißt (vor allem in Schulterminologie) *zentrische Streckung*, manchmal auch — im Fall $\alpha \in]0,1[\subseteq \mathbb{R}$ *zentrische Stauchung*. Wir zeigen, dass sie linear ist: Für beliebige $v_1, v_2 \in V$, $\alpha_1, \alpha_2 \in \mathbb{K}$ gilt nämlich

  $$\begin{aligned} & m_\alpha(\alpha_1 \cdot v_1 + \alpha_2 \cdot v_2) = \alpha \cdot (\alpha_1 \cdot v_1 + \alpha_2 \cdot v_2) = && \text{(DG,KG)} \\ & \alpha_1 \cdot \alpha \cdot v_1 + \alpha_2 \cdot \alpha \cdot v_2 = \alpha_1 \cdot m_\alpha(v_1) + \alpha_2 \cdot m_\alpha(v_2). \end{aligned}$$

- Für $\alpha = 0 \in \mathbb{K}$ ist die obige Abbildung m_0 die lineare Abbildung, die jeden Vektor $v \in V$ auf den Nullvektor $\vec{0}$ abbildet. Sie heißt *Nullabbildung*.

- Für $\alpha = 1 \in \mathbb{K}$ ist m_1 die lineare Abbildung, die jeden Vektor $v \in V$ auf sich selbst abbildet. Wir kennen den Namen dieser Abbildung bereits (vgl. Seite 15), es ist die identische Abbildung:

  $$m_1 = \mathrm{id}_V.$$

Satz 15 (LA1: Eigenschaften von linearen Abbildungen)
Es sei $f : V \to W$ eine lineare Abbildung zwischen zwei $\mathbb{K}$–Vektorräumen.

(i) Die Abbildung f bildet den Nullvektor $\vec{0} \in V$ auf den Nullvektor $\vec{0} \in W$ ab.

(ii) Die Bildmenge des gesamten Vektorraums V

$$\mathrm{im}\, f \ := \ f(V) = \{w \in W \mid \text{ Es ex. } v \in V \text{ mit } f(v) = w\},$$

sie heißt auch das Bild *von f, ist ein Unterraum von W.*

(iii) Das Urbild des Nullvektors $\vec{0} \in W$

$$\ker f \ := \ f^{-1}(\vec{0}) = \{v \in V \mid f(v) = \vec{0}\},$$

es heißt der Kern *von f, ist ein Unterraum von V.*

Beweis
(i) Es gilt:

$$f(\vec{0}) = f(\vec{0} + \vec{0}) = f(\vec{0}) + f(\vec{0}).$$

Wir ziehen auf beiden Seiten dieser Gleichung den Vektor $f(\vec{0})$ ab und erhalten so $f(\vec{0}) = \vec{0}$.

(ii) Es seien $w_1, w_2 \in \operatorname{im} f$ zwei Vektoren im Bild von V und $\alpha_1, \alpha_2 \in \mathbb{K}$. Dann gibt es Vektoren $v_1, v_2 \in V$, so dass

$$f(v_1) = w_1, \qquad f(v_2) = w_2.$$

Dann gilt aber weiter

$$\alpha_1 w_1 + \alpha_2 w_2 = \alpha_1 f(v_1) + \alpha_2 f(v_2) = f(\alpha_1 v_1 + \alpha_2 v_2),$$

also liegt auch jede beliebige Linearkombination von $\operatorname{im} f$ in $\operatorname{im} f$.

(iii) Es seien $v_1, v_2 \in \ker f$ zwei Vektoren im Kern von f, $\alpha_1, \alpha_2 \in \mathbb{K}$. Dann gilt

$$f(\alpha_1 v_1 + \alpha_2 v_2) = \alpha_1 f(v_1) + \alpha_2 f(v_2) = \vec{0},$$

also liegt auch jede beliebige Linearkombination von $\ker f$ in $\ker f$. ♦

4.2 Lineare Abbildungen und Basen

Eine Abbildung $f : X \to Y$ zwischen zwei Mengen X und Y ist durch die Angabe des Wertes $f(x)$ für jedes $x \in X$ eindeutig charakterisiert.

Bei linearen Abbildungen genügt es, die Bilder der Elemente einer Basis zu kennen.

Satz 16 (LA 2: Lineare Abbildungen und Basen) *Für zwei $\mathbb{K}$–Vektorräume V, W seien vorgegeben …*

- *eine Basis $B = \{v_1, \dots, v_n\}$ mit n Elementen von V,*
- *eine Teilmenge $W' = \{w_1, \dots, w_n\}$ mit n Elementen von W.*

(i) Dann gibt es genau eine lineare Abbildung $f : V \to W$ mit

$$f(v_j) = w_j \qquad \text{für } j = 1, \dots, n.$$

(ii) Die in der folgenden Tabelle aufgeführten Eigenschaften der Menge W' und der linearen Abbildung f sind zeilenweise äquivalent. Die lineare Abbildung f heißt dann jeweils, wie in der dritten Spalte angegeben.

Die Menge W' ist …	*Die Abbildung f ist …*	*f heißt dann auch …*
ein Erzeugendensystem	*surjektiv*	Epimorphismus
linear unabhängig	*injektiv*	Monomorphismus
eine Basis	*bijektiv*	Isomorphismus

Beweis Um f zu definieren, müssen wir zu jedem Vektor $p \in V$ den Bildvektor angeben. Es sei $p = \sum_{j=1}^{n} \alpha_j v_j$ die Basisentwicklung von p bzgl. der Basis B. Dann definieren wir

$$f(p) \ := \ \sum_{j=1}^{n} \alpha_j w_j.$$

Es ist klar, dass f die Eigenschaft $f(v_j) = w_j$ hat. Außerdem ist f linear. Sind v, v' Vektoren aus V mit Basisentwicklungen

$$v = \sum_{j=1}^{n} \beta_j v_j \quad \text{und} \quad v' = \sum_{j=1}^{n} \beta_j' v_j,$$

und $\alpha_1, \alpha_2 \in \mathbb{K}$, so gilt tatsächlich

$$f(\alpha_1 v + \alpha_2 v') = f\left(\sum_{j=1}^{n} (\alpha_1 \beta_j + \alpha_2 \beta_j') v_j\right) =$$

$$\sum_{j=1}^{n} (\alpha_1 \beta_j + \alpha_2 \beta_j') w_j = \alpha_1 \sum_{j=1}^{n} \beta_j w_j + \alpha_2 \sum_{j=1}^{n} \beta_j' w_j = \alpha_1 f(v) + \alpha_2 f(v').$$

Würde es zwei verschiedene lineare Abbildungen f_1 und f_2 mit der geforderten Eigenschaft geben, so gäbe es mindestens ein $v \in V$, so dass $f_1(v) \neq f_2(v)$. Es sei $v = \sum_{j=1}^{n} \alpha_j v_j$ die Basisentwicklung von v. Dann gilt wegen der Linearität von f_1 und f_2

$$\vec{0} \neq f_1(v) - f_2(v) = f_1(\sum_{j=1}^{n} \alpha_j v_j) - f_2(\sum_{j=1}^{n} \alpha_j v_j) =$$

$$\sum_{j=1}^{n} \alpha_j w_j - \sum_{j=1}^{n} \alpha_j w_j = \vec{0}.$$

Das ist ein Widerspruch.

Zu (ii/1) $\Longrightarrow$: Es sei $W' = \{w_1, \ldots, w_n\}$ ein Erzeugendensystem von W. Dann lässt sich jeder Vektor $w \in W$ schreiben als $w = \sum_{j=1}^{n} \alpha_j w_j$. Dann gilt aber

$$w = \sum_{j=1}^{n} \alpha_j f(v_j) = f(\sum_{j=1}^{n} \alpha_j v_j).$$

Also ist $w \in \operatorname{im} f$. Es liegt also jeder Vektor w im Bild von f, das heißt f ist surjektiv.

Zu (ii/1) $\Longleftarrow$: Es sei f surjektiv. Dann gibt es zu jedem $w \in \operatorname{im} f$ ein $v \in V$, so dass $f(v) = w$. Ist $v = \sum_{j=1}^{n} \alpha_j v_j$ die Basisentwicklung, so gilt

$$w = f(\sum_{j=1}^{n} \alpha_j v_j) = \sum_{j=1}^{n} \alpha_j f(v_j) = \sum_{j=1}^{n} \alpha_j w_j.$$

Also ist W' ein Erzeugendensystem.

Zu (ii/2) $\Longrightarrow$: Es seien $v, v' \in V$ mit Basisentwicklungen

$$v = \sum_{j=1}^{n} \alpha_j v_j \quad \text{und} \quad v' = \sum_{j=1}^{n} \alpha_j' v_j$$

und $f(v) = f(v')$. Dann gilt

$$\vec{0} = f(v) - f(v') = f(\sum_{j=1}^{n} \alpha_j v_j) - f(\sum_{j=1}^{n} \alpha'_j v_j) = \sum_{j=1}^{n} (\alpha_j - \alpha'_j) w_j.$$

Aufgrund der linearen Unabhängigkeit von W' folgt $\alpha_j - \alpha'_j = 0$ für alle $j = 1, \ldots, n$, das heißt $v = v'$. f ist injektiv.
Zu (ii/2) $\Longleftarrow$: Es sei f injektiv und

$$\vec{0} = \sum_{j=1}^{n} \alpha_j w_j$$

eine Linearkombination, die den Nullvektor ergibt. Da f injektiv ist, ist $\vec{0} \in V$ der einzige Vektor in V, der durch f auf den Nullvektor abgebildet wird. Es folgt

$$\vec{0} = \sum_{j=1}^{n} \alpha_j v_j.$$

Da B linear unabhängig ist, folgt $\alpha_j = 0$ für alle j.

Die Einträge in der dritten Zeile sind genau dann erfüllt, wenn die der beiden ersten Zeilen erfüllt sind. Als folgt die dritte Zeile aus den ersten beiden. ♦

4.3 Matrizen

4.3.1 Der Matrizen–Vektorraum $\mathbb{K}^{m\times n}$

Definition: Eine *$m \times n$–Matrix* A ist mathematisch fundiert definiert als eine Abbildung

$$A : \begin{cases} \{1,\ldots,m\} \times \{1,\ldots,n\} & \to & \mathbb{K} \\ (j,k) & \mapsto & a_{jk}. \end{cases}$$

Für uns genügt aber die mehr anschauliche Charakterisierung einer $m \times n$–Matrix A als rechteckiges Schema von Zahlen aus $\mathbb{K}$ mit m Zeilen (erster Index) und n Spalten (zweiter Index). Man schreibt

$$A = (a_{jk}) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}.$$

Umgekehrt wird der Eintrag an der j–ten Zeile und der k–ten Spalte einer Matrix A mit $(A)_{jk}$ bezeichnet. Wir bezeichnen die Menge der $m \times n$–Matrizen mit $\mathbb{K}^{m\times n}$.

Satz 17 (LA 3) *Die Menge der Matrizen $\mathbb{K}^{m\times n}$ bildet unter komponentenweiser Addition und skalarer Multiplikation einen $\mathbb{K}$–Vektorraum der Dimension $m \cdot n$.*

Beweis Es ist offensichtlich, dass die Matrizen

$$E_{jk} = \begin{pmatrix} 0 & \cdots & \cdots & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & & & \vdots & & & & \vdots \\ \vdots & & & \vdots & & & & \vdots \\ 0 & \cdots & \cdots & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & \cdots & 0 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & \cdots & \cdots & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & & & \vdots & & & & \vdots \\ 0 & \cdots & \cdots & 0 & \cdots & \cdots & \cdots & 0 \end{pmatrix}$$

mit einer Eins in der j–ten Zeile und k–ten Spalte und sonst lauter Nullen eine Basis des Vektorraums $\mathbb{K}^{m\times n}$ bilden. ♦

4.3.2 Multiplikation von Matrizen

Definition: Für jeden Körper $\mathbb{K}$ und Zahlen $\ell, m, n \in \mathbb{N}$ ist die Abbildung

$$\cdot : \begin{cases} \mathbb{K}^{\ell\times m} \times \mathbb{K}^{m\times n} & \to & \mathbb{K}^{\ell\times n} \\ (A,B) & \mapsto & C = A \cdot B, \end{cases}$$

— sie heißt *Matrixmultiplikation* oder *Bildung der Produktmatrix* — definiert durch

$$(C)_{jk} = c_{jk} = \sum_{i=1}^{m} a_{ji} b_{ik}. \qquad (\clubsuit)$$

Diese Definition mutet einen Neuling unheimlich an. Man kann sie aber mit Hilfe des folgenden Diagramms (Hakentrick) anschaulich machen.

$$
\begin{array}{ccccc|cccccc}
 & & & & & b_{11} & \cdots & \cdots & b_{1k} & \cdots & b_{1n} \\
 & & & & & \vdots & & & \vdots & & \vdots \\
 & & & & & \vdots & & & \vdots & & \vdots \\
 & & & & & \vdots & & & \vdots & & \vdots \\
 & & & & & b_{m1} & \cdots & \cdots & b_{mk} & \cdots & b_{mn} \\
\hline
a_{11} & \cdots & \cdots & \cdots & a_{1m} & c_{11} & \cdots & \cdots & \cdots & \cdots & c_{1n} \\
\vdots & & & & \vdots & \vdots & & & \downarrow & & \vdots \\
a_{j1} & \cdots & \cdots & \cdots & a_{jm} & \vdots & & \rightarrow & c_{jk} & & \vdots \\
\vdots & & & & \vdots & \vdots & & & & & \vdots \\
a_{\ell 1} & \cdots & \cdots & \cdots & a_{\ell m} & c_{\ell 1} & \cdots & \cdots & \cdots & \cdots & c_{\ell n}
\end{array}
$$

Der Eintrag c_{jk} in der Produktmatrix $C = A \cdot B$ ergibt sich, indem man
den ersten, zweiten, $\ldots$, m–ten Eintrag der j–ten Zeile von A jeweils mit
dem ersten, zweiten, $\ldots$, m–ten Eintrag der k–ten Spalte von B
multipliziert und dann alle Summen aufaddiert.

