Lineare Algebra und Analytische Geometrie

Dr. V. Drumm

Prof. Dr. W. Weil

Institut für Algebra und Geometrie – Universität Karlsruhe(TH)

Vorwort

Die Vorlesung "Lineare Algebra und Analytische Geometrie" erstreckt sich über zwei Semester. Sie ist eine Pflichtvorlesung für alle, die Mathematik und Informatik studieren, wird aber auch den Studierenden der Physik empfohlen.

Der Stoff des ersten Teils der Vorlesung ist für alle Fachrichtungen im wesentlichen derselbe. Im zweiten Teil wird die Vorlesung auch inhaltlich getrennt, da dann der Studienplan für die Fachrichtung Informatik nur noch zwei Semesterwochenstunden vorsieht.

Das vorliegende Skriptum, das aus Vorlesungen hervorgegangen ist, die wir mehrfach in Karlsruhe gehalten haben, berücksichtigt diese Trennung. Es enthält im wesentlichen den Inhalt der Vorlesung für die Fachrichtung Mathematik und darüber hinaus noch einige Ergänzungen, jedoch können ohne Schwierigkeiten Teile davon für die verkürzte Vorlesung Mathematik für die Fachrichtung Informatik ausgewählt werden.

Das Skriptum soll allen Hörerinnen und Hörern das Mitverfolgen der Vorlesung erleichtern, ist aber kein Ersatz für die Vorlesung. Trotz seines Umfanges sind manche Beweise recht knapp gefaßt und einige Bemerkungen überhaupt nicht bewiesen. Weiterhin soll und kann das Skriptum auch kein Lehrbuch ersetzen. Wir haben deshalb am Ende eine umfangreiche Liste deutschsprachiger Lehrbücher aufgeführt.

Im Unterschied zu früheren Fassungen werden Vektoren, wie inzwischen allgemein üblich, jetzt mit kleinen lateinischen Buchstaben bezeichnet. Wir hoffen, daß dadurch die Lesbarkeit nicht erschwert wird. Im übrigen haben wir die alte Rechtschreibung beibehalten, aber auch das sollte das Verständnis nicht beeinträchtigen.

Karlsruhe, im Oktober 2007 V. Drumm, W. Weil

Inhaltsverzeichnis

Einleitung

Die lineare Algebra bildet neben der Analysis die Grundlage weiter Teile der Mathematik und damit auch der Mathematikausbildung. Sie behandelt die Theorie der Vektorräume und linearen Abbildungen sowie deren Anwendung auf lineare Gleichungssysteme und Eigenwertprobleme.

Systeme von linearen Gleichungen und Methoden zu deren Lösung waren schon den Chinesen vor über 1500 Jahren bekannt. Die Probleme bei der Auflösung linearer und nichtlinearer Gleichungen führten zur Entwicklung der Algebra (ca. $1000 - 1600$).

Die Beschreibung von Punkten durch Koordinaten und von Geraden und Ebenen durch lineare Gleichungen erwies sich als sehr nützlich für die Behandlung geometrischer Probleme. Diese "analytische Geometrie" hat zu der Einführung von Vektoren und der Entstehung der Vektorraumtheorie geführt. Bis zur Mitte des 20. Jahrhunderts dienten die Vektorräume in der Grundvorlesung hauptsächlich als formaler Rahmen, in dem geometrische Probleme behandelt wurden.

Das hat sich inzwischen grundlegend geändert. Zum einen verlangt der zunehmende Abstraktionsprozeß in der Mathematik, aber auch in Anwendungsgebieten wie Informatik, die Behandlung abstrakter Vektorräume, zum andern sind lineare Gleichungs– und Ungleichungssysteme sowie Eigenwertprobleme für die Anwendungen inzwischen von so grundlegender Bedeutung, daß ihrer Behandlung in der mathematischen Grundausbildung besonderes Gewicht zukommt.

Wir werden deshalb im folgenden zunächst hauptsächlich die lineare Algebra behandeln, geometrische Sprechweisen und Begriffe aber zur Veranschaulichung benutzen. Die affine und euklidische Geometrie wird dann in Kapitel 6 ausführlicher dargestellt.

Vorbemerkungen über Mengen, Abbildungen, Relationen

Die folgenden Bemerkungen umfassen eine Sammlung von Begriffen und Aussagen, die zur mathematischen Allgemeinbildung gehören und teilweise von der Schule her bekannt sein sollten. Diese Begriffe sind grundlegend für die weiteren Betrachtungen, sie gehören aber nicht zum eigentlichen Stoffgebiet der linearen Algebra.

1. Logische Symbole

Aufgabe der Mathematik ist es, abstrakte Srukturen zu entwickeln und Aussagen über diese Strukturen herzuleiten. Wird dazu die Umgangssprache benutzt, so kann das zu Unklarheiten und Mehrdeutigkeiten führen. Um mathematische Aussagen und Schlüsse einwandfrei formulieren zu können, wurde eine formalisierte Sprache entwickelt, die nur Symbole benutzt; ihre Untersuchung ist Gegenstand der *Mathematischen Logik.*

Da sie eine präzise und knappe Darstellung erlaubt, fand die formalisierte Schreibweise Eingang in viele Lehrbücher und zum Teil sogar in die Schulmathematik. Insbesondere für Informatiker ist eine formale Beschreibung mathematischer Vorgänge von Bedeutung.

Andererseits hat Mathematik auch viel mit Intuition, Fantasie und Vorstellungskraft zu tun, die nur durch Verwendung der Umgangssprache entstehen können. Die formalisierte Schreibweise erschwert das Verständnis eher. Sie ist deshalb aus den neueren Lehrbüchern wieder weitgehend verschwunden und wird auch im folgenden meistens nicht benutzt.

Damit man sich aber in der Literatur zurechtfindet, sei hier eine Liste der gebräuchlichsten Symbole (Abkürzungen) aufgeführt:

$\neg$ Negation (einer Aussage)

$\wedge$	Konjunktion (Verbindung zweier Aussagen durch *und*); häufig wird $\wedge$ durch ein Komma ersetzt
$\vee$	Disjunktion (Verbindung zweier Aussagen durch *oder*)
$\Longrightarrow$	Implikation (aus einer Aussage folgt eine andere); wenn ..., dann...; daraus folgt
$\Longleftrightarrow$	Äquivalenz (zweier Aussagen); ...genau dann, wenn...
$\forall$	Allquantor (für alle ...)
$\exists$	Existenzquantor (es gibt ein ...)
$\in$	Element von
$\notin$	nicht Element von

Die Symbole $:=$ und $:\Longleftrightarrow$ (bzw. $=:$ und $\Longleftrightarrow:$) werden benutzt, wenn Größen oder Begriffe, die auf der Seite des Doppelpunktes stehen, durch die andere Seite erklärt werden sollen.

Wer sich über die Mathematische Logik (und ihre Anwendungen in der Informatik) informieren möchte, dem sei das einführende Buch

Böhme, G. : Einstieg in die Mathematische Logik, Hanser, München u.a. 1981

empfohlen.

2. Mengen

Beim Aufbau mathematischer Strukturen werden aus bekannten Begriffen neue abgeleitet. Verfolgt man diesen Aufbau zurück, so stößt man zwangsläufig auf Grundbegriffe, die mathematisch nicht weiter erklärt werden können, wie z.B. Punkte in einem axiomatischen Aufbau der Geometrie. Man kann solche Begriffe nur dadurch festlegen, daß man den Umgang mit ihnen durch Gesetze (*Axiome*) regelt.

Ein für die gesamte Mathematik grundlegender Begriff ist der der Menge. Der Mengenbegriff wird hier nicht axiomatisch eingeführt, es genügt uns vielmehr der "naive Standpunkt" der Mengenlehre, der auf Cantor (1845 – 1918) zurückgeht:

Eine Menge ist eine Zusammenfassung von "Objekten", den Elementen der Menge.

Eine Menge ist also festgelegt, wenn ihre Elemente festgelegt sind; damit muß für jedes "Objekt" feststehen, ob es zu der Menge gehört oder nicht; ob man das auch entscheiden kann oder nicht, ist ein anderes Problem.

Zwei Mengen A und B sind somit *gleich*, wenn sie die gleichen Elemente besitzen.

Um Widersprüche zu vermeiden, wird festgelegt, daß eine Menge nicht sich selbst als Element enthalten darf. Mehr über den axiomatischen Aufbau der Mengenlehre und dabei mögliche Widersprüche findet man in dem elementaren Buch

Halmos, P.R. : Naive Mengenlehre, Vandenhoek & Ruprecht, Göttingen 1976.

Beispiele.

$\mathbb{N}$ Menge der natürlichen Zahlen.

$\mathbb{N}_0$ Menge der natürlichen Zahlen und der Null.

$\mathbb{Z}$ Menge der ganzen Zahlen.

$\mathbb{Q}$ Menge der rationalen Zahlen.

$\mathbb{R}$ Menge der reellen Zahlen.

Die Beschreibung von Mengen erfolgt dadurch, daß ihre Elemente aufgezählt oder durch eine charakteristische Eigenschaft festgelegt werden. Die Aufzählung kann dabei (besonders bei Mengen mit unendlich vielen Elementen) auch in symbolischer Form vorgenommen werden.

Beispiele.

$\mathbb{N} = \{1,2,3,...\}$,

$\mathbb{N}_0 = \{0,1,2,3,...\}$,

$\mathbb{Z} = \{0,1,-1,2,-2,...\}$ oder $\mathbb{Z} = \{...,-2,-1,0,1,2,...\}$,

$\mathbb{Q} = \{x \mid x = \frac{p}{q},\ p,q \in \mathbb{Z},\ q \neq 0\}$.

Wir verwenden immer geschweifte Klammern $\{...\}$ zur Angabe von Mengen.

Die drei Punkte "..." sollen bedeuten, daß die Folge der aufgeführten Elemente in offensichtlicher Weise fortgesetzt werden soll; das setzt voraus, daß die Fortsetzung wirklich offensichtlich ist. Wird eine Menge durch eine Eigenschaft ihrer Elemente angegeben, so werden die Elemente und die kennzeichnende Eigenschaft (bzw. die Eigenschaften) durch einen senkrechten Strich getrennt, wie wir es oben bei der Beschreibung von $\mathbb{Q}$ schon getan haben. Nicht alle Mengen können durch Aufzählen ihrer Elemente angegeben werden; das ist z.B. bei $\mathbb{R}$ nicht möglich.

Aus mathematischen Gründen benötigt man auch eine Menge, die keine Elemente besitzt, also "leer" ist; es gibt nur eine solche Menge.

Definition. $\emptyset$ sei die Menge, die keine Elemente hat. Sie heißt die *leere Menge.*

Bezeichnung. Für eine Menge A sei $|A|$ die Anzahl der Elemente von A. Ist A endlich, so ist $|A| \in \mathbb{N}_0$, ist A unendlich, so schreiben wir $|A| = \infty$.

Ein weiterer, viel benutzter Begriff ist der der Teilmenge.

Definition. Eine Menge B heißt *Teilmenge* einer Menge A, wenn alle Elemente von B auch Elemente von A sind. Schreibweise : $B \subset A$ oder $A \supset B$.

Wir wollen diese Definition zur Übung auch rein formal schreiben:

$$B \subset A \;:\Longleftrightarrow\; [x \in B \implies x \in A].$$

Beispiele. $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$. Für jede Menge A gilt $A \subset A$ und $\emptyset \subset A$.

Die Gesamtheit aller Teilmengen einer Menge A bildet wieder eine Menge, die *Potenzmenge* $\mathcal{P}(A)$ von A :

$$\mathcal{P}(A) := \{B \mid B \subset A\}$$

$\mathcal{P}(A)$ und jede Teilmenge $\mathcal{M} \subset \mathcal{P}(A)$ ist eine Menge von Mengen. Um das besser ausdrücken zu können, spricht man auch von einem *Mengensystem* $\mathcal{M}$. Man be-

achte aber, daß aufgrund unserer Vereinbarung, daß eine Menge nicht sich selbst als Element enthalten darf, die "Menge aller Mengen" als System $\mathcal{M}$ nicht zulässig ist.

3. Mengenoperationen

Definition. Es seien A,B Mengen. Dann heißt

$A \cup B := \{x \mid x \in A \text{ oder } x \in B\}$ die *Vereinigung* von A und B,

$A \cap B := \{x \mid x \in A \text{ und } x \in B\}$ der *Durchschnitt* von A und B,

$A \setminus B := \{x \mid x \in A, x \notin B\}$ die *Differenz* von A und B,

$A \Delta B := (A \setminus B) \cup (B \setminus A)$ die *symmetrische Differenz* von A und B.

Ist $B \subset A$ und ist die Grundmenge A fest vorgegeben, so schreibt man für $A \setminus B$ auch B^c und nennt das das *Komplement von B in A*.

Bemerkung. Einige einfache Aussagen über Mengen lassen sich unmittelbar verifizieren. So gelten für alle Mengen A und B: **(a)** $A = B \iff A \subset B, B \subset A$.

(b) $B \subset A \iff A \cup B = A \iff A \cap B = B \iff A \Delta B = A \setminus B$.

(c) $A \cup A = A \cap A = A$, $A \cup \emptyset = A$, $A \cap \emptyset = \emptyset$.

Die etwas weniger trivialen Rechenregeln fassen wir in dem folgenden Satz zusammen.

Satz 1. *Es seien A,B,C Mengen. Dann gilt:*

(a) $(A \cup B) \cup C = A \cup (B \cup C)$,
$(A \cap B) \cap C = A \cap (B \cap C)$, *("Assoziativgesetze")*

(b) $A \cup B = B \cup A$,
$A \cap B = B \cap A$, *("Kommutativgesetze")*

(c) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$,
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, *("Distributivgesetze")*

(d) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$,
$A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$. *("de Morgan–Regeln")*

Beweis. Ein beliebtes Beweisprinzip für Mengengleichungen ist auf der vorangehenden Bemerkung (a) aufgebaut. Man zeigt zunächst, daß die Menge links Teilmenge der Menge rechts ist, dann umgekehrt, daß die Menge rechts Teilmenge der Menge links ist. Wir wollen das Prinzip jeweils an der ersten Gleichung von (c) und von (d) deutlich machen. Die restlichen Beweise werden als Übungsaufgabe empfohlen.

Beh. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

" $\subset$ ": Sei $x \in A \cup (B \cap C) \Rightarrow x \in A$ oder $x \in (B \cap C)$.

1. Fall: $x \in A \Rightarrow x \in A \cup B$ und $x \in A \cup C \Rightarrow x \in (A \cup B) \cap (A \cup C)$.

2. Fall: $x \in B \cap C \Rightarrow x \in B$ und $x \in C \Rightarrow x \in A \cup B$ und $x \in A \cup C \Rightarrow x \in (A \cup B) \cap (A \cup C)$.

" $\supset$ ": Sei $x \in (A \cup B) \cap (A \cup C) \Rightarrow x \in A \cup B$ und $x \in A \cup C \Rightarrow (x \in A$ oder $x \in B)$ und $(x \in A$ oder $x \in C) \Rightarrow x \in A$ oder $(x \in B$ und $x \in C) \Rightarrow x \in A$ oder $x \in B \cap C \Rightarrow x \in A \cup (B \cap C)$. ∎

Beh. $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

" $\subset$ ": Sei $x \in A \setminus (B \cup C) \Rightarrow x \in A, x \notin B \cup C \Rightarrow x \in A, x \notin B, x \notin C \Rightarrow x \in A \setminus B$, $x \in A \setminus C \Rightarrow x \in (A \setminus B) \cap (A \setminus C)$.

" $\supset$ ": Sei $x \in (A \setminus B) \cap (A \setminus C) \Rightarrow x \in A \setminus B, x \in A \setminus C \Rightarrow x \in A, x \notin B, x \notin C \Rightarrow$ $x \in A, x \notin B \cup C \Rightarrow x \in A \setminus (B \cup C)$. ∎

Es ist offensichtlich, wie sich die Aussagen von Satz 1 auf endlich viele Mengen verallgemeinern lassen. Wir wollen nun aber zeigen, daß man sogar ganze Mengensysteme zulassen kann.

Definition. Es sei $\mathcal{M}$ ein nichtleeres Mengensystem. Dann sei

$$\bigcup_{B \in \mathcal{M}} B := \{x \mid \text{Es gibt ein } B \in \mathcal{M} \text{ mit } x \in B\},$$

$$\bigcap_{B \in \mathcal{M}} B := \{x \mid \text{Für alle } B \in \mathcal{M} \text{ gilt } x \in B\}.$$

Ist $\mathcal{M} = \{B_1,\ldots,B_n\}$, so schreibt man

$$\bigcup_{i=1}^{n} B_i \ , \quad \bigcap_{i=1}^{n} B_i .$$

Ist $\mathcal{M} = \{B_1,B_2,\ldots\}$, so schreibt man formal

$$\bigcup_{i=1}^{\infty} B_i \ , \quad \bigcap_{i=1}^{\infty} B_i .$$

Entsprechend vereinfachte Schreibweisen werden wir später häufig benutzen; z.B. bezeichnet im folgenden Satz

$$\bigcup_{B\in\mathcal{M}} (A \cup B)$$

die Vereinigung über das Mengensystem $\mathcal{M}' = \{A \cup B \mid B \in \mathcal{M}\}$, usw.

Satz 2. *Es seien $\mathcal{M}$ ein nichtleeres Mengensystem und A eine Menge. Dann gilt:*

(a) $$A \cup \Big(\bigcup_{B\in\mathcal{M}} B\Big) = \bigcup_{B\in\mathcal{M}} (A \cup B),$$

$$A \cap \Big(\bigcap_{B\in\mathcal{M}} B\Big) = \bigcap_{B\in\mathcal{M}} (A \cap B),$$

(b) $$A \cup \Big(\bigcap_{B\in\mathcal{M}} B\Big) = \bigcap_{B\in\mathcal{M}} (A \cup B),$$

$$A \cap \Big(\bigcup_{B\in\mathcal{M}} B\Big) = \bigcup_{B\in\mathcal{M}} (A \cap B),$$

(c) $$A \setminus \Big(\bigcup_{B\in\mathcal{M}} B\Big) = \bigcap_{B\in\mathcal{M}} (A \setminus B),$$

$$A \setminus \Big(\bigcap_{B\in\mathcal{M}} B\Big) = \bigcup_{B\in\mathcal{M}} (A \setminus B).$$

Beweis. Da alle Aussagen nach der gleichen Methode bewiesen werden können, wollen wir uns auf je eine Aussage beschränken. Wir werden hier allerdings ein etwas kürzeres Beweisprinzip anwenden, indem wir die Aussage, daß x Element der linken Menge ist, äquivalent umformen.

Beh. $A \cap \left(\bigcap_{B \in \mathcal{M}} B \right) = \bigcap_{B \in \mathcal{M}} (A \cap B)$.

Es gilt:

$$x \in A \cap \left(\bigcap_{B \in \mathcal{M}} B \right) \iff x \in A, x \in \bigcap_{B \in \mathcal{M}} B \iff x \in A, x \in B \text{ für alle } B \in \mathcal{M}$$

$$\iff x \in A \cap B \text{ für alle } B \in \mathcal{M} \iff x \in \bigcap_{B \in \mathcal{M}} (A \cap B). \qquad \blacksquare$$

Beh. $A \cap \left(\bigcup_{B \in \mathcal{M}} B \right) = \bigcup_{B \in \mathcal{M}} (A \cap B)$.

Es gilt:

$$x \in A \cap \left(\bigcup_{B \in \mathcal{M}} B \right) \iff x \in A, x \in \bigcup_{B \in \mathcal{M}} B \iff x \in A, x \in B \text{ für mindestens ein}$$

$$B \in \mathcal{M} \iff x \in A \cap B \text{ für mindestens ein } B \in \mathcal{M} \iff x \in \bigcup_{B \in \mathcal{M}} (A \cap B). \qquad \blacksquare$$

Beh. $A \setminus \left(\bigcap_{B \in \mathcal{M}} B \right) = \bigcup_{B \in \mathcal{M}} (A \setminus B)$.

Es gilt:

$$x \in A \setminus \left(\bigcap_{B \in \mathcal{M}} B \right) \iff x \in A, x \notin \bigcap_{B \in \mathcal{M}} B \iff x \in A, x \notin B \text{ für mindestens ein}$$

$$B \in \mathcal{M} \iff x \in A \setminus B \text{ für mindestens ein } B \in \mathcal{M} \iff x \in \bigcup_{B \in \mathcal{M}} (A \setminus B). \qquad \blacksquare$$

Für die Anzahl der Elemente einer Vereinigungsmenge gibt es eine nützliche Formel, die insbesondere in der Kombinatorik und der Stochastik benutzt wird. Wir benutzen sie in § 1.6 beim Beweis des Chinesischen Restsatzes.

Satz 3. *Es seien $A_1,\dots A_k$ endliche Mengen. Dann gilt :*

$$\Big|\bigcup_{i=1}^{k} A_i\Big| = \sum_{i=1}^{k} |A_i| - \sum_{1\le i<j\le k} |A_i\cap A_j|$$

$$+ - \cdots + (-1)^k \sum_{1\le i_1<\dots<i_{k-1}\le k} |A_{i_1}\cap\cdots\cap A_{i_{k-1}}| + (-1)^{k+1}\,|A_1\cap\cdots\cap A_k|\,.$$

Bemerkung. Das Summenzeichen Σ ist die Abkürzung für mehrfache Additionen. Im ersten Fall wird über alle $i \in \{1,\dots,k\}$ summiert, im zweiten Fall über alle $i \in \{1,\dots,k-1\}$ und für gewähltes i über alle $j \in \{i+1,\dots,k\}$, usw.

Beweis. Wir führen den Beweis durch vollständige Induktion nach k. Induktionsanfang: Für $k = 1$ steht links und rechts jeweils nur $|A_1|$ und die Behauptung ist trivial. Für $k = 2$ gilt :

$$|A_1 \cup A_2| = |A_1 \cup (A_2 \setminus (A_1 \cap A_2))| = |A_1| + |A_2 \setminus (A_1 \cap A_2)|$$
$$= |A_1| + |A_2| - |A_1 \cap A_2|.$$

Induktionsvoraussetzung : Die Behauptung sei richtig für k.

Induktionsschluß von k auf $k+1$: Es ist

$$\bigcup_{i=1}^{k+1} A_i = \Big(\bigcup_{i=1}^{k} A_i\Big) \cup A_{k+1}\,.$$

Nach dem eben bewiesenen Induktionsanfang, angewendet auf die zwei Mengen $A_1 \cup \cdots \cup A_k$ und A_{k+1}, erhalten wir

$$(*) \quad \Big|\bigcup_{i=1}^{k+1} A_i\Big| = \Big|\bigcup_{i=1}^{k} A_i\Big| + |A_{k+1}| - \Big|\Big(\bigcup_{i=1}^{k} A_i\Big) \cap A_{k+1}\Big|.$$

Nach Induktionsvoraussetzung gilt

$$\Big|\bigcup_{i=1}^{k} A_i\Big| = \sum_{i=1}^{k} |A_i| - \sum_{1 \le i < j \le k} |A_i \cap A_j| + - \cdots + (-1)^{k+1} |A_1 \cap \cdots \cap A_k|$$

und

$$\Big|\Big(\bigcup_{i=1}^{k} A_i\Big) \cap A_{k+1}\Big| = \Big|\bigcup_{i=1}^{k} (A_i \cap A_{k+1})\Big| = \sum_{i=1}^{k} |A_i \cap A_{k+1}| - + \cdots$$

$$+ (-1)^k \sum_{1 \le i_1 < \ldots < i_{k-1} \le k} |(A_{i_1} \cap A_{k+1}) \cap \cdots \cap (A_{i_{k-1}} \cap A_{k+1})|$$

$$+ (-1)^{k+1} |(A_1 \cap A_{k+1}) \cap \cdots \cap (A_k \cap A_{k+1})|$$

Dies in (*) eingesetzt, ergibt

$$\Big|\bigcup_{i=1}^{k+1} A_i\Big| = \sum_{i=1}^{k} |A_i| - \sum_{1 \le i < j \le k} |A_i \cap A_j| + - \cdots + (-1)^{k+1} |A_1 \cap \cdots \cap A_k|$$

$$+ |A_{k+1}| - \sum_{i=1}^{k} |A_i \cap A_{k+1}| + - \cdots$$

$$+ (-1)^{k+1} \sum_{1 \le i_1 < \ldots < i_{k-1} \le k} |(A_{i_1} \cap A_{k+1}) \cap \cdots \cap (A_{i_{k-1}} \cap A_{k+1})|$$

$$+ (-1)^{k+2} |(A_1 \cap A_{k+1}) \cap \cdots \cap (A_k \cap A_{k+1})|$$

$$= \sum_{i=1}^{k+1} |A_i| - \sum_{1 \le i < j \le k+1} |A_i \cap A_j| + - \cdots$$

$$+ (-1)^{k+1} \sum_{1 \le i_1 < \ldots < i_k \le k+1} |A_{i_1} \cap \cdots \cap A_{i_k}| + (-1)^{k+2} |A_1 \cap \cdots \cap A_{k+1}|. \quad \blacksquare$$

Eine sehr wichtige Methode, aus Mengen neue Mengen zu konstruieren, ist das Bilden von Produktmengen. Dazu geben wir zunächst eine vorbereitende Erklärung.

Seien $A_1,\ldots,A_n$ Mengen. Aus je n Elementen $x_1 \in A_1,\ldots,x_n \in A_n$ kann ein neues Objekt gebildet werden, das *geordnete n–Tupel* $(x_1,\ldots,x_n)$. Dabei heißen zwei n–Tupel $(x_1,\ldots,x_n)$ und $(y_1,\ldots,y_n)$ *gleich*, wenn $x_i = y_i$ für alle $i = 1,\ldots,n$ gilt. Ein n–Tupel ist also eine Zusammenfassung von n Elementen (i.a. aus verschiedenen Mengen), wobei es auf die Reihenfolge ankommt.

Definition. Es seien $A_1,\ldots,A_n$ Mengen. Dann heißt die Menge

$$A_1 \times \cdots \times A_n := \{(x_1,\ldots,x_n) |\ x_1 \in A_1,\ldots,x_n \in A_n\}$$

das (*kartesische*) *Produkt* von $A_1,\ldots,A_n$. Sind alle A_i gleich A, so schreibt man für die Produktmenge auch kürzer A^n.

In der linearen Algebra spielt die Produktmenge $\mathbb{R}^n$ eine wichtige Rolle.

4. Abbildungen

Gegeben seien zwei Mengen A und B. Eine *Abbildung* f von A nach (oder in) B, Schreibweise: $f\colon A \longrightarrow B$, ist eine Zuordnungsvorschrift, die jedem $x \in A$ genau ein $y \in B$ zuordnet. Man schreibt für y auch $f(x)$ und für die Zuordnung : $x \longmapsto f(x)$. Kurzschreibweisen:

$$\begin{array}{l} f\colon A \longrightarrow B \\ \quad x \longmapsto y = f(x) \end{array} \qquad \text{oder} \qquad \begin{array}{l} A \xrightarrow{f} B \\ x \xmapsto{f} y \end{array}$$

Andere gebräuchliche Namen für Abbildung sind *Funktion* (besonders, wenn $B \subset \mathbb{R}$

ist), *Transformation* oder *Operator*. Die Menge aller Abbildungen von A nach B bezeichnen wir mit B^A.

Bemerkung. Der Begriff der Abbildung ist hier mit Hilfe des zwar anschaulichen, aber mathematisch nicht definierten Wortes "Zuordnungsvorschrift" umgangssprachlich erklärt worden; es wurde somit wieder der "naive" Standpunkt eingenommen. Prinzipiell läßt sich der Abbildungsbegriff aber auch rein mengentheoretisch erklären:

Da jedem $x \in A$ genau ein $y \in B$ zugeordnet werden soll, ist die Abbildung f gegeben durch die Menge $\{(x,f(x))|\ x \in A\} \subset A \times B$. Umgekehrt wird zu jeder Menge $C \subset A \times B$ mit den Eigenschaften

(a) für alle $x \in A$, $y,\overline{y} \in B$ gilt: Aus $(x,y) \in C$, $(x,\overline{y}) \in C$ folgt $y = \overline{y}$,

(b) zu jedem $x \in A$ gibt es ein $y \in B$ mit $(x,y) \in C$,

eine Zuordnungsvorschrift gegeben durch $x \longmapsto y$, wobei y das nach (a) und (b) eindeutig bestimmte Element aus B ist, für das $(x,y) \in C$ gilt.

Als mathematische Definition können wir deshalb wählen:

Definition. Eine *Abbildung* $f\colon A \longrightarrow B$ ist eine Teilmenge von $A \times B$, die (a) und (b) erfüllt.

Wir bevorzugen im folgenden die anschauliche Vorstellung der Abbildung und geben der Menge $\{(x,f(x))|\ x \in A\}$ gleich einen anderen Namen.

Definition. Es sei $f\colon A \longrightarrow B$ eine Abbildung. Dann heißt A *Definitionsbereich*, B *Wertebereich*, und $f(A) := \{f(x)|\ x \in A\}$ *Bild* von A (unter f).

Für $x \in A$ heißt $f(x)$ *Bild(-punkt)* von x und für $y \in f(A)$ heißt x (ein) *Urbild* von y, wenn $f(x) = y$ gilt.

Für $C \subset B$ heißt $f^{-1}(C) := \{x \in A|\ f(x) \in C\}$ das *Urbild der Menge* C.

Die Menge $\{(x,f(x))|\ x \in A\}$ heißt *Graph* von f.

Bemerkungen. **(a)** Es gilt $f(A) \subset B$, aber es muß nicht Gleichheit gelten. Jedoch ist

es üblich, Abbildungen $f: A \longrightarrow B$ und $g: A \longrightarrow f(A)$ als gleich anzusehen, wenn $f(x) = g(x)$ für alle $x \in A$ gilt.

Die Begriffe "Wertebereich", "Bild" oder ähnliche wie "Wertemenge", "Bildmenge" werden in der Literatur nicht einheitlich benutzt.

(b) Jedes $x \in A$ hat ein eindeutiges Bild $f(x) \in f(A)$, aber ein $y \in f(A)$ kann mehrere (sogar unendlich viele) Urbilder haben.

Definition. Es sei $f: A \longrightarrow B$ eine Abbildung.

(a) f heißt *surjektiv* oder *Abbildung auf*, falls $f(A) = B$ gilt.

(b) f heißt *injektiv* oder *eineindeutig*, wenn aus $x_1, x_2 \in A$, $x_1 \neq x_2$ folgt, daß $f(x_1) \neq f(x_2)$.

(c) f heißt *bijektiv*, wenn f surjektiv und injektiv ist.

Beispiele.

(a) $f: \mathbb{R} \longrightarrow \mathbb{R}$
$x \longmapsto (x-1)^2$

ist weder injektiv noch surjektiv.

(b) $f: \mathbb{R} \longrightarrow \mathbb{R}$
$x \longmapsto x\,(x-1)\,(x+1)$

ist surjektiv aber nicht injektiv.

(c) $f: \mathbb{N} \longrightarrow \mathbb{Z}$

$$n \longmapsto \begin{cases} \frac{n-1}{2} & \text{falls } n \text{ ungerade} \\ -\frac{n}{2} & \text{falls } n \text{ gerade} \end{cases}$$

ist bijektiv.

Mit Hilfe des Abbildungsbegriffes können wir nun die Aufzählbarkeit einer unendlichen Menge genauer definieren.

Definition. Eine unendliche Menge A heißt *abzählbar*, wenn eine bijektive Abbildung $f: \mathbb{N} \longrightarrow A$ existiert. Eine nichtabzählbare unendliche Menge heißt *überabzählbar*.

Beispiel. Die Mengen $\mathbb{Z}$ und $\mathbb{Q}$ sind abzählbar, $\mathbb{R}$ ist überabzählbar.

Eine triviale Möglichkeit, eine Abbildung $f\colon A \longrightarrow A$ zu definieren, ist durch die Vorschrift $x \longmapsto x$ gegeben. Da diese Abbildung öfter auftritt, soll sie einen Namen erhalten. Weiterhin wollen wir aus gegebenen Abbildungen neue Abbildungen konstruieren.

Definitionen. **(a)** Es sei A eine Menge. Die Abbildung $\mathrm{id}_A : \begin{array}{c} A \longrightarrow A \\ x \longmapsto x \end{array}$ heißt *Identität* (auf A) oder *identische Abbildung.*

(b) Es seien $f\colon \begin{array}{c} A \longrightarrow B \\ x \longmapsto f(x) \end{array}$ eine Abbildung und $C \subset A$. Dann heißt $f|_C\colon \begin{array}{c} C \longrightarrow B \\ x \longmapsto f(x) \end{array}$ *Einschränkung* oder *Restriktion* von f auf C. Ist $g : C \longrightarrow B$ eine Abbildung mit $g = f|_C$, so heißt f *Fortsetzung* von g auf A.

(c) Es sei $f : A \longrightarrow B$ eine bijektive Abbildung. Dann heißt die Abbildung $f^{-1}\colon \begin{array}{c} B \longrightarrow A \\ y \longmapsto x \end{array}$ mit $f(x) = y$ *Umkehrabbildung* oder *inverse Abbildung* von f.

(d) Es seien $f\colon \begin{array}{c} A \longrightarrow B \\ x \longmapsto f(x) \end{array}$ und $g : \begin{array}{c} B \longrightarrow C \\ y \longmapsto g(y) \end{array}$ Abbildungen. Dann heißt die Abbildung $g \circ f\colon \begin{array}{c} A \longrightarrow C \\ x \longmapsto g(f(x)) \end{array}$ *zusammengesetzte Abbildung* oder *Komposition* oder auch *Verkettung.* Sprechweise: "g Kreis f" oder "g nach f".

Bemerkungen. **(a)** Ist f bijektiv, so auch f^{-1} und es gilt $(f^{-1})^{-1} = f$.

(b) Ist f bijektiv, so gilt $f^{-1} \circ f = \mathrm{id}_A$ und $f \circ f^{-1} = \mathrm{id}_B$.

(c) Die Komposition ist nicht kommutativ (siehe (b)) aber assoziativ. Es gilt nämlich $h \circ (g \circ f) = (h \circ g) \circ f$.

(d) Man beachte folgendes: Ist $f\colon A \longrightarrow B$ eine Abbildung und ist $C \subset B$, so existiert das Urbild $f^{-1}(C)$ immer, auch wenn die Umkehrabbildung f^{-1} nicht existiert. Existiert aber f^{-1}, so ist $f^{-1}(C)$ gerade das Bild von C unter f^{-1}.

Beispiele. **(a)** Für die Funktion aus dem obigen Beispiel (c) existiert die Umkehrfunktion. Es ist

$$f^{-1}: \mathbb{Z} \longrightarrow \mathbb{N}$$

$$z \longmapsto \begin{cases} 2z+1 & \text{für } z \geq 0 \\ -2\ z & \text{für } z < 0 \end{cases}$$

(b) Für $f: \mathbb{R} \setminus \{0\} \longrightarrow \mathbb{R} \setminus \{0\}$ mit $f(x) = \frac{1}{x}$ gilt $f^{-1} = f$.

In den voranstehenden Beispielen haben wir die Umkehrabbildung f^{-1} einfach angegeben, d.h. wir haben eine Abbildung $f: A \longrightarrow B$ und eine weitere $f^{-1}: B \longrightarrow A$ mit $f^{-1} \circ f = \mathrm{id}_A$ und $f \circ f^{-1} = \mathrm{id}_B$. Reicht das nun aus, oder müssen wir noch nachweisen, daß f überhaupt bijektiv ist? Die Antwort gibt der folgende Satz.

Satz 4. *Es seien A, B nichtleere Mengen und $f: A \longrightarrow B$ eine Abbildung. Dann gilt:*

(a) *f ist genau dann injektiv, wenn eine Abbildung $g: B \longrightarrow A$ mit $g \circ f = id_A$ existiert.*

(b) *f ist genau dann surjektiv, wenn eine Abbildung $g: B \longrightarrow A$ mit $f \circ g = id_B$ existiert.*

(c) *f ist genau dann bijektiv, wenn eine Abbildung $g: B \longrightarrow A$ mit $g \circ f = id_A$ und $f \circ g = id_B$ existiert.*

Beweis. (a) Sei f injektiv, d.h. jedes $y \in f(A)$ hat genau ein Urbild $x \in A$. Wir erklären die Abbildung $g: B \longrightarrow A$ durch folgende Vorschrift

$$g: y \longmapsto \begin{cases} x & \text{, falls } y \in f(A) \text{ und } f(x) = y \\ x_0 & \text{, falls } y \notin f(A) \end{cases}$$

Hierbei ist $x_0 \in A$ ein festes Element, das wegen $A \neq \emptyset$ existiert. Dann gilt $g \circ f(x) = x$ für alle $x \in A$, also $g \circ f = \mathrm{id}_A$.

Umgekehrt sei eine Abbildung $g: B \longrightarrow A$ gegeben mit $g \circ f = \mathrm{id}_A$. Seien $x_1, x_2 \in A$ mit $f(x_1) = f(x_2)$. Dann gilt $x_1 = g \circ f(x_1) = g(f(x_1)) = g(f(x_2)) = g \circ f(x_2) = x_2$, d.h. f ist injektiv.

(b) Sei f surjektiv. Wir erklären $g: B \longrightarrow A$ dadurch, daß wir zu jedem $y \in B$ ein Urbild $x \in f^{-1}(\{y\})$ auswählen. Damit folgt für alle $y \in B$: $f \circ g(y) = f(g(y)) = f(x) = y$.

Umgekehrt sei $g : B \longrightarrow A$ mit $f \circ g = \mathrm{id}_B$ gegeben. Sei $y \in B$. Dann ist $y = f \circ g\,(y) = f(g\,(y))$, d.h. $y \in f(A)$ und f ist surjektiv.
(c) Ist f bijektiv, so erfüllt $g = f^{-1}$ die Bedingungen. Existiert umgekehrt eine Abbildung $g : B \longrightarrow A$ mit $g \circ f = \mathrm{id}_A$ und $f \circ g = \mathrm{id}_B$, so ist f nach (a) injektiv und nach (b) surjektiv, also bijektiv. ∎

Bemerkung. Bei der Behauptung (b) haben wir g dadurch definiert, daß wir aus den Mengen $f^{-1}(\{y\})$, $y \in B$, jeweils ein Element x ausgewählt haben. Dieses plausible Vorgehen ist aber nur deswegen möglich, weil wir an dieser Stelle stillschweigend das sogenannte *Auswahlaxiom* der axiomatischen Mengenlehre verwendet haben.

