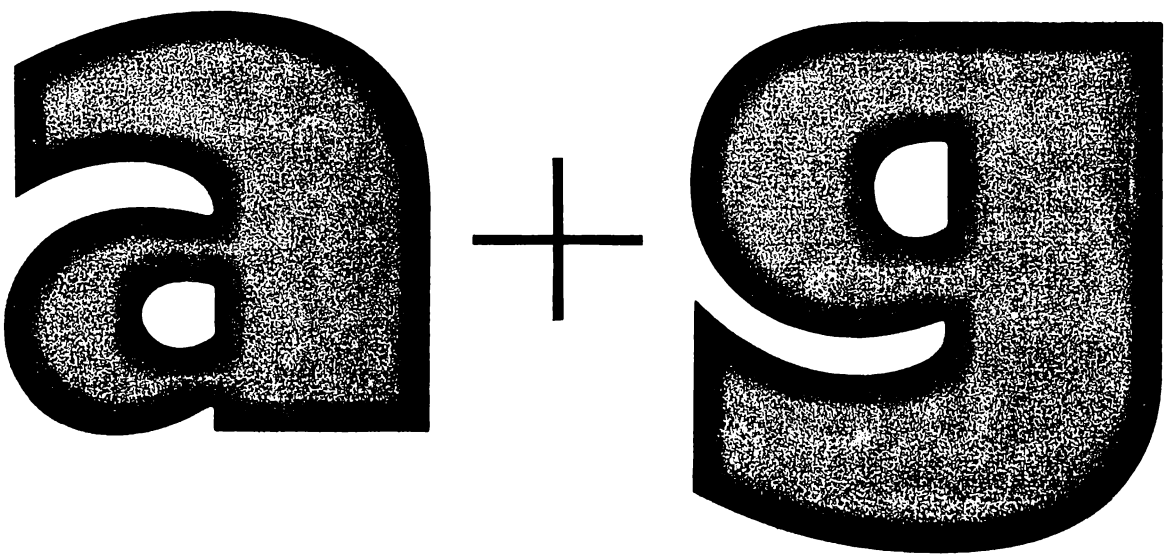
A. L. Oniščik R. Sulanke

ALGEBRA UND GEOMETRIE

Eine Einführung



Hochschulbücher für Mathematik

Gegründet von H. Grell, K. Maruhn und W. Rinow

Band 87

Algebra und Geometrie

1. Eine Einführung

von A. L. Oniščik und R. Sulanke

Mit 12 Abbildungen

VEB Deutscher Verlag der Wissenschaften
Berlin 1986

ISBN 3-326-00020-0
ISSN 0073-2842

Verlagslektor: Erika Arndt
Verlagshersteller: Sabine Ziebell, Norma Braun
Umschlaggestaltung: Alfred Mähler

Lizenz-Nr. 206 · 435/65/86
Printed in the German Democratic Republic
Gesamtherstellung: IV/2/14 VEB Druckerei „Gottfried Wilhelm Leibniz“,
4450 Gräfenhainichen · 6547
LSV 1024
Bestellnummer: 571 440 2
03600

Vorwort

Die Struktur des Lehrbuches blieb erhalten, lediglich die Gliederung in die Teile I, II wurde aufgehoben. Im einzelnen wurden zahlreiche Verbesserungen ausgeführt; das betrifft besonders die Übungen. Gegenüber dem 1977 erschienenen Studienbuch wurden folgende Ergänzungen vorgenommen: Es wurden die rationalen Funktionen in mehreren Unbestimmten aufgenommen, die äquiaffine Geometrie und die spezielle lineare Gruppe kurz erwähnt und die Beziehungen zwischen den Begriffen „alternierend" und „schiefsymmetrisch" präzisiert. Ferner haben wir den Sturmschen Satz über die Nullstellen reeller Polynome eingefügt. Dagegen konnten wir uns nicht entschließen, die Mengenlehre streng axiomatisch aufzubauen, wie es einer unser Kritiker forderte; wir betrachten sie als einen Bestandteil der „naiven" Logik, die wir wie in jeder Wissenschaft üblich anwenden, ohne sie näher zu begründen. In diesem Sinne spielt das Kapitel 0, die Einführung, eine besondere Rolle gegenüber den anderen; es dient nur der Präzisierung des mathematischen Sprachgebrauchs und erhebt nicht den Anspruch einer strengen Einführung in die Grundlagen der Mathematik. Gleichfalls mußten wir uns aus Zeit- und Raumgründen historischer Kommentare enthalten. Wenn mitunter einzelne Sätze oder Begriffe nach einem Mathematiker benannt werden, so geschieht das der Tradition folgend und bedeutet keine Aussage über die Quellen. Schließlich wurde das Literaturverzeichnis aktualisiert; dem Inhaltsverzeichnis wurden Angaben über die folgenden Bände 2, „Moduln und Algebren", und 3, „Projektive und Cayley-Kleinsche Geometrien" angefügt, die in den nächsten Jahren erscheinen werden.

Wir danken Frau J. Kerger für die technische Vorbereitung des Manuskripts der zweiten Auflage und Fräulein E. Arndt für die wiederum sehr präzise redaktionelle Bearbeitung herzlich. Frau I. Gröger machte uns beim Lesen der Korrekturen auf eine Reihe von Druckfehlern aufmerksam und half, einige Flüchtigkeiten zu korrigieren, wofür wir uns verbindlichst bedanken. Dem VEB Druckerei „Gottfried Wilhelm Leibniz" gebührt Dank und Anerkennung für den sorgfältigen Satz und die ausgezeichnete Arbeit bei der Herstellung des Buches.

Berlin und Moskau, im Juni 1986

A. L. Oniščik
R. Sulanke

Vorwort zur Studienbuchausgabe

Die Entwicklung der Mathematik in der zweiten Hälfte unseres Jahrhunderts läßt neben einer immer weiter gehenden Aufspaltung in anwendungsorientierte Spezialgebiete zweifellos auch die Tendenz erkennen, die für die Vielfalt aller Anwendungen grundlegenden klassischen Disziplinen Geometrie, Analysis und Algebra als eine Einheit zu betrachten und zu einer Synthese dieser Gebiete zu gelangen. Diese für die mathematische Forschung sehr fruchtbare Tendenz zu fördern und sie bereits vom ersten Studienjahr an den Mathematikstudenten nahezubringen ist ein wesentliches Anliegen unseres Lehrbuches. Es beginnt nach einer kurzen Beschreibung der notwendigen mengentheoretischen Begriffe mit einem algebraischen Teil, den Kapiteln 1 bis 3, in dem die wichtigsten Tatsachen über Gruppen, Ringe und Körper dargestellt sind. Darauf aufbauend führen die Kapitel 4 bis 6 von der axiomatischen Begründung der Punkt- und Vektorräume über die affine zur euklidischen Geometrie. Die Beziehungen zur Analysis kommen direkt nur in einigen Beispielen und Bemerkungen zur Sprache; wir waren jedoch bemüht, durch Stoffauswahl und Art der Darstellung einen großen Teil der für eine moderne Analysis-Ausbildung benötigten algebraischen und geometrischen Hilfsmittel bereitzustellen. Die Traditionen und Erfahrungen in der Grundausbildung der Mathematikstudenten an der Humboldt-Universität zu Berlin und der Staatlichen Lomonosov-Universität in Moskau sind natürlich in dieses Lehrbuch eingeflossen. Den Leitungen der genannten Universitäten möchten wir herzlich dafür danken, daß sie unser Vorhaben in ihren Freundschaftsvertrag aufnahmen und so unsere Zusammenarbeit ermöglichten.

Für eine vielseitige und anwendungsbereite Darlegung der n-dimensionalen affinen Geometrie über einem beliebigen Körper sind natürlich einige algebraische Kenntnisse notwendig. Daher ist der algebraische Teil dem geometrischen vorangestellt. Ein Leser, der schneller zur Geometrie vordringen möchte, braucht jedoch nicht das gesamte algebraische Material durchzuarbeiten; es genügt, neben der Mengenlehre (Kapitel 0) die §§ 1.1, 1.2, 1.4, 2.1, 2.2, 2.9 zu lesen. Die übrigen beim Aufbau der Geometrie benötigten algebraischen Hilfsmittel können später nachgeholt werden. Durch viele Verweise, ein ausführliches Register und ein kurzes Verzeichnis ähnlicher oder weiterführender Literatur bemühten wir uns, ein Lehrbuch zu schreiben, das zu recht unterschiedlich konzipierten Vorlesungen benutzt werden kann.

Trotz verhältnismäßig knapper Darstellung waren der Stoffauswahl durch den vorgesehenen Umfang enge Grenzen gesetzt. Die Anzahl der Abbildungen und motivierenden einfachen Beispiele wurden auf ein Minimum beschränkt. Wir möchten den Leser daher ermuntern, sich selbst Skizzen anzufertigen, einfache Beispiele zu bilden und durchzurechnen und sich intensiv mit den zahlreich eingefügten Übungen zu beschäftigen, die zum Teil später im Haupttext angewandt werden. Die Arbeit an den Übungen wird durch Hinweise erleichtert. Wir haben einen Teil der Übungen auch dazu benutzt, in kurzer Form wichtiges ergänzendes Material bereitzustellen.

Für die sorgfältige Ausführung der mühevollen Schreibmaschinenarbeit danken wir Frau Bärwolf und Frau Rohde. Unser Dank gebührt auch Herrn Prof. Dr. H. Reichardt, der das Manuskript begutachtete und durch kritische und interessante Bemerkungen zu seiner Verbesserung beitrug. Den Herren Dr. H. Gollek und Dr. J. Lehmann danken wir für ihre sehr schnelle und wertvolle Hilfe bei der Bogenkorrektur. Die sachkundige und präzise redaktionelle Bearbeitung des Manuskripts leistete Fräulein E. Arndt, der wir für zahlreiche Ratschäge und Korrekturen herzlich danken.

Berlin und Moskau, im Februar 1976

A. L. Oniščik
R. Sulanke

Inhalt

Zum Inhalt der Bände 2 und 3

Band 2. Moduln und Algebren

7. Moduln

Freie Moduln — Noethersche und Artinsche Ringe und Moduln — Struktur endlich erzeugter Moduln über einem Hauptidealring — Hauptsatz über endlich erzeugte abelsche Gruppen — Tensorprodukte von Moduln

8. Algebren

Tensoralgebren, symmetrische und äußere Algebren — Liesche Algebren — Körpererweiterungen, Galoissche Theorie — Lineare Darstellungen von Gruppen, assoziativen und Lieschen Algebren — Halbeinfache Moduln, Ringe und Algebren — Divisionsalgebren — Cliffordsche und Weylsche Algebren — Endlich erzeugte kommutative Algebren und affine algebraische Mannigfaltigkeiten

9. Darstellungen endlicher Gruppen

Charaktere und Darstellungsringe endlicher Gruppen — Die irreduziblen Darstellungen der symmetrischen Gruppen — Young-Diagramme — Tensordarstellungen

Band 3. Projekte und Cayley-Kleinsche Geometrien

10. Projektive Geometrie

Zentralprojektionen, projektive Räume, homogene Koordinaten — Kollineationen, projektive Abbildungen und Doppelverhältnisse — Affine Geometrie vom projektiven Standpunkt — Dualität, Korrelationen — Nullsysteme und lineare Geradenkomplexe — Polaritäten und Quadriken — Hopfsche Faserungen

11. Geometrien der klassischen Gruppen

Das Exponential für lineare Liesche Gruppen — Die klassischen Gruppen und ihre Lie-Algebren — Affine und projektive Geometrien der klassischen Gruppen — Der Satz von WITT — Elliptische und hyperbolische Geometrien — Pseudo-euklidische Geometrien und spezielle Relativitätstheorie — Möbius-Geometrie — Liesche Kugelgeometrie — Symplektische Geometrie — F. KLEINS Erlanger Programm

0. Einleitung, Mengenlehre

§ 1. Einleitung

Ohne erschöpfend sein zu wollen, möchten wir in diesen einführenden Bemerkungen versuchen, den allgemeinen Charakter der mathematischen Disziplinen Algebra und Geometrie anzudeuten und ihre Wechselbeziehungen, soweit sie den in diesem Lehrbuch behandelten Stoff betreffen, kurz zu beschreiben.

Dem Anfänger wird die Algebra häufig als „Buchstabenrechnen" dargestellt. Das ist natürlich nur ein äußeres Erscheinungsbild: Die Buchstaben stehen als Variable oder Symbole für bestimmte mathematische Objekte mit gegebenen Eigenschaften, und die zwischen ihnen auftretenden mathematischen Relations- oder Operationszeichen $=, \leq, \mapsto, +, -, \cdot$ usw. drücken Beziehungen zwischen diesen Objekten aus. Die Eigenschaften der zu untersuchenden Objekte werden durch eine Reihe von Axiomen beschrieben, die einige Grundbegriffe des zu betrachtenden Bereiches und deren Grundeigenschaften fixieren. Aus den Axiomensystemen wird dann die jeweilige Theorie entwickelt. So werden in der Algebra sogenannte „algebraische Strukturen" untersucht; das sind Mengen, in denen eine oder mehrere Operationen gegeben sind, welche bestimmte, die jeweilige Struktur charakterisierende Axiome erfüllen.

In der Algebra haben sich etwa gegen Ende des vorigen Jahrhunderts drei wichtige Klassen von algebraischen Strukturen herausgeschält: die Gruppen, Ringe und Körper. Die Entwicklung dieser Strukturen hängt eng mit den Anwendungen der Mathematik zusammen: Insbesondere war die Frage nach der Lösung algebraischer Gleichungen ein wichtiger Ausgangspunkt. Zum Beispiel hat die Untersuchung der Nullstellen von Polynomen mit zur Entwicklung der Gruppentheorie geführt. Auch heute beruhen viele Näherungsverfahren der numerischen Mathematik letztlich auf der Lösung linearer Gleichungssysteme oder auf Betrachtungen über Polynome.

Andererseits hat man es seit R. DESCARTES und in immer stärkerem Maße seit Beginn des vorigen Jahrhunderts verstanden, mit Hilfe von Koordinatensystemen, Vektoren und anderen algebraischen Begriffen geometrische Probleme in algebraischer Form darzustellen und mit algebraischen Methoden zu behandeln. Hierdurch entstand eine intensive Wechselwirkung zwischen Algebra und Geometrie, die die Entwicklung der modernen Mathematik auch heute noch entscheidend bestimmt. Der wichtigste, gleichzeitig geometrische und algebraische Begriff ist

hier der des Vektorraumes, auf dem bei „analytischer" Darstellung die Axiomatik der Geometrie aufbaut. Wir bemerken, daß man früher (und oft auch heute noch) die Koordinaten oder Vektoren anwendende Geometrie als „analytische Geometrie" bezeichnete; diesen Namen wollen wir vermeiden, einerseits, weil er eine irreführende Assoziation zur Analysis hin weckt, und andererseits, weil neuerdings die geometrische Theorie der analytischen Funktionen mehrerer Variabler mit ihm bedacht wird.

In unserer Einführung erscheint die Geometrie als Anwendungsgebiet der Algebra, was die Wechselwirkung zwischen beiden Gebieten etwas verschleiert. Man möge stets beachten, daß viele algebraische Bereiche, vor allem die grundlegenden Zahlenbereiche, eine unmittelbare geometrische Veranschaulichung besitzen und daß viele algebraische Begriffe im Zusammenhang mit der Lösung geometrischer Probleme entstanden sind. Daß wir mit den Elementen der Algebra beginnen, hat vor allem zwei Gründe: Erstens sind die algebraischen Strukturen begrifflich einfacher zu fassen als die geometrischen, und zweitens sind sie besser geeignet, die abstrakte, der modernen Mathematik eigene axiomatische Methode herauszuarbeiten. Wir wollen uns im folgenden bemühen, die Zusammenhänge zwischen Algebra und Geometrie hervorzuheben, und dabei nicht auf diesem abstrakten Standpunkt verharren, sondern spätestens von Kapitel 4 an auch die geometrische Anschauung gehörig zu Worte kommen lassen.

Zum Verständnis dieses Lehrbuches genügt die Kenntnis des üblichen Schulstoffes, von dem ausgiebig Gebrauch gemacht wird. Auch die Beweismethode der vollständigen Induktion wird als bekannt vorausgesetzt. Einige Bezeichnungen und Definitionen der Mengenlehre werden im folgenden Paragraphen zusammengestellt.

§ 2. Elemente der Mengenlehre

In diesem Abschnitt behandeln wir die wichtigsten Begriffe und Regeln der Mengenlehre. Dabei stellen wir uns auf einen naiven Standpunkt, d. h., wir betrachten die Mengenlehre als Bestandteil der Logik, die wir als gegeben voraussetzen und in diesem Buch nicht exakt begründen. Für einen axiomatischen, strengen Aufbau der Mengenlehre verweisen wir auf D. Klaua [1, 2] und für eine breitere Erläuterung ihrer Grundlagen auf G. Asser [1].

Schon aus der Elementarmathematik ist bekannt, daß die mathematischen Objekte uns nicht nur als Individuen gegenübertreten, sondern in Gesamtheiten organisiert sind, die man Mengen nennt. Beispiele solcher Mengen, für die wir gleich Bezeichnungen festlegen wollen, da sie sehr häufig auftreten, sind:

$\mathbf{N}$ – die Menge der natürlichen Zahlen (ohne Null),
$\mathbf{N}_0$ – die Menge der natürlichen Zahlen einschließlich der Null,
$\mathbf{Z}$ – die Menge der ganzen Zahlen,
$\mathbf{Q}$ – die Menge der rationalen Zahlen,
$\mathbf{R}$ – die Menge der reellen Zahlen,
$\mathbf{C}$ – die Menge der komplexen Zahlen (vgl. § 2.3).

In der Geometrie können wir eine Ebene als Menge ihrer Punkte betrachten, wir können die Menge aller Geraden der Ebene bilden usw.

Im allgemeinen bezeichnen wir Mengen mit großen Buchstaben, etwa A, B, ..., M, ..., X. Die Elemente einer Menge werden häufig mit kleinen Buchstaben bezeichnet; die Schreibweise

$$a \in M \tag{1}$$

bedeutet, daß *a Element der Menge M* ist; die Verneinung dieser Beziehung wird durch

$$a \notin M \tag{2}$$

(lies: „*a ist nicht Element von M*") gekennzeichnet.

Der Mengenbegriff und die Elementbeziehung (1) sind Grundbegriffe, die keiner expliziten Definition unterliegen. Wir stellen uns eine Menge stets als wohlbestimmte Zusammenfassung ihrer Elemente vor; eine Menge ist gegeben, wenn klar ist, für welche Individuen a die Beziehung (1) gilt, wobei jedes Individuum a höchstens einmal in der Menge M vorkommt. Zum Beispiel deutet die Schreibweise $N_3 = \{1, 2, 3\}$, $\mathbf{N}_0 = \{0, 1, ..., n, ...\}$ an, aus welchen Elementen diese Mengen bestehen; allgemein definieren wir Mengen durch Angabe ihrer Elemente in geschweiften Klammern. Besteht eine Menge nur aus endlich vielen Elementen, so kann man sie durch direkte Angabe definieren; z. B. ist

$$N_n := \{1, ..., n\} \qquad (n \in \mathbf{N}) \tag{3}$$

die Menge der ersten n natürlichen Zahlen. Das Zeichen $:=$ bedeutet stets, daß das links stehende (neue) Symbol durch den rechts stehenden Ausdruck definiert wird, dessen Bestandteile bereits gegeben (bekannt) sind. Allgemeiner kann man Mengen durch eine sie charakterisierende Eigenschaft definieren. So bedeutet z. B.

$$2\mathbf{Z} := \{m \mid m \in \mathbf{Z} \text{ und } m = 2k,\ k \in \mathbf{Z}\} \tag{4}$$

die Menge aller geraden Zahlen. Kürzer schreibt man dafür auch

$$2\mathbf{Z} := \{2k\}_{k \in \mathbf{Z}}; \tag{5}$$

das angefügte $k \in \mathbf{Z}$ gibt an, daß k die Menge $\mathbf{Z}$ durchläuft. Das allgemeine Schema der Definition einer Menge ist

$$A := \{a \mid H(a)\}; \tag{6}$$

dabei ist a das Symbol für die Elemente der zu definierenden Menge und $H(a)$ eine sie eindeutig charakterisierende Bedingung; in Worten bedeutet (6): A ist die Menge aller derjenigen Elemente a, welche die Bedingung $H(a)$ erfüllen. Zum Beispiel ist (3) gleichbedeutend mit $N_n = \{a \mid a \in \mathbf{Z} \text{ und } 1 \leqq a \leqq n\}$.

Definition 1. Wir sagen, die Menge *A sei enthalten in der Menge B* oder *B* enthalte A, in Zeichen $A \subseteq B$ (oder auch $B \supseteq A$), wenn mit $a \in A$ auch stets $a \in B$ gilt. Ist dabei $A \neq B$, so schreiben wir $A \subset B$.

Beispiel 1. Es gilt

$$\mathbf{N} \subset \mathbf{N}_0 \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}. \tag{7}$$

Beispiel 2. Unter der *leeren Menge* $\emptyset$ versteht man die Menge, die kein Element enthält. Offenbar gilt für alle Mengen A

$$\emptyset \subseteqq A, \qquad A \subseteqq A . \tag{8}$$

Den einfachen Beweis der folgenden Eigenschaften der Enthaltenseinsrelation $\subseteqq$ überlassen wir dem Leser:

1. *Aus* $A \subseteqq B$ *und* $B \subseteqq C$ *folgt* $A \subseteqq C$.
2. *Aus* $A \subseteqq B$ *und* $B \subseteqq A$ *folgt* $A = B$.

Definition 2. Es sei E eine Menge. Unter der *Potenzmenge* $\mathfrak{P}(E)$ versteht man die Menge aller *Teilmengen* von E:

$$\mathfrak{P}(E) := \{A \mid A \subseteqq E\} . \tag{9}$$

Nach (8) gilt also $\emptyset \in \mathfrak{P}(E)$, $E \in \mathfrak{P}(E)$. Die Teilmengen von $\mathfrak{P}(E)$ nennt man auch *Mengensysteme*.

Übung 1. Für die Menge N_n (vgl. (3)) beweise man: $\mathfrak{P}(N_n)$ enthält genau 2^n Elemente.

Für $A, B \in \mathfrak{P}(E)$ definiert man folgende *Mengenoperationen*:

1. *Durchschnitt* von A und B

$$A \cap B := \{x \mid x \in A \text{ und } x \in B\}; \tag{10}$$

gilt speziell $A \cap B = \emptyset$, so heißen A, B *disjunkt*.

2. *Vereinigung* von A und B

$$A \cup B := \{x \mid x \in A \text{ oder } x \in B\} . \tag{11}$$

3. *Differenz* von A und B

$$A \setminus B := \{x \mid x \in A \text{ und } x \notin B\} . \tag{12}$$

Ist eine feste Menge E als „Grundmenge" gegeben, so versteht man unter dem *Komplement der Menge* $A \in \mathfrak{P}(E)$ die Menge

$$\mathsf{C}A := E \setminus A . \tag{13}$$

Für die so erklärten Operationen $\cap$, $\cup$, $\setminus$ beweist man leicht folgende Eigenschaften

1. die *assoziativen Gesetze*

$$(A \cap B) \cap C = A \cap (B \cap C) , \tag{14}$$

$$(A \cup B) \cup C = A \cup (B \cup C) ; \tag{15}$$

2. die *distributiven Gesetze*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) , \tag{16}$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) ; \tag{17}$$

3. die *kommutativen Gesetze*

$$A \cap B = B \cap A\,, \tag{18}$$

$$A \cup B = B \cup A\,; \tag{19}$$

4. $$(A \setminus B) \cap C = (A \cap C) \setminus (B \cap C)\,, \tag{20}$$

$$(A \setminus B) \cup B = A \cup B\,. \tag{21}$$

Auf Grund von (14) und (15) kann man leicht die Definition (10) bzw. (11) auf endlich viele Mengen ausdehnen; wegen der Assoziativität kommt es ja nicht auf die Reihenfolge der Anwendung der Operationen an. Jedoch braucht man sich damit nicht aufzuhalten, da man leicht die folgende, allgemeine Definition formulieren kann:

Definition 3. Es sei E eine Menge und $\mathfrak{S} \subseteq \mathfrak{P}(E)$ ein System von Teilmengen. Dann heißt

$$\bigcap_{A \in \mathfrak{S}} A := \{x \mid x \in A \text{ für alle } A \in \mathfrak{S}\} \tag{22}$$

der *Durchschnitt des Mengensystems* $\mathfrak{S}$ und

$$\bigcup_{A \in \mathfrak{S}} A := \{x \mid \text{es gibt ein } A \in \mathfrak{S} \text{ mit } x \in A\} \tag{23}$$

die *Vereinigung des Mengensystems* $\mathfrak{S}$.

Man beweist leicht: $\bigcap_{A \in \mathfrak{S}} A$ *ist die größte Menge, die in allen Mengen* $A \in \mathfrak{S}$ *enthalten ist*, d. h., gilt für eine Menge B die Beziehung $B \subseteq A$ für alle $A \in \mathfrak{S}$, so ist auch $B \subseteq \bigcap_{A \in \mathfrak{S}} A$. Analog *ist* $\bigcup_{A \in \mathfrak{S}} A$ *die kleinste Menge, die alle Mengen* $A \in \mathfrak{S}$ *enthält*, d. h., gilt $B \supseteq A$ für alle $A \in \mathfrak{S}$, so ist auch $B \supseteq \bigcup_{A \in \mathfrak{S}} A$. Man sagt, daß $\mathfrak{P}(E)$ bezüglich der Ordnungsrelation $\subseteq$ ein *vollständiger Verband sei*, vgl. Beispiel 15 weiter unten.

Übung 2. Man beweise für $\mathfrak{S} \subseteq \mathfrak{P}(E)$:

$$C\left(\bigcap_{A \in \mathfrak{S}} A\right) = \bigcup_{A \in \mathfrak{S}} CA\,,$$

$$C\left(\bigcup_{A \in \mathfrak{S}} A\right) = \bigcap_{A \in \mathfrak{S}} CA\,.$$

Ein zweiter fundamentaler Begriff, den wir hier nicht explizit definieren wollen, ist der einer Zuordnung. Um ihn in voller Allgemeinheit beschreiben zu können, müssen wir den Begriff einer Klasse erläutern. Unter einer *Klasse* versteht man eine Gesamtheit mathematischer Objekte, die lediglich durch ihre Eigenschaften, nicht aber als geschlossene Gesamtheit von Individuen, charakterisiert sind. Jede Menge können wir als eine Klasse betrachten, aber nicht umgekehrt. Zum Beispiel können wir von der Klasse aller Mengen sprechen, nicht aber von der Menge aller Mengen. Offenbar können wir nämlich „alle Mengen" niemals als eine in sich geschlossene Gesamtheit von Individuen auffassen; denn durch einen rein gedanklichen Akt läßt sich etwa eine beliebige Anzahl von Mengen reeller Zahlen $\mathbf{R}_1$, $\mathbf{R}_2$, ... betrach-

ten, wir können also sinnvoll nicht die Frage stellen, wie viele Exemplare von Mengen reeller Zahlen es gibt. Haben wir andererseits eine Menge, beispielsweise $\mathbf{R}$, vor uns, so ist jedes Element dieser Menge, etwa $0 \in \mathbf{R}$, ein Individuum, das einmal und nur einmal in $\mathbf{R}$ vorkommt. Wenn wir hervorheben wollen, daß eine Gesamtheit eine Klasse, aber keine Menge ist, so verwenden wir für sie häufig Symbole in Schreibschrift, beispielsweise $\mathfrak{M}$ für die Klasse aller Mengen. Für Klassen bedeutet die Formel $M \in \mathfrak{A}$, daß M die $\mathfrak{A}$ charakterisierende Eigenschaft besitzt, $M \notin \mathfrak{A}$, daß dies nicht der Fall ist. Viele der für Mengen erklärten Begriffe und Operationen sind auch für Klassen sinnvoll. Zum Beispiel bedeutet $\mathfrak{A} \subseteq \mathfrak{B}$, daß aus der $\mathfrak{A}$ definierenden Eigenschaft die $\mathfrak{B}$ definierende folgt; die Definitionen (10) bis (13) und die daraus folgenden Regeln (14) bis (21) sind auch auf Klassen anwendbar. Wir bemerken, daß die Verwendung von Begriffen wie der „Menge aller Mengen" auf Widersprüche führen würde, die man in einer axiomatisch begründeten Mengenlehre (vgl. etwa D. Klaua [2]) vermeiden kann.