Satz 18 (LA 5: Eigenschaften der Matrixmultiplikation)

(i) *Für eine Matrix $A \in \mathbb{K}^{m \times n}$ gilt*

$$I_m \cdot A = A \qquad \textit{und} \qquad A \cdot I_n = A.$$

(ii) *Die Matrixmultiplikation ist assoziativ, für drei Matrizen $A \in \mathbb{K}^{m \times n}, B \in \mathbb{K}^{n \times \ell}, C \in \mathbb{K}^{\ell \times p}$ gilt:*

$$(A \cdot B) \cdot C = A \cdot (B \cdot C).$$

(iii) *Die Matrixmultiplikation ist linear: Für „passende" Matrizen A, B, C und Skalare $\alpha, \beta, \gamma \in \mathbb{K}$ gilt:*

$$\begin{aligned} (\alpha A + \beta B) \cdot C &= \alpha\, A \cdot C + \beta\, B \cdot C \\ A \cdot (\beta B + \gamma C) &= \beta\, A \cdot B + \gamma\, A \cdot C \end{aligned}$$

(Für $\alpha = \beta = \gamma = 1$ sind hier Distributivgesetze enthalten).

(iv) *Bei der Matrixmultiplikation gibt es Nullteiler, d.h. es existieren „passende" Matrizen*

$$A \neq 0, \quad B \neq 0 \qquad \textit{mit} \qquad A \cdot B = 0.$$

(v) *Für $n \geq 2$ ist innerhalb von $\mathbb{K}^{n \times n}$ die Matrixmultiplikation nicht kommutativ, d.h. es gibt Matrizen*

$$A, B \in \mathbb{K}^{n \times n} \qquad \textit{mit} \qquad A \cdot B \neq B \cdot A.$$

Beweis
Zu (i): Nachrechnen. Zu (ii): Es seien drei Matrizen

$$A \in \mathbb{K}^{m \times n}, \quad B \in \mathbb{K}^{n \times \ell}, \quad C \in \mathbb{K}^{\ell \times p}$$

gegeben. Es gilt dann für $j = 1, \ldots, p$ und $k = 1, \ldots, m$

$$[(A \cdot B) \cdot C]_{jk} = \sum_{i=1}^{\ell} (A \cdot B)_{ji} c_{ik} = \sum_{i=1}^{\ell} \left(\sum_{h=1}^{n} a_{jh} b_{hi} \right) c_{ik} = \underbrace{\sum_{i=1}^{\ell} \sum_{h=1}^{n} a_{jh} b_{hi} c_{ik}}_{\ell \cdot n \text{ Summanden}} =$$

$$\sum_{h=1}^{n} \sum_{i=1}^{\ell} a_{jh} b_{hi} c_{ik} = \sum_{h=1}^{n} \left(a_{jh} \sum_{i=1}^{\ell} b_{hi} c_{ik} \right) = \sum_{h=1}^{n} a_{jh} (B \cdot C)_{hk} = [A \cdot (B \cdot C)]_{jk}$$

(iii) Nachrechnen.
(iv) und (v) weisen wir durch Beispiele nach:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

♦

4.3.3 Matrizen und lineare Abbildungen $\mathbb{K}^n \to \mathbb{K}^m$

Es sei f eine lineare Abbildung zwischen den Tupel–Vektorräumen $\mathbb{K}^n \to \mathbb{K}^m$. Wie wir gesehen haben, ist diese Abbildung durch die Bilder der Vektoren einer Basis von $\mathbb{K}^n$ eindeutig bestimmt.

Hier bietet es sich an, als Basis die kanonische Basis

$$\{e_k | k = 1, \ldots, n\}$$

vorzugeben. Ist diese Basis fest gewählt, so ist die Information über die lineare Abbildung in den Bildvektoren

$$a_k = \begin{pmatrix} a_{1k} \\ a_{2k} \\ \vdots \\ a_{mk} \end{pmatrix} = f(e_k), \quad k = 1, \ldots, n,$$

gespeichert. Noch besser zusammenfassen lässt sich diese Information in einer $m \times n$–Matrix

$$A_f = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \qquad (\spadesuit)$$

mit m Zeilen und n Spalten. Der Bildvektor $f(e_k)$ von e_k ist gerade die k–te Spalte in dieser Matrix.

Umgekehrt ist durch eine Matrix der obigen Form ($\spadesuit$) eine lineare Abbildung f festgelegt:

$$f(v) = \begin{pmatrix} a_{11}v_1 + a_{12}v_2 + \cdots + a_{1n}v_n \\ a_{21}v_1 + a_{22}v_2 + \cdots + a_{2n}v_n \\ \vdots \\ a_{m1}v_1 + a_{m2}v_2 + \cdots + a_{mn}v_n \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ & \vdots & & \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}$$

Beachte, dass in dem Abbildungsdiagramm und in der Notation für Matrizen die Reihenfolge der Dimensionen von Urbildraum und Bildraum gerade vertauscht ist:

$$f : \mathbb{K}^n \to \mathbb{K}^m \qquad \leftrightsquigarrow \qquad m \times n \text{ –Matrix } A_f.$$

Es seien $f : \mathbb{K}^n \to \mathbb{K}^m$ und $g : \mathbb{K}^m \to \mathbb{K}^\ell$ zwei lineare Abbildungen

$$\mathbb{K}^n \quad \xrightarrow{f} \quad \mathbb{K}^m \quad \xrightarrow{g} \quad \mathbb{K}^\ell$$

mit zugehörigen Matrizen A_f und A_g. Welche Matrix gehört zu der Abbildung $g \circ f : \mathbb{K}^n \to \mathbb{K}^\ell$?

Satz 19 (LA 4: Beziehung zwischen linearen Abbildungen und Matrizen)

(i) Es seien $f : \mathbb{K}^n \to \mathbb{K}^m$ und $g : \mathbb{K}^m \to \mathbb{K}^\ell$ zwei lineare Abbildungen

$$\mathbb{K}^n \quad \xrightarrow{f} \quad \mathbb{K}^m \quad \xrightarrow{g} \quad \mathbb{K}^\ell,$$

denen die $m \times n$–Matrix A_f und die $\ell \times m$–Matrix A_g zugeordnet sind. Dann gilt:

$$A_{g \circ f} = A_g \cdot A_f.$$

Beachte die umgekehrte Reihenfolge in dem Diagramm und in der Matrixgleichung.

(ii) Zur identischen Abbildung

$$\mathrm{id}_{\mathbb{K}^n} : \begin{cases} \mathbb{K}^n & \to & \mathbb{K}^n \\ v & \mapsto & v \end{cases}$$

gehört die $n \times n$–Einheitsmatrix:

$$I = I_n = \begin{pmatrix} 1 & 0 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & 0 & & & \vdots \\ 0 & 0 & 1 & & & \vdots \\ \vdots & & & \ddots & & \vdots \\ \vdots & & & & 1 & 0 \\ 0 & \cdots & \cdots & \cdots & 0 & 1 \end{pmatrix} \qquad \text{(Einheitsmatrix)},$$

die an der Position (j,k) die Zahl

$$(I)_{jk} = \delta_{jk} = \begin{cases} 1, & \text{falls } j = k, \\ 0, & \text{falls } j \neq k. \end{cases} \qquad \text{(Kronecker–Delta–Symbol).}$$

hat.

Beweis Zu (i): Die Einträge der beiden Matrizen seien gegeben durch

$$A_f = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}, \qquad A_g = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1m} \\ b_{21} & b_{22} & \cdots & b_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ b_{\ell 1} & b_{\ell 2} & \cdots & b_{\ell m} \end{pmatrix}.$$

Es seien

$$\{e_j | j = 1, \ldots, n\} \qquad \text{und} \qquad \{e'_j | j = 1, \ldots, m\}$$

die kanonischen Basen von $\mathbb{K}^n$ bzw. $\mathbb{K}^m$.

Gemäß der Zuordnung (♠) ist $f(e_k)$ gerade die k–te Spalte von A_f und $g(e'_j)$ die j–te Spalte von A_g.

$$f(e_k) = \begin{pmatrix} a_{1k} \\ a_{2k} \\ \vdots \\ a_{mk} \end{pmatrix} \qquad \text{und} \qquad g(e'_i) = \begin{pmatrix} b_{1i} \\ b_{2i} \\ \vdots \\ b_{\ell i} \end{pmatrix}$$

Wir müssen den Bildvektor $(g \circ f)(e_k) = g(f(e_k))$ für ein $k \in \{1, \ldots, n\}$ berechnen:

$$\begin{aligned}
g(f(e_k)) &= g(\begin{pmatrix} a_{1k} \\ a_{2k} \\ \vdots \\ a_{mk} \end{pmatrix}) = g(a_{1k}\, e'_1 + a_{2k}\, e'_2 + \cdots + a_{mk}\, e'_m) \\
&= a_{1k}\, g(e'_1) + a_{2k}\, g(e'_2) + \cdots + a_{mk}\, g(e'_m) \\
&= a_{1k} \begin{pmatrix} b_{11} \\ b_{21} \\ \vdots \\ b_{\ell 1} \end{pmatrix} + a_{2k} \begin{pmatrix} b_{12} \\ b_{22} \\ \vdots \\ b_{\ell 2} \end{pmatrix} + \cdots + a_{mk} \begin{pmatrix} b_{1m} \\ b_{2m} \\ \vdots \\ b_{\ell m} \end{pmatrix} \\
&= \begin{pmatrix} b_{11}\, a_{1k} + b_{12}\, a_{2k} + \cdots + b_{1m}\, a_{mk} \\ b_{21}\, a_{1k} + b_{22}\, a_{2k} + \cdots + b_{2m}\, a_{mk} \\ \vdots \\ b_{\ell 1} a_{1k} + b_{\ell 2} a_{2k} + \cdots + b_{\ell m} a_{mk} \end{pmatrix} = \begin{pmatrix} c_{1k} \\ c_{2k} \\ \vdots \\ c_{\ell k} \end{pmatrix}
\end{aligned}$$

Also steht an der Position (j, k) von $C = A_{g \circ f}$ die Zahl

$$c_{jk} = \sum_{i=1}^{m} b_{ji} a_{ik},$$

das ist aber gemäß (♣) das (j, k)–Element in der Matrix $A_g \cdot A_f$.
Zu (ii): Das muss man halt nachrechnen. ♦

4.4 Lineare Gleichungssysteme

Definition Es seien $n, m \in \mathbb{N}$.

(i) Für eine gegebene Matrix $A \in \mathbb{K}^{m \times n}$ und einen gegebenen Vektor $b \in \mathbb{K}^m$ ist durch die Gleichung

$$A \cdot x = b,$$

für den unbekannten Vektor $x \in \mathbb{K}^n$ ein *lineares Gleichungssystem*, abgekürzt *LGS*, gegeben.

(ii) Das lineare Gleichungssystem heißt *homogen*, falls $b = \vec{0}$, anderenfalls heißt es *inhomogen*.

(iii) Im Fall $m = n$ heißt das Gleichungssystem *quadratisch*.

Der Begriff Gleichungssystem kommt daher, dass man die Vektorgleichung in Komponenten schreiben kann und so ein System von Gleichungen entsteht:

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

Es besteht die Aufgabe, die Lösungsmenge

$$\mathcal{L}(A|b) \ := \ \{x \in \mathbb{K}^n | Ax = b\}$$

des LGSs näher zu beschreiben und zu bestimmen.

Satz 20 (LA 6)

(i) Für ein homogenes LGS

$$Ax = \vec{0}$$

ist die Lösungsmenge

$$\mathcal{L}(A|\vec{0}) = \ker A$$

ein Unterraum von $\mathbb{K}^n$. Deutlicher: Sind $x, \widetilde{x} \in \mathbb{K}^n$ Lösungen, $\alpha, \widetilde{\alpha} \in \mathbb{K}$ so ist auch

$$\alpha\, x + \widetilde{\alpha}\, \widetilde{x}$$

eine Lösung.

(ii) WENN $X \in \mathbb{K}^n$ eine Lösung des inhomogenen LGS

$$Ax = b$$

ist, DANN ist die Lösungsmenge ein affiner Raum:

$$\mathcal{L}(A|b) = X + \ker A \ := \ \{X + y \in \mathbb{K}^n | y \in \ker A\}.$$

Sind $x, \widetilde{x}$ Lösungen des inhomogenen LGS, so ist

$$x - \widetilde{x}$$

eine Lösung des homogenen LGS.

(iii) Ein inhomogenes LGS muss nicht unbedingt eine Lösung haben. Beispiel: A ist Nullmatrix, b ist ungleich dem Nullvektor.

Beweis (i) Die erste Aussage ist in LA 1 (iii) enthalten.
(ii) Es sei $x \in \mathcal{L}(A|b)$. Dann gilt

$$A(x - X) = Ax - AX = b - b = \vec{0},$$

also

$$x = X + (x - X) \in X + \ker A.$$

Umgekehrt sei $x \in X + y$ mit $y \in \ker A$. Dann folgt

$$Ax = A(X + y) = AX + Ay = b + \vec{0} = b.$$

♦

Satz 21 (LA 7) *Wir betrachten das LGS*

$$Ax = b$$

mit der quadratischen Matrix $A \in \mathbb{K}^{n \times n}$. Die n Spaltenvektoren von A seien linear unabhängig. Dann hat das LGS genau eine Lösung X:

$$\mathcal{L}(A|b) = \{X\}.$$

Beweis Die Matrix A hat n linear unabhängige Spaltenvektoren aus $\mathbb{K}^n$. Diese bilden eine Basis (vgl. Satz VR 8(i)), die das Bild der kanonischen Basis von $\mathbb{K}^n$ ist. Gemäß Satz LA 2(ii), Tabelle 3. Zeile, ist die lineare Abbildung $x \mapsto Ax$ bijektiv. Also besitzt $b \in \mathbb{K}^n$ genau ein Urbild unter A, anders formuliert: Die Gleichung besitzt genau eine Lösung. ♦

Wir wollen jetzt ein Verfahren angeben, das es gestattet, diese Lösung systematisch–algorithmisch aufzufinden.