Über die Verwendung dieses Axioms und seiner äquivalenten Formen herrschen unterschiedliche Auffassungen, zum Teil wegen der manchmal absurd erscheinenden Folgerungen daraus. Man versucht daher häufig, soweit wie möglich ohne Auswahlaxiom auszukommen, andererseits ist es aber für bestimmte mathematische Gebiete wie etwa die Funktionalanalysis unerläßlich. Abgesehen von der obigen, nicht wesentlichen Stelle werden wir das Auswahlaxiom, bzw. eine dazu äquivalente Aussage, nur noch einmal, beim Beweis des Basisergänzungssatzes für unendlich dimensionale Vektorräume, explizit verwenden.

5. Relationen

Eine Relation auf einer Menge A ist eine Beziehung, die zwischen den Elementen von A bestehen kann oder nicht. Es werden hier nur Beziehungen zwischen je zwei Elementen betrachtet. Man kann allgemeiner auch n–stellige Relationen untersuchen und Elemente aus verschiedenen Mengen zulassen; dann fällt z.B. der Abbildungsbegriff darunter.

Da eine Relation auf der Menge A vollständig durch die Paare $(x,y) \in A^2$ beschrieben wird, die in dieser Relation stehen, ist eine *Relation* R mathematisch nichts anderes als eine Teilmenge von A^2. Statt $(x,y) \in R$ schreiben wir aber $x\,R\,y$ und sagen, daß x *in Relation* R *zu* y *steht.*

Beispiele für Relationen sind etwa die Kleinerbeziehung, die Kleiner–Gleich–Beziehung und die Gleichheitsbeziehung bei reellen Zahlen oder die Teilerbeziehung bei natürlichen Zahlen. Besonders wichtig sind zwei spezielle Typen von Relationen, die Ordnungsrelationen und die Äquivalenzrelationen, die wir im folgenden näher untersuchen wollen. In der Informatik spielen allerdings auch andere Relationen eine Rolle.

Ordnungsrelationen

Hier versuchen wir die Beziehung $\leq$ von $\mathbb{R}$ auf allgemeinere Mengen zu übertragen, indem wir charakteristische Eigenschaften von $\leq$ als Axiome übernehmen.

Definition. Eine Relation R auf einer Menge A heißt *Ordnungsrelation* oder *Ordnung* (in älteren Büchern auch *partielle Ordnung* oder *Halbordnung*), wenn folgende Gesetze gelten. Statt $x\,R\,y$ schreiben wir $x \leq y$.

(a) Für alle $x \in A$ gilt: $x \leq x$. *("Reflexivität")*

(b) Für alle $x,y \in A$ gilt: Aus $x \leq y$ und $y \leq x$ folgt $x = y$. *("Antisymmetrie")*

(c) Für alle $x,y,z \in A$ gilt: Aus $x \leq y$ und $y \leq z$ folgt $x \leq z$. *("Transitivität")*

Ist $\leq$ Ordnung auf A, so heißt $(A,\leq)$ *geordnete Menge.*

Erfüllt eine Ordnung $\leq$ außerdem noch die Bedingung

(d) Für alle $x,y \in A$ gilt: $x \leq y$ oder $y \leq x$, *("Vergleichbarkeit")*

so heißt sie *Totalordnung* und $(A,\leq)$ heißt dann *total geordnete Menge.*

Beispiele. **(a)** Die übliche Ordnung $\leq$ auf $\mathbb{R}$ ist eine Totalordnung.

(b) Auf $\mathbb{R}^n$ wird durch

$$(x_1,\ldots,x_n) \leq (y_1,\ldots,y_n) \;:\Longleftrightarrow\; x_i \leq y_i\,, \quad i = 1,\ldots,n\,,$$

eine Ordnung erklärt, die keine Totalordnung ist.

(c) Die Inklusion $\subset$ von Mengen ist eine Ordnung, $(\mathcal{P}(A),\subset)$ ist geordnete Menge.

(d) Ist $(A,\leq)$ eine geordnete Menge und $B \subset A$, so ist $(B, \leq)$ mit der auf B eingeschränkten Ordnung ebenfalls geordnet. Man spricht dann von der *induzierten*

Ordnung auf B.

Wie bei den reellen Zahlen können wir auch bei geordneten Mengen von oberen und unteren Schranken, größten und kleinsten Elementen sowie von Supremum und Infimum sprechen.

Definition. Es seien $(A,\leq)$ eine geordnete Menge und $B \subset A$. Ein Element $z \in A$ heißt *obere Schranke* von B, falls $x \leq z$ für alle $x \in B$ gilt und *untere Schranke* von B, falls $z \leq x$ für alle $x \in B$ gilt. Gilt außerdem $z \in B$, so heißt z *größtes*, bzw. *kleinstes* Element von B.

$z \in A$ heißt *Supremum* von B oder *kleinste obere Schranke* von B, falls z obere Schranke von B ist und für jede obere Schranke z' von B gilt: $z \leq z'$. Schreibweise: $z = \sup B$ oder $z = \sup_{x \in B} x$.

$z \in A$ heißt *Infimum* von B oder *größte untere Schranke* von B, falls z untere Schranke von B ist und für jede untere Schranke z' von B gilt: $z' \leq z$. Schreibweise: $z = \inf B$ oder $z = \inf_{x \in B} x$.

Beispiele. **(a)** In $(\mathbb{R},\leq)$ besitzt jede nichtleere endliche Teilmenge $A \subset \mathbb{R}$ Supremum und Infimum. Für die abzählbare Teilmenge $\mathbb{N} \subset \mathbb{R}$ existiert zwar $\inf \mathbb{N} = 1$ aber nicht $\sup \mathbb{N}$.

(b) In $(\mathcal{P}(A),\subset)$ besitzt jede nichtleere Teilmenge $\mathcal{M} \subset \mathcal{P}(A)$ Infimum und Supremum, nämlich

$$\inf \mathcal{M} = \bigcap_{B \in \mathcal{M}} B, \quad \sup \mathcal{M} = \bigcup_{B \in \mathcal{M}} B.$$

Definition. Eine geordnete Menge $(A, \leq)$, in der je zwei Elemente immer ein Infimum und ein Supremum besitzen, heißt *Verband*. Besitzt jede nichtleere Teilmenge $B \subset A$ Infimum und Supremum, so heißt der Verband *vollständig*.

Beispiele. $(\mathbb{R},\leq)$ ist ein Verband, $(\mathcal{P}(A),\subset)$ ist ein vollständiger Verband.

Existiert das Supremum z einer geordneten Menge $(A, \leq)$, und ist $z \in A$, so ist

z das größte Element von A. Entsprechend ist inf A, falls es existiert und zu A gehört, das kleinste Element von A.

Nicht zu verwechseln mit diesen Begriffen sind die Begriffe maximales bzw. minimales Element von A.

Definition. Es sei $(A, \leq)$ eine geordnete Menge. Dann heißt $y \in A$ *maximales Element*, falls aus $y \leq x$, $x \in A$, stets $y = x$ folgt.

$y \in A$ heißt *minimales Element*, falls aus $x \leq y$, $x \in A$, stets $y = x$ folgt.

In einer totalgeordneten Menge $(A, \leq)$ ist jedes maximale Element auch größtes Element und umgekehrt ist ein größtes Element auch maximal. Entsprechendes gilt für minimale Elemente.

Die folgende Aussage ist ein hinreichendes Kriterium für die Existenz eines maximalen Elementes in einer geordneten Menge $(A, \leq)$. Sie ist zum Auswahlaxiom äquivalent und heißt Zornsches Lemma. Für einen Beweis mit Hilfe des Auswahlaxioms verweisen wir auf das schon zitierte Buch von Halmos.

Zornsches Lemma. *Es sei $(A,\leq)$ eine geordnete Menge und jede Menge $B \subset A$, die bezüglich der induzierten Ordnung totalgeordnet ist, besitze eine obere Schranke $z \in A$. Dann gibt es in A ein maximales Element.*

Äquivalenzrelationen

Eine wichtige Konstruktion in der Mathematik ist das Zusammenfassen von vergleichbaren (äquivalenten) Objekten, d.h. die Einteilung der Elemente einer Menge in Klassen. Jede Klasseneinteilung entspricht aber einer Relation auf dieser Menge, allerdings von einer anderen Art als die Ordnungsrelationen.

Definition. Eine Relation R auf einer Menge A heißt *Äquivalenzrelation*, wenn die folgenden Gesetze gelten. Statt $x\,R\,y$ schreiben wir $x \sim y$.

(a) Für alle $x \in A$ gilt: $x \sim x$. *("Reflexivität")*

(b) Für alle $x,y \in A$ gilt: Aus $x \sim y$ folgt $y \sim x$. *("Symmetrie")*

(c) Für alle $x,y,z \in A$ gilt: Aus $x \sim y$ und $y \sim z$ folgt $x \sim z$. *("Transitivität")*

Ist $\sim$ Äquivalenzrelation auf A und $x \in A$, so sei

$$[x]_\sim := \{y \in A \mid x \sim y\}.$$

$[x]_\sim$ heißt die *Äquivalenzklasse* von x, und x heißt *Repräsentant* der Äquivalenzklasse. Die Menge aller Äquivalenzklassen von Elementen $x \in A$ wird mit $A/_\sim$ bezeichnet und *Quotienten–* oder *Faktormenge* genannt.

Satz 5 und Definition. *Sei $\sim$ Äquivalenzrelation auf der Menge A. Dann gilt:*

(a) $[x]_\sim \neq \emptyset$ *für alle* $x \in A$,

(b) $[x]_\sim \neq [y]_\sim \Longrightarrow [x]_\sim \cap [y]_\sim = \emptyset$,

(c) $\bigcup_{x \in A} [x]_\sim = A$.

Man sagt, daß das System $\mathcal{M} = A/_\sim$ der Äquivalenzklassen eine *Partition* oder *Klasseneinteilung* von A bildet.

Ist umgekehrt $\mathcal{M} \subset \mathcal{P}(A)$ eine Partition von A, d.h. ein System nichtleerer, paarweise disjunkter Mengen, deren Vereinigung A ist, so gibt es eine Äquivalenzrelation $\sim$ auf A mit $\mathcal{M} = A/_\sim$.

Beweis. (a) Wegen $x \sim x$ ist $x \in [x]_\sim$, also $[x]_\sim \neq \emptyset$.

(b) Wir führen einen Widerspruchsbeweis und nehmen dazu an, daß $[x]_\sim \neq [y]_\sim$ und $[x]_\sim \cap [y]_\sim \neq \emptyset$ gilt. Dann existiert ein $z \in [x]_\sim \cap [y]_\sim$. Daraus folgt $z \sim x$ und $z \sim y$, also wegen der Eigenschaften (b),(c) einer Äquivalenzrelation auch $x \sim y$. Seien nun $x' \in [x]_\sim$, $y' \in [y]_\sim$. Aus $x' \sim x$, $x \sim y$ folgt $x' \sim y$, d.h. $x' \in [y]_\sim$ und aus $y' \sim y$, $y \sim x$ folgt analog $y' \in [x]_\sim$, also $[x]_\sim = [y]_\sim$. Dies ist ein Widerspruch. Es gilt daher $[x]_\sim \cap [y]_\sim = \emptyset$.

(c) ist trivial wegen $x \in [x]_\sim$.

Nun beweisen wir die Umkehrung. Da $\mathcal{M}$ eine Partition von A ist, liegt jedes Element $x \in A$ in genau einem $B_x \in \mathcal{M}$. Dadurch wird eine Abbildung $f: A \longrightarrow \mathcal{M}$ mit $f(x) = B_x$ definiert. Wir setzen nun $x \sim y :\Longleftrightarrow f(x) = f(y)$. Dann folgt sofort,

daß $\sim$ eine Äquivalenzrelation ist mit $B_x = [x]_\sim$. ∎

Bei dem Beweis von Satz 5 haben wir gleich auch die wichtigste Methode zur Entstehung von Äquivalenzrelationen kennengelernt, die *Faktorisierung nach einer Abbildung.*

Satz 6. *Es sei* $f: A \longrightarrow B$ *eine Abbildung. Dann wird durch* $x \sim y :\Longleftrightarrow f(x) = f(y)$ *eine Äquivalenzrelation auf* A *erklärt.*

Beweis. Einfache Übungsaufgabe. ∎

Schreibweise: Statt $A/_\sim$ schreibt man hier $A/_f$.

Bemerkung. Auf triviale Weise wird jede Äquivalenzrelation $\sim$ durch eine Abbildung erzeugt. Sei nämlich

$$\begin{aligned} k: A &\longrightarrow A/_\sim \\ x &\longmapsto [x]_\sim \end{aligned}$$

die sogenannte *kanonische Abbildung.* Diese ist surjektiv und es gilt $A/_\sim = A/_k$.

Nun können wir einen Satz beweisen, der den Ausgangspunkt einer Reihe später oft benutzter Sätze bildet. Dabei erklärt sich auch der Ausdruck *Faktorisieren* bzw. *Faktormenge*, da Abbildungen in "Faktoren" zerlegt werden (bezüglich der Komposition als "Multiplikation").

Satz 7 (Grundform des Homomorphie–Satzes). *Es seien* $f: A \longrightarrow B$ *eine Abbildung und* $k: A \longrightarrow A/_f$ *die kanonische Abbildung. Dann existiert eine injektive Abbildung* $\bar{f}: A/_f \longrightarrow B$ *mit* $f = \bar{f} \circ k$. *Ist* f *surjektiv, so ist* $\bar{f}$ *bijektiv.*

Beweis. Wir definieren $\bar{f}$ durch $\bar{f}([x]_\sim) = f(x)$ für alle $x \in A$. Diese Definition ist unabhängig von der speziellen Wahl des Repräsentanten $x \in [x]_\sim$, denn aus $[x]_\sim = [y]_\sim$ folgt $x \sim y$ und somit nach Definition von $\sim$ auch $f(x) = f(y)$. Offensichtlich ist $f = \bar{f} \circ k$. Schließlich folgt aus $f(x) = f(y)$ noch $x \sim y$ und $[x]_\sim = [y]_\sim$, also ist $\bar{f}$ injektiv. Ist f surjektiv, so ist auch $\bar{f}$ surjektiv, also insgesamt bijektiv. ∎

Kapitel 1 Grundbegriffe der Algebra

§ 1 Lineare Gleichungssysteme

Wie wir schon in der Einleitung gesagt haben, stand das Lösen von (linearen) Gleichungen bzw. Systemen von Gleichungen nicht nur am Anfang der historischen Entwicklung der linearen Algeba, sondern es stellt auch gegenwärtig eines der wichtigsten Anwendungsgebiete für diese mathematische Theorie dar. Wir wollen deshalb mit der Betrachtung linearer Gleichungssysteme beginnen und damit die nachfolgenden theoretischen Überlegungen motivieren. Wir betrachten zunächst ein Beispiel.

Beispiel. Ein Betrieb produziere n Nahrungsmittel $N_1,\ldots,N_n$, wozu m Rohstoffe $R_1,\ldots,R_m$ benötigt werden. Zur Herstellung einer Einheit des Nahrungsmittels N_j werden dabei a_{ij} Einheiten des Rohstoffs R_i gebraucht, $i = 1,\ldots,m$, $j = 1,\ldots,n$.

Gesucht ist ein optimaler Produktionsplan, d.h. ein Plan, wieviele Einheiten x_j von N_j produziert werden sollen, wenn insgesamt b_i Einheiten von R_i vorhanden sind und wenn möglichst keine Rohstoffe übrig bleiben sollen. Dies ist natürlich nur eine, auf unsere weiteren Überlegungen zugeschnittene Fragestellung; oft wird man in Kauf nehmen, daß Rohstoffe übrig bleiben, und dafür lieber die Produktionskosten minimieren oder den Gewinn maximieren.

Werden jeweils $x_1,\ldots,x_n$ Einheiten produziert, so benötigt man insgesamt

$$a_{i1}\,x_1 + \cdots + a_{in}\,x_n$$

Einheiten des Rohstoffs R_i. Ein Produktionsplan $(x_1,\ldots,x_n) \in \mathbb{R}^n$, der im obigen Sinne optimal ist, muß also das folgende System von Gleichungen erfüllen:

$$(*) \qquad \begin{array}{ccc} a_{11}\,x_1 + \cdots + a_{1n}\,x_n & = & b_1 \\ \vdots \qquad\qquad\quad \vdots & & \vdots \\ a_{m1}\,x_1 + \cdots + a_{mn}\,x_n & = & b_m \end{array}$$

Hierbei ist $a_{ij} \in \mathbb{R}$ und $b_i \in \mathbb{R}$. (*) ist die allgemeine Form eines *linearen Gleichungssystems* (Kurzschreibweise: LGS) und $x_1,\ldots,x_n$ sind die *Unbekannten* des LGS. Jedes n–Tupel $(x_1,\ldots,x_n) \in \mathbb{R}^n$, das (*) erfüllt, heißt *Lösung* des linearen Gleichungssystems. Alle Lösungen von (*) bilden die *Lösungsmenge.*

Wegen $a_{ij} \in \mathbb{R}$, $b_i \in \mathbb{R}$, $x_j \in \mathbb{R}$ sprechen wir auch von einem *reellen* LGS oder einem LGS über $\mathbb{R}$. In unserem Beispiel war sogar $a_{ij} \geq 0$, $b_i \geq 0$, und nur Lösungen mit $x_j \geq 0$ waren von Interesse. Wir wollen aber solche Vorzeichenbedingungen jetzt außer acht lassen, um die Theorie nicht zu speziell zu machen.

Welche Möglichkeiten ergeben sich für die Lösungsmenge eines linearen Gleichungssystems? Offensichtlich spielt der Fall $(b_1,\ldots,b_m) = (0,\ldots,0)$ eine besondere Rolle, da hier die triviale Lösung $(x_1,\ldots,x_n) = (0,\ldots,0)$ existiert. Ist $(b_1,\ldots,b_m) = (0,\ldots,0)$, so heißt das lineare Gleichungssystem (*) *homogen*, andernfalls *inhomogen* .

Wir geben nun einige Beispiele für des Lösungsverhalten linearer Gleichungs–systeme.

Beispiele. **(a)** Das reelle LGS

$$\begin{aligned} &(1) && x_1 + x_2 + x_3 = 3 \\ &(2) && x_1 - x_2 + 2\,x_3 = 2 \\ &(3) && 2\,x_1 \quad + 3\,x_3 = 1 \end{aligned}$$

ist unlösbar, denn durch Addition der ersten beiden Gleichungen erhalten wir mit $2\,x_1 + 3\,x_3 = 5$ einen Widerspruch zur 3. Gleichung.

(b) Wir betrachten das reelle LGS

$$\begin{aligned} &(1) && x_1 + x_2 + x_3 = 3 \\ &(2) && x_1 - x_2 + 2\,x_3 = 2 \\ &(3) && \quad x_2 + x_3 = 2 \end{aligned}$$

Aus (1), (3) folgt $x_1 = 1$. Aus (1) + (2) erhalten wir $2 + 3\,x_3 = 5$, also $x_3 = 1$. Aus (3) folgt schließlich $x_2 = 1$. Also kann höchstens $(1,1,1)$ Lösung sein. Daß dieses Tripel auch Lösung ist, folgt sofort durch Einsetzen. Hier liegt also eine eindeutige Lösung

vor.

(c) Als drittes Beispiel sei das reelle LGS

$$\begin{aligned} &(1) && x_1 + x_2 + x_3 = 3 \\ &(2) && x_1 - x_2 + 2\,x_3 = 2 \\ &(3) && 2\,x_1 + 3\,x_3 = 5 \end{aligned}$$

gegeben. Wegen (1) + (2) = (3) kann die Gleichung (3) weggelassen werden. Aus (1) und (2) folgen $2\,x_1 = 5 - 3\,x_3$, $2\,x_2 = 1 + x_3$. Also ist jedes Tripel

$$(\tfrac{5}{2} - \tfrac{3}{2}\,a, \tfrac{1}{2} + \tfrac{1}{2}\,a, a)\,, \qquad a \in \mathbb{R}\,,$$

eine Lösung.

Für ein reelles LGS gibt es somit folgende Möglichkeiten: Es ist unlösbar, oder es ist lösbar und besitzt genau eine Lösung, oder es ist lösbar und hat unendlich viele Lösungen.

Ein homogenes LGS ist immer lösbar; hier interessiert man sich dafür, ob nichttriviale Lösungen existieren.

Bei der Betrachtung eines allgemeinen linearen Gleichungssystems (*) ergeben sich nun die folgenden Fragen:

Ist es möglich, einem linearen Gleichungssystem die Lösbarkeit anzusehen? Dazu kann man zunächst eine übersichtliche Schreibweise für (*) einführen, etwa durch Einklammern zusammengehöriger Ausdrücke:

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}$$

Für eine weitere Behandlung müssen dann Rechenoperationen und Rechenregeln für solche Klammern (Matrizen) gefunden werden.

Welche Struktur hat die Lösungsmenge eines linearen Gleichungssystems? Im homogenen Fall sind beispielsweise mit $(x_1,\ldots,x_n)$ und $(y_1,\ldots,y_n)$ auch die n–Tupel

$(x_1 + y_1,\ldots,x_n + y_n)$ sowie $(a\,x_1,\ldots,a\,x_n)$, $a \in \mathbb{R}$, Lösungen. Hier werden Rechenregeln für n–Tupel benötigt.

Es erweist sich nun als vorteilhaft, von der konkreten Situation des LGS (*) abzusehen und Mengen mit Rechenoperationen (Verknüpfungen) zunächst in allgemeinerem Rahmen zu untersuchen. Dabei wird man auch die Menge $\mathbb{R}$ der reellen Zahlen durch eine allgemeinere Menge mit entsprechenden Rechengesetzen (Körper) ersetzen. Dieses Vorgehen, das typisch ist für die Mathematik, erlaubt es, allgemeine Prinzipien und Gesetze zu erkennen, die sich im Spezialfall dann auf die Ausgangsfragestellung (hier: die Behandlung des LGS (*)) anwenden lassen. Der abstrakte Standpunkt der Algebra ist aber auch von den Anwendungen her gerechtfertigt; in der Physik (Schwingungen und Wellen) treten häufig Probleme auf, denen der Zahlkörper der komplexen Zahlen zugrundeliegt, in der Informatik (Codierungstheorie) arbeitet man oft mit endlichen Körpern.

Wir werden im folgenden also Mengen behandeln, auf denen eine oder mehrere Verknüpfungen gegeben sind. Man nennt solche Mengen auch *algebraische Strukturen*. Die wichtigsten algebraischen Strukturen mit einer Verknüpfung sind die Gruppen, sie werden in § 2 untersucht. In § 3 betrachten wir dann algebraische Strukturen mit zwei Verknüpfungen, nämlich Körper und Ringe. Eine umfassende Behandlung all dieser Strukturen ist Aufgabe der Algebra. Hier, im Rahmen der linearen Algebra, müssen wir uns im wesentlichen auf die Definitionen und einige für das spätere Verständnis wichtige Eigenschaften beschränken.

§ 2 Gruppen

Gruppen spielen nicht nur in der Mathematik selbst eine bedeutende Rolle, sondern auch in der Informatik sowie in vielen Naturwissenschaften wie etwa Physik, Chemie, Biologie oder Kristallographie. Dort werden insbesondere die Symmetriegruppen von Kristallen untersucht.

Wir präzisieren zunächst den Begriff Verknüpfung. Darunter verstehen wir eine Vorschrift, mit deren Hilfe wir aus je zwei Elementen einer Menge A ein weiteres Element dieser Menge erhalten, also mathematisch ausgedrückt:

Eine (*innere*) *Verknüpfung* auf der Menge A ist eine Abbildung $f\colon A \times A \longrightarrow A$.

Wir schreiben die Verknüpfungen üblicherweise nicht als Abbildungen f_1 , f_2 , f_3 ,... sondern verwenden Symbole wie $+$, $\cdot$, $\circ$ usw. Statt $f(x,y)$ heißt es dann $x+y$, $x\cdot y$ und $x \circ y$.

Beispiele. **(a)** Addition und Multiplikation auf $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.

(b) Komposition von Abbildungen $g,h : B \longrightarrow B$ einer Menge B in sich, $g \circ h : B \longrightarrow B$.

(c) Auf der Potenzmenge $\mathcal{P}(B)$ einer Menge B sind $\cup$, $\cap$, $\setminus$, Δ Verknüpfungen.

Die meisten dieser Verknüpfungen haben die Eigenschaft assoziativ zu sein, einige sind auch kommutativ. Genauer bedeutet dies:

Eine Verknüpfung $\circ$ auf einer Menge A heißt *assoziativ*, falls für alle x, y, $z \in A$

$$(x \circ y) \circ z = x \circ (y \circ z) \qquad (\text{"Assoziativgesetz"})$$

gilt, und sie heißt *kommutativ*, falls für alle x, $y \in A$ gilt:

$$x \circ y = y \circ x\,. \qquad (\text{"Kommutativgesetz"})$$

Als erste einfache algebraische Strukturen betrachten wir nun Halbgruppen.

Definition. Es seien A eine nichtleere Menge und $\circ$ eine Verknüpfung auf A. Ist diese assoziativ, so heißt $(A,\circ)$ eine *Halbgruppe*. Ist die Verknüpfung außerdem kommutativ, so sprechen wir von einer *kommutativen Halbgruppe*.

In einer Halbgruppe sind Klammern entbehrlich, wir schreiben deshalb z.B. statt $(x \circ y) \circ z$ einfacher $x \circ y \circ z$. Außerdem läßt sich jedes Element x beliebig oft mit sich selbst verknüpfen. Wir verwenden hierfür die abkürzende Potenzschreibweise

$$x^k := \underbrace{x \circ x \circ \cdots \circ x}_{k\text{-mal}}, \quad k \in \mathbb{N}.$$

In vielen Halbgruppen $(A,\circ)$ gibt es ein Element, das vor allen anderen Elementen dadurch ausgezeichnet ist, daß es sich bezüglich der Verknüpfung $\circ$ neutral verhält.

Definition. $e \in A$ heißt *neutrales Element* oder *Neutralelement* der Halbgruppe $(A,\circ)$, falls für alle $x \in A$ gilt: $x \circ e = e \circ x = x$.

In einer Halbgruppe gibt es höchstens ein neutrales Element: Ist nämlich e' ebenfalls ein neutrales Element von $(A,\circ)$, so gilt nach Definition $e \circ e' = e' \circ e = e$ und $e' \circ e = e \circ e' = e'$, also $e = e'$.

In Halbgruppen, in denen ein neutrales Element existiert, können wir auch vom Invertieren eines Elementes reden.

Definition. Es sei $(A,\circ)$ eine Halbgruppe mit Neutralelement e. $x \in A$ heißt *invertierbar*, genau dann wenn ein $x^{-1} \in A$ existiert mit $x \circ x^{-1} = x^{-1} \circ x = e$. x^{-1} heißt dann *inverses Element* oder *Inverses* zu x.

In einer Halbgruppe $(A,\circ)$ mit Neutralelement e gibt es zu jedem $x \in A$ höchstens ein inverses Element: Ist nämlich x' ebenfalls ein inverses Element von x, so gilt nach Definition $x \circ x' = x' \circ x = e$ und $x \circ x^{-1} = x^{-1} \circ x = e$. Also ist $x \circ x^{-1} = x \circ x'$ und somit $x^{-1} \circ (x \circ x^{-1}) = x^{-1} \circ (x \circ x')$. Mit der Assoziativität folgt $e \circ x^{-1} = e \circ x'$, also $x^{-1} = x'$.

Beispiel. Ist $A \neq \emptyset$, so sind $(\mathcal{P}(A),\cup)$ und $(\mathcal{P}(A),\cap)$ kommutative Halbgruppen mit Neutralelement ($\emptyset$ im ersten Fall, A im zweiten), aber es gibt im allgemeinen keine Inversen. Dagegen ist $(\mathcal{P}(A),\Delta)$ eine kommutative Halbgruppe mit dem neutralen

Element $\emptyset$, in der zu jedem $B \in \mathcal{P}(A)$ ein inverses Element existiert, nämlich B selbst.

Besonders wichtige Beispiele von Halbgruppen sind die Gruppen, mit denen wir uns im folgenden eingehender beschäftigen wollen.

Definition. Es seien A eine Menge und $\circ$ eine Verknüpfung auf A. $(A,\circ)$ heißt *Gruppe*, wenn folgende Bedingungen erfüllt sind:

(a) $(A,\circ)$ ist eine Halbgruppe.

(b) $(A,\circ)$ besitzt ein neutrales Element e.

(c) Zu jedem $x \in A$ gibt es ein inverses Element.

Die Gruppe $(A,\circ)$ heißt *kommutativ* oder *abelsch* (nach Nils Henrik Abel, 1802 – 1829), wenn die Halbgruppe $(A,\circ)$ kommutativ ist.

Beim Rechnen in einer Gruppe $(A,\circ)$ schreibt man statt $x \circ y$ oft xy. In abelschen Gruppen wird als Verknüpfungssymbol meist + gewählt. Statt e schreibt man dann 0, statt x^{-1} auch $-x$ und statt $x + (-y)$ kurz $x - y$.

Ist klar, welche Verknüpfung gemeint ist, so redet man oft von der Gruppe A.

Bemerkung. Die Gruppenaxiome (b) und (c) können durch schwächere Axiome ersetzt werden:

(b') $(A,\circ)$ besitzt ein rechtsneutrales Element e, d.h. es gibt ein Element $e \in A$, so daß für alle $x \in A$ gilt: $x \circ e = x$.

(c') Zu jedem $x \in A$ gibt es ein rechtsinverses Element, d.h. es gibt ein $x^{-1} \in A$ mit $x \circ x^{-1} = e$.

Um den Umgang mit den Gruppenaxiomen einzuüben, beweisen wir das folgende Gruppenkriterium.

Satz 1. *Eine Halbgruppe $(A,\circ)$ ist genau dann eine Gruppe, wenn es zu jedem $x \in A$ und zu jedem $y \in A$ Elemente $z, \overline{z} \in A$ gibt mit $x \circ z = y$ und $\overline{z} \circ x = y$.*

Ist dies der Fall, so sind z und $\overline{z}$ eindeutig bestimmt.

Beweis. Sei zunächst $(A,\circ)$ eine Gruppe. Setzen wir $z := x^{-1} \circ y$, so gilt $x \circ z =$

$x \circ (x^{-1} \circ y) = (x \circ x^{-1}) \circ y = e \circ y = y$. Entsprechend ist $\overline{z} := y \circ x^{-1}$ eine Lösung der Gleichung $\overline{z} \circ x = y$.

Ist $(A,\circ)$ eine Halbgruppe, so folgern wir umgekehrt zunächst aus der Lösbarkeit der obigen Gleichungen die Existenz eines Neutralelementes in $(A,\circ)$: Wegen $A \neq \emptyset$ gibt es ein $x_0 \in A$. Nach Voraussetzung existieren dann in A Elemente e und e' mit $x_0 \circ e = x_0$ und $e' \circ x_0 = x_0$. Sei nun $x \in A$ beliebig. Dann gibt es wiederum nach Voraussetzung Elemente $z,\overline{z} \in A$ mit $x_0 \circ z = x$ und $\overline{z} \circ x_0 = x$. Daraus folgt

$$e' \circ x = e' \circ (x_0 \circ z) = (e' \circ x_0) \circ z = x_0 \circ z = x\,,$$

$$x \circ e = (\overline{z} \circ x_0) \circ e = \overline{z} \circ (x_0 \circ e) = \overline{z} \circ x_0 = x\,,$$

also speziell $e = e' \circ e = e'$. Damit ist e Neutralelement von $(A,\circ)$.

Nachweis von Axiom (c): Sei $x \in A$ beliebig. Zu x und e existieren $z \in A$ und $\overline{z} \in A$ mit $x \circ z = e$ und $\overline{z} \circ x = e$. Wegen $z = e \circ z = \overline{z} \circ x \circ z = \overline{z} \circ e = \overline{z}$ ist z inverses Element von x. Damit sind alle Gruppenaxiome nachgewiesen, also ist $(A,\circ)$ eine Gruppe.

Eindeutigkeit: Aus $x \circ z = y$ und $x \circ z' = y$ folgt $x \circ z = x \circ z'$ und daraus $x^{-1} \circ x \circ z = x^{-1} \circ x \circ z'$, also $z = z'$. Die Eindeutigkeit von $\overline{z}$ wird analog bewiesen. ∎

Beispiele. **(a)** $(\mathbb{N},+)$ und $(\mathbb{N}_0,+)$ sind kommutative Halbgruppen, aber keine Gruppen. In $\mathbb{N}$ gibt es kein neutrales Element. In $\mathbb{N}_0$ gibt es zwar ein neutrales Element, nämlich die 0, aber zu keinem $n \neq 0$ ein inverses Element. Dagegen sind $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ abelsche Gruppen mit dem neutralen Element 0.

(b) $(\mathbb{Z},\cdot)$, $(\mathbb{Q},\cdot)$, $(\mathbb{R},\cdot)$ sind kommutative Halbgruppen mit Neutralelement 1, aber keine Gruppen. In $(\mathbb{Z},\cdot)$ gibt es zu keinem $z \neq \pm 1$ ein inverses Element, in $(\mathbb{Q},\cdot)$ und $(\mathbb{R},\cdot)$ hat 0 kein Inverses. Aber $(\mathbb{Q} \setminus \{0\},\cdot)$ und $(\mathbb{R} \setminus \{0\},\cdot)$ sind abelsche Gruppen mit Neutralelement 1.

(c) Die Produktmengen $\mathbb{R}^n$, $\mathbb{Q}^n$, $\mathbb{Z}^n$, $n \in \mathbb{N}$, sind abelsche Gruppen, wenn die Addition + komponentenweise erklärt wird:

$$(x_1,\ldots,x_n) + (y_1,\ldots,y_n) := (x_1 + y_1,\ldots,x_n + y_n).$$

Dann ist $e = (0,\ldots,0)$ und $(x_1,\ldots,x_n)^{-1} = (-x_1,\ldots,-x_n)$.

(d) Ist A endlich, $A = \{a_1,\ldots,a_n\}$, so wird eine Verknüpfung $\circ$ oft durch eine Tabelle angegeben. Wir sprechen dann von einer *Verknüpfungstafel*:

$\circ$	a_1	a_2	$\cdots$	a_n
a_1	$*$	$*$	$\cdots$	$*$
a_2	$*$	$*$	$\cdots$	$*$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
a_n	$*$	$*$	$\cdots$	$*$

Anhand dieser Tabelle läßt sich direkt nachprüfen, ob die Gruppenaxiome erfüllt sind. Ist dies der Fall, so spricht man von einer *Gruppentafel*. Wegen Satz 1 darf dann in jeder Zeile und in jeder Spalte jedes Element von A nur einmal auftreten.

Beispiel. $A = \{0,1\}$ mit der Verknüpfungstafel

$+$	0	1
0	0	1
1	1	0

ist eine Gruppe.

(e) Es sei B eine nichtleere Menge. Die Menge B^B aller Abbildungen $f: B \longrightarrow B$ ist mit der Komposition $\circ$ als Verknüpfung eine Halbgruppe mit neutralem Element, nämlich der identischen Abbildung, aber im allgemeinen keine Gruppe. Für $|B| \geq 2$ hat die "konstante" Abbildung

$$\begin{aligned} f: B &\longrightarrow B \\ x &\longmapsto x_0 \end{aligned} \quad , \quad x_0 \in B \text{ fest},$$

kein Inverses. Ist dagegen f bijektiv, so ist die Umkehrabbildung f^{-1} von f das inverse Element zu f. Also ist

$$S_B := \{f \mid f: B \longrightarrow B \text{ bijektiv}\}$$

eine Gruppe, die im allgemeinen nicht abelsch ist. Sie heißt die *symmetrische Gruppe* von B.

Das letzte Beispiel wollen wir uns noch etwas genauer ansehen, und zwar für endliche Mengen B. Wir beschränken uns auf $B = \{1,\ldots,m\}$ und schreiben für die

symmetrische Gruppe S_B kurz S_m. Die Elemente von S_m heißen *Permutationen* und werden im folgenden meistens mit dem griechischen Buchstaben π bezeichnet.

Es ist üblich, Permutationen in Gestalt einer "Wertetabelle" anzugeben. Wir schreiben deshalb eine Permutation π in der Form

$$\pi = \begin{bmatrix} 1 & \cdots\cdots & m \\ \pi(1) & \cdots\cdots & \pi(m) \end{bmatrix}.$$

Der Name Permutation (= Vertauschung) rührt daher, daß bei einer bijektiven Abbildung $f\colon \{1,...,m\} \longrightarrow \{1,...,m\}$ die Elemente $1,...,m$ umgeordnet werden.

Satz 2. *Für die Anzahl der Elemente der Permutationsgruppe S_m gilt $|S_m| = m!$ (mit $m! := 1 \cdot 2 \cdot 3 \cdots m$).*

Beweis. Wir zeigen sogar etwas mehr: Es seien $A = \{a_1,...,a_m\}$, $B = \{b_1,...,b_m\}$ zwei Mengen mit m Elementen. Dann gilt: $|\{f \mid f\colon A \longrightarrow B \text{ bijektiv}\}| = m!$.

Diese Behauptung wird durch vollständige Induktion über $m \in \mathbb{N}$ bewiesen:
Induktionsanfang: $m = 1$: $A = \{a_1\}$, $B = \{b_1\}$. Hier gibt es genau eine bijektive Abbildung $f\colon A \longrightarrow B$, nämlich $a_1 \longmapsto b_1$.
Induktionsannahme: Die Behauptung sei richtig für $m-1$.
Induktionsschluß von $m-1$ auf m : Wir betrachten alle bijektiven Abbildungen $f\colon A \longrightarrow B$. Es gibt m Möglichkeiten für $f(a_m)$. Für ein festes $b_k \in B$ gibt es nach Induktionsannahme $(m-1)!$ bijektive Abbildungen von $\{a_1,...,a_{m-1}\}$ auf $B \setminus \{b_k\}$, also $(m-1)!$ bijektive Abbildungen $f\colon A \longrightarrow B$ mit $f(a_m) = b_k$. Somit gibt es insgesamt $(m-1)! \cdot m = m!$ bijektive Abbildungen von A auf B. ∎

Beispiel. Die Gruppe S_3 hat $3! = 6$ Elemente:

$$\pi_1 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}.$$

π_1 ist die identische Abbildung id. Wir vertauschen nun die Elemente 1,2,3 zyklisch und erhalten

$$\pi_2 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \quad \pi_3 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}.$$

Die restlichen drei Permutationen lassen jeweils ein Element fest:

$$\pi_4 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \quad \pi_5 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}, \quad \pi_6 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}.$$

Man erhält die folgende Gruppentafel für S_3:

$\circ$	π_1	π_2	π_3	π_4	π_5	π_6
π_1	π_1	π_2	π_3	π_4	π_5	π_6
π_2	π_2	π_3	π_1	π_6	π_4	π_5
π_3	π_3	π_1	π_2	π_5	π_6	π_4
π_4	π_4	π_5	π_6	π_1	π_2	π_3
π_5	π_5	π_6	π_4	π_3	π_1	π_2
π_6	π_6	π_4	π_5	π_2	π_3	π_1

Es ist $\pi_2 \circ \pi_4 = \pi_6$ aber $\pi_4 \circ \pi_2 = \pi_5$, also ist die Gruppe S_3 nicht abelsch.