Haben wir eine Klasse $\mathfrak{K}$ und eine Klasse $\mathfrak{L}$ mathematischer Objekte, so sprechen wir von einer *Zuordnung* $\Phi: \mathfrak{K} \to \mathfrak{L}$ von $\mathfrak{K}$ in $\mathfrak{L}$, wenn jedem Objekt $K \in \mathfrak{K}$ ein eindeutig bestimmtes Objekt $L = \Phi(K) \in \mathfrak{L}$ zugeordnet ist. Wollen wir die Tatsache, daß L zu K gehört, besonders hervorheben, so schreiben wir ausführlicher

$$\Phi: K \in \mathfrak{K} \mapsto L = \Phi(K) \in \mathfrak{L} .$$

Beispiel 3. Es bezeichne $\mathfrak{M}$ die Klasse aller Mengen. Dann ist $\mathfrak{P}: E \in \mathfrak{M} \mapsto \mathfrak{P}(E) \in \mathfrak{M}$ eine Zuordnung von $\mathfrak{M}$ in $\mathfrak{M}$, die jeder Menge ihre Potenzmenge zuordnet.

Beispiel 4. Es seien A, B Mengen. Eine Zuordnung $f: a \in A \mapsto b = f(a) \in B$, kurz $f: A \to B$, heißt eine *Abbildung von A in B*, A heißt der *Definitionsbereich* und B der *Wertebereich* der Abbildung. Statt Abbildung sagt man häufig auch *Funktion*. Die Menge aller Abbildungen von A in B bezeichnen wir mit $M(A, B)$; gilt $A = B$, so schreiben wir kürzer $M(A) := M(A, A)$.

Ist $A \subseteq \mathbf{R}$, $B \subseteq \mathbf{R}$, so heißt f eine reelle Funktion einer reellen Variablen; Beispiele hierfür sind alle elementaren Funktionen, etwa

$$x \in \mathbf{R} \mapsto x^n \in \mathbf{R} \qquad (n \in \mathbf{N}) ,$$

$$x \in \mathbf{R} \mapsto e^x \in \mathbf{R} ,$$

$$x \in \mathbf{R} \mapsto \sin x \in \mathbf{R} \quad \text{usw.}$$

Gilt $y = f(x)$, so heißt y das *Bild von x bei f* und x ein *Urbild von y bei f*.

Beispiel 5. Es sei $f: A \to B$ eine Abbildung von A in B. Wir definieren

$$M \in \mathfrak{P}(A) \mapsto f(M) := \{f(x)\}_{x \in M} \in \mathfrak{P}(B) , \tag{24}$$

$$C \in \mathfrak{P}(B) \mapsto f^{-1}(C) := \{x \mid x \in A \text{ und } f(x) \in C\} \in \mathfrak{P}(A) . \tag{25}$$

Mit jeder Abbildung $f: A \to B$ sind also zwei neue Abbildungen $f: \mathfrak{P}(A) \to \mathfrak{P}(B)$ und $f^{-1}: \mathfrak{P}(B) \to \mathfrak{P}(A)$ gegeben. Daß die Abbildung (24) mit demselben Buchstaben bezeichnet wird, führt nicht zu Verwechslungen und ist recht sinnvoll; wendet man nämlich (24) auf die Einermengen $M = \{x\} \in \mathfrak{P}(A)$ an, so ist $\{y\} = f(\{x\})$ gleich-

bedeutend mit $y=f(x)$, so daß man (24) als eine Ausdehnung der ursprünglichen Abbildung $f\colon A\to B$ ansehen kann. $f(M)$ heißt das *Bild von* M bei der Abbildung f. Speziell nennt man

$$\operatorname{Im} f := f(A) \tag{26}$$

das *Bild von* f. Man beweist leicht

$$f\Big(\bigcap_{M\in\mathfrak{S}} M\Big) \subseteq \bigcap_{M\in\mathfrak{S}} f(M)\,, \tag{27}$$

$$f\Big(\bigcup_{M\in\mathfrak{S}} M\Big) = \bigcup_{M\in\mathfrak{S}} f(M) \qquad (\mathfrak{S}\subseteq\mathfrak{P}(A))\,. \tag{28}$$

Für $C\in\mathfrak{P}(B)$ heißt $f^{-1}(C)$ das *Urbild der Menge* C. Man beachte, daß $C\cap\operatorname{Im} f=\emptyset$ mit $f^{-1}(C)=\emptyset$ gleichbedeutend ist. Ist $C=\{y\}$ einelementig, $y\in B$, so läßt man meist die geschweiften Klammern fort und nennt $f^{-1}(y):=f^{-1}(\{y\})$ das *Urbild des Elementes* y. Man beachte, daß $f^{-1}(y)$ eine Teilmenge von A ist, die auch mehrere Elemente enthalten kann. Ist beispielsweise $f\colon x\in\mathbf{R}\mapsto x^2\in\mathbf{R}$, so gilt $f^{-1}(y)=\{+\sqrt{y},-\sqrt{y}\}$, falls $y>0$ ist, $f^{-1}(0)=\{0\}$ und $f^{-1}(y)=\emptyset$ für $y<0$. Man beweist leicht

$$f^{-1}\Big(\bigcap_{C\in\mathfrak{S}} C\Big) = \bigcap_{C\in\mathfrak{S}} f^{-1}(C)\,, \tag{29}$$

$$f^{-1}\Big(\bigcup_{C\in\mathfrak{S}} C\Big) = \bigcup_{C\in\mathfrak{S}} f^{-1}(C) \qquad (\mathfrak{S}\subseteq\mathfrak{P}(B))\,. \tag{30}$$

Übung 3. Man finde ein Beispiel, für das in (27) $f\big(\bigcap_{M\in\mathfrak{S}} M\big)\neq\bigcap_{M\in\mathfrak{S}} f(M)$ ist.

Definition 4. Eine Abbildung $f\colon A\to B$ heißt *surjektiv* (oder Abbildung *auf* B), wenn $\operatorname{Im} f=B$ gilt. f heißt *injektiv* (oder *eineindeutig*), wenn jedes $y\in B$ höchstens ein Urbild $x\in f^{-1}(y)$ aus A hat, wenn also aus $f(x)=f(\hat{x})$ die Gleichheit $x=\hat{x}$ folgt. Eine Abbildung $f\colon A\to B$ heißt *bijektiv* (oder *umkehrbar*), wenn sie injektiv und surjektiv ist. In diesem Fall hat jedes Element $y\in B$ ein und nur ein Urbild $\{x\}=f^{-1}(y)\subseteq A$, und man definiert die *inverse Abbildung* $f^{-1}\colon B\to A$ durch

$$y\in B\mapsto f^{-1}(y):=x, \qquad \text{wenn} \qquad f(x)=y \qquad \text{ist.} \tag{31}$$

Beispiel 6. Es sei $b_0\in B$ fest. Die durch $f(x):=b_0$ für alle $x\in A$ definierte Abbildung heißt eine *konstante* Abbildung. Sie ist surjektiv genau dann, wenn $B=\{b_0\}$ einelementig ist, injektiv, wenn A einelementig ist, und bijektiv, wenn beide Mengen A, B einelementig sind.

Beispiel 7. Es sei $A\subseteq B$ eine Teilmenge. Die durch $\iota\colon x\in A\mapsto\iota(x):=x\in B$ definierte Abbildung heißt die *Einbettung* von A in B. Eine Einbettung ist stets injektiv, sie ist bijektiv genau dann, wenn $A=B$ ist. Man nennt

$$\mathrm{id}_A\colon x\in A\mapsto \mathrm{id}_A(x):=x\in A \tag{32}$$

die *identische Abbildung von* A; sie ist bijektiv. Die bijektiven Abbildungen $f\colon A\to A$ nennt man auch *Transformationen von* A.

Beispiel 8. Es sei $f\colon A\to B$ eine Abbildung und $M\subseteq A$ eine Teilmenge. Unter der *Einschränkung* $f\mid M$ von f auf M versteht man die Abbildung $f\mid M\colon M\to B$,

die auf M mit f übereinstimmt. Sie ist definiert durch

$$x \in M \mapsto f \mid M(x) := f(x) \in B\,. \tag{33}$$

Ist f injektiv, so ist auch die Einschränkung $f \mid M$ injektiv.

Man beachte, daß zur Definition einer Abbildung (Beispiel 4) stets die Angabe des ins Auge gefaßten Wertebereiches B gehört; sonst wäre die Definition des Begriffes surjektiv nicht sinnvoll. Ist $f\colon A \to B$ gegeben und definiert man $\hat{B} := \operatorname{Im} f$ und $\hat{f}\colon A \to \hat{B}$ durch $\hat{f}(x) := f(x)$ für $x \in A$, so ist $\hat{f}\colon A \to \hat{B}$ surjektiv. Da diese Einschränkung des Wertebereiches jedoch selten notwendig ist, wollen wir für $\hat{f}$ kein besonderes Symbol einführen.

Beispiel 9. Es sei $I \neq \emptyset$ eine nichtleere Menge, die wir *Indexmenge* nennen, $\alpha \in I$ variiere in I. Ist jedem $\alpha \in I$ ein mathematisches Objekt m_α zugeordnet, so schreiben wir $(m_\alpha)_{\alpha \in I}$ und sprechen von der *Familie* $(m_\alpha)_{\alpha \in I}$. Die m_α können dabei einer Menge oder einer Klasse angehören oder auch in verschiedenen Mengen oder Klassen liegen. Formal können wir jede nichtleere Menge A als Familie auffassen, indem wir $(x)_{x \in A}$ schreiben, d. h. $A = I$ als Indexmenge wählen. In einer beliebigen Familie $(m_\alpha)_{\alpha \in I}$ brauchen die Elemente m_α jedoch nicht paarweise verschieden zu sein, es kann $m_\alpha = m_\beta$ für $\alpha \neq \beta$ gelten.

Beispiel 10. In Beispiel 9 sei $I = \{1, 2\}$ zweielementig. Man nennt dann die Familien mit I als Indexmenge (*geordnete*) *Paare* und schreibt für sie (a, b), wenn $1 \mapsto m_1 = a$, $2 \mapsto m_2 = b$ gilt. Es sei nun (M_1, M_2) ein Mengenpaar. Unter dem *Produkt* $M_1 \times M_2$ versteht man die Menge aller Paare (m_1, m_2) mit $m_\alpha \in M_\alpha$, $\alpha = 1, 2$:

$$M_1 \times M_2 := \{(m_1, m_2) \mid m_1 \in M_1,\, m_2 \in M_2\}\,. \tag{34}$$

Die Abbildung

$$p_\alpha\colon (m_1, m_2) \in M_1 \times M_2 \mapsto p_\alpha(m_1, m_2) := m_\alpha \in M_\alpha\,, \qquad \alpha = 1, 2\,, \tag{35}$$

heißt die α-te *Projektion* des Produkts. Die Projektionen sind surjektiv. Die Urbilder, z. B.

$$p_1^{-1}(m_1) = \{m_1\} \times M_2 \subseteq M_1 \times M_2\,, \tag{36}$$

analog für $\alpha = 2$, heißen *Schnitte* des Produkts.

Diese Begriffe lassen sich leicht verallgemeinern: Ist $(M_\alpha)_{\alpha \in I}$ eine beliebige Mengenfamilie, so versteht man unter ihrem *Produkt*

$$\bigtimes_{\alpha \in I} M_\alpha := \{(m_\alpha)_{\alpha \in I} \mid m_\alpha \in M_\alpha\} \tag{37}$$

die Menge aller Familien $(m_\alpha)_{\alpha \in I}$ mit $m_\alpha \in M_\alpha$. Die Projektionen $p_\beta\colon \bigtimes_{\alpha \in I} M_\alpha \to M_\beta$ $(\beta \in I)$ und die Schnitte sind analog zum Fall $I = \{1, 2\}$ definiert.

Beispiel 11. Sind in der Familie $(M_\alpha)_{\alpha \in I}$ alle Mengen $M_\alpha = M$, so ist $\bigtimes_{\alpha \in I} M_\alpha$ gleich der *Menge M^I aller Abbildungen von I in M*:

$$M^I := M(I, M) = \{f \mid f\colon I \to M \text{ Abbildung}\}\,. \tag{38}$$

Jeder Familie $(m_\alpha)_{\alpha\in I}$ entspricht umkehrbar eindeutig eine Abbildung $f\colon \alpha\in I\mapsto f(\alpha) := m_\alpha\in M$. Besonders wichtig für uns sind folgende drei Fälle:

1. Es sei $I=\{1, ..., n\}$, M beliebig. Dann schreibt man $M^n := M^I$; die Elemente von M^n sind die *n-Tupel* $(m_1, ..., m_n)$ mit $m_\alpha\in M$. Wenn keine Mißverständnisse zu befürchten sind, schreiben wir kürzer (m_α) für $(m_1, ..., m_n)$.

2. Es sei $I=\mathbf{N}_0$ (oder $I=\mathbf{N}$). Dann ist $M^{\mathbf{N}_0}$ die Menge der *Folgen* $(m_\alpha)_{\alpha\in\mathbf{N}_0} = (m_0, m_1, ..., m_k, ...)$ mit Werten in M.

3. Es sei $I=N_n\times N_m$, vgl. (3), und M eine beliebige nichtleere Menge. Die Elemente aus M^I sind Abbildungen $(i, j)\in I\mapsto a_{ij}\in M$, die man in Form einer Tabelle in runden Klammern aufschreibt:

$$(a_{ij})=\begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \cdot & \cdots & \cdot \\ a_{n1} & \cdots & a_{nm} \end{pmatrix}; \tag{39}$$

(a_{ij}) ist einfach eine Kurzbezeichnung der rechten Seite von (39). Die Elemente $(a_{ij})\in M^I$ heißen *Matrizen* mit *n Zeilen* und *m Spalten* aus Elementen von M.

Beispiel 12. Wir betrachten eine Abbildung $f\colon A\to B$ und ordnen ihr ihren *Graph* $G_f\subseteq A\times B$ durch die Definition $G_f := \{(x, f(x))\}_{x\in A}$ zu. G_f ist eine naheliegende Verallgemeinerung der graphischen Darstellung der elementaren Funktionen. Ist $p_1\colon A\times B\to A$ die erste Projektion des Produktes $A\times B$, so gilt: $p_1 \mid G_f\colon G_f\to A$ ist bijektiv; offenbar ist umgekehrt f durch G_f eindeutig bestimmt, vgl. (40). Man sagt, eine Menge $G\subseteq A\times B$ liegt *schlicht über* A, wenn $p_1 \mid G$ bijektiv ist. Zu jeder derartigen Menge G gibt es genau eine Abbildung f mit $G=G_f$, nämlich

$$x\in A\mapsto p_2((p_1 \mid G)^{-1}(x))\in B\,. \tag{40}$$

f ist injektiv genau dann, wenn G_f schlicht über Im f liegt, d. h. $p_2 \mid G_f\colon G_f\to \mathrm{Im}\, f$ bijektiv ist; f ist bijektiv genau dann, wenn G_f schlicht über A und über B ist. Aus dem Gesagten erkennt man, daß die Abbildungen $f\colon A\to B$ mit den über A schlichten Teilmengen $G\subseteq A\times B$ identifiziert werden können; häufig benutzt man diese Tatsache zur Definition der Abbildungen, die so als ein aus dem Mengenbegriff abgeleiteter Begriff und nicht als ein Grundbegriff erscheinen.

Beispiel 13. Es sei $(M_\alpha)_{\alpha\in I}$ eine Mengenfamilie, $M_\alpha\in\mathfrak{P}(E)$. Dann sind Durchschnitt und Vereinigung der Familie analog (22) und (23) definiert:

$$\bigcap_{\alpha\in I} M_\alpha := \{x \mid x\in M_\alpha \text{ für alle } \alpha\in I\}\,, \tag{41}$$

$$\bigcup_{\alpha\in I} M_\alpha := \{x \mid \text{es gibt ein } \alpha\in I \text{ mit } x\in M_\alpha\}\,. \tag{42}$$

Beispiel 14. Eine Menge M heißt *endlich*, wenn es ein $n\in\mathbf{N}$ und eine bijektive Abbildung $f\colon M\to N_n$ gibt; n heißt die *Anzahl* der Elemente von M oder auch die *Mächtigkeit von* M; wir schreiben $|M|=n$. Eine Menge M heißt *abzählbar*, wenn es eine bijektive Abbildung $f\colon M\to\mathbf{N}$ gibt. Man kann beweisen, daß die Menge $\mathbf{R}$ der reellen Zahlen nicht abzählbar ist. Für die allgemeine Theorie der Mächtigkeiten beliebiger (unendlicher) Mengen verweisen wir auf D. Klaua [3], Teil II.

Wir wollen nun den wichtigen Begriff der Verknüpfung zweier Abbildungen einführen.

Definition 5. Es seien $f: A \to B$ und $g: B \to C$ zwei Abbildungen. Unter ihrer *Verknüpfung* $g \circ f: A \to C$ versteht man die Abbildung

$$a \in A \mapsto g \circ f(a) := g(f(a)) \in C .$$

Analog wird die Verknüpfung allgemeiner Zuordnungen erklärt. Man beachte, daß die Verknüpfung $g \circ f$ nur für solche Zuordnungen g, f definiert ist, für die der Definitionsbereich B von g gleich dem Wertebereich von f ist. Es würde auch genügen, daß Im f im Definitionsbereich von g enthalten ist. Die Verknüpfung $\circ$ hat folgende Eigenschaften:

1. *Ist* $f: A \to B$ *eine Abbildung, so gilt*

$$f \circ \mathrm{id}_A = \mathrm{id}_B \circ f = f .$$

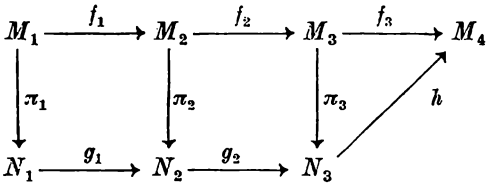
2. *Die Assoziativität: Für* $f: A \to B$, $g: B \to C$ *und* $h: C \to D$ *gilt*

$$(h \circ g) \circ f = h \circ (g \circ f) .$$

Wegen der zweiten Eigenschaft kann man die Klammern bei der Hintereinanderausführung von Verknüpfungen auch fortlassen. Die erste Eigenschaft bedeutet, daß die identischen Abbildungen „Einselemente" der Verknüpfung sind.

Übung 4. Es sei $f: A \to B$ eine Abbildung. Man beweise: f ist bijektiv genau dann, wenn Abbildungen $h_1, h_2: B \to A$ existieren, so daß $h_1 \circ f = \mathrm{id}_A$ und $f \circ h_2 = \mathrm{id}_B$ gilt. In diesem Fall ist $h_1 = h_2 = f^{-1}$ die zu f inverse Abbildung.

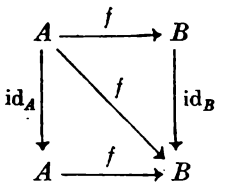
Häufig hat man gleichzeitig mehrere Abbildungen zu betrachten, die in verschiedener Weise miteinander verknüpft sind. Um die Beziehungen übersichtlich darzustellen, schreibt man die Abbildungen in Form eines Diagramms auf, z. B.



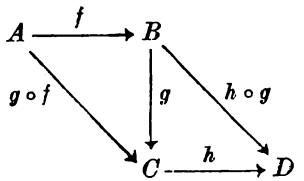
Die Pfeile bedeuten Abbildungen, an ihrem Anfang steht der Definitionsbereich der Abbildung und am Ende der Wertebereich der Abbildung. Aufeinanderfolgende Pfeile gehören zu Abbildungen, die miteinander verknüpft werden können. Eine endliche Folge $(f_1, f_2, \ldots, f_n)$ von Abbildungen heißt eine *Kette*, wenn ihre Verknüpfung $f_n \circ f_{n-1} \circ \ldots \circ f_1$ definiert ist; z. B. ist (f_1, f_2, f_3) bei dem obigen Diagramm eine Kette, während (f_1, π_2, g_1) keine Kette ist. Ein *Diagramm* heißt *kommutativ*, wenn für zwei in ihm vorkommende Mengen M, N die Verknüpfung jeder M mit N verbindenden Abbildungskette dieselbe Abbildung ergibt. Für das obige Diagramm ist die Kommutativität gleichbedeutend mit den Beziehungen

$$\pi_{i+1} \circ f_i = g_i \circ \pi_i , \qquad i = 1, 2 ; \qquad f_3 = h \circ \pi_3 ;$$

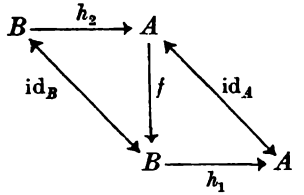
die übrigen möglichen Identitäten ergeben sich aus diesen. Zum Beispiel kann man die Eigenschaft 1 der Verknüpfung $\circ$ durch die Kommutativität des Diagramms



beschreiben; das assoziative Gesetz 2 der Verknüpfung wird durch das kommutative Diagramm



ausgedrückt. Nach Übung 4 folgt aus der Kommutativität des Diagramms



daß f bijektiv und $h_1 = h_2 = f^{-1}$ ist.

Zum Abschluß dieses Paragraphen wollen wir noch den Begriff der Relation einführen und uns besonders mit den Äquivalenzrelationen beschäftigen, die ein wichtiges Hilfsmittel für die Bildung neuer mathematischer Begriffe sind.

Definition 6. Es sei $A \neq \emptyset$ eine nichtleere Menge. Unter einer *Relation* über A verstehen wir eine Teilmenge $\Omega \subseteq A \times A$. Für zwei Elemente $a, b \in A$ sagt man, sie stehen in der Relation Ω, und schreibt $a \Omega b$, falls $(a, b) \in \Omega$ gilt; falls $(a, b) \notin \Omega$ ist, schreibt man $a \not\Omega b$.

Beispiel 15. Eine Relation $\Omega \subseteq A \times A$ heißt eine *Ordnung*, wenn sie folgende Eigenschaften besitzt: 1. Für alle $a \in A$ gilt $a \Omega a$; 2. gilt $a \Omega b$ und $b \Omega a$, so ist $a = b$; 3. aus $a \Omega b$ und $b \Omega c$ folgt $a \Omega c$. Zum Beispiel ist für jede Menge E die Enthaltenseinsrelation $\subseteq$ eine Ordnung über $\mathfrak{P}(E)$; für die Zahlenbereiche $\mathbf{N}, \mathbf{N}_0, \mathbf{Z}, \mathbf{Q}, \mathbf{R}$ ist $\leq$ eine Ordnung. Es sei $[A, \prec]$ eine Menge, $A \neq \emptyset$ und $\prec$ eine Ordnung über A. Ein $b \in A$ heißt eine *obere* (*untere*) *Schranke* der Teilmenge $M \subseteq A$, wenn $m \prec b$ (bzw. $b \prec m$) für alle $m \in M$ gilt. Eine obere Schranke b_0 (bzw. untere Schranke c_0) von M heißt das *Supremum* sup M (bzw. das *Infimum* inf M) von M, wenn $b_0 \prec b$ (bzw. $b \prec c_0$) für jede obere (bzw. untere) Schranke b von M gilt. Supremum und In-

fimum sind offenbar auf Grund ihrer Definition eindeutig bestimmt, brauchen jedoch im allgemeinen nicht zu existieren, wie man am Beispiel der üblichen Ordnung $\leqq$ über der Menge $\mathbf{Q}$ der rationalen Zahlen erkennt. Existiert zu beliebigen $a, b \in A$ stets $a \vee b := \sup\{a, b\}$ und $a \wedge b := \inf\{a, b\}$, so heißt das Paar $[A, \prec]$ ein *Verband*; existieren sup M und inf M für beliebige nichtleere $M \subseteqq A$, $M \neq \emptyset$, so heißt $[A, \prec]$ ein *vollständiger Verband*. Wie bereits nach Definition 3 bemerkt, ist $[\mathfrak{P}(E), \subseteqq]$ ein vollständiger Verband; das Supremum ist hier die Vereinigung und das Infimum der Durchschnitt eines Mengensystems. Die reellen Zahlen $[\mathbf{R}, \leqq]$ mit der üblichen Ordnungsrelation bilden keinen vollständigen Verband, weil z. B. inf $\mathbf{R}$ und sup $\mathbf{R}$ in $\mathbf{R}$ nicht existieren. Bildet man jedoch mit den neuen Symbolen $-\infty, +\infty$ die Menge $\mathbf{R}' := \mathbf{R} \cup \{-\infty, +\infty\}$ und setzt $-\infty \leqq a$, $a \leqq +\infty$ für alle $a \in \mathbf{R}$ und $-\infty \leqq +\infty$, so wird $[\mathbf{R}', \leqq]$ ein vollständiger Verband.

Man beachte, daß es bei einer Ordnung $\prec$ im allgemeinen auch *unvergleichbare Elemente* geben kann, d. h. $a, b \in A$, für die weder $a \prec b$ noch $b \prec a$ gilt. Erfüllt eine Ordnungsrelation $\prec$ neben den Eigenschaften 1 bis 3 noch die Eigenschaft 4: Für beliebige Elemente $a, b \in A$ gilt wenigstens eine der Beziehungen $a \prec b$ oder $b \prec a$, so heißt $\prec$ eine *lineare Ordnung*. Jede linear geordnete Menge $[A, \prec]$ ist ein Verband. Die Relation $\leqq$ über $\mathbf{N}, \mathbf{N}_0, \mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{R}'$ ist eine lineare Ordnung. Ausführlicher ist die Theorie der Verbände z. B. in A. G. Kuroš [2], Abschnitt 4, dargestellt.