Wir erstellen zuerst eine Liste von möglichen *Äquivalenz–Zeilenumformungen*:

- Zwei Zeilen j und k in dem LGS werden vertauscht. Dies entspricht der Multiplikation des LGS mit einer Vertauschungsmatrix P_{jk} von links:

$$P_{jk}A\,x = P_{jk}b.$$

- Die Zeile j in dem LGS wird mit einer Zahl $\alpha \in \mathbb{K}\setminus\{0\}$ multipliziert. Dies entspricht der Multiplikation des LGS mit der Matrix $Q_{j,\alpha}$ von links:

$$Q_{j,\alpha}A\,x = Q_{j,\alpha}b.$$

- Die Zeile j wird durch die Summe der Zeilen j und k ersetzt. Anders formuliert: Die Zeile k wird zu der Zeile j addiert. Dies entspricht der Multiplikation des LGS mit der Matrix $R_{j,k}$ von links:

$$R_{jk}A\,x = R_{jk}b.$$

- Die Kombination der zweiten und dritten Methode führt zu der Umformung, dass die j–te Zeile durch Addition des α–fachen der Zeile k verändert wird.

Satz 22 (LA 8: Gauß'scher Algorithmus I)
Wir betrachten das LGS von Satz LA 7 unter den gleichen Bedingungen. Die Matrix $A|b$ kann durch elementare Zeilenumformungen in die Gestalt

$$\left(\begin{array}{ccccc|c} a_{11}^* & 0 & \cdots & \cdots & 0 & b_1^* \\ 0 & a_{22}^* & \ddots & & \vdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & \cdots & 0 & a_{nn}^* & b_n^* \end{array}\right)$$

mit

$$a_{jj}^* \neq 0, \qquad j = 1, \ldots, n$$

gebracht werden. Damit ist die eindeutige Lösung des LGSs gegeben durch

$$x = \begin{pmatrix} \frac{b_1^*}{a_{11}^*} \\ \frac{b_2^*}{a_{22}^*} \\ \vdots \\ \frac{b_n^*}{a_{nn}^*} \end{pmatrix}.$$

Beweis Wir beweisen durch Induktion über $k = 0, 1, \ldots, n$ die folgenden Aussagen $\mathcal{A}(k)$:
$\mathcal{A}(k)$: Durch elementare Zeilenumformungen kann die Matrix $A|b$ in die Gestalt

$$(A|b)^{(k)} = \left(\begin{array}{ccccc|ccc|c}
a_{11}^{(k)} & 0 & \cdots & \cdots & 0 & a_{1,k+1}^{(k)} & \cdots & a_{1n}^{(k)} & b_1^{(k)} \\
0 & a_{22}^{(k)} & \ddots & & \vdots & \vdots & & \vdots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \vdots & \vdots & & \vdots & \vdots \\
\vdots & & \ddots & \ddots & 0 & \vdots & & \vdots & \vdots \\
0 & \cdots & \cdots & 0 & a_{kk}^{(k)} & a_{k,k+1}^{(k)} & \cdots & a_{kn}^{(k)} & \vdots \\
\hline
0 & \cdots & \cdots & \cdots & 0 & a_{k+1,k+1}^{(k)} & \cdots & a_{k+1,n}^{(k)} & \vdots \\
\vdots & & & & \vdots & \vdots & & \vdots & \vdots \\
0 & \cdots & \cdots & \cdots & 0 & a_{n,k+1}^{(k)} & \cdots & a_{nn}^{(k)} & b_n^{(k)}
\end{array}\right)$$

mit $a_{jj}^{(k)} \neq 0$, $j = 1, \ldots, k$ gebracht werden.

Für $k = 0$ ist

$$(A|b)^{(0)} = A|b.$$

Wir müssen den Induktionsschritt $k \mapsto k+1$ für $k = 0, \ldots, n-1$ durchführen.
(a) Es gilt

$$\begin{pmatrix} a_{k+1,k+1}^{(k)} \\ \vdots \\ a_{n,k+1}^{(k)} \end{pmatrix} \neq \vec{0}.$$

Anderenfalls wären alle Einträge $a_{j\ell}^{(k)}$ in der $(n-k) \times (k+1)$–Teilmatrix unten links gleich Null. Die ersten $k+1$ Spaltenvektoren von $A^{(k)}$ wären linear abhängig. Das kann aber nicht sein aufgrund des Satzes LA 7 oder LA 11 im nächsten Abschnitt.

(b) Durch evtl. Vertauschung zweier Zeilen p und q mit $p, q \in \{k+1, \ldots, n\}$ entsteht die Matrix $(A|b)'$, die an der Position $(k+1, k+1)$ den Eintrag $a'_{k+1,k+1} \neq 0$ hat.

(c) Ziel ist es jetzt, in der $(k+1)$–ten Spalte alle Einträge außer den in der $(k+1)$–ten Zeile „zu Null" zu machen. Dies geschieht dadurch, dass zu der j–ten Zeile (für $j \in \{1, \ldots, k, k+2, \ldots, n\}$) von $(A|b)'$ das

$$(-\frac{a'_{j,k+1}}{a'_{k+1,k+1}})\text{–fache}$$

der Zeile k addiert wird. Es entsteht die Matrix

$$(A|b)^{(k+1)} = \left(\begin{array}{ccccc|ccc|c}
a_{11}^{(k+1)} & 0 & \cdots & \cdots & 0 & a_{1,k+1}^{(k+1)} & \cdots & a_{1n}^{(k+1)} & b_1^{(k+1)} \\
0 & a_{22}^{(k+1)} & \ddots & & \vdots & \vdots & & \vdots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \vdots & \vdots & & \vdots & \vdots \\
\vdots & & \ddots & \ddots & 0 & \vdots & & \vdots & \vdots \\
0 & \cdots & \cdots & 0 & a_{k+1,k+1}^{(k+1)} & a_{k+1,k+2}^{(k+1)} & \cdots & a_{k+1,n}^{(k+1)} & \vdots \\
\hline
0 & \cdots & \cdots & \cdots & 0 & a_{k+2,k+2}^{(k+1)} & \cdots & a_{k+2,n}^{(k+1)} & \vdots \\
\vdots & & & & \vdots & \vdots & & \vdots & \vdots \\
0 & \cdots & \cdots & \cdots & 0 & a_{n,k+2}^{(k+1)} & \cdots & a_{nn}^{(k+1)} & b_n^{(k+1)}
\end{array}\right)$$

mit

$$a_{k+1,k+1}^{(k+1)} = a'_{k+1,k+1} \neq 0 \quad \text{und} \quad a_{jj}^{(k+1)} = a_{jj}^{(k)} \neq 0 \quad \text{für } j = 1, \ldots, k.$$

Damit ist die Aussage auch für $k = n$ gezeigt. Setzt man $(A|b)^* = (A|b)^{(n)}$, so hat man die Aussage des Satzes. ♦

4.5 Der Rang einer Matrix

Definition: Es seien $A \in \mathbb{K}^{m\times n}$ eine Matrix. Die Maximalzahl linear unabhängiger Spaltenvektoren der Matrix A heißt der *Spaltenrang* von A. Die Maximalzahl der linear unabhängiger Zeilenvektoren der Matrix A heißt der *Zeilenrang* von A.

Satz 23 (LA 9) *Wir betrachten die Matrix*

$$A|a^* = \left(\begin{array}{ccc|c} a_{11} & \cdots & a_{1n} & a_1^* \\ \vdots & & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & a_m^* \end{array}\right),$$

sie besteht aus der $m \times n$ –Matrix A und dem Spaltenvektor $a^* \in \mathbb{K}^m$.
Dann gelten die folgenden Aussagen:

(i) Spaltenrang $A \ \leq\ $ Spaltenrang $A|a^*$

(ii) Zeilenrang $A \ \leq\ $ Zeilenrang $A|a^*$

Ist der Spaltenvektor a^* eine Linearkombination der Spaltenvektoren von A, so gelten die folgenden Aussagen:

(iii) Spaltenrang $A \ =\ $ Spaltenrang $A|a^*$

(iv) Zeilenrang $A \ =\ $ Zeilenrang $A|a^*$

Die entsprechend dualen Aussagen gelten genauso für das Weglassen bzw. Hinzufügen einer Zeile bei einer Matrix

$$\underset{a^*}{A} = \left(\begin{array}{ccc} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \\ \hline a_1^* & \cdots & a_n^* \end{array}\right).$$

Beweis Die Aussagen (i) und (iii) sind trivial. Die letzte Aussage wird, wie gesagt, dual zu den anderen bewiesen.
Zu (ii): Es sei $r \leq m$ der Zeilenrang von A. Wir können **O**hne **B**eschränkung **d**er **A**llgemeinheit (O.B.d.A) annehmen, dass gerade die oberen r Zeilen

$$(a_{j1}, \ldots, a_{jn}), \qquad j = 1, \ldots, r$$

von A linear unabhängig sind. Anderenfalls führen wir Zeilenvertauschungen durch, die ja den Zeilenrang nicht verändern.
Es sei nun

$$(0, \ldots, 0) = \sum_{j=1}^{r} \beta_j (a_{j1}, \ldots, a_{jn}, a_j^*) \qquad \in \mathbb{K}^{1\times(n+1)}$$

eine Linearkombination der ersten Zeilen von $A|a^*$, die die ,,Nullzeile" ergibt. Durch Weglassen der letzten Koordinate in der Linearkombination folgt

$$(0, \ldots, 0) = \sum_{j=1}^{r} \beta_j (a_{j1}, \ldots, a_{jn}) \qquad \in \mathbb{K}^{1\times n}.$$

Da aber diese Zeilenvektoren linear unabhängig sind, folgt

$$\beta_j = 0 \qquad j = 1, \ldots, r.$$

Das bedeutet, dass auch die ersten r Zeilenvektoren von $A|a^*$ linear unabhängig sind.

Zu (iv): Es sei jetzt $r \leq m$ der Zeilenrang von $A|a^*$. Wir können wieder O.B.d.A. annehmen, dass gerade die oberen r Zeilen

$$(a_{j1}, \ldots, a_{jn}, a_j^*), \qquad j = 1, \ldots, r$$

von $A|a^*$ linear unabhängig sind. Es sei nun

$$(0, \ldots, 0) = \sum_{j=1}^{r} \beta_j (a_{j1}, \ldots, a_{jn}) \qquad \in \mathbb{K}^{1 \times n} \qquad (*)$$

eine Linearkombination der oberen r Zeilen von A, die die „Nullzeile" ergibt. Da a^* eine Linearkombination der Spaltenvektoren von A ist, können wir schreiben:

$$a^* = \begin{pmatrix} a_1^* \\ \vdots \\ a_m^* \end{pmatrix} = \sum_{k=1}^{n} \gamma_k \begin{pmatrix} a_{1k} \\ \vdots \\ a_{mk} \end{pmatrix}.$$

Daraus folgt, dass

$$\begin{aligned}
&\sum_{j=1}^{r} \beta_j a_j^* = \sum_{j=1}^{r} \beta_j \cdot \big(\sum_{k=1}^{n} \gamma_k a_{jk}\big) = \\
&\sum_{j=1}^{r} \sum_{k=1}^{n} \beta_j \gamma_k \cdot a_{jk} = \sum_{k=1}^{n} \sum_{j=1}^{r} \gamma_k \beta_j \cdot a_{jk} = \qquad \text{(Doppelsumme mit } r \cdot n \text{ Summanden)} \\
&\sum_{k=1}^{n} \gamma_k \cdot \big(\sum_{j=1}^{r} \beta_j \cdot a_{jk}\big) = \sum_{k=1}^{n} \gamma_k \cdot 0 = 0.
\end{aligned}$$

Das bedeutet aber, dass die Gleichung $(*)$ zu

$$(0, \ldots, 0) = \sum_{j=1}^{r} \beta_j (a_{j1}, \ldots, a_{jn}, a_j^*) \qquad \in \mathbb{K}^{1 \times (n+1)}$$

erweitert werden kann. Wegen der linearen Unabhängigkeit der Zeilenvektoren auf der rechten Seite dieser Gleichung folgt

$$\beta_j = 0, \quad \text{für} \quad j = 1, \ldots, r,$$

also sind auch die oberen r Zeilenvektoren von A linear unabhängig. ♦

Satz 24 (LA 10) *Für eine beliebige $m \times n$–Matrix A gilt:*

$$\textit{Zeilenrang } A \;=\; \textit{Spaltenrang } A.$$

Beweis (1) Wir lassen nacheinander in der $m \times n$–Matrix A Spaltenvektoren weg, die Linearkombinationen der anderen Spalten sind. Anschließend lassen wir nacheinander Zeilenvektoren weg, die Linearkombinationen der anderen Zeilen sind. Es entsteht eine $p \times q$–Matrix A', deren Spalten– bzw. Zeilenrang mit dem von A aufgrund von (iii),(iv) Satz 23 übereinstimmt.

(2) A' enthält nur noch linear unabhängige Spalten und linear unabhängige Zeilen.

Im Fall $q > p$ hätte man $q > p$ linear unabhängige Vektoren im Raum $\mathbb{K}^{p\times 1}$ der Spaltenvektoren. Widerspruch.

Im Fall $p > q$ hätte man $p > q$ linear unabhängige Vektoren im Raum $\mathbb{K}^{1\times q}$ der Zeilenvektoren. Widerspruch.

Es muss also $p = q$ sein.

(3) Zusammengefasst gilt nun

$$\text{Spaltenrang } A \;=\; \text{Spaltenrang } A' \;=\; q \;=\; p = \text{Zeilenrang } A' \;=\; \text{Zeilenrang } A.$$

♦

Definitionen:

- Wegen der gerade festgestellten Übereinstimmung von Spaltenrang und Zeilenrang wird diese Zahl einfach als *Rang* der Matrix A bzw. als Rang der zugehörigen linearen Abbildung bezeichnet.

- Hat eine $m \times n$–Matrix den größtmöglichen Rang, d.h.

  $$\operatorname{Rang} A = \min\{m, n\},$$

  so sagt man, sie hat *Vollrang*.