Die Permutationen π_4, π_5, π_6 sind von besonders einfacher Art. Sie heißen Transpositionen und man sieht, daß sich alle anderen Permutationen aus S_3 durch Verkettung dieser Transpositionen darstellen lassen.

So ist z.B. $\pi_1 = \pi_4 \circ \pi_4$, $\pi_2 = \pi_5 \circ \pi_6$ und $\pi_3 = \pi_5 \circ \pi_4$.

Allgemein nennen wir jede Permutation von $\{1,\ldots,m\}$, welche zwei Elemente i,j mit $i < j$ vertauscht und die restlichen festläßt, eine *Transposition.*
Schreibweise:

$$\tau^{(i,j)} = \begin{bmatrix} 1 & 2 & \cdots & i\text{–}1 & i & i\text{+}1 & \cdots & j\text{–}1 & j & j\text{+}1 & \cdots & m \\ 1 & 2 & \cdots & i\text{–}1 & j & i\text{+}1 & \cdots & j\text{–}1 & i & j\text{+}1 & \cdots & m \end{bmatrix}$$

Bemerkung. Es gilt $\tau^{(i,j)} \circ \tau^{(i,j)} = \mathrm{id}$, d.h. Transpositionen sind selbst–invers.

Satz 3. *Jede Permutation $\pi \in S_m$ $(m \geq 2)$ läßt sich als Verkettung endlich vieler Transpositionen darstellen.*

Beweis. Wir führen den Beweis durch vollständige Induktion nach m. Für $m = 2$ gilt:

$$S_2 = \{\pi_1, \pi_2\} \text{ mit } \pi_1 = \begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix} \text{ und } \pi_2 = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}.$$

$\pi_2 = \tau^{(1,2)}$ ist eine Transposition und π_1 hat die Darstellung $\pi_1 = \pi_2 \circ \pi_2$.
Schluß von $m-1$ auf m: Sei $\pi \in S_m$. Ist $\pi(m) = m$, so ist

$$\tilde{\pi} = \begin{bmatrix} 1 & \cdots\cdots & m-1 \\ \pi(1) & \cdots\cdots & \pi(m-1) \end{bmatrix} \in S_{m-1}.$$

Nach Induktionsannahme existieren Transpositionen $\tilde{\tau}_1,\ldots,\tilde{\tau}_k \in S_{m-1}$ mit $\tilde{\pi} = \tilde{\tau}_1 \circ \cdots \circ \tilde{\tau}_k$. Jede Transposition $\tilde{\tau}_j \in S_{m-1}$ geht aber in eine Transposition $\tau_j \in S_m$ über, wenn wir

$$\tau_j(i) = \begin{cases} \tilde{\tau}_j(i) & \text{für } i = 1,\ldots,m-1 \\ m & \text{für } i = m \end{cases}$$

setzen. Damit erhalten wir $\pi = \tau_1 \circ \cdots \circ \tau_k$.

Ist $\pi(m) = n \neq m$, so ist $\tau^{(n,m)} \circ \pi = \pi'$ eine Permutation aus S_m, die m festläßt. Wegen $\pi = \tau^{(n,m)} \circ \pi'$ folgt mit dem zuvor bewiesenen Teil auch in diesem Fall die Behauptung. ∎

Beispiel. Für

$$\pi = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 2 & 6 & 4 & 1 \end{bmatrix} \in S_6$$

gilt

$$\pi = \tau^{(1,4)} \circ \tau^{(4,6)} \circ \tau^{(2,3)} \circ \tau^{(1,5)}.$$

Bemerkung und Definition. Die Darstellung $\pi = \tau_1 \circ \cdots \circ \tau_k$ ist nicht eindeutig, so gilt etwa in dem vorangehenden Beispiel auch

$$\pi = \tau^{(1,6)} \circ \tau^{(4,5)} \circ \tau^{(1,4)} \circ \tau^{(2,3)}.$$

Wir werden aber später (S. 164) sehen, daß bei verschiedenen solchen Darstellungen die Anzahl der auftretenden Transpositionen entweder immer gerade oder immer ungerade ist.

Man nennt deshalb eine Permutation π *gerade*, wenn es eine Darstellung mit einer geraden Anzahl von Transpositionen gibt, andernfalls heißt π *ungerade*.

Die Verkettung gerader Permutationen ergibt wieder eine gerade Permu-

tation. Da das inverse Element einer Transposition $\tau^{(i,j)}$ wieder eine Transposition ist (nämlich $\tau^{(i,j)}$ selbst), ist auch die inverse Permutation einer geraden Permutation wieder gerade. Das führt uns auf den Begriff der Untergruppe.

Definition. Es seien $(A,\circ)$ eine Gruppe und $B \subset A$. Genau dann heißt B eine *Untergruppe* von A, falls die auf $B \times B$ eingeschränkte Abbildung $\circ$ eine Verknüpfung ist und $(B,\circ)$ eine Gruppe.

Ist B eine Untergruppe von A, so sind die Neutralelemente e_B von B und e_A von A gleich. Es gilt nämlich $e_B = e_B \circ e_B = e_A \circ e_B$, woraus nach Satz 1 $e_B = e_A$ folgt. Damit ist notwendigerweise für jedes $x \in B$ das inverse Element bezüglich $\circ$ in B gleich dem Inversen bezüglich $\circ$ in A.

Diese Eigenschaften genügen nun auch, um nachzuweisen, daß eine Teilmenge $B \subset A$ eine Untergruppe von A ist.

Satz 4. *Es seien $(A,\circ)$ eine Gruppe und $B \subset A$. Dann ist B genau dann Untergruppe von A, wenn B das Neutralelement von A enthält und mit x und y stets auch x^{-1} und $x \circ y$ zu B gehören.*

Beweis. Wir müssen nur noch die eine Richtung der Behauptung zeigen. Die Abbildung $\circ : (x,y) \mapsto x \circ y$, eingeschränkt auf $B \times B$, bildet nach Voraussetzung $B \times B$ in B ab, ist also eine Verknüpfung auf B. Sie ist in B assoziativ, weil sie schon in A assoziativ ist. Also ist $(B,\circ)$ eine Halbgruppe und wegen der übrigen Voraussetzungen sogar eine Gruppe. Somit ist B Untergruppe von A. ∎

Bemerkung. Das Untergruppenkriterium wird oft auch in der folgenden, leicht abgewandelten Fassung benutzt, die jedoch zu Satz 4 äquivalent ist:

Es seien $(A,\circ)$ eine Gruppe und $B \subset A$. Dann ist B genau dann Untergruppe von A, wenn $B \neq \emptyset$ ist und mit x und y stets auch $x \circ y^{-1}$ zu B gehört.

Beweis. Wegen $B \neq \emptyset$ gibt es zunächst ein $x_0 \in B$. Also folgt $e = x_0 \circ x_0^{-1} \in B$. Mit

jedem $x \in B$ ist dann auch $x^{-1} = e \circ x^{-1} \in B$. Somit folgt aus $x, y \in B$ auch $x, y^{-1} \in B$ und damit nach Voraussetzung $x \circ y = x \circ (y^{-1})^{-1} \in B$. Nach Satz 4 ist dann B eine Untergruppe von A. Die umgekehrte Richtung ist offensichtlich. ∎

Beispiel. Die geraden Permutationen aus der Gruppe S_m bilden eine Untergruppe von S_m, die ungeraden dagegen nicht.

Wie immer im folgenden, wenn wir Mengen mit Strukturen betrachten, sind auch die Abbildungen von Interesse, die die Struktur erhalten. Sie heißen Homomorphismen.

Definition. Es seien $(A,\circ)$ und $(A',*)$ Gruppen und $f: A \longrightarrow A'$ eine Abbildung. f heißt (*Gruppen–*) *Homomorphismus*, wenn für alle $x,y \in A$ gilt: $f(x \circ y) = f(x) * f(y)$. Ein bijektiver Homomorphismus heißt *Isomorphismus*. Gibt es einen Isomorphismus $f: A \longrightarrow A'$, so heißen die Gruppen $(A,\circ)$ und $(A',*)$ *isomorph*, und wir schreiben dann $(A,\circ) \cong (A',*)$. Ist außerdem $A = A'$ und $\circ = *$, so heißt f *Automorphismus* von A.

Bemerkung. Jede Gruppe A ist isomorph zu einer geeigneten Untergruppe von S_A.

Bemerkungen. **(a)** Ein Gruppenhomomorphismus $f: A \longrightarrow A'$ besitzt folgende einfache Eigenschaften:

$f(e) = e'$, e' neutrales Element von A'.

$(f(x))^{-1} = f(x^{-1})$, $x \in A$.

(b) Zu jedem Homomorphismus $f: A \longrightarrow A'$ gehören in natürlicher Weise zwei Untergruppen:

$f(A) = \{f(x) \mid x \in A\}$ ist Untergruppe von A'.

Kern $f := \{x \in A \mid f(x) = e'\}$ ist Untergruppe von A.

(c) Der Homomorphismus f ist genau dann surjektiv, wenn $f(A) = A'$ und genau dann injektiv, wenn Kern $f = \{e\}$.

Wir beweisen nur den zweiten Teil von (b) und (c) und überlassen die restlichen Behauptungen als Übungsaufgaben:

(b) Es ist Kern $f \neq \emptyset$, da $e \in$ Kern f. Aus $x,y \in$ Kern f folgt $f(x \circ y^{-1}) = f(x) * f(y^{-1})$ $= e' * (f(y))^{-1} = (f(y))^{-1} = e'^{-1} = e'$, d.h. $x \circ y^{-1} \in$ Kern f. ∎

(c) Es sei f injektiv. Aus $x \in$ Kern f folgt $f(x) = e'$. Da auch $f(e) = e'$ gilt, erhalten wir $f(x) = f(e)$ und daraus $x = e$.

Ist umgekehrt Kern $f = \{e\}$, so folgt aus $f(x) = f(y)$ zunächst $f(x) * f(y)^{-1} = e'$ und daraus $f(x \circ y^{-1}) = e'$. Also gilt $x \circ y^{-1} \in$ Kern f, $x \circ y^{-1} = e$ und somit $x = y$. ∎

Die Untergruppe Kern f hat nun eine wichtige Eigenschaft. Es gilt nämlich für alle $x \in A$ und alle $y \in$ Kern f

$$(*) \qquad x \circ y \circ x^{-1} \in \text{Kern } f,$$

denn es ist $f(x \circ y \circ x^{-1}) = f(x) * e' * f(x)^{-1} = e'$.

Also ist Kern f invariant unter allen Abbildungen der Form

$$\begin{aligned} A &\longrightarrow A \\ y &\longmapsto x \circ y \circ x^{-1} \end{aligned} \quad , \; x \in A.$$

Diese Abbildungen sind, wie man leicht nachprüft, Automorphismen von A. Sie heißen *innere Automorphismen* von A. Die Eigenschaft (*) bedeutet somit, daß jeder innere Automorphismus von A die Untergruppe Kern f in sich abbildet, also *invariant* läßt. Wir nennen dies die Normalteilereigenschaft von Kern f.

Allgemein definieren wir:

Definition. Eine Untergruppe B einer Gruppe $(A,\circ)$ heißt *Normalteiler* von A, wenn für alle $x \in A$ und alle $y \in B$ stets $x \circ y \circ x^{-1} \in B$ gilt.

Beispiele. **(a)** A und $\{e\}$ sind triviale Normalteiler von A.

(b) Der Kern eines Homomorphismus ist Normalteiler.

(c) Jede Untergruppe einer abelschen Gruppe ist Normalteiler.

Satz 5. *Es seien $(A,\circ)$ eine Gruppe und B eine Untergruppe von A. Dann sind folgende Aussagen äquivalent:*

(a) *B ist Normalteiler.*

(b) *Für alle* $x \in A$ *gilt* $x \circ B \circ x^{-1} = B$.

(c) *Für alle* $x \in A$ *gilt* $x \circ B = B \circ x$.

(d) *Für alle* $x,x' \in A$ *und alle* $y,y' \in A$ *gilt: Aus* $x' \circ x^{-1} \in B$ *und* $y' \circ y^{-1} \in B$ *folgt stets* $x' \circ y' \circ y^{-1} \circ x^{-1} \in B$.

Hierbei ist $x \circ B \circ x^{-1} := \{x \circ b \circ x^{-1} \mid b \in B\}$, $x \circ B := \{x \circ b \mid b \in B\}$ und $B \circ x := \{b \circ x \mid b \in B\}$.

Beweis. (a) $\Longrightarrow$ (b): Wegen der Normalteilereigenschaft von B gilt offensichtlich $x \circ B \circ x^{-1} \subset B$. Sei nun $y \in B$. Dann ist $x^{-1} \circ y \circ (x^{-1})^{-1} \in B$ und somit

$$y = x \circ (x^{-1} \circ y \circ x) \circ x^{-1} \in x \circ B \circ x^{-1},$$

also $B \subset x \circ B \circ x^{-1}$.

(b) $\Longrightarrow$ (c): trivial

(c) $\Longrightarrow$ (a): trivial

(a) $\Longrightarrow$ (d): Mit $x' \circ x^{-1} \in B$ ist wegen der Normalteilereigenschaft von B auch $x^{-1} \circ x' = x'^{-1} \circ (x' \circ x^{-1}) \circ x' \in B$. Damit folgt aus $x' \circ x^{-1} \in B$ und $y' \circ y^{-1} \in B$ auch $x^{-1} \circ x' \circ y' \circ y^{-1} \in B$, woraus sich wieder wegen der Voraussetzung, daß B Normalteiler ist, die Behauptung

$$x' \circ y' \circ y^{-1} \circ x^{-1} = x \circ (x^{-1} \circ x' \circ y' \circ y^{-1}) \circ x^{-1} \in B$$

ergibt.

(d) $\Longrightarrow$ (a): Aus $x \in A$, $y \in B$ folgt für $x' = x$ und $y' = y \circ y$ zunächst

$$x' \circ x^{-1} = e \in B \text{ und } y' \circ y^{-1} = y \in B.$$

Damit sind die Voraussetzungen von (d) erfüllt, wir erhalten $x' \circ y' \circ y^{-1} \circ x^{-1} \in B$, d.h. $x \circ y \circ x^{-1} \in B$. ∎

Jede Untergruppe B einer Gruppe $(A,\circ)$ definiert auf dieser eine Äquivalenzrelation:

$$x \sim y :\Longleftrightarrow x \circ y^{-1} \in B \ , \ x,y \in A.$$

Zum Nachweis prüfen wir die drei definierenden Eigenschaften einer Äquiva-

lenzrelation nach.

Reflexivität: Für alle $x \in A$ gilt $x \sim x$, da $x \circ x^{-1} = e \in B$.

Symmetrie: Für alle $x,y \in A$ folgt aus $x \sim y$ stets $y \sim x$, da mit $x \circ y^{-1} \in B$ auch $y \circ x^{-1} = (x \circ y^{-1})^{-1} \in B$ gilt.

Transitivität: Für alle $x,y,z \in A$ folgt aus $x \sim y$, $y \sim z$ stets $x \sim z$, da mit $x \circ y^{-1} \in B$, $y \circ z^{-1} \in B$ auch $x \circ z^{-1} = (x \circ y^{-1}) \circ (y \circ z^{-1}) \in B$ gilt. ∎

Für die Faktormenge $A/_{\sim}$ schreiben wir, um den Zusammenhang von $\sim$ mit B zu betonen, auch $A/_B$.

Wir versuchen nun, diese Menge durch Definition einer geeigneten Verknüpfung $\cdot$, die mit der Verknüpfung $\circ$ von A zusammenhängen soll, zu einer Gruppe zu machen. Naheliegend ist der Ansatz

$$[x]_{\sim} \cdot [y]_{\sim} = [x \circ y]_{\sim} \quad , \; x,y \in A.$$

Dies ist aber nur dann eine sinnvolle Definition, wenn sie repräsentantenunabhängig ist, d.h. wenn für $x' \in [x]_{\sim}$, $y' \in [y]_{\sim}$ auch $x' \circ y' \in [x \circ y]_{\sim}$ gilt. Nach der Definition von $\sim$ bedeutet dies, daß aus $x' \circ x^{-1} \in B$, $y' \circ y^{-1} \in B$ stets $x' \circ y' \circ y^{-1} \circ x^{-1} \in B$ folgt, also nach Satz 5, daß B ein Normalteiler von A ist.

In der Gruppentheorie sind tatsächlich nur solche Faktormengen $A/_B$ von Interesse, bei denen B ein Normalteiler ist. Für diese Mengen gilt

Satz 6 und Definition. *Es seien $(A,\circ)$ eine Gruppe und $B \subset A$ ein Normalteiler. Dann ist die Faktormenge $A/_B$ zusammen mit der induzierten Verknüpfung $\cdot$*

$$[x]_{\sim} \cdot [y]_{\sim} = [x \circ y]_{\sim} \quad , \; x,y \in A,$$

eine Gruppe. $(A/_B, \cdot)$ heißt Quotienten– oder Faktorgruppe.

Beweis. Wir prüfen die Gruppeneigenschaften nach:

(a) Für alle $[x]_{\sim}$, $[y]_{\sim}$, $[z]_{\sim} \in A/_B$ gilt $([x]_{\sim} \cdot [y]_{\sim}) \cdot [z]_{\sim} = [x \circ y]_{\sim} \cdot [z]_{\sim} = [(x \circ y) \circ z]_{\sim} = [x \circ (y \circ z)]_{\sim} = [x]_{\sim} \cdot [y \circ z]_{\sim} = [x]_{\sim} \cdot ([y]_{\sim} \cdot [z]_{\sim})$.

(b) Neutrales Element von $A/_B$ ist $[e]_\sim$, weil $[e]_\sim \cdot [x]_\sim = [e \circ x]_\sim = [x]_\sim = [x \circ e]_\sim = [x]_\sim \cdot [e]_\sim$ für alle $[x]_\sim \in A/_B$ gilt. Weiterhin ist $[x^{-1}]_\sim$ inverses Element zu $[x]_\sim$, da $[x]_\sim \cdot [x^{-1}]_\sim = [x \circ x^{-1}]_\sim = [e]_\sim$ und $[x^{-1}]_\sim \cdot [x]_\sim = [e]_\sim$ gelten. ∎

Spezielle Normalteiler sind die Kerne von Gruppenhomomorphismen. Für die Faktorgruppen nach solchen Kernen ist der folgende Satz von besonderer Wichtigkeit.

Satz 7 (Homomorphiesatz für Gruppen). *Es seien $(A,\circ)$ und $(A',*)$ Gruppen sowie $f: A \longrightarrow A'$ ein Homomorphismus. Dann gilt:*

(a) $A/_{\text{Kern } f}$ *ist eine Faktorgruppe und die kanonische Abbildung*

$$k : A \longrightarrow A/_{\text{Kern } f}$$
$$x \longmapsto [x]_\sim$$

ist ein Homomorphismus.

(b) *Es gibt einen injektiven Homomorphismus $\bar{f} : A/_{\text{Kern } f} \longrightarrow A'$ mit $f = \bar{f} \circ k$.*

(c) *Ist f surjektiv, so sind $A/_{\text{Kern } f}$ und A' isomorph.*

Beweis. Die Behauptung (a) ist schon bewiesen. Bei (b) und (c) müssen wir wegen Satz 7 aus den Vorbemerkungen nur noch zeigen, daß die durch $\bar{f}([x]_\sim) := f(x)$ definierte Abbildung $\bar{f}$ ein Homomorphismus ist, was aber wegen

$$\bar{f}([x]_\sim \cdot [y]_\sim) = \bar{f}([x \circ y]_\sim) = f(x \circ y) = f(x) * f(y) = \bar{f}([x]_\sim) * \bar{f}([y]_\sim)$$

der Fall ist. ∎

Korollar 8. *Es gilt* $A/_{\text{Kern } f} \cong f(A)$.

§ 3 Körper und Ringe

Während der Gruppenbegriff sich auf nur eine Verknüpfung bezog, werden wir nun Mengen mit zwei Verknüpfungen betrachten und diese in Anlehnung an das übliche Zahlenrechnen mit + und · bezeichnen und Addition bzw. Multiplikation nennen. Neutralelemente werden mit 0 (bezüglich +) und 1 (bezüglich ·) bezeichnet und Inverse mit $-x$ (bezüglich +) sowie $x^{-1} = \frac{1}{x}$ (bezüglich ·).

Definition. Eine Menge A mit zwei Verknüpfungen + und · heißt *Körper*, wenn folgende Bedingungen erfüllt sind:

(a) $(A,+)$ ist eine abelsche Gruppe,

(b) $(A \setminus \{0\},\cdot)$ ist eine abelsche Gruppe,

(c) für alle $x,y,z \in A$ gilt: $x\cdot(y+z) = x\cdot y + x\cdot z$, $(x+y)\cdot z = x\cdot z + y\cdot z$. (*"Distributivgesetze"*)

Bemerkungen. **(a)** Es ist eine gängige Verabredung, statt $x\cdot y$ auch xy und statt $(x\cdot y) + z$ auch $xy + z$ zu schreiben. Letzteres bedeutet, daß die Multiplikation stärker binden soll als die Addition. Diese Konvention wurde schon bei der Formulierung der Distributivgesetze (c) benutzt. Außerdem schreiben wir statt xy^{-1} auch $\frac{x}{y}$.

(b) Das Axiom (c) läßt sich nicht aus den ersten beiden Axiomen folgern. Dies zeigt folgendes Beispiel:

Auf der Menge $A = \{0,1\}$ definieren wir Addition + und Multiplikation · durch die Verknüpfungstafeln

+	0	1
0	0	1
1	1	0

·	0	1
0	1	0
1	0	1

Dann sind $(A,+)$ und $(A \setminus \{0\},\cdot)$ abelsche Gruppen, aber es gilt keines der beiden Distributivgesetze.

(c) Ein Körper besitzt mindestens zwei Elemente, nämlich 0 und 1.

(d) Für alle $x \in A$ gilt $x\cdot 0 = 0\cdot x = 0$.

Aus $x\cdot x = x(x+0) = x\cdot x + x\cdot 0$ folgt nämlich $x\cdot 0 = 0$ und aus $x\cdot x = (x+0)x = x\cdot x + 0\cdot x$ folgt $0\cdot x = 0$. ∎

(e) Für alle $x,y \in A$ gilt $x(-y) = (-x)y = -(xy)$.
Aus $xy + x(-y) = x(y-y) = x\cdot 0 = 0$ folgt nämlich $x(-y) = -(xy)$ und aus $xy + (-x)y = (x-x)y = 0\cdot y = 0$ folgt $(-x)y = -(xy)$. ∎

(f) Bezüglich der Multiplikation gelten das Assoziativgesetz, die Neutraleigenschaft der 1 und das Kommutativgesetz zunächst nur für Elemente, die von 0 verschieden sind. Wegen (d) gelten diese Eigenschaften aber uneingeschränkt.

(g) In einem Körper folgt aus $xy = 0$ stets $x = 0$ oder $y = 0$, denn $A \setminus \{0\}$ ist bezüglich der Multiplikation abgeschlossen, d.h. aus $x \neq 0$ und $y \neq 0$ folgt $xy \neq 0$. Man sagt auch, ein Körper sei *nullteilerfrei*.

Beispiele. **(a)** $(\mathbb{Z},+,\cdot)$ ist kein Körper, da es in $(\mathbb{Z} \setminus \{0\},\cdot)$ zu $z \neq \pm 1$ kein inverses Element gibt. Dagegen sind $\mathbb{Q}$ und $\mathbb{R}$ Körper.

(b) $A = \{x + \sqrt{2}\, y \mid x,y \in \mathbb{Q}\}$ ist bezüglich der Addition und Multiplikation reeller Zahlen ein Körper, der echt zwischen $\mathbb{Q}$ und $\mathbb{R}$ liegt (Übungsaufgabe).

(c) $A = \{0,1\}$ ist mit den durch die folgenden Verknüpfungstafeln gegebenen Verknüpfungen

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

ein Körper und zwar der "kleinste" Körper.

Weitere endliche Körper sind die sogenannten *Restklassenkörper*:

Es sei m eine feste natürliche Zahl. Wir definieren auf $\mathbb{Z}$ eine Relation $\sim$ durch

$$x \sim y :\Longleftrightarrow x - y \in m\cdot\mathbb{Z} := \{mz \mid z \in \mathbb{Z}\}.$$

Es ist leicht nachzuprüfen, daß $\sim$ eine Äquivalenzrelation ist und daß x und y genau dann äquivalent sind, wenn sie bei der Division durch m den gleichen Rest $r \in \{0,...,m-1\}$ besitzen. Die Äquivalenzklassen bezüglich $\sim$ heißen deshalb auch *Restklassen.*

Für die Menge $\mathbb{Z}/_{\sim}$ der Äquivalenzklassen schreiben wir $\mathbb{Z}_m$. Da es zu jedem $x \in \mathbb{Z}$ ein $z \in \mathbb{Z}$ und ein $r \in \{0,...,m-1\}$ gibt mit $x = mz + r$, ist $[x]_\sim = [r]_\sim$ und daher $\mathbb{Z}_m = \{[0]_\sim, ..., [m-1]_\sim\}$.

Wir wollen $\mathbb{Z}_m$ nun mit einer Addition und einer Multiplikation versehen. Dazu definieren wir

$$[x]_\sim + [y]_\sim := [x+y]_\sim$$

und

$$[x]_\sim \cdot [y]_\sim := [xy]_\sim .$$

Zunächst müssen wir die Wohldefiniertheit dieser Verknüpfungen nachprüfen, d.h. mit $x' \in [x]_\sim$, $y' \in [y]_\sim$ muß auch $x'+y' \in [x+y]_\sim$ und $x'y' \in [xy]_\sim$ gelten:
Aus $x' - x = mz$, $y' - y = mz'$ folgen $(x'+y') - (x+y) = m(z+z')$ und $x'y' - xy = m(zy + z'x + mzz')$. ∎

Die meisten Rechenregeln übertragen sich nun sofort von $\mathbb{Z}$ auf $\mathbb{Z}_m$. Es folgt, daß $(\mathbb{Z}_m, +)$ eine abelsche Gruppe ist mit dem neutralen Element $[0]_\sim$, daß in $(\mathbb{Z}_m, \cdot)$ Assoziativgesetz und Kommutativgesetz gelten, daß $[1]_\sim$ neutrales Element der Multiplikation ist und daß die Distributivgesetze gelten. Trotzdem ist für gewisse m $(\mathbb{Z}_m \setminus \{[0]_\sim\}, \cdot)$ keine abelsche Gruppe und damit $\mathbb{Z}_m$ kein Körper.

In $\mathbb{Z}_1$ zum Beispiel gilt wegen $1 - 0 \in 1 \cdot \mathbb{Z}$, daß $[0]_\sim = [1]_\sim$, also ist $\mathbb{Z}_1 \setminus \{[0]_\sim\} = \emptyset$. In $\mathbb{Z}_4$ gilt wegen $4 - 0 \in 4 \cdot \mathbb{Z}$, daß $[2]_\sim \cdot [2]_\sim = [0]_\sim$, also ist die Multiplikation auf $\mathbb{Z}_4 \setminus \{[0]_\sim\}$ keine Verknüpfung.

Das letzte Beispiel läßt sich verallgemeinern: Ist nämlich $m \geq 2$ keine Primzahl, so gibt es natürliche Zahlen $p,q \in \{2,...,m-1\}$ mit $m = p \cdot q$. Dann ist $[p]_\sim \neq [0]_\sim$, $[q]_\sim \neq [0]_\sim$, aber $[p]_\sim \cdot [q]_\sim = [p \cdot q]_\sim = [m]_\sim = [0]_\sim$, ein Wider-

spruch zur Nullteilerfreiheit in einem Körper, also kann $\mathbb{Z}_m$ dann kein Körper sein.

Bevor wir jedoch die Frage beantworten, für welche $m \in \mathbb{N}$ wir einen Körper erhalten, wollen wir einige Beispiele für das Rechnen in $\mathbb{Z}_m$ geben.

Beispiele. **(a)** $\mathbb{Z}_2$ hat genau zwei Elemente, nämlich $[0]_\sim = \{0 + 2z |\ z \in \mathbb{Z}\}$ und $[1]_\sim = \{1 + 2z |\ z \in \mathbb{Z}\}$.
$\mathbb{Z}_9 = \{[0]_\sim , [1]_\sim ,\ldots,[8]_\sim\}$ mit $[0]_\sim = \{9z |\ z \in \mathbb{Z}\}$, $[1]_\sim = \{1 + 9z |\ z \in \mathbb{Z}\}$, $[2]_\sim = \{2 + 9z |\ z \in \mathbb{Z}\}$, ... , $[8]_\sim = \{8 + 9z |\ z \in \mathbb{Z}\}$.

(b) Was ist $[137]_\sim$ in $\mathbb{Z}_{15}$? Wegen $137 = 9 \cdot 15 + 2$ ist $137 \sim 2$, d.h. $[137]_\sim = [2]_\sim$.
Was ist $[-79]_\sim$ in $\mathbb{Z}_8$? Wegen $-79 = (-10) \cdot 8 + 1$ ist $[-79]_\sim = [1]_\sim$.

Satz 9. *Genau dann ist $\mathbb{Z}_m$, $m \in \mathbb{N}$, ein Körper, wenn m eine Primzahl ist.*

Beweis. Ist $\mathbb{Z}_m$ ein Körper, so muß nach dem oben gesagten m eine Primzahl sein.

Sei jetzt m eine Primzahl. Wir müssen nur noch zeigen, daß die Multiplikation eine Verknüpfung auf $\mathbb{Z}_m \setminus \{[0]_\sim\}$ ist und daß jedes Element $[x]_\sim \neq [0]_\sim$ in $(\mathbb{Z}_m \setminus \{[0]_\sim\}, \cdot)$ ein inverses Element besitzt. Dazu beweisen wir zunächst, daß für alle $[x]_\sim , [y]_\sim , [z]_\sim \in \mathbb{Z}_m$ mit $[x]_\sim \neq [0]_\sim$ aus $[x]_\sim \cdot [y]_\sim = [x]_\sim \cdot [z]_\sim$ stets $[y]_\sim = [z]_\sim$ folgt:

$[x]_\sim \cdot [y]_\sim = [x]_\sim \cdot [z]_\sim$ ist äquivalent zu $[xy - xz]_\sim = [0]_\sim$. Somit gilt $x(y - z) = km$, $k \in \mathbb{Z}$. Wegen $[x]_\sim \neq [0]_\sim$ ist m kein Teiler von x. Da m jedoch das Produkt $x(y - z)$ teilt, muß m Teiler von $y - z$ sein, woraus sich $[y - z]_\sim = [0]_\sim$ und $[y]_\sim = [z]_\sim$ ergeben.

Aus $[x]_\sim \neq [0]_\sim$, $[y]_\sim \neq [0]_\sim$ folgt nun $[x]_\sim \cdot [y]_\sim \neq [0]_\sim$. Damit ist $\cdot$ eine Verknüpfung auf $\mathbb{Z}_m \setminus \{[0]_\sim\}$. Außerdem sind für $[x]_\sim \neq [0]_\sim$ die Produkte $[x]_\sim \cdot [1]_\sim$, $[x]_\sim \cdot [2]_\sim$,...,$[x]_\sim \cdot [m-1]_\sim$ paarweise verschieden; eines von ihnen muß daher gleich $[1]_\sim$ sein. Also besitzt jedes Element $[x]_\sim \in \mathbb{Z}_m \setminus \{[0]_\sim\}$ ein inverses Element bezüglich der Multiplikation. ∎

Bemerkung. Um die Abhängigkeit der Äquivalenzrelation $\sim$ von der festgewählten Zahl $m \in \mathbb{N}$ deutlich zu machen, schreibt man statt $x \sim y$ auch $x \equiv y \bmod m$ und

sagt, *x ist kongruent y modulo m* .

Beispiel. Wir suchen alle ganzen Zahlen x, für die $5 \equiv x \bmod 12$ gilt:

Das Rechnen mit Kongruenzen ergibt $x - 5 \equiv 0 \bmod 12$, $x - 5 = k \cdot 12$, $k \in \mathbb{Z}$, und somit $x = 5 + k \cdot 12$, $k \in \mathbb{Z}$.

Die Rechnung in $\mathbb{Z}_{12}$ ergibt $[5]_{\sim} = [x]_{\sim}$, $[x-5]_{\sim} = [0]_{\sim}$, also $x - 5 = k \cdot 12$, $k \in \mathbb{Z}$, und somit ebenfalls $x = 5 + k \cdot 12$, $k \in \mathbb{Z}$.

Das Rechnen mit Kongruenzen und insbesondere das Lösen von Systemen von Kongruenzgleichungen gehört in den Bereich der Zahlentheorie, spielt aber auch in der Informatik eine wichtige Rolle. Wir werden deshalb in Paragraph 1.6 einige Aussagen über Kongruenzen, wie etwa den Chinesischen Restsatz, herleiten.

Wie bei den Gruppen sollen nun auch bei den Körpern die strukturerhaltenden Abbildungen eingeführt werden.

Definition. Es seien $(A,+,\cdot)$ und $(A',+',\cdot')$ Körper und $f\colon A \longrightarrow A'$ eine Abbildung mit den Eigenschaften

$$f(x+y) = f(x) +' f(y) \ , \ x,y \in A \ ,$$

$$f(x \cdot y) = f(x) \cdot' f(y) \ , \ x,y \in A$$

und

$$f(1) = 1 \ .$$

Dann heißt f *(Körper–) Homomorphismus.* Ist f bijektiv, so heißt f *Isomorphismus* und die Körper A und A' heißen *isomorph* ; wir schreiben dann $A \cong A'$.

Bemerkungen und Bezeichnungen. **(a)** Es hat sich in der Algebra eingebürgert, für endliche Körper mit q Elementen, $q \in \mathbb{N}$, die Bezeichnungen $\mathbb{F}_q$ (für "field") oder $GF(q)$ (für "Galoisfeld" nach Evariste Galois, 1811 – 1832) zu verwenden. Es läßt sich zeigen, daß genau für die Primzahlpotenzen $q = p^n$, p Primzahl, $n \in \mathbb{N}$, solche endlichen Körper existieren und daß je zwei Körper mit q Elementen isomorph sind. Für $q = p$ sind daher alle Körper mit p Elementen zu $\mathbb{Z}_p$ isomorph, insbesondere auch der Körper $\mathbb{F}_p = \{0,\ldots,p-1\}$ mit den von $\mathbb{Z}_p$ induzierten Verknüpfungen. Der kleinste Körper ist $\mathbb{F}_2 = \{0,1\}$ aus Beispiel (c).

(b) In $\mathbb{F}_p$ gilt

$$\underbrace{1 + \cdots + 1}_{p \text{ Summanden}} = 0$$

und p ist die kleinste natürliche Zahl mit dieser Eigenschaft. Man nennt p die *Charakteristik* des Körpers $\mathbb{F}_p$.

Analog nennt man bei einem beliebigen Körper $\mathbb{K}$, sofern ein derartiges p existiert, diese Zahl die *Charakteristik* von $\mathbb{K}$. Gilt jedoch in $\mathbb{K}$ für alle $m \in \mathbb{N}$

$$\underbrace{1 + \cdots + 1}_{m \text{ Summanden}} \neq 0 ,$$

so sagt man, der Körper $\mathbb{K}$ habe die *Charakteristik* 0.

So sind zum Beispiel $\mathbb{Q}$ und $\mathbb{R}$ Körper der Charakteristik 0. Die Charakteristik eines Körpers ist entweder 0 oder eine Primzahl. (Übungsaufgabe).

(c) Da wir im folgenden meist einen beliebigen Körper zugrundelegen, wollen wir für Körper – so wie wir es schon in (b) getan haben – in Zukunft das Symbol $\mathbb{K}$ benutzen (analog zu $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{F}_p$). Für die Charakteristik schreiben wir dann char $\mathbb{K}$.

Wir wollen die Körpertheorie nicht weiter ausbauen, sondern uns hier damit begnügen, noch ein weiteres Beispiel für einen Körper kennenzulernen, nämlich den Körper $\mathbb{C}$ der komplexen Zahlen, der für die lineare Algebra besonders wichtig ist.

Komplexe Zahlen

Ausgangspunkt unserer Betrachtungen ist die abelsche Gruppe $(\mathbb{R}^2,+)$. Auf der Menge $\mathbb{R}^2$ werden wir eine Multiplikation "$\cdot$" so definieren, daß $(\mathbb{R}^2,+,\cdot)$ ein Körper ist.

Definition. Für alle $(a,b), (c,d) \in \mathbb{R}^2$ sei

$$(a,b)\cdot(c,d) := (ac - bd, ad + bc)$$

Diese Multiplikation ist offensichtlich kommutativ. Sie ist auch assoziativ:

$$\begin{aligned}[(a,b)\cdot(c,d)]\cdot(e,f) &= (ac - bd, ad + bc)\cdot(e,f) \\ &= (eac - ebd - adf - bcf,\ acf - bdf + ade + bce) ,\end{aligned}$$

$$(a,b)\cdot[(c,d)\cdot(e,f)] = (a,b)\cdot(ce - df, cf + de)$$
$$= (ace - adf - bcf - bde\ ,\ acf + ade + bce - bdf)\ .$$

Es gelten die Distributivgesetze. Wegen der Kommutativität der Multiplikation auf $\mathbb{R}^2$ genügt es, eines davon nachzurechnen:

$$(a,b)\cdot[(c,d) + (e,f)] = (a,b)\cdot(c + e, d + f)$$
$$= (ac + ae - bd - bf,\ ad + af + bc + be)\ ,$$

$$(a,b)\cdot(c,d) + (a,b)\cdot(e,f) = (ac - bd, ad + bc) + (ae - bf, af + be)$$
$$= (ac - bd + ae - bf\ ,\ ad + bc + af + be).$$

Die Multiplikation ist eine Verknüpfung auf $\mathbb{R}^2 \setminus \{(0,0)\}$:

Seien $(a,b) \neq (0,0)$ und $(c,d) \neq (0,0)$. Wäre $(a,b)\cdot(c,d) = (0,0)$, so folgte $ac - bd = 0$, $ad + bc = 0$ und somit $0 = (ac - bd)^2 + (ad + bc)^2 = (a^2 + b^2)\cdot(c^2 + d^2)$. Also wäre $a^2 + b^2 = 0$ und daher $(a,b) = (0,0)$ oder $c^2 + d^2 = 0$ und somit $(c,d) = (0,0)$. In beiden Fällen ergibt sich ein Widerspruch zur Voraussetzung.