Wir bemerken, daß man die mengentheoretischen Operationen wie Vereinigung, Differenz, Durchschnitt, Produkt sowie den Begriff der Relation sinngemäß auch auf Klassen anwenden kann, wobei als Ergebnis wiederum Klassen entstehen. Das trifft insbesondere auf den folgenden grundlegenden Begriff zu:

Definition 7. Eine Relation $\equiv$ über A heißt eine *Äquivalenzrelation*, wenn sie folgende Eigenschaften besitzt:

1. Für alle $a \in A$ gilt $a \equiv a$ (*Reflexivität*).
2. Aus $a \equiv b$ folgt $b \equiv a$ $(a, b \in A)$ (*Symmetrie*).
3. Aus $a \equiv b$ und $b \equiv c$ folgt $a \equiv c$ $(a, b, c \in A)$ (*Transitivität*).

Es sei nun $\equiv$ eine Äquivalenzrelation über A. Für jedes $a \in A$ definieren wir die zu a gehörende *Äquivalenzklasse* $\hat{a}$ durch

$$\hat{a} := \{x \mid x \in A \text{ und } x \equiv a\}. \tag{43}$$

Dann gilt

Satz 1. *Das System* $\mathfrak{S} := \{\hat{a} \mid a \in A\}$ *der Äquivalenzklassen einer Äquivalenzrelation* $\equiv$ *über* A *ist eine Klasseneinteilung von* A, *d. h., es gilt:*

1. $\bigcup_{M \in \mathfrak{S}} M = A$.
2. *Aus* $M_1, M_2 \in \mathfrak{S}$ *und* $M_1 \cap M_2 \neq \emptyset$ *folgt* $M_1 = M_2$.
3. *Für alle* $M \in \mathfrak{S}$ *gilt* $M \neq \emptyset$.

Ist umgekehrt eine Klasseneinteilung $\mathfrak{S}$ *mit den Eigenschaften* 1, 2 *und* 3 *über* A *gegeben, so wird durch*

$$\equiv_{\mathfrak{S}} := \{(a,b) \mid (a,b) \in A \times A, \text{ und es gibt ein } M \in \mathfrak{S} \text{ mit } a \in M \text{ und } b \in M\} \tag{44}$$

eine Äquivalenzrelation über A *definiert, deren Klasseneinteilung gerade das vorgegebene System* $\mathfrak{S}$ *ist.*

Beweis. Aus (43) und Eigenschaft 1 aus Definition 7 folgt $a \in \hat{a}$, also $\hat{a} \neq \emptyset$ und $A = \bigcup_{\hat{a} \in \mathfrak{S}} \hat{a}$. Wir zeigen die Eigenschaft 2 der Klasseneinteilung. Es sei $M_1 = \hat{a}$ und $M_2 = \hat{b}$. Wegen $M_1 \cap M_2 \neq \emptyset$ gibt es ein $c \in \hat{a} \cap \hat{b}$. Nach (43) gilt $c \equiv a$ und $c \equiv b$. Aus der Symmetrie-Eigenschaft 2, Definition 7, erhalten wir $a \equiv c$ und $c \equiv b$, und aus der Transitivität 3 folgt $a \equiv b$ und analog $b \equiv a$. Somit gilt $b \in \hat{a}$; ist nun $x \in \hat{b}$ beliebig, so gilt $x \equiv b$ und $b \equiv a$, also nach der Transitivität $x \equiv a$ und nach (43) $x \in \hat{a}$, also $\hat{b} \subseteq \hat{a}$. Genauso zeigt man $\hat{a} \subseteq \hat{b}$, woraus $\hat{a} = \hat{b}$ folgt.

Wir beweisen nun die Umkehrung. Es sei $\equiv_{\mathfrak{S}}$ durch (44) definiert. Da $\bigcup_{M \in \mathfrak{S}} M = A$ gilt, gibt es zu jedem $a \in A$ ein $M \in \mathfrak{S}$ mit $a \in M$, und es gilt die Reflexivität $a \equiv_{\mathfrak{S}} a$. Die Symmetrie 2 aus Definition 7 folgt unmittelbar aus (44). Für den Beweis der Transitivität 3 sei $a \equiv_{\mathfrak{S}} b$ und $b \equiv_{\mathfrak{S}} c$. Dann gibt es $M_1, M_2 \in \mathfrak{S}$ mit $a, b \in M_1$ und $b, c \in M_2$. Folglich gilt $b \in M_1 \cap M_2 \neq \emptyset$, und aus der Bedingung 2 für $\mathfrak{S}$ folgt $M_1 = M_2$. Somit sind $a, c \in M_1 = M_2 \in \mathfrak{S}$, also $a \equiv_{\mathfrak{S}} c$. Die letzte Behauptung ergibt sich so: Wegen Eigenschaft 3 ist für $M \in \mathfrak{S}$ die Menge M nicht leer, und nach (44) folgt für $a \in M$ sofort $\hat{a} = M$. □

Definition 8. Die Menge $\mathfrak{S} \subseteq \mathfrak{P}(A)$ der Äquivalenzklassen von A nach einer Äquivalenzrelation $\equiv$ heißt die *Faktormenge* $A/\equiv$ von A nach $\equiv$. Die Abbildung

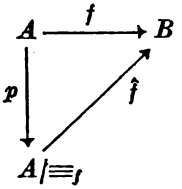
$$p: a \in A \mapsto \hat{a} \in A/\equiv \tag{45}$$

nennt man die zu $\equiv$ gehörende *kanonische Abbildung.*

Beispiel 16. Es sei $f: A \to B$ eine Abbildung. Dann wird durch

$$\equiv_f := \{(a, b) \mid (a, b) \in A \times A \text{ und } f(a) = f(b)\} \tag{46}$$

eine Äquivalenzrelation über A definiert. Es gibt genau eine Abbildung $\hat{f}: A/\equiv_f \to B$, für die das Diagramm



kommutativ wird; sie ist durch $\hat{f}(\hat{a}) := f(a)$ definiert. Ist f surjektiv, so ist $\hat{f}$ bijektiv, und man kann $A/\equiv_f$ und B durch die Festsetzung $\hat{f}(\hat{a}) = \hat{a}$ identifizieren. Dann gilt $p = f$. Die Äquivalenzklassen von $\equiv_f$ sind die sogenannten *Niveaumengen*

$f^{-1}(x) \neq \emptyset$, $x \in B$, von f, d. h. die nichtleeren Urbilder von Einermengen. Es gilt $\hat{a} = f^{-1}(f(a))$; die Äquivalenzrelation $\equiv_f$ stimmt genau dann mit der Gleichheit $=$ überein, wenn f injektiv ist.

Beispiel 17. Es sei $A = \mathbf{R}$. Wir definieren für $a, b \in \mathbf{R}$: $a \equiv b \bmod 2\pi$ („*a ist kongruent b modulo* 2π"), wenn $a - b = k \cdot 2\pi$ für ein $k \in \mathbf{Z}$ gilt. Man beweist leicht, daß hierdurch eine Äquivalenzrelation gegeben ist. Die Äquivalenzklassen dieser Relation können wir als Niveaumengen der Abbildung

$$f: t \in \mathbf{R} \mapsto (\cos t, \sin t) \in S^1$$

erhalten; hierbei bezeichnet $S^1 \subseteq \mathbf{R}^2$ den Einheitskreis $x^2 + y^2 = 1$ der Ebene $\mathbf{R}^2 = \mathbf{R} \times \mathbf{R}$. Die Urbilder sind $f^{-1}((\cos t, \sin t)) = \{t + k2\pi\}_{k \in \mathbf{Z}}$. In diesem Sinne sagt man, daß der orientierte Winkel t zwischen dem Radius $(1, 0)$ und dem Radius $(\cos t, \sin t)$ des Einheitskreises bis auf ein ganzzahliges Vielfaches von 2π eindeutig bestimmt sei.

1. Gruppen

Schon beim elementaren Rechnen haben wir es mit algebraischen Operationen zu tun, nämlich mit den Operationen der Addition, der Subtraktion, der Multiplikation und der Division von Zahlen. Ein anderes wichtiges Beispiel einer algebraischen Operation ist die Verknüpfung von Abbildungen, vgl. Definition 0.2.5. In diesem Kapitel werden wir den für die Algebra fundamentalen Begriff einer Menge mit einer Operation betrachten. Vom Standpunkt der Anwendungen aus sind gewisse algebraische Operationen mit bestimmten speziellen Eigenschaften, die wir in § 1 angeben werden, besonders interessant; sie führen uns auf den Begriff der Gruppe, einen der Grundbegriffe der Algebra und überhaupt der gesamten Mathematik. Die Gruppentheorie hängt besonders eng mit der Geometrie zusammen, in der die Gruppen als Transformationsgruppen auftreten. Historisch gesehen begann die Gruppentheorie mit dem Studium spezieller Transformationsgruppen, nämlich der Permutationsgruppen.

In § 5 schließlich behandeln wir kurz Grundbegriffe der Kategorien und Funktoren. Dabei gehen wir jedoch auf die eigentliche Theorie der Kategorien nicht ein; wir begnügen uns damit, anhand von wichtigen Beispielen, etwa der Kategorie der Mengen oder der Kategorie der Gruppen, die Ansätze dieser Theorie zu motivieren. Diese wenigen Begriffe genügen schon, eine für die Beschreibung begrifflicher, struktureller Zusammenhänge geeignete und in der neueren Literatur viel benutzte Terminologie verständlich zu machen.

§ 1. Monoide, Halbgruppen, Gruppen

In diesem Paragraphen führen wir den Begriff einer algebraischen Operation in einer beliebigen Menge ein und betrachten gewisse Klassen von Mengen mit einer algebraischen Operation.

Definition 1. Es sei M eine nichtleere Menge. Unter einer *algebraischen Operation auf* M verstehen wir eine Vorschrift, die jedem geordneten Paar (a, b) aus Elementen der Menge M ein eindeutig bestimmtes Element $a * b$ derselben Menge M

zuordnet. Anders gesagt ist eine algebraische Operation auf M einfach eine Abbildung von $M \times M$ in M. Die Menge M zusammen mit einer auf ihr gegebenen algebraischen Operation $*$ nennen wir ein *Monoid*; wir bezeichnen es mit $[M, *]$ (oder einfach mit M, wenn klar ist, welche algebraische Operation gerade betrachtet wird).

Mit $\mathbf{R}$ bezeichnen wir die Menge der reellen Zahlen mit den üblichen Rechenoperationen.

Beispiel 1. $M = \mathbf{R}$, $a * b := a + b$.

Beispiel 2. $M = \mathbf{R}$, $a * b := ab$.

Beispiel 3. $M = \mathbf{R}$, $a * b := a - b$.

Beispiel 4. $M = \mathbf{R}$, $a * b := \max(a, b)$.

Man bemerkt, daß man in den Beispielen 1 bis 4 die Menge $\mathbf{R}$ der reellen Zahlen auch durch die Menge $\mathbf{Q}$ der rationalen Zahlen oder die Menge $\mathbf{Z}$ der ganzen Zahlen ersetzen könnte.

Beispiel 5. Mit der Definition $a * b := a/b$ ist $[\mathbf{R}, *]$ kein Monoid, da die Operation der Division nicht für alle Paare erklärt ist. Ist aber $\mathbf{R}^* := \{a \mid a \in \mathbf{R}, a \neq 0\}$ die Menge der von 0 verschiedenen reellen Zahlen, so ist $[\mathbf{R}^*, *]$ ein Monoid.

Beispiel 6. Es sei $M = V$ die Menge aller Vektoren der Ebene, die von einem festen Punkt o ausgehen. Setzt man $\mathfrak{a} * \mathfrak{b} := \mathfrak{a} + \mathfrak{b}$, wobei die Vektoren nach der bekannten Parallelogrammregel addiert werden, so ist $[V, *]$ ein Monoid.

Beispiel 7. Es sei X eine nichtleere Menge und $M(X) := M(X, X)$ die Menge aller Abbildungen von X in X. Durch die Verknüpfung $\circ$ der Abbildungen wird dann $[M(X), \circ]$ ein Monoid.

Beispiel 8. *Punktweise Operationen für Funktionen.* Es sei X eine nichtleere Menge und $[H, *]$ irgendein Monoid. Die Menge $M(X, H)$ aller Abbildungen $X \to H$ nennt man manchmal auch Menge der *H-wertigen Funktionen auf X*. Die Operation $*$ auf H gestattet es nun, eine gleichbezeichnete Operation in der Menge der *H-wertigen* Funktionen $M(X, H)$ zu definieren, indem man

$$(f * g)(x) := f(x) * g(x) \qquad (f, g \in M(X, H), x \in X)$$

setzt. Man nennt diese Operation *„punktweise"*, weil sie in der Ausführung der ursprünglichen Operation $*$ von H für die Werte der Funktionen in jedem „Punkt" $x \in X$ besteht. Gilt $X \subseteq \mathbf{R}$ und ist H eines der Monoide von Beispiel 1 bis 3, so ergeben sich die üblichen, in der Analysis betrachteten Operationen für reelle Funktionen einer reellen Variablen als Spezialfall.

Der Begriff des Monoids ist sehr allgemein und daher inhaltsarm. Im weiteren werden wir Monoide untersuchen, deren Operation gewissen Bedingungen genügt.

Definition 2. Ein Monoid $[M, *]$ heißt eine *Halbgruppe*, wenn die zugehörige Operation $*$ *assoziativ* ist, d. h., wenn

$$(a * b) * c = a * (b * c) \qquad (a, b, c \in M)$$

gilt. Für Halbgruppen bezeichnet man die algebraische Operation gewöhnlich als Multiplikation und schreibt entsprechend ab oder $a \cdot b$, anstatt $a * b$; diese Schreibweise nennt man *multiplikativ*.

Wir wollen nun eine Eigenschaft der Halbgruppen herleiten, die wir im folgenden häufig anzuwenden haben. Es sei $a_1, a_2, \ldots, a_n$ eine Folge von Elementen der Halbgruppe M. Um das Produkt dieser Elemente in der durch die Numerierung gegebenen Anordnung zu bilden, müssen wir eigentlich Klammern setzen, die angeben, in welcher Reihenfolge wir die Operationen auszuführen wünschen. Hier gilt nun

Satz 1. *In einer beliebigen Halbgruppe M hängt das Produkt einer Folge $a_1, a_2, \ldots, a_n$ von Elementen aus M in der durch die Numerierung gegebenen Anordnung nicht von der Verteilung der Klammern in dem Produkt ab.*

Beweis. Wir führen den Beweis durch vollständige Induktion nach der Anzahl n der Faktoren. Für $n=2$ ist die Behauptung trivial. Wir beweisen sie für n unter der Annahme, daß sie für eine kleinere Anzahl von Faktoren gilt. Ausgehend von irgendeiner Verteilung der Klammern führen wir die hierdurch vorgeschriebenen Multiplikationen schrittweise aus und erhalten als letzten Schritt ein Produkt der Gestalt $(a_1 \ldots a_i)\,(a_{i+1} \ldots a_n)$ mit $1 \leqq i \leqq n-1$. Nach Induktionsvoraussetzung sind nämlich die in den Klammern stehenden Produkte eindeutig bestimmt. Von einer anderen Verteilung der Klammern ausgehend kommen wir analog auf ein Produkt der Gestalt $(a_1 \ldots a_j)\,(a_{j+1} \ldots a_n)$ mit $1 \leqq j \leqq n-1$. Es bleibt also

$$(a_1 \ldots a_i)\,(a_{i+1} \ldots a_n) = (a_1 \ldots a_j)\,(a_{j+1} \ldots a_n)$$

zu beweisen. Im Fall $i=j$ ist das klar. Es sei etwa $i<j$. Nach Induktionsvoraussetzung gilt

$$a_{i+1} \ldots a_n = (a_{i+1} \ldots a_j)\,(a_{j+1} \ldots a_n)$$

und

$$a_1 \ldots a_j = (a_1 \ldots a_i)\,(a_{i+1} \ldots a_j)\,.$$

Aus der Assoziativität der Multiplikation, die übrigens mit unserer Behauptung für $n=3$ übereinstimmt, erhalten wir bei Anwendung auf die Elemente $a = a_1 \ldots a_i$, $b = a_{i+1} \ldots a_j$, $c = a_{j+1} \ldots a_n$ die zu zeigende Gleichheit. □

Definition 3. Ein Element $e \in M$ heißt *neutrales Element* (oder *Einselement*) des Monoids $[M, *]$, wenn für alle $a \in M$

$$e * a = a * e = a$$

gilt. Wenn ein neutrales Element existiert, heißt das Monoid $[M, *]$ ein *Monoid mit neutralem Element* (*mit Einselement*).

Satz 2. *Wenn in einem Monoid ein Einselement existiert, ist es eindeutig bestimmt.*

Beweis. Es seien e, e' Einselemente des Monoids M. Dann gilt $e = e * e' = e'$. □

Definition 4. Es sei $[M, *]$ ein Monoid mit Einselement e und $a \in M$. Ein Element $b \in M$ heißt *invers zu* a, wenn

$$a * b = b * a = e$$

gilt. Wenn ein solches Element $b \in M$ existiert, heißt a *invertierbar*. Die Menge der invertierbaren Elemente des Monoids M bezeichnen wir mit M^*.

Offenbar ist das Element e zu sich selbst invers, also $e \in M^*$. Ist ferner $a \in M^*$ und b invers zu a, so ist auch a invers zu b, also $b \in M^*$.

Satz 3. *Es sei M eine Halbgruppe mit Einselement. Dann gilt:*

1. *Für jedes $a \in M^*$ ist das zu a inverse Element eindeutig bestimmt; man bezeichnet es mit a^{-1}.*

2. *Sind $a_1, \ldots, a_k \in M^*$, so ist auch $a_1 \ldots a_k \in M^*$, und es gilt*

$$(a_1 \ldots a_k)^{-1} = a_k^{-1} \ldots a_1^{-1}.$$

Beweis. 1. Es seien b, b' invers zu a. Dann ist $b(ab') = be = b$. Andererseits gilt $b(ab') = (ba)\, b' = eb' = b'$, also $b = b'$.

2. Offenbar gilt nach Satz 1

$$(a_1 \ldots a_k)\,(a_k^{-1} \ldots a_1^{-1}) = a_1(\ldots (a_{k-1}(a_k a_k^{-1})\, a_{k-1}^{-1}) \ldots)\; a_1^{-1} = e\,.$$

Ebenso erhält man $(a_k^{-1} \ldots a_1^{-1})\,(a_1 \ldots a_k) = e$. □

Wir erwähnen noch folgende Beziehungen, die sich aus dem oben Gesagten ergeben:

$$e^{-1} = e, \qquad (a^{-1})^{-1} = a \qquad (a \in M^*)\,. \tag{1}$$

Definition 5. Ein Monoid $[M, *]$ heißt *kommutativ*, wenn

$$a * b = b * a \qquad (a, b \in M)$$

gilt.

Beispiele. In den oben angegebenen Beispielen 1, 2 und 6 sind die Monoide kommutative Halbgruppen mit Einselement. Beispiel 4 ist eine kommutative Halbgruppe ohne Einselement. Die Monoide der Beispiele 3 und 5 sind weder assoziativ noch kommutativ noch besitzen sie ein Einselement. Aus den Eigenschaften der Verknüpfung von Abbildungen (vgl. § 0.2) erkennt man, daß das Monoid $[M(X), \circ]$ aus Beispiel 7 eine Halbgruppe ist; ihr Einselement ist die identische Abbildung id_X. Die Menge $M(X)^*$ besteht aus allen umkehrbaren, d. h. den bijektiven Abbildungen von X in X, die wir auch *Transformationen von* X nennen.

Einer der grundlegenden algebraischen Begriffe, der in vielen Teilen der Mathematik wichtige Anwendungen findet, ist der Begriff einer Gruppe, den wir nun definieren wollen.

Definition 6. Unter einer *Gruppe* versteht man eine Halbgruppe mit Einselement, deren sämtliche Elemente invertierbar sind.

Nach dem oben Gesagten ist eine Gruppe also ein Monoid $[G, \cdot]$, das die folgenden Eigenschaften besitzt:

1. $(ab)\,c = a(bc) \qquad (a, b, c \in G)$.

2. Es existiert ein $e \in G$, für das $ae = ea = a$ gilt für alle $a \in G$.

3. Für jedes $a \in G$ existiert ein $b \in G$, so daß $ab = ba = e$ gilt.

Das Element e heißt *Einselement* und ist eindeutig bestimmt; das Element b in Eigenschaft 3 ist durch a eindeutig bestimmt, es heißt das *Inverse zu* a und wird mit $b = a^{-1}$ bezeichnet.

Statt „kommutative Gruppe" sagt man auch *abelsche* Gruppe.

Beispiel 9. Das Monoid aus Beispiel 1 ist eine abelsche Gruppe, die *additive Gruppe* $[\mathbf{R}, +]$ der reellen Zahlen. Analog wird die additive Gruppe der ganzen Zahlen $[\mathbf{Z}, +]$ und die der rationalen Zahlen $[\mathbf{Q}, +]$ definiert. Das Monoid V aus Beispiel 6 ist ebenfalls eine abelsche Gruppe.

Neben der multiplikativen Schreibweise und Terminologie, wie wir sie für beliebige Halbgruppen vereinbart haben, wird in der Gruppentheorie auch die *additive Schreibweise* viel angewandt, allerdings *nur bei abelschen Gruppen.* Beide Bezeichnungsarten werden durch die entsprechenden Operationen in den Zahlenbereichen nahegelegt. Bei der additiven Terminologie wird die Operation mit $+$ und das neutrale Element, *die Null,* mit 0 bezeichnet; das zu a inverse Element nennt man auch *zu* a *entgegengesetzt* und bezeichnet es mit $-a$; der Division entspricht die Subtraktion, für die man zur Abkürzung

$$b - a := b + (-a)$$

schreibt (vgl. auch Satz 4 und Formel (5)).

Beispiel 10. *Ist M eine beliebige Halbgruppe mit Einselement, so ist die Menge M^* ihrer invertierbaren Elemente eine Gruppe bezüglich der in M gegebenen Operation* (genauer: deren Einschränkung auf $M^* \times M^*$). In der Tat, aus Satz 3, 2., folgt, daß diese Operation nicht aus M^* hinausführt. Nach (1) besitzt M^* ein Einselement, und zu jedem $a \in M^*$ gibt es ein $a^{-1} \in M^*$.

Wenden wir das in Beispiel 10 Ausgeführte auf die Halbgruppe aus Beispiel 2 an, so erhalten wir die *multiplikative Gruppe* $[\mathbf{R}^*, \cdot]$ *der reellen Zahlen,* $\mathbf{R}^* = \mathbf{R} \setminus \{0\}$. Sie ist abelsch. Beispiel 7 gibt uns die wichtige *Gruppe* $S(X) := M(X)^*$ *aller Transformationen der nichtleeren Menge* X.

Übung 1. Man beweise: Das Monoid $M(X, H)$ aus Beispiel 8 besitzt genau dann eine der folgenden Eigenschaften: 1. assoziativ zu sein; 2. ein neutrales Element zu haben; 3. kommutativ zu sein; 4. eine Gruppe zu sein, wenn das Monoid H die entsprechende Eigenschaft besitzt. Enthält H ein Einselement e, so ist die konstante Funktion $e(x) = e$, $x \in X$, das Einselement des Monoids $M(X, H)$, und es gilt $M(X, H)^* = M(X, H^*)$, wobei das zu $f \in M(X, H)^*$ inverse Element durch $f^{-1}(x) = (f(x))^{-1}$, $x \in X$, gegeben wird. (Achtung! Man verwechsle diese Inversenbildung nicht mit der Umkehrfunktion f^{-1} (inversen Abbildung) z. B. in $S(H)$! Aus dem Zusammenhang wird immer klar sein, welche Funktion gemeint ist.)

Aus den oben angegebenen Beispielen erkennt man, daß die Operationen in Halbgruppen oder Gruppen natürliche Verallgemeinerungen der Addition und Multiplikation von Zahlen sind. Die Subtraktion bzw. Division wird in der Elementarmathematik als Umkehrung der Addition bzw. Multiplikation betrachtet; es zeigt sich nun, daß man in einer beliebigen Halbgruppe mit Einselement eine analoge Umkehrung finden kann:

Satz 4. *Es sei M eine Halbgruppe mit Einselement, $a \in M^*$, $b \in M$. Dann haben die Gleichungen*

$$ax = b, \qquad ya = b \tag{2}$$

in M je eine und nur eine Lösung, die entsprechend die folgende Gestalt hat:

$$x = a^{-1}b, \qquad y = ba^{-1}. \tag{3}$$

Beweis. Offensichtlich genügt $x = a^{-1}b$ der ersten der Gleichungen (2):

$$a(a^{-1}b) = (aa^{-1})\, b = b\,. \tag{4}$$

Ist andererseits x_0 irgendeine Lösung dieser Gleichung, so erhalten wir aus $ax_0 = b$ durch Multiplikation mit a^{-1} von links $x_0 = a^{-1}b$. Analog behandelt man die zweite Gleichung. □

Speziell existieren in einer beliebigen Gruppe G stets Lösungen der Gleichungen (2), welche eindeutig bestimmt sind und die Gestalt (3) bzw. (4) haben. Die Formeln (3) und (4) definieren in G zwei Operationen, die „Umkehrungen" der Multiplikation sind; man nennt sie entsprechend die *linke* und *rechte Division*. Ist G abelsch, so stimmen beide Operationen überein und bestimmen die Operation der *Division* in G, die man folgendermaßen schreibt:

$$\frac{b}{a} = a^{-1}b = ba^{-1}. \tag{5}$$

Aus drucktechnischen Gründen benutzt man für den Bruch auch häufig das Symbol b/a statt $\frac{b}{a}$. Den Bruch b/a kann man in einer beliebigen kommutativen Halbgruppe M mit Einselement betrachten; er ist aber nur für Paare (a, b) mit $a \in M^*$ definiert.

Übung 2. Es sei M eine Halbgruppe mit Einselement und $a \in M$. Man beweise: Existieren Lösungen der Gleichungen $ax = e$ und $ya = e$ (*rechtes* und *linkes Inverse von a*), so stimmen sie überein, und es gilt $a \in M^*$. Wenn die Gleichung $ax = e$ für beliebiges a eine Lösung hat, ist M eine Gruppe.

Übung 3. Man beweise: Besitzen in einer Halbgruppe M beide Gleichungen (2) für alle Paare (a, b) wenigstens eine Lösung, so ist M eine Gruppe.

Definition 7. Unter der *Ordnung einer Gruppe G* versteht man ihre Mächtigkeit $|G|$. Eine Gruppe G heißt *endlich*, wenn ihre Ordnung endlich ist, und *unendlich* sonst.

Beispiel 11. Es sei $N_n = \{1, ..., n\}$ die Menge der ersten n natürlichen Zahlen. Man setzt $S_n := S(N_n)$, vgl. Beispiel 10, und spricht von der *symmetrischen Gruppe*

S_n. Ihre Elemente sind die Transformationen von N_n, die man auch *Permutationen* nennt. Die Permutationen $s \in S_n$ beschreibt man durch ihre Wertetabellen:

$$s = \begin{pmatrix} 1 & \dots & n \\ s(1) & \dots & s(n) \end{pmatrix}. \tag{6}$$

Weil die Transformation s bijektiv ist, kommt jedes Element der Menge N_n in der unteren Zeile der Tabelle (6) einmal und nur einmal vor, und umgekehrt entspricht jeder Anordnung der Zahlen aus N_n eine eindeutig bestimmte Permutation. Durch vollständige Induktion beweist man leicht $|S_n| = n!$; also ist die Gruppe S_n endlich. Da die Multiplikation von Permutationen durch die Verknüpfung von Abbildungen definiert wird, ergibt sich für das Produkt $t \cdot s$ zweier Permutationen

$$\begin{pmatrix} 1 & \dots & n \\ t(1) & \dots & t(n) \end{pmatrix} \begin{pmatrix} 1 & \dots & n \\ s(1) & \dots & s(n) \end{pmatrix} = \begin{pmatrix} 1 & \dots & n \\ t(s(1)) & \dots & t(s(n)) \end{pmatrix}.$$

Übung 4. Man beweise, daß die Gruppe S_n für $n \geqq 3$ nicht abelsch ist.