Beachte, dass aufgrund der Definition des Spaltenrangs gilt:

$$\operatorname{Rang} A = \dim(\operatorname{im} A).$$

(Dabei fassen wir die Matrix A als lineare Abbildung $\mathbb{K}^{m\times n}$ auf).

Analog zu den elementaren Äquivalenz–Zeilenumformungen (vgl. S. 70) gibt es auch die elementaren *Äquivalenz–Spaltenumformungen*. Ihre Definition ist dual zu der der Äquivalenz–Zeilenumformungen. Den Spaltenumformungen entsprechen die Multiplikationen mit den Matrizen P_{jk}, $Q_{j,\alpha}$ bzw. R_{jk} von rechts.

Satz 25 (LA 11) *Bei Äquivalenz–Zeilenumformungen oder Äquivalenz–Spaltenumformungen ändert sich der Rang einer Matrix nicht.*

Beweis Bei Äquivalenz–Zeilenumformungen ändert sich der Zeilenrang nicht, bei Äquivalenz–Spaltenumformungen ändert sich der Spaltenrang nicht. ♦

4.6 Lineare Gleichungssysteme II

Bevor wir jetzt den vollen Gauß–Algorithmus studieren, müssen wir noch angeben, welche Auswirkung eine Spaltenvertauschung in der Matrix $A \in \mathbb{K}^{m\times n}$ eines LGSs hat: Sie ist gleichbedeutend mit einer Zeilenvertauschung bei dem gesuchten Vektor $x \in \mathbb{K}^n$, für die einzelnen Variablen x_j heißt das, dass sie ,,umnummeriert" werden.

$$A\,x = b$$

$$\Updownarrow$$

$$\begin{pmatrix} a_{11} & \cdots & a_{1k} & \cdots & a_{1\ell} & \cdots & a_{1n} \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{m1} & \cdots & a_{mk} & \cdots & a_{m\ell} & \cdots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_k \\ \vdots \\ x_\ell \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

$$\Updownarrow$$

$$\begin{array}{l} a_{11}x_1 + \cdots + a_{1k}x_k + \cdots + a_{1\ell}x_\ell + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + \cdots + a_{2k}x_k + \cdots + a_{2\ell}x_\ell + \cdots + a_{2n}x_n = b_2 \\ \qquad\qquad\vdots \\ a_{m1}x_1 + \cdots + a_{mk}x_k + \cdots + a_{m\ell}x_\ell + \cdots + a_{mn}x_n = b_m \end{array}$$

$$\Updownarrow$$

$$\begin{array}{l} a_{11}x_1 + \cdots + a_{1\ell}x_\ell + \cdots + a_{1k}x_k + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + \cdots + a_{2\ell}x_\ell + \cdots + a_{2k}x_k + \cdots + a_{2n}x_n = b_2 \\ \qquad\qquad\vdots \\ a_{m1}x_1 + \cdots + a_{m\ell}x_\ell + \cdots + a_{mk}x_k + \cdots + a_{mn}x_n = b_m \end{array}$$

$$\Updownarrow$$

$$\begin{pmatrix} a_{11} & \cdots & a_{1\ell} & \cdots & a_{1k} & \cdots & a_{1n} \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{m1} & \cdots & a_{m\ell} & \cdots & a_{mk} & \cdots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_\ell \\ \vdots \\ x_k \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

$$\Updownarrow$$

$$A'\,x' = b$$

Viel eleganter lässt sich diese Umformung mit Hilfe der Matrixmultiplikation nachvollziehen. Das Quadrat einer $n \times n$–Vertauschungsmatrix $P_{k\ell}$ ist gleich der $n \times n$–Einheitsmatrix:

$$P_{k\ell}^2 = P_{k\ell} \cdot P_{k\ell} = I_n.$$

Also können wir äquivalent umformen

$$A\,x = b \quad \Longleftrightarrow \quad A \cdot I \cdot x = b \quad \Longleftrightarrow \quad \underbrace{A \cdot P_{k\ell}}_{A'} \cdot \underbrace{P_{k\ell} \cdot x}_{x'} = b.$$

Satz 26 (LA 12: Gauß–Algorithmus II)
Wir betrachten das LGS $Ax = b$ bzw. die damit verknüpfte $n \times m$–Matrix

$$A|b = \left(\begin{array}{ccc|c} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{array}\right).$$

Es ist nicht notwendig quadratisch, die Spaltenvektoren sind nicht notwendig linear unabhängig.

Das LGS lässt sich durch elementare Äquivalenz–Zeilenumformungen und Spaltenvertauschungen in die Gestalt

$$(A|b)^\diamond = \left(\begin{array}{ccccc|ccc|c} a_{11}^\diamond & 0 & \cdots & \cdots & 0 & a_{1,r+1}^\diamond & \cdots & a_{1n}^\diamond & b_1^\diamond \\ 0 & a_{22}^\diamond & \ddots & & \vdots & \vdots & & \vdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots & & \vdots & \vdots \\ \vdots & & \ddots & \ddots & 0 & \vdots & & \vdots & \vdots \\ 0 & \cdots & \cdots & 0 & a_{rr}^\diamond & a_{r,r+1}^\diamond & \cdots & a_{rn}^\diamond & b_r^\diamond \\ \hline 0 & \cdots & \cdots & \cdots & 0 & 0 & \cdots & 0 & b_{r+1}^\diamond \\ \vdots & & & & \vdots & \vdots & & \vdots & \vdots \\ 0 & \cdots & \cdots & \cdots & 0 & 0 & \cdots & 0 & b_m^\diamond \end{array}\right)$$

mit $a_{jj}^\diamond \neq 0$, $j = 1, \ldots, r$, überführen. Dabei ist r der Rang von A.
Zur Darstellung: Im Fall $r = n$ fehlt einfach der Mittelteil dieser Matrix. Im Fall $r = m$ fehlt der untere Teil der Matrix.

Bemerkung: Für eine quadratische Matrix mit Vollrang ($r = m = n$) reduziert sich die obige Darstellung auf die von Satz LA 8.

Beweis In Abänderung des Beweises von Satz LA 8. Es wird wieder die Aussage $\mathcal{A}(k)$ per Induktion über k bewiesen. Diese Induktion „stoppt" aber bei $k = r = \operatorname{Rang} A$ mit dem obigen Ergebnis.
Der Schritt (c) im Induktionsschritt $k \mapsto k+1$ für $k = 0, 1 \ldots, r-1$ muss dabei neu formuliert werden.
Wegen $k < r$ gibt es einen Vektor

$$\begin{pmatrix} a_{k+1,\ell}^{(k)} \\ \vdots \\ a_{m\ell}^{(k)} \end{pmatrix} \neq \vec{0}$$

mit $\ell \in \{k+1, \ldots, n\}$ in der Matrix $(A|b)^{(k)}$. Anderenfalls könnte der Rang der Matrix A nicht gleich r sein.

Es werden (eventuell) die Spalten ℓ und $k+1$ der Matrix A vertauscht. Beachte, dass dies eine Vertauschung der unbekannten Variablen x_{k+1} und x_ℓ entspricht. Dann kann der Induktionsschritt genau wie im Beweis von Satz LA 8 vollendet werden. ♦

Multipliziert man die oberen r Zeilen jeweils mit $\frac{1}{a_{jj}^\diamond}$, $j = 1, \ldots, r$, so wird die Matrix bzw. das LGS noch weiter vereinfacht.

Folgerung 27 (Zusatz zu LA 12) *Das LGS $Ax = b$ bzw. die damit verknüpfte Matrix*

$$A|b = \left(\begin{array}{ccc|c} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{array}\right)$$

lässt sich durch elementare Äquivalenz–Zeilenumformungen und Spaltenvertauschungen in die Gestalt

$$(A|b)^* = \left(\begin{array}{ccccc|ccc|c} 1 & 0 & \cdots & \cdots & 0 & a^*_{1,r+1} & \cdots & a^*_{1n} & b^*_1 \\ 0 & 1 & \ddots & & \vdots & \vdots & & \vdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots & & \vdots & \vdots \\ \vdots & & \ddots & \ddots & 0 & \vdots & & \vdots & \vdots \\ 0 & \cdots & \cdots & 0 & 1 & a^*_{r,r+1} & \cdots & a^*_{rn} & b^*_r \\ \hline 0 & \cdots & \cdots & \cdots & 0 & 0 & \cdots & 0 & b^*_{r+1} \\ \vdots & & & & \vdots & \vdots & & \vdots & \vdots \\ 0 & \cdots & \cdots & \cdots & 0 & 0 & \cdots & 0 & b^*_m \end{array}\right)$$

mit einer $r \times r$–Einheitsmatrix links oben überführen. Dabei ist r der Rang von A.

Satz 28 (LA 13: Lösung des LGS) *Betrachte das zu der Matrix aus Satz LA 13 gehörende LGS.*

(i) Ist der Vektor

$$\begin{pmatrix} b^*_{r+1} \\ \vdots \\ b^*_m \end{pmatrix} \neq 0, \qquad (*)$$

so besitzt das LGS keine Lösung.

(ii) Ist der Vektor $(*)$ gleich dem Nullvektor, so ist für jedes $(n-r)$–Tupel

$(\lambda_1, \lambda_2, \ldots, \lambda_{n-r}) \in \mathbb{K}^{1\times(n-r)}$ *der Vektor*

$$x(\lambda_1, \lambda_2, \ldots, \lambda_{n-r}) = \begin{pmatrix} b_1^* - a_{1,r+1}^*\lambda_1 - a_{1,r+2}^*\lambda_2 - & \cdots & - a_{1n}^*\lambda_{n-r} \\ b_2^* - a_{2,r+1}^*\lambda_1 - a_{2,r+2}^*\lambda_2 - & \cdots & - a_{2n}^*\lambda_{n-r} \\ & \vdots & \\ b_r^* - a_{r,r+1}^*\lambda_1 - a_{r,r+2}^*\lambda_2 - & \cdots & - a_{rn}^*\lambda_{n-r} \\ & \lambda_1 & \\ & \vdots & \\ & \lambda_{n-r} & \end{pmatrix} =$$

$$\begin{pmatrix} b_1^* \\ b_2^* \\ \vdots \\ b_r^* \\ 0 \\ \vdots \\ \vdots \\ \vdots \\ 0 \end{pmatrix} + \lambda_1 \begin{pmatrix} -a_{1,r+1}^* \\ -a_{2,r+1}^* \\ \vdots \\ -a_{r,r+1}^* \\ 1 \\ 0 \\ \vdots \\ \vdots \\ 0 \end{pmatrix} + \lambda_2 \begin{pmatrix} -a_{1,r+2}^* \\ -a_{2,r+2}^* \\ \vdots \\ -a_{r,r+2}^* \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \ldots + \lambda_{n-r} \begin{pmatrix} -a_{1n}^* \\ -a_{2n}^* \\ \vdots \\ -a_{rn}^* \\ 0 \\ \vdots \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

eine Lösung des zugehörigen LGSs.

Beweis Die Tatsache, dass $x(\lambda_1, \ldots, \lambda_{n-r})$ eine Lösung ist, lässt sich unmittelbar aus dem LGS ablesen.

Ist umgekehrt y irgendeine Lösung des LGS, so setze man

$$\lambda_1 := y_{r+1}, \quad \lambda_2 := y_{r+2}, \quad \ldots \lambda_{n-r} := y_n.$$

Es folgt für $j = 1, \ldots, r$ aus $A^* y = b^*$, dass

$$\begin{aligned} & y_j + a_{j,r+1}^*\lambda_1 + \cdots + a_{jn}^*\lambda_{n-r} \\ & y_j + a_{j,r+1}^* y_{r+1} + \cdots + a_{jn}^* y_n = b_j = \\ & x_j(\lambda_1, \ldots, \lambda_{n-r}) + a_{j,r+1}^*\lambda_1 + \cdots + a_{jn}^*\lambda_{n-r}, \end{aligned}$$

also $y_j = x_j(\lambda_1, \ldots, \lambda_{n-r})$. Insgesamt bedeutet das, dass $y = x(\lambda_1, \ldots, \lambda_{n-r})$. ♦

Folgerung 29 (LA 14) *(i) Für eine beliebige Matrix $A \in \mathbb{K}^{m \times n}$ (bzw. die dazu gehörige lineare Abbildung) gilt*

$$\dim \ker A + \operatorname{Rang} A = n.$$

Beachte, dass $\ker A$ *der Lösungsraum des homogenen Gleichungssystems $Ax = \vec{0}$ ist.*

(ii) Das inhomogene LGS

$$Ax = b$$

besitzt eine Lösung X genau dann, wenn

$$\operatorname{Rang}(A|b) \ = \ \operatorname{Rang} A.$$

Ist dies der Fall, so ist der Lösungsraum gegeben durch den affinen Raum

$$X + \ker A$$

der Dimension $n - \operatorname{Rang} A$.

Beweis
(i) Man betrachte den obigen Satz für $b = \vec{0}$. Man kann ablesen, dass die Dimension des Kerns gleich $n - r$ ist.