Das neutrale Element bezüglich der Multiplikation ist $(1,0)$, denn es gilt für alle $(a,b) \in \mathbb{R}^2$, daß $(a,b)\cdot(1,0) = (a,b)$.

Das inverse Element zu $(a,b) \neq (0,0)$ ist

$$\left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right).$$

Insgesamt haben wir folgenden Satz bewiesen:

Satz 10. $(\mathbb{R}^2,+,\cdot)$ *ist ein Körper.*

$(\mathbb{R}^2,+,\cdot)$ heißt Körper der *komplexen Zahlen.* Wir verwenden in Zukunft die Bezeichnung $\mathbb{C}$. Die Elemente $z = (a,b) \in \mathbb{C}$ heißen *komplexe Zahlen* ; a heißt *Realteil* und b heißt *Imaginärteil* von z .

Die Teilmenge $\mathbb{R} \times \{0\} = \{(a,0) |\ a \in \mathbb{R}\}$ von $\mathbb{C}$ ist bezüglich der in $\mathbb{C}$ erklärten Addition und Multiplikation selbst ein Körper, und die Abbildung

$$f\colon \mathbb{R} \longrightarrow \mathbb{R} \times \{0\}$$
$$a \longmapsto (a,0)$$

ist ein Körperisomorphismus. Die reellen Zahlen sind also in den Körper der komplexen Zahlen eingebettet, und wir können sie als spezielle komplexe Zahlen auffassen.

Jede komplexe Zahl $z = (a,b)$ läßt sich nun folgendermaßen darstellen:

$$z = (a,b) = (a,0) + (0,b) = (a,0) + (0,1)\cdot(b,0).$$

Verwenden wir die Abkürzung

$$i := (0,1)$$

und beachten wir, daß a mit $(a,0)$ und b mit $(b,0)$ identifiziert wird, so gilt

$$z = a + ib.$$

Ist $z \neq 0$, so schreiben wir für z^{-1} auch $\frac{1}{z} = \frac{1}{a + ib}$.

In dieser Darstellung können wir mit den komplexen Zahlen wie im Körper $\mathbb{R}$ rechnen. Wir müssen nur beachten, daß $i^2 = -1$ gilt.

Beispiel. Sei $z = a + ib$, $w = c + id$. Dann ist

$$z\cdot w = (a + ib)\cdot(c + id) = ac + ibc + iad + i^2bd = (ac - bd) + i(bc + ad).$$

Ist $z \neq 0$, so gilt

$$\frac{1}{z} = \frac{1}{a + ib} = \frac{a - ib}{(a + ib)(a - ib)} = \frac{a}{a^2 + b^2} - i\frac{b}{a^2 + b^2}.$$

Mit $z = a + ib \in \mathbb{C}$ ist auch $\overline{z} := a - ib \in \mathbb{C}$. $\overline{z}$ heißt die zu z *konjugiert komplexe Zahl*.
Es gelten folgende Rechenregeln:

(a) $\overline{z + w} = \overline{z} + \overline{w}$ und $\overline{z\cdot w} = \overline{z}\cdot\overline{w}$, $z,w \in \mathbb{C}$,

(b) $\overline{(\overline{z})} = z$, $z \in \mathbb{C}$,

(c) $z \in \mathbb{R} \iff z = \overline{z}$, $z \in \mathbb{C}$,

(d) $z\cdot\overline{z} \in \mathbb{R}$, $z\cdot\overline{z} \geq 0$ und $(z\cdot\overline{z} = 0 \iff z = 0)$, $z \in \mathbb{C}$.

Die reelle Zahl $|z| := (z\cdot\overline{z})^{1/2}$ heißt der *Betrag* von z.

Bemerkung. Die Abbildung $z \longmapsto \overline{z}$, $z \in \mathbb{C}$, ist wegen (b) offensichtlich bijektiv. Wegen (a) und (b) ist sie ein Isomorphismus von $\mathbb{C}$ in sich, also ein Automorphismus, und wegen (c) läßt sie den Körper $\mathbb{R}$ elementweise fest. Sie ist neben $\mathrm{id}_{\mathbb{C}}$ der einzige Automorphismus von $\mathbb{C}$ mit dieser Eigenschaft (Beweis als Übungsaufgabe).

Nun wenden wir uns algebraischen Strukturen mit zwei Verknüpfungen zu, die keine Körper sind. Beispiele dafür sind die Mengen $\mathbb{Z}_m$, wenn m keine Primzahl ist. Dann ist die Multiplikation auf $\mathbb{Z}_m$ zwar immer noch assoziativ und es gelten die Distributivgesetze, aber $\mathbb{Z}_m$ ist kein Körper mehr. Wir sprechen in diesem Fall von einem Ring.

Definition. Eine Menge A mit zwei Verknüpfungen $+$ und $\cdot$ heißt *Ring*, wenn folgende Bedingungen erfüllt sind:

(a) $(A,+)$ ist eine abelsche Gruppe,

(b) $(A,\cdot)$ ist eine Halbgruppe,

(c) für alle $x,y,z \in A$ gilt: $x\cdot(y + z) = x\cdot y + x\cdot z$, $(x + y)\cdot z = x\cdot z + y\cdot z$. (*"Distributivgesetze"*)

Ist $(A,\cdot)$ auch kommutativ, so sprechen wir von einem *kommutativen Ring*.

Besitzt $(A,\cdot)$ ein Neutralelement 1 (*Einselement*), so sprechen wir von einem *Ring mit* 1.

Beispiele. **(a)** Jeder Körper ist ein kommutativer Ring mit 1.

(b) $\mathbb{Z}_m$ ist für jedes $m \in \mathbb{N}$ ein kommutativer Ring mit 1. Falls m keine Primzahl ist, sprechen wir von dem *Restklassenring* $\mathbb{Z}_m$.

(c) $\mathbb{Z}$ ist ein kommutativer Ring mit 1.

(d) $(\mathcal{P}(A),\Delta,\cap)$ ist ein kommutativer Ring mit 1 (Übungsaufgabe).

Die nächsten Beispiele sind besonders wichtig. Wir wollen sie deshalb in einem eigenen Paragraphen behandeln.

§ 4 Matrizen und Polynome

Zunächst wollen wir uns mit den Matrizen beschäftigen.

Definition. Seien $m,n \in \mathbb{N}$. Eine (m,n)–*Matrix* A über einem Körper $\mathbb{K}$ ist ein $m \cdot n$–Tupel von Elementen von $\mathbb{K}$, das als rechteckiges Schema mit m Zeilen und n Spalten angeordnet ist:

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots\cdots & a_{1n} \\ a_{21} & a_{22} & \cdots\cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots\cdots & a_{mn} \end{bmatrix}, \quad a_{ij} \in \mathbb{K}.$$

Andere Schreibweisen:

$$A = (\!(a_{ij})\!)_{m \times n} \text{ oder } A = (\!(a_{ij})\!) \text{ oder auch } A = (a_{ij}).$$

$(1,n)$–Matrizen heißen *Zeilen*, $(m,1)$–Matrizen heißen *Spalten*. (n,n)–Matrizen heißen *n–reihige quadratische Matrizen* (über $\mathbb{K}$). Speziell heißt die (n,n)–Matrix

$$E_n = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & \ddots & \ddots & & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots\cdots & 0 & 0 & 1 \end{bmatrix}$$

n–reihige Einheitsmatrix. Unter Verwendung des Kroneckersymbols

$$\delta_{ij} := \begin{cases} 0 & \text{für } i \neq j \\ 1 & \text{für } i = j \end{cases}$$

können wir auch kurz $E_n = (\!(\delta_{ij})\!)$ schreiben. Mit $\mathbb{K}^{m \times n}$ bezeichnen wir die Menge aller (m,n)–Matrizen über dem Körper $\mathbb{K}$.

Bemerkung. Da eine (m,n)–Matrix über $\mathbb{K}$ im Prinzip ein Element von $\mathbb{K}^{mn}$ in anderer Schreibweise ist, ergibt sich sofort, wann zwei Matrizen gleich sind.

Außerdem erhalten wir, daß $\mathbb{K}^{m\times n}$ mit der komponentenweisen Addition eine abelsche Gruppe ist.

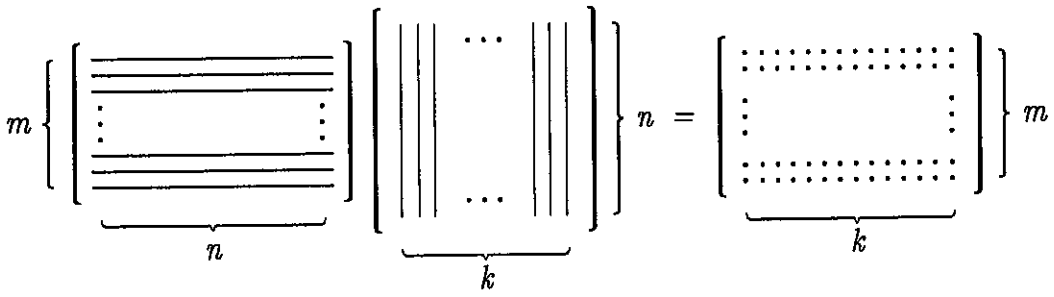
Nun wollen wir für Matrizen eine Multiplikation erklären.

Definition. Es seien $A \in \mathbb{K}^{m\times n}$ und $B \in \mathbb{K}^{n\times k}$. Dann heißt die Matrix $(\!(c_{ij})\!) \in \mathbb{K}^{m\times k}$, die durch

$$c_{ij} := \sum_{l=1}^{n} a_{il}\, b_{lj} \qquad i = 1,\ldots,m, \quad j = 1,\ldots,k$$

definiert ist, das *Produkt AB von A und B.*

Merkschema zur Matrizenmultiplikation ("i–te Zeile von A mal j–te Spalte von B ergibt das Element c_{ij} von C"):



Beispiel. Für $A = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \in \mathbb{R}^{2\times 3}$, $B = \begin{bmatrix} 0 & 2 \\ 1 & -1 \\ 0 & 1 \end{bmatrix} \in \mathbb{R}^{3\times 2}$ ist

$$AB = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \begin{bmatrix} 0 & 2 \\ 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 2 & 5 \end{bmatrix},$$

$$BA = \begin{bmatrix} 0 & 2 \\ 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 6 & 4 & 2 \\ -2 & 0 & 2 \\ 3 & 2 & 1 \end{bmatrix}.$$

Diese Art der Matrizenmultiplikation scheint zunächst etwas merkwürdig zu sein. Naheliegender wäre ja wohl, die Multiplikation, analog zur Addition, komponentenweise zu erklären. Wie wir später jedoch sehen werden, haben Matrizen etwas mit Abbildungen zu tun, und die Multiplikation von Matrizen ist deshalb so definiert,

daß sie mit der Verkettung der zugehörigen Abbildungen verträglich ist.

Satz 11. *Die folgenden Matrizenprodukte und Matrizensummen seien jeweils erklärt (über* $\mathbb{K}$*). Dann gilt:*

(a) $(AB)C = A(BC)$, *("Assoziativität")*

(b) $(A + B)C = AC + BC$, *("Distributivität")*

$A(B + C) = AB + AC$,

(c) $E_n A = A, \quad AE_n = A$.

Beispiel zur Interpretation. Das Produkt $E_n A$ ist erklärt für alle $A \in \mathbb{K}^{n\times k}$, das Produkt AE_n dagegen für alle $A \in \mathbb{K}^{m\times n}$. Also gilt $E_n A = A$ für alle $A \in \mathbb{K}^{n\times k}$ und $AE_n = A$ für alle $A \in \mathbb{K}^{m\times n}$.

Beweis. Zum Beweis wird man natürlich die entsprechenden Eigenschaften des Körpers $\mathbb{K}$ ausnutzen.

(a) In der i–ten Zeile von AB steht an der k–ten Stelle das Element $\sum_l a_{il}\, b_{lk}$, $k = 1,2,\ldots$; das (i,j)–te Element der Matrix $(AB)C$ ist daher $\sum_k (\sum_l a_{il}\, b_{lk}) c_{kj}$.

Nutzen wir in $\mathbb{K}$ die Kommutativität bezüglich $+$, die Assoziativität bezüglich $\cdot$ und die Distributivität aus, so können wir umformen:

$$\sum_k (\sum_l a_{il}\, b_{lk}) c_{kj} = \sum_k \sum_l (a_{il}\, b_{lk}\, c_{kj}) = \sum_l \sum_k (a_{il}\, b_{lk}\, c_{kj}) = \sum_l a_{il} (\sum_k b_{lk}\, c_{kj}).$$

Es ist $\sum_k b_{lk}\, c_{kj}$ das l–te Element in der j–ten Spalte von BC. Somit gibt das letzte Element das (i,j)–te Element von $A(BC)$ an.

(b) (i,j)–tes Element von $(A + B)C$: $\sum_k (a_{ik} + b_{ik}) c_{kj}$,

(i,j)–tes Element von AC: $\sum_k a_{ik}\, c_{kj}$,

(i,j)–tes Element von BC: $\sum_k b_{ik}\, c_{kj}$.

Das andere Distributivgesetz wird analog bewiesen.

(c) (i,j)–tes Element von $E_n A$: $\sum_k \delta_{ik}\, a_{kj} = a_{ij}$,

(i,j)–tes Element von AE_n : $\sum_k a_{ik}\, \delta_{kj} = a_{ij}$. ■

Bemerkung. Für beliebige Matrizen haben die Produkte AB und BA (wenn beide existieren) meist verschiedenes Format. Aber auch für quadratische Matrizen gilt im allgemeinen **nicht** $AB = BA$.

Beispiel. Für die (n,n)–Matrizen

$$A = \begin{bmatrix} 1\,0 & \cdots\cdots & 0 \\ 0 & \cdots\cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots\cdots & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & \cdots\cdots & 0\,1 \\ 0 & \cdots\cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots\cdots & 0 \end{bmatrix},$$

folgt

$$AB = \begin{bmatrix} 0 & \cdots\cdots & 0\,1 \\ 0 & \cdots\cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots\cdots & 0 \end{bmatrix}, \quad BA = \begin{bmatrix} 0 & \cdots\cdots & 0 \\ 0 & \cdots\cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots\cdots & 0 \end{bmatrix}.$$

Aus Satz 11 erhalten wir nun sofort das folgende Ergebnis:

Satz 12. *Die Menge* $\mathbb{K}^{n\times n}$ *aller* n*–reihigen quadratischen Matrizen über* $\mathbb{K}$ *bildet einen Ring mit* 1.

Bemerkungen und Definitionen. **(a)** Das obige Beispiel zeigt, daß $\mathbb{K}^{n\times n}$ für keinen Körper $\mathbb{K}$ und kein $n \geq 2$ ein Körper ist.

(b) Ist eine Matrix A in der Halbgruppe $(\mathbb{K}^{n\times n}, \cdot)$ invertierbar, so heißt A *regulär*. Ist A nicht regulär, so heißt A *singulär*.

Die Menge $GL(n,\mathbb{K})$ der regulären (n,n)–Matrizen ist eine Gruppe bezüglich der Matrizenmultiplikation. Sie heißt *allgemeine lineare Gruppe* (über $\mathbb{K}$).

Die obigen Matrizen A und B sind für $n \geq 2$ singulär, da andernfalls aus $BA = O$ folgte, daß A oder B die Nullmatrix wäre. Dagegen ist die (n,n)–Matrix

$$A = \begin{bmatrix} 1 & 0 & \cdots & 0 & 1 \\ 0 & \ddots & \ddots & & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots\cdots & 0 & 1 \end{bmatrix}$$

regulär, denn

$$A^{-1} = \begin{bmatrix} 1 & 0 & \cdots & 0 & -1 \\ 0 & \ddots & \ddots & & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots\cdots & 0 & 1 \end{bmatrix}$$

ist die zu A inverse Matrix.

Man beachte, daß auch die Menge der regulären (n,n)–Matrizen für $n \geq 2$ keinen Körper bildet, da die Summe zweier regulärer Matrizen keine reguläre Matrix sein muß. So ist z.B. für die obige reguläre Matrix A die Matrix

$$A + (-E_n) = \begin{bmatrix} 0 & \cdots\cdots & 0 & 1 \\ 0 & \cdots\cdots & & 0 \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ 0 & \cdots\cdots & & 0 \end{bmatrix}$$

nicht regulär.

(c) Später werden wir ein Verfahren kennenlernen, mit dem man prüfen kann, ob eine Matrix regulär ist, und mit dem man im Fall der Regularität auch die inverse Matrix berechnen kann.

(d) Sei $A = (\!(a_{ij})\!) \in \mathbb{K}^{m\times n}$. Dann heißt die Matrix $(\!(b_{ij})\!) \in \mathbb{K}^{n\times m}$ mit $b_{ij} = a_{ji}$ die *transponierte Matrix* zu A ; Schreibweise: A^T.

A^T ist also die an der "Diagonalen a_{11}, a_{22},... gespiegelte" Matrix A.

Es gelten folgende Rechenregeln:

(i) $(A^T)^T = A$, $(A + B)^T = A^T + B^T$, $(AB)^T = B^T A^T$.

(ii) Ist A regulär, so auch A^T und es gilt $(A^T)^{-1} = (A^{-1})^T$.

(e) Eine Matrix A mit $A = A^\top$ heißt *symmetrisch*. Es können natürlich nur quadratische Matrizen symmetrisch sein. Die Summe symmetrischer Matrizen ist wieder symmetrisch, das Produkt im allgemeinen aber nicht. So ist beispielsweise das Produkt

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$$

nicht symmetrisch.

Eine weitere Matrizenoperation, die später noch eine wichtige Rolle spielen wird, ist die Multiplikation von Matrizen mit Körperelementen.

Definition. Es seien $A = (\!(a_{ij})\!) \in \mathbb{K}^{m\times n}$ und $c \in \mathbb{K}$. Dann sei cA die Matrix $(\!(b_{ij})\!) \in \mathbb{K}^{m\times n}$ mit $b_{ij} := c\,a_{ij}$ für $i = 1,\ldots,m$ und $j = 1,\ldots,n$.

Bemerkung. Es gelten die Distributivgesetze

$$(a+b)\,C = a\,C + b\,C\ , \quad a, b \in \mathbb{K},\ C \in \mathbb{K}^{m\times n}\ ,$$
$$a\,(B+C) = a\,B + a\,C\ , \quad a \in \mathbb{K},\ B, C \in \mathbb{K}^{m\times n}\ ,$$

sowie die Assoziativgesetze

$$(a\,b)\,C = a\,(b\,C)\ , \quad a, b \in \mathbb{K},\ C \in \mathbb{K}^{m\times n}\ ,$$
$$a\,(B\,C) = (a\,B)\,C = B\,(a\,C)\ , \quad a \in \mathbb{K},\ B \in \mathbb{K}^{m\times n},\ C \in \mathbb{K}^{n\times k}\ .$$

Ferner gilt $(c\,A)^\top = c\,A^\top$ für alle $c \in \mathbb{K}$ und alle $A \in \mathbb{K}^{m\times n}$.

Zum Abschluß wollen wir noch bemerken, daß die Definition einer Matrix $A = (\!(a_{ij})\!)$ sinnvoll bleibt, wenn die a_{ij} keine Körperelemente, sondern Elemente eines kommutativen Rings mit 1 sind. Auch die Ergebnisse dieses Paragraphen bleiben in diesem Fall richtig, weil sie nicht von der Division Gebrauch machen.

Polynome

In der Schule lernt man Polynome gewöhnlich als reelle Funktionen auf $\mathbb{R}$ kennen, die von der Form

$$(*) \qquad x \longmapsto a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \,,\ n \in \mathbb{N}_0,\ a_i \in \mathbb{R}\,,$$

sind.

Nun kann man aber ebensogut Funktionen mit der Abbildungsvorschrift (*) über einem beliebigen Körper $\mathbb{K}$ betrachten, oder, wenn wir noch einen Schritt weitergehen, kann man in (*) statt Körperelemente x auch Elemente eines Ringes mit 1 einsetzen, z.B. Matrizen $A \in \mathbb{K}^{n\times n}$. Dabei ist $A^k = \underbrace{A\cdot A\cdots A}_{k}$ für $k \in \mathbb{N}$ und a_0 wird ersetzt durch $a_0 E_n$. Man erhält dann eine Abbildung von $\mathbb{K}^{n\times n}$ in sich.

Es ist deshalb empfehlenswert, den Begriff des Polynoms abstrakter zu fassen und die Größe x als "unbestimmte Größe", d.h. einfach als Symbol aufzufassen, für das bei Bedarf andere Elemente eingesetzt werden können. Dann ist das Polynom also durch die Koeffizienten $a_0,a_1,\ldots,a_n \in \mathbb{K}$ gegeben, d.h. es ist einfach ein Element $(a_0,\ldots,a_n) \in \mathbb{K}^{n+1}$.

Da wir aber Verknüpfungen für Polynome ganz verschiedener "Längen" n erklären wollen, ist es günstiger, das $(n+1)$-Tupel $(a_0,\ldots,a_n)$ durch Nullen zu einer Folge von Elementen aus $\mathbb{K}$ zu ergänzen: $(a_0,a_1,\ldots,a_n,0,0,\ldots)$.

Definition. Ein *Polynom* p über dem Körper $\mathbb{K}$ ist eine Folge $(a_0,a_1,\ldots,a_n,a_{n+1},\ldots)$ von Körperelementen, also ein Element von $\mathbb{K}^{\mathbb{N}_0}$, derart daß ein $n \in \mathbb{N}$ existiert mit $a_k = 0$ für alle $k > n$: $p = (a_0,\ldots,a_n,0,0,\ldots)$.

Wir schreiben auch $p = (a_i)_{i \in \mathbb{N}_0}$ oder in symbolischer Form

$$p = \sum_{i=0}^{\infty} a_i X^i \quad \text{bzw.} \quad p = \sum_{i=0}^{n} a_i X^i \,.$$

$p = (0,0,\ldots)$ heißt das *Nullpolynom;* Kurzschreibweise: $p = o$.

Ist $p \neq o$, so heißt das größte $n \in \mathbb{N}_0$ mit $a_n \neq 0$ der *Grad* von p und a_n heißt der *Leitkoeffizient* von p. Wir verwenden die Schreibweise Grad $p = n$ und für $p = o$ setzen wir Grad $p = -1$. Ein Polynom vom Grad n, $n \geq 0$, heißt *normiert*, wenn $a_n = 1$ ist.

Die Menge aller Polynome über $\mathbb{K}$ bezeichnen wir mit $\mathbb{K}[X]$.

Auf der Menge $\mathbb{K}[X]$ wollen wir nun eine Addition und eine Multiplikation so einführen, daß wir formal wie mit Körperelementen rechnen können, z.B.:

$$(a_0 + a_1X)(b_0 + b_1X + b_2X^2) = a_0b_0 + (a_0b_1 + a_1b_0)X + (a_0b_2 + a_1b_1)X^2 + a_1b_2X^3 .$$

Definition. Für Polynome $p,q \in \mathbb{K}[X]$, $p = (a_i)_{i \in \mathbb{N}_0}$, $q = (b_i)_{i \in \mathbb{N}_0}$, sei

$$p + q := (a_i + b_i)_{i \in \mathbb{N}_0} ,$$

$$p \cdot q := (c_i)_{i \in \mathbb{N}_0} \text{ mit } c_i = \sum_{k=0}^{i} a_k b_{i-k} .$$

Da für endlich viele Polynome die Verknüpfungen praktisch in $\mathbb{K}^n$ mit geeignetem n ausgeführt werden (die verschwindenden Koeffizienten spielen ja keine Rolle), wissen wir sofort, daß $(\mathbb{K}[X],+)$ eine abelsche Gruppe ist. Das neutrale Element in dieser Gruppe ist das Nullpolynom. Inverses Element zu $p = (a_i)_{i \in \mathbb{N}_0}$ ist das Polynom $-p := (-a_i)_{i \in \mathbb{N}_0}$. Analog wie bei den Matrizen ergeben sich die Assoziativität von $\cdot$ und die Distributivgesetze. Wegen

$$p \cdot q = \Big(\sum_{l=0}^{i} a_l b_{i-l}\Big)_{i \in \mathbb{N}_0} \overset{i-l=k}{=} \Big(\sum_{k=0}^{i} a_{i-k} b_k\Big)_{i \in \mathbb{N}_0} = \Big(\sum_{k=0}^{i} b_k a_{i-k}\Big)_{i \in \mathbb{N}_0} = q \cdot p$$

ist die Multiplikation sogar kommutativ. Das konstante Polynom $1 = (1,0,0,\ldots)$ ist das Einselement. Also erhalten wir das folgende Ergebnis:

Satz 13. $(\mathbb{K}[X], +, \cdot)$ *ist ein kommutativer Ring mit* 1.

Bemerkungen. **(a)** Für alle Polynome $p,q \in \mathbb{K}[X]$ gilt:

$$\text{Grad } (p+q) \leq \max (\text{Grad } p, \text{Grad } q).$$

Für alle Polynome $p \neq o$, $q \neq o$ gilt: Grad $(p \cdot q)$ = Grad p + Grad q.

(b) Jedes Polynom $p = a_0 + a_1 X + \cdots + a_n X^n$ erzeugt eine Funktion auf $\mathbb{K}$, die Polynomfunktion $x \longmapsto a_0 + a_1 x + \cdots + a_n x^n$, $x \in \mathbb{K}$.

Die Menge der Polynomfunktionen $f: \mathbb{K} \longrightarrow \mathbb{K}$ bildet bezüglich der punktweise erklärten Addition und Multiplikation

$$(f+g)(x) := f(x) + g(x), \quad x \in \mathbb{K},$$
$$(f \cdot g)(x) := f(x) \cdot g(x), \quad x \in \mathbb{K},$$

einen kommutativen Ring mit Eins. Die Abbildung, die jedem Polynom $p \in \mathbb{K}[X]$ die zugehörige Polynomfunktion $x \longmapsto p(x)$, $x \in \mathbb{K}$, zuordnet, ist ein surjektiver Homomorphismus.

Bei endlichen Körpern ist diese Zuordnung nicht injektiv. Hier ist es wichtig, zwischen einem Polynom und der zugehörigen Polynomfunktion zu unterscheiden. Wir wollen dies an einem Beispiel verdeutlichen.

Beispiel. Wir betrachten die Polynome über dem Körper $\mathbb{F}_2$. Das Polynom $p = X + X^2 = (0,1,1,0,\ldots) \in \mathbb{F}_2[X]$ ist vom Nullpolynom $o = (0,0,\ldots)$ verschieden. Die Funktion $f : x \longmapsto x + x^2$, $x \in \mathbb{F}_2$, ist aber identisch 0, denn es gilt $f(0) = 0$ und $f(1) = 1 + 1 = 0$. Also ergeben die beiden Polynome p und o die gleiche Polynomfunktion f auf $\mathbb{F}_2$.

(c) $\mathbb{K}[X]$ ist kein Körper. Das Polynom $p = X$ besitzt z.B. kein inverses Element, denn für alle $p = (a_i)_{i \in \mathbb{N}_0} \in \mathbb{K}[X]$ gilt:

$$X \cdot (a_0 + a_1 X + \cdots + a_n X^n) = a_0 X + a_1 X^2 + \cdots + a_n X^{n+1} \neq 1.$$

Im Polynomring gelten bezüglich der Division ähnliche Aussagen, wie man sie vom Ring der ganzen Zahlen her kennt.

Satz 14. *Zu den Polynomen $p,q \in \mathbb{K}[X]$, $q \neq o$, gibt es eindeutig bestimmte Polynome $r,s \in \mathbb{K}[X]$ mit $p = s \cdot q + r$ und* Grad $r <$ Grad q.

Beweis. Wir zeigen zunächst die Existenz solcher Polynome r und s. Die Aussage ist trivial für Grad $p <$ Grad q. Dann setzen wir nämlich $s = o$ und $r = p$. Somit können wir Grad $p \geq$ Grad q annehmen. Der weitere Beweis erfolgt durch vollständige Induktion nach Grad p:

Grad $p = 0$: Dann ist $p = a_0$, $a_0 \neq 0$. Nach Voraussetzung ist dann auch q vom Grad 0, also $q = b_0$, $b_0 \neq 0$. In diesem Fall gilt $p = a_0 b_0^{-1} q$.

Induktionsschluß von Grad $p \leq k-1$ auf Grad $p = k$: Seien

$$p = a_0 + a_1 X + \cdots + a_k X^k \ , \ a_k \neq 0 \ ,$$

$$q = b_0 + b_1 X + \cdots + b_m X^m \ , \ b_m \neq 0 \ ,$$

und $m \leq k$. Wir betrachten das Polynom

$$p_1 = p - \frac{a_k}{b_m} X^{k-m} \cdot q$$

vom Grad $p_1 < k$. Für Grad $p_1 <$ Grad q folgt nach dem obigen, für Grad $p_1 \geq$ Grad q folgt nach Induktionsannahme, daß Polynome $r_1, s_1 \in \mathbb{K}[X]$ existieren mit $p_1 = s_1 q + r_1$ und Grad $r_1 <$ Grad q. Damit erhalten wir

$$p = (s_1 + \frac{a_k}{b_m} X^{k-m}) \cdot q + r_1$$

mit Grad $r_1 <$ Grad q.

Eindeutigkeit: Aus $p = s_1 q + r_1$, Grad $r_1 <$ Grad q und $p = s_2 q + r_2$, Grad $r_2 <$ Grad q, folgt durch Differenzbildung $r_2 - r_1 = (s_1 - s_2) \cdot q$. Wäre $s_1 - s_2 \neq o$, so folgte mit Grad $q \leq$ Grad $(r_2 - r_1) \leq \max \{\text{Grad } r_2, \text{Grad } r_1\}$ ein Widerspruch. Also gilt $s_1 = s_2$ und damit auch $r_1 = r_2$. ∎

Ein Element $x_0 \in \mathbb{K}$ heißt *Nullstelle* des Polynoms $p \in \mathbb{K}[X]$, wenn x_0 Nullstelle der zugehörigen Polynomfunktion $x \longmapsto p(x)$, $x \in \mathbb{K}$, ist, also $p(x_0) = 0$ gilt.

Ist x_0 Nullstelle von p, so erhalten wir als Spezialfall von Satz 14 für p die Darstellung $p = s \cdot (X - x_0)$ mit $s \in \mathbb{K}[X]$. Umgekehrt folgt aus einer solchen Darstellung

unmittelbar, daß x_0 Nullstelle des Polynoms p ist.

Korollar 15. *Genau dann ist x_0 Nullstelle eines Polynoms $p \in \mathbb{K}[X]$, wenn es eine Faktorisierung*

$$p = (X - x_0) \cdot s$$

mit $s \in \mathbb{K}[X]$ gibt.

Bemerkungen. **(a)** Ein Polynom vom Grad n , $n \geq 0$, besitzt höchstens n paarweise verschiedene Nullstellen.

(b) Hat der Körper $\mathbb{K}$ unendlich viele Elemente, so gehören zu verschiedenen Polynomen $p, q \in \mathbb{K}[X]$ auch verschiedene Polynomfunktionen. Wäre nämlich $p(x) = q(x)$ für alle $x \in \mathbb{K}$, so hätte das Polynom $p - q$ unendlich viele Nullstellen.

In diesem Fall sind $\mathbb{K}[X]$ und der Ring der Polynomfunktionen über $\mathbb{K}$ isomorph.

Nicht jedes Polynom besitzt eine Nullstelle, wie das Beispiel $X^2 + 1 \in \mathbb{R}[X]$ zeigt. Fassen wir dieses Polynom jedoch als Polynom über $\mathbb{C}$ auf, so besitzt es Nullstellen (nämlich i und $-i$). Dies ist eine Folge des Fundamentalsatzes der Algebra, den wir hier ohne Beweis zitieren wollen.

Fundamentalsatz der Algebra. *Jedes Polynom $p \in \mathbb{C}[X]$ mit* Grad $p \geq 1$ *besitzt eine Nullstelle.*

Als Folgerung ergibt sich wegen Korollar 15, daß über $\mathbb{C}$ jedes Polynom p mit Grad $p \geq 1$ vollständig in Linearfaktoren zerfällt, d.h. Produkt von Polynomen vom Grad 1 ist.

Das Polynom s heißt *Teiler* des Polynoms $p \in \mathbb{K}[X]$, wenn es ein $r \in \mathbb{K}[X]$ mit $p = s \cdot r$ gibt. Zwei Polynome heißen *teilerfremd*, wenn sie keinen gemeinsamen Teiler vom Grad ≥ 1 haben. Sind p und q teilerfremd, so muß eines der beiden Polynome vom Nullpolynom verschieden sein.

Zum Schluß dieses Paragraphen wollen wir noch einige wichtige Eigenschaften teilerfremder Polynome beweisen.

Satz 16. *Die Polynome $p,q \in \mathbb{K}[X]$ sind genau dann teilerfremd, wenn es Polynome $r,s \in \mathbb{K}[X]$ gibt mit*

$$r \cdot p + s \cdot q = 1.$$

Beweis. Seien p und q teilerfremde Polynome. Wir betrachten zunächst die Menge $I := \{rp + sq \mid r,s \in \mathbb{K}[X]\}$. Offensichtlich ist I eine Untergruppe der additiven Gruppe von $\mathbb{K}[X]$. Weiter gilt für jedes Polynom $rp + sq \in I$ und jedes $t \in \mathbb{K}[X]$, daß das Produkt $t(rp + sq) = trp + tsq$ Element von I ist. (I ist ein Ideal im Ring $\mathbb{K}[X]$).

Unter den normierten Polynomen in I gibt es ein Polynom $\tilde{t}$ vom kleinsten Grad. Sei nun $t \in I$ beliebig. Dann folgt aus Satz 14, daß es Polynome s_1, r_1 gibt mit $t = s_1\tilde{t} + r_1$ und Grad $r_1 <$ Grad $\tilde{t}$. Wegen $r_1 = t - s_1\tilde{t} \in I$ muß $r_1 = o$ sein. Somit folgt $t = s_1\tilde{t}$. Speziell können wir für t die Polynome p und q nehmen. Dann gilt $p = s_1\tilde{t}$ und $q = s_2\tilde{t}$. Da p und q teilerfremd sind, muß $\tilde{t}$ konstant sein, also $\tilde{t} = 1$. Wegen $\tilde{t} \in I$ folgt die Behauptung.

Umgekehrt gebe es nun Polynome $r,s \in \mathbb{K}[X]$ mit $rp + sq = 1$. Dann folgt für jeden gemeinsamen Teiler t von p und q aus $p = tp'$ und $q = tq'$ sofort $t(rp' + sq') = 1$, also Grad $t \leq$ Grad $1 = 0$. Somit sind p,q teilerfremd. ∎

Bemerkungen. **(a)** Es seien $k \in \mathbb{N}$, $p_1,\ldots,p_k, q \in \mathbb{K}[X]$, und jedes der Polynome $p_1,\ldots,p_k$ sei zu q teilerfremd. Dann sind auch $p_1 \cdots p_k$ und q teilerfremd.

Beweis. Vollständige Induktion nach k : Der Induktionsanfang $k = 1$ ist trivial. Schluß von $k-1$ auf k : Nach Induktionsvoraussetzung ist $p := p_1 \cdots p_{k-1}$ teilerfremd zu q. Daher gibt es Polynome $s,t \in \mathbb{K}[X]$ mit $sp + tq = 1$. Weil p_k und q teilerfremd sind, gibt es analog $s',t' \in \mathbb{K}[X]$ mit $s'p_k + t'q = 1$. Wir multiplizieren und erhalten $ss'pp_k + (spt' + ts'p_k + qtt')q = 1$. Also sind $p_1 \cdots p_k$ und q teilerfremd. ∎

(b) Die Polynome r und s aus Satz 16 lassen sich mit dem *Euklidischen Algorithmus* bestimmen.

Beispiel. Gegeben seien die Polynome $p = X^5 + 2X^3 - 3X^2 + 4$ und $q = X^2 + 1$ aus

$\mathbb{R}[X]$. Wir dividieren p durch q und erhalten

$$p = (X^3 + X - 3)q + (-X + 7) = s_1 q + r_1 .$$

Nun dividieren wir q durch r_1 und erhalten

$$q = (-X - 7)r_1 + 50 = s_2 r_1 + 50.$$

Damit ergibt sich durch Rückwärtseinsetzen

$$50 = q - s_2 r_1 = q - s_2(p - s_1 q) = -s_2 p + (1 + s_2 s_1)q$$

$$= (X + 7)p + (-X^4 - 7X^3 - X^2 - 4X + 22)q .$$

Für

$$r = \frac{1}{50}(x + 7) \quad \text{und} \quad s = \frac{1}{50}(-X^4 - 7X^3 - X^2 - 4X + 22)$$

folgt somit

$$rp + sq = 1.$$

§ 5 Der Gaußsche Algorithmus

Wir kommen nun wieder auf die Behandlung linearer Gleichungssysteme

$$(*) \qquad \begin{array}{c} a_{11}\, x_1 + \cdots + a_{1n}\, x_n = b_1 \\ \vdots \qquad\qquad\quad \vdots \quad \vdots \\ a_{m1}\, x_1 + \cdots + a_{mn}\, x_n = b_m \end{array}$$

zurück. Dabei können wir jetzt ein LGS (*) über einem beliebigen Körper $\mathbb{K}$ zulassen, d.h. ein LGS mit $a_{ij} \in \mathbb{K}$, $b_i \in \mathbb{K}$ und Variablen $x_j \in \mathbb{K}$.

Wir wollen ein konkretes Verfahren zur systematischen Lösung von (*) angeben. Grundlage dieses Verfahrens sind die *elementaren Umformungen* (genauer die *elementaren Zeilenumformungen* im Gegensatz zu den später benutzten *elementaren Spaltenumformungen*). Darunter verstehen wir die folgenden drei Umformungen eines linearen Gleichungssystems:

(a) *Vertauschen zweier Gleichungen.*

(b) *Multiplikation einer der Gleichungen mit* $c \in \mathbb{K}$, $c \neq 0$.