Mitunter benötigen wir eine etwas andere Schreibweise für die Permutationen. Wenn man nämlich in der Tabelle (6) die Spalten in irgendeiner Weise umordnet, beschreibt die neue Tabelle offenbar dieselbe Permutation

$$s = \begin{pmatrix} i_1 & \dots & i_n \\ s(i_1) & \dots & s(i_n) \end{pmatrix}; \tag{7}$$

hierbei ist $i_1, i_2, \dots, i_n$ irgendeine Anordnung der Zahlen $1, 2, \dots, n$. Hat daher s die Form (6), so können wir s^{-1} wie folgt schreiben:

$$s^{-1} = \begin{pmatrix} s(1) & \dots & s(n) \\ 1 & \dots & n \end{pmatrix}.$$

Wir betrachten nun eine Gruppe $G = \{a_1, \dots, a_n\}$ der Ordnung n, wobei $a_1 = e$ sei. Die Produkte von je zwei Elementen aus G ordnen wir in Form einer Tabelle an, die man die *Gruppentafel der Gruppe G* nennt:

$$\begin{array}{llll} e & a_2 & \dots & a_j & \dots & a_n \\ a_2 & a_2a_2 & \dots & a_2a_j & \dots & a_2a_n \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_i & a_ia_2 & \dots & a_ia_j & \dots & a_ia_n \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_n & a_na_2 & \dots & a_na_j & \dots & a_na_n \end{array} \tag{8}$$

Die Vorgabe der Gruppentafel bestimmt die Operation der Gruppe G eindeutig. Die Anordnung der Elemente in der Gruppentafel ist natürlich nicht willkürlich; z. B. folgt aus Satz 4, daß in jeder Zeile und in jeder Spalte der Tafel (8) jedes Element der Gruppe G genau einmal vorkommt.

Übung 5. Es sei G eine Gruppe der Ordnung n. Man beweise, daß eine quadratische Tabelle

$$\begin{array}{lll} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{array} \tag{9}$$

mit $a_{ij} \in G$, $i, j = 1, ..., n$, existiert, die folgende Eigenschaften besitzt: 1. In jeder Zeile und in jeder Spalte der Tabelle (9) kommt jedes Element der Gruppe G genau einmal vor: 2. es gilt

$$a_{ij}a_{jk} = a_{ik} \qquad (i, j, k = 1, ..., n) . \tag{10}$$

Umgekehrt beweise man: Ist eine Tabelle (9) aus Elementen einer Menge G gegeben, welche die Eigenschaft 1 besitzt, und wird durch (10) eine Operation in G korrekt definiert, so wird G mit der Operation (10) eine Gruppe. (Dabei bedeutet „korrekt definiert", daß sich aus (10) immer dasselbe Produkt $a \cdot b$ ergibt, unabhängig davon, in welcher Zeile man das Element $a = a_{ij}$ aufsucht.)

Übung 6. Für $n = 2, 3, 4$ bestimme man alle möglichen Tabellen aus Elementen der Menge $\{a_1, ..., a_n\}$, die Gruppentafeln von Gruppen der Ordnung n sind. (Tabellen, die durch Umnumerierung der Elemente ineinander übergehen, brauchen wir dabei nicht zu unterscheiden.)

Der Begriff einer algebraischen Operation kann wesentlich verallgemeinert werden. Es seien A, M, N beliebige nichtleere Mengen; unter einer Operation kann man dann eine Abbildung $(a, b) \in A \times M \mapsto a * b \in N$ verstehen, die jedem Paar $(a, b) \in A \times M$ ein eindeutig bestimmtes Element $a * b \in N$ zuordnet. Derartige Operationen werden wir im folgenden häufig antreffen. Ist speziell $M = N$, so sagt man, daß eine *Aktion der Menge A auf der Menge M* gegeben sei. Diese Terminologie rührt daher, daß jedem $a \in A$ eine Abbildung l_a von M in M entspricht, die durch die Formel $l_a(x) = a * x$ $(x \in M)$ definiert wird.

Eine andere Verallgemeinerung besteht in Folgendem. Es sei n eine natürliche Zahl. Unter einer *n-stelligen Operation* auf der Menge M versteht man eine beliebige Abbildung

$$(a_1, ..., a_n) \in M^n \mapsto c = a_1 * ... * a_n \in M . \tag{11}$$

Die oben betrachteten algebraischen Operationen sind binär (zweistellig); als Beispiel einer unären (einstelligen) Operation erwähnen wir die Abbildung $a \mapsto a^{-1}$ in einer beliebigen Gruppe. Im folgenden werden uns noch einige n-stellige Operationen begegnen, so daß wir hier auf Beispiele verzichten können.

§ 2. Untergruppen und Homomorphismen

In diesem Paragraphen wollen wir einige wichtige Grundbegriffe der Gruppentheorie entwickeln, die es uns gestatten, verschiedene Gruppen miteinander zu vergleichen. Eine einfache Relation zwischen Gruppen kann darin bestehen, daß eine Gruppe als „Untergruppe" in einer anderen enthalten ist. Hierunter verstehen wir folgendes:

Definition 1. Eine Teilmenge H der Gruppe G heißt eine *Untergruppe von G*, wenn H eine Gruppe bezüglich der Einschränkung der auf $G \times G$ gegebenen Multiplikation auf $H \times H$ ist.

Satz 1. *Eine Teilmenge H der Gruppe G ist eine Untergruppe dann und nur dann, wenn sie die folgenden Bedingungen erfüllt:*

1. $H \neq \emptyset$;
2. *mit* $a, b \in H$ *gilt auch* $ab \in H$;
3. *mit* $a \in H$ *gilt auch* $a^{-1} \in H$.

Beweis. Offenbar besitzt eine beliebige Untergruppe die Eigenschaften 1 bis 3. Möge umgekehrt die Teilmenge H diese Bedingungen erfüllen. Infolge der Eigenschaften 1 und 2 ist $[H, \cdot]$ ein Monoid. Da die Operation in G assoziativ ist, ist das Monoid eine Halbgruppe. Wegen der Eigenschaften 2 und 3 gilt mit $a \in H$ auch $e = aa^{-1} \in H$. Offenbar ist e auch Einselement in H. Aus der Eigenschaft 3 ergibt sich schließlich, daß $[H, \cdot]$ eine Gruppe ist. □

Beispiel 1. In einer beliebigen Gruppe ist die nur aus dem Einselement bestehende Teilmenge $\{e\}$ eine Untergruppe, die man die *triviale Untergruppe* nennt.

Beispiel 2. Jede Gruppe ist Untergruppe in sich selbst. Ist eine Untergruppe nicht trivial und von der ganzen Gruppe G verschieden, so nennt man sie eine *eigentliche Untergruppe*.

Beispiel 3. Die additiven Gruppen $\mathbf{Z}$ und $\mathbf{Q}$ sind Untergruppen von $[\mathbf{R}, +]$, und $\mathbf{Z}$ ist eine Untergruppe von $\mathbf{Q}$.

Beispiel 4. Die Menge $\{1, -1\}$ ist eine Untergruppe in der multiplikativen Gruppe $\mathbf{R}^*$. Ein weiteres Beispiel einer Untergruppe von $\mathbf{R}^*$ ist die Menge $\mathbf{R}_+$ aller positiven reellen Zahlen.

Beispiel 5. Für jedes $k \in \mathbf{Z}$ ist die Menge $k\mathbf{Z} := \{km \mid m \in \mathbf{Z}\}$ der durch k teilbaren ganzen Zahlen eine Untergruppe von $\mathbf{Z}$. Es ist bemerkenswert, daß überhaupt jede nichttriviale Untergruppe von $\mathbf{Z}$ diese Gestalt hat:

Satz 2. *Jede nichttriviale Untergruppe* $H \subset \mathbf{Z}$ *hat die Form* $H = n\mathbf{Z}$, *wobei* n *die kleinste natürliche Zahl ist, die in* H *liegt.*

Beweis. Wir bemerken zunächst, daß jede nichttriviale Untergruppe $H \subset \mathbf{Z}$ wenigstens eine natürliche Zahl enthält. In der Tat, gilt $m \in H$ und $m \neq 0$, so ist entweder $m > 0$ oder $m < 0$; aber im zweiten Fall ist $-m \in H$ und $-m > 0$. Offensichtlich existiert in H eine kleinste natürliche Zahl n. Ist $k \in \mathbf{Z}$ und $k > 0$, so folgt induktiv aus $nk = n(k-1) + n$, daß nk auch in H liegt. Ist $k \in \mathbf{Z}$ und $k < 0$, so ist $nk = -(n(-k)) \in H$, denn es gilt $-k > 0$. Schließlich ist $n0 = 0 \in H$. Damit ist gezeigt, daß die gesamte Untergruppe $n\mathbf{Z}$ in H enthalten ist. Wir zeigen, daß die Untergruppen H und $n\mathbf{Z}$ zusammenfallen. Dazu teilen wir ein beliebiges $m \in H$ mit Rest durch n, d. h., wir stellen es in der Form $m = nq + r$, $q, r \in \mathbf{Z}$, $0 \leqq r < n$, dar. Da nq in H liegt, gilt auch $r = m - nq \in H$. Wäre nun $r > 0$, so erhielten wir einen Widerspruch, da n die kleinste natürliche Zahl ist, die in H liegt. Also gilt $r = 0$ und $m = nq \in n\mathbf{Z}$. □

Übung 1. Man beweise, daß die Gruppe $[\mathbf{R}, +]$ keine nichttrivialen endlichen Untergruppen enthält und daß die einzige nichttriviale endliche Untergruppe der multiplikativen Gruppe $\mathbf{R}^*$ die Gruppe $\{1, -1\}$ ist.

Wir wollen nun eine wichtige Untergruppe der symmetrischen Gruppe S_n beschreiben. Dazu benötigen wir einige Eigenschaften dieser Gruppe, die auch an sich

von Interesse sind. Es sei $i, j \in N_n = \{1, 2, ..., n\}$, $i \neq j$. Mit $(i\ j)$ bezeichnen wir die Permutation, die auf N_n folgendermaßen wirkt:

$$(i\ j)(x) = \begin{cases} j & \text{für} \quad x = i, \\ i & \text{für} \quad x = j, \\ x & \text{für} \quad x \neq i, j\,. \end{cases}$$

Anders gesagt ist $(i\ j)$ die Permutation

$$(i\ j) = \begin{pmatrix} 1 & \dots & i & \dots & j & \dots & n \\ 1 & \dots & j & \dots & i & \dots & n \end{pmatrix}.$$

Diese Permutationen $(i\ j)$ heißen *Transpositionen*. Offenbar gilt

$$(i\ j)^{-1} = (j\ i) = (i\ j)\,.$$

Satz 3. *Jedes Element der symmetrischen Gruppe S_n, $n \geqq 2$, läßt sich als Produkt von endlich vielen Transpositionen darstellen.*

Beweis. Wir führen den Beweis durch Induktion nach n. Für $n = 2$ gilt der Satz offensichtlich. Die Behauptung sei schon für S_{n-1} bewiesen, und es sei $s \in S_n$. Wir unterscheiden die beiden Fälle

$$1.\ s(n) = n, \qquad 2.\ s(n) \neq n\,.$$

Im ersten Fall führt s die Teilmenge $N_{n-1} \subset N_n$ in sich über und induziert eine gewisse Permutation $s' \in S_{n-1}$. Nach Induktionsvoraussetzung gilt

$$s' = (i_1\ j_1) \circ \dots \circ (i_k\ j_k)$$

mit $i_\alpha, j_\alpha \in N_{n-1}$. Dann gilt aber auch

$$s = (i_1\ j_1) \circ \dots \circ (i_k\ j_k)\,,$$

wobei jetzt die rechts stehenden Transpositionen als Elemente der Gruppe S_n betrachtet werden. In der Tat führen die rechts und links stehende Permutation das Element $n \in N_n$ in sich über, während sie auf N_{n-1} übereinstimmen. Im zweiten Fall betrachten wir die Permutation $s_1 = (s(n)\ n) \circ s$. Offensichtlich gilt $s_1(n) = n$. Nach dem bereits Bewiesenen können wir s_1 als Produkt

$$s_1 = (i_1\ j_1) \circ \dots \circ (i_k\ j_k)$$

darstellen. Hieraus ergibt sich

$$s = (s(n)\ n)^{-1} \circ s_1 = (s(n)\ n) \circ (i_1\ j_1) \circ \dots \circ (i_k\ j_k)\,. \quad \square$$

Man bemerkt unschwer, daß die Zerlegung einer Permutation in ein Produkt von Transpositionen nicht eindeutig bestimmt ist; nicht einmal die Anzahl der Faktoren einer solchen Zerlegung ist eindeutig bestimmt. Wir werden jedoch gleich sehen, daß die Eigenschaft dieser Zahl, gerade oder ungerade zu sein, nicht von der Wahl der Zerlegung abhängt. Für eine beliebige Permutation $s \in S_n$ bezeichne $N(s)$ die Anzahl der Paare $(i, j) \in N_n \times N_n$, für die $i < j$ und $s(i) > s(j)$ gilt. Diese Zahl $N(s)$ kann man leicht aus der Gestalt (1.6) einer gegebenen Permutation bestimmen.

Definition 2. Eine Permutation $s \in S_n$ heißt *gerade*, wenn $N(s)$ gerade ist, und *ungerade* sonst.

Lemma 1. *Es sei $s \in S_n$, $(i\ j)$ eine beliebige Transposition aus S_n und $s_1 = s \circ (i\ j)$. Dann ist s gerade (bzw. ungerade) genau dann, wenn s_1 ungerade (bzw. gerade) ist.*

Beweis. Es sei zunächst $j = i+1$. Dann gilt

$$s_1 = \begin{pmatrix} 1 & \dots & i & i+1 & \dots & n \\ s(1) & \dots & s(i) & s(i+1) & \dots & s(n) \end{pmatrix} \circ (i\ i+1)$$
$$= \begin{pmatrix} 1 & \dots & i & i+1 & \dots & n \\ s(1) & \dots & s(i+1) & s(i) & \dots & s(n) \end{pmatrix}.$$

Man sieht, daß $N(s_1) = N(s)+1$ ist, falls $s(i+1) > s(i)$ gilt, und $N(s_1) = N(s)-1$ im umgekehrten Fall. Für beliebige i, j mit $i < j$ ist

$$(i\ j) = (i\ i+1) \circ \dots \circ (j-2\ j-1) \circ (j-1\ j)$$
$$\circ (j-2\ j-1) \circ \dots \circ (i+1\ i+2) \circ (i\ i+1)$$

ein Produkt aus $2(j-i)-1$ Transpositionen zweier aufeinanderfolgender Zahlen. Also entsteht s_1 aus s durch sukzessive Multiplikation einer ungeraden Anzahl von Transpositionen der Form $(k\ k+1)$ von rechts, woraus unsere Behauptung folgt. □

Satz 4. *Die Permutation $s \in S_n$, $n \geqq 2$, ist dann und nur dann gerade, wenn bei einer beliebigen Zerlegung von s in ein Produkt von Transpositionen die Anzahl der Faktoren gerade ist.*

Beweis. Für eine beliebige Zerlegung von s kann man auch

$$s = (\dots (e \circ (i_1\ j_1)) \circ \dots) \circ (i_k\ j_k)$$

schreiben. Da $N(e) = 0$ gilt, ist $N(s)$ nach Lemma 1 genau dann gerade, wenn die Anzahl der Faktoren gerade ist. □

Satz 5. *Es seien $s, t \in S_n$, $n \geqq 2$. Dann ist $s \circ t$ gerade genau dann, wenn entweder s und t beide gerade oder beide ungerade sind. Mit $s \in S_n$ ist auch s^{-1} gerade (bzw. ungerade).*

Beweis. Zerlegen wir s und t irgendwie in Transpositionen, so erhalten wir durch Multiplikation dieser Zerlegung eine Zerlegung von $s \circ t$, wobei die Anzahl der Faktoren von $s \circ t$ gleich der Summe der Anzahlen der Faktoren von s und t ist. Die erste Behauptung folgt dann unmittelbar aus Satz 4. Die zweite Behauptung ergibt sich aus der ersten und der Bemerkung, daß $e = s \circ s^{-1}$ gerade ist. □

Aus den Sätzen 5 und 1 erhält man sofort

Folgerung 1. *Die Menge A_n aller geraden Permutationen s aus S_n ist eine Untergruppe von S_n*, die man die *alternierende Gruppe* nennt. □

Für das Weitere ist es zweckmäßig, das Symbol

$$\operatorname{sgn} s := (-1)^{N(s)} \qquad (s \in S_n) \tag{1}$$

(lies: „*Signum von s*") einzuführen. Es gilt $\operatorname{sgn} s = 1$, wenn s gerade ist, und $\operatorname{sgn} s = -1$ im entgegengesetzten Fall. Aus Satz 5 ergibt sich

Folgerung 2. $\operatorname{sgn}(s \circ t) = \operatorname{sgn} s \cdot \operatorname{sgn} t$, $\operatorname{sgn}(s^{-1}) = \operatorname{sgn} s$. □

Übung 2. Man beweise $|A_n| = \frac{1}{2}|S_n| = \frac{1}{2} n!$.

Übung 3. Wir betrachten die folgende Funktion von n Variablen $x_i \in \mathbf{R}$, $i = 1, \ldots, n$:

$$f(x_1, \ldots, x_n) := \prod_{1 \leq i < j \leq n} (x_i - x_j) .$$

Man beweise, daß für $s \in S_n$

$$f(x_{s(1)}, \ldots, x_{s(n)}) = \operatorname{sgn} s \cdot f(x_1, \ldots, x_n)$$

gilt. Hieraus leite man Lemma 1 her.

Übung 4. Man beweise $N(s^{-1}) = N(s)$.

Übung 5. Man beweise, daß das Signum einer Permutation s, die in der Form (1.7) gegeben ist, nach der Formel $\operatorname{sgn} s = (-1)^{p+q}$ bestimmt werden kann, wobei p die Anzahl der Paare (α, β) mit $\alpha < \beta$ und $i_\alpha > i_\beta$ ist, während q die Anzahl der Paare (α, β) bezeichnet, für die $\alpha < \beta$ und $s(i_\alpha) > s(i_\beta)$ gilt.

Wir wollen noch eine Verallgemeinerung des Begriffs einer Transposition definieren. Es sei $(i_1, \ldots, i_k)$ ein k-Tupel aus $k \geq 1$ verschiedenen Elementen von N_n. Unter dem Symbol $(i_1 \ldots i_k)$ verstehen wir diejenige Permutation s, die folgendermaßen auf N_n definiert ist:

$$s(i_1) = i_2, \ldots, s(i_{k-1}) = i_k , \qquad s(i_k) = i_1, \qquad s(j) = j$$

für alle $j \notin \{i_1, \ldots, i_k\}$. Eine solche Permutation heißt ein *Zyklus der Länge k*. Zwei Zyklen heißen *unabhängig*, wenn die sie definierenden Tupel elementfremd sind. Jeder Zyklus der Länge $k = 1$ ist gleich der identischen Permutation $(j) = e = \mathrm{id}_{N_n}$.

Übung 6. Man beweise, daß jede Permutation $s \neq e$ bis auf die Reihenfolge der Faktoren eindeutig in ein Produkt paarweise unabhängiger Zyklen der Länge $k > 1$ zerlegt werden kann. Ferner gilt $\operatorname{sgn} s = (-1)^{n+p-q}$, wobei p die Anzahl der Faktoren dieser Zerlegung und q die Anzahl derjenigen Elemente der Menge N_n bezeichnet, die bei Anwendung von $s \in S_n$ in sich übergehen.

Es sei nun $S \subset G$ eine beliebige nichtleere Teilmenge einer Gruppe G. Mit $[S]$ bezeichnen wir die Menge aller derjenigen Elemente $a \in G$, die als ein Produkt der Form $a = a_1 \ldots a_r$ darstellbar sind, wobei für alle i die Faktoren a_i oder ihre Inversen a_i^{-1} zu S gehören und $r \in \mathbf{N}$ gilt.

Satz 6. *Für beliebiges nichtleeres $S \subseteq G$ ist die Menge $[S]$ eine Untergruppe von G, die S enthält. Diese Untergruppe ist die kleinste aller derjenigen Untergruppen, die S enthalten: Ist H eine Untergruppe von G und gilt $S \subseteq H$, so ist $[S] \subseteq H$.*

Beweis. Aus der Definition ergibt sich sofort, daß das Produkt $a \cdot b$ zweier Elemente $a, b \in [S]$ wieder in $[S]$ liegt. Nach Satz 1.3 liegt mit a auch das inverse Element a^{-1} in $[S]$. Da S nicht leer ist und offenbar $S \subseteq [S]$ gilt, folgt aus Satz 1, daß

$[S]$ eine Untergruppe ist. Ist schließlich H eine S enthaltende Untergruppe, so muß H auch alle Inversen zu Elementen von S und daher auch alle in $[S]$ liegenden Produkte enthalten, womit auch die zweite Behauptung bewiesen ist. □

Definition 3. Die Untergruppe $[S]$ heißt die *von S erzeugte Untergruppe* und S eine *erzeugende Menge* von $[S]$. Ist speziell $G=[S]$, so heißt S eine *erzeugende Menge der Gruppe G*. Es ist zweckmäßig, $[\emptyset]:=\{e\}$ zu verabreden.

Zum Beispiel ist nach Satz 3 die Menge aller Transpositionen eine erzeugende Menge der Gruppe S_n.

Übung 7. Man beweise, daß S_n durch die Menge $\{(1\ 2), ..., (n-1\ n)\}$ erzeugt wird.

Übung 8. Man beweise, daß in einer kommutativen Halbgruppe die Regel

$$a_{s(1)} \cdots a_{s(n)} = a_1 \cdots a_n$$

für alle $s \in S_n$ gilt.

Übung 9. Man beweise, daß A_n durch die Menge $\{(1\ 2\ 3), ..., (1\ 2\ n)\}$ erzeugt wird.

In der Gruppe G sei nun eine beliebige Familie von Untergruppen $(H_\alpha)_{\alpha\in A}$ gegeben; hierbei sei A eine endliche oder unendliche beliebige Indexmenge. Nach Satz 6 kann man leicht die kleinste Untergruppe der Gruppe G angeben, die alle H_α, $\alpha\in A$, enthält; es ist dies $H:=\left[\bigcup_{\alpha\in A} H_\alpha\right]$. Wir nennen H die *von der Familie $(H_\alpha)_{\alpha\in A}$ erzeugte Untergruppe*. Andererseits können wir leicht die größte Untergruppe bestimmen, die in allen H_α, $\alpha\in A$, enthalten ist:

Satz 7. *Ist $(H_\alpha)_{\alpha\in A}$ eine beliebige Familie von Untergruppen der Gruppe G, so ist der Durchschnitt $\bigcap_{\alpha\in A} H_\alpha$ eine Untergruppe, die in allen H_α, $\alpha\in A$, enthalten ist. Für jede Untergruppe $K\subseteq G$, die die Bedingung $K\subset H_\alpha$ für alle $\alpha\in A$ erfüllt, gilt $K\subseteq \bigcap_{\alpha\in A} H_\alpha$.*

Beweis. Die erste Behauptung folgt leicht aus Satz 1 und die zweite ist offensichtlich. □

Bemerkung. Mit der in Beispiel 0.2.15 eingeführten Terminologie können wir Satz 7 und die davor stehende Behauptung folgendermaßen zusammenfassen: *Das System $\mathfrak{U}(G):=\{H \mid H\subseteq G$ Untergruppe$\}$ der Untergruppen von G ist bezüglich der Ordnung $\subseteq$ ein vollständiger Verband.*

Übung 10. Man beweise, daß $[S]$ gleich dem Durchschnitt aller derjenigen Untergruppen der Gruppe G ist, die S enthalten.

Wir wollen nun einige Begriffe einführen, die im folgenden häufig gebraucht werden. Es sei $[M, \cdot]$ irgendein Monoid, und S, T seien Teilmengen von M. Mit ST bezeichnen wir die Menge aller Produkte der Form ab mit $a\in S$ und $b\in T$. Besteht eine der Mengen S, T nur aus einem Element, so schreibt man auch $aT=\{a\}\,T$ bzw. $Sb=S\{b\}$. Ist $[M, \cdot]$ eine Halbgruppe und $S_i\subseteq M$, $i=1, ..., r$, eine endliche Familie von Teilmengen, so bezeichne $\prod_{i=1}^{r} S_i = S_1 \cdots S_r$ die Menge aller Produkte der Form $a_1 \cdots a_r$ mit $a_i\in S_i$. Man nennt $\prod_{i=1}^{r} S_i$ das *Produkt der Teilmengen* $S_1, ..., S_r$.

Wir betrachten schließlich den Fall, daß $M=G$ eine *abelsche* Gruppe ist, in der wir die Operation additiv schreiben. Hier läßt sich die soeben gegebene Definition auf eine beliebige Familie $(H_i)_{i\in I}$ von Untergruppen der Gruppe G verallgemeinern. Unter der *Summe* $\sum_{i\in I} H_i$ *der Untergruppen* H_i versteht man die Menge aller derjenigen Elemente $g\in G$, die in der Form $g=h_{i_1}+\ldots+h_{i_n}$ mit $n\in\mathbf{N}$, $i_\alpha\in I$, $i_\alpha\neq i_\beta$ für $\alpha\neq\beta$, $\alpha=1, \ldots, n$, dargestellt werden können. Ein solches Element g schreibt man auch als *formal unendliche Summe* $g=\sum_{i\in I} h_i$ mit $h_i\in H_i$ und $h_i=0$ für fast alle, d. h. alle bis auf endlich viele, $i\in I$.

Satz 8. *Es sei* $[G,+]$ *eine abelsche Gruppe und* $(H_i)_{i\in I}$ *eine Familie von Untergruppen* $H_i\subseteq G$. *Dann ist die Summe* $\sum_{i\in I} H_i$ *gleich der von der Familie* $(H_i)_{i\in I}$ *erzeugten Untergruppe.*

Beweis. Es sei H die von der Familie $(H_i)_{i\in I}$ erzeugte Untergruppe. Offenbar gilt $\sum_{i\in I} H_i\subseteq H$. Gilt umgekehrt $h\in H$, so läßt sich h in der Form $h=h_{i_1}+\ldots+h_{i_r}$ mit $h_{i_\alpha}\in H_{i_\alpha}$ darstellen, weil die H_{i_α} Untergruppen sind. Wegen der Kommutativität und Assoziativität der Operation und weil die H_i Untergruppen sind, können wir die Summanden, die zu derselben Untergruppe gehören, zusammenfassen und erhalten $h=h_{j_1}+\ldots+h_{j_k}$, wobei die j_λ paarweise verschieden sind. Daher gilt $h\in\sum_{i\in I} H_i$. □

Bemerkung. Für nichtabelsche Gruppen wird eine Verallgemeinerung dieses Satzes durch Satz 3.2.2 gegeben.