(ii) Die Rang–Bedingung ist gleichbedeutend damit, dass b als Linearkombination von Spaltenvektoren geschrieben werden kann. Die Koeffizienten einer solchen Linearkombination bilden einen Lösungsvektor X. Die Aussage über den Lösungsraum folgt aus Satz 20(ii) und (i) dieser Folgerung. ♦

Beispiel 1: Wir betrachten das LGS

$$\begin{array}{rcrcrcr} 2x_1 & + & 3x_2 & - & 2x_3 & = & -3 \\ 5x_1 & - & x_2 & + & 3x_3 & = & K \\ x_1 & + & x_2 & + & x_3 & = & 5 \\ -3x_1 & + & 4x_2 & - & 4x_3 & = & 2 \end{array}$$

in dem ein Parameter $K \in \mathbb{R}$ auftritt. Es soll in Abhängigkeit von K die Lösungsmenge $\mathcal{L}(A|b)_K$ bestimmt werden.
Die Äquivalenz–Zeilenumformungen laufen nun beispielsweise wie folgt ab. Es ist günstig zunächst die Zeilen so zu ordnen, dass Einsen weiter oben auftauchen und der Parameter ganz unten.

$$\begin{array}{rrr|r||r} 2 & 3 & -2 & -3 & \\ 5 & -1 & 3 & K & \\ 1 & 1 & 1 & 5 & \\ -3 & 4 & -4 & 2 & \\ \hline 1 & 1 & 1 & 5 & \\ 2 & 3 & -2 & -3 & -2\ \mathrm{I} \\ -3 & 4 & -4 & 2 & +3\ \mathrm{I} \\ 5 & -1 & 3 & K & -5\ \mathrm{I} \\ \hline 1 & 1 & 1 & 5 & -1\ \mathrm{II} \\ 0 & 1 & -4 & -13 & \\ 0 & 7 & -1 & 17 & -7\ \mathrm{II} \\ 0 & -6 & -2 & K-25 & +6\ \mathrm{II} \\ \hline 1 & 0 & 5 & 18 & \\ 0 & 1 & -4 & -13 & \\ 0 & 0 & 27 & 108 & :27 \\ 0 & 0 & -26 & K-103 & \\ \hline 1 & 0 & 5 & 18 & -5\ \mathrm{III} \\ 0 & 1 & -4 & -13 & +4\ \mathrm{III} \\ 0 & 0 & 1 & 4 & \\ 0 & 0 & -26 & K-103 & +26\ \mathrm{III} \\ \hline 1 & 0 & 0 & -2 & \\ 0 & 1 & 0 & 3 & \\ 0 & 0 & 1 & 4 & \\ 0 & 0 & 0 & K+1 & \\ \hline \end{array}$$

für $K \neq -1$ ist die Lösungsmenge leer. Für $K = -1$ ergibt sich die Lösung

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} -2 \\ 3 \\ 4 \end{pmatrix}.$$

Beispiel 2: Wir betrachten das LGS

$$\begin{array}{rcrcrcrcr} 6x_1 & + & 4x_2 & - & 4x_3 & + & 2x_4 & = & 12 \\ -x_1 & + & 2x_2 & - & 2x_3 & + & 3x_4 & = & -5 \\ 3x_1 & - & x_2 & - & x_3 & - & x_4 & = & 0 \end{array}$$

Die Äquivalenz–Zeilenumformungen laufen nun beispielsweise wie folgt ab.

$$\begin{array}{rrrr|r||r}
6 & 4 & -4 & 2 & 12 & :2 \to \ \mathrm{II} \\
-1 & 2 & -2 & 3 & -5 & \cdot(-1) \to \ \mathrm{I} \\
3 & -1 & -1 & -1 & 0 & \\
\hline
1 & -2 & 2 & -3 & 5 & \\
3 & 2 & -2 & 1 & 6 & -3\ \mathrm{I} \\
3 & -1 & -1 & -1 & 0 & -3\ \mathrm{I} \\
\hline
1 & -2 & 2 & -3 & 5 & \\
0 & 8 & -8 & 10 & -9 & :8 \\
0 & 5 & -7 & 8 & -15 & \\
\hline
1 & -2 & 2 & -3 & 5 & +2\ \mathrm{II} \\
0 & 1 & -1 & \frac{5}{4} & -\frac{9}{8} & \\
0 & 5 & -7 & 8 & -15 & -5\ \mathrm{II} \\
\hline
1 & 0 & 0 & -\frac{1}{2} & \frac{11}{4} & \\
0 & 1 & -1 & \frac{5}{4} & -\frac{9}{8} & \\
0 & 0 & -2 & \frac{7}{4} & -\frac{75}{8} & :(-2) \\
\hline
1 & 0 & 0 & -\frac{1}{2} & \frac{11}{4} & \\
0 & 1 & -1 & \frac{5}{4} & -\frac{9}{8} & +\ \mathrm{III} \\
0 & 0 & 1 & -\frac{7}{8} & \frac{75}{16} & \\
\hline
1 & 0 & 0 & -\frac{1}{2} & \frac{11}{4} & \\
0 & 1 & 0 & \frac{3}{8} & \frac{57}{16} & \\
0 & 0 & 1 & -\frac{7}{8} & \frac{75}{16} & \\
\hline
\end{array}$$

Damit ergibt sich als allgemeine Lösung

$$x(\lambda) = \begin{pmatrix} \frac{11}{4} \\ \frac{57}{16} \\ \frac{75}{16} \\ 0 \end{pmatrix} + \lambda \begin{pmatrix} \frac{1}{2} \\ -\frac{3}{8} \\ \frac{7}{8} \\ 1 \end{pmatrix}.$$

5 Permutationen

5.1 Einführung

Definitionen:

1. Es sei X eine Menge. Eine bijektive Abbildung $f : X \to X$ heißt auch *Permutation von* X.

2. Die Menge aller Permutationen einer Menge X bezeichnen wir mit

$$\mathcal{S}(X) \ := \ \{f : X \to X | f \text{ ist bijektiv } \}.$$

Beobachtung: Die Menge $\mathcal{S}(X)$ bildet mit der Hintereinanderausführung als Verknüpfung

$$\circ \begin{cases} \mathcal{S}(X) \times \mathcal{S}(X) & \to & \mathcal{S}(X) \\ (f, g) & \mapsto & f \circ g \end{cases}$$

eine Gruppe.

Begründung: Die Hintereinanderausführung von Funktionen ist immer assoziativ: Für drei Abbildungen $f, g, h : X \to X$ gilt:

$$[(h \circ g) \circ f](x) = (h \circ g)(f(x)) = (h(g(f(x))) = h((g \circ f)(x)) = [h \circ (g \circ f)](x).$$

Das neutrale Element ist durch die identische Abbildung id_X gegeben. Die zu einer Abbildung $f \in \mathcal{S}(X)$ inverse Abbildung ist gegeben durch die Umkehrabbildung f^{-1}.

Beispiel: Wir betrachten auf der Menge $\mathbb{R}$ die beiden Abbildungen $f, g \in \mathcal{S}(\mathbb{R})$

$$f(x) = 2x, \qquad g(x) = x + 1.$$

Dann gilt:

$$(f \circ g)(x) = f(x + 1) = 2(x + 1), \qquad (g \circ f)(x) = g(2x) = 2x + 1).$$

Es ist also $f \circ g \neq g \circ f$. Die Gruppe $\mathcal{S}(\mathbb{R})$ ist nicht kommutativ.

Definition: Ist X eine endliche Menge der Mächtigkeit n, so heißt $\mathcal{S}(X)$ die *Symmetrische Gruppe auf n Elementen (oder n Buchstaben).*
Im allgemeinen hat man es mit der Menge $X = \{1, 2, \ldots, n\}$ zu tun.
Man kürzt $\mathcal{S}_n = \mathcal{S}(\{1, 2, \ldots, n\})$ ab. Die Elemente werden im allgemeinen durch den Buchstaben π gekennzeichnet. Die Hintereinanderausführung zweier Permutationen schreiben wir ab jetzt als Multiplikation:

$$\pi_1 \cdot \pi_2 = \pi_1 \circ \pi_2.$$

Wie sonst auch üblich, kann das Multiplikationszeichen $\cdot$ auch weggelassen werden.

Beispiele:

- $\mathcal{S}_1$ besteht nur aus der identischen Abbildung $\mathrm{id} : \{1\} \to \{1\}$. Als Gruppe ist dies wieder die triviale Gruppe. $\mathcal{S}_1 = \{\mathrm{id}\}$.

- $\mathcal{S}_2$ enthält zwei Abbildungen, nämlich die identische Abbildung $\iota = \mathrm{id}_X$ und die Vertauschung der beiden Elemente 1 und 2. Bezeichnen wir letztere mit τ, so gilt für die Verknüpfungen:

$\cdot$	ι	τ
ι	ι	τ
τ	τ	ι

  Diese Struktur ist wieder die gleiche wie die von $\mathbb{Z}_2 = \{g, u\}$. Man sagt, die Gruppen $(\mathbb{Z}_2, \oplus)$ und $(\mathcal{S}_2, \circ)$ sind *isomorph (gleichstrukturiert)*. Auch die Gruppe $(\{-1, +1\}, \cdot)$ ist isomorph zu diesen beiden Gruppen.

- Wir betrachten jetzt die Gruppe $\mathcal{S}_3$ der bijektiven Abbildungen in $\{1, 2, 3\}$. Wir bezeichnen für $a, b, c \in \{1, 2, 3\}$ die Abbildung

$$\pi : \begin{cases} 1 \mapsto a \\ 2 \mapsto b \\ 3 \mapsto c \end{cases} \qquad \text{mit} \qquad \begin{pmatrix} 1 & 2 & 3 \\ a & b & c \end{pmatrix}.$$

  Dann gilt:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

  Die Gruppe $\mathcal{S}_3$ ist nicht kommutativ.

  Allgemein ist $\mathcal{S}(X)$ nicht kommutativ, falls $|X| \geq 3$.

- Allgemeiner bezeichnen wir ein Element $f \in \mathcal{S}_n$

$$\pi : \begin{cases} 1 & \mapsto & x_1 \\ 2 & \mapsto & x_2 \\ & \vdots & \\ n & \mapsto & x_n \end{cases} \qquad \text{mit} \qquad \begin{pmatrix} 1 & 2 & \cdots & n \\ x_1 & x_2 & \cdots & x_n \end{pmatrix}.$$

- Es gilt $|\mathcal{S}_n| = n!$ (Induktions–Beweis in der Übung)

5.2 Zyklen und Transpositionen

Definitionen:

1. Eine Permutation $\pi \in \mathcal{S}_n$ heißt *Zyklus (der Länge k*, wenn die Menge $\{1, 2, \ldots, n\}$ in zwei disjunkte Teilmengen zerfällt

$$\{1, 2, \ldots, n\} = \{m_1, m_2, \ldots, m_k\} \,\dot{\cup}\, \{\ell_1, \ell_2, \ldots, \ell_{n-k}\},$$

so dass

$$\begin{aligned} \pi(m_i) &= m_{i+1} \quad \text{für } i = 1, \ldots, k-1, \qquad \pi(m_k) = m_1 \\ \pi(\ell_i) &= \ell_i \quad \text{für } i = 1, \ldots, n-k. \end{aligned}$$

2. Die Zahlen $m_1, m_2, \ldots, m_k$ heißen die *Elemente* des Zyklus. Zwei Zyklen heißen *disjunkt*, wenn sie keine zwei gleichen Elemente haben.

3. Ein Zyklus der Länge 2 heißt *Transposition*.

4. In diesem Zusammenhang wird die identische Permutation als Zyklus der Länge 1 aufgefasst.

Wenn die Zahl n aus dem Kontext bekannt ist, werden hier andere Schreibweise verwendet:

$$\begin{aligned} \big(1\,3\big) &:= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \quad \text{(Transposition)} \\ \big(1\,4\,5\big) = \big(4\,5\,1\big) = \big(5\,1\,4\big) &:= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 5 & 1 \end{pmatrix} \\ \big(2\,5\,3\,7\,4\big) &:= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 5 & 7 & 2 & 3 & 6 & 4 & 8 \end{pmatrix} \\ \big(1\big) &:= \text{id}. \end{aligned}$$

Beobachtung: Sind zwei Zyklen disjunkt, so ist ihr Produkt von der Reihenfolge unabhängig:

$$\big(p_1\, p_2, \ldots, p_k\big) \cdot \big(q_1\, q_2, \ldots, q_j\big) = \big(q_1\, q_2, \ldots, q_j\big) \cdot \big(p_1\, p_2, \ldots, p_k\big).$$

Bei der Multiplikation von nicht disjunkten Zyklen muss man ,,höllisch” aufpassen. Dies wollen wir aber nur für Transpositionen ausprobieren:

$$\big(2\,3\big)\big(3\,5\big) = \big(2\,3\,5\big).$$

(Teste dabei nacheinander die Wirkung dieser Abbildung auf die einzelnen Zahlen aus $\{1, 2, \ldots, n\}$ aus. Beachte, dass Permutationen Abbildungen sind und daher von rechts nach links ausgeführt werden.)

$$\big(3\,5\big)\big(2\,3\big) = \big(2\,5\,3\big).$$

5.3 Zerlegung von Permutationen

Satz 30 (P1 Zerlegung von Permutationen)

(i) Jede Permutation π, kann als Produkt von paarweise disjunkten Zyklen geschrieben werden. Die Faktoren sind eindeutig.

(ii) Jeder Zyklus der Länge k kann als Produkt von $k-1$ Transpositionen geschrieben werden.

(iii) Folgerung: Jede Permutation π, kann als Produkt von Transpositionen geschrieben werden.