(c) *Addition einer, mit einem beliebigen* $c \in \mathbb{K}$ *multiplizierten, Gleichung zu einer anderen Gleichung.*

Satz 17. *Ändert man ein lineares Gleichungssystem durch elementare Zeilenumformungen, so ändert sich die Lösungsmenge des linearen Gleichungssystems nicht.*

Beweis. Offensichtlich ist jede Lösung des ursprünglichen LGS (*) auch Lösung des durch elementare Umformungen abgeänderten LGS (**). Da jede Zeilenumformung durch eine Zeilenumformung wieder rückgängig gemacht werden kann, ist umgekehrt auch jede Lösung von (**) eine Lösung von (*). ∎

Definition und Bemerkung. Zwei lineare Gleichungssysteme heißen *äquivalent*, wenn sie dieselbe Lösungsmenge besitzen. Satz 17 besagt also, daß elementare Zeilenumformungen ein lineares Gleichungssystem in ein dazu äquivalentes überführen.

Zur Vorbereitung des Algorithmus wollen wir ein Beispiel rechnen.

Beispiel. Gegeben sei das lineare Gleichungssystem (*) über den reellen Zahlen $\mathbb{R}$.

$$(*) \qquad \begin{array}{rrrrrrr} -2x_1 & + 4x_2 & - 2x_3 & - x_4 & + 4x_5 & = & -3 \\ 4x_1 & - 8x_2 & + 3x_3 & - 3x_4 & + x_5 & = & 2 \\ x_1 & - 2x_2 & + x_3 & - x_4 & + x_5 & = & 0 \\ x_1 & - 2x_2 & & - 3x_4 & + 4x_5 & = & a \end{array} \quad , \quad a \in \mathbb{R}$$

Durch Vertauschen der 1. und 3. Gleichung ergibt sich folgende Form

$$\begin{array}{rrrrrrr} x_1 & - 2x_2 & + x_3 & - x_4 & + x_5 & = & 0 \\ 4x_1 & - 8x_2 & + 3x_3 & - 3x_4 & + x_5 & = & 2 \\ -2x_1 & + 4x_2 & - 2x_3 & - x_4 & + 4x_5 & = & -3 \\ x_1 & - 2x_2 & & - 3x_4 & + 4x_5 & = & a \end{array} \begin{array}{l} \\ \left.\begin{array}{l} \\ \\ \end{array}\right. \\ \\ \end{array} \begin{array}{l} \\ -4 \\ \\ \\ \end{array} \quad \left.\begin{array}{l} \\ 2 \\ \\ \end{array}\right| \begin{array}{l} \\ \\ -1 \end{array}$$

Indem wir die angedeuteten Elementarumformungen des Typs (c) anwenden, erhalten wir daraus zunächst

$$\begin{array}{rrrrrrr} x_1 & - 2x_2 & + x_3 & - x_4 & + x_5 & = & 0 \\ & & - x_3 & + x_4 & - 3x_5 & = & 2 \\ & & & - 3x_4 & + 6x_5 & = & -3 \\ & & - x_3 & - 2x_4 & + 3x_5 & = & a \end{array} \begin{array}{l} \\ \\ \left.\begin{array}{l} \\ \\ \end{array}\right. \\ \\ \end{array} \begin{array}{l} \\ \\ -1 \\ \\ \end{array}$$

dann

$$\begin{array}{rrrrrrr} x_1 & - 2x_2 & + x_3 & - x_4 & + x_5 & = & 0 \\ & & - x_3 & + x_4 & - 3x_5 & = & 2 \\ & & & - 3x_4 & + 6x_5 & = & -3 \\ & & & - 3x_4 & + 6x_5 & = & a-2 \end{array} \begin{array}{l} \\ \\ \\ \left.\begin{array}{l} \\ \end{array}\right. \\ \end{array} \begin{array}{l} \\ \\ \\ -1 \\ \end{array}$$

und schließlich

$$\begin{array}{rrrrrrr} x_1 & - 2x_2 & + x_3 & - x_4 & + x_5 & = & 0 \\ & & - x_3 & + x_4 & - 3x_5 & = & 2 \\ & & & - 3x_4 & + 6x_5 & = & -3 \\ & & & & 0 & = & a+1 \end{array}$$

Multiplizieren wir jetzt die 2. Gleichung mit -1 und die 3. Gleichung mit $-\frac{1}{3}$, so

ergibt sich die folgende *Treppennormalform* des linearen Gleichungssystems (*):

$$(**) \qquad \begin{array}{rrrrrrr} x_1 & -2x_2 & + x_3 & - x_4 & + x_5 & = & 0 \\ & & x_3 & - x_4 & + 3x_5 & = & -2 \\ & & & x_4 & - 2x_5 & = & 1 \\ & & & & 0 & = & a{+}1 \end{array}$$

Offensichtlich ist (**) und damit auch (*) unlösbar, wenn $a+1 \neq 0$, also $a \neq -1$ ist.

Was läßt sich nun im Fall $a = -1$ über das Lösungsverhalten des LGS (**) aussagen ?

Die Unbekannte x_5 kann eine beliebige reelle Zahl sein, $x_5 = s$. Dann ist x_4 eindeutig festgelegt, nämlich $x_4 = 1 + 2s$. Setzen wir x_5 und x_4 in die 2. Gleichung ein, so ergibt sich für x_3 der Wert $x_3 = -1 - s$. Nun setzen wir x_5, x_4, x_3 in die 1. Gleichung ein und erhalten $x_1 - 2x_2 - 2s - 2 = 0$. In dieser Gleichung kann die Unbekannte x_2 beliebig gewählt werden, $x_2 = t$. Danach kann x_1 ausgerechnet werden, $x_1 = 2s + 2t + 2$.

Will man die Lösung direkt an dem linearen Gleichungssystem ablesen, so muß man dieses noch weiter umformen. Bei unserem Beispiel erhalten wir für $a = -1$ aus der Treppennormalform (**)

$$\begin{array}{rrrrrrr} x_1 & -2x_2 & + x_3 & - x_4 & + x_5 & = & 0 \\ & & x_3 & - x_4 & + 3x_5 & = & -2 \\ & & & x_4 & - 2x_5 & = & 1 \\ & & & & 0 & = & 0 \end{array} \quad \begin{array}{l} \\ \\ \Big] +1 \\ \Big] +1 \end{array}$$

durch die angedeuteten Elementarumformungen zunächst

$$\begin{array}{rrrrrrr} x_1 & -2x_2 & + x_3 & & - x_5 & = & 1 \\ & & x_3 & & + x_5 & = & -1 \\ & & & x_4 & - 2x_5 & = & 1 \\ & & & & 0 & = & 0 \end{array} \quad \Big] -1$$

und daraus schließlich die *Gaußsche Normalform* des linearen Gleichungssystems, wobei wir die Gleichung $0 = 0$ natürlich weglassen können:

$$(***) \qquad \begin{array}{rcl} x_1 - 2x_2 - 2x_5 &=& 2 \\ x_3 + x_5 &=& -1 \\ x_4 - 2x_5 &=& 1 \,. \end{array}$$

Aus dieser Normalform läßt sich nun die allgemeine Lösung von (***) und damit auch von (*) im Fall $a = -1$ direkt ablesen. Die Unbekannten x_5 und x_2 können beliebig gewählt werden:

$$\begin{array}{rcl} x_5 &=& s \\ x_2 &=& t \end{array} \quad , \; s,t \in \mathbb{R}.$$

Für die restlichen Unbekannten folgt aus (***) sofort

$$\begin{array}{rcl} x_1 &=& 2 + 2t + 2s \\ x_3 &=& -1 \quad - s \\ x_4 &=& 1 \quad + 2s \,. \end{array}$$

Bemerkung und Bezeichnung. Jedes lineare Gleichungssystem über dem Körper $\mathbb{K}$

$$\begin{array}{rcl} a_{11}\, x_1 + \cdots + a_{1n}\, x_n &=& b_1 \\ \vdots \qquad\qquad\quad \vdots & & \vdots \\ a_{m1}\, x_1 + \cdots + a_{mn}\, x_n &=& b_m \end{array}$$

läßt sich als Matrizengleichung in der Kurzform $A\, x = b$ schreiben mit

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \in \mathbb{K}^{m\times n}, \quad x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \in \mathbb{K}^{n\times 1}, \quad b = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix} \in \mathbb{K}^{m\times 1}$$

A heißt die zu dem LGS *gehörige Matrix* und ist ebenso wie die $(m,1)$–Matrix b gegeben, und x ist eine unbekannte $(n,1)$–Matrix.

Bei den Elementarumformungen ändern sich nur die Koeffizienten a_{ij} und die b_i. Es genügt daher, anstatt des LGS nur die zugehörige Matrix A bzw. die *erweiterte Matrix*

$$(A|\,b) := \begin{bmatrix} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{bmatrix} \in \mathbb{K}^{m\times(n+1)}$$

zu betrachten und die Elementarumformungen als Zeilenumformungen von $(A|b)$ aufzufassen. Die ersten Schritte im vorigen Beispiel sind dann

$$(A|\,b) = \left[\begin{array}{rrrrr|r} -2 & 4 & -2 & -1 & 4 & -3 \\ 4 & -8 & 3 & -3 & 1 & 2 \\ 1 & -2 & 1 & -1 & 1 & 0 \\ 1 & -2 & 0 & -3 & 4 & a \end{array}\right] \begin{matrix} \\ \\ \downarrow \\ \downarrow \end{matrix} \quad \text{und} \quad \left[\begin{array}{rrrrr|r} 1 & -2 & 1 & -1 & 1 & 0 \\ 4 & -8 & 3 & -3 & 1 & 2 \\ -2 & 4 & -2 & -1 & 4 & -3 \\ 1 & -2 & 0 & -3 & 4 & a \end{array}\right] \begin{matrix} \\ \downarrow -4 \\ \downarrow 2 \\ \downarrow -1 \end{matrix}$$

und für $a = -1$ erhalten wir schließlich

$$\left[\begin{array}{rrrrr|r} 1 & -2 & 0 & 0 & -2 & 2 \\ 0 & 0 & 1 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 & -2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

Gaußscher Algorithmus (Grundform unter ausschließlicher Verwendung von Zeilenumformungen)

Wir beschreiben den Algorithmus ganz allgemein für Matrizen $A \in \mathbb{K}^{m\times n}$. Die durch Zeilenumformungen veränderte Matrix werden wir, wie bei Algorithmen üblich, wieder mit A bezeichnen. Danach wenden wir den Algorithmus auf lineare Gleichungssysteme an, sowie auf n–reihige quadratische Matrizen um gegebenenfalls die Inverse zu bestimmen.

1. Schritt : Ist in der 1. Spalte von A mindestens ein Element von Null verschieden, so kann man durch eventuelles Vertauschen der Zeilen erreichen, daß

$a_{11} \neq 0$ ist. Dann gehe man zum 2. Schritt.

Besteht die 1. Spalte nur aus Nullen, so gehe man zum 3. Schritt.

2. Schritt : Wir multiplizieren die erste Zeile mit $(a_{11})^{-1}$ und addieren dann das $(-a_{i1})$–fache der neuen 1. Zeile zur i–ten Zeile, $i = 2,...,m$. Danach hat die 1. Spalte die Form

$$\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

und wir gehen zum 3. Schritt.

3. Schritt : Wir ersetzen die Matrix A durch die Restmatrix

$$\begin{bmatrix} a_{12} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m2} & \cdots & a_{mn} \end{bmatrix} \in \mathbb{K}^{m\times(n-1)}, \text{ falls die 1. Spalte die Form } \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} \text{ hat,}$$

bzw. durch

$$\begin{bmatrix} a_{22} & \cdots & a_{2n} \\ \vdots & & \vdots \\ a_{m2} & \cdots & a_{mn} \end{bmatrix} \in \mathbb{K}^{(m-1)\times(n-1)}, \text{ falls die 1. Spalte die Form } \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \text{ hat.}$$

Dann gehen wir zurück zum 1. Schritt, der nun auf die Restmatrix angewendet wird, u.s.w.

Das Verfahren endet, wenn im 3. Schritt keine Restmatrix mehr gebildet werden kann. Da in diesem Schritt jeweils entweder eine Spalte oder eine Spalte und eine Zeile gestrichen wird, muß das Verfahren spätestens nach n–maligem Anwenden der 3. Schritte enden. Setzen wir dann alle Spalten und Zeilen, die im 3. Schritt

gestrichen, also beim Weiterlaufen des Algorithmus unverändert geblieben sind, zusammen, so ergibt sich für A die folgende *Treppennormalform*

$$A = \begin{bmatrix} 0 \cdots 0 & \boxed{1} * \cdots & & & & & \\ 0 \cdots\cdots 0 & \boxed{1} * \cdots & & & * & & \\ 0 \cdots\cdots\cdots 0 & \boxed{1} * \cdots & & & & & \\ \vdots & & \ddots & & & & \\ 0 \cdots\cdots\cdots\cdots\cdots 0 & \boxed{1} * \cdots\cdots & * & & & & \\ 0 \cdots\cdots\cdots\cdots\cdots\cdots 0 & \boxed{1} * \cdots & * & & & & \\ 0 \cdots\cdots\cdots\cdots\cdots\cdots\cdots & & & & & & 0 \\ \vdots & & & & & & \vdots \\ 0 \cdots\cdots\cdots\cdots\cdots\cdots\cdots & & & & & & 0 \end{bmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \} k \\ \\ \\ \\ \\ \\ \} m-k \\ \\ \end{matrix}$$

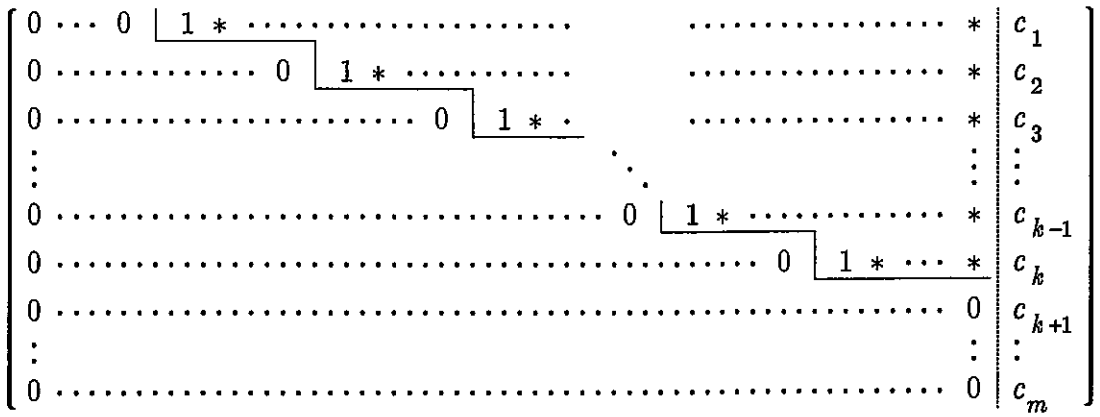
Dabei stehen unterhalb der "Treppe" nur Nullen, oberhalb an den "Stufen" Einsen und sonst irgendwelche Elemente von $\mathbb{K}$, die durch $*$ angedeutet sind.

Die Treppennormalform kann sukzessive durch weitere Zeilenumformungen (vgl. Beispiel) auf die folgende *Gaußsche Normalform* gebracht werden:

$$A = \begin{bmatrix} 0 \cdots 0 & \boxed{1} * \cdots * & 0 * \cdots * & 0 * \cdots & 0 * \cdots * \\ 0 \cdots\cdots 0 & \boxed{1} * \cdots * & 0 * \cdots & 0 * \cdots & 0 * \cdots * \\ 0 \cdots\cdots\cdots 0 & \boxed{1} * \cdots & & \vdots\ \vdots & \vdots\ \vdots\ \vdots\ \vdots \\ \vdots & & \ddots & 0 * \cdots & 0 * \cdots * \\ 0 \cdots\cdots\cdots\cdots\cdots 0 & \boxed{1} * \cdots * & 0 * \cdots & 0 * \cdots & 0 * \cdots * \\ 0 \cdots\cdots\cdots\cdots\cdots\cdots 0 & \boxed{1} * \cdots & & & * \\ 0 \cdots\cdots\cdots\cdots\cdots\cdots\cdots & & & & 0 \\ \vdots & & & & \vdots \\ 0 \cdots\cdots\cdots\cdots\cdots\cdots\cdots & & & & 0 \end{bmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \} k \\ \\ \\ \\ \\ \\ \} m-k \\ \\ \end{matrix}$$

Anwendung auf lineare Gleichungssysteme

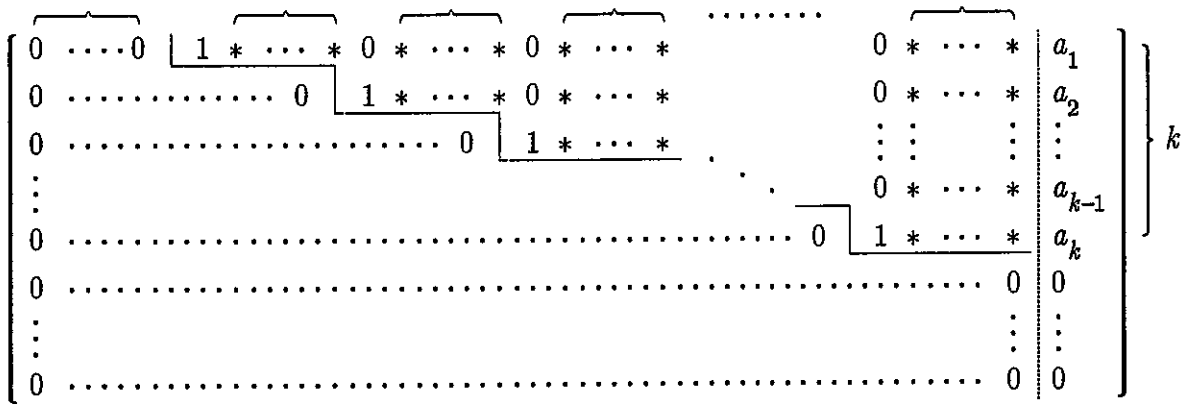
Wir wenden den Gaußschen Algorithmus auf ein lineares Gleichungssystem (*) mit der zugehörigen erweiterten Matrix $(A|b)$ an, und zwar zunächst so lange, bis die Matrix A Treppennormalform annimmt. Dann gehört zu dem umgeformten LGS (**) die erweiterte Matrix



Hieraus liest man ab:

Das LGS (**) und damit auch das LGS (*) ist unlösbar, falls einer der Koeffizienten $c_{k+1},\ldots,c_m$ von Null verschieden ist.

Ist $c_{k+1} = \cdots = c_m = 0$, so können wir das LGS (**) weiter umformen, bis die zugehörige Matrix Gaußsche Normalform hat. Die erweiterte Matrix ist dann von der Gestalt



Hieraus liest man wieder ab:

Das LGS (*) ist lösbar. Die durch geschweifte Klammern gekennzeichneten $(n-k)$ Spalten entsprechen den $(n-k)$ Unbekannten des linearen Gleichungssystems, die frei wählbar sind. Die restlichen k Unbekannten lassen sich dann direkt ausrechnen, und wir erhalten so die allgemeine Lösung des LGS (*). Insbesondere gilt:

Satz 18. *Ein homogenes LGS, das mehr Unbekannte als Gleichungen besitzt* $(m < n)$, *ist immer nichttrivial lösbar.*

Beweis. Es ist $k \leq m$. Also gibt es $n-k \geq n-m > 0$ frei wählbare Variablen. ∎

Beispiel. Wir betrachten das folgende lineare Gleichungssystem über $\mathbb{R}$

$$\begin{aligned} 2x_1 + 4x_2 - 2x_3 - 8x_4 &= 16 \\ x_1 \quad\quad - x_3 + 2x_4 &= 2 \\ 3x_4 &= -6 \\ 2x_1 - 2x_2 - 2x_3 &= 18 \end{aligned}$$

und wenden den Gaußschen Algorithmus auf die zugehörige erweiterte Matrix an:

$$\left[\begin{array}{cccc|c} 2 & 4 & -2 & -8 & 16 \\ 1 & 0 & -1 & 2 & 2 \\ 0 & 0 & 0 & 3 & -6 \\ 2 & -2 & -2 & 0 & 18 \end{array}\right] \begin{array}{l} \cdot\frac{1}{2} \\ \\ \\ \end{array} \begin{array}{l} \rfloor \\ \rfloor -1 \\ \\ \rfloor -2 \end{array} \longrightarrow \left[\begin{array}{cccc|c} 1 & 2 & -1 & -4 & 8 \\ 0 & -2 & 0 & 6 & -6 \\ 0 & 0 & 0 & 3 & -6 \\ 0 & -6 & 0 & 8 & 2 \end{array}\right] \begin{array}{l} \\ \cdot(-\frac{1}{2}) \\ \\ \rfloor 6 \end{array}$$

Treppennormalform:

$$\longrightarrow \left[\begin{array}{cccc|c} 1 & 2 & -1 & -4 & 8 \\ 0 & 1 & 0 & -3 & 3 \\ 0 & 0 & 0 & 3 & -6 \\ 0 & 0 & 0 & -10 & 20 \end{array}\right] \begin{array}{l} \\ \\ \cdot\frac{1}{3} \\ \rfloor 10 \end{array} \longrightarrow \left[\begin{array}{cccc|c} \underline{1} & 2 & -1 & -4 & 8 \\ 0 & \underline{1} & 0 & -3 & 3 \\ 0 & 0 & 0 & \underline{1} & -2 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right] \begin{array}{l} \\ \\ \rfloor 3 \\ \rfloor 4 \end{array}$$

Normalform:

$$\longrightarrow \left[\begin{array}{cccc|c} 1 & 2 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -3 \\ 0 & 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right] \begin{array}{l} \rfloor \\ \\ \\ \rfloor -2 \end{array} \longrightarrow \left[\begin{array}{cccc|c} \underline{1} & 0 & -1 & 0 & 6 \\ 0 & \underline{1} & 0 & 0 & -3 \\ 0 & 0 & 0 & \underline{1} & -2 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

Daraus liest man als allgemeine Lösung des linearen Gleichungssystems ab:

$$\begin{aligned} x_4 &= -2 \\ x_3 &= s \\ x_2 &= -3 \\ x_1 &= 6 + s \end{aligned} \quad , s \in \mathbb{R}.$$

Anwendung auf n–reihige quadratische Matrizen

Wir wollen mit Hilfe des Gaußschen Algorithmus prüfen, ob eine Matrix regulär ist und gegebenenfalls ihre Inverse berechnen. Dazu zeigen wir

Satz 19. *Es sei $A \in \mathbb{K}^{n\times n}$. Hat die Matrix $(A|E_n)$ die Gaußsche Normalform $(E_n|A')$, so ist A regulär und A' ist die zu A inverse Matrix.*

Beweis. Wir bezeichnen die k–te Spalte von A' bzw. E_n mit a_k' bzw. e_k $(k = 1,...,n)$. Geht nun $(A|E_n)$ bei den elementaren Zeilenumformungen in die Normalform $(E_n|A')$ über, so bedeutet dies für die n linearen Gleichungssysteme mit den zugehörigen erweiterten Matrizen $(A|e_1),...,(A|e_n)$, daß sie eindeutig lösbar sind und weiter, daß $a_1',...,a_n'$ die entsprechenden Lösungen sind. Also gilt $AA' = E_n$.

Machen wir die obigen Elementarumformungen wieder rückgängig, so geht die Matrix $(E_n|A')$ wieder über in $(A|E_n)$. Da es bei den elementaren Zeilenumformungen nicht auf die Reihenfolge der Spalten ankommt, bedeutet dies, daß die Matrix $(A'|E_n)$ übergeht in die Matrix $(E_n|A)$. Also gilt nach den obigen Überlegungen $A'A = E_n$. Somit ist A regulär und die Inverse ist A'. ∎

Es gilt auch die Umkehrung dieses Satzes:

Ist $A \in \mathbb{K}^{n\times n}$ regulär mit $A^{-1} = A'$, so hat die Matrix $(A|E_n)$ die Gaußsche Normalform $(E_n|A')$.

Den Beweis überlassen wir als Übungsaufgabe.

Beispiel. Gegeben sei die Matrix

$$A = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 2 & 1 \\ 0 & -1 & 0 & 1 \\ 1 & 0 & 0 & 2 \end{bmatrix} \in \mathbb{R}^{4\times 4}.$$

Wir wenden den Gaußschen Algorithmus auf die Matrix $(A|E_4)$ an und erhalten

$$\left[\begin{array}{cccc|cccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 2 & 1 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 2 & 0 & 0 & 0 & 1 \end{array}\right] \longrightarrow \cdots \longrightarrow \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 2 & -1 & -1 & 0 \\ 0 & 1 & 0 & 0 & -1 & 1/2 & -1/2 & 1/2 \\ 0 & 0 & 1 & 0 & 0 & 1/2 & 1/2 & -1/2 \\ 0 & 0 & 0 & 1 & -1 & 1/2 & 1/2 & 1/2 \end{array}\right]$$

Also ist A regulär, und es gilt

$$A^{-1} = \begin{bmatrix} 2 & -1 & -1 & 0 \\ -1 & 1/2 & -1/2 & 1/2 \\ 0 & 1/2 & 1/2 & -1/2 \\ -1 & 1/2 & 1/2 & 1/2 \end{bmatrix}$$

Wir wenden nun Satz 19 und dessen Umkehrung auf *obere* bzw. *untere Dreiecksmatrizen* an. Darunter verstehen wir quadratische Matrizen, bei denen unterhalb bzw. oberhalb der Diagonalen nur Nullen stehen. Die Einzelheiten überlassen wir wieder als Übungsaufgabe:

Eine obere (untere) Dreiecksmatrix A ist genau dann regulär, wenn die Diagonalelemente von A alle von Null verschieden sind. Die inverse Matrix A^{-1} ist dann ebenfalls eine obere (untere) Dreiecksmatrix.

Da das Produkt zweier oberer (unterer) Dreiecksmatrizen wieder eine obere (untere) Dreiecksmatrix ist, bilden die regulären oberen (unteren) Dreiecksmatrizen eine Untergruppe der allgemeinen linearen Gruppe $GL(n,\mathbb{K})$.

Zum Abschluß dieses Paragraphen machen wir noch zwei Bemerkungen über lineare Gleichungssysteme.

Bemerkungen. **(a)** Ist A eine reguläre quadratische Matrix, so ist das lineare Gleichungssystem $Ax = b$ eindeutig lösbar, denn es gilt in diesem Fall $x = A^{-1}b$.

(b) Es seien L_{inh} die Lösungsmenge des inhomogenen LGS $Ax = b$ und $\tilde{x}$ eine beliebige Lösung. Ist L_h die Lösungsmenge des zugehörigen homogenen LGS $Ax = o$, so gilt

$$L_{inh} = \tilde{x} + L_h := \{ \tilde{x} + y \mid y \in L_h \}.$$

Damit lassen sich die Lösungsmengen der Beispiele von S.70 bzw. von S.77 nun folgendermaßen darstellen:

$$L_{inh} = \{\begin{bmatrix} 2+2t+2s \\ t \\ -1-s \\ 1+2s \\ s \end{bmatrix} \mid s,t \in \mathbb{R}\} = \begin{bmatrix} 2 \\ 0 \\ -1 \\ 1 \\ 0 \end{bmatrix} + \{s \begin{bmatrix} 2 \\ 0 \\ -1 \\ 2 \\ 1 \end{bmatrix} + t \begin{bmatrix} 2 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \mid s,t \in \mathbb{R}\}$$

bzw.

$$L_{inh} = \{\begin{bmatrix} 6+s \\ -3 \\ s \\ -2 \end{bmatrix} \mid s \in \mathbb{R}\} = \begin{bmatrix} 6 \\ -3 \\ 0 \\ -2 \end{bmatrix} + \{s \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} \mid s \in \mathbb{R}\}.$$

Die weitere Behandlung linearer Gleichungssysteme wird im Rahmen der Vektorraumtheorie in den nächsten Kapiteln erfolgen.

§ 6 Anwendungen der Kongruenzrechnung

In § 3 haben wir die Restklassenringe $\mathbb{Z}_m$ eingeführt und bewiesen, daß sie genau dann Körper sind, wenn $m \in \mathbb{N}$ eine Primzahl ist. Sie spielen in vielen Anwendungen eine wichtige Rolle. So führt z.B. die Frage, auf welchen Wochentag ein bestimmtes Datum fällt, auf den Ring $\mathbb{Z}_7$, und wenn in der Datenverarbeitung nur eine begrenzte Anzahl von Symbolen zur Verfügung steht, werden Rechnungen in einem der Ringe $\mathbb{Z}_m$ erforderlich.

Wir wollen im folgenden zwei Problemstellungen behandeln und verwenden dazu wieder die klassische Kongruenzschreibweise

$$x \equiv y \bmod m$$

für $x - y \in m\,\mathbb{Z}$, d.h. für $[x]_\sim = [y]_\sim$ in $\mathbb{Z}_m$.

(1) Zu gegebenen $a \in \mathbb{Z}$, $n \in \mathbb{N}$ und $m \in \mathbb{N}$ wird ein $x \in \{0,1,\ldots,m-1\}$ gesucht mit

$$a^n \equiv x \bmod m.$$

Während man für Zahlen $a \in \mathbb{Z}$, auch wenn sie sehr groß sind, leicht ausrechnen kann, welcher Rest bei Division durch m bleibt, ist dies bei Potenzen a^n wesentlich schwieriger. Wie sieht man z.B. der Zahl 4^{10259} an, welchen Rest sie bei Division durch 18 hat?

(2) Es soll ein System von k Kongruenzen gelöst werden. Zu gegebenen Zahlen $k \in \mathbb{N}$, $a_1,\ldots,a_k \in \mathbb{N}_0$, $m_1,\ldots,m_k \in \mathbb{N}$ wird ein $x \in \mathbb{N}_0$ gesucht mit

$$\begin{aligned} x &\equiv a_1 \bmod m_1 \\ x &\equiv a_2 \bmod m_2 \\ &\vdots \\ x &\equiv a_k \bmod m_k \end{aligned}$$

Offensichtlich spielen bei der Behandlung solcher Fragen die Teilbarkeitseigenschaften ganzer Zahlen eine wesentliche Rolle. Einige dieser Eigenschaften haben wir schon in § 1.4 bei den Polynomen benutzt. Zum besseren Verständnis wol-

len wir hier nochmals einige grundlegende Tatsachen zusammenstellen (zum Teil ohne Beweis), soweit wir sie zur Behandlung der Probleme (1) und (2) benötigen.

Division mit Rest. *Für $a,b \in \mathbb{Z}$, $b \neq 0$, gibt es eindeutig bestimmte Zahlen $k \in \mathbb{Z}$ und $r \in \{0,1,\ldots,|b|-1\}$ mit*

$$(*) \qquad a = k\,b + r\,.$$

Ist $r = 0$, so ist b *Teiler* von a und wir schreiben dann $b \mid a$ (b teilt a). Die größte Zahl $d \in \mathbb{N}$, die sowohl a als auch b teilt, heißt *größter gemeinsamer Teiler* von a und b. Schreibweise: $d = \mathrm{ggT}\,(a,b)$. Ist $\mathrm{ggT}\,(a,b) = 1$, so heißen a und b *teilerfremd*.

Zur Ermittlung des ggT von a und b dient der *Euklidische Algorithmus* :

Durch mehrfache Anwendung von (*) erhält man:

$$\begin{aligned}
a &= kb + r && , && r \in \{0,\ldots,|b|-1\}\\
b &= k_1 r + r_1 && , && r_1 \in \{0,\ldots,r-1\}\\
r &= k_2 r_1 + r_2 && , && r_2 \in \{0,\ldots,r_1-1\}\\
&\vdots && && \vdots\\
r_{j-2} &= k_j\, r_{j-1} + r_j\,, && && r_j \in \{0,\ldots,r_{j-1}-1\}\\
r_{j-1} &= k_{j+1} r_j\,. && &&
\end{aligned}$$

Das Verfahren bricht ab, weil $r, r_1, r_2, \ldots$ eine monoton fallende Folge von Zahlen aus $\mathbb{N}_0$ ist.

Satz 20. Es gilt: $r_j = \mathrm{ggT}\,(a,b)$.

Beweis. Wir zeigen zunächst, daß r_j ein Teiler von a und von b ist, indem wir den Euklidischen Algorithmus von unten nach oben durchlaufen:

$$\begin{aligned}
&r_j \text{ teilt } r_{j-1} \Rightarrow r_j \text{ teilt } r_{j-2} \Longrightarrow r_j \text{ teilt } r_{j-3}\\
\Longrightarrow \cdots \Longrightarrow\ & r_j \text{ teilt } r \Longrightarrow r_j \text{ teilt } b \Longrightarrow r_j \text{ teilt } a\,.
\end{aligned}$$

Sei nun $c \in \mathbb{N}$ ein Teiler von a und b. Dann folgt analog, wenn wir das Verfahren von oben nach unten durchlaufen:

$$c \text{ teilt } r \Rightarrow c \text{ teilt } r_1 \Rightarrow \cdots \Rightarrow c \text{ teilt } r_{j-2} \Rightarrow c \text{ teilt } r_{j-1} \Rightarrow c \text{ teilt } r_j .$$

Also ist $c \leq r_j$ und somit $r_j = \text{ggT}\,(a,b)$. ∎

Beispiel. Wir wollen den ggT von 24 und 614 bestimmen:

$$\begin{aligned} 614 &= 25 \cdot 24 + 14 \\ 24 &= 1 \cdot 14 + 10 \\ 14 &= 1 \cdot 10 + 4 \\ 10 &= 2 \cdot 4 + 2 \\ 4 &= 2 \cdot 2 \end{aligned}$$

Also ist ggT (24,614) = 2.

Mit Hilfe des Euklidischen Algorithmus erhalten wir folgendes Kriterium für die Teilerfremdheit ganzer Zahlen.

Satz 21. *Die Zahlen $a,b \in \mathbb{Z}$ sind genau dann teilerfremd, wenn es Zahlen $x,y \in \mathbb{Z}$ gibt mit $a\,x + b\,y = 1$.*

Beweis. Sei ggT $(a,b) = 1$. Lösen wir im Euklidischen Algorithmus die Gleichungen nacheinander nach $r, r_1, r_2, \ldots, r_{j-1}$ und $r_j = 1$ auf, so erhalten wir

$$r = a - k\,b \;,\; r_1 = x_1\,a + y_1\,b \;,\cdots,\; 1 = r_j = x_j\,a + y_j\,b$$

mit $x_i\,,\; y_i \in \mathbb{Z}$.

Gilt umgekehrt $a\,x + b\,y = 1$, und ist ggT $(a,b) = m \in \mathbb{N}$, so folgt $a = u \cdot m$, $b = v \cdot m$ mit $u,v \in \mathbb{N}$ und somit $(x\,u + y\,v)\,m = 1$. Also ist $m = 1$. ∎

Wir wollen einige Folgerungen aus Satz 21 ziehen.

Folgerungen. **(a)** *Für $a,b,c \in \mathbb{Z}$ mit* ggT $(a,b) = 1$, ggT $(a,c) = 1$ *folgt* ggT $(a,bc) = 1$.

Beweis. Nach Satz 21 gilt $a\,u + b\,v = 1$ und $a\,x + c\,y = 1$ mit $u,v,x,y \in \mathbb{Z}$. Daraus folgt $a\,(a\,u\,x + c\,u\,y + b\,v\,x) + b\,c\,v\,y = 1$ und somit nach Satz 21 die Behauptung. ∎

(b) *Für $a,b,c \in \mathbb{Z}$ mit $a \mid bc$ und* ggT $(a,b) = 1$ *folgt* $a \mid c$.

Beweis. Nach Voraussetzung und nach Satz 21 gilt $a\,z = b\,c$ sowie $a\,x + b\,y = 1$ mit

geeigneten $x,y,z \in \mathbb{Z}$. Daraus folgt $a\,z\,y - b\,c\,y = 0$ und $a\,x\,c + b\,y\,c = c$. Wir addieren beide Gleichungen und erhalten $a\,(z\,y + x\,c) = c$, also $a \mid c$. ∎

(c) *Für $m \in \mathbb{N}$, $a,x,y \in \mathbb{Z}$ mit* ggT $(a,m) = 1$ *und* $a\,x \equiv a\,y \bmod m$ *folgt* $x \equiv y \bmod m$.

Beweis. Aus $a\,x \equiv a\,y \bmod m$ folgt $a\,(x - y) = z\,m$ mit $z \in \mathbb{Z}$. Wegen $a \mid z\,m$ und ggT $(a,m) = 1$ erhalten wir unter Verwendung von (b), daß $z = z'\,a$ mit $z' \in \mathbb{Z}$ gilt. Somit folgt $x - y = z'\,m$ und $x \equiv y \bmod m$. ∎

(d) *Für $x,y \in \mathbb{Z}$, $m \in \mathbb{N}$ mit* ggT $(x,m) = 1$ *und* $x \equiv y \bmod m$ *folgt* ggT $(y,m) = 1$.

Beweis. Nach Satz 21 gibt es ganze Zahlen u,v mit $u\,x + v\,m = 1$, und nach Voraussetzung ist $x - y = z\,m$ mit $z \in \mathbb{Z}$. Damit erhalten wir $u\,(y + z\,m) + v\,m = 1$ und weiter $u\,y + (u\,z + v)\,m = 1$. Also folgt wieder mit Satz 21, daß ggT $(y,m) = 1$. ∎

(e) *Für $x,y \in \mathbb{Z}$, $m_1,m_2 \in \mathbb{N}$ mit* ggT $(m_1,m_2) = 1$ *und* $x \equiv y \bmod m_1$, $x \equiv y \bmod m_2$ *folgt* $x \equiv y \bmod m_1 m_2$.

Beweis. Es gilt nach Voraussetzung $x - y = z_1 m_1$ und $x - y = z_2 m_2$ mit $z_1,z_2 \in \mathbb{Z}$. Daraus folgt $z_1 m_1 = z_2 m_2$ und wegen (b) $m_1 \mid z_2$, $m_2 \mid z_1$. Somit gilt $z_2 = z_2'\,m_1$, $z_2' \in \mathbb{Z}$ und $x - y = z_2'\,m_1\,m_2$. Also ist $x \equiv y \bmod m_1 m_2$. ∎

Definition. Für $m \in \mathbb{N}$ sei

$$\varphi\,(m) := |\{k \in \{1,\ldots,m\} \mid \text{ggT}\,(k,m) = 1\}|.$$

Die Abbildung $\varphi : m \longmapsto \varphi\,(m)$ heißt *Eulersche φ–Funktion.*

Für $m \in \mathbb{N}$ gibt es also $\varphi\,(m)$ Zahlen $x_1,\ldots,x_{\varphi(m)} \in \{1,\ldots,m\}$, die zu m teilerfremd sind. Deren Restklassen in $\mathbb{Z}_m$ bilden bezüglich der Multiplikation eine Gruppe. Dies ist die Aussage des nächsten Satzes.