Wir wollen nun Homomorphismen untersuchen, das sind Abbildungen, die mit den gerade betrachteten Operationen vertauschbar sind. Zuerst definieren wir Homomorphismen für beliebige Monoide und spezialisieren dann auf den Fall der Gruppen.

Definition 4. Es seien $[M,\cdot]$ und $[N,\cdot]$ Monoide. Eine Abbildung $f\colon M\to N$ heißt ein *Homomorphismus*, wenn für alle $a, b\in M$

$$f(ab)=f(a)\cdot f(b)$$

gilt. Ein Homomorphismus eines Monoids in sich heißt ein *Endomorphismus* des Monoids M.

Beispiel 6. Die Exponentialfunktion $f(x)=2^x$ ist ein Homomorphismus der additiven Gruppe $\mathbf{R}$ in die multiplikative Gruppe $\mathbf{R}^*$.

Beispiel 7. Die Funktion $f(x)=|x|$ ist ein Endomorphismus des Monoids $[\mathbf{R},\cdot]$.

Beispiel 8. Nach Folgerung 2 ist die durch (1) definierte Abbildung sgn: $S_n\to\mathbf{R}^*$ ein Homomorphismus der Gruppen.

Beispiel 9. Es sei H eine Untergruppe der Gruppe G. Dann ist die durch $a\in H\mapsto i(a):=a\in G$ definierte *Einbettung ein Gruppenhomomorphismus.*

Satz 9. *Sind* $f: M \to N$ *und* $g: N \to P$ *Homomorphismen von Monoiden, so ist auch* $g \circ f: M \to P$ *ein Homomorphismus. Ist der Homomorphismus* $f: M \to N$ *umkehrbar, so ist auch* $f^{-1}: N \to M$ *ein Homomorphismus.*

Beweis. Für $a, b \in M$ gilt

$$(g \circ f)(ab) = g(f(ab)) = g(f(a)\, f(b)) = g(f(a))\, g(f(b)) = (g \circ f)(a) \cdot (g \circ f)(b) .$$

Ist f umkehrbar und sind $a, b \in N$, so gilt

$$f(f^{-1}(a) \cdot f^{-1}(b)) = f(f^{-1}(a)) \cdot f(f^{-1}(b)) = ab .$$

Wendet man auf diese Gleichung f^{-1} an, so folgt $f^{-1}(a) \cdot f^{-1}(b) = f^{-1}(ab)$. □

Definition 5. Ein Homomorphismus von Monoiden heißt ein *Isomorphismus*, wenn er umkehrbar, d. h. bijektiv, ist. Einen Isomorphismus eines Monoids auf sich nennt man auch *Automorphismus*. Zwei Monoide M, N heißen *isomorph*, wenn es einen Isomorphismus von M auf N gibt; es können natürlich mehrere derartige Isomorphismen existieren. Ist M isomorph zu N, so schreiben wir $M \cong N$.

Satz 10. *Die Isomorphie* $\cong$ *ist eine Äquivalenzrelation in der Klasse aller Monoide.*

Beweis. Offenbar ist die identische Abbildung eines Monoids ein Automorphismus, also $M \cong M$. Gilt $M \cong N$, so existiert ein Isomorphismus $f: M \to N$. Nach Satz 9 ist $f^{-1}: N \to M$ ebenfalls ein Isomorphismus, d. h. $N \cong M$. Gilt $M \cong N$ und $N \cong P$ und sind $f: M \to N$ und $g: N \to P$ entsprechende Isomorphismen, so folgt aus Satz 9, daß auch $g \circ f: M \to P$ ein Isomorphismus ist, also $M \cong P$ gilt. □

Die Operationen in zwei isomorphen Monoiden besitzen offenbar vollkommen gleiche algebraische Eigenschaften. Ist z. B. ein Monoid einer Gruppe isomorph, so ist es selbst eine Gruppe. Daher werden isomorphe Monoide mitunter identifiziert.

Beispiel 10. Der Homomorphismus aus Beispiel 6 bildet $[\mathbf{R}, +]$ isomorph auf die multiplikative Gruppe $\mathbf{R}_+$ ab (vgl. Beispiel 4).

Beispiel 11. Der Homomorphismus sgn aus Beispiel 8 bildet die Gruppe S_2 isomorph auf die Untergruppe $\{1, -1\} \subseteq \mathbf{R}^*$ ab.

Übung 11. Man beweise, daß die Menge End M der Endomorphismen eines beliebigen Monoids M bezüglich der Verknüpfung $\circ$ eine Halbgruppe mit Einselement bildet; die Automorphismen bilden sogar eine Gruppe Aut M. Man bestimme End M und Aut M für die Gruppen $M = \mathbf{Z}$ und $M = S_2$.

Übung 12. Wir bezeichnen mit Hom (G, H) die Menge aller Homomorphismen $G \to H$ der Monoide. Man beweise: Ist H eine abelsche Gruppe, so ist Hom (G, H) eine Untergruppe der abelschen Gruppe $M(G, H)$ (vgl. Übung 1.1).

Übung 13. Man beweise, daß $S(X) \cong S_n$, wobei $n = |X|$ ist, für eine beliebige endliche Menge $X \neq \emptyset$ gilt.

Übung 14. Man beweise, daß jede Gruppe der Ordnung 2 zur Gruppe S_2 und jede Gruppe der Ordnung 3 zur Gruppe A_3 isomorph ist (vgl. Übung 1.6).

Übung 15. Man beweise, daß die additive Gruppe $\mathbf{Q}$ nicht isomorph ist zur multiplikativen Gruppe $\mathbf{Q}_+$ aller positiven rationalen Zahlen (vgl. Beispiel 6).

Wir wollen nun die wichtigsten Eigenschaften der Homomorphismen von Gruppen herleiten.

Satz 11. *Es sei* $f: G \to H$ *ein Homomorphismus der Gruppen. Dann gilt* $f(e)=e$ *und* $f(a)^{-1}=f(a^{-1})$, $a \in G$. *Sind* G *und* H *abelsch, so gilt für alle* $a, b \in G$ *die Beziehung* $f(a/b)=f(a)/f(b)$.

Beweis. Aus $e \cdot e = e$ folgt $f(e) \cdot f(e) = f(e)$. Multipliziert man diese Gleichung von links mit $f(e)^{-1}$, so erhält man $f(e)=e$. Wendet man f auf die Gleichung $aa^{-1} = a^{-1}a = e$ an, so folgt aus dem eben Bewiesenen

$$f(a)\, f(a^{-1}) = f(a^{-1})\, f(a) = e\,.$$

Also ist nach Definition des Inversen $f(a^{-1})=f(a)^{-1}$. Schließlich ist nach Definition $a/b = ab^{-1}$, also

$$f(a/b) = f(a)\, f(b)^{-1} = f(a)/f(b). \quad \square$$

Definition 6. Unter dem *Kern* des Homomorphismus der Gruppen $f: G \to H$ versteht man die Teilmenge $\operatorname{Ker} f := f^{-1}(e) \subseteq G$.

Satz 12. *Es sei* $f: G \to H$ *ein Homomorphismus der Gruppen. Dann ist das Bild* $\operatorname{Im} f = f(G)$ *eine Untergruppe von* H. *Für beliebige Untergruppen* $H' \subseteq H$ *ist das Urbild* $f^{-1}(H') \subseteq G$ *eine Untergruppe. Speziell ist* $\operatorname{Ker} f$ *eine Untergruppe von* G. *Ist schließlich* G' *eine beliebige Untergruppe von* G, *so ist* $f(G')$ *Untergruppe von* H.

Beweis. Wir zeigen, daß $\operatorname{Im} f$ und $f^{-1}(H')$ den Bedingungen von Satz 1 genügen. Es seien $x, y \in \operatorname{Im} f$. Dann gilt $x = f(a)$, $y = f(b)$ mit $a, b \in G$. Weiter ist $xy = f(a)\, f(b) = f(ab) \in \operatorname{Im} f$ und nach Satz 11

$$x^{-1} = f(a)^{-1} = f(a^{-1}) \in \operatorname{Im} f\,.$$

Nach Satz 11 ist $e \in f^{-1}(H')$. Sind $a, b \in f^{-1}(H')$, so gilt $f(ab) = f(a)\, f(b) \in H'$, also $ab \in f^{-1}(H')$; aus $f(a^{-1}) = f(a)^{-1} \in H'$ folgt $a^{-1} \in f^{-1}(H')$. Die dritte Behauptung des Satzes folgt aus der ersten wegen $f(G') = \operatorname{Im} f \mid G'$. $\square$

Satz 13. *Der Gruppenhomomorphismus* $f: G \to H$ *ist injektiv dann und nur dann, wenn* $\operatorname{Ker} f = \{e\}$ *gilt. In diesem Fall ist* f *ein Isomorphismus von* G *auf die Gruppe* $\operatorname{Im} f$.

Beweis. Offensichtlich ist der Kern eines injektiven Homomorphismus trivial. Es sei umgekehrt $\operatorname{Ker} f = \{e\}$. Sind $a, b \in G$ und gilt $f(a) = f(b)$, so ist nach Satz 11 $f(ab^{-1}) = f(a)\, f(b)^{-1} = e$, d. h. $ab^{-1} \in \operatorname{Ker} f$. Hieraus folgt $ab^{-1} = e$, also $a = b$; f ist injektiv. Die zweite Behauptung ist offensichtlich. $\square$

Folgerung 3. *Ein Gruppenhomomorphismus* $f: G \to H$ *ist ein Isomorphismus dann und nur dann, wenn* $\operatorname{Im} f = H$ *und* $\operatorname{Ker} f = \{e\}$ *gilt.* $\square$

Beispiel 12. Für den Homomorphismus sgn aus Beispiel 8 gilt $\operatorname{Im} \operatorname{sgn} = \{1, -1\}$, $\operatorname{Ker} \operatorname{sgn} = A_n$.

§ 3. Die Ordnung eines Elementes. Zyklische Gruppen

Es sei $[G, \cdot]$ eine Gruppe, $a \in G$. Für eine beliebige ganze Zahl $k \in \mathbf{Z}$ definieren wir die *k-te Potenz* des Elementes a folgendermaßen:

$$a^0 := e, \qquad a^{k+1} := a^k \cdot a \qquad \text{induktiv für } k = 0, 1, \ldots,$$

und

$$a^k := (a^{-1})^{-k} \qquad \text{für } k \in \mathbf{Z},\ k < 0\,.$$

Bei einer additiv geschriebenen Gruppe spricht man vom *k-ten Vielfachen* statt von der k-ten Potenz und schreibt ka statt a^k. Die entsprechende Definition ist:

$$0a := 0, \qquad (k+1)\,a := ka + a \qquad \text{induktiv für } k = 0, 1, \ldots,$$

und

$$ka := (-k)\,(-a) \qquad \text{für } k \in \mathbf{Z},\ k < 0\,.$$

Wir kehren nun wieder zur multiplikativen Schreibweise zurück und formulieren einige Eigenschaften der Potenz.

Satz 1. a) *Für festes $a \in G$ ist die Abbildung $k \mapsto a^k$ ein Homomorphismus der additiven Gruppe von $\mathbf{Z}$ in G, d. h., es gilt*

$$a^{k+l} = a^k \cdot a^l\,. \tag{1}$$

b) *Für jeden Gruppenhomomorphismus $f: G \to H$ gilt $f(a^k) = f(a)^k$ für alle $k \in \mathbf{Z}$, $a \in G$.*

Beweis. Die Behauptung (1) gilt offenbar für alle $k \geqq 0$ und $l = 0$. Bei festem $k \geqq 0$ beweisen wir sie für alle positiven l durch vollständige Induktion: $a^{k+l+1} = a^{k+l} \cdot a = a^k \cdot a^l \cdot a = a^k \cdot a^{l+1}$. Dabei haben wir die Induktionsvoraussetzung und zweimal die induktive Definition angewandt. Als nächstes betrachten wir den Fall $k \geqq 0$, $l < 0$, aber $k + l \geqq 0$. Durch vollständige Induktion beweist man leicht $a^l \cdot a^{-l} = e$ für alle $l \in \mathbf{Z}$. Da wir bereits gezeigt haben, daß (1) für alle nichtnegativen k, l gilt, erhalten wir aus $k + l \geqq 0$, $-l > 0$ die Beziehung $a^{k+l} \cdot a^{-l} = a^k$; aus der eben erwähnten Identität folgt (1) durch Multiplikation der letzten Gleichung mit a^l von links. Ähnlich beweist man die noch ausstehenden Fälle. Die Behauptung b) folgt leicht aus der Definition eines Homomorphismus und Satz 2.11. □

Übung 1. Man beweise, daß in der Gruppe $\mathbf{Z}$ das k-te Vielfache kl mit dem Produkt der Zahlen kl übereinstimmt.

Übung 2. a) Aus Übung 1 und Satz 1, b), leite man her, daß für eine beliebige Gruppe G

$$a^{kl} = (a^k)^l, \qquad a \in G,\ k, l \in \mathbf{Z}\,, \tag{2}$$

gilt. — b) Es sei $[M, \cdot]$ eine Halbgruppe mit Einselement. Man beweise: Die in der ersten Formelzeile des Paragraphen gegebene induktive Definition der Potenz a^k, $a \in M$, $k \in \mathbf{N}_0$, bleibt auch in diesem Fall sinnvoll, und es gelten die Regeln (1), (2) für $k, l \in \mathbf{N}_0$. Man formuliere und beweise die Analoga von Satz 1 und Satz 2 für diesen Fall.

Übung 3. Man zeige, daß für eine abelsche Gruppe G und beliebiges $k \in \mathbf{Z}$ die durch $a \in G \mapsto p_k(a) := a^k \in G$ definierte Abbildung p_k ein Endomorphismus von G ist.

Für ein festes Element a der Gruppe G sind die folgenden Fälle möglich:

1. Es gibt ein $k>0$, $k\in\mathbf{Z}$, mit $a^k=e$.
2. Es gilt $a^k\neq e$ für alle $k>0$, $k\in\mathbf{Z}$.

Definition 1. Genügt das Element $a\in G$ der Bedingung 1, so heißt die kleinste der natürlichen Zahlen $k>0$, für die $a^k=e$ gilt, die *Ordnung* $o(a)$ *des Elementes* a. Wenn a der Bedingung 2 genügt, sagen wir, a *sei von unendlicher Ordnung*, und schreiben $o(a)=\infty$.

Definition 2. Das Bild des Homomorphismus $f\colon k\in\mathbf{Z}\mapsto a^k\in G$ heißt die *vom Element* $a\in G$ *erzeugte zyklische Untergruppe der Gruppe* G; sie wird mit $[a]$ bezeichnet. Das Element a heißt ein *erzeugendes Element* der Untergruppe $[a]$.

Nach Satz 2.12 ist nämlich das Bild eines Homomorphismus eine Untergruppe. Offensichtlich ist $[a]$ die Menge aller ganzzahligen Potenzen des Elementes a und stimmt daher mit der von der Einermenge $\{a\}$ erzeugten Untergruppe $[\{a\}]$ überein (vgl. Satz 2.6).

Satz 2. *Es sei* G *eine Gruppe,* $a\in G$, $n\in\mathbf{N}$, $o(a)=n$. *Für den Homomorphismus* f *aus Definition 2 gilt dann* $\operatorname{Ker} f=n\mathbf{Z}$, $|[a]|=n$ *und* $[a]=\{e, a, \ldots, a^{n-1}\}$. *Ist jedoch* $o(a)=\infty$, *so bildet* f *die Gruppe* $\mathbf{Z}$ *isomorph auf* $[a]$ *ab.*

Beweis. Nach Satz 2.12 ist $\operatorname{Ker} f$ eine Untergruppe von $\mathbf{Z}$. Offenbar ist n die kleinste natürliche Zahl, die in $\operatorname{Ker} f$ liegt. Daher gilt $\operatorname{Ker} f=n\mathbf{Z}$ (vgl. Satz 2.2). Für $k\in\mathbf{Z}$, $k=nq+r$ mit $q, r\in\mathbf{Z}$, $0\leqq r<n$, gilt $a^k=f(k)=f(nq)\,f(r)=f(r)=a^r$. Da jede ganze Zahl in der angegebenen Form darstellbar ist (Division durch n mit Rest), gilt $[a]=\{e, a, \ldots, a^{n-1}\}$. Zum Beweis von $o(a)=|[a]|=n$ zeigen wir, daß alle diese Elemente verschieden sind. Angenommen, k und l sind ganze Zahlen mit $0\leqq k\leqq l<n$, für die $a^k=a^l$ gilt. Dann ist $f(k)=f(l)$, also $f(l-k)=e$, d. h. $l-k\in\operatorname{Ker} f=n\mathbf{Z}$. Aus $0\leqq l-k<n$ und weil n die Zahl $l-k$ teilt, folgt $l=k$.

Es sei nun $o(a)=\infty$. Dann ist $\operatorname{Ker} f=\{0\}$. Gilt nämlich $f(k)=a^k=e$, so kann nach Voraussetzung nicht $k>0$ gelten. Wäre etwa $k<0$, so wäre auch $f(-k)=a^{-k}=e$, was wegen $-k>0$ wiederum nicht möglich ist. Somit muß $k=0$ sein. Die Behauptung folgt nun aus Satz 2.13. □

Beispiel 1. Ist $s\in S_n$ ein Zyklus der Länge k, so ist $o(s)=k$. Folglich hat die zyklische Untergruppe $[s]$ die Ordnung k.

Definition 3. Eine Gruppe G heißt *zyklisch*, wenn sie mit einer ihrer zyklischen Untergruppen übereinstimmt, d. h., wenn es ein $a\in G$ gibt mit $[a]=G$; a heißt dann ein *erzeugendes Element von* G.

Beispiel 2. Offenbar gilt $\mathbf{Z}=[1]$; daher ist $\mathbf{Z}$ eine unendliche zyklische Gruppe.

Beispiel 3. Es bezeichne d_φ die Drehung der euklidischen Ebene E im positiven Sinne um den festen Punkt o und den Winkel φ, $-\infty<\varphi<+\infty$. Offenbar gilt $d_{\varphi+\psi}=d_\varphi\circ d_\psi$, $d_\varphi^{-1}=d_{-\varphi}$, $d_0=\mathrm{id}_E$. Daher bilden die Drehungen d_φ eine Untergruppe $C\subseteqq S(E)$ der Gruppe aller Transformationen der Ebene E, nämlich das Bild des

Homomorphismus $\varphi \in \mathbf{R} \mapsto d_\varphi \in S(E)$. Für $n \in \mathbf{N}$ gilt $o(d_{2\pi/n}) = n$. Die entsprechende zyklische Untergruppe $C_n = [d_{2\pi/n}]$ besteht aus den Drehungen $d_0, d_{2\pi/n}, \ldots, d_{(n-1)2\pi/n}$; man kann sie auch als die Gruppe derjenigen Drehungen definieren, die ein gewisses reguläres n-Eck mit dem Zentrum in o in sich überführen.

Nach der in § 2 eingeführten Terminologie können wir die zyklischen Gruppen auch als diejenigen Gruppen charakterisieren, die eine erzeugende Menge aus nur einem Element besitzen. Sie bilden daher eine natürliche Klasse von Gruppen, die eine besonders einfache Struktur haben. Wir wollen nun eine Klassifikation aller zyklischen Gruppen bis auf Isomorphie angeben, d. h. die Klassen isomorpher zyklischer Gruppen eindeutig kennzeichnen.

Satz 3. *Jede unendliche zyklische Gruppe ist isomorph zur Gruppe* $\mathbf{Z}$. *Zwei endliche zyklische Gruppen sind isomorph dann und nur dann, wenn sie dieselbe Ordnung haben.*

Beweis. Nach Voraussetzung gibt es ein $a \in G$ mit $[a] = G$. Ist G unendlich, so muß nach Satz 2 auch $o(a) = \infty$ gelten, und der Homomorphismus $k \in \mathbf{Z} \mapsto a^k \in G$ ist ein Isomorphismus. Es sei nun $|G| = n$ und $H = [b]$ eine weitere zyklische Gruppe derselben Ordnung n. Nach Satz 2 gilt dann $o(a) = o(b) = n$ und $G = \{e, a, \ldots, a^{n-1}\}$, $H = \{e, b, \ldots, b^{n-1}\}$. Wir definieren die Abbildung φ durch die Formel $\varphi(a^k) = b^k$ für $k = 0, 1, \ldots, n-1$. Offenbar ist φ bijektiv; wir zeigen, daß φ ein Isomorphismus ist. Es seien $k, l \in \mathbf{Z}$, $0 \leqq k < n$, $0 \leqq l < n$, und $k + l = nq + r$, $0 \leqq r < n$, sei die durch Division von $k + l$ durch n mit Rest entstehende Darstellung. Dann gilt $a^k a^l = a^{k+l} = a^r$, also $\varphi(a^k a^l) = \varphi(a^r) = b^r$. Andererseits ist

$$\varphi(a^k)\, \varphi(a^l) = b^k b^l = b^{k+l} = b^r .$$

Hieraus ergibt sich die Behauptung. □

Übung 4. Man zeige, daß jede zyklische Gruppe abelsch ist.

Übung 5. Man bestimme alle erzeugenden Elemente der Gruppe $\mathbf{Z}$.

Übung 6. Es sei $G = [a]$ eine zyklische Gruppe der Ordnung n, $b \in G$. Man beweise die Äquivalenz der folgenden Aussagen: 1. $G = [b]$. 2. $o(b) = n$. 3. Es gilt $b = a^k$, wobei k und n teilerfremd sind.

Übung 7. Man beweise, daß der in Übung 3 definierte Endomorphismus p_k im Fall einer zyklischen Gruppe G der Ordnung n dann und nur dann ein Automorphismus ist, wenn k und n teilerfremd sind.

Übung 8. Aus Übung 2.14 folgt, daß alle Gruppen der Ordnungen 2 und 3 zyklisch sind. Man beweise, daß eine Gruppe der Ordnung 4 entweder zyklisch oder zur „*Kleinschen Vierergruppe*“ V isomorph ist, die aus den vier Permutationen e, $(1\ 2) \circ (3\ 4)$, $(1\ 3) \circ (2\ 4)$, $(1\ 4) \circ (2\ 3) \in S_4$ besteht (vgl. Übung 1.6).

Satz 4. *Jedes homomorphe Bild einer zyklischen Gruppe und jede Untergruppe einer zyklischen Gruppe sind selbst wieder zyklisch.*

Beweis. Es sei $G = [a]$ und $\varphi: G \to G'$ ein Gruppenhomomorphismus. Dann ist jedes $b \in \operatorname{Im} \varphi$ in der Form $b = \varphi(a^k) = \varphi(a)^k$, $k \in \mathbf{Z}$, darstellbar, also $\operatorname{Im} \varphi = [\varphi(a)]$.

Es sei nun H eine Untergruppe der zyklischen Gruppe $G = [a]$. Wir betrachten den Homomorphismus $f: k \mapsto a^k$ der Gruppe $\mathbf{Z}$ auf G. Nach Satz 2.12 ist $f^{-1}(H)$

eine Untergruppe von $\mathbf{Z}$. Aber aus Satz 2.2 erkennt man, daß jede Untergruppe von $\mathbf{Z}$ zyklisch ist. Nun gilt $H = f(f^{-1}(H))$; H ist also Bild der zyklischen Untergruppe $f^{-1}(H) \subset \mathbf{Z}$ bei dem eingeschränkten Homomorphismus $f \mid f^{-1}(H)$ und ist nach dem zuerst Bewiesenen selbst zyklisch. □

Übung 9. Es sei $G = [a]$ eine zyklische Gruppe der Ordnung n. Man beweise, daß für jede natürliche Zahl m, die n teilt, eine einzige Untergruppe $H \subseteq G$ der Ordnung m existiert, nämlich $H = [a^{n/m}]$; auf diese Weise erhält man alle Untergruppen von G.

Übung 10. Es seien G, H zyklische Gruppen. Man zeige, daß die Gruppe Hom (G, H) (vgl. Übung 2.12) eine zyklische Gruppe ist, bestimme ihre Ordnung und finde ein erzeugendes Element.

§ 4. Transformationsgruppen

Es sei X eine nichtleere Menge. In Beispiel 1.10 haben wir die Gruppe $S(X)$ aller Transformationen der Menge X eingeführt. Wir wollen nun die Grundbegriffe der Theorie der Transformationsgruppen darlegen, die sich auf die Untergruppen von $S(X)$ stützt.

Definition 1. Unter einer *Wirkung der Gruppe* G auf einer nichtleeren Menge X versteht man eine Abbildung

$$(a, x) \in G \times X \mapsto ax \in X$$

der Menge $G \times X$ in X, welche die folgenden Eigenschaften besitzt:

1. $a(bx) = (ab)\, x$ für alle $a, b \in G$ und $x \in X$;
2. $ex = x$ für alle $x \in X$.

Wir wollen zuerst eine andere Formulierung dieses Begriffs angeben. Jedem beliebigen $a \in G$ entspricht eine Abbildung

$$t_a : x \in X \mapsto ax \in X\,,$$

und für diese Abbildungen sind nach den Eigenschaften 1 und 2 folgende Beziehungen erfüllt:

$$t_a \circ t_b = t_{ab}\,, \tag{1}$$

$$t_e = \mathrm{id}_X\,. \tag{2}$$

Aus (1) und (2) ergibt sich $t_a \circ t_{a^{-1}} = t_{a^{-1}} \circ t_a = \mathrm{id}_X$, d. h., jede Abbildung t_a ist bijektiv und daher eine Transformation $t_a \in S(X)$; ferner gilt $t_{a^{-1}} = t_a^{-1}$. Daher ist nach (1) die Abbildung

$$\varphi : a \in G \mapsto t_a \in S(X) \tag{3}$$

ein Homomorphismus der Gruppe G in die Gruppe $S(X)$. Ist nun umgekehrt ein Homomorphismus $\varphi : G \to S(X)$ gegeben, so erfüllen die Transformationen $t_a := \varphi(a)$ die Eigenschaften (1) und (2), vgl. Satz 2.11. Definieren wir: $(a, x) \in G \times X \mapsto$

$\mapsto ax := \varphi(a)(x) \in X$, so erhalten wir offenbar eine Wirkung der Gruppe G auf X. *Die Vorgabe einer Wirkung der Gruppe G auf der Menge X ist also gleichwertig zur Vorgabe eines Homomorphismus $G \to S(X)$.*

Beispiel 1. Die Gruppe $S(X)$ und jede ihrer Untergruppen *wirkt in natürlicher Weise* auf der Menge X nach der Formel $sx = s(x)$ für $x \in X$, $s \in S(X)$. Dabei gilt $t_s = s$.

Beispiel 2. Für jede beliebige Gruppe G kann man die *triviale Wirkung* von G auf X durch die Festsetzung $ax = x$ für alle $a \in G$, $x \in X$ definieren. Dabei gilt $t_a = \mathrm{id}_X$ für alle $a \in G$.