Beispiele:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 8 & 2 & 7 & 1 & 6 & 4 & 3 \end{pmatrix} = \big(1\,5\big) \cdot \big(2\,8\,3\big) \cdot \big(4\,7\big).$$

Beweis Zu (i):
1. Für die gegebene Permutation π bestimme man zunächst die Menge M der Zahlen, die nicht auf sich selbst abgebildet werden.
2. Wähle eine Zahl $j \in M$ und „starte" den zugehörigen Zyklus

$$j \mapsto \pi(j) \mapsto \pi^2(j) \mapsto \ldots \mapsto \pi^k(j) = j,$$

wir haben den Zyklus

$$\big(j \quad \pi(j) \quad \pi^2(j) \quad \pi^{k-1}(j)\big)$$

der Länge k „herausgefiltert". Der Zyklus endet mit der Zahl j, ohne dass zwischenzeitlich eine der beteiligten Zahlen zweimal aufgetreten wäre. (Warum?)
3. Wähle aus M solange weitere Zahlen aus und konstruiere die zugehörigen Zyklen, bis alle Zahlen aus M erfasst sind.
Zu (ii):

$$\big(j_1\,j_2\,\ldots\,j_k\big) = \big(j_1\,j_2\big) \cdot \big(j_2\,j_3\big) \cdot \ldots \cdot \big(j_{k-2}\,j_{k-1}\big) \cdot \big(j_{k-1}\,j_k\big).$$

♦

5.4 Das Signum einer Permutation

Definition:
Für eine Permutation $\pi \in \mathcal{S}_n$ definieren wir das *Signum* (oder die *Signatur*) durch

$$\sigma(\pi) \ := \prod_{1 \le i < j \le n} \frac{\pi(j) - \pi(i)}{j - i}. \qquad (*)$$

Für jede zwei–elementige Teilmenge $\{i, j\} \subseteq \{1, \ldots, n\}$ tritt in dem Produkt ein Faktor $\frac{\pi(j)-\pi(i)}{j-i}$. Die Reihenfolge von i und j ist dabei unwesentlich, da eine Vertauschung eine Erweiterung mit -1 in dem Bruch bedeutet.
Beispiele:

- Für $\pi = \big(1\,2\,3\big)$ ergibt sich

$$\sigma(\pi) = \frac{\pi(2)-\pi(1)}{2-1} \cdot \frac{\pi(3)-\pi(1)}{3-1} \cdot \frac{\pi(3)-\pi(2)}{3-2} = \frac{3-2}{2-1} \cdot \frac{1-2}{3-1} \cdot \frac{1-3}{3-2} = 1.$$

- Für $\pi = \big(1\,4\big) \in \mathcal{S}_4$ gilt

$$\sigma(\pi) =$$
$$\frac{\pi(2)-\pi(1)}{2-1} \cdot \frac{\pi(3)-\pi(1)}{3-1} \cdot \frac{\pi(4)-\pi(1)}{4-1} \cdot \frac{\pi(3)-\pi(2)}{3-2} \cdot \frac{\pi(4)-\pi(2)}{4-2} \cdot \frac{\pi(4)-\pi(3)}{4-3} =$$
$$\frac{2-4}{2-1} \cdot \frac{3-4}{3-1} \cdot \frac{1-4}{4-1} \cdot \frac{3-2}{3-2} \cdot \frac{1-2}{4-2} \cdot \frac{1-3}{4-3} =$$
$$\frac{-2}{1} \cdot \frac{-1}{2} \cdot \frac{-3}{3} \cdot \frac{1}{1} \cdot \frac{-1}{2} \cdot \frac{-2}{1} = -1$$

Satz 31 (P2 Eigenschaften des Signums)

(i) Es gilt für eine beliebige Permutation π:

$$\sigma(\pi) \in \{-1, +1\}.$$

(ii) Für zwei Permutationen $\pi_1, \pi_2 \in \mathcal{S}_n$ gilt

$$\sigma(\pi_1 \cdot \pi_2) = \sigma(\pi_1) \cdot \sigma(\pi_2).$$

(iii) Für die identische Permutation gilt $\sigma((1)) = +1$.

(iv) Für eine Permutation π und ihre Umkehr–Permutation π^{-1} gilt

$$\sigma(\pi) = \sigma(\pi^{-1}).$$

(v) Für eine Transposition $(k\,\ell)$ gilt

$$\sigma((k\,\ell)) = -1.$$

Beweis (i) Betrachte die definierende Formel $(*)$. Da π bijektiv ist, gibt es zu jedem Paar (i, j) mit $i < j$ zwei Zahlen $k, \ell \in \{1, \dots, n\}$, so dass $\pi(k) = i$ und $\pi(\ell) = j$. Also gibt es zu jeder Nenner–Kombination $j - i$ die Zählerkombination $\pi(k) - \pi(\ell) = i - j$ oder $\pi(\ell) - \pi(k) = j - i$. Diese Zuordnung ist umkehrbar eindeutig. Also kürzen sich alle Beträge ungleich 1 heraus. Es bleibt ,,nur das Vorzeichen" übrig.
(ii) Es gilt:

$$\begin{aligned}
\sigma(\pi_1 \cdot \pi_2) &\overset{\text{def}}{=} \prod_{1 \le i < j \le n} \frac{\pi_1(\pi_2(j)) - \pi_1(\pi_2(i))}{j - i} \\
&= \underbrace{\prod_{1 \le i < j \le n} \frac{\pi_1(\pi_2(j)) - \pi_1(\pi_2(i))}{\pi_2(j) - \pi_2(i)}}_{\sigma(\pi_1)} \cdot \underbrace{\prod_{1 \le i < j \le n} \frac{\pi_2(j) - \pi_2(i)}{j - i}}_{\sigma(\pi_2)}.
\end{aligned}$$

Dass auch die erste geschweifte Unterklammer stimmt, liegt daran, dass man statt über alle Paare $\{i, j\}$ zu multiplizieren, auch über alle Paare $\{\pi_2(i), \pi_2(j)\}$ multiplizieren kann.
(iii)

$$\sigma((1)) = \sigma((1) \cdot (1)) = \sigma((1)) \cdot \sigma((1)) \quad \Longrightarrow \quad \sigma((1)) = 1.$$

(iv) Es gilt

$$\sigma(\pi) \cdot \sigma(\pi^{-1}) = \sigma(\pi \cdot \pi^{-1}) = \sigma((1)) = +1.$$

(v) Dies erfordert mehrere Schritte:
(1) Lässt eine Permutation $\pi \in \mathcal{S}_n$ die Zahl n fest, $\pi(n) = n$, so gilt

$$\begin{aligned}
\sigma(\pi) &= \prod_{1 \le i < j \le n} \frac{\pi(j) - \pi(i)}{j - i} = \prod_{1 \le i < j < n} \frac{\pi(j) - \pi(i)}{j - i} \cdot \prod_{1 \le i < j = n} \frac{\pi(j) - \pi(i)}{j - i} \\
&= \prod_{1 \le i < j < n} \frac{n - \pi(i)}{n - i} \cdot \underbrace{\prod_{1 \le i \le n-1} \frac{n - \pi(i)}{n - i}}_{=1}
\end{aligned}$$

Das zweite Produkt ist gleich 1, da in den Zählern die gleichen Faktoren auftreten wie in den Nennern. Dies zeigt also, dass man bei der Berechnung des Signums nur die Zahlen $1, \dots, n - 1$ berücksichtigen muss.
(2) Durch einen einfachen Induktionsschluss über $n, n - 1, \dots, 3$ sieht man, dass für $\pi = (1\,2)$ gilt

$$\sigma(\pi) = \prod_{1 \le i < j \le 2} \frac{\pi(j) - \pi(i)}{j - i} = \frac{1 - 2}{2 - 1} = -1.$$

(3) Für eine beliebige Transposition $(k\,\ell)$ sei jetzt $\widetilde{\pi}$ eine Permutation mit $\widetilde{\pi}(1) = k$ und $\widetilde{\pi}(2) = \ell$. Dann gilt

$$\widetilde{\pi} \cdot (1\,2) \cdot \widetilde{\pi}^{-1} = (k\,\ell).$$

(4) Mit Eigenschaft (iv) des Satzes folgt:

$$\sigma((k\,\ell)) = \sigma(\widetilde{\pi} \cdot (1\,2) \cdot \widetilde{\pi}^{-1}) = \sigma(\widetilde{\pi}) \cdot \sigma((1\,2)) \cdot \sigma(\widetilde{\pi}^{-1}) = \sigma((1\,2)) = -1.$$

♦

Folgerung 32 (und Definition) *Eine Permutation π heißt* gerade*, wenn eine der folgenden äquivalenten Bedingungen erfüllt ist:*

(i) Es ist $\sigma(\pi) = +1$.

(ii) π läßt sich als Produkt einer geraden Anzahl von Transpositionen darstellen.

(iii) π läßt sich nicht als Produkt einer ungeraden Anzahl von Transpositionen darstellen.

Beweis (i) $\Longrightarrow$ (ii). Nach Satz P1 kann π als Produkt von Transpositionen geschrieben werden:

$$\pi = \vartheta_1 \cdot \vartheta_2 \cdot \ldots \cdot \vartheta_m.$$

Dann folgt mit den Eigenschaften (iii) und (v):

$$+1 = \sigma(\pi) = \sigma(\vartheta_1) \cdot \sigma(\vartheta_2) \cdot \ldots \cdot \sigma(\vartheta_m) = (-1)^m,$$

also ist m gerade. Den anderen Implikationen liegen ähnliche Überlegungen zugrunde. ♦

Folgerung 33 *Ein Zykel, dessen Länge* $\begin{cases} \textit{gerade} \\ \textit{ungerade} \end{cases}$ *ist, ist* $\begin{cases} \textit{ungerade} \\ \textit{gerade} \end{cases}$.

Folgerung 34 *Die Menge der geraden Permutationen*

$$\mathcal{A}_n \ := \ \{\pi \in \mathcal{S}_n | \sigma(\pi) = +1\}$$

bildet eine Untergruppe von $\mathcal{S}_n$, d.h. das Produkt zweier Permutationen aus $\mathcal{A}_n$ liegt wieder in $\mathcal{A}_n$.

6 Determinanten

6.1 Definition und Beispiele

Eine lineare Abbildung $\mathbb{K}^n \to \mathbb{K}^n$ kann mit einer quadratischen $n \times n$ –Matrix A identifiziert werden.

Wir betrachten eine quadratische Matrix

$$A = (a_{jk}) = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \in \mathbb{K}^{n \times n}.$$

1. Wähle aus den n^2 Einträgen a_{jk} der Matrix eine n–Kombination aus, darunter versteht man n Einträge so, dass jede Zeile und jede Spalte genau einmal vorkommt.

   Man kann auch sagen, dass zu jedem Zeilenindex $j \in \{1, \ldots, n\}$ ein Spaltenindex k — bijektiv — ausgewählt wird. Das bedeutet aber gerade dass die Auswahl durch eine Permutation $\pi \in \mathcal{S}_n$ über $k = \pi(j)$ gegeben ist:

   $$a_{1,\pi(1)}, a_{2,\pi(2)}, \ldots, a_{n,\pi(n)}.$$

   Mit gleicher Berechtigung kann man sagen, dass zu jedem Spaltenindex k ein Zeilenindex j durch die Permutation π^{-1} ausgewählt wird:

   $$a_{\pi^{-1}(1),1}, a_{\pi^{-1}(2),2}, \ldots, a_{\pi^{-1}(n),n}.$$

2. Die Elemente der n–Kombination werden multipliziert und mit dem Vorzeichen $\sigma(\pi)$ versehen:

   $$\sigma(\pi) \cdot a_{1,\pi(1)} \cdot a_{2,\pi(2)} \cdot \ldots \cdot a_{n,\pi(n)} = \sigma(\pi^{-1}) \cdot a_{\pi^{-1}(1),1} \cdot a_{\pi^{-1}(2),2} \cdot \ldots \cdot a_{\pi^{-1}(n),n}.$$

   (Vgl. Satz P2 (iv)).

3. Dann werden alle nach diesem Verfahren herstellbaren Produkte aufaddiert. Das heißt, man muss über alle möglichen Permutationen $\pi \in \mathcal{S}_n$ addieren: Es ergibt sich die Gesamtformel

   $$\begin{aligned} \det A \quad &:= \sum_{\pi \in \mathcal{S}_n} \sigma(\pi) \cdot \prod_{j=1}^{n} a_{j,\pi(j)} && (Z) \\ &= \sum_{\pi \in \mathcal{S}_n} \sigma(\pi) \cdot \prod_{j=1}^{n} a_{\pi^{-1}(j),j} \\ &\overset{(*)}{=} \sum_{\pi \in \mathcal{S}_n} \sigma(\pi) \cdot \prod_{j=1}^{n} a_{\pi(j),j} && (S) \end{aligned}$$

   Da es einerlei ist, ob man über alle Permutationen oder über alle inversen Permutationen aus $\mathcal{S}_n$ addiert, ergibt sich die Umformung $(*)$.

Definition: Es sei A eine quadratische Matrix. Die durch die *Leibniz–Formel* (Z) bzw. (S) definierte Zahl heißt *Determinante* der Matrix A. Die zugehörige Abbildung

$$\det : \mathbb{K}^{n\times n} \to \mathbb{K}$$

heißt *Determinantenfunktion*.

Beispiele:

- Im Fall $n = 1$ ist die Matrix $A = (a)$ einfach eine Zahl. Es gilt

$$\det A = a.$$

- Es sei $n = 2$ und $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$. Dann gilt

$$\begin{aligned} \det A &= \sum_{\pi\in\mathcal{S}_2} \sigma(\pi)\cdot\prod_{j=1}^{n} a_{j,\pi(j)} = \underbrace{(+1)\cdot a_{11}a_{22}}_{\pi=(1)} + \underbrace{(-1)\cdot a_{12}a_{21}}_{\pi=(1\,2)} \\ &= a_{11}\cdot a_{22} - a_{12}\cdot a_{21}. \end{aligned}$$

- $n = 3$ und $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$. Die Gruppe $\mathcal{S}_3$ enthält sechs Permutationen, nämlich

$$\mathcal{S}_3 = \{(1), (1\,2\,3), (1\,3\,2), (1\,2)(1\,3), (2\,3)\}.$$

Damit ergibt sich

$$\begin{aligned} \det(A) &= +\,a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{32}a_{21} \\ &\quad - a_{12}a_{21}a_{33} - a_{13}a_{31}a_{22} - a_{23}a_{32}a_{11}. \end{aligned}$$

Diese Formel lässt sich graphisch durch die *Regel von Sarrus* repräsentieren:

$$\begin{array}{ccccc} + & + & +\;- & - & - \end{array}$$
$$\left(\begin{array}{ccc|cc} a_{11} & a_{12} & a_{13} & a_{11} & a_{12} \\ a_{21} & a_{22} & a_{23} & a_{21} & a_{22} \\ a_{31} & a_{32} & a_{33} & a_{31} & a_{32} \end{array}\right)$$

6.2 Eigenschaften

Satz 35 (D1 Eigenschaften) *Die Determinantenfunktion hat folgende Eigenschaften:*

(i) det *ist linear in jeder* ***einzelnen*** *Zeile. Bezeichnen wir eine j–te Zeile mit $\mathbf{a}_j = (a_{j1}, \ldots, a_{jn})$, so gilt für jedes $\ell \in \{1, \ldots, n\}$ und $\alpha \in \mathbb{K}$:*

$$\det \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_{\ell-1} \\ \mathbf{a}_\ell + \mathbf{a}'_\ell \\ \mathbf{a}_{\ell+1} \\ \vdots \\ \mathbf{a}_n \end{pmatrix} = \det \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_{\ell-1} \\ \mathbf{a}_\ell \\ \mathbf{a}_{\ell+1} \\ \vdots \\ \mathbf{a}_n \end{pmatrix} + \det \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_{\ell-1} \\ \mathbf{a}'_\ell \\ \mathbf{a}_{\ell+1} \\ \vdots \\ \mathbf{a}_n \end{pmatrix}$$

$$\det \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_{\ell-1} \\ \alpha \cdot \mathbf{a}_\ell \\ \mathbf{a}_{\ell+1} \\ \vdots \\ \mathbf{a}_n \end{pmatrix} = \alpha \cdot \det \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_{\ell-1} \\ \mathbf{a}_\ell \\ \mathbf{a}_{\ell+1} \\ \vdots \\ \mathbf{a}_n \end{pmatrix}$$

(ii) Die Determinantenfunktion det *ist alternierend in den Zeilen, d.h. sie wechselt bei der Vertauschung zweier Zeilen das Vorzeichen:*

$$\det \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_m \\ \vdots \\ \mathbf{a}_\ell \\ \vdots \\ \mathbf{a}_n \end{pmatrix} = -\det \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_\ell \\ \vdots \\ \mathbf{a}_m \\ \vdots \\ \mathbf{a}_n \end{pmatrix}$$

(iii) det *ist normiert, das heißt die Determinante der Einheitsmatrix I ist gleich* 1

$$\det I = 1.$$

(iv) Ohne Beweis: Umgekehrt legen diese drei Eigenschaften die Determinantenfunktion eindeutig fest.