Satz 22. *Es sei $m \in \mathbb{N}$, $x_1,\ldots,x_{\varphi(m)}$ seien die zu m teilerfremden Zahlen aus $\{1,\ldots,m\}$ und $B = \{[x_1]_\sim,\ldots,[x_{\varphi(m)}]_\sim\} \subset \mathbb{Z}_m$. Dann ist $(B,\cdot)$ eine abelsche Gruppe.*

Beweis. B ist bezüglich der Multiplikation abgeschlossen, denn aus $[x_i]_\sim \in B$, $[x_j]_\sim \in B$ mit $x_i,x_j \in \{1,\ldots,m\}$ folgt nach (a), daß $x_i\,x_j$ teilerfremd zu m ist, und nach

(d) überträgt sich dies auf die Elemente der Restklasse $[x_i\, x_j]_\sim$, die somit ebenfalls zu B gehört. Weiterhin besitzt jede Restklasse $[x_i]_\sim$, $i = 1,\ldots,\varphi(m)$, auch eine Inverse bezüglich der Multiplikation. Denn zu x_i gibt es nach Satz 21 $z,y \in \mathbb{Z}$ mit $m\,z + y\,x_i = 1$. Also ist y teilerfremd zu m und $[y]_\sim \in \{[x_1]_\sim,\ldots,[x_{\varphi(m)}]_\sim\}$. Aus der obigen Darstellung der Eins folgt nun

$$[1]_\sim = [m\,z + y\,x_i]_\sim = [m\,z]_\sim + [y\,x_i]_\sim = [0]_\sim + [y]_\sim\,[x_i]_\sim = [y]_\sim\,[x_i]_\sim .$$

Also ist $[y]_\sim = [x]_\sim^{-1}$. Schließlich sind in $(B,\cdot)$ auch die restlichen Gruppenaxiome erfüllt, da $\mathbb{Z}_m$ ein kommutativer Ring mit Eins ist. ∎

Aus Satz 22 erhalten wir ein erstes Resultat zur Lösung von Problem (1).

Korollar 23 (Satz von Fermat–Euler). *Es seien a und m teilerfremde natürliche Zahlen. Dann gilt:*

$$a^{\varphi(m)} \equiv 1 \bmod m .$$

Beweis. Die abelsche Gruppe B aus Satz 22 besitzt genau $\varphi(m)$ Elemente $[x_1]_\sim,\ldots,[x_{\varphi(m)}]_\sim$, und $[a]_\sim$ ist in B. Weil $[x_1]_\sim\,[a]_\sim,\ldots,[x_{\varphi(m)}]_\sim\,[a]_\sim$ in B und paarweise verschieden sind, ist das Produkt dieser Elemente gleich $[x_1]_\sim\cdots[x_{\varphi(m)}]_\sim$. Daraus folgt $[a]_\sim^{\varphi(m)} = [1]_\sim$ und somit $[a^{\varphi(m)}]_\sim = [1]_\sim$. ∎

Um dieses Ergebnis zur Lösung von (1) einsetzen zu können, benötigen wir noch eine Darstellung von $\varphi(m)$, die eine Berechnung dieser Funktion erlaubt. Dazu wollen wir die Zahl m zunächst in Primfaktoren zerlegen.

Satz 24. *Jede natürliche Zahl $m > 1$ ist Produkt endlich vieler Primzahlen.*

Beweis: Ist m eine Primzahl, so ist die Behauptung trivial. Andernfalls ist $m \geq 4$ und wir erhalten durch vollständige Induktion mit dem Induktionsanfang $m = 4 = 2\cdot 2$ sofort die Behauptung. ∎

Für jede natürliche Zahl $m \geq 2$ gibt es also eine Primzahldarstellung

$$m = p_1^{n_1} \cdots p_k^{n_k} ,$$

wobei $k \in \mathbb{N}$, $p_1,\ldots,p_k$ paarweise verschiedene Primzahlen und $n_1,\ldots,n_k \in \mathbb{N}$ sind. Diese Darstellung ist bis auf die Reihenfolge der Faktoren eindeutig, wie man mit Hilfe von Folgerung (b) leicht beweist.

Weiterhin ist jeder nichttriviale Teiler von m ebenfalls Produkt von Primzahlen aus $\{p_1,\ldots,p_k\}$. Damit besitzt jede Zahl $k \in \{1,\ldots,m\}$, die nicht teilerfremd zu m ist, mindestens eine der Primzahlen $p_1,\ldots,p_k$ als Teiler, ist also Element einer der Mengen

$$A_i = \{1,\ldots,m\} \cap p_i \mathbb{N} \quad , \quad 1 \leq i \leq k \, .$$

Es gibt daher genau

$$m - \varphi(m) = |\bigcup_{i=1}^{k} A_i|$$

Zahlen aus $\{1,\ldots,m\}$, die nicht zu m teilerfremd sind. Nun nutzen wir Satz 3 der Vorbemerkungen über Mengen, Abbildungen, Relationen aus. Wir wissen

$$|A_i| = \frac{m}{p_i} \, , \qquad 1 \leq i \leq k \, ,$$

$$|A_i \cap A_j| = \frac{m}{p_i \cdot p_j} \, , \qquad 1 \leq i < j \leq k \, ,$$

$$\vdots$$

$$|A_{i_1} \cap \cdots \cap A_{i_{k-1}}| = \frac{m}{p_{i_1} \cdots p_{i_{k-1}}} \, , \qquad 1 \leq i_1 < \cdots < i_{k-1} \leq k \, ,$$

$$|A_1 \cap \cdots \cap A_k| = \frac{m}{p_1 \cdots p_k} \, .$$

Das ergibt

$$m - \varphi(m) = \sum_{i=1}^{k} \frac{m}{p_i} - \sum_{1 \leq i < j \leq k} \frac{m}{p_i \cdot p_j} + - \cdots + (-1)^{k+1} \frac{m}{p_1 \cdots p_k}$$

$$\varphi(m) = m \left(1 - \sum_{i=1}^{k} \frac{1}{p_i} + \sum_{1 \leq i < j \leq k} \frac{1}{p_i \cdot p_j} - + \cdots + (-1)^k \frac{1}{p_1 \cdots p_k}\right)$$

$$= m\,(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_k}).$$

Dies ist die gewünschte Darstellung von φ und wir erhalten den folgenden Satz:

Satz 25. *Sei $m \in \mathbb{N}$ und seien $p_1,\ldots,p_k$ die Primzahlen, die m teilen. Dann gilt :*

$$\varphi\,(m) \;=\; m\,(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_k})\,.$$

Beispiel. Für welches $x \in \{1,2,\ldots,14\}$ gilt $4^{10259} \equiv x \bmod 15$?

Es ist $\varphi\,(15) = 15(1-\frac{1}{5})(1-\frac{1}{3}) = 8$. Wegen $2^8 \equiv 1 \bmod 15$ und $4^{10259} = 2^{20518}$ $= (2^8)^{2564}\cdot 2^6$ folgt $4^{10259} \equiv 2^6 \bmod 15$. Also ist $x \equiv 2^6 \bmod 15$ und somit $x = 4$ die gesuchte Lösung.

Nun wenden wir uns Problem (2) zu und betrachten das System von Kongruenzen

$$(*)\qquad \begin{array}{l} x \equiv a_1 \bmod m_1 \\ \quad\vdots \qquad\quad \vdots \\ x \equiv a_k \bmod m_k \end{array} \qquad\qquad a_i \in \{0,1,\ldots,m_i-1\}.$$

Die Herleitung allgemeiner Lösungskriterien gehört zum Bereich der Zahlentheorie, weswegen wir uns hier auf den wichtigen Spezialfall beschränken, daß $m_1,\ldots,m_k$ paarweise teilerfremd sind.

Satz 26 (Chinesischer Restsatz). *Sind $m_1,\ldots,m_k$ paarweise teilerfremd, so hat (*) die Lösung*

$$x \;=\; m_1\cdots m_k \sum_{i=1}^{k} n_i \frac{a_i}{m_i}\,.$$

Dabei ist $n_i \in \{0,\ldots,m_i-1\}$ eindeutig durch

$$n_i \frac{m_1\cdots m_k}{m_i} \equiv 1 \bmod m_i$$

gegeben, $i = 1,\ldots,k$. Ist y eine weitere Lösung von (*), so gilt $y = x + k\,m_1\cdots m_k$, $k \in \mathbb{Z}$.

Beweis. Sei $i \in \{1,...,k\}$. Wiederholte Anwendung von Folgerung (a) ergibt, daß m_i und $\frac{m_1 \cdot \cdots \cdot m_k}{m_i}$ teilerfremd sind. Nach Satz 21 existieren dann Zahlen x_i , $y_i \in \mathbb{Z}$ mit

$$x_i\, m_i + \frac{m_1 \cdot \cdots \cdot m_k}{m_i}\, y_i = 1,$$

woraus

$$\frac{m_1 \cdot \cdots \cdot m_k}{m_i}\, y_i \equiv 1 \bmod m_i$$

folgt. Sei n_i die eindeutige Zahl aus $\{0,...m_i\text{–}1\}$, die $n_i \equiv y_i \bmod m_i$ erfüllt. Wir erhalten

$$\frac{m_1 \cdot \cdots \cdot m_k}{m_i}\, n_i \equiv 1 \bmod m_i\,,$$

und für

$$x = m_1 \cdot \cdots\, m_k \sum_{i=1}^{k} n_i \frac{a_i}{m_i}$$

gilt dann

$$x \equiv n_i\, a_i \frac{m_1 \cdot \cdots \cdot m_k}{m_i} \bmod m_i\,,$$

also

$$x \equiv a_i \bmod m_i\,, \quad i = 1,...,k\,.$$

Damit ist x Lösung von (*). Ist $y \in \mathbb{Z}$ ebenfalls Lösung von (*), so folgt $y \equiv x \bmod m_i$, $i = 1,...,k$, und weil die m_i teilerfremd sind, erhalten wir mit Folgerung (e) von Satz 21 $y \equiv x \bmod (m_1 \cdot \cdots \cdot m_k)$. ∎

Bemerkungen. **(a)** Der Beweis war konstruktiv, erlaubt also die Bestimmung von x . Zur Berechnung der n_i kann dabei Satz 25 und Korollar 23 benutzt werden. Danach ist ja

$$\frac{m_1 \cdot \cdots \cdot m_k}{m_i} \cdot \left(\frac{m_1 \cdot \cdots \cdot m_k}{m_i}\right)^{\varphi(m_i)-1} \equiv 1 \bmod m_i\,,$$

also

$$n_i \equiv \left(\frac{m_1 \cdot \ldots \cdot m_k}{m_i}\right)^{\varphi(m_i)-1} \bmod m_i .$$

(b) Satz 26 besagt, daß jede Zahl $x \in \{0,1,\ldots,m_1 \cdot \ldots \cdot m_k - 1\}$ in eindeutiger Weise durch das k–Tupel $(a_1,\ldots,a_k)$ dargestellt wird. Solche Zahlendarstellungen sind für die Informatik interessant, weil sich die Rechenoperationen + und · auf die einzelnen "Koordinaten" übertragen.

Beispiel. Wir suchen das kleinste $x \in \mathbb{N}$ mit

$$\begin{aligned} x &\equiv 5 \bmod 7 \\ x &\equiv 7 \bmod 11 \\ x &\equiv 3 \bmod 13. \end{aligned}$$

Es ist $m_1 = 7$, $m_2 = 11$, $m_3 = 13$, also $m_1 \cdot m_2 \cdot m_3 = 1001$. Weiterhin gilt $\varphi(m_1) = 6$, $\varphi(m_2) = 10$ und $\varphi(m_3) = 12$. Damit erhalten wir für die Zahlen n_1, n_2, n_3

$$n_1 \equiv (11 \cdot 13)^5 \equiv (4 \cdot 6)^5 \equiv 3^5 \equiv 5 \bmod 7, \text{ da } 3^6 \equiv 1 \bmod 7$$

$$n_2 \equiv (7 \cdot 13)^9 \equiv (7 \cdot 2)^9 \equiv 3^9 \equiv 4 \bmod 11, \text{ da } 3^{10} \equiv 1 \bmod 11$$

$$n_3 \equiv (7 \cdot 11)^{11} \equiv 12^{11} \equiv 12 \bmod 13, \text{ da } 12^{12} \equiv 1 \bmod 13,$$

also $n_1 = 5$, $n_2 = 4$, $n_3 = 12$, und für x ergibt sich

$$x \equiv 5 \cdot 5 \cdot 11 \cdot 13 + 4 \cdot 7 \cdot 7 \cdot 13 + 12 \cdot 3 \cdot 7 \cdot 11 \equiv 8895 \equiv 887 \bmod 1001.$$

Somit ist $x = 887$ und diese Zahl wird durch das Tripel (5,7,3) dargestellt.

Kapitel 2 Vektorräume

§ 1 Vektorräume und Untervektorräume

Bisher haben wir algebraische Strukturen betrachtet, bei denen innere Verknüpfungen, also Abbildungen $A \times A \longrightarrow A$ auf der Grundmenge A eine Rolle spielten. Nun wenden wir uns Mengen zu, auf denen neben einer inneren Verknüpfung (Addition) auch eine äußere Verknüpfung (Skalarmultiplikation) erklärt ist. Solche Mengen haben wir in Kapitel 1 mit dem Ring $\mathbb{K}^{n\times n}$ der Matrizen, dem Polynomring $\mathbb{K}[x]$ und den Lösungsmengen L_h homogener linearer Gleichungssysteme schon kennengelernt. Es sind erste Beispiele für den zentralen Begriff der linearen Algebra, den Vektorraum.

Definition. Es sei $\mathbb{K}$ ein Körper. Ein $\mathbb{K}$*–Vektorraum* oder auch *Vektorraum über dem Körper* $\mathbb{K}$ ist eine Menge V zusammen mit zwei Abbildungen $+ : V \times V \longrightarrow V$ und $\cdot : \mathbb{K} \times V \longrightarrow V$, wobei folgende Gesetze gelten:

(a) $(V,+)$ ist eine abelsche Gruppe,

(b) $a\cdot(x+y) = a\cdot x + a\cdot y$ für alle $a \in \mathbb{K}$, $x,y \in V$,

(c) $(a+b)\cdot x = a\cdot x + b\cdot x$ für alle $a,b \in \mathbb{K}$, $x \in V$,

(d) $a\cdot(b\cdot x) = (ab)\cdot x$ für alle $a,b \in \mathbb{K}$, $x \in V$,

(e) $1\cdot x = x$ für alle $x \in V$.

Die Elemente von V heißen *Vektoren*, das Neutralelement von $(V,+)$ ist der *Nullvektor* und die innere Verknüpfung $+$ heißt *Vektoraddition*.

Die Elemente von $\mathbb{K}$ werden *Skalare* genannt und die "äußere" Verknüpfung $\cdot$ heißt *Multiplikation mit Skalaren* .

Bemerkungen und Bezeichnungen. **(a)** Im Fall $\mathbb{K} = \mathbb{R}$ sprechen wir von einem *reellen Vektorraum*, im Fall $\mathbb{K} = \mathbb{C}$ von einem *komplexen Vektorraum* . Spielt der Körper $\mathbb{K}$ keine Rolle, so sagt man statt $\mathbb{K}$–Vektorraum auch kurz Vektorraum (VR).

(b) Sowohl Vektoren als auch Skalare werden mit kleinen lateinischen Buchstaben bezeichnet, insbesondere der Nullvektor mit o. Aus dem Kontext ist zu erkennen, was Skalare und was Vektoren sind. Statt $a \cdot x$ schreiben wir einfacher $a\,x$.

(c) Das Axiom (e) hat den Zweck, die sogenannte triviale Multiplikation mit Skalaren auszuschließen, bei der $a\,x = o$ für jedes $x \in V$ und jeden Skalar $a \in \mathbb{K}$ gesetzt wird. Eine solche Definition würde zu keiner sinnvollen Theorie führen.

(d) Es seien $x_1,\ldots,x_k$ endlich viele Vektoren aus V. Dann heißt jeder Vektor der Form

$$a_1\,x_1 + \cdots + a_k\,x_k\,, \quad \text{Kurzschreibweise:} \quad \sum_{i=1}^{k} a_i\,x_i\,,$$

mit $a_1,\ldots,a_k \in \mathbb{K}$ eine *Linearkombination* der Vektoren $x_1,\ldots,x_k$.

Beispiele. **(a)** $V = \mathbb{K}^n$, $n \in \mathbb{N}$, ist mit den folgenden Verknüpfungen ein $\mathbb{K}$–Vektorraum:

Addition: $(a_1,\ldots,a_n) + (b_1,\ldots,b_n) := (a_1 + b_1,\ldots,a_n + b_n)$ für alle $(a_1,\ldots,a_n) \in \mathbb{K}^n$ und alle $(b_1,\ldots,b_n) \in \mathbb{K}^n$,

Multiplikation mit Skalaren: $c\,(a_1,\ldots,a_n) := (ca_1,\ldots,ca_n)$ für alle $c \in \mathbb{K}$, $(a_1,\ldots,a_n) \in \mathbb{K}^n$.

(b) $V = \mathbb{K}^{m\times n}$, $m,n \in \mathbb{N}$, ist mit den in § 1.4 erklärten Verknüpfungen ein $\mathbb{K}$–Vektorraum.

Man beachte, daß $\mathbb{K}^{m\times n}$ und $\mathbb{K}^{mn}$ bis auf die Schreibweise übereinstimmen.

Bemerkung zur Schreibweise. Die drei $\mathbb{K}$–Vektorräume $\mathbb{K}^n$, $\mathbb{K}^{1\times n}$ und $\mathbb{K}^{n\times 1}$ unterscheiden sich nur durch die Schreibweise ihrer Elemente. Es ist für das weitere praktisch, $\mathbb{K}^n$ und $\mathbb{K}^{n\times 1}$ zu identifizieren, d.h. zu erlauben, daß n–Tupel wahlweise auch als Spalten geschrieben werden können (*Spaltenvektoren*):

$$\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = (a_1,\ldots,a_n) \in \mathbb{K}^n.$$

Bei der Spaltenschreibweise lassen sich z.B. die Vektorraumverknüpfungen einfacher überblicken. Dagegen wollen wir $\mathbb{K}^{n\times 1}$ und $\mathbb{K}^{1\times n}$ auseinanderhalten, damit bei der Matrizenmultiplikation keine Mißverständnisse auftreten.

(c) Der Polynomring $\mathbb{K}[X]$ wird ein $\mathbb{K}$–Vektorraum, wenn die Multiplikation mit Skalaren komponentenweise erklärt wird:

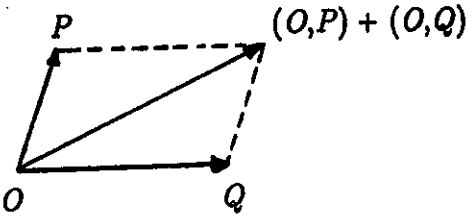
$$c\,(a_0,a_1,\ldots) := (ca_0,ca_1,\ldots) \text{ für alle } c \in \mathbb{K}, \text{ für alle } (a_0,a_1,\ldots) \in \mathbb{K}[X].$$

(d) Es seien A eine nichtleere Menge und $V = \mathbb{K}^A$. Erklären wir die Addition durch $(f,g) \longmapsto f+g$ mit $(f+g)(t) := f(t) + g(t)$ für alle $t \in A$ und die Multiplikation mit Skalaren durch $(a,f) \longmapsto af$ mit $(af)(t) := af(t)$ für alle $t \in A$, so ist V ein $\mathbb{K}$–Vektorraum.

(e) (leichte Verallgemeinerung von (d)) Es seien A eine nichtleere Menge und V ein $\mathbb{K}$–Vektorraum. Dann wird auch die Menge V^A mit analog erklärten Verknüpfungen ein $\mathbb{K}$–Vektorraum. Da $\mathbb{K}$ selbst ein $\mathbb{K}$–Vektorraum ist, erhält man für $V = \mathbb{K}$ wieder $\mathbb{K}^A$.

In den folgenden Beispielen legen wir den uns umgebenden Raum zugrunde und verwenden die Begriffe Punkt, Strecke, Länge, Richtung in ihrer anschaulichen Bedeutung. Eine gerichtete Strecke des Anschauungsraumes, zeichnerisch durch einen Pfeil symbolisiert und deshalb auch *Pfeil* genannt, ist durch ihren Anfangspunkt und ihre Spitze gekennzeichnet. Sie ist also nichts anderes als ein geordnetes Punktepaar.

Sei nun V die Menge aller Pfeile im Anschauungsraum mit einem beliebigen, aber festen Anfangspunkt O. Wir erklären die Addition zweier Pfeile mit Hilfe der "Parallelogrammregel"



und die Multiplikation mit Skalaren wie folgt.

Für $c > 0$ ist $c\,(O,P)$ der Pfeil mit Anfangspunkt O, c–facher Länge und gleicher Richtung wie (O,P), für $c < 0$ ist $c\,(O,P)$ der Pfeil mit Anfangspunkt O, $|c|$–facher Länge und entgegengesetzter Richtung wie (O,P) und für $c = 0$ ist $c\,(O,P)$ der Pfeil (O,O).

Damit wird V zu einem reellen Vektorraum. Seine Elemente heißen *Ortsvektoren.*

Die Menge aller physikalischen Kräfte, die an einem festen Punkt O angreifen, läßt sich durch diesen Vektorraum beschreiben.

Nun legen wir wieder den Anschauungsraum zugrunde, betrachten aber diesmal alle möglichen Pfeile. Dabei wollen wir zwei Pfeile (P,Q) und (R,S) als *gleich* (*äquivalent*) ansehen, wenn sie durch eine Parallelverschiebung (Translation) ineinander übergeführt werden können. Dies ist genau dann der Fall, wenn die Pfeile parallel, gleichlang und gleichgerichtet sind.

Die Punkte P des Anschauungsraums können als diejenigen speziellen Pfeile (P,P) aufgefaßt werden, bei denen Anfangspunkt und Spitze zusammenfallen. Jede Äquivalenzklasse $\overrightarrow{PQ}$ von Pfeilen heißt dann *Vektor* (*freier Vektor* im Gegensatz zu den Ortsvektoren).

Addition und Multiplikation mit Skalaren wird mit Hilfe geeigneter Pfeile wie bei den Ortsvektoren erklärt. Diese Definitionen sind unabhängig von der Wahl des Anfangspunktes O. Andere Anfangspunkte führen zu Figuren, die durch Parallelverschiebungen aus den alten hervorgehen.

Der so erklärte reelle Vektorraum heißt *Vektorraum der Pfeilklassen* oder der *freien Vektoren.* Er hat den Vorteil gegenüber dem Vektorraum der Ortsvektoren, daß man mit den freien Vektoren leichter rechnen kann. So gilt z.B. für beliebige Punkte P,Q,R des Anschauungsraumes die "Dreiecksgleichung" $\overrightarrow{PQ} + \overrightarrow{QR} + \overrightarrow{RP} = \overrightarrow{PP} = o$.

Bemerkung für Physiker. In der Physik treten viele Größen auf, wie z.B. Geschwindigkeit, Kraft, Impuls, elektrische und magnetische Feldstärke u.s.w., bei denen es

nicht genügt, ihre Größe bzw. Intensität durch eine einzige Zahl anzugeben, sondern bei denen auch die Angabe einer Richtung notwendig ist. Alle diese Größen werden von den Physikern meist als Vektoren bezeichnet. In unserem Sinn ist dies nicht immer ganz zutreffend. So sind z.B. zwei gleichgroße, gleichgerichtete Kräfte physikalisch gesehen durchaus etwas Verschiedenes, wenn sie an verschiedenen Punkten angreifen. Damit sind es aber weder Ortsvektoren noch freie Vektoren, sondern Pfeile.

Zur Einübung der Vektorraumaxiome wollen wir nun einige einfache Folgerungen beweisen.

Satz 1. *Es sei V ein $\mathbb{K}$–Vektorraum. Dann gilt*

(a) $a\,o = o$ *für alle* $a \in \mathbb{K}$,

(b) $0\,x = o$ *für alle* $x \in V$,

(c) *aus* $a\,x = o$ *folgt stets* $a = 0$ *oder* $x = o$,

(d) $(-1)\,x = -x$ *für alle* $x \in V$.

Beweis. (a) $a\,o = a\,(o + o) = a\,o + a\,o$. Daraus folgt $a\,o = o$.

(b) $0\,x = (0 + 0)\,x = 0\,x + 0\,x$. Daraus folgt $0\,x = o$.

(c) Aus $a\,x = o$, $a \neq 0$, folgt $o = a^{-1}(a\,x) = (a^{-1}a)\,x = 1 \cdot x = x$.

(d) Aus $o = 0x = (1 - 1)\,x = x + (-1)\,x$ folgt $(-1)\,x = -x$. ∎

Für den Rest dieses Paragraphen beschäftigen wir uns mit Teilmengen von Vektorräumen, die selbst wieder Vektorräume sind.

Definition. Es seien V ein $\mathbb{K}$–Vektorraum und $U \subset V$ eine nichtleere Teilmenge. U heißt *Untervektorraum* (Kurzschreibweise: UVR) von V oder (*linearer*) *Unterraum* oder *Teilraum*, wenn U mit den auf $U \times U$ bzw. $\mathbb{K} \times U$ eingeschränkten Abbildungen $+$ und $\cdot$ ein $\mathbb{K}$–Vektorraum ist.

Der Nachweis, daß eine Menge $U \subset V$ Untervektorraum ist, wird meist mit dem folgenden einfachen Kriterium geführt, das sich unmittelbar aus Satz 1.4 ergibt.

Satz 2. *Es seien V ein $\mathbb{K}$–Vektorraum und $U \subset V$. Genau dann ist U ein Untervektorraum von V, wenn U nichtleer ist und wenn für alle $x,y \in U$ und alle $a \in \mathbb{K}$ gilt: $x + y \in U$ und $a\,x \in U$.*

Beispiele. **(a)** Für jeden Vektorraum V sind V und $\{o\}$ triviale Untervektorräume von V.

(b) Die Lösungsmenge eines homogenen linearen Gleichungssystems über $\mathbb{K}$ mit n Unbekannten ist ein Untervektorraum von $\mathbb{K}^n$. Die Lösungsmenge eines inhomogenen linearen Gleichungssystems mit n Unbekannten ist dagegen kein Untervektorraum von $\mathbb{K}^n$.

(c) Es seien A eine nichtleere Menge und $t \in A$. Dann ist $\{f \in \mathbb{K}^A \mid f(t) = 0\}$ ein Untervektorraum von $\mathbb{K}^A$, aber $\{f \in \mathbb{K}^A \mid f(t) = 1\}$ ist kein Untervektorraum von $\mathbb{K}^A$.

Mit Hilfe von Satz 2 folgt unmittelbar:

Korollar 3. *Der Durchschnitt beliebig vieler Untervektorräume von V ist ein Untervektorraum von V.*

Nach diesem Korollar gibt es zu jeder Teilmenge $A \subset V$ einen "kleinsten" Untervektorraum von V, der A enthält, nämlich den Durchschnitt aller Untervektorräume von V, die A enthalten. Wir geben diesem neuen Untervektorraum einen besonderen Namen.

Definition. Es seien V ein $\mathbb{K}$–Vektorraum und $A \subset V$. Dann heißt

$$[A] := \bigcap_{\substack{U \text{ UVR von } V \\ A \subset U}} U$$

die *lineare Hülle* von A. Ist $A = \{x_1,\ldots,x_k\}$, so schreiben wir für $[A]$ auch $[x_1,\ldots,x_k]$ und sagen, daß die Vektoren $x_1,\ldots,x_k$ den Untervektorraum $[x_1,\ldots,x_k]$ *erzeugen* oder auch

aufspannen. Ist U ein Untervektorraum von V mit $U = [A]$, so heißt A *Erzeugendensystem* von U.

Beispiele. Die lineare Hülle des Vektorraumes V ist V selbst, die lineare Hülle der leeren Menge ist $\{o\}$ und die lineare Hülle eines Vektors $x \in V$ ist der Untervektorraum $\{a\,x \mid a \in \mathbb{K}\}$ von V.

Die lineare Hülle einer Teilmenge eines Vektorraumes läßt sich auch noch anders darstellen.

Satz 4. *Es seien V ein $\mathbb{K}$-Vektorraum und $\emptyset \neq A \subset V$. Dann ist $[A]$ die Menge aller Linearkombinationen von Vektoren aus A.*

Beweis. Sei U die Menge aller Linearkombinationen von Vektoren aus A. Mit Hilfe von Satz 2 überzeugt man sich leicht, daß U ein Untervektorraum von V ist. Wegen $A \subset U$ folgt somit $[A] \subset U$. Umgekehrt gilt $A \subset [A]$ und da $[A]$ ein Untervektorraum ist, folgt aus Satz 2 sofort, daß alle Linearkombinationen mit Vektoren aus A in $[A]$ liegen. Also gilt auch $U \subset [A]$. ∎

Bemerkung. Enthält A den Nullvektor, so benötigt man zur Beschreibung von $[A]$ nicht alle Linearkombinationen von Vektoren aus A, sondern nur diejenigen, bei denen die Summe der Koeffizienten konstant ist. Seien also $o \in A$ und $c \in \mathbb{K}$. Dann gilt:

$$[A] = \{ \sum_{i=1}^{k} a_i\, x_i \mid k \in \mathbb{N},\ a_1,\ldots,a_k \in \mathbb{K},\ x_1,\ldots,x_k \in A,\ \sum_{i=1}^{k} a_i = c \}\ .$$

Beweis. Die Menge rechts vom Gleichheitszeichen ist nach Satz 4 in $[A]$ enthalten. Umgekehrt liegt jede Linearkombination $x = a_1\, x_1 + \cdots + a_m\, x_m$ von Vektoren aus A wegen $x = a_1\, x_1 + \cdots + a_m\, x_m + (c - a_1 - \cdots - a_m)\, o$ auch in der rechten Menge. Also gilt Gleichheit. ∎

§ 2 Lineare Abhängigkeit und Unabhängigkeit

Der Nullvektor läßt sich stets als Linearkombination von k Vektoren $x_1,\dots,x_k$ darstellen, denn es gilt immer $o = 0\ x_1 + \cdots + 0\ x_k$. Gibt es neben dieser trivialen Linearkombination auch eine nichttriviale $o = a_1\ x_1 + \cdots + a_k\ x_k$ mit Skalaren $a_1,\dots,a_k$, die nicht alle Null sind, so wollen wir dieser Eigenschaft der Vektoren $x_1,\dots,x_k$ einen besonderen Namen geben.

Definition. Es seien V ein $\mathbb{K}$–Vektorraum, $k \in \mathbb{N}$ und $x_1,\dots,x_k \in V$. Die Vektoren $x_1,\dots,x_k$ heißen *linear abhängig*, wenn es Skalare $a_1,\dots,a_k$ gibt, die nicht alle Null sind, so daß $a_1\ x_1 + \cdots + a_k\ x_k = o$ gilt. Die Vektoren $x_1,\dots,x_k$ heißen *linear unabhängig*, wenn für alle $a_1,\dots,a_k \in \mathbb{K}$ gilt: Aus $a_1\ x_1 + \cdots + a_k\ x_k = o$ folgt stets $a_1 = 0,\dots,\ a_k = 0$.

Bemerkungen. **(a)** k Vektoren $x_1,\dots,x_k \in V$ sind stets entweder linear abhängig oder linear unabhängig.

(b) Ist einer der Vektoren $x_1,\dots,x_k$ der Nullvektor, so sind sie linear abhängig. Ebenso, wenn zwei der Vektoren $x_1,\dots,x_k$ gleich sind.

(c) Die Vektoren $x_1,\dots,x_k$, $k \geq 2$, sind genau dann linear abhängig, wenn einer von ihnen Linearkombination der restlichen ist. Der Vektor x ist genau dann linear abhängig, wenn er der Nullvektor ist.

Die folgende Bemerkung ist nicht so direkt einzusehen. Wir werden sie deshalb beweisen. Es liege folgende Situation vor:

(d) In dem $\mathbb{K}$–Vektorraum V seien k Vektoren $x_1,\dots,x_k$ gegeben sowie m Linearkombinationen

$$y_1 = \sum_{i=1}^{k} a_{i1}\ x_i\ ,\dots,\ y_m = \sum_{i=1}^{k} a_{im}\ x_i\ .$$

Wir wollen feststellen, ob $y_1,\dots,y_m$ linear unabhängig oder linear abhängig sind. Hierzu machen wir den Ansatz $\sum_{j=1}^{m} t_j\ y_j = o$, $t_j \in \mathbb{K}$, und erhalten

$$(*) \qquad o = \sum_{j=1}^{m} t_j y_j = \sum_{j=1}^{m} t_j \Big(\sum_{i=1}^{k} a_{ij} x_i \Big) = \sum_{i=1}^{k} \Big(\sum_{j=1}^{m} t_j a_{ij} \Big) x_i .$$

Also gilt, falls die Vektoren $x_1,...,x_k$ linear unabhängig sind:

Die Vektoren $y_1,...,y_m$ aus V sind genau dann linear unabhängig, wenn die Spaltenvektoren

$$\hat{y}_1 = \begin{bmatrix} a_{11} \\ \vdots \\ a_{k1} \end{bmatrix} \in \mathbb{K}^k, \ldots, \hat{y}_m = \begin{bmatrix} a_{1m} \\ \vdots \\ a_{km} \end{bmatrix} \in \mathbb{K}^k$$

linear unabhängig sind.

Beweis. Weil $x_1,...,x_k$ linear unabhängig sind, erhalten wir aus den obigen Gleichungen $\sum_{j=1}^{m} t_j a_{ij} = 0$ für $i = 1,...,k$, und umgekehrt hat dies $\sum_{i=1}^{k} \big(\sum_{j=1}^{m} t_j a_{ij} \big) x_i = o$ zur Folge. Also ist $\sum_{j=1}^{m} t_j y_j = o \in V$ äquivalent mit $\sum_{j=1}^{m} t_j \hat{y}_j = o \in \mathbb{K}^k$. Daraus folgt unmittelbar die Behauptung. ∎

Satz 5. *In jedem Vektorraum sind m Linearkombinationen von k Vektoren $x_1,...,x_k$ stets linear abhängig, falls $m \geq k + 1$.*

Beweis. Es seien

$$y_j = \sum_{i=1}^{k} a_{ij} x_i \ , \quad j = 1,...,m \, ,$$

beliebige m Linearkombinationen der Vektoren $x_1,...,x_k$. Wegen $k < m$ hat das homogene lineare Gleichungssystem

$$\begin{aligned} t_1 a_{11} + \cdots + t_m a_{1m} &= 0 \\ &\vdots \\ t_1 a_{k1} + \cdots + t_m a_{km} &= 0 \end{aligned}$$

nach Satz 1.18 eine nichttriviale Lösung $(t_1,...,t_m) \in \mathbb{K}^m$. Aus der obigen Gleichung

(*) folgt dann unmittelbar die Behauptung. ∎

Wie kann man nun die lineare Abhängigkeit bzw. Unabhängigkeit im konkreten Fall nachprüfen? Wir ziehen dazu unsere Kenntnisse über das Lösen linearer Gleichungssysteme heran.

Beispiele. **(a)** In dem reellen Vektorraum $V = \mathbb{R}^4$ seien die Vektoren

$$x_1 = \begin{bmatrix} 2 \\ -3 \\ 1 \\ 4 \end{bmatrix}, \quad x_2 = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 2 \end{bmatrix}, \quad x_3 = \begin{bmatrix} -2 \\ 1 \\ -1 \\ 1 \end{bmatrix}$$

gegeben. Sind x_1, x_2, x_3 linear unabhängig? Der Ansatz

$$a_1 \begin{bmatrix} 2 \\ -3 \\ 1 \\ 4 \end{bmatrix} + a_2 \begin{bmatrix} 1 \\ 0 \\ 1 \\ 2 \end{bmatrix} + a_3 \begin{bmatrix} -2 \\ 1 \\ -1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

führt auf das homogene lineare Gleichungssystem

$$\begin{aligned} 2a_1 + a_2 - 2a_3 &= 0 \\ -3a_1 + \quad + a_3 &= 0 \\ a_1 + a_2 - a_3 &= 0 \\ 4a_1 + 2a_2 + a_3 &= 0 \end{aligned}$$

Wir wenden den Gaußschen Algorithmus an:

$$\begin{bmatrix} 1 & 1 & -1 \\ 2 & 1 & -2 \\ -3 & 0 & 1 \\ 4 & 2 & 1 \end{bmatrix} \begin{matrix} \\ \downarrow -2 \\ \\ \downarrow 3 \\ \downarrow -4 \end{matrix} \longrightarrow \begin{bmatrix} 1 & 1 & -1 \\ 0 & -1 & 0 \\ 0 & 3 & -2 \\ 0 & -2 & 5 \end{bmatrix} \begin{matrix} \\ \\ \downarrow 3 \\ \downarrow -2 \end{matrix}$$

$$\longrightarrow \begin{bmatrix} 1 & 1 & -1 \\ 0 & -1 & 0 \\ 0 & 0 & -2 \\ 0 & 0 & 5 \end{bmatrix} \begin{matrix} \\ \\ \mid (-1) \\ \downarrow \frac{5}{2} \end{matrix} \longrightarrow \begin{bmatrix} 1 & 1 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

Aus der Treppennormalform erhalten wir der Reihe nach $a_3 = 0$, $a_2 = 0$, $a_1 = 0$. Somit sind die Vektoren x_1, x_2, x_3 linear unabhängig.

(b) Es seien x_1, x_2, x_3, x_4 linear unabhängige Vektoren eines reellen Vektorraumes V und

$$\begin{aligned} y_1 &= x_1 - 2x_2 + x_3 - x_4 \\ y_2 &= -4x_1 - 2x_2 + 4x_4 \\ y_3 &= 2x_1 + 3x_2 - x_3 - 3x_4 \\ y_4 &= 17x_1 - 10x_2 + 11x_3 + x_4 \end{aligned}$$

Sind die Vektoren y_1, y_2, y_3, $y_4 \in V$ linear unabhängig? Dazu prüfen wir nach, ob die Spaltenvektoren

$$\begin{bmatrix} 1 \\ -2 \\ 1 \\ -1 \end{bmatrix}, \begin{bmatrix} -4 \\ -2 \\ 0 \\ 4 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ -1 \\ -3 \end{bmatrix}, \begin{bmatrix} 17 \\ -10 \\ 11 \\ 1 \end{bmatrix} \in \mathbb{R}^4$$

linear unabhängig sind. Dies ist nicht der Fall, da das entsprechende lineare Gleichungssystem mit $a_1 = 7$, $a_2 = 15$, $a_3 = 18$ und $a_4 = 1$ nichttrivial lösbar ist. Also gilt $7\,y_1 + 15\,y_2 + 18\,y_3 + y_4 = o$ und y_1, y_2, y_3, y_4 sind linear abhängig.