Beispiel 3. Es sei G irgendeine Gruppe. Die Multiplikation von G ist eine Operation $G \times G \to G$, die den Bedingungen der Definition 1 für $X = G$ genügt. Hierdurch ist eine Wirkung der Gruppe G auf sich definiert, für die

$$t_a(x) = ax \qquad (x \in G) \tag{4}$$

gilt. Diese Transformation $t_a \in S(G)$ heißt die *Linkstranslation um das Element a*; sie wird gewöhnlich mit l_a bezeichnet. Die Wirkung selbst nennt man die *Wirkung von G auf sich mit Hilfe der Linkstranslationen.*

Beispiel 4. Unter der *Rechtstranslation um das Element $a \in G$* versteht man die durch

$$r_a(x) := xa \qquad (x \in G) \tag{5}$$

definierte Transformation $r_a \in S(G)$; nach Satz 1.4 ist r_a nämlich bijektiv. Man prüft leicht die Formel

$$r_{ab} = r_b \circ r_a \qquad (a, b \in G)$$

nach. Definiert man t_a durch

$$t_a := r_{a^{-1}} \qquad (a \in G),$$

so ist die Zuordnung $\varphi: a \in G \mapsto t_a \in S(G)$ ein Gruppenhomomorphismus. Die entsprechende Wirkung heißt *Wirkung von G auf sich mit Hilfe der Rechtstranslationen.* Wir erwähnen noch die Beziehung

$$l_b \circ r_a = r_a \circ l_b \qquad (a, b \in G),$$

die nur eine andere Formulierung des Axioms der Assoziativität ist.

Beispiel 5. Noch eine Wirkung der Gruppe G auf sich erhält man durch die Definition

$$\alpha_a := l_a \circ r_{a^{-1}} = r_{a^{-1}} \circ l_a, \quad \text{d. h.} \quad \alpha_a(x) = axa^{-1} \qquad (x \in G). \tag{6}$$

Aus (5) und (6) folgt leicht $\alpha_a \circ \alpha_b = \alpha_{ab}$, d. h., die Zuordnung $a \mapsto \alpha_a$ definiert eine Wirkung von G auf sich, die man die *Wirkung mit Hilfe der inneren Automorphismen* nennt; denn es gilt

Satz 1. *Die durch* (6) *definierte Transformation der Gruppe G ist ein Automorphismus von G* („*der zu a gehörige innere Automorphismus*"). *Die inneren Automorphismen bilden eine Untergruppe* $\mathrm{Int}\, G \subset \mathrm{Aut}\, G$ (vgl. Übung 2.11).

Beweis. Es gilt $\alpha_a(xy)=axya^{-1}=(axa^{-1})\ (aya^{-1})=\alpha_a(x)\,\alpha_a(y)$. Hieraus und aus Beispiel 5 folgt, daß die Zuordnung $a\mapsto\alpha_a$ ein Homomorphismus der Gruppe G in die Gruppe Aut G ist. Nach Satz 2.12 ist sein Bild eine Untergruppe. □

Definition 2. Die Wirkung der Gruppe G auf X heißt *effektiv*, wenn der zugehörige, durch (3) definierte Homomorphismus $\varphi: G\to S(X)$ injektiv ist. Im allgemeinen Fall heißt die Untergruppe $N:=\operatorname{Ker}\varphi\subset G$ der *Nichteffektivitätskern* der gegebenen Wirkung.

Aus Satz 2.13 folgt, daß die Gruppe G dann und nur dann effektiv auf X wirkt, wenn $N=\{e\}$ gilt; in diesem Fall ist $G\cong\operatorname{Im}\varphi$.

Definition 3. Gegeben sei eine Wirkung von G auf X. Ein Element $x\in X$ heißt *Fixpunkt* des Elementes $a\in G$, wenn $ax=x$, d. h. $t_a(x)=x$, gilt. Die Menge aller derjenigen $x\in X$, für die $t_a(x)=x$ für alle $a\in G$ gilt, wird mit X_G bezeichnet.

Bemerkung zur Terminologie. Ist etwa durch einen Homomorphismus φ nach (3) eine Wirkung von G auf X gegeben, so nennt man das Tripel $[G, X, \varphi]$ eine *Transformationsgruppe*; ist klar, um welche Wirkung von G auf X es sich handelt, so spricht man einfach von der Transformationsgruppe $[G, X]$. Weil die Transformationsgruppen in der Geometrie ihre wichtigsten Anwendungen finden und um sich einer anschaulichen Redeweise zu bedienen, nennt man X auch den *Raum* der Transformationsgruppe und die Elemente von X *Punkte*. Leider ist die Terminologie nicht ganz einheitlich. So wird die im folgenden Satz 2 definierte stationäre Untergruppe G_x auch der *Stabilisator* oder die *Isotropiegruppe* von x genannt; statt Fixpunkt sagt man auch *stabiler* Punkt usw.

Satz 2. *Die Menge aller der Elemente $a\in G$, für die ein gegebenes Element $x\in X$ Fixpunkt ist, ist eine Untergruppe G_x von G, die die stationäre Untergruppe des Punktes x heißt. Es gilt*

$$G_{ax}=\alpha_a(G_x)\qquad(a\in G)\,. \tag{7}$$

Der Nichteffektivitätskern der Transformationsgruppe ist

$$N=\bigcap_{x\in X} G_x\,. \tag{8}$$

Beweis. Es gilt $(bc)\,x=b(cx)=bx=x$, falls $b, c\in G_x$ sind. Weiter ist $ex=x$. Ist $bx=x$, so folgt $b^{-1}x=b^{-1}(bx)=x$. Somit erfüllt G_x die Bedingungen von Satz 2.1 und ist eine Untergruppe. Wir beweisen nun (7). Gilt $bx=x$, so ist $(aba^{-1})\ ax=a(bx)=$ $=ax$, d. h. $\alpha_a(G_x)\subseteq G_{ax}$. Ebenso folgt $\alpha_a^{-1}(G_{ax})\subseteq G_x$, also $G_{ax}\subseteq\alpha_a(G_x)$. Die Gleichung (8) ergibt sich unmittelbar aus den Definitionen. □

Definition 4. Die Wirkung der Gruppe G auf der Menge X heißt *frei*, wenn kein von e verschiedenes Element $a\in G, a\neq e$, einen Fixpunkt besitzt, d. h., wenn $G_x=\{e\}$ für alle $x\in X$ gilt.

Aus (8) ergibt sich sofort, daß *eine freie Wirkung effektiv ist.*

Beispiel 6. Die Wirkung einer Gruppe G auf sich mit Hilfe der linken (bzw. rechten) Translationen ist stets frei. In der Tat, gilt für gewisse $a, x\in G$ die Gleichung $ax=x$, so folgt $a=e$.

Mit Hilfe der Linkstranslationen beweisen wir nun den folgenden Satz, der zeigt, welche Rolle die Transformationsgruppen in der allgemeinen Gruppentheorie spielen.

Satz 3 (Theorem von CAYLEY). *Eine beliebige Gruppe G ist isomorph zu einer Untergruppe von $S(G)$. Eine beliebige endliche Gruppe G der Ordnung n ist isomorph zu einer Untergruppe der symmetrischen Gruppe S_n.*

Beweis. Die Wirkung der Gruppe G mit Hilfe der Linkstranslationen auf sich ist frei und daher effektiv. Somit bildet der zugehörige Homomorphismus $\varphi: G \to S(G)$ die Gruppe G isomorph auf die Gruppe aller Linkstranslationen ab. Gilt $|G| = n$, so existiert ein Isomorphismus $\beta: S(G) \to S_n$ (vgl. Übung 2.13). Dann ist $\beta \circ \varphi$ ein Isomorphismus von G auf eine gewisse Untergruppe von S_n. □

Beispiel 7. Wir betrachten die Wirkung der Gruppe G auf sich mit Hilfe der inneren Automorphismen (Beispiel 5). Ein Element $x \in G$ ist dann und nur dann ein Fixpunkt für $a \in G$, wenn $axa^{-1} = x$, d. h.

$$ax = xa\,,$$

gilt. Man sagt, daß zwei derartige Elemente x und a der Gruppe G *kommutieren*. Die stationäre Untergruppe eines Elementes $x \in G$ ist die Menge aller mit x kommutierenden Elemente. Sie heißt der *Zentralisator des Elementes* x und wird mit Z_x bezeichnet. Nach (8) ist der Nichteffektivitätskern der betrachteten Wirkung gleich $\bigcap_{x \in G} Z_x$. Diese Untergruppe ist die Menge aller derjenigen Elemente der Gruppe G, die mit *allen* $x \in G$ *kommutieren*; sie heißt das *Zentrum der Gruppe* G und wird mit Z_G bezeichnet.

Gegeben sei nun eine Transformationsgruppe $[G, X]$. Wir definieren eine Relation $\sim$ in X folgendermaßen:

$$y \sim x :\Leftrightarrow \text{es gibt ein } a \in G \text{ mit } y = ax\,. \tag{9}$$

Satz 4. *Die Relation* (9) *ist eine Äquivalenzrelation in* X.

Beweis. Offenbar gilt $x = ex$, also $x \sim x$. Ferner folgt aus $y \sim x$, d. h. $y = ax$ für ein $a \in G$, daß $x = a^{-1}y$, also $x \sim y$ ist. Es sei schließlich $y \sim x$ und $z \sim y$, und $a, b \in G$ seien so beschaffen, daß $y = ax$ und $z = by$ gilt. Dann ist $z = b(ax) = (ba)\,x$, d. h. $z \sim x$. □

Die Äquivalenzklasse des Elementes $x \in X$ ist die Menge aller Elemente der Gestalt ax, wobei a die Gruppe G durchläuft; sie heißt der *Orbit von* x bezüglich der Wirkung von G und wird mit $G(x)$ (auch Gx) bezeichnet. *Aus Satz* 4 *und Satz* 0.2.1 *folgt, daß* X *disjunkte Vereinigung der Orbits ist.* Unter dem *Orbitraum* X/G versteht man die Faktormenge $X/G := X/\sim$, vgl. Definition 0.8.

Definition 5. Eine Wirkung der Gruppe G auf X heißt *transitiv*, wenn für beliebige $x, y \in X$ ein $a \in G$ existiert mit $y = ax$, d. h., wenn X der Orbit eines beliebigen seiner Punkte ist; in diesem Fall nennt man X einen *homogenen Raum mit der Gruppe* G. Die Wirkung heißt *einfach transitiv*, wenn sie transitiv und frei ist.

Beispiel 8. Die natürliche Wirkung der Gruppe S_n auf N_n (Beispiel 1) ist transitiv, aber für $n>2$ nicht einfach transitiv. Die stationäre Untergruppe $(S_n)_k$ des Punktes $k\in N_n$ ist isomorph zur Gruppe S_{n-1}.

Beispiel 9. Die Wirkungen der Gruppe G auf sich mit Hilfe der linken bzw. rechten Translationen (Beispiele 3 und 4) sind einfach transitiv.

Beispiel 10. Die Wirkung der Gruppe G auf sich mit Hilfe der inneren Automorphismen (Beispiel 5) ist nicht transitiv, wenn $G\neq\{e\}$ gilt. Der Orbit des Punktes $e\in G$ ist nämlich gleich $\{e\}$. In diesem Fall gilt $x\sim y$ dann und nur dann, wenn ein $a\in G$ existiert, für das

$$y=axa^{-1}$$

gilt; derartige Elemente $x, y\in G$ heißen *konjugiert.*

Wir wollen nun einige einfache notwendige und hinreichende Bedingungen für die Transitivität und die einfache Transitivität einer Transformationsgruppe angeben. Zu jedem beliebigen Element $x\in X$ definieren wir die Abbildung

$$p_x: a\in G\mapsto p_x(a):=ax\in X\ . \tag{10}$$

Man erkennt leicht $\operatorname{Im} p_x=Gx$ und $p_x^{-1}(x)=G_x$. Den einfachen Beweis des folgenden Satzes überlassen wir dem Leser.

Satz 5. *Es sei $[G, X]$ eine Transformationsgruppe. Dann gilt: Für alle $x\in X$ besitzt die Abbildung p_x die Eigenschaft*

$$p_x\circ l_a=t_a\circ p_x \qquad (a\in G)\ . \tag{11}$$

Die Wirkung der Gruppe G auf X ist frei dann und nur dann, wenn p_x für alle $x\in X$ injektiv ist; sie ist transitiv genau dann, wenn p_x für irgendein $x\in X$ surjektiv ist; sie ist einfach transitiv dann und nur dann, wenn p_x für irgendein $x\in X$ bijektiv ist. □

Übung 1. Man gebe eine geometrische Interpretation der Translationen $l_a=r_a$ in der Gruppe V der Vektoren der Ebene (Beispiel 1.6).

Übung 2. Es sei $f: G\to G$ eine Abbildung von G in G, für die $f\circ l_a=l_a\circ f$ für alle a aus der Gruppe G gilt. Man beweise, daß f dann eine Rechtstranslation ist.

Übung 3. Mit Hilfe des Theorems von CAYLEY finde man eine Realisierung der zyklischen Gruppe der Ordnung n als eine Untergruppe der Gruppe S_n.

Übung 4. Man beweise, daß die Gruppe der Drehungen C (Beispiel 3.3) einfach transitiv auf einer Kreislinie mit dem Zentrum o wirkt und daß die Gruppe C_n einfach transitiv auf der Menge der Ecken eines regulären n-Ecks wirkt.

Übung 5. Man zeige, daß eine zyklische Untergruppe der Form $[(i_1\, i_2 \ldots i_n)]\subseteq S_n$ einfach transitiv auf N_n wirkt und daß die Kleinsche Vierergruppe V (Übung 3.8) einfach transitiv auf N_4 wirkt.

Übung 6. Man beweise Übung 2.6 mit Hilfe von Satz 4. (Hinweis. Man betrachte die Orbits $[s]\, i$ für $i\in N_n$; die Elemente der Orbits, genommen in der durch sukzessive Anwendung von s entstehenden zyklischen Anordnung, bilden die unabhängigen Zyklen. Gilt $[s]\, i=\{i\}$, so setze man $(i):=e\in S_n$.)

§ 5. Kategorien und Funktoren

In diesem Paragraphen wollen wir einige einfache, jedoch recht abstrakte Begriffe einführen, die in der modernen Mathematik häufig gebraucht werden. Wir benötigen dabei nur die Terminologie der Kategorien und Funktoren; für die eigentliche Theorie verweisen wir auf die Spezialliteratur, vgl. etwa H. SCHUBERT [1]. Der Leser kann diesen Paragraphen zunächst überspringen und später bei Bedarf auf ihn zurückkommen.

Definition 1. Eine *Kategorie* $[\mathcal{A}, \mathrm{Hom}, \circ]$ besteht aus einer Klasse $\mathcal{A}$ von Objekten $A, B, \ldots, X \in \mathcal{A}$, einer Zuordnung Hom, die jedem geordneten Paar $(X, Y) \in \mathcal{A} \times \mathcal{A}$ eine Menge $\mathrm{Hom}\,(X, Y)$ zuordnet, deren Elemente die *Morphismen* von X in Y heißen, und einer *Komposition* $\circ$ der Morphismen, wobei folgende Bedingungen erfüllt sind:

1. Ist $(X, Y) \neq (X_0, Y_0)$, so gilt $\mathrm{Hom}\,(X, Y) \cap \mathrm{Hom}\,(X_0, Y_0) = \emptyset$.
2. Für alle Tripel (X, Y, Z) von Objekten ist die Komposition $\circ$ eine Abbildung

$$(f, g) \in \mathrm{Hom}\,(X, Y) \times \mathrm{Hom}\,(Y, Z) \mapsto g \circ f \in \mathrm{Hom}\,(X, Z)\,.$$

3. Die Komposition ist assoziativ, d. h., für alle $f \in \mathrm{Hom}\,(X, Y)$, $g \in \mathrm{Hom}\,(Y, Z)$, $h \in \mathrm{Hom}\,(Z, U)$ gilt

$$h \circ (g \circ f) = (h \circ g) \circ f\,.$$

4. Zu jedem Objekt $X \in \mathcal{A}$ gibt es ein zugehöriges *Einselement* e_X, d. h. einen Morphismus $e_X \in \mathrm{Hom}\,(X, X)$, der für alle $Y \in \mathcal{A}$, $f \in \mathrm{Hom}\,(Y, X)$ und $g \in \mathrm{Hom}\,(X, Y)$ die Gleichungen

$$e_X \circ f = f, \qquad g \circ e_X = g$$

erfüllt.

Beispiel 1. Die Klasse $\mathcal{A} := \mathfrak{M}$ aller Mengen wird zu einer Kategorie, wenn wir als Morphismen $f \in \mathrm{Hom}\,(X, Y) := M(X, Y)$ die Abbildungen f von X in Y und als Komposition die Verknüpfung der Abbildungen definieren, vgl. Beispiel 0.2.4 und Definition 0.2.5. Die *Einselemente* sind dann die identischen Abbildungen $e_X = \mathrm{id}_X$. In diesem Sinne spricht man von der *Kategorie aller Mengen*.

Beispiel 2. Es sei $\mathcal{G}$ die Klasse aller Gruppen, $\mathrm{Hom}\,(X, Y)$ für $X, Y \in \mathcal{G}$ die Menge der Homomorphismen von X in Y und $\circ$ die Verknüpfung der Homomorphismen. Nach Satz 2.9 erhalten wir so eine Kategorie, die *Kategorie aller Gruppen*. Analog kann man von der *Kategorie aller Monoide* sprechen. Die Einselemente e_X sind wieder die identischen Abbildungen; man verwechsle sie nicht mit den Einselementen $e \in X$ der multiplikativ geschriebenen Gruppen $X \in \mathcal{G}$, die streng genommen ebenfalls alle unterschiedlich bezeichnet werden müßten. Man nennt eine Kategorie $\mathcal{B}$ eine *Unterkategorie* von $\mathcal{A}$, wenn die Objekte von $\mathcal{B}$ auch Objekte von $\mathcal{A}$ sind, für die Morphismenmengen $\mathrm{Hom}_{\mathcal{B}}(X, Y) \subseteq \mathrm{Hom}_{\mathcal{A}}(X, Y)$ für alle $(X, Y) \in \mathcal{B} \times \mathcal{B}$ gilt und die Komposition der Morphismen in $\mathcal{B}$ die Einschränkung der Komposition der Morphismen in $\mathcal{A}$ ist. Somit ist die Kategorie der Gruppen eine Unterkategorie der Kategorie der Monoide, und beide sind Unterkategorien der Kategorie der Mengen.

Definition 2. Es sei $\mathfrak{K}$ eine beliebige Kategorie. Ein Morphismus $f \in \mathrm{Hom}(X, Y)$ heißt ein *Isomorphismus*, wenn er ein *Inverses* $g \in \mathrm{Hom}(Y, X)$ besitzt, das ist ein Morphismus, der

$$g \circ f = e_X \quad \text{und} \quad f \circ g = e_Y$$

erfüllt. Ein Isomorphismus $f \in \mathrm{Hom}(X, X)$ heißt ein *Automorphismus*.

Man beweist leicht

Satz 1. *Zu jedem Objekt X einer Kategorie $\mathfrak{K}$ gibt es genau ein Einselement e_X; e_X ist ein Automorphismus. Zu jedem Isomorphismus f der Kategorie $\mathfrak{K}$ gibt es genau einen inversen Isomorphismus, den man mit f^{-1} bezeichnet. Für jedes Objekt $X \in \mathfrak{K}$ ist*

$$\mathrm{Aut}(X) := \{f \mid f \in \mathrm{Hom}(X, X), f \text{ Automorphismus}\}$$

bezüglich der Komposition $\circ$ eine Gruppe, die man die Automorphismengruppe von X nennt; ihr Einselement ist e_X. □

Zwei Objekte X, Y der Kategorie $\mathfrak{K}$ heißen *isomorph*, wenn ein Isomorphismus $f \in \mathrm{Hom}(X, Y)$ existiert. Genauso wie Satz 2.10 beweist man, daß *die Isomorphie eine Äquivalenzrelation in der Klasse der Objekte der Kategorie ist.* Unter dem Klassifikationsproblem versteht man die Aufgabe, die Isomorphieklassen dieser Äquivalenzrelation aufzuzählen und zu beschreiben. Für die Kategorie der Gruppen z. B. ist dieses Problem ungelöst. In der Kategorie der Mengen nennt man die Isomorphieklassen *Mächtigkeiten*, und statt von isomorphen Mengen spricht man von *gleichmächtigen*. Da zwei endliche Mengen genau dann gleichmächtig sind, wenn sie dieselbe Anzahl von Elementen besitzen, können wir die Mächtigkeiten als Verallgemeinerungen der natürlichen Zahlen ansehen (vgl. auch Beispiel 0.2.14).

Beispiel 3. Es bezeichne $\mathfrak{T}$ die Klasse aller Transformationsgruppen $[G, X, \varphi]$, vgl. Definition 4.1.3. Oft unterdrückt man die explizite Angabe der Wirkung φ; man beachte jedoch, daß es in der Regel sehr viele Wirkungen von G über X gibt und daß man sich stets eine bestimmte dieser Wirkungen vorzustellen hat, wenn man von einer Transformationsgruppe $[G, X]$ spricht. Man nennt (F, f) einen *äquivarianten Morphismus* der Transformationsgruppe $[G, X]$ in die Transformationsgruppe $[H, Y]$, wenn $F \in \mathrm{Hom}(G, H)$ ein Gruppenhomomorphismus, $f \in M(X, Y)$ eine Abbildung ist und für alle $g \in G$ das Diagramm

$$\begin{array}{ccc} X & \xrightarrow{t_g} & X \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ Y & \xrightarrow{t_{F(g)}} & Y \end{array} \tag{1}$$

kommutativ ist, d. h.

$$f(g \cdot x) = F(g) \cdot f(x) \tag{2}$$

gilt. Die Komposition zweier äquivarianter Morphismen

$$(F, f): [G, X] \to [H, Y] \quad \text{und} \quad (P, p): [H, Y] \to [L, Z]$$

wird durch die Verknüpfung der Abbildungen erklärt:

$$(P, p) \circ (F, f) := (P \circ F, p \circ f); \tag{3}$$

$(P, p) \circ (F, f)$ ist dann ein äquivarianter Morphismus von $[G, X]$ in $[L, Z]$. Das zu dem Objekt $[G, X]$ gehörende Einselement ist $(\mathrm{id}_G, \mathrm{id}_X)$, und die Komposition (3) ist assoziativ. Folglich können wir von der *Kategorie $\mathfrak{T}$ der Transformationsgruppen* sprechen. Insbesondere ist der Begriff der Isomorphie für Transformationsgruppen definiert.

Übung 1. Man beweise: Ein äquivarianter Morphismus $(F, f): [G, X] \to [H, Y]$ der Kategorie $\mathfrak{T}$ ist ein Isomorphismus dann und nur dann, wenn F und f bijektiv sind, und es gilt

$$(F, f)^{-1} = (F^{-1}, f^{-1}). \tag{4}$$

Beispiel 4. Es sei G eine bestimmte Gruppe. Wir definieren die *Unterkategorie $\mathfrak{T}(G)$ von $\mathfrak{T}$* als die Klasse aller Transformationsgruppen der Form $[G, X]$; als Morphismen werden nur die äquivarianten Morphismen der Gestalt (id_G, f) der Kategorie $\mathfrak{T}$ angesehen. Ein derartiger Morphismus ist also allein durch Angabe der Abbildung $f: X \to Y$ bestimmt, welche wegen (2) die Bedingung

$$f(g \cdot x) = g \cdot f(x) \qquad (g \in G, x \in X) \tag{5}$$

erfüllen muß; derartige Abbildungen nennt man *G-Abbildungen* oder *G-Invarianten*.

Übung 2. Die Wirkungen einer Gruppe G auf sich mit Hilfe der Linkstranslationen l_a und mit Hilfe der Rechtstranslationen $r_{a^{-1}}$ (vgl. die Beispiele 4.3 und 4.4) definieren zwei Objekte der Kategorie $\mathfrak{T}(G)$. Man beweise, daß diese Objekte isomorph sind.

Man macht sich leicht klar, daß man die Kategorien als eine Verallgemeinerung der Halbgruppen $[H, \circ]$ mit Einselement betrachten kann (vgl. die Definitionen 1.2, 1.3). In jeder Kategorie $\mathfrak{A}$ ist nämlich für alle $X \in \mathfrak{A}$ die Morphismenmenge $\mathrm{Hom}(X, X)$ mit der Operation $\circ$ eine Halbgruppe mit Einselement e_X. Daher können wir eine Halbgruppe H als eine Kategorie betrachten, deren Objektklasse nur ein einziges Element X enthält, für das $H = \mathrm{Hom}(X, X)$ gilt (vgl. auch Übung 5). Es ist deshalb nicht verwunderlich, daß man auch für Kategorien selbst „Homomorphismen" hat, die man hier, um sie nicht mit den Morphismen der Kategorien zu verwechseln, Funktoren nennt:

Definition 3. Unter einem *kovarianten* (bzw. *kontravarianten*) *Funktor* $T: \mathfrak{A} \to \mathfrak{B}$ der Kategorie $\mathfrak{A}$ in die Kategorie $\mathfrak{B}$ versteht man eine Zuordnung, die jedem Objekt $X \in \mathfrak{A}$ ein Objekt $T(X) \in \mathfrak{B}$ und jedem Morphismus $f \in \mathrm{Hom}_{\mathfrak{A}}(X, Y)$ einen Morphismus $Tf \in \mathrm{Hom}_{\mathfrak{B}}(T(X), T(Y))$ (bzw. $Tf \in \mathrm{Hom}_{\mathfrak{B}}(T(Y), T(X))$) zuordnet, so daß

$$T(e_X) = e_{T(X)} \tag{6}$$

und

$$T(g \circ f) = T(g) \circ T(f) \tag{7}$$

(bzw.

$$T(g \circ f) = T(f) \circ T(g)) \tag{8}$$

für alle $f \in \mathrm{Hom}_{\mathfrak{A}}(X, Y)$, $g \in \mathrm{Hom}_{\mathfrak{A}}(Y, Z)$, $X, Y, Z \in \mathfrak{A}$, erfüllt sind.

Beispiel 5. Ordnen wir jeder Transformationsgruppe $[G, X] \in \mathfrak{T}$ die Gruppe $H_1(G, X) := G$ und jedem äquivarianten Morphismus (F, f) der Kategorie $\mathfrak{T}$ den Homomorphismus $H_1(F, f) := F$ zu, so erhalten wir einen kovarianten Funktor $H_1: \mathfrak{T} \to \mathfrak{G}$. Analog können wir durch $H_2(G, X) := X$ und $H_2(F, f) := f$ einen kovarianten Funktor $H_2: \mathfrak{T} \to \mathfrak{M}$ von $\mathfrak{T}$ in die Kategorie der Mengen definieren.