(v) Die gleichen Regeln gelten analog bzgl. der Spalten.

Beweis Eine Multiplikation über alle Indices $j \in \{1, \ldots, n\}$ außer $j = \ell$ schreiben wir mit dem Zeichen $\prod_{j \neq \ell}$.

$$\begin{aligned}
\det \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_{\ell-1} \\ \mathbf{a}_\ell + \mathbf{a}'_\ell \\ \mathbf{a}_{\ell+1} \\ \vdots \\ \mathbf{a}_n \end{pmatrix} &= \sum_{\pi \in \mathcal{S}_n} \sigma(\pi) \cdot (a_{\ell,\pi(\ell)} + a'_{\ell,\pi(\ell)}) \cdot \prod_{j \neq \ell} a_{j,\pi(j)} \\
&= \sum_{\pi \in \mathcal{S}_n} \sigma(\pi) \cdot a_{\ell,\pi(\ell)} \cdot \prod_{j \neq \ell} a_{j,\pi(j)} + \sum_{\pi \in \mathcal{S}_n} \sigma(\pi) \cdot a'_{\ell,\pi(\ell)} \cdot \prod_{j \neq \ell} a_{j,\pi(j)} \\
&= \det \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_{\ell-1} \\ \mathbf{a}_\ell \\ \mathbf{a}_{\ell+1} \\ \vdots \\ \mathbf{a}_n \end{pmatrix} + \det \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_{\ell-1} \\ \mathbf{a}'_\ell \\ \mathbf{a}_{\ell+1} \\ \vdots \\ \mathbf{a}_n \end{pmatrix}
\end{aligned}$$

$$\begin{aligned}
\det \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_{\ell-1} \\ \alpha \cdot \mathbf{a}_\ell \\ \mathbf{a}_{\ell+1} \\ \vdots \\ \mathbf{a}_n \end{pmatrix} &= \sum_{\pi \in \mathcal{S}_n} \sigma(\pi) \cdot \alpha \, a_{\ell,\pi(\ell)} \cdot \prod_{j \neq \ell} a_{j,\pi(j)} \\
&= \alpha \cdot \sum_{\pi \in \mathcal{S}_n} \sigma(\pi) \cdot a_{\ell,\pi(\ell)} \cdot \prod_{j \neq \ell} a_{j,\pi(j)} = \alpha \cdot \det \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_{\ell-1} \\ \mathbf{a}_\ell \\ \mathbf{a}_{\ell+1} \\ \vdots \\ \mathbf{a}_n \end{pmatrix}
\end{aligned}$$

(ii) Es sei $\vartheta = (k\,\ell)$ und A' die durch Vertauschung von k– und ℓ–ter Zeile aus A hervorgehende Matrix, d.h.

$$a'_{jk} = a_{\vartheta(j),k}.$$

Dann gilt

$$\begin{aligned}\det A' &= \sum_{\pi\in\mathcal{S}_n}\sigma(\pi)\cdot\prod_{j=1}^{n}a'_{j,\pi(j)} = \sum_{\pi\in\mathcal{S}_n}\sigma(\pi)\cdot\prod_{j=1}^{n}a_{\vartheta(j),\pi(j)}\\ &= \sum_{\pi\in\mathcal{S}_n}(-\sigma(\pi\circ\vartheta))\cdot\prod_{j=1}^{n}a_{j,\pi\circ\vartheta(j)} = -\sum_{\pi\in\mathcal{S}_n}\sigma(\pi)\cdot\prod_{j=1}^{n}a_{j,\pi(j)} = -\det(A).\end{aligned}$$

(iii) Es gibt nur eine n–Kombination der Einträge von I, bei der das zugehörige Produkt ungleich Null ist. Dies ist das Produkt, das zur identischen Permutation gehört:

$$a_{11}\cdot a_{22}\cdot\ldots\cdot a_{nn} = 1,$$

alle anderen Produkte enthalten mindestens einen Eintrag a_{jk} mit $j\neq k$, also $a_{jk}=0$. Das bedeutet aber:

$$\det A = \sum_{\pi\in\mathcal{S}_n}\sigma(\pi)\cdot\prod_{j=1}^{n}a_{j,\pi(j)} = \sum_{\pi=(1)}\sigma(\pi)\cdot\prod_{j=1}^{n}a_{j,\pi(j)} = 1.$$

(v) Die Beweise erfolgen genau analog zu den Beweisen von (i) und (ii). Man verwendet einfach die Leibniz–Formel (S) anstelle der Formel (Z). ♦

Folgerung 36 (D2 Weitere Eigenschaften)
Die Determinantenfunktion hat die folgenden weiteren Eigenschaften:

(i) Für jedes $\alpha\in\mathbb{K}$ gilt:

$$\det(\alpha\cdot A) = \alpha^n\cdot\det A.$$

(ii) Ist eine Zeile oder Spalte von A gleich Null, so gilt:

$$\det A = 0.$$

(iii) Hat A zwei gleiche Zeilen oder zwei gleich Spalten, so gilt:

$$\det A = 0.$$

(iv) Entsteht die Matrix A' aus der Matrix A dadurch, dass eine Zeile (Spalte) von A zu einer anderen Zeile (Spalte) von A addiert wird, so gilt:

$$\det A' = \det A.$$

(Vgl. Abschnitt 4.4, S. 63)

(v) Die Gleichung

$$\det(A+B) = \det A + \det B$$

für zwei $n\times n$–Matrizen A, B ist im allgemeinen nicht richtig.

Beweis In der Übung. ♦

6.3 Der Multiplikationssatz

Satz 37 (D3: Multiplikation von Determinanten)
Es seien A, B zwei $n \times n$–Matrizen. Dann gilt

$$\det(A \cdot B) = \det A \cdot \det B.$$

Beispiele

- Produkt zweier 2×2–Matrizen:

$$\begin{pmatrix} 2 & -3 \\ 1 & 6 \end{pmatrix} \cdot \begin{pmatrix} 0 & 3 \\ 1 & -2 \end{pmatrix} = \begin{pmatrix} -3 & 12 \\ 6 & -9 \end{pmatrix}$$

  Entsprechend gilt für die Determinanten:

$$15 \cdot (-3) = -45.$$

- Produkt zweier 3×3–Matrizen:

$$\begin{pmatrix} 1 & 3 & -2 \\ 5 & -1 & -4 \\ 2 & 0 & 5 \end{pmatrix} \cdot \begin{pmatrix} 4 & -3 & 0 \\ 0 & 1 & -5 \\ 3 & 2 & -6 \end{pmatrix} = \begin{pmatrix} -2 & -4 & -3 \\ 8 & -24 & 29 \\ 23 & 4 & -30 \end{pmatrix}$$

  Die drei Determinanten haben die Werte

$$\begin{aligned} -5 - 24 - 4 - 75 &= -108 \\ -24 + 45 + 40 &= 61 \\ -1440 - 2668 - 96 - 1656 + 232 - 960 &= -6588 \end{aligned}$$

Beweis Der Beweis dieser Beziehung für beliebige n ist mathematisch–elementar, leider aber schreibtechnisch sehr aufwendig.

Es seien also zwei $n \times n$–Matrizen A, B gegeben. Wir können jeden einzelnen Spaltenvektor b_k von B als Linearkombination der kanonischen Einheitsvektoren darstellen. Es gilt

$$b_1 = \sum_{j=1}^{n} b_{j1} e_j, \quad b_2 = \sum_{j=1}^{n} b_{j2} e_j, \quad \ldots \quad b_n = \sum_{j=1}^{n} b_{jn} e_j.$$

Da bei den Umformungen weiter unten alle diese Linearkombinationen simultan verwendet werden sollen, ist es notwendig, n verschiedene Summationsindices $j_1, \ldots, j_n$ zu verwenden, also die Linearkombinationen zu schreiben als

$$b_1 = \sum_{j_1=1}^{n} b_{j_1 1} e_{j_1}, \quad b_2 = \sum_{j_2=1}^{n} b_{j_2 2} e_{j_2}, \quad \ldots \quad b_n = \sum_{j_n=1}^{n} b_{j_n n} e_{j_n}.$$

Unter Benutzung der Spalten–Linearität und der Alternierungseigenschaft rechnen wir jetzt nach:

$$\begin{aligned}
\det(A\cdot B) &= \det(A\,b_1, A\,b_2,\ldots,A\,b_n)\\
&= \det(A\sum_{j_1=1}^{n} b_{j_1 1}e_{j_1}, A\sum_{j_2=1}^{n} b_{j_2 2}e_{j_2},\ldots, A\sum_{j_n=1}^{n} b_{j_n n}e_{j_n})\\
&= \det(\sum_{j_1=1}^{n} b_{j_1 1}A\,e_{j_1}, \sum_{j_2=1}^{n} b_{j_2 2}A\,e_{j_2},\ldots, \sum_{j_n=1}^{n} b_{j_n n}A\,e_{j_n})\\
&= \sum_{j_1=1}^{n} b_{j_1,1}\cdot\det(A\,e_{j_1}, \sum_{j_2=1}^{n} b_{j_2 2}A\,e_{j_2},\ldots, \sum_{j_n=1}^{n} b_{j_n n}A\,e_{j_n})\\
&= \quad (\text{Linearität von det in den Spalten } 2,\ldots,n)\\
&= \sum_{j_1=1}^{n} b_{j_1,1}\cdot\sum_{j_2=1}^{n} b_{j_2,2}\cdot\ldots\cdot\sum_{j_1=1}^{n} b_{j_n,n}\cdot\det(A\,e_{j_1},A\,e_{j_2},\ldots,A\,e_{j_n})\\
&= \sum_{(j_1,\ldots,j_n)\in\{1,\ldots,n\}^n} b_{j_1,1}\cdot b_{j_2,2}\cdot\ldots\cdot b_{j_n,n}\cdot\det(A\,e_{j_1},A\,e_{j_2},\ldots,A\,e_{j_n})\\
&\overset{(*)}{=} \sum_{\substack{(j_1,\ldots,j_n)\in\{1,\ldots,n\}^n\\ j_s\neq j_t \text{ für } s\neq t}} b_{j_1,1}\cdot b_{j_2,2}\cdot\ldots\cdot b_{j_n,n}\cdot\det(A\,e_{j_1},A\,e_{j_2},\ldots,A\,e_{j_n})\\
&= \sum_{\pi\in\mathcal{S}_n} b_{\pi(1),1}\cdot b_{\pi(2),2}\cdot\ldots\cdot b_{\pi(n),n}\cdot\det(A\,e_{\pi(1)},A\,e_{\pi(2)},\ldots,A\,e_{\pi(n)})\\
&= \sum_{\pi\in\mathcal{S}_n} b_{\pi(1),1}\cdot b_{\pi(2),2}\cdot\ldots\cdot b_{\pi(n),n}\cdot(-1)^{\operatorname{sgn}(\pi)}\det A\\
&= \det B\cdot\det A.
\end{aligned}$$

In der dritt–letzten Zeile bezeichnet $\pi\in\mathcal{S}_n$ die Permutation der Elemente von $\{1,\ldots,n\}$, für die $\pi(i)=j_i$ ist. In der fünft–letzten Zeile sind die Summanden, für die ein j_s mit einem j_t, $(s,t\in\{1,\ldots,n\})$ übereinstimmt, gleich Null, da die Matrix unter der Determinante dann zwei gleiche Spalten enthält. Daraus ergibt sich die Umformung $(*)$. ♦

6.4 Die Entwicklung einer Determinante

Es sei A eine $n \times n$–Matrix.

Für $m, \ell \in \{1, \ldots, n\}$ sei die Matrix $A^{(m\ell)}$ die $(n-1) \times (n-1)$–Matrix, die aus A durch Streichung der m–ten Zeile und ℓ–ten Spalte entsteht.