Für die folgenden Überlegungen ist es nötig, die Begriffe der linearen Abhängigkeit bzw. Unabhängigkeit auf unendlich viele Vektoren zu übertragen. Die Verallgemeinerung einer endlichen indizierten Anzahl von Vektoren wäre eine unendliche (indizierte) Familie von Vektoren. Wir wollen die obigen Definitionen aber nur auf beliebige Mengen von Vektoren übertragen.

Definition. Es seien V ein $\mathbb{K}$–Vektorraum und $A \subset V$. Die Menge A heißt *linear abhängig*, wenn es (paarweise) verschiedene Vektoren $x_1, \ldots, x_k \in A$, $k \in \mathbb{N}$, gibt, die linear abhängig sind. Ist A nicht linear abhängig, so heißt A *linear unabhängig*.

Bemerkungen. **(a)** A ist genau dann linear unabhängig, wenn $A = \emptyset$ oder wenn $A \neq \emptyset$ und für jedes $k \in \mathbb{N}$ alle paarweise verschiedenen Vektoren $x_1, \ldots, x_k \in A$ linear unabhängig sind.

(b) Ist A endlich mit m Elementen, $A = \{x_1,...,x_m\}$, $m \in \mathbb{N}$, so gilt: A ist linear abhängig (linear unabhängig) genau dann, wenn $x_1,...,x_m$ linear abhängig (linear unabhängig) sind.

(c) Enthält A den Nullvektor, so ist A linear abhängig.

(d) Jede Obermenge einer linear abhängigen Menge ist linear abhängig. Jede Teilmenge einer linear unabhängigen Menge ist linear unabhängig.

Die folgenden zwei Bemerkungen sind wieder nicht so direkt einzusehen, weshalb wir sie beweisen.

(e) A ist genau dann linear abhängig, wenn es einen Vektor $x \in A$ gibt mit

$$[A] = [A \setminus \{x\}].$$

Beweis. Ist A linear abhängig, so gibt es k paarweise verschiedene Vektoren $x_1,...,x_k \in A$, $k \in \mathbb{N}$, die linear abhängig sind. Für $k = 1$ ist $x_1 = o$ und $[A \setminus \{x_1\}] = [A]$. Für $k \geq 2$ ist einer der Vektoren $x_1,...,x_k$ eine Linearkombination der anderen. Sei dieser Vektor etwa x_1. Ersetzen wir in jeder Linearkombination von Vektoren aus A, in der x_1 vorkommt, diesen Vektor durch die Linearkombination der Vektoren $x_2,...,x_k$, so erhalten wir $[A] \subset [A \setminus \{x_1\}]$ und somit $[A] = [A \setminus \{x_1\}]$.

Umgekehrt existiere ein Vektor $x \in A$ mit $[A] = [A \setminus \{x\}]$. Ist $A \setminus \{x\} = \emptyset$, so ist $[A \setminus \{x\}] = \{o\}$, also $x = o$. Nach (c) ist A dann linear abhängig. Ist $A \setminus \{x\} \neq \emptyset$, so ist x nach Satz 4 eine Linearkombination von Vektoren $x_1,...,x_k \in A \setminus \{x\}$, von denen wir o.E. annehmen können, daß sie paarweise verschieden sind. Dann sind x, $x_1,...,x_k$ ebenfalls paarweise verschieden und außerdem linear abhängig. Also ist auch A linear abhängig. ∎

(f) Es sei $x \in V$. Ist A linear unabhängig und $x \notin [A]$, so ist $A \cup \{x\}$ ebenfalls linear unabhängig. Umgekehrt folgt aus der linearen Unabhängigkeit von $A \cup \{x\}$ und $x \notin A$, daß A linear unabhängig ist und $x \notin [A]$.

Beweis. Wir beweisen nur die erste Behauptung und überlassen die zweite als Übung. Aus $x \notin [A]$ folgt zunächst $x \neq o$. Seien nun $x_1,...,x_k$ paarweise verschiedene

Vektoren aus $A \cup \{x\}$ und $a_1 x_1 + \cdots + a_k x_k = o$. Sind alle x_i von x verschieden, so gilt $x_i \in A$, $i = 1,...,k$, und aus der linearen Unabhängigkeit von A folgt $a_1 = \cdots = a_k = 0$. Ist etwa $x_k = x$, so muß $a_k = 0$ sein, da sonst $x \in [A]$ wäre. Dann folgt wie zuvor, daß auch $a_1 = \cdots = a_{k-1} = 0$ gilt. ∎

Beispiele. **(a)** Seien $V = \mathbb{K}^n$ und $A = \{e_1,...,e_n\}$ mit

$$e_i := \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \longleftarrow i\text{-te Stelle.}$$

A ist linear unabhängig, denn aus $o = a_1 e_1 + \cdots + a_n e_n$ folgt

$$\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix},$$

also $a_1 = \cdots = a_n = 0$.

(b) In $V = \mathbb{K}[X]$ betrachten wir die Teilmenge $A = \{p_i \mid p_i = X^i , i \in \mathbb{N}_0\}$.

Es seien $k \in \mathbb{N}$, $p_{i_1},...,p_{i_k}$, $i_1 < i_2 < \cdots < i_k$, endlich viele verschiedene Vektoren aus A und $a_{i_1} p_{i_1} + \cdots + a_{i_k} p_{i_k} = o$. Dann folgt

$$(0,...,0,a_{i_1},0,...,0,a_{i_2},0,...,...,0,a_{i_k},0,...) = (0,0,...)$$

und somit $a_{i_1} = \cdots = a_{i_k} = 0$. Also ist A linear unabhängig.

§ 3 Basis und Dimension

In einem Vektorraum V sind besonders jene linear unabhängigen Mengen A wichtig, die die Eigenschaft haben, daß sich jeder Vektor aus V durch Vektoren von A linear kombinieren läßt.

Definition. Es sei V ein $\mathbb{K}$–Vektorraum.

(a) Ein Erzeugendensystem A von V heißt *minimal*, wenn keine echte Teilmenge von A Erzeugendensystem von V ist.

(b) Eine linear unabhängige Teilmenge $A \subset V$ heißt *maximal*, wenn in V jede echte Obermenge von A linear abhängig ist.

(c) Jedes linear unabhängige Erzeugendensystem von V heißt *Basis* von V.

Der Zusammenhang zwischen den obigen Definitionen wird im folgenden Satz hergestellt.

Satz 6. *Es seien V ein $\mathbb{K}$–Vektorraum und B eine nichtleere Teilmenge von V. Dann sind folgende Aussagen äquivalent:*

(a) *B ist Basis von V.*

(b) *B ist minimales Erzeugendensystem von V.*

(c) *B ist eine maximale linear unabhängige Teilmenge von V.*

(d) *Jeder Vektor $x \in V$ ist Linearkombination paarweise verschiedener Vektoren aus B, und jede derartige Linearkombination ist eindeutig, d.h. aus*

$$x = \sum_{i=1}^{k} a_i x_i = \sum_{i=1}^{k} b_i x_i$$

mit $a_1,\ldots,a_k$, $b_1,\ldots,b_k \in \mathbb{K}$, $x_1,\ldots,x_k \in B$ folgt $a_1 = b_1,\ldots, a_k = b_k$.

Bemerkung. Für $B = \emptyset$ sind (a), (b), (c) äquivalent (Übungsaufgabe).

Beweis. (a) $\Rightarrow$ (b): B ist nach Voraussetzung ein Erzeugendensystem von V. Ist B nicht minimal, so gibt es eine echte Teilmenge A von B, die Erzeugendensystem von

V ist. Für $A = \emptyset$ erhalten wir $V = \{o\}$ und damit $B = \emptyset$ im Widerspruch dazu, daß A echte Teilmenge von B ist. Also ist $A \neq \emptyset$. Dann gibt es einen Vektor aus $B \setminus A$, der Linearkombination von Vektoren aus A ist, und B ist linear abhängig im Widerspruch zur Voraussetzung.

(b) $\Rightarrow$ (c): B ist linear unabhängig. Anderfalls existiert ein Vektor $x \in B$ mit $[B] = [B \setminus \{x\}]$ und B ist nicht minimal. B muß auch maximale linear unabhängige Teilmenge von V sein, da es sonst in V eine echte Obermenge A von B gibt, die linear unabhängig ist, und somit einen Vektor $x \in A \setminus B$, der keine Linearkombination von Vektoren aus B ist, ein Widerspruch zur Voraussetzung.

(c) $\Rightarrow$ (d): Es ist $V = [B]$. Anderfalls existiert ein Vektor $x \in V$, $x \notin [B]$ und $B \cup \{x\}$ ist eine echte linear unabhängige Obermenge von B und B ist nicht maximal. Daher ist jeder Vektor $x \in V$ Linearkombination paarweise verschiedener Vektoren $x_1,\ldots,x_k$ aus B. Daß die Linearkombination eindeutig ist, folgt unmittelbar aus der linearen Unabhängigkeit der Vektoren $x_1,\ldots,x_k$.

(d) $\Rightarrow$ (a): B ist offensichtlich Erzeugendensystem von V. B ist auch linear unabhängig. Seien nämlich $x_1,\ldots,x_k$ paarweise verschiedene Vektoren aus B, $a_1,\ldots,a_k \in \mathbb{K}$ und $a_1 x_1 + \cdots + a_k x_k = o$. Da auch $0 x_1 + \cdots + 0 x_k = o$ gilt, folgt aus der Eindeutigkeit $a_1 = 0,\ldots, a_k = 0$. ∎

Bemerkung. Die Aussage (d) in Satz 6 kann verallgemeinert werden:

Es seien B eine Basis von V und $x_1,\ldots,x_k$ sowie $y_1,\ldots,y_m$ jeweils paarweise verschiedene Vektoren aus B. Ist $x \in V$ eine Linearkombination sowohl von $x_1,\ldots,x_k$ als auch von $y_1,\ldots,y_m$, so sind in beiden Linearkombinationen die vom Nullvektor verschiedenen Summanden bis auf die Reihenfolge gleich.

Beweis. Sei $x = \sum_{i=1}^{k} a_i x_i = \sum_{j=1}^{m} b_j y_j$ und o.B.d.A. $a_i \neq 0$, $b_j \neq 0$ für $i = 1,\ldots,k$ und $j = 1,\ldots,m$. Wäre $\{x_1,\ldots,x_k\} \cap \{y_1,\ldots,y_m\} = \emptyset$, so folgte, daß $x_1,\ldots,x_k, y_1,\ldots,y_m$ paarweise verschieden sind, und wegen $\sum_{i=1}^{k} a_i x_i - \sum_{j=1}^{m} b_j y_j = o$ erhielten wir $a_1 = \cdots = a_k = 0$,

$b_1 = \cdots = b_m = 0$, also einen Widerspruch zur Voraussetzung.

Seien also o.B.d.A. $x_1 = y_1,\ldots,x_l = y_l$, $1 \leq l \leq k$, $l \leq m$, und die restlichen Vektoren paarweise verschieden. Ist $l < m$, so sind $x_1,\ldots,x_k$, $y_{l+1},\ldots,y_m$ paarweise verschieden und linear unabhängig. Aus $\sum_{i=1}^{k} a_i x_i = \sum_{j=1}^{m} b_j y_j$ folgt dann $b_{l+1} = \cdots =$ $b_m = 0$, ein Widerspruch. Also ist $l = m$, und analog zeigen wir auch $l = k$.

Damit gilt $k = m = l$, also $x = \sum_{i=1}^{l} a_i x_i = \sum_{j=1}^{l} b_j x_j$. Daraus folgt schließlich $a_i = b_i$ für $i = 1,\ldots,l$. ∎

Beispiele. **(a)** Im Nullraum $V = \{o\}$ ist $\emptyset$ Basis.

(b) In $\mathbb{K}^n$ ist $B = \{e_1,\ldots,e_n\}$ eine Basis: B ist linear unabhängig; dies haben wir schon gezeigt. B ist auch Erzeugendensystem von $\mathbb{K}^n$:

$$\text{Für } x = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \in \mathbb{K}^n \text{ gilt } x = \sum_{i=1}^{n} a_i e_i .$$

Also ist B Basis von $\mathbb{K}^n$. B heißt *Standardbasis* oder *kanonische Basis* von $\mathbb{K}^n$. Entsprechend definiert man die Standardbasis des Vektorraumes $\mathbb{K}^{m\times n}$.

(c) Seien $V = \mathbb{K}[X]$ und $B = \{p_i \mid p_i = X^i , i \in \mathbb{N}_0\}$.

B ist, wie wir schon wissen, linear unabhängig. B ist auch Erzeugendensystem von V. Dies zeigt man wie in Beispiel (b).

(d) Sei $V = \mathbb{K}^A$. Hier können wir keine Basis angeben, falls $|A| = \infty$. Ist beispielsweise $A = \mathbb{N}$, so ist $\mathbb{K}^A$ die Menge aller Folgen $(a_1,a_2,\ldots)$ mit Elementen aus $\mathbb{K}$. Die Menge

$$\{(0,0,\ldots,0,\underbrace{1}_{i\text{-te Stelle}},0,\ldots) \mid i \in \mathbb{N}\}$$

ist zwar linear unabhängig, aber sie ist kein Erzeugendensystem von $\mathbb{K}^{\mathbb{N}}$.

(e) Seien $V = \mathbb{R}^4$ und

$$A = \{\begin{bmatrix} 2 \\ -3 \\ 1 \\ 4 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} -2 \\ 1 \\ -1 \\ 1 \end{bmatrix}\}.$$

A ist linear unabhängig, aber kein Erzeugendensystem von V, da sich der Standardbasisvektor e_4 nicht aus den Elementen von A linear kombinieren läßt. Das entsprechende inhomogene lineare Gleichungssystem besitzt nämlich keine Lösung.

Wegen $e_4 \notin [A]$ ist $A \cup \{e_4\}$ linear unabhängig und wegen Satz 5 auch maximal, also eine Basis von V.

Wie das letzte Beispiel zeigt, kann es in einem Vektorraum mehrere Basen geben, man kann also nicht von **der** Basis sprechen. Unabhängig von der speziellen Wahl einer Basis ist aber die Anzahl ihrer Vektoren. Dies zeigt der folgende Satz.

Satz 7. *Es seien V ein $\mathbb{K}$–Vektorraum und B, B' Basen von V. Dann gilt $|B| = |B'|$.*

Beweis. Für $B = \emptyset$ ist $V = \{o\}$ und somit $B' = \emptyset$. Entsprechend folgt aus $B' = \emptyset$, daß auch $B = \emptyset$ gilt. Ist $|B| = k$, $k \in \mathbb{N}$, so muß $B \neq \emptyset$ sein, und wegen Satz 5 gilt $|B'| \leq k$. Daraus folgt wiederum wegen Satz 5 $|B| \leq |B'|$, insgesamt also $|B| = |B'|$. Entsprechend schließt man im Fall $|B'| = k$, $k \in \mathbb{N}$. Für $|B| = |B'| = \infty$ ist nichts zu beweisen. ∎

Wir wollen uns nun dem Problem zuwenden, ob es in jedem $\mathbb{K}$–Vektorraum V eine Basis gibt. Wir wissen auf jeden Fall, daß in V ein Erzeugendensystem existiert, nämlich V selbst. Gibt es dann auch ein minimales Erzeugendensystem in V? Dazu unterscheiden wir zwei Fälle:

1. **Fall** : In V gibt es ein endliches Erzeugendensystem.
2. **Fall** : Jedes Erzeugendensystem von V ist unendlich.

Im ersten Fall können wir jedes Erzeugendensystem von V zu einer Basis von V "abmagern". Wie das geht, zeigt der folgende Satz.

Satz 8. *Es seien V ein $\mathbb{K}-$Vektorraum und $A' \subset V$ ein endliches Erzeugendensystem von V. Dann gibt es zu jedem Erzeugendensystem A von V eine endliche Teilmenge $B \subset A$, die Basis von V ist.*

Beweis. Da jeder der endlich vielen Vektoren aus A' Linearkombination von endlich vielen Vektoren aus A ist, gibt es eine endliche Teilmenge $A_1 \subset A$, die Erzeugendensystem von V ist. Ist A_1 minimal, so sind wir fertig. Ist dies nicht der Fall, so gibt es eine echte Teilmenge $A_2 \subset A_1$, die Erzeugendensystem ist. Nach maximal $|A_1|$ Schritten erhalten wir so in V ein endliches Erzeugendensystem $B \subset A$, das auch minimal ist, also eine Basis von V. ∎

Korollar 9. *Es seien V ein $\mathbb{K}-$Vektorraum, B eine Basis von V und A ein Erzeugendensystem von V mit $|A| = |B| < \infty$. Dann ist A ebenfalls eine Basis von V.*

Beweis. Nach Satz 8 gibt es eine Teilmenge B' von A, die Basis von V ist. Nach Satz 7 gilt $|B'| = |B|$. Somit folgt $|B'| = |A|$ und schließlich $B' = A$. ∎

Im zweiten Fall ist die Vorgehensweise aus dem Beweis von Satz 8 unbrauchbar, da sie immer wieder zur Ausgangssituation eines unendlichen Erzeugendensystems zurückführen kann, das noch nicht minimal ist. Hier gibt es kein konstruktives Verfahren, das von dem unendlichen Erzeugendensystem A ausgehend zu einer Basis führt, aber man kann mit Hilfe des Zornschen Lemmas (siehe S. 26) auch in diesem Fall die Existenz einer Basis $B \subset A$ beweisen. Wir verzichten hier auf einen Beweis, da wir das Zornsche Lemma gleich bei dem Gegenstück von Satz 8, dem Basisergänzungssatz, verwenden werden.

Zunächst geben wir aufgrund der vorstehenden Überlegungen folgende Definition.

Definition. Es sei V ein $\mathbb{K}-$Vektorraum. Besitzt V ein endliches Erzeugendensystem, so heißt V *endlich dimensional* und die allen Basen von V gemeinsame Anzahl $n \in \mathbb{N}_0$ der Elemente heißt die *Dimension* von V. Schreibweise: $\dim V < \infty$ bzw. $\dim V = n$. Hat V kein endliches Erzeugendensystem, so heißt V *unendlich dimensional* und wir schreiben $\dim V = \infty$.

Bemerkung. ∞ ist nur ein Symbol. Es ist aber praktisch, ∞ als "unendlich große" Zahl aufzufassen und folgende Vereinbarung zu treffen:

$$\infty + \infty := \infty \ , \ \infty + a := \infty \text{ für alle } a \in \mathbb{R}.$$

Satz 10 (Basisergänzungssatz). *Es seien V ein $\mathbb{K}-$Vektorraum und $A \subset V$ eine linear unabhängige Teilmenge. Dann gibt es eine Basis von V, die A enthält.*

Beweis. Ist A maximal, so ist A eine Basis von V. Ist A nicht maximal, so gibt es eine echte linear unabhängige Obermenge A_1 von A.

Ist dim $V = n < \infty$, so gilt wegen Satz 5 $|A_1| \leq n$. Nach höchstens n Schritten erhalten wir so eine linear unabhängige Obermenge B von A mit $|B| = n$. Da jede echte Obermenge von B wegen Satz 5 linear abhängig sein muß, ist B maximal und somit eine Basis von V.

Ist dim $V = \infty$, so führt dieses Verfahren nicht zum Ziel. Hier müssen wir uns mit einem nichtkonstruktiven Existenzbeweis begnügen, der mit Hilfe des Zornschen Lemmas geführt wird: Wir betrachten dazu das Mengensystem

$$\mathcal{M} = \{A' | A \subset A' \subset V, A' \text{ linear unabhängig}\}$$

$\mathcal{M}$ ist bezüglich der Inklusion $\subset$ eine geordnete Menge. Um das Zornsche Lemma anwenden zu können, müssen wir zeigen, daß jede bezüglich $\subset$ totalgeordnete Teilmenge $\mathcal{N}$ von $\mathcal{M}$ eine obere Schranke C in $\mathcal{M}$ besitzt. Wir wählen

$$C = \bigcup_{A' \in \mathcal{N}} A'$$

Dann ist $A \subset C \subset V$, und C ist linear unabhängig: Für $C = \emptyset$ ist dies klar. Für $C \neq \emptyset$ seien $x_1,\ldots,x_k$ beliebige, paarweise verschiedene Vektoren aus C. Nach Definition von C gibt es Mengen $A_i' \in \mathcal{N}$ mit $x_i \in A_i'$ für $i = 1,\ldots,k$. Da $\mathcal{N}$ totalgeordnet ist, gibt es unter den k Mengen $A_1',\ldots,A_k'$ eine Menge $\tilde{A} = A_{i_0}'$ mit $A_i' \subset \tilde{A}$ für $i = 1,\ldots,k$. Somit gilt $x_1,\ldots,x_k \in \tilde{A}$, und weil $\tilde{A}$ linear unabhängig ist, sind es auch die Vektoren $x_1,\ldots,x_k$. Also ist C linear unabhängig und damit ein Element von $\mathcal{M}$. Da offensichtlich $A' \subset C$ für alle $A' \in \mathcal{N}$ gilt, ist C auch obere Schranke von $\mathcal{N}$.

Nach dem Zornschen Lemma existiert nun in $\mathcal{M}$ ein maximales Element B,

d.h. B ist linear unabhängig, es ist $A \subset B$ und aus $B \subset A'$ für $A' \in \mathcal{M}$ folgt stets $B = A'$. Damit ist B auch eine maximale linear unabhängige Teilmenge von V, also eine Basis von V. ∎

Bemerkung. Jeder $\mathbb{K}$–Vektorraum V besitzt eine Basis B. Es ist dim $V = |B|$.

Korollar 11. *Es seien V ein endlich dimensionaler $\mathbb{K}$–Vektorraum, B eine Basis von V und $A \subset V$ eine linear unabhängige Teilmenge mit $|A| = |B|$. Dann ist A ebenfalls eine Basis von V.*

Beweis. Nach Satz 10 gibt es eine Basis B' von V mit $A \subset B'$. Dann gilt $|A| = |B| = |B'|$ und somit $A = B'$. ∎

Der nächste Satz zeigt, daß die Dimension eines Untervektorraumes höchstens so groß sein kann wie die des Vektorraumes selbst.

Satz 12. *Es seien V ein n–dimensionaler $\mathbb{K}$–Vektorraum und $U \subset V$ ein Untervektorraum. Dann gilt:*

(a) dim $U \leq n$.

(b) *Genau dann ist* dim $U = n$, *wenn* $U = V$.

Beweis. (a) Sei A eine beliebige linear unabhängige Teilmenge von U. Nach Satz 10 kann A zu einer Basis B von V ergänzt werden. Dann gilt $A \subset B$ und $|A| \leq n$. Somit gibt es auch eine maximale linear unabhängige Teilmenge $A \subset U$, die nach Satz 6 Basis von U ist. Daraus folgt dim $U \leq n$.

(b) Seien dim $U = n$, B eine Basis von U und $x \in V$. Gilt $x \notin [B]$, so ist $B \cup \{x\}$ linear unabhängig, ein Widerspruch zu Satz 5. Also ist $V \subset [B] = U$ und damit $V = U$. Die umgekehrte Richtung ist trivial. ∎

Bemerkung. Für unendlich dimensionale Vektorräume V ist die Ungleichung dim $U \leq$ dim V trivial, aus dim $U =$ dim V folgt aber nicht $U = V$.

Beispiel. Im $\mathbb{R}^5$ seien die Vektoren

$$x_1 = \begin{bmatrix} 1 \\ 2 \\ -1 \\ -1 \\ -1 \end{bmatrix}, \quad x_2 = \begin{bmatrix} 2 \\ -1 \\ 1 \\ 2 \\ -2 \end{bmatrix}, \quad x_3 = \begin{bmatrix} 3 \\ -4 \\ 3 \\ 5 \\ -3 \end{bmatrix}, \quad x_4 = \begin{bmatrix} -1 \\ 8 \\ -5 \\ -6 \\ 1 \end{bmatrix}$$

gegeben und es sei $U = [x_1,...,x_4]$.

(a) Wir wollen unter den Vektoren $x_1,...,x_4$ eine Basis von U finden. Dazu prüfen wir zunächst nach, ob die Vektoren $x_1,...,x_4$ linear unabhängig sind. Der Ansatz

$$a_1 x_1 + a_2 x_2 + a_3 x_3 + a_4 x_4 = o$$

führt auf ein lineares Gleichungssystem mit der zugehörigen Matrix

$$\begin{bmatrix} 1 & 2 & 3 & -1 \\ 2 & -1 & -4 & 8 \\ -1 & 1 & 3 & -5 \\ -1 & 2 & 5 & -6 \\ -1 & -2 & -3 & 1 \end{bmatrix} \begin{matrix} \\ -2 \\ 1 \\ 1 \\ 1 \end{matrix}$$

Durch elementare Zeilenumformungen erhalten wir mit dem Gaußschen Algorithmus:

$$\begin{bmatrix} 1 & 2 & 3 & -1 \\ 0 & -5 & -10 & 10 \\ 0 & 3 & 6 & -6 \\ 0 & 4 & 8 & -7 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{matrix} \\ :-5 \\ :3 \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ -1 \\ \\ -4 \end{matrix} \longrightarrow \begin{bmatrix} 1 & 2 & 3 & -1 \\ 0 & 1 & 2 & -2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{matrix} \\ \\ \\ 2 \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ 1 \end{matrix}$$

$$\longrightarrow \begin{bmatrix} 1 & 2 & 3 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{matrix} \\ \\ -2 \\ \\ \end{matrix} \longrightarrow \begin{bmatrix} \underline{1} & 0 & -1 & 0 \\ 0 & \underline{1} & 2 & 0 \\ 0 & 0 & 0 & \underline{1} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Anhand der Normalform sehen wir, daß x_1, x_2, x_4 linear unabhängig sind, weil das lineare Gleichungssystem $a_1 x_1 + a_2 x_2 + a_4 x_4 = o$ nur trivial lösbar ist, und weiter, daß x_3 Linearkombination von x_1, x_2 ist, weil das lineare Gleichungssystem $b_1 x_1 + b_2 x_2 = x_3$ lösbar ist. Also gilt $U = [x_1, x_2, x_4]$ und $\{x_1, x_2, x_4\}$ ist Basis von U.

(b) Wir wollen eine möglichst einfache Basis von U finden, indem wir die Vek-

toren $x_1,\ldots,x_4$ durch geeignete Linearkombinationen ersetzen. Zur praktischen Durchführung schreiben wir die Vektoren $x_1,\ldots,x_4$ in die Zeilen einer Matrix und wenden wieder das Gaußsche Verfahren an.

$$\begin{bmatrix} 1 & 2 & -1 & -1 & -1 \\ 2 & -1 & 1 & 2 & -2 \\ 3 & -4 & 3 & 5 & -3 \\ -1 & 8 & -5 & -6 & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 2 & -1 & -1 & -1 \\ 0 & -5 & 3 & 4 & 0 \\ 0 & -10 & 6 & 8 & 0 \\ 0 & 10 & -6 & -7 & 0 \end{bmatrix}$$

$$\longrightarrow \begin{bmatrix} 1 & 2 & -1 & -1 & -1 \\ 0 & 1 & -3/5 & -4/5 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 2 & -1 & 0 & -1 \\ 0 & 1 & -3/5 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\longrightarrow \begin{bmatrix} \boxed{1} & 0 & 1/5 & 0 & -1 \\ 0 & \boxed{1} & -3/5 & 0 & 0 \\ 0 & 0 & 0 & \boxed{1} & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Also ist

$$U = [\underbrace{\begin{bmatrix} 1 \\ 0 \\ 1/5 \\ 0 \\ -1 \end{bmatrix}}_{u_1}, \underbrace{\begin{bmatrix} 0 \\ 1 \\ -3/5 \\ 0 \\ 0 \end{bmatrix}}_{u_2}, \underbrace{\begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}}_{u_3}] .$$

Die Vektoren u_1, u_2, u_3 bilden eine Basis von U, denn sie sind auch linear unabhängig: Aus $a_1\,u_1 + a_2\,u_2 + a_3\,u_3 = o$ folgt nämlich $a_1 = a_2 = a_3 = 0$.

Das in den beiden vorangehenden Beispielen angewendete Verfahren soll nun allgemein dargestellt werden. Insbesondere soll geklärt werden, wie sich die elementaren Zeilenumformungen auf die Spalten bzw. Zeilen einer Matrix auswirken. Sei

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \in \mathbb{K}^{m\times n}.$$

Zu A kann man zwei Systeme von Vektoren aus $\mathbb{K}^m$ bzw. $\mathbb{K}^n$ betrachten. Zunächst bilden die Spalten

$$s_1 = \begin{bmatrix} a_{11} \\ \vdots \\ a_{m1} \end{bmatrix}, \ldots, s_n = \begin{bmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{bmatrix}$$

n Vektoren im $\mathbb{K}^m$. Sie spannen einen Untervektorraum $U \subset \mathbb{K}^m$ auf, $U = [s_1,\ldots,s_n]$.

Dann bilden auch die Zeilen von A, wenn man sie als Spaltenvektoren schreibt

$$z_1 = \begin{bmatrix} a_{11} \\ \vdots \\ a_{1n} \end{bmatrix}, \ldots, z_m = \begin{bmatrix} a_{m1} \\ \vdots \\ a_{mn} \end{bmatrix}$$

m Vektoren im $\mathbb{K}^n$. Sie spannen einen Untervektorraum $W \subset \mathbb{K}^n$ auf, $W = [z_1,\ldots,z_m]$.

Für die Matrix A gilt somit

$$A = (s_1 \mid \cdots \mid s_n) = \begin{bmatrix} z_1^T \\ \cdots \\ z_m^T \end{bmatrix}.$$

Sei nun $\tilde{A}$ die beim Gaußschen Algorithmus durch Anwendung von Zeilenumformungen entstehende Endmatrix, also die Gaußsche Normalform von A, und seien

$$\tilde{s}_1,\ldots,\tilde{s}_n \text{ bzw. } \tilde{z}_1,\ldots,\tilde{z}_m$$

die zugehörigen Spalten– bzw. Zeilenvektoren. Wir wollen überlegen, welcher Zusammenhang zwischen den Spaltenvektoren s_j und $\tilde{s}_j$, $j = 1,\ldots,n$, bzw. den Zeilenvektoren z_i und $\tilde{z}_i$, $i = 1,\ldots,m$, besteht.

Satz 13. *Es ist* $[\tilde{z}_1,\ldots,\tilde{z}_m] = W$ *und diejenigen Vektoren* $\tilde{z}_i$, *welche vom Nullvektor verschieden sind, bilden eine (besonders einfache) Basis von* W.

Beweis. Da $\tilde{A}$ durch endlich viele elementare Zeilenumformungen aus A entstanden ist, sind die Vektoren $\tilde{z}_1,\ldots,\tilde{z}_m$ Linearkombinationen der ursprünglichen Vektoren $z_1,\ldots,z_m$. Also gilt $[\tilde{z}_1,\ldots,\tilde{z}_m] \subset W$. Da jede der angewendeten Zeilenumformungen wieder rückgängig gemacht werden kann, ensteht umgekehrt A durch endlich viele Zeilenumformungen aus $\tilde{A}$. Somit sind die Vektoren $z_1,\ldots,z_m$ Linearkombinationen der Vektoren $\tilde{z}_1,\ldots,\tilde{z}_m$ und es gilt $W \subset [\tilde{z}_1,\ldots,\tilde{z}_m]$.

Weiterhin erkennt man aus der Gestalt der Normalform

$$\tilde{A} = \left[\begin{array}{ccccccccccccc}
0 & \cdots & 0 & 1 & * & \cdots & * & 0 & * & \cdots & * & 0 & * \\
0 & \cdots & \cdots & \cdots & 0 & 1 & * & \cdots & * & 0 & * & \cdots & * \\
0 & \cdots & \cdots & \cdots & \cdots & 0 & 1 & * & \cdots & * & 0 & * & \cdots \\
\vdots & & & & & & & \ddots & & & & & \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 & * & \cdots & * & 0 \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 & * & \cdots & * \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
\vdots & & & & & & & & & & & & \vdots \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0
\end{array}\right] \begin{array}{l} \\ \\ \\ \\ \\ \\ \\ \\ \end{array} \begin{array}{l} \} k \\ \\ \\ \\ \\ \\ \} m-k \\ \\ \end{array}$$

unmittelbar, daß die ersten k Zeilen linear unabhängig sind. Das sind aber genau die Vektoren $\tilde{z}_i$, die von o verschieden sind. ∎

Nicht ganz so einfach ist der Zusammenhang zwischen den alten und den neuen Spaltenvektoren, denn im allgemeinen ist der Untervektorraum $[\tilde{s}_1,\ldots,\tilde{s}_n]$ von U verschieden. Es gilt aber:

Satz 14. *Es ist* $\dim [\tilde{s}_1,\ldots,\tilde{s}_n] = \dim U$. *Diejenigen Vektoren* $s_{j_1},\ldots,s_{j_k}$, *deren Indizes* $j_1,\ldots,j_k \in \{1,\ldots,n\}$ *zu den "Treppenstufen" in* $\tilde{A}$ *gehören, die also bei dem Gaußschen Algorithmus in Vektoren der Standardbasis*

$$\tilde{s}_{j_1} = e_1 , \ldots , \tilde{s}_{j_k} = e_k$$

übergehen, bilden eine Basis von U.

Beweis. Wir betrachten die linearen Gleichungssysteme $A\ y = o$ bzw. $\tilde{A}\ y = o$, $y = (y_1,\ldots,y_n) \in \mathbb{K}^n$, die wir in der Form

$$y_1\ s_1 + \cdots + y_n\ s_n = o \text{ bzw. } y_1\ \tilde{s}_1 + \cdots + y_n\ \tilde{s}_n = o$$

schreiben. Sie haben dieselbe Lösungsmenge. Aus der Gestalt von $\tilde{A}$ ergibt sich, daß die y_j mit $j \notin \{j_1,\ldots,j_k\}$ beliebig gewählt werden können. Damit ist jeder Vektor s_j mit $j \notin \{j_1,\ldots,j_k\}$ Linearkombination von $s_{j_1},\ldots,s_{j_k}$ und ebenso jeder Vektor $\tilde{s}_j$ mit $j \notin \{j_1,\ldots,j_k\}$ Linearkombination von $\tilde{s}_{j_1},\ldots,\tilde{s}_{j_k}$. Also gilt

$$U = [s_{j_1},\ldots,s_{j_k}] \text{ bzw. } [\tilde{s}_1,\ldots,\tilde{s}_n] = [\tilde{s}_{j_1},\ldots,\tilde{s}_{j_k}]$$

und die Vektoren $\tilde{s}_{j_1},\ldots,\tilde{s}_{j_k}$ sind linear unabhängig. Ist $y_{j_1}\ s_{j_1} + \cdots + y_{j_k}\ s_{j_k} = o$, $y_{j_1},\ldots,y_{j_k} \in \mathbb{K}$, so ist

$$y = (0,\ldots,0,\underbrace{y_{j_1}}_{j_1\text{-te Stelle}},0,\ldots,0,y_{j_2},\ldots,\ldots,\underbrace{y_{j_k}}_{j_k\text{-te Stelle}},0,\ldots,0)$$

Lösung von $A\ y = o$ also auch von $\tilde{A}\ y = o$. Damit folgt aber sofort $y_{j_1} = \cdots = y_{j_k} = 0$. Die Vektoren $s_{j_1},\ldots,s_{j_k}$ sind daher linear unabhängig und bilden eine Basis von U. Somit gilt auch $\dim U = \dim [\tilde{s}_{j_1},\ldots,\tilde{s}_{j_k}] = \dim [\tilde{s}_1,\ldots,\tilde{s}_n]$. ∎

Zusammenfassung. Es seien m Vektoren $x_1,\ldots,x_m \in \mathbb{K}^n$ gegeben und es soll der Untervektorraum $U = [x_1,\ldots,x_m] \subset \mathbb{K}^n$ untersucht werden.

Ist man an einer Basis von U in "Treppenform" interessiert, so wende man den Gaußschen Algorithmus auf die Matrix

$$\begin{bmatrix} x_1^T \\ \cdots\cdots \\ \vdots \\ \cdots\cdots \\ x_m^T \end{bmatrix}$$

an. Man kann dann auch sagen, daß man *elementare Spaltenumformungen* auf $x_1,\ldots,x_m$ anwendet.

Ist man an der Frage interessiert, welche der Vektoren $x_1,\ldots,x_m$ eine Basis von

U bilden, so muß man den Gaußschen Algorithmus auf die Matrix

$$(x_1 \mid \cdots \mid x_m)$$

anwenden.

Zur Bestimmung der Dimension von U können beide Verfahren benutzt werden.

Es sei nun wieder eine Matrix $A \in \mathbb{K}^{m\times n}$ gegeben mit den Spalten $s_1,\ldots,s_n$ aus $\mathbb{K}^m$ und den Zeilen $z_1^\top,\ldots,z_m^\top$, $z_i \in \mathbb{K}^n$. Die Zahl dim $[s_1,\ldots,s_n]$ heißt der *Spaltenrang* von A, die Zahl dim $[z_1,\ldots,z_m]$ heißt der *Zeilenrang* von A.

Satz 15 und Definition. *Zeilenrang und Spaltenrang einer Matrix $A \in \mathbb{K}^{m\times n}$ sind gleich. Wir nennen diese Zahl den Rang von A, Schreibweise:* Rang A *oder* Rg A.

Beweis. Nach Satz 13 ist der Zeilenrang von A gleich der Anzahl k der Treppen in der Normalform $\tilde{A}$. Nach Satz 14 ist auch der Spaltenrang gleich k. ∎

Bemerkung. Der Rang einer Matrix A ist also die Maximalzahl linear unabhängiger Spalten (Zeilen) von A. Er läßt sich mit Hilfe des Gaußschen Algorithmus bestimmen.

Korollar 16. **(a)** *Für alle $A \in \mathbb{K}^{m\times n}$ gilt:* Rg A = Rg $A^\top$.

(b) *Für alle $A \in \mathbb{K}^{n\times n}$ gilt: A ist genau dann regulär, wenn* Rg $A = n$.

(c) *Für alle $A \in \mathbb{K}^{m\times n}$ und alle $b \in \mathbb{K}^m$ gilt: Das lineare Gleichungssystem $A\,x = b$ ist genau dann lösbar, wenn* Rg A = Rg $(A \mid b)$.