Beispiel 6. Es sei G irgendeine (z. B. multiplikativ geschriebene) Gruppe. Nach Beispiel 1.8 und Übung 1.1 wird dann durch $G^X := [M(X, G), \cdot]$ jeder nichtleeren Menge $X \in \mathfrak{M}$ eine Gruppe, die Gruppe der Abbildungen von X in G, zugeordnet. Bezeichnet $e \in G$ das Einselement von G und setzen wir $G^\emptyset := \{e\}$, so erhalten wir eine Zuordnung $F_G^*: X \in \mathfrak{M} \mapsto G^X \in \mathfrak{G}$ der Klasse der Mengen in die Klasse der Gruppen. Es sei nun $\varphi \in M(X, Y)$. Wir definieren einen Gruppenhomomorphismus $F_G(\varphi): G^Y \to G^X$ durch

$$F_G(\varphi): f \in G^Y \mapsto f^\varphi := f \circ \varphi \in G^X. \tag{9}$$

Man beweist leicht, daß die Abbildung (9) wirklich ein Gruppenhomomorphismus ist, daß

$$F_G(\mathrm{id}_X) = \mathrm{id}_{F_G(X)} \tag{10}$$

gilt und daß $F_G: \mathfrak{M} \to \mathfrak{G}$ ein kontravarianter Funktor ist: Aus der Beziehung $f^{\psi \circ \varphi} = f \circ (\psi \circ \varphi) = (f \circ \psi) \circ \varphi$ folgt ja sofort

$$F_G(\psi \circ \varphi) = F_G(\varphi) \circ F_G(\psi)\,. \tag{11}$$

Zur Veranschaulichung stellen wir noch die entsprechenden Diagramme gegenüber, wobei wir zur Abkürzung $\varphi' := F_G(\varphi)$ setzen:

Beispiel 7. Wir behalten die Bezeichnungen von Beispiel 6 bei, betrachten nun aber X als fest und $G \in \mathfrak{G}$ als variabel. Setzen wir für $\theta \in \mathrm{Hom}\,(G, H)$

$$\theta_*: f \in G^X \mapsto \theta_* f := \theta \circ f \in H^X,$$

so zeigt folgende einfache Rechnung, daß $\theta_* \in \mathrm{Hom}\,(G^X, H^X)$ gilt:

$$\begin{aligned}\theta_*(f \cdot g)(x) &= \theta \circ (f \cdot g)(x) = \theta(f(x) \cdot g(x)) = \theta(f(x)) \cdot \theta(g(x)) \\ &= \theta_* f(x) \cdot \theta_* g(x) = (\theta_* f \cdot \theta_* g)(x)\,.\end{aligned}$$

Man beweist leicht, daß die Zuordnung

$$G \in \mathfrak{G} \mapsto G^X \in \mathfrak{G}, \qquad \theta \in \mathrm{Hom}\,(G, H) \mapsto \theta_* \in \mathrm{Hom}\,(G^X, H^X)\,,$$

einen kovarianten Funktor der Kategorie $\mathfrak{G}$ in sich definiert.

Die Beispiele 6 und 7 kann man zusammenfassen, indem man sagt, daß $(G, X) \in \mathfrak{G} \times \mathfrak{M} \mapsto G^X \in \mathfrak{G}$, $\theta \mapsto \theta_*$, $\varphi \mapsto \varphi'$, ein *Bifunktor* sei, der im ersten Argument

kovariant und im zweiten Argument kontravariant ist. Analog kann man *Multifunktoren* von endlich vielen Argumenten betrachten.

Übung 3. Man beweise: Ordnet man jeder Menge X ihre Potenzmenge $\mathfrak{P}(X)$ und jeder Abbildung $f \in M(X, Y)$ ihre ebenso bezeichnete Ausdehnung $f \in M(\mathfrak{P}(X), \mathfrak{P}(Y))$ (vgl. (0.2.24)) zu, so entsteht ein kovarianter Funktor von $\mathfrak{M}$ in $\mathfrak{M}$. Analog definiert die Zuordnung

$$X \in \mathfrak{M} \mapsto \mathfrak{P}(X) \in \mathfrak{M}, \qquad f \in M(X, Y) \mapsto f^{-1} \in M(\mathfrak{P}(Y), \mathfrak{P}(X)),$$

nach (0.2.25) einen kontravarianten Funktor von $\mathfrak{M}$ in sich.

Übung 4. Man beweise, daß die folgenden Zuordnungen τ kovariante Funktoren der Kategorie $\mathfrak{C}$ in die Kategorie $\mathfrak{S}$ sind: Für jede Gruppe G bezeichne $\tau(G)$ die Transformationsgruppe $[G, G]$, für die die Wirkung von G entweder über die Linkstranslationen oder die Rechtstranslationen oder über die inneren Automorphismen von G definiert ist (vgl. die Beispiele 4.3 bis 4.5); für jeden Homomorphismus $\varphi \in \mathrm{Hom}(G, H)$ wird $\tau(\varphi)$ durch $\tau(\varphi) := (\varphi, \varphi)$ definiert.

Übung 5. Es sei $\mathfrak{M}$ eine Klasse mit einer Operation $f \circ g$, die nicht notwendig für alle Paare $f, g \in \mathfrak{M}$ definiert zu sein braucht. Eine derartige Operation $\circ$ heißt *assoziativ*, wenn für beliebige $f, g, h \in \mathfrak{M}$ folgende Bedingung erfüllt ist: Sind $f \circ g$ und $g \circ h$ oder $f \circ g$ und $(f \circ g) \circ h$ oder $g \circ h$ und $f \circ (g \circ h)$ definiert, so sind auch die übrigen zwei der vier Produkte $f \circ g$, $g \circ h$, $(f \circ g) \circ h$ und $f \circ (g \circ h)$ definiert, und es gilt $(f \circ g) \circ h = f \circ (g \circ h)$. Ein Element $e \in \mathfrak{M}$ heißt eine *Einheit*, wenn $e \circ f = f$ und $g \circ e = g$ für alle diejenigen $f, g \in \mathfrak{M}$ gelten, für die $e \circ f$ und $g \circ e$ definiert sind. Es bezeichne $\mathfrak{E}$ die Klasse aller Einheiten von $\mathfrak{M}$. Ein Element $f \in \mathfrak{M}$ heißt *invertierbar*, wenn ein $g \in \mathfrak{M}$ existiert, für das $f \circ g \in \mathfrak{E}$ und $g \circ f \in \mathfrak{E}$ gilt. — a) Für eine beliebige Kategorie $[\mathfrak{A}, \mathrm{Hom}, \circ]$ betrachten wir die Klasse $\mathfrak{M} := \bigcup_{X, Y \in \mathfrak{A}} \mathrm{Hom}(X, Y)$ aller Morphismen der Kategorie mit der Operation $\circ$. Man beweise, daß $\circ$ eine assoziative Operation ist, daß $\mathfrak{E} = \{e_X\}_{X \in \mathfrak{A}}$ gilt und daß ein $f \in \mathfrak{M}$ dann und nur dann invertierbar ist, wenn f ein Isomorphismus ist. — b) Es sei umgekehrt $\mathfrak{M}$ eine Klasse mit einer nicht notwendig überall definierten Operation $\circ$, welche die folgenden Eigenschaften besitzen möge: 1. die Operation $\circ$ ist assoziativ; 2. für jedes $f \in \mathfrak{M}$ existieren Einheiten $e, e' \in \mathfrak{E}$, so daß $e \circ f$ und $f \circ e'$ definiert (und gleich f) sind; 3. für beliebige $e, e' \in \mathfrak{E}$ ist die Klasse $\mathrm{Mor}(e, e')$ aller derjenigen $f \in \mathfrak{M}$, für die $e' \circ f$ und $f \circ e$ definiert sind, eine Menge. Man beweise, daß $[\mathfrak{E}, \mathrm{Mor}, \circ]$ eine Kategorie ist. Falls die Operation $\circ$ für alle $f, g \in \mathfrak{M}$ definiert ist, ist $[\mathfrak{M}, \circ]$ eine Halbgruppe mit Einselement.

Nach Übung 5 können die Kategorien also auch als Klassen definiert werden, in denen eine nicht notwendig überall definierte algebraische Operation gegeben ist, welche die Eigenschaften 1 bis 3 besitzt. In dieser Sprache sind die kovarianten (bzw. kontravarianten) Funktoren dann Zuordnungen τ zwischen Klassen, welche Einheiten in Einheiten überführen und die Bedingung $\tau(f \circ g) = \tau(f) \circ \tau(g)$ (bzw. $\tau(f \circ g) = \tau(g) \circ \tau(f)$) erfüllen. Abschließend sei bemerkt, daß eine Kategorie, in der alle Morphismen invertierbar, d. h. Isomorphismen sind, ein *Gruppoid* heißt. Ist $[\mathfrak{A}, \mathrm{Hom}, \circ]$ eine beliebige Kategorie und bezeichnen wir mit $\mathrm{Iso}(X, Y) \subseteq \mathrm{Hom}(X, Y)$ die Menge aller Isomorphismen $f: X \to Y$, so ist $[\mathfrak{A}, \mathrm{Iso}, \circ]$ eine Unterkategorie, die sogar ein Gruppoid ist. Da in einem Gruppoid alle Morphismen invertierbar sind, können wir die Gruppoide als Verallgemeinerungen der Gruppen betrachten.

2. Ringe und Körper

Im ersten Kapitel betrachteten wir Monoide, das sind Mengen mit *einer* Operation. Dieses Kapitel ist eine Einführung in die Theorie der Ringe und Körper, das sind Mengen, in denen zwei algebraische Operationen mit gewissen Eigenschaften gegeben sind. Der Begriff eines Ringes ist komplizierter als der einer Gruppe; jedoch wird er vielen Lesern eher vertraut sein, da er eine direkte Verallgemeinerung der Bereiche der ganzen, der rationalen und der reellen Zahlen mit den beiden Operationen der Addition und der Multiplikation ist. Ein anderes wichtiges Beispiel ist der Ring der Polynome. Die Untersuchung dieses Ringes hängt eng mit der Aufgabe, die Lösungen algebraischer Gleichungen zu bestimmen, zusammen, die eine der Quellen für die Entstehung der modernen Algebra darstellt. Wir werden speziell die Frage nach der Anzahl und der Lage der reellen Nullstellen eines Polynoms mit reellen Koeffizienten behandeln und das Kapitel mit einer Methode zur Lösung linearer Gleichungssysteme abschließen.

§ 1. Definition und einfachste Eigenschaften der Ringe

Definition 1. Ein Tripel $[A, +, \cdot]$ einer Menge A mit zwei algebraischen Operationen, der Addition $+$ und der Multiplikation $\cdot$, heißt ein *Ring*, wenn folgende Bedingungen erfüllt sind:

1. $[A, +]$ ist eine abelsche Gruppe;
2. es gelten die *Distributivgesetze*

$$a(b+c) = ab + ac, \qquad (b+c)a = ba + ca \qquad (a, b, c \in A).$$

Die Gruppe $[A, +]$ heißt die *additive Gruppe* des Ringes, ihre Null heißt die Null des Ringes. Für die additive Gruppe gelten natürlich alle Definitionen und Sätze der Theorie der abelschen Gruppen; speziell ist in jedem Ring die Operation der Subtraktion erklärt: $a - b = a + (-b)$ (vgl. § 1.1).

Ein Ring $[A, +, \cdot]$ heißt *assoziativ*, wenn die Multiplikation assoziativ, d. h. $[A, \cdot]$ eine Halbgruppe ist, und *kommutativ*, wenn die Multiplikation kommutativ ist. Wenn in $[A, \cdot]$ ein Einselement e existiert, sprechen wir von einem *Ring mit*

Einselement; die Menge der invertierbaren Elemente von $[A, \cdot]$ wird mit A^* bezeichnet; wir nennen ihre Elemente die *invertierbaren Elemente des Ringes.*

Wir wollen nun einige einfache Eigenschaften der Ringe beweisen, die unmittelbar aus den Definitionen folgen. Zunächst bemerken wir, daß $[A^*, \cdot]$ für einen assoziativen Ring A mit Einselement eine Gruppe ist (vgl. Beispiel 1.1.10), welche die *multiplikative Gruppe* des Ringes A heißt.

Definiert man die Links- und Rechtstranslationen in einem Ring analog zu (1.4.4) bzw. (1.4.5) im Fall einer Gruppe

$$l_a(x) = ax, \qquad r_a(x) = xa \qquad (x \in A),$$

so können wir die Distributivgesetze auch folgendermaßen schreiben:

$$l_a(b+c) = l_a(b) + l_a(c), \qquad r_a(b+c) = r_a(b) + r_a(c) \qquad (a, b, c \in A);$$

sie drücken also aus, daß l_a und r_a Endomorphismen der additiven Gruppe des Ringes A sind.

Satz 1. *In einem beliebigen Ring A gelten die Beziehungen*

$$\left.\begin{aligned} &a0 = 0a = 0, \\ &a(-b) = (-a)\,b = -ab, \\ &a(b-c) = ab - ac, \\ &(b-c)\,a = ba - ca \end{aligned}\right\} \qquad (a, b, c \in A).$$

Beweis. Man wende Satz 1.2.11 auf die Endomorphismen l_a, r_a der additiven Gruppe A an. □

Satz 2. *Ist A ein Ring mit Einselement e, $A \neq \{0\}$, so gilt $0 \notin A^*$.*

Beweis. Angenommen, die Behauptung sei falsch. Dann würde sich aus Satz 1 die Identität $e = 0 \cdot 0^{-1} = 0$ ergeben. Multiplizieren wir diese Gleichung von rechts mit einem beliebigen $a \in A$, so folgt $a = ea = 0 \cdot a = 0$, was der Voraussetzung $A \neq \{0\}$ widerspricht. □

Übung 1. Für einen beliebigen Ring A beweise man

$$(ma)(nb) = (mn)(ab) \qquad (m, n \in \mathbf{Z};\ a, b \in A).$$

Beispiel 1. Die Mengen $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ mit den üblichen Operationen der Addition und Multiplikation sind kommutative, assoziative Ringe mit Einselement. Die additiven und multiplikativen Gruppen dieser Ringe betrachteten wir schon in § 1.1. Speziell gilt $\mathbf{Z}^* = \{1, -1\}$.

Beispiel 2. Es sei $M(X, \mathbf{R})$ die Menge der auf einem Intervall $X \subseteq \mathbf{R}$ definierten reellwertigen Funktionen. Dann wird $M(X, \mathbf{R})$ bei punktweiser Definition der Addition und Multiplikation (vgl. Beispiel 1.1.8) ein kommutativer, assoziativer Ring mit dem Einselement e: $e(x) = 1$ $(x \in X)$. Dieses Beispiel läßt sich leicht verallgemeinern: Ist A ein Ring und X eine nichtleere Menge, so wird die Menge $M(X, A)$ aller Abbildungen $X \to A$ bei punktweiser Definition der Addition und der Multiplikation zu einem Ring.

Beispiel 3. Es sei $[G,+]$ eine abelsche Gruppe und End G die Gruppe ihrer Endomorphismen (vgl. Übung 1.2.12). Nach Satz 1.2.9 ist in End G eine Operation $\circ$, die Verknüpfung der Endomorphismen, definiert. Nehmen wir diese als Multiplikation, so wird End G ein assoziativer Ring mit Einselement, der sogenannte *Endomorphismenring* der abelschen Gruppe G. Zum Beweis braucht man nur die Distributivgesetze zu überprüfen. Wir beweisen z. B.

$$f\circ(g+h)=f\circ g+f\circ h \qquad (f,g,h\in \mathrm{End}\, G)\,.$$

Für beliebiges $x\in G$ gilt

$$\begin{aligned}(f\circ(g+h))\,(x)&=f(g(x)+h(x))=f(g(x))+f(h(x))\\&=(f\circ g)\,(x)+(f\circ h)\,(x)=(f\circ g+f\circ h)\,(x)\,.\end{aligned}$$

Beispiel 4. Es sei X irgendeine Menge und $\mathfrak{P}(X)$ die Menge ihrer Teilmengen. In $\mathfrak{P}(X)$ betrachten wir die Operation der *symmetrischen Differenz*

$$Y\triangle Z=(Y\setminus Z)\cup(Z\setminus Y) \qquad (Y,Z\in\mathfrak{P}(X))$$

als „Addition" und die Durchschnittsbildung $Y\cap Z$ als „Multiplikation". Mit diesen Operationen wird $\mathfrak{P}(X)$ ein kommutativer, assoziativer Ring mit Einselement. $X\in\mathfrak{P}(X)$ ist das Einselement und die leere Menge $\emptyset\in\mathfrak{P}(X)$ die Null des Ringes. Man beachte, daß $[\mathfrak{P}(X),\cup,\cap]$ für $|X|\neq 0,1$ kein Ring ist, obwohl sogar zwei Distributivgesetze gelten, vgl. (0.2.16), (0.2.17).

Definition 2. Es sei A ein beliebiger Ring. Ein Element $a\in A$ heißt ein *linker* (bzw. *rechter*) *Nullteiler*, wenn $a\neq 0$ gilt und ein $b\in A$, $b\neq 0$, existiert, so daß $a\cdot b=0$ (bzw. $b\cdot a=0$) ist. Ein Ring A heißt *nullteilerfrei*, wenn in A weder rechte noch linke Nullteiler existieren.

Die Ringe $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ sind nullteilerfrei; der Ring $M(X,\mathbf{R})$ aus Beispiel 2 besitzt offenbar Nullteiler, wenn X mehr als ein Element enthält.

Offenbar ist ein Ring nullteilerfrei, wenn er keine rechten oder keine linken Nullteiler enthält. Aus Definition 2 ist ersichtlich, daß ein Element $a\in A$ genau dann linker (bzw. rechter) Nullteiler ist, wenn der Endomorphismus l_a (bzw. r_a) der Gruppe $[A,+]$ einen von Null verschiedenen Kern hat. Nach Satz 1.2.13 ist also a genau dann nicht linker (bzw. rechter) Nullteiler, wenn l_a (bzw. r_a) injektiv ist. Hieraus folgt unmittelbar

Satz 3. *In einem nullteilerfreien Ring A gilt die folgende Kürzungsregel: Aus $ab_1=ab_2$ (oder $b_1a=b_2a$) und $a\neq 0$, $a,b_1,b_2\in A$, folgt $b_1=b_2$.* □

Es sei nun A ein assoziativer Ring mit Einselement. Wir erwähnten bereits, daß in diesem Fall $[A^*,\cdot]$ eine Gruppe ist. Durch die Multiplikation in A ist eine Abbildung $(u,a)\in A^*\times A\mapsto ua\in A$ definiert, die eine Wirkung von A^* über A ist. Die dieser Wirkung entsprechenden Transformationen t_u $(u\in A^*)$ sind die Linkstranslationen l_u. Analog läßt sich eine Wirkung der Gruppe A^* über A mit Hilfe der Rechtstranslationen definieren.

Definition 3. Die Elemente a, b eines Ringes A mit Einselement heißen *assoziiert* – wir schreiben hierfür $a \sim b -$, wenn ein Element $u \in A^*$ existiert, so daß $b = ua$ gilt.

Satz 4. *In einem assoziativen Ring mit Einselement ist die Assoziiertheit $\sim$ eine Äquivalenzrelation. Die Äquivalenzklasse des Einselementes e ist gleich A^*. Die Elemente $u \in A^*$ sind weder rechte noch linke Nullteiler.*

Beweis. Die Assoziiertheit ist gerade die durch die Wirkung von A^* über A mit Hilfe der Linkstranslationen erzeugte Äquivalenzrelation (vgl. Satz 1.4.4). Offenbar gilt $a \sim e$ genau dann, wenn $a \in A^*$ ist. Da für $a \in A^*$ die l_a und r_a als Transformationen der entsprechenden Wirkungen bijektiv sind, kann a weder rechter noch linker Nullteiler sein. □

Für den Ring der ganzen Zahlen $\mathbf{Z}$ beispielsweise ist $\mathbf{Z}^* = \{1, -1\}$, so daß in $\mathbf{Z}$ die Beziehung $a \sim b$ genau dann gilt, wenn $b = \pm a$ ist.

Natürlich definiert auch die Wirkung r_a, $a \in A^*$, mit Hilfe der Rechtstranslationen eine Äquivalenzrelation über A. Wenn A ein kommutativer Ring ist, stimmen beide Relationen überein, und mit diesem Fall werden wir uns im folgenden hauptsächlich beschäftigen.

Definition 4. Eine Teilmenge B des Ringes A heißt ein *Unterring*, wenn B bezüglich der Einschränkung der über A definierten Operationen ein Ring ist.

Man erkennt leicht (vgl. Satz 1.2.1), daß *eine Teilmenge $B \subseteq A$ ein Unterring ist genau dann, wenn die folgenden Bedingungen erfüllt sind*:

1. *$[B, +]$ ist eine Untergruppe der additiven Gruppe $[A, +]$;*
2. *für beliebige $a, b \in B$ gilt $a \cdot b \in B$.*

Zum Beispiel ist $\mathbf{Z}$ Unterring von $\mathbf{Q}$ und von $\mathbf{R}$, und $\mathbf{Q}$ ist Unterring von $\mathbf{R}$.

Offenbar ist jeder Unterring eines nullteilerfreien Ringes ebenfalls nullteilerfrei.

Definition 5. Es seien A, B Ringe. Eine Abbildung $f: A \to B$ heißt ein *Ringhomomorphismus*, wenn f gleichzeitig Homomorphismus der additiven Gruppen $[A, +] \to [B, +]$ und der multiplikativen Monoide $[A, \cdot] \to [B, \cdot]$ ist, d. h., wenn folgende Bedingungen erfüllt sind:

$$\left.\begin{array}{l} 1.\ f(a+b) = f(a) + f(b), \\ 2.\ f(a \cdot b) = f(a) \cdot f(b) \end{array}\right\} \quad (a, b \in A) .$$

Aus Satz 1.2.9 folgt leicht

Satz 5. *Sind $f: A \to B$ und $g: B \to C$ Ringhomomorphismen, so ist auch $g \circ f: A \to C$ ein Ringhomomorphismus. Ist der Ringhomomorphismus $f: A \to B$ umkehrbar, so ist auch $f^{-1}: B \to A$ ein Ringhomomorphismus.* □

Definition 6. Ein bijektiver (d. h. umkehrbarer) Ringhomomorphismus $f: A \to B$ heißt ein *Isomorphismus*. Wenn ein derartiger Isomorphismus existiert, heißen die Ringe A und B *isomorph*, in Zeichen: $A \cong B$. Die Homomorphismen $f: A \to A$ heißen auch *Endomorphismen*, und die Isomorphismen von A auf sich werden *Automorphismen* genannt.

Ist $f: A \to B$ ein Isomorphismus, so ist auch $f^{-1}: B \to A$ ein Isomorphismus. Die Relation $\cong$ ist eine Äquivalenzrelation in der Klasse aller Ringe (vgl. Satz 1.2.10). Man beweist leicht, daß die Klasse aller Ringe mit den Ringhomomorphismen als Morphismen und deren Verknüpfung $\circ$ als Komposition eine Kategorie bildet, vgl. Satz 1.5.1 und die darauf folgenden Bemerkungen.

Beispiel 5. Es sei A ein Ring mit Einselement e. Dann ist die Abbildung $\varphi: k \in \mathbf{Z} \mapsto ke \in A$ ein Ringhomomorphismus (vgl. Übung 1 und Satz 1.3.1).

Übung 2. Man finde Isomorphismen, die a) $\mathrm{End}([\mathbf{Z}, +]) \cong \mathbf{Z}$ und b) $\mathrm{End}\, S_2 \cong \mathfrak{P}(\{x\})$ beweisen.

Übung 3. Man zeige: Ist f ein Ringhomomorphismus von $\mathbf{R}$ in sich, so ist entweder $f(x) = 0$ für alle $x \in \mathbf{R}$ oder $f = \mathrm{id}_{\mathbf{R}}$.

Definition 7. Unter dem *Kern* des Ringhomomorphismus $f: A \to B$ versteht man den Kern $\mathrm{Ker}\, f = f^{-1}(0)$ des entsprechenden Homomorphismus der additiven Gruppen.

Satz 6. *Es sei $f: A \to B$ ein Ringhomomorphismus. Dann sind das Bild* $\mathrm{Im}\, f = f(A) \subseteq B$ *und der Kern* $\mathrm{Ker}\, f \subseteq A$ *Unterringe.*

Beweis. Nach Satz 1.2.12 sind $\mathrm{Im}\, f$ und $\mathrm{Ker}\, f$ Untergruppen der entsprechenden additiven Gruppen. Sind $x, y \in \mathrm{Im}\, f$, so gilt $x = f(a)$, $y = f(b)$ für gewisse $a, b \in A$. Also ist auch $x \cdot y = f(a)\, f(b) = f(a \cdot b) \in \mathrm{Im}\, f$. Sind ferner $a, b \in \mathrm{Ker}\, f$, so gilt nach Satz 1

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

d. h. $a \cdot b \in \mathrm{Ker}\, f$. □

Folgerung 1. *Ist* $\mathrm{Ker}\, f = 0$, *so ist f ein Isomorphismus des Ringes A auf den Ring* $\mathrm{Im}\, f$. *Ein Ringhomomorphismus $f: A \to B$ ist ein Isomorphismus dann und nur dann, wenn* $\mathrm{Ker}\, f = 0$ *und* $\mathrm{Im}\, f = B$ *gilt.* □

Übung 4. Es sei A ein Ring mit Einselement e und $f: A \to B$ ein Ringhomomorphismus. Dann ist $f(e)$ Einselement des Ringes B, wenn eine der beiden Bedingungen erfüllt ist: 1. $\mathrm{Im}\, f = B$ oder 2. $\mathrm{Im}\, f \neq \{0\}$, B ist nullteilerfrei und besitzt ein Einselement.

Definition 8. Es sei A ein Ring mit Einselement e. Ist die Ordnung $O(e)$ von e in der additiven Gruppe $[A, +]$ unendlich, so sagen wir, A habe die *Charakteristik* 0, und schreiben $\mathrm{char}\, A = 0$; ist $O(e)$ endlich, so definieren wir $\mathrm{char}\, A := O(e)$.

Satz 8. *Ist A ein nullteilerfreier Ring mit Einselement, so ist* $\mathrm{char}\, A = 0$, *oder* $\mathrm{char}\, A$ *ist eine Primzahl.*

Beweis. Ist $m = \mathrm{char}\, A \neq 0$ und $m = O(e)$ keine Primzahl, so gibt es eine echte Zerlegung $m = r \cdot s$ mit $1 < r < m$, $1 < s < m$, und nach Übung 1 gilt $(re)\,(se) = (rs)\,(ee) = me = 0$. Andererseits ist $re \neq 0$, $se \neq 0$, und wir erhielten Nullteiler im Widerspruch zur Voraussetzung. □

Beispiel 6. Offenbar gilt $\mathrm{char}\, \mathbf{Z} = \mathrm{char}\, \mathbf{Q} = \mathrm{char}\, \mathbf{R} = 0$. Für den Ring $\mathfrak{P}(X)$ aus Beispiel 4 gilt $\mathrm{char}\, \mathfrak{P}(X) = 2$. In § 2 werden wir Beispiele für Ringe mit beliebiger Charakteristik angeben.

Übung 5. Es sei A ein nullteilerfreier Ring mit Einselement. Man beweise, daß alle von Null verschiedenen Elemente dieselbe Ordnung (in der additiven Gruppe $[A, +]$) haben.

Übung 6. Man beweise, daß jeder Ring A mit char $A = 0$ einen zum Ring der ganzen Zahlen $\mathbf{Z}$ isomorphen Unterring enthält.

§ 2. Körper, Schiefkörper, Integritätsbereiche

In diesem Paragraphen wollen wir zunächst bestimmte Klassen von Ringen untersuchen, in denen eine zur Multiplikation inverse Operation, die Division, existiert.