Satz 38 (D4: Entwicklung einer Determinante)

(i) Für eine Zeilennummer m gilt:

$$\det A = \sum_{k=1}^{n} a_{mk} \cdot (-1)^{m+k} \det A^{(mk)}.$$

(ii) Für eine Spaltennummer ℓ gilt:

$$\det A = \sum_{j=1}^{n} a_{j\ell} \cdot (-1)^{j+\ell} \det A^{(j\ell)}.$$

Beispiel: Wir entwickeln die Determinante einer 4×4–Matrix. Dabei benutzen wir eine vereinfachende Schreibweise für Determinanten:

$$\begin{aligned}
\begin{vmatrix} 0 & 2 & 3 & 0 \\ 2 & -1 & 0 & -2 \\ 4 & 0 & 0 & -3 \\ 1 & 1 & 2 & 0 \end{vmatrix} &= -2 \cdot \begin{vmatrix} 2 & 0 & -2 \\ 4 & 0 & -3 \\ 1 & 2 & 0 \end{vmatrix} + 3 \cdot \begin{vmatrix} 2 & -1 & -2 \\ 4 & 0 & -3 \\ 1 & 1 & 0 \end{vmatrix} \\
&= (-2) \cdot (-2) \begin{vmatrix} 2 & -2 \\ 4 & -3 \end{vmatrix} + 3 \cdot \left[1 \cdot 3 - 1 \begin{vmatrix} 2 & -2 \\ 4 & -3 \end{vmatrix} \right] \\
&= 9 + \begin{vmatrix} 2 & -2 \\ 4 & -3 \end{vmatrix} = 9 + 2 = 11.
\end{aligned}$$

Beweis Wir zeigen die Aussage (i) für $m = n$. Die allgemeine Aussage folgt dann mit Satz D1 (ii).

$$\begin{aligned}
\det A &= \sum_{\pi \in \mathcal{S}_n} \sigma(\pi) \cdot \prod_{j=1}^{n} a_{j,\pi(j)} = \sum_{k=1}^{n} \sum_{\pi \in \mathcal{S}_n, \pi(n)=k} \sigma(\pi) \cdot \prod_{j=1}^{n} a_{j,\pi(j)} \\
&= \sum_{k=1}^{n} \sum_{\pi \in \mathcal{S}_n, \pi(n)=k} \sigma(\pi) \cdot a_{nk} \cdot \prod_{j=1}^{n-1} a_{j,\pi(j)} \\
&= \sum_{k=1}^{n} a_{nk} \cdot \sum_{\pi \in \mathcal{S}_n, \pi(n)=k} \sigma(\pi) \cdot \prod_{j=1}^{n-1} a_{j,\pi(j)}
\end{aligned}$$

Es bleibt zu zeigen, dass

$$\sum_{\pi \in \mathcal{S}_n, \pi(n)=k} \sigma(\pi) \cdot \prod_{j=1}^{n-1} a_{j,\pi(j)} = (-1)^{n+k} \cdot \det A^{(nk)}.$$

Dazu sei ϑ die Permutation, die die Zahl k an die letzte Stelle n „verschiebt“:

$$\vartheta = (n\, n-1) \dots (k+2\, k+1)(k+1\, k), \qquad \sigma(\vartheta) = (-1)^{n-k} = (-1)^{n+k}.$$

Dann sind die Einträge von $A^{(nk)}$ gegeben durch

$$a_{j\ell}^{(nk)} = a_{j,\vartheta^{-1}(\ell)}, \qquad 1 \leq j, \ell \leq n-1.$$

Es gilt dann:

$$\begin{aligned}
&\sum_{\pi \in \mathcal{S}_n, \pi(n)=k} \sigma(\pi) \cdot \prod_{j=1}^{n-1} a_{j,\pi(j)} = \qquad \text{(Transformation } \pi = \vartheta^{-1}\widetilde{\pi} \text{)} \\
&\sum_{\widetilde{\pi} \in \mathcal{S}_n, \vartheta^{-1}\widetilde{\pi}(n)=k} \sigma(\vartheta^{-1}\widetilde{\pi}) \cdot \prod_{j=1}^{n-1} a_{j,\vartheta^{-1}\widetilde{\pi}(j)} = \\
&(-1)^{n+k} \cdot \sum_{\widetilde{\pi} \in \mathcal{S}_n, \widetilde{\pi}(n)=n} \sigma(\widetilde{\pi}) \cdot \prod_{j=1}^{n-1} a_{j,\vartheta^{-1}\widetilde{\pi}(j)} = \\
&(-1)^{n+k} \cdot \sum_{\widetilde{\pi} \in \mathcal{S}_n, \widetilde{\pi}(n)=n} \sigma(\widetilde{\pi}) \cdot \prod_{j=1}^{n-1} a_{j,\widetilde{\pi}(j)}^{(nk)} = \\
&(-1)^{n+k} \cdot \sum_{\widetilde{\pi} \in \mathcal{S}_{n-1}} \sigma(\widetilde{\pi}) \cdot \prod_{j=1}^{n-1} a_{j,\widetilde{\pi}(j)}^{(nk)} = \\
&(-1)^{n+k} \cdot \det A^{(nk)}.
\end{aligned}$$

♦

6.5 Einschub: Transposition einer Matrix

Definition: Es sei A eine $m \times n$–Matrix. Vertauscht man die Rollen von Zeilen und Spalten, so entsteht die $n \times m$–Matrix $A^T = {}^tA$ mit den Einträgen

$$(A^T)_{jk} = a_{kj}, \qquad j = 1, \ldots, n,\ k = 1, \ldots, m.$$

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & & a_{2n} \\ \vdots & & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}^T = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & & a_{m2} \\ \vdots & & \ddots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{pmatrix}$$

Sie heißt die zu A *transponierte* Matrix.

Eine quadratische Matrix A heißt *symmetrisch*, wenn $A^T = A$, sie heißt schiefsymmetrisch, wenn $A^T = -A$.

Satz 39 (Eigenschaften der Transposition)
Für das Produkt zweier Matrizen $A \in \mathbb{K}^{m \times n}$ und $B \in \mathbb{K}^{n \times \ell}$ gilt:

$$(A \cdot B)^T = B^T \cdot A^T.$$

Für eine quadratische Matrix A gilt:

$$\det A^T = \det A.$$

Beweis (i) Für die einzelnen Einträge von $A \cdot B$ gilt:

$$((A \cdot B)^T)_{jk} = (A \cdot B)_{kj} = \sum_{i=1}^{n} (A)_{ki}(B)_{ij} = \sum_{i=1}^{n} (B^T)_{ji}(A^T)_{ik} = (B^T \cdot A^T)_{jk}.$$

(ii)

$$\det A^T \overset{(Z)}{=} \sum_{\pi \in \mathcal{S}_n} \sigma(\pi) \cdot \prod_{j=1}^{n} (A^T)_{j\pi(j)} = \sum_{\pi \in \mathcal{S}_n} \sigma(\pi) \cdot \prod_{j=1}^{n} (A)_{\pi(j)j} \overset{(S)}{=} \det A.$$

♦

6.6 Invertierbare Matrizen und Determinanten

Satz 40 *Zu einer gegebenen quadratischen Matrix A sei die Matrix $A^\diamond$ definiert durch die Einträge*

$$a^\diamond_{jk} = (-1)^{j+k} \det A^{(jk)}.$$

Ausgeschrieben ergibt sich die Matrix mit einer Vorzeichen–Schachbrettverteilung:

$$A^\diamond = \begin{pmatrix} +\det A^{(11)} & -\det A^{(12)} & \cdots & \cdots & (-1)^{1+n}\det A^{(1n)} \\ -\det A^{(12)} & +\det A^{(22)} & \cdots & \cdots & (-1)^{2+n}\det A^{(2n)} \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ (-1)^{n+1}\det A^{(n1)} & (-1)^{n+2}\det A^{(n2)} & \cdots & \cdots & +\det A^{(nn)} \end{pmatrix}$$

Dann gilt für das Produkt der Matrizen A und $A^{\diamond T}$

$$A \cdot A^{\diamond T} = A^{\diamond T} \cdot A = \det A \cdot I = \begin{pmatrix} \det A & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & \det A & \ddots & & & \vdots \\ \vdots & \ddots & \det A & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots & 0 & \det A \end{pmatrix}$$

Beweis Wir rechnen einfach das Produkt aus:

$$(A \cdot A^{\diamond T})_{jk} = \sum_{i=1}^{n} (A)_{ji} (A^{\diamond T})_{ik} = \sum_{i=1}^{n} a_{ji} \cdot (-1)^{k+i} \det A^{(ki)}$$

(Entwicklung der folgenden Determinante nach der k–ten Zeile)

$$= \det \begin{pmatrix} a_{11} & \cdots & \cdots & a_{1n} \\ \vdots & & & \vdots \\ a_{k-1,1} & \cdots & \cdots & a_{k-1,n} \\ a_{j1} & \cdots & \cdots & a_{jn} \\ a_{k+1,1} & \cdots & \cdots & a_{k+1,n} \\ \vdots & & & \vdots \\ a_{n1} & \cdots & \cdots & a_{nn} \end{pmatrix} \longleftarrow k\text{–te Zeile}$$

$$= \begin{cases} \det A, & \text{falls } j = k, \\ 0, & \text{falls } j \neq k. \end{cases}$$

Die Matrix in der vorletzten Zeile entsteht aus der Matrix A dadurch, dass die k–te Zeile von A durch die j–te Zeile von A ersetzt ist. Für $j = k$ ist diese Matrix gleich der Matrix A. Für $i \neq k$ sind in dieser Matrix die Zeilen j und k identisch. Daraus folgt die letzte Gleichung.

Die andere Eigenschaft $A^{\diamond T} \cdot A = \det A \cdot I$ folgt mit einer dualen Betrachtung, d.h. einer Spaltenentwicklung. ♦

Definition Eine quadratische Matrix A heißt *invertierbar* oder *regulär*, wenn es eine Matrix B gibt, so dass $A \cdot B = I$ (Einheitsmatrix). Eine Matrix, die nicht regulär ist, heißt auch *singulär*.

Satz 41 (D5 Matrixgruppe) *Die Menge der invertierbaren $n \times n$–Matrizen über $\mathbb{K}$ bildet eine Gruppe. Sie wird mit $\mathbf{GL}(\mathbb{K}, n)$ (General linear group) bezeichnet. Für $n \geq 2$ ist die Gruppe nicht kommutativ.*

Beweis Er ist Ihnen zur Übung überlassen. ♦
Aus der Gruppentheorie ist bekannt, dass inverse Elemente einer Gruppe eindeutig bestimmt ist. Die zu einer gegebenen invertierbaren Matrix A inverse Matrix wird daher mit A^{-1} bezeichnet.

Folgerung 42 (D6 Matrixinversion) *Hat eine quadratische Matrix A eine nicht–verschwindende Determinante*

$$\det A \neq 0,$$

so ist sie invertierbar. Es gilt

$$A^{-1} = \frac{1}{\det A} \cdot A^{\diamond T}.$$

Folgerung 43 (D7 Cramer'sche Regel) *Ist die Matrix $A \in \mathbb{K}^{n\times n}$ in dem LGS*

$$Ax = b$$

invertierbar, so ist die Lösung x gegeben durch

$$x_j = \frac{1}{\det A} \cdot \det \begin{pmatrix} a_{11} & \cdots & a_{1,j-1} & b_1 & a_{1,j+1} & \cdots & a_{1n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & \cdots & a_{n,j-1} & b_n & a_{n,j+1} & \cdots & a_{nn} \end{pmatrix}, \qquad j = 1, \ldots, n.$$

Beweis Es ist

$$\frac{1}{\det A} \cdot \det \begin{pmatrix} a_{11} & \cdots & a_{1,j-1} & b_1 & a_{1,j+1} & \cdots & a_{1n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & \cdots & a_{n,j-1} & b_n & a_{n,j+1} & \cdots & a_{nn} \end{pmatrix} =$$

(Entwicklung nach der j–ten Spalte)

$$\frac{1}{\det A} \cdot \sum_{i=1}^{n} b_i \cdot (-1)^{i+j} \det A^{(ij)} =$$

$$\frac{1}{\det A} \cdot \sum_{i=1}^{n} (A^{\diamond T})_{ji}\, b_i = \frac{1}{\det A} \cdot (A^{\diamond T} b)_j = (A^{-1}\, b)_j = x_j.$$

♦

Satz 44 (D8 Charakterisierung regulärer Matrizen) *Die folgenden Aussagen über eine $n \times n$–Matrix A sind äquivalent:*

(i) Der Rang von A ist gleich n (Zeilenrang = Spaltenrang = Vollrang).

(ii) Das Gleichungssystem $A \cdot x = b$ hat für jedes $b \in \mathbb{K}^n$ genau eine Lösung $x \in \mathbb{K}^n$.

(iii) A ist invertierbar.

(iv) Es ist $\det A \neq 0$.

Beweis Die Implikation $(i) \Longrightarrow (ii)$ ist durch Satz LA 7 (Vorlesung LAL01) gegeben.
Zu $(ii) \Longrightarrow (iii)$: Existenz und Eindeutigkeit einer Lösung ermöglichen die Definition einer Abbildung

$$B \left\{ \begin{array}{rcl} \mathbb{K}^n & \to & \mathbb{K}^n \\ b & \mapsto & x. \end{array} \right.$$

Es gilt dann $A \cdot Bb = A \cdot x = b$ und $B \cdot Ax = Bb = x$, also ist die Abbildung B die Umkehrabbildung zur Abbildung A. Die Abbildung ist linear:

$$B(\alpha_1 b_1 + \alpha_2 b_2) = \alpha_1 x_1 + \alpha_2 x_2,$$

da der Linearkombination zweier rechten Seiten eines LGS die entsprechende Linearkombination der Lösungen gehört. Also kann B durch eine Matrix repräsentiert werden, die dann die Inverse zu A ist.
$(iii) \Longrightarrow (iv)$: Wenn A invertierbar ist, so gilt

$$\det A \cdot \det(A^{-1}) = \det(A \cdot A^{-1}) = \det I = 1,$$

also kann nicht $\det A = 0$ sein.
$(iv) \Longrightarrow (i)$: Wir nehmen an, dass A nicht Vollrang hat. Dann ist eine — sagen wir die k–te — Spalte eine Linearkombination der anderen Spalten. Zieht man diese Linearkombination von der k–ten Spalte ab, so entsteht eine Matrix A' mit lauter Nullen in der k–ten Spalte. Dann gilt aber mit Satz D2 (iv) und (ii)

$$\det A = \det A' = 0$$

im Widerspruch zu (iv). ♦