Bei homogenen linearen Gleichungssystemen können wir nun auch eine Aussage über die Dimension des Lösungsraumes machen. Es gilt

Korollar 17. *Es sei $A \in \mathbb{K}^{m\times n}$. Dann hat der Lösungsraum L des homogenen linearen Gleichungssystems $A\,x = o$ die Dimension $n -$ Rg A.*

Beweis. Die Matrix A habe die Normalform $\tilde{A}$ wie auf Seite 113. L und der Lösungsraum $\tilde{L}$ von $\tilde{A}\,x = o$ stimmen überein, und in jeder Lösung $x \in \tilde{L}$ sind die x_j mit $j \notin \{j_1,\ldots,j_k\}$ frei wählbar, und die restlichen x_j sind dann eindeutig festgelegt. Dabei

sind $j_1,\ldots,j_k$ wieder die Indizes, für die

$$\tilde{s}_{j_1} = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad \tilde{s}_{j_2} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \ldots.$$

gilt. Somit folgt $\dim L = n - k = n - \operatorname{Rg} A$. ∎

Bemerkung. Jeder Untervektorraum $U \subset \mathbb{K}^n$ ist Lösungsraum eines geeigneten homogenen linearen Gleichungssystems:

Es sei $U = [x_1,\ldots,x_m] \subset \mathbb{K}^n$ und $\dim U = r$. Wir schreiben die Vektoren $x_1,\ldots,x_m$ als Zeilen einer Matrix

$$A = \begin{bmatrix} x_1^\top \\ \cdots\cdots \\ \vdots \\ \cdots\cdots \\ x_m^\top \end{bmatrix} \in \mathbb{K}^{m\times n}$$

und betrachten das lineare Gleichungssystem $A\ y = o$, dessen Lösungsraum nach Korollar 17 die Dimension $k = n - \operatorname{Rg} A = n - \dim U = n - r$ hat.

In diesem Lösungsraum wählen wir eine Basis $\{y_1,\ldots,y_k\}$ und schreiben die Basisvektoren wieder als Zeilen einer Matrix

$$B = \begin{bmatrix} y_1^\top \\ \cdots\cdots \\ \vdots \\ \cdots\cdots \\ y_k^\top \end{bmatrix} \in \mathbb{K}^{k\times n}$$

mit $\operatorname{Rg} B = k$. Dann ist U der Lösungsraum des linearen Gleichungssystems $B\ x = o$.

Beweis. Es sei L_h der Lösungsraum von $B\ x = o$. Nach Korollar 17 gilt dann $\dim L_h = n - \operatorname{Rg} B = n - k = r$. Also ist $\dim L_h = \dim U$. Aus $A\ y_j = o$, $j = 1,\ldots,k$, folgt $x_i^\top y_j = 0$ für $i = 1,\ldots,m$ und $j = 1,\ldots,k$ und somit auch $y_j^\top x_i = 0$ für $j = 1,\ldots,k$ und

$i = 1,...,m$. Also gilt $B\,x_i = o$, $i = 1,...,m$ und daher $U \subset L_h$. Aus der Gleichheit der Dimensionen folgt schließlich $U = L_h$. ∎

Beispiel. Das eben beschriebene Verfahren ist oft praktisch bei der Bestimmung des Durchschnitts von Untervektorräumen des $\mathbb{K}^n$.

Im $\mathbb{R}^5$ seien die Untervektorräume

$$U_1 = \left[\begin{bmatrix}1\\-1\\-1\\-2\\1\end{bmatrix}, \begin{bmatrix}0\\3\\3\\3\\0\end{bmatrix}, \begin{bmatrix}1\\-3\\1\\-2\\4\end{bmatrix}\right] , \quad U_2 = \left[\begin{bmatrix}-1\\0\\-4\\-5\\1\end{bmatrix}, \begin{bmatrix}-5\\-1\\2\\2\\-6\end{bmatrix}, \begin{bmatrix}1\\2\\-1\\3\\2\end{bmatrix}, \begin{bmatrix}3\\1\\0\\3\\3\end{bmatrix}\right]$$

gegeben. Wir suchen Ihren Durchschnitt $U_1 \cap U_2$. Hierzu stellen wir U_1 und U_2 durch lineare Gleichungssysteme dar und schreiben deshalb die erzeugenden Vektoren jeweils als Zeilen einer Matrix eines LGS:

$$A_1 = \begin{bmatrix}1 & -1 & -1 & -2 & 1\\0 & 3 & 3 & 3 & 0\\1 & -3 & 1 & -2 & 4\end{bmatrix} , \quad A_2 = \begin{bmatrix}-1 & 0 & -4 & -5 & 1\\-5 & -1 & 2 & 2 & -6\\1 & 2 & -1 & 3 & 2\\3 & 1 & 0 & 3 & 3\end{bmatrix}$$

Mit Hilfe des Gaußschen Verfahrens erhalten wir die Gaußschen Normalformen

$$\tilde{A}_1 = \begin{bmatrix}1 & 0 & 0 & -1 & 1\\0 & 1 & 0 & 1/2 & -3/4\\0 & 0 & 1 & 1/2 & 3/4\end{bmatrix} , \quad \tilde{A}_2 = \begin{bmatrix}1 & 0 & 0 & 0 & 12/13\\0 & 1 & 0 & 0 & 6/13\\0 & 0 & 1 & 0 & -5/13\\0 & 0 & 0 & 1 & -1/13\end{bmatrix}$$

Die Lösungsräume L_1 von $A_1\,x = o$ und L_2 von $A_2\,x = o$ sind

$$L_1 = \left[\begin{bmatrix}2\\-1\\-1\\2\\0\end{bmatrix}, \begin{bmatrix}-4\\3\\-3\\0\\4\end{bmatrix}\right] , \quad L_2 = \left[\begin{bmatrix}-12\\-6\\5\\1\\13\end{bmatrix}\right] .$$

Damit ist U_1 Lösungsraum des linearen Gleichungssystems

$$\begin{aligned} 2\,x_1 - x_2 - x_3 + 2\,x_4 &= 0 \\ -4\,x_1 + 3\,x_2 - 3\,x_3 + 4\,x_5 &= 0 \end{aligned}$$

und U_2 ist Lösungsraum von

$$-12\,x_1 - 6\,x_2 + 5\,x_3 + x_4 + 13\,x_5 = 0\,.$$

$U_1 \cap U_2$ ist nun Lösungsmenge des homogenen linearen Gleichungssystems mit der Matrix

$$\begin{bmatrix} 2 & -1 & -1 & 2 & 0 \\ -4 & 3 & -3 & 0 & 4 \\ -12 & -6 & 5 & 1 & 13 \end{bmatrix},$$

deren Normalform

$$\begin{bmatrix} 1 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 & -1 \\ 0 & 0 & 1 & -1 & -1 \end{bmatrix}$$

lautet. Daraus folgt

$$U_1 \cap U_2 = \left[\begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}\right].$$

§ 4 Summen und Faktorräume

Die Vereinigung von Untervektorräumen ist im allgemeinen kein Untervektorraum, wohl aber ihre Summe, die folgendermaßen definiert ist.

Definitionen. **(a)** Unter der *Summe* von k Teilmengen $A_1,...,A_k$ des $\mathbb{K}$–Vektorraumes V, $k \geq 2$, verstehen wir die Menge

$$A_1 + \cdots + A_k := \{x_1 + \cdots + x_k \mid x_i \in A_i,\ i = 1,...,k\}, \text{ Kurzschreibweise: } \sum_{i=1}^{k} A_i .$$

Ist $A = \{x\}$ und $B \subset V$, so schreiben wir statt $\{x\} + B$ kurz $x + B$.

(b) Sind $U_1,...,U_k$, $k \geq 2$, Untervektorräume von V und gilt für $i = 1,...,k$

$$U_i \cap \sum_{\substack{j=1 \\ j \neq i}}^{k} U_j = \{o\} ,$$

so heißt die Summe $U_1 + \cdots + U_k$ *direkt*. Wir schreiben in diesem Fall $U_1 \oplus \cdots \oplus U_k$.

Bemerkungen. **(a)** Die Summe von Teilmengen eines Vektorraumes ist im allgemeinen kein Untervektorraum. Man betrachte etwa die Summe $\{x\} + \{y\} = \{x + y\}$, die für $x + y \neq o$ kein Untervektorraum ist. Dagegen ist die Summe von Untervektorräumen eines Vektorraumes V stets ein Untervektorraum von V, wie man mit Hilfe von Satz 2 sofort erkennt.

(b) Für alle Teilmengen $A_1,...,A_k$ von V gilt $[A_1] + \cdots + [A_k] = [A_1 \cup \cdots \cup A_k]$.

Beweis. Nach Satz 4 ist $[A_1] + \cdots + [A_k] \subset [A_1 \cup \cdots \cup A_k]$. Umgekehrt gilt auch $A_1 \cup \cdots \cup A_k \subset [A_1] + \cdots + [A_k]$ und somit $[A_1 \cup \cdots \cup A_k] \subset [A_1] + \cdots + [A_k]$. ∎

Im folgenden Satz klären wir, wann eine Summe von Untervektorräumen direkt ist.

Satz 18. *Es seien V ein $\mathbb{K}$–Vektorraum und $U_1,\dots,U_k$, $k \geq 2$, Untervektorräume von V. Dann gilt:*

Die Summe $U = U_1 + \cdots + U_k$ ist genau dann direkt, wenn jeder Vektor $x \in U$ eine eindeutige Darstellung $x = u_1 + \cdots + u_k$ mit $u_i \in U_i$ für $i = 1,\dots,k$ besitzt.

Beweis. Sei $U = U_1 \oplus \cdots \oplus U_k$ und seien $x = u_1 + \cdots + u_k$ und $x = \tilde{u}_1 + \cdots + \tilde{u}_k$ Darstellungen von $x \in U$. Dann folgt $(u_1 - \tilde{u}_1) + \cdots + (u_k - \tilde{u}_k) = o$, also

$$u_i - \tilde{u}_i = \sum_{\substack{j=1 \\ j \neq i}}^{k} (\tilde{u}_j - u_j).$$

Auf der linken Seite steht ein Element von U_i, auf der rechten ein Element der Summe $U_1 + \cdots + U_{i-1} + U_{i+1} + \cdots + U_k$. Somit ist $u_i - \tilde{u}_i = o$. Dies gilt für alle $i = 1,\dots,k$, die Darstellung ist daher eindeutig.

Die Umkehrung beweisen wir indirekt und nehmen dazu an, die Summe sei nicht direkt. Es gibt somit ein $i \in \{1,\dots,k\}$ mit

$$U_i \cap \sum_{\substack{j=1 \\ j \neq i}}^{k} U_j \neq \{o\}.$$

Sei $u_i \neq o$ aus diesem Durchschnitt. Dann gilt $u_i = u_1 + \cdots + u_{i-1} + u_{i+1} + \cdots + u_k$ mit $u_j \in U_j$, $j = 1,\dots,k$, $j \neq i$, und $u_i = u_i$, ein Widerspruch zur Voraussetzung. ∎

Für die Summe zweier Untervektorräume gilt der folgende Dimensionssatz.

Satz 19 (Dimensionssatz). *Es seien V ein $\mathbb{K}$–Vektorraum und U, W Untervektorräume von V. Dann gilt:*

$$\dim (U + W) + \dim (U \cap W) = \dim U + \dim W.$$

Beweis. Für $\dim U = \infty$ oder $\dim W = \infty$ ist auch $\dim (U + W) = \infty$ und die Aussage ist trivial. Seien also $\dim U = m < \infty$ und $\dim W = n < \infty$. Nach Satz 12 gilt dann auch $\dim (U \cap W) = k < \infty$. Im Fall $k > 0$ sei $B_0 = \{u_1,\dots,u_k\}$ eine Basis von

$U \cap W$. Nach dem Basisergänzungssatz können wir B_0 zu einer Basis B_1 von U und zu einer Basis B_2 von W ergänzen:

$$B_1 = \{u_1,\dots,u_k\,,\ u_{k+1},\dots,u_m\}\,,\quad B_2 = \{u_1,\dots,u_k\,,\ w_{k+1},\dots,w_n\}.$$

Für $k = 0$ ist $B_0 = \emptyset$; hier können $B_1 = \{u_1,\dots,u_m\}$ und $B_2 = \{w_1,\dots,w_n\}$ beliebige Basen von U bzw. W sein. Nun gilt $U + W = [u_1,\dots,u_m\,,w_{k+1},\dots,w_n]$, d.h. $U + W$ ist ebenfalls endlich dimensional.

Wir zeigen, daß die Vektoren $u_1,\dots,u_m\,,w_{k+1},\dots,w_n$ linear unabhängig sind. Aus $a_1\,u_1 + \cdots + a_m\,u_m + b_{k+1}\,w_{k+1} + \cdots + b_n\,w_n = o$ erhalten wir $a_1\,u_1 + \cdots + a_m\,u_m = -b_{k+1}\,w_{k+1} - \cdots - b_n\,w_n$ und somit $b_{k+1}\,w_{k+1} + \cdots + b_n\,w_n \in U \cap W$. Daraus folgt $b_{k+1} = \cdots = b_n = 0$ und damit $a_1\,u_1 + \cdots + a_m\,u_m = o$. Wegen der linearen Unabhängigkeit von B_1 ist $a_1 = \cdots = a_m = 0$.

Also ist $B_1 \cup B_2$ Basis von $U + W$ und wir erhalten $\dim(U + W) = m + n - k$ $= \dim U + \dim W - \dim(U \cap W)$. ∎

Korollar 20. *Es gilt* $\dim(U \oplus W) = \dim U + \dim W$.

Definition. Es seien V ein $\mathbb{K}$–Vektorraum und $U, W \subset V$ Untervektorräume. Gilt $V = U \oplus W$, so heißen U und W *komplementär*, W heißt ein *Komplementärraum* von U und analog heißt U ein *Komplementärraum* von W.

Wir zeigen, daß jeder Untervektorraum einen Komplementärraum besitzt.

Satz 21. *Es seien V ein $\mathbb{K}$–Vektorraum und U ein Untervektorraum von V. Dann gibt es zu U einen Komplementärraum.*

Beweis. Wir ergänzen eine Basis B' von U zu einer Basis B von V. Dann ist $W = [B \setminus B']$ ein solcher Komplementärraum. ∎

Bemerkung. In einem endlich dimensionalen Vektorraum V kann man zu jedem Untervektorraum U einen Komplementärraum konkret angeben. Im allgemeinen gibt es hierzu aber viele Möglichkeiten und kein Untervektorraum von V bietet sich

dann in natürlicher Weise als Komplementärraum von U an.

Beispiel. Sei $V = \mathbb{R}^5$. Der Untervektorraum U von V werde von den Vektoren

$$u_1 = \begin{bmatrix} 1 \\ 2 \\ -1 \\ 1 \\ -1 \end{bmatrix}, \quad u_2 = \begin{bmatrix} 2 \\ -2 \\ 1 \\ -2 \\ -1 \end{bmatrix}, \quad u_3 = \begin{bmatrix} 1 \\ 2 \\ -1 \\ -1 \\ -2 \end{bmatrix}$$

erzeugt. Wir suchen einen Komplementärraum W von U. Dazu bestimmen wir eine Basis von U in "Treppenform", die durch Hinzunahme weiterer "Treppen" zu einer Basis von V ergänzt wird.

Der Gaußsche Algorithmus, angewendet auf die Matrix

$$\begin{bmatrix} 1 & 2 & -1 & 1 & -1 \\ 2 & -2 & 1 & -2 & -1 \\ 1 & 2 & -1 & -1 & -2 \end{bmatrix}$$

ergibt die Normalform

$$\begin{bmatrix} 1 & 0 & 0 & 0 & -1/2 \\ 0 & 1 & -1/2 & 0 & -1/2 \\ 0 & 0 & 0 & 1 & 1/2 \end{bmatrix}$$

Wir ergänzen diese zu einer Treppennormalform mit 5 Stufen

$$\begin{bmatrix} 1 & 0 & 0 & 0 & -1/2 \\ 0 & 1 & -1/2 & 0 & -1/2 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1/2 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Somit ist

$$W = \left[\begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \right] \text{ ein Komplementärraum von } U = \left[\begin{bmatrix} 2 \\ 0 \\ 0 \\ 0 \\ -1 \end{bmatrix}, \begin{bmatrix} 0 \\ 2 \\ -1 \\ 0 \\ -1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 2 \\ 1 \end{bmatrix} \right].$$

Mit einer anderen Ergänzung der Treppennormalform erhält man einen anderen Komplementärraum, z.B.

$$W' = \left[\begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \right].$$

In unendlich dimensionalen Vektorräumen ist es im allgemeinen nicht möglich, Komplementärräume konkret anzugeben.

Wir beschreiben nun eine natürliche Konstruktion, die von U ausgehend zu einem neuen Vektorraum führt, der dann in allen praktischen Problemen die Rolle eines Komplementärraumes von U spielt. Diese Konstruktion ist unabhängig von der Dimension von V.

Gegeben seien ein $\mathbb{K}$–Vektorraum V und ein Untervektorraum $U \subset V$. Mit Hilfe von U wird auf V eine Relation $\sim$ erklärt durch

$$x \sim y \;:\Longleftrightarrow\; x - y \in U \;,\; x,y \in V \,.$$

Nach Kap. 1.2 (S.44) ist $\sim$ eine Äquivalenzrelation. Diese ist nun auch mit den Vektorraumverknüpfungen verträglich, d.h. es gilt für alle $x_1, x_2, y_1, y_2 \in V$ und alle $a \in \mathbb{K}$:

(*)
$$\begin{array}{c} \text{Aus } x_1 \sim y_1 \,,\, x_2 \sim y_2 \text{ folgt stets } x_1 + x_2 \sim y_1 + y_2 \,. \\ \\ \text{Aus } x_1 \sim y_1 \text{ folgt stets } a\, x_1 \sim a\, y_1 \,. \end{array}$$

Aus $x_1 \sim y_1$, $x_2 \sim y_2$ folgt nämlich $x_1 - y_1 \in U$, $x_2 - y_2 \in U$, und damit gilt auch $(x_1 + x_2) - (y_1 + y_2) \in U$. Ebenso folgt aus $x_1 \sim y_1$ zunächst $x_1 - y_1 \in U$ und daher auch $a\, x_1 - a\, y_1 = a\,(x_1 - y_1) \in U$.

Für die Faktormenge $V/_{\sim}$ schreiben wir wieder $V/_U$. Jede Äquivalenzklasse $[x]_{\sim}$ ist eine Summe:

$$[x]_{\sim} = \{y \mid y - x \in U\} = x + U.$$

Die Faktormenge $V/_U$ wird mit den folgenden Verknüpfungen zu einem $\mathbb{K}$–Vektorraum:

$$[x]_\sim + [y]_\sim := [x+y]_\sim \quad \text{für alle } [x]_\sim, [y]_\sim \in V/_U,$$
$$a\,[x]_\sim := [a\,x]_\sim \quad \text{für alle } a \in \mathbb{K}, [x]_\sim \in V/_U.$$

Wegen der Eigenschaften (*) sind diese Definitionen unabhängig von der speziellen Wahl der Repräsentanten.

Satz 22 und Definition. *Es seien V ein $\mathbb{K}$–Vektorraum und U ein Untervektorraum von V. Dann ist $V/_U$ mit den durch*

$$[x]_\sim + [y]_\sim := [x+y]_\sim, \quad [x]_\sim, [y]_\sim \in V/_U,$$
$$a[x]_\sim := [a\,x]_\sim, \quad a \in \mathbb{K}, [x]_\sim \in V/_U,$$

gegebenen Verknüpfungen ein $\mathbb{K}$–Vektorraum; er heißt Faktor– oder Quotientenraum von V nach U.

Beweis. Die Vektorraumaxiome lassen sich unmittelbar nachprüfen, wobei das Neutralelement in $(V/_U, +)$ die Klasse $[o]_\sim$ und das Inverse zur Klasse $[x]_\sim$ die Klasse $[-x]_\sim$ ist. ∎

Bemerkung. Für $U = \{o\}$ gilt $[x]_\sim = x + \{o\} = \{x\}$. In diesem Fall kann $V/_{\{o\}}$ mit V identifiziert werden. Für $U = V$ erhalten wir $V/_U = \{[o]_\sim\}$.

Satz 23. *Es seien V ein $\mathbb{K}$–Vektorraum und U ein Untervektorraum von V. Dann gilt:*

$$\dim V/_U + \dim U = \dim V.$$

Beweis. Sei B eine Basis von U. Wir ergänzen B zu einer Basis $B \cup B'$ von V mit $B \cap B' = \emptyset$. Dann gilt $V = U \oplus [B']$. Wir zeigen, daß $\tilde{B} := \{[x]_\sim \mid x \in B'\}$ eine Basis von $V/_U$ ist und daß $|\tilde{B}| = |B'|$ gilt:

$\tilde{B}$ ist ein Erzeugendensystem: Sei $[v]_\sim \in V/_U$ beliebig. Der Vektor $v \in V$ hat

die Darstellung $v = a_1 u_1 + \cdots + a_k u_k + b_1 x_1 + \cdots + b_m x_m$ mit $u_i \in B$, $a_i \in \mathbb{K}$ für $i = 1,\ldots,k$ und mit $x_j \in B'$, $b_j \in \mathbb{K}$ für $j = 1,\ldots,m$. Daraus folgt $[v]_\sim = b_1 [x_1]_\sim + \cdots + b_m [x_m]_\sim$ mit $[x_i]_\sim \in \tilde{B}$ für $i = 1,\ldots,m$.

$\tilde{B}$ ist linear unabhängig und es gilt $|\tilde{B}| = |B'|$: Hierzu genügt es zu zeigen, daß für alle $k \in \mathbb{N}$ und alle linear unabhängigen Vektoren $x_1,\ldots,x_k \in B'$ die Vektoren $[x_1]_\sim,\ldots,[x_k]_\sim$ ebenfalls linear unabhängig sind:

Aus $a_1 [x_1]_\sim + \cdots + a_k [x_k]_\sim = [o]_\sim$ folgt $[a_1 x_1 + \cdots + a_k x_k]_\sim = [o]_\sim$, also $a_1 x_1 + \cdots + a_k x_k \in U$. Wegen $U \cap [B'] = \{o\}$ folgt $a_1 x_1 + \cdots + a_k x_k = o$. Daraus ergibt sich $a_1 = \cdots = a_k = 0$.

Somit gilt: $\dim V = \dim U + \dim [B'] = \dim U + \dim {}^{V}/_{U}$. ∎

Aus dem Beweis von Satz 23 ergibt sich unmittelbar die Aussage (a) des folgenden Korollars.

Korollar 24. **(a)** *Es seien V ein $\mathbb{K}$-Vektorraum, U ein Untervektorraum von V und B eine Basis von U. Ist $B \cup B'$ eine Basis von V und $B \cap B' = \emptyset$, so ist $\{[x]_\sim \mid x \in B'\}$ eine Basis von ${}^{V}/_{U}$.*

(b) *Für jeden Komplementärraum W von U gilt ${}^{V}/_{U} \cong W$.*

Beispiel. Sei $U \subset \mathbb{R}^5$ wieder der Untervektorraum aus dem vorigen Beispiel. Dann bilden die Vektoren

$$\begin{bmatrix} 2 \\ 0 \\ 0 \\ 0 \\ -1 \end{bmatrix}, \begin{bmatrix} 0 \\ 2 \\ -1 \\ 0 \\ -1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 2 \\ 1 \end{bmatrix} \quad \text{bzw.} \quad \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

eine Basis von U bzw. von einem Komplementärraum W von U. Also ist

$$\left\{ \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} + U, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} + U \right\}$$

eine Basis von ${}^{V}/_{U}$.

§ 5 Affine Unterräume eines Vektorraumes

Bisher haben wir die Äquivalenzklassen $x + U$, $x \in V$, U Untervektorraum von V, hauptsächlich im Zusammenhang mit dem Begriff Faktorraum als Elemente eines neuen Vektorraumes kennengelernt. In diesem Abschnitt dagegen wollen wir ihre geometrischen Eigenschaften als Teilmengen des Vektorraumes V untersuchen. Um dies auch durch die Sprechweise deutlich zu machen, geben wir ihnen gleich einen anderen Namen.

Definition. Es seien V ein $\mathbb{K}$–Vektorraum, $x \in V$ und U ein Untervektorraum von V. Dann heißt die Teilmenge $L = x + U$ von V *affiner Unterraum* von V, und U heißt *Richtungsraum* oder kurz *Richtung* von L.

Bemerkung. Sind $L = x + U$ und $\tilde{L} = \tilde{x} + \tilde{U}$ affine Unterräume des $\mathbb{K}$–Vektorraumes V, so ist L genau dann eine Teilmenge von $\tilde{L}$, wenn $U \subset \tilde{U}$ und $x - \tilde{x} \in \tilde{U}$.

Beweis. Sei $x + U \subset \tilde{x} + \tilde{U}$. Dann ist $x \in \tilde{x} + \tilde{U}$, also $x - \tilde{x} \in \tilde{U}$. Für $y \in U$ folgt $x + y \in x + U \subset \tilde{x} + \tilde{U}$, also $x + y - \tilde{x} \in \tilde{U}$. Somit ist $y \in \tilde{U}$, und es gilt $U \subset \tilde{U}$. Umgekehrt folgt aus $x + y \in x + U$ wegen $x - \tilde{x} \in \tilde{U}$ und $U \subset \tilde{U}$ sofort $x + y = \tilde{x} + (x - \tilde{x}) + y \in \tilde{x} + \tilde{U}$. ∎

Aus $L = x + U = \tilde{x} + \tilde{U}$ folgt somit $U = \tilde{U}$, d.h. der Richtungsraum von L ist eindeutig bestimmt. Für den Vektor x gilt dies jedoch nicht, denn für jedes $\tilde{x} \in x + U$ gilt $\tilde{x} - x \in U$, also $x + U = \tilde{x} + U$.

Bezeichnungen und Bemerkungen. **(a)** Die *Dimension* eines affinen Unterraumes $L = x + U$ definieren wir durch $\dim L := \dim U$.

Die nulldimensionalen affinen Unterräume von V heißen *Punkte*. Es sind genau die einelementigen Mengen $x + \{o\} = \{x\}$, $x \in V$. Weil wir sie üblicherweise mit ihrem einzigen Element x identifizieren, nennen wir die Vektoren von V, insbesondere wenn wir geometrische Sachverhalte beschreiben wollen, ebenfalls *Punkte*. Der Punkt x in der Darstellung $L = x + U$ heißt dann auch der *Aufpunkt* von L.

Die eindimensionalen affinen Unterräume heißen *Geraden* und die zweidimensionalen affinen Unterräume heißen *Ebenen*. Ist V n–dimensional und $\dim L = n-1$, so heißt L eine *Hyperebene*.

(b) Affine Unterräume werden oft in Form einer Parameterdarstellung beschrieben:

Es sei $L = x_0 + U$ ein k–dimensionaler affiner Unterraum von V. Ist $\{u_1,...,u_k\}$ eine Basis von U, so läßt sich jeder Punkt $x \in L$ in der Form

$$x = x_0 + a_1 u_1 + \cdots + a_k u_k$$

mit $a_1,...,a_k \in \mathbb{K}$ darstellen. Man nennt dies eine *Parameterdarstellung* von L mit den *Richtungsvektoren* $u_1,...,u_k$ und den *Parametern* $a_1,...,a_k$.

Beispiele. Parameterdarstellung einer Geraden: $x = x_0 + a\,u$, $a \in \mathbb{K}$, $u \neq o$.
Parameterdarstellung einer Ebene: $x = x_0 + a_1 u_1 + a_2 u_2$, $a_1, a_2 \in \mathbb{K}$, u_1, u_2 linear unabhängig.

(c) Seien $A \in \mathbb{K}^{m\times n}$ und $b \in \mathbb{K}^m$. Die Lösungsmenge des linearen Gleichungssystems $A\,x = b$ ist entweder die leere Menge oder ein affiner Unterraum von $\mathbb{K}^n$ der Dimension $n - \operatorname{Rg} A$. Insbesondere ist die Lösungsmenge der linearen Gleichung $a_1 x_1 + \cdots + a_n x_n = b$, $b \in \mathbb{K}$, für $(a_1,...,a_n) \neq (0,...,0)$ eine Hyperebene in $\mathbb{K}^n$.

(d) Umgekehrt ist in $\mathbb{K}^n$ jeder k–dimensionale affine Unterraum auch Lösungsmenge eines linearen Gleichungssystems $A\,x = b$ mit $A \in \mathbb{K}^{m\times n}$, $\operatorname{Rg} A = n - k$ und $b \in \mathbb{K}^m$.

Beweis. Sei $L = x_0 + U$, $\dim U = k$. Der Untervektorraum U ist nach der Bemerkung von S.116 Lösungsmenge eines LGS $A\,x = o$ mit $A \in \mathbb{K}^{m\times n}$ und $\operatorname{Rg} A = n - k$. Damit gilt $x \in L$ genau dann, wenn $A\,(x - x_0) = o$, d.h. wenn $A\,x = A\,x_0 =: b$. ∎

Die Bemerkungen (c) und (d) lassen sich auch geometrisch formulieren: Der Schnitt endlich vieler Hyperebenen in $\mathbb{K}^n$ ist entweder leer oder ein affiner Unterraum von $\mathbb{K}^n$. Umgekehrt ist jeder k–dimensionale affine Unterraum in $\mathbb{K}^n$ Schnitt von endlich vielen Hyperebenen.

Allgemein gilt für den Schnitt affiner Unterräume die folgende Aussage.

Satz 25. *Es seien V ein $\mathbb{K}-$Vektorraum und $\mathcal{M}$ ein nichtleeres System affiner Unterräume von V. Dann ist der Schnitt*

$$M = \bigcap_{L \in \mathcal{M}} L$$

entweder leer oder ein affiner Unterraum von V mit Richtungsraum

$$U_M = \bigcap_{L \in \mathcal{M}} U_L .$$

Dabei bezeichnet U_L den Richtungsraum von L.

Beweis. Sei $M \neq \emptyset$. Dann gibt es einen Punkt $x \in V$, der in allen Unterräumen $L \in \mathcal{M}$ liegt. Diese lassen sich damit in der Form $L = x + U_L$ darstellen. Es folgt

$$\bigcap_{L \in \mathcal{M}} L = \bigcap_{L \in \mathcal{M}} x + U_L = x + \bigcap_{L \in \mathcal{M}} U_L = x + U_M .$$

Da nach Korollar 3 der Schnitt U_M ein Untervektorraum von V ist, gilt die Behauptung. ∎

Beispiel. Im $\mathbb{R}^4$ seien die affinen Unterräume L_1 und L_2 gegeben:

$$L_1 = \begin{bmatrix} 2 \\ 0 \\ 0 \\ 1 \end{bmatrix} + \left[\begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} \right] , \quad L_2 = \begin{bmatrix} 3 \\ 1 \\ 0 \\ 0 \end{bmatrix} + \left[\begin{bmatrix} -1 \\ 1 \\ 2 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \right] .$$

Wir wollen ihren Schnitt bestimmen. Dies kann mit Hilfe der obigen Bemerkung (d) geschehen oder aber wie folgt:

$x \in L_1 \cap L_2 \iff$ es gibt reelle Zahlen a_1, a_2, a_3, b_1, b_2 mit

$$\begin{bmatrix} 2 \\ 0 \\ 0 \\ 1 \end{bmatrix} + a_1 \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} + a_2 \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} + a_3 \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} = x = \begin{bmatrix} 3 \\ 1 \\ 0 \\ 0 \end{bmatrix} + b_1 \begin{bmatrix} -1 \\ 1 \\ 2 \\ 0 \end{bmatrix} + b_2 \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} .$$

Wir erhalten daraus ein inhomogenes lineares Gleichungssystem mit den Unbekannten a_1, a_2, a_3, b_1, b_2 und der zugehörigen erweiterten Matrix

$$\left[\begin{array}{ccccc|c} 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & -1 & -1 & 1 \\ 0 & 1 & 1 & -2 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 \end{array}\right]$$

Der Gaußsche Algorithmus führt nach einfacher Rechnung zu folgender Treppennormalform

$$\left[\begin{array}{ccccc|c} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -2 & -1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{array}\right]$$

Daraus lesen wir ab: $b_2 = 1$, $b_1 \in \mathbb{R}$ beliebig. Somit gilt

$$x = \begin{bmatrix} 3 \\ 1 \\ 0 \\ 0 \end{bmatrix} + b_1 \begin{bmatrix} -1 \\ 1 \\ 2 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 3 \\ 2 \\ 0 \\ 0 \end{bmatrix} + b_1 \begin{bmatrix} -1 \\ 1 \\ 2 \\ 0 \end{bmatrix}, \quad b_1 \in \mathbb{R}.$$

Also ist $L_1 \cap L_2$ eine Gerade.

Zum Abschluß dieses Paragraphen wollen wir die gegenseitige Lage affiner Unterräume an einigen Beispielen erläutern. Hierbei spielt der Begriff der Parallelität eine wichtige Rolle.

Definition. Die affinen Unterräume L_1 und L_2 heißen *parallel*, in Zeichen $L_1 \parallel L_2$, falls für die zugehörigen Richtungsräume U_1, U_2 gilt: $U_1 \subset U_2$ oder $U_2 \subset U_1$.

Bemerkungen. **(a)** Parallelität ist offensichtlich eine reflexive und symmetrische Relation, sie ist aber im allgemeinen nicht transitiv. So sind zwei sich schneidende Geraden in einer Ebene des Raumes zwar zu dieser Ebene parallel, aber sie selbst

sind nicht parallel. Beschränkt man sich jedoch auf affine Unterräume gleicher Dimension, so ist die Parallelität auch transitiv, also eine Äquivalenzrelation.

(b) Parallele affine Unterräume, die nicht ineinander enthalten sind, haben einen leeren Durchschnitt.

Speziell bei Geraden ist noch eine weitere Bezeichnung üblich: Zwei Geraden heißen *windschief*, falls sie weder parallel sind noch einen Punkt gemeinsam haben.

Zwei Geraden sind also genau dann windschief, wenn sie keinen Punkt gemeinsam haben und ihre Richtungen verschieden sind. In diesem Fall gibt es keine Ebene, die beide Geraden enthält (vgl. folgende Beispiele).

Beispiele. **(a)** Gegenseitige Lage zweier Geraden g und h in $\mathbb{R}^n$, $n \geq 2$:

Es seien $g = x + U_g$ und $h = y + U_h$.

$n = 2$: Ist $g \cap h \neq \emptyset$, so erhalten wir für $\dim (U_g \cap U_h) = 0$ als Schnittmenge einen Punkt und für $\dim (U_g \cap U_h) = 1$ folgt $U_g = U_h$, also $g = h$.

Ist $g \cap h = \emptyset$, so folgt aus $\dim (U_g \cap U_h) = 1$ wieder $U_g = U_h$, also $g \parallel h$, $g \neq h$. Der Fall $\dim (U_g \cap U_h) = 0$ kann hier nicht auftreten. Andernfalls wäre $\mathbb{R}^2$ direkte Summe von U_g und U_h und wir erhielten $x - y = z_1 + z_2$ mit $z_1 \in U_g$ und $z_2 \in U_h$. Also wäre $x - z_1 = y + z_2 \in g \cap h$ im Widerspruch zur Vorausetzung $g \cap h = \emptyset$.

$n \geq 3$: Für $g \cap h \neq \emptyset$ ergibt sich wie oben, daß entweder $g = h$ ist oder g und h sich in einem Punkt schneiden.

Für $g \cap h = \emptyset$ erhalten wir im Fall $\dim (U_g \cap U_h) = 0$, daß g und h windschief sind. Dann gibt es keine Ebene L, die sowohl g als auch h enthält. Andernfalls wäre $U_L = U_g \oplus U_h$ und $x - y \in U_g \oplus U_h$, woraus wieder $g \cap h \neq \emptyset$ folgte. Gilt $\dim (U_g \cap U_h) = 1$, so sind g und h parallel.

(b) Gegenseitige Lage zweier Ebenen L_1 und L_2 in $\mathbb{R}^n$, $n \geq 3$:

Es seien $L_1 = x_1 + U_1$ und $L_2 = x_2 + U_2$.

$n = 3$: Ist $L_1 \cap L_2 \neq \emptyset$, so ist der Schnitt nach Satz 25 ein affiner Unterraum. Je nach der Dimension des zugehörigen Richtungsraumes $U = U_1 \cap U_2$ erhalten wir

die folgenden Fälle: Für dim $U = 2$ ist $U_1 = U_2$, also $L_1 = L_2$ und für dim $U = 1$ ist der Schnitt eine Gerade. Der Fall dim $U = 0$ kann hier nicht auftreten, da andernfalls die Summe von U_1 und U_2 direkt wäre, also die Dimension 4 hätte, im Widerspruch dazu, daß $U_1 \oplus U_2$ ein Untervektorraum von $\mathbb{R}^3$ ist.

Ist $L_1 \cap L_2 = \emptyset$, so erhalten wir für dim $U = 2$, daß die Ebenen parallel sind. Die restlichen Fälle können nicht auftreten: Gilt nämlich dim $U = 1$, so ergänzen wir eine Basis $\{u\}$ von U mit geeigneten Vektoren $u_1 \in U_1$ und $u_2 \in U_2$ zu einer Basis $\{u_1, u_2, u\}$ von $\mathbb{R}^3$. Für die Aufpunkte $x_1 \in L_1$ und $x_2 \in L_2$ erhalten wir dann

$$x_1 - x_2 = a_1 u_1 + a_2 u_2 + a u, \text{ also } x_1 - a_1 u_1 - \frac{a}{2} u = x_2 + a_2 u_2 + \frac{a}{2} u$$

und somit den Widerspruch $L_1 \cap L_2 \neq \emptyset$. Der Fall dim $U = 0$ führt wieder zu dem Widerspruch dim $(U_1 \oplus U_2) = 4$.

$n = 4$: Hier kann für $L_1 \cap L_2 \neq \emptyset$ der Schnitt auch noch ein Punkt sein, und für $L_1 \cap L_2 = \emptyset$ ist jetzt auch der Fall dim $U = 1$ möglich. Dann sind die Ebenen nicht parallel und haben auch keinen Punkt gemeinsam, aber es gibt eine Gerade, die sowohl zu L_1 als auch L_2 parallel ist. Der Fall $L_1 \cap L_2 = \emptyset$ und dim $U = 0$ kann für $n = 4$ ebenfalls nicht auftreten, er führt wieder zu dem Widerspruch $L_1 \cap L_2 \neq \emptyset$.

Für $n > 4$ sind alle Fälle möglich.

Mit den gleichen Methoden wird die gegenseitige Lage von Geraden und Ebenen in $\mathbb{R}^n$, $n \geq 3$, untersucht. Wir überlassen die Einzelheiten der Durchführung als Übungsaufgabe.

Eine ausführlichere Behandlung affiner Unterräume wird im Rahmen der affinen Geometrie in Kapitel 6 erfolgen.