Definition 1. Ein Ring K heißt ein *Schiefkörper*, wenn folgende Bedingungen erfüllt sind:

1. $K \neq \{0\}$;
2. K ist ein assoziativer Ring mit Einselement;
3. $K^* = K \setminus \{0\}$.

Wenn außerdem die Bedingung

4. K kommutativ

erfüllt ist, heißt K ein *Körper*.

Ist K ein Körper, so ist die multiplikative Gruppe $K^* = K \setminus \{0\}$ abelsch. Nach Satz 1.4 ist jeder Schiefkörper nullteilerfrei. In einem Körper ist die Operation der Division $(b, a) \in K \times K^* \to b/a \in K$ für Elemente $a \neq 0$ definiert (vgl. (1.1.5)).

Beispiel 1. Die Ringe $\mathbf{Q}$, $\mathbf{R}$ sind Körper. Der Ring $\mathbf{Z}$ ist kein Körper, da Bedingung 3 nicht erfüllt ist.

Beispiel 2. Der Ring $\mathfrak{P}(\{x\})$ der Teilmengen einer einelementigen Menge $\{x\}$ ist ein Körper, der nur die beiden Elemente $0 = \emptyset$ und $e = \{x\}$ enthält (Beispiel 1.4). Wenn X wenigstens zwei Elemente enthält, hat $\mathfrak{P}(X)$ Nullteiler und ist daher kein Schiefkörper.

Als Beispiel für einen nichtkommutativen Schiefkörper werden wir im nächsten Paragraphen die Quaternionen kennenlernen. Es sei bemerkt, daß außerhalb der §§ 2.1, 2.2 der Begriff des Schiefkörpers in dieser Einführung nur in den Übungen gelegentlich benötigt wird.

Definition 2. Eine Teilmenge L des Körpers K heißt ein *Teilkörper*, wenn L bezüglich der Einschränkungen der über K definierten algebraischen Operationen ein Körper ist. In diesem Fall sagt man auch, daß K eine *Erweiterung* von L ist (analog für Schiefkörper).

Zum Beispiel ist der Körper $\mathbf{R}$ der reellen Zahlen eine Erweiterung des Körpers $\mathbf{Q}$ der rationalen Zahlen.

Satz 1. *Eine Teilmenge $L \subseteq K$ ist ein Teilkörper dann und nur dann, wenn die folgenden Bedingungen erfüllt sind:*

1. *L ist ein Unterring von K;*
2. $L \neq \{0\}$;
3. *gilt $a \in L$ und $a \neq 0$, so ist auch $a^{-1} \in L$.*

Beweis. Die Notwendigkeit der Bedingungen ist klar. Es möge umgekehrt L die Bedingungen 1 bis 3 erfüllen. Dann ist L ein assoziativer und kommutativer Ring, und es gibt ein $a \in L$, $a \neq 0$. Nach Bedingung 3 ist auch $a^{-1} \in L$, und weil L ein Unterring ist, enthält er die Einheit $e = a \cdot a^{-1}$. Nach Bedingung 3 ist $L^* = L \setminus \{0\}$, d. h., L ist ein Körper. □

Wir wollen nun Homomorphismen eines Körpers untersuchen. Für sie gilt der folgende Satz, dessen Aussage man mit dem in Übung 8 beschriebenen Beispiel vergleichen möge:

Satz 2. *Es sei K ein Körper, B ein Ring und $f: K \to B$ ein Ringhomomorphismus. Dann ist entweder* $\operatorname{Im} f = \{0\}$, *oder f ist injektiv und bildet K isomorph auf den Unterring* $\operatorname{Im} f \subseteq B$ *ab, der ein Körper ist.*

Beweis. Angenommen, es ist $\operatorname{Im} f \neq \{0\}$. Dann existiert ein $a \in K$ mit $f(a) \neq 0$. Wir behaupten, daß in diesem Fall $\operatorname{Ker} f = \{0\}$ gilt. Wäre nämlich $b \in \operatorname{Ker} f$, $b \neq 0$, so folgt aus $a = b \cdot (a/b)$ nach Satz 1.1 $f(a) = f(b) \cdot f(a/b) = 0$ im Widerspruch zu $f(a) \neq 0$. Aus $\operatorname{Ker} f = \{0\}$ erhalten wir nach Folgerung 1.1, daß f den Körper K isomorph auf den Unterring $\operatorname{Im} f$ abbildet. Aber offensichtlich ist jeder Ring, der einem Körper isomorph ist, selbst ein Körper. □

Wie bereits bemerkt wurde, ist in einem Körper die Division durch von 0 verschiedene Elemente stets ausführbar. In einem beliebigen Ring dagegen hat man stattdessen nur den Begriff der Teilbarkeit. Um nicht rechte und linke Teilbarkeit unterscheiden zu müssen, wollen wir jetzt voraussetzen, daß der Ring kommutativ sei.

Definition 4. Es sei A ein kommutativer Ring und $a, b \in A$. Man sagt, *a teile b*, oder *b ist ein Vielfaches von a*, wenn ein $c \in A$ existiert, so daß $b = ac$ gilt, d. h., die Gleichung

$$ax = b \tag{1}$$

lösbar ist. In diesem Fall schreiben wir $a \mid b$; die Verneinung „a teilt nicht b" drücken wir durch $a \nmid b$ aus.

Die Menge aller derjenigen Elemente des Ringes A, die durch ein gegebenes Element a geteilt werden, ist gleich dem Bild von l_a; wir bezeichnen sie mit $aA := \operatorname{Im} l_a = \{ax\}_{x \in A}$. Die Eigenschaft $a \mid b$ ist also äquivalent zu $b \in aA$.

Satz 4. *Die Teilbarkeitsrelation in einem kommutativen Ring A besitzt folgende Eigenschaften:*

1. *Aus $a \mid b$ und $a \mid c$ folgt $a \mid (b + c)$;*
2. *aus $a \mid b$ folgt $a \mid (-b)$;*

3. *ist A assoziativ, so folgt aus $a \mid b$ auch $a \mid bc$ für alle $c \in A$;*

4. *ist A assoziativ, so folgt aus $a \mid b$ und $b \mid c$ die Beziehung $a \mid c$;*

5. *ist A ein Ring mit Einselement, so ist $a \in A^*$ dann und nur dann, wenn $a \mid e$ gilt.*

6. *ist A ein Ring mit Einselement, so folgt aus $a, b \in A$ und $a \sim b$, daß $a \mid b$ und $b \mid a$ gilt.*

Beweis. Die Eigenschaften 1 und 2 gelten, weil $aA = \operatorname{Im} l_a$ eine Untergruppe von $[A, +]$ ist, vgl. Satz 1.2.12. Die Eigenschaft 3 folgt unmittelbar aus der Assoziativität. Wir beweisen Eigenschaft 4. Aus $a \mid b$ und $b \mid c$ folgt die Existenz von Elementen $a', b' \in A$ mit $b = aa'$ und $c = bb'$. Nach dem assoziativen Gesetz gilt $c = (aa')\,b' = a(a'b')$, d. h. $a \mid c$. Die Eigenschaft 5 ist offensichtlich. Wir beweisen Eigenschaft 6. Aus $a \sim b$ folgt die Existenz eines $u \in A^*$ mit $b = ua$, also $a \mid b$. Da die Relation $\sim$ symmetrisch ist, folgt ebenso $b \mid a$. □

Wir wollen nun eine recht natürliche Klasse von Ringen definieren, die alle in Satz 4 formulierten Teilbarkeitseigenschaften besitzen und für die außerdem die Lösung der Gleichung (1) mit $a \neq 0$, wenn sie existiert, eindeutig bestimmt ist.

Definition 5. Ein Ring A heißt ein *Integritätsbereich*, wenn er folgende Eigenschaften besitzt: $A \neq \{0\}$, A ist kommutativ, assoziativ, nullteilerfrei und hat ein Einselement.

Beispiel 3. Jeder Körper ist ein Integritätsbereich. Der Ring der ganzen Zahlen $\mathbf{Z}$ ist ein Integritätsbereich, aber kein Körper.

Nach Satz 1.3 hat eine Gleichung der Form (1), falls $a \neq 0$ gilt, höchstens eine Lösung. Gilt also in einem Integritätsbereich $a \mid b$, $a \neq 0$, so gibt es genau ein Element $c \in A$ mit $b = ac$.

Definition 6. Ist A ein Integritätsbereich, $a \in A$, $a \neq 0$, $b = ac$, so nennen wir das eindeutig bestimmte Element c den *Quotienten von b* durch a und schreiben $c = b/a$.

Wenn A ein Körper ist, stimmt diese Definition mit den üblichen, bei der Division verwendeten Bezeichnungen überein.

Satz 5. *Ist A ein Integritätsbereich, so sind für $a, b \in A$ folgende Aussagen äquivalent:*

1. $a \sim b$;

2. $a \mid b$ *und* $b \mid a$;

3. $aA = bA$.

Beweis. Die Äquivalenz der Aussagen 2 und 3 ergibt sich aus Satz 4, Eigenschaft 4. Nach Satz 4, 6., gilt mit Aussage 1 auch Aussage 2. Wir beweisen nun die Umkehrung. Es gelte $a \mid b$ und $b \mid a$. Dann gibt es $a', b' \in A$ mit $a = bb'$, $b = aa'$. Wir erhalten also $a = (aa')\,b' = a(a'b')$. Ist $a = 0$, so muß wegen $a \mid b$ auch $b = 0$ sein, und daher gilt $a \sim b$. Wenn $a \neq 0$ gilt, können wir die eben bewiesene Identität durch a kürzen und erhalten $a'b' = e$; somit gilt $a', b' \in A^*$ und $a \sim b$. □

Definition 7. Es seien a, b Elemente des Ringes A. Ein Element $d \in A$ heißt *gemeinsamer Teiler* der Elemente a, b, wenn $d \mid a$ und $d \mid b$ gilt. Ein Element $d \in A$

heißt *größter gemeinsamer Teiler* (Abkürzung ggT) von a und b, wenn d gemeinsamer Teiler ist und $d_1 \mid d$ für jeden gemeinsamen Teiler d_1 von a, b gilt.

In einem beliebigen Ring brauchen größte gemeinsame Teiler nicht zu existieren (vgl. Beispiel 5.4). Im folgenden werden wir einige Klassen von Ringen angeben, in denen der ggT stets existiert. Zunächst wollen wir nur eine Eindeutigkeitsaussage beweisen:

Satz 6. *Ist A ein Integritätsbereich, $a, b \in A$, und sind d, d' ggT von a und b, so gilt $d \sim d'$. Mit anderen Worten: Der ggT ist bis auf Assoziiertheit eindeutig bestimmt.*

Beweis. Ist d ggT von a und b und gilt $d \sim d'$, so ist auch d' ggT von a und b, wie man leicht aus Satz 4, 6., erhält. Es seien umgekehrt d und d' ggT von a und b. Dann gilt offenbar $d \mid d'$ und $d' \mid d$, nach Satz 5 also $d \sim d'$. □

Im Sinne dieser Eindeutigkeitsaussage spricht man auch von *dem ggT* der Elemente a, b und bezeichnet ihn mit (a, b).

Übung 1. Die Definition des ggT läßt sich leicht auf n Elemente $a_1, \ldots, a_n$ eines Ringes A ausdehnen. Ein Element $d \in A$ heißt ggT der Elemente $a_1, \ldots, a_n$, wenn $d \mid a_i$ für $i = 1, \ldots, n$ gilt und wenn für alle d', für die $d' \mid a_i$, $i = 1, \ldots, n$, gilt, auch $d' \mid d$ erfüllt ist. Offenbar gilt das Analogon von Satz 6 auch in diesem Fall; für den ggT schreibt man entsprechend $d = (a_1, \ldots, a_n)$. Man beweise: Existiert für je zwei Elemente a, b des Ringes A der ggT, so existiert er auch für je n Elemente $a_1, \ldots, a_n \in A$, $n \geqq 1$. (Hinweis. Man betrachte die Folge $d_1 = (a_1, a_2)$, $d_2 = (d_1, a_3)$, ..., $d_{n-1} = (d_{n-2}, a_n)$ und beweise $d_{n-1} = (a_1, \ldots, a_n)$.)

Offenbar sind die invertierbaren Elemente gemeinsame Teiler von zwei beliebigen Elementen $a, b \in A$. Haben zwei Elemente a, b keine anderen gemeinsamen Teiler, so nennt man sie *relativ prim* (oder *teilerfremd*) und schreibt dafür $(a, b) = e$.

Übung 2. Es seien $a, b \in A$, A Integritätsbereich, $a \neq 0$, $b \neq 0$ und $d = (a, b)$. Man beweise $(a/d, b/d) = e$.

Definition 8. Ein Element p des Ringes A heißt ein *Primelement*, wenn es folgende Eigenschaften besitzt: 1. $p \neq 0$; 2. $p \notin A^*$; 3. wenn $a \mid p$, so gilt $a \in A^*$ oder $a \sim p$.

Satz 7. *Es sei A Integritätsbereich, $p \in A \setminus A^*$, $p \neq 0$. Wir behaupten: p ist Primelement genau dann, wenn $a \in A^*$ oder $b \in A^*$ für jede Zerlegung $p = ab$ gilt. Ein zu einem Primelement assoziiertes Element ist ebenfalls prim.*

Beweis. Es sei p prim und $p = ab$. Ist $a \notin A^*$, so ist $a \sim p$, d. h. $p = ab = au$ mit $u \in A^*$. Aus $p \neq 0$ folgt $a \neq 0$, und wir können diese Gleichung durch a kürzen. Es folgt $b = u \in A^*$. Umgekehrt besitze p die Eigenschaft aus Satz 7. Gilt $a \mid p$, so folgt $p = ab$ mit $b \in A$. Also ist $a \in A^*$ oder $b \in A^*$, und im zweiten Fall gilt $a \sim p$. Die zweite Behauptung ergibt sich aus der Tatsache, daß assoziierte Elemente dieselben Teiler haben. □

Beispiel 4. Die Primelemente des Ringes $\mathbf{Z}$ sind die gewöhnlichen Primzahlen $p = 2, 3, 5, 7, 11, \ldots$ und die dazu negativen $p = -2, -3, -5, \ldots$

Satz 8. *Ist $p \in A$ Primelement, so gilt für jedes $a \in A$ entweder $p \mid a$ oder $(p, a) = e$.*

Beweis. Sind p und a nicht teilerfremd, so existiert ein „echter" gemeinsamer Teiler $d \notin A^*$. Da p prim ist, folgt $d \sim p$, und aus $d \mid a$ folgt $p \mid a$. □

Zum Abschluß dieses Paragraphen wollen wir eine interessante Folge von Ringen untersuchen, die sogenannten *Restklassenringe*. Es sei $n \neq 0$ eine feste natürliche Zahl. Wir sagen, zwei ganze Zahlen $a, b \in \mathbf{Z}$ seien *kongruent* modulo n, und schreiben

$$a \equiv b \bmod n ,$$

wenn $n \mid a-b$ gilt. Diese Beziehung ist eine Äquivalenzrelation im Ring $\mathbf{Z}$. Offenbar ist sie reflexiv und symmetrisch. Wir beweisen die Transitivität. Es sei $a \equiv b \bmod n$ und $b \equiv c \bmod n$, *also* $n \mid a-b$ und $n \mid b-c$. Aus $a-c=(a-b)+(b-c)$ folgt $n \mid a-c$, d. h. $a \equiv c \bmod n$.

Wir bezeichnen mit $\bar{m}$ die Äquivalenzklasse unserer Kongruenzrelation, zu der m gehört, d. h. die Menge aller derjenigen ganzen Zahlen, die zu m kongruent sind. Hierdurch wird $\mathbf{Z}$ in ein System paarweise disjunkter Äquivalenzklassen zerlegt (vgl. Satz 0.2.1). Wir wollen zeigen, daß die Klasseneinteilung gerade aus den n Klassen $\bar{0}, \bar{1}, \ldots, \overline{n-1}$ besteht. In der Tat, gilt $0 \leqq i < j \leqq n-1$, so ist $0 < j-i \leqq n-1$, also $n \nmid j-i$, und somit $j \not\equiv i \bmod n$. Somit sind die angegebenen Äquivalenzklassen alle verschieden. Es bleibt zu zeigen, daß jede ganze Zahl $m \in \mathbf{Z}$ in einer dieser Klassen liegt. Das folgt aus dem bekannten Satz über die *Division mit Rest*: Ist m eine ganze Zahl und $n > 0$ eine natürliche Zahl, so gibt es eindeutig bestimmte ganze Zahlen q, r mit $0 \leqq r < n$ so, daß $m = q \cdot n + r$ gilt. Aus der letzten Gleichung folgt $m \equiv r \bmod n$, d. h. $m \in \bar{r}$. Man beweist leicht: Es gilt $m \equiv m' \bmod n$ dann und nur dann, wenn m und m' bei Division durch n denselben Rest $r = r'$ ergeben. Hieraus erklärt sich die Bezeichnung *Restklassen* modulo n, die wir im folgenden verwenden.

Mit $\mathbf{Z}_n$ bezeichnen wir die Menge $\{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ der Restklassen modulo n. In $\mathbf{Z}_n$ führen wir durch

$$\bar{k} + \bar{l} := \overline{k+l}, \qquad \bar{k} \cdot \bar{l} := \overline{k \cdot l} \qquad (k, l \in \mathbf{Z}) \tag{2}$$

eine Addition und eine Multiplikation ein; es ist zu zeigen, daß diese Definitionen korrekt, d. h. unabhängig von der Auswahl der Vertreter sind: Es seien $\overline{k_1} = \bar{k}$, $\overline{l_1} = \bar{l}$, d. h. $k_1 - k = nx$, $l_1 - l = ny$ mit $x, y \in \mathbf{Z}$. Dann gilt

$$k_1 + l_1 = k + l + n\,(x+y) \equiv k + l \bmod n ,$$
$$k_1 \cdot l_1 = k \cdot l + n\,(xl + yk + nx \cdot y) \equiv k \cdot l \bmod n .$$

Den recht einfachen Beweis des folgenden Satzes wollen wir dem Leser überlassen:

Satz 9. *Die durch* (2) *definierten Operationen verwandeln* $\mathbf{Z}_n$ *in einen kommutativen, assoziativen Ring mit Einselement* $\bar{1}$, *und die kanonische Abbildung* $m \in \mathbf{Z} \mapsto \bar{m} \in \mathbf{Z}_n$ *ist ein Ringhomomorphismus.* □

Definition 9. Der durch Satz 9 definierte Ring $\mathbf{Z}_n$ heißt der *Restklassenring* modulo n.

Satz 10. *Folgende Aussagen sind äquivalent:*

1. *n ist eine Primzahl;*
2. *$\mathbf{Z}_n$ ist ein Integritätsbereich;*
3. *$\mathbf{Z}_n$ ist ein Körper.*

Beweis. Wir verwenden die folgende Eigenschaft der ganzen Zahlen (sie ist ein Spezialfall von Satz 5.4): Ist p eine Primzahl und gilt $p \mid ab$, $a, b \in \mathbf{Z}$, so gilt $p \mid a$ oder $p \mid b$. Es sei nun n prim; wir zeigen, daß $\mathbf{Z}_n$ nullteilerfrei ist. Aus $\bar{k} \cdot \bar{l} = \overline{k \cdot l} = \bar{0}$ folgt nämlich $n \mid k \cdot l$, also nach der eben formulierten Eigenschaft $n \mid k$ oder $n \mid l$, d. h. $\bar{k} = \bar{0}$ oder $\bar{l} = \bar{0}$. Ist $n > 1$ nicht prim, so gibt es eine echte Zerlegung $n = r \cdot s$ mit $1 < r < n$, $1 < s < n$, also $\bar{r} \cdot \bar{s} = \bar{0}$, $\bar{r} \neq \bar{0}$, $\bar{s} \neq \bar{0}$, d. h., $\bar{r}$, $\bar{s}$ sind Nullteiler. $\mathbf{Z}_1 = \{\bar{0}\}$ ist ebenfalls kein Integritätsbereich. Es bleibt zu zeigen, daß aus der Aussage 2 die Aussage 3 folgt; denn die Umkehrung ist trivial. Hierfür genügt es zu beweisen, daß jedes $\alpha \in \mathbf{Z}_n$, $\alpha \neq \bar{0}$, invertierbar ist. Multiplizieren wir alle Elemente aus $\mathbf{Z}_n$ mit α, so erhalten wir die Restklassen $\alpha \cdot \bar{0}$, $\alpha \cdot \bar{1}$, ..., $\alpha \cdot \overline{(n-1)}$. Alle diese Klassen sind verschieden; denn aus $\alpha\bar{k} = \alpha\bar{l}$, $\alpha \neq 0$, folgt $\bar{k} = \bar{l}$, weil $\mathbf{Z}_n$ ein Integritätsbereich ist. Da die Anzahl dieser Klassen gleich n ist, ergibt sich der ganze Ring $\mathbf{Z}_n$; es existiert also ein $\bar{k}$ mit $\alpha\bar{k} = \bar{1}$, also $\bar{k} = \alpha^{-1}$. □

Wenn n prim ist, nennt man $\mathbf{Z}_n$ auch den *Restklassenkörper* modulo n.

Übung 3. Man beweise, daß char $\mathbf{Z}_n = n$ gilt und daß $[\mathbf{Z}_n, +]$ eine zyklische Gruppe der Ordnung n ist.

Übung 4. Man beweise, daß jeder Ring der Charakteristik n mit Einselement einen zu $\mathbf{Z}_n$ isomorphen Unterring enthält; jeder Körper der Charakteristik p (p prim) enthält einen zu $\mathbf{Z}_p$ isomorphen Teilkörper; jeder Körper der Charakteristik 0 enthält einen zu $\mathbf{Q}$ isomorphen Teilkörper.

Übung 5. Man beweise, daß die Äquivalenzrelation $\equiv \bmod n$ durch eine Wirkung der Gruppe $\mathbf{Z}$ über sich definiert werden kann (vgl. Satz 1.4.4).

Übung 6. Man zeige, daß ein endlicher Integritätsbereich stets ein Körper ist.

Übung 7. Ein Körper K_0 heißt *Primkörper*, wenn er keinen echten Teilkörper $L \subset K_0$ besitzt. Man zeige: Jeder Körper K enthält genau einen Primkörper K_0, und dieser liegt in jedem Teilkörper $L \subset K$. Dabei ist K_0 zu einem der Körper $\mathbf{Q}$, $\mathbf{Z}_p$, p prim, isomorph; es gilt char $K = p$ (bzw. $= 0$) genau dann, wenn $K_0 \cong \mathbf{Z}_p$ (bzw. $\cong \mathbf{Q}$) ist. Alle Teilkörper des Körpers K haben folglich dieselbe Charakteristik.

Übung 8. Es sei K ein Körper. In der Menge $K \times K$ der Paare führen wir die Operationen $+$, $\cdot$ durch komponentenweise Definition ein:

$$(a, b) + (c, d) := (a + c, b + d), \qquad (a, b) \cdot (c, d) := (ac, bd) .$$

Man beweise: a) $[K \times K, +, \cdot]$ ist ein Ring (vgl. Beispiel 1.2). – b) $[K \times K, +, \cdot]$ ist kein Körper. – c) Die Abbildung $f: a \in K \mapsto (a, 0) \in K \times K$ ist ein Ringhomomorphismus, Im f ist ein Körper, und jedes von 0 verschiedene Element aus Im f ist ein Nullteiler in $K \times K$, besitzt also in $K \times K$ kein Inverses. (Man beachte, daß das Einselement von $K \times K$ nicht in Im f liegt.)

Übung 9. Es sei K ein Körper und $A \subseteq K$, $A \neq \{0\}$, ein Unterring von K. Man beweise: Ist ε ein Einselement in A, so ist ε gleich dem Einselement e von K (vgl. dagegen Übung 8c)).

§ 3. Komplexe Zahlen

Die komplexen Zahlen verdanken ihre Entstehung dem Umstand, daß viele algebraische Gleichungen mit reellen Koeffizienten keine reellen Lösungen besitzen. Das einfachste Beispiel ist die Gleichung

$$x^2+1=0\,. \tag{1}$$

Wir stellen uns nun die Aufgabe, eine Erweiterung K des Körpers $\mathbf{R}$ zu konstruieren, in der die Gleichung (1) lösbar ist. Hierdurch ist K nicht eindeutig bestimmt; fordert man jedoch, daß K eine kleinste derartige Erweiterung ist, so ist K bis auf einen Isomorphismus eindeutig festgelegt.

Zuerst wollen wir direkt einen Körper mit den erforderlichen Eigenschaften angeben. Wir gehen von der Menge $\mathbf{C}=\mathbf{R}\times\mathbf{R}$ der geordneten Paare (a, b) reeller Zahlen aus und definieren in ihr komponentenweise die Addition

$$(a, b)+(c, d):=(a+c, b+d)\,. \tag{2}$$

Man erkennt leicht, daß $\mathbf{C}$ hierdurch eine abelsche Gruppe mit dem Nullelement $0=(0, 0)$ wird; ferner gilt $-(a, b)=(-a, -b)$. Die Multiplikation definieren wir in $\mathbf{C}$ folgendermaßen:

$$(a, b)\cdot(c, d):=(ac-bd, ad+bc)\,. \tag{3}$$

Satz 1. *Durch die Operationen* (2), (3) *wird* $\mathbf{C}$ *ein Körper. Sein Einselement ist* $(1, 0)$, *und das zu* $(a, b)\neq 0$ *inverse Element hat die Gestalt*

$$(a, b)^{-1}=\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right). \tag{4}$$

Beweis. Offenbar ist die Multiplikation kommutativ. Die Assoziativität ergibt sich durch etwas umständliches Nachrechnen:

$$\begin{aligned}((a, b)\cdot(c, d))\,(p, q)&=(ac-bd, ad+bc)\,(p, q)\\&=((ac-bd)\,p-(ad+bc)\,q, (ac-bd)\,q+(ad+bc)\,p)\\&=(acp-bdp-adq-bcq, acq-bdq+adp+bcp)\\&=(a\,(cp-dq)-b\,(cq+dp), a\,(cq+dp)+b(cp-dq))\\&=(a, b)\,(cp-dq, cq+dp)=(a, b)\,((c, d)\cdot(p, q))\,.\end{aligned}$$

Die Nachprüfung des distributiven Gesetzes überlassen wir dem Leser. Aus (3) folgt $(1, 0)\,(c, d)=(c, d)$. Schließlich rechnet man mit Hilfe von (3) leicht aus, daß

$$(a, b)\cdot\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)=(1, 0)$$

ist. □

Nun wollen wir zeigen, daß wir $\mathbf{C}$ in recht natürlicher Weise als eine Erweiterung von $\mathbf{R}$ auffassen können:

Satz 2. *Die Abbildung*

$$\alpha: a\in\mathbf{R}\mapsto\alpha(a):=(a, 0)\in\mathbf{C}$$

ist ein Isomorphismus von $\mathbf{R}$ *auf den Teilkörper* $\hat{\mathbf{R}} := \operatorname{Im} \alpha \subset \mathbf{C}$. *Identifizieren wir* $\mathbf{R}$ *und* $\hat{\mathbf{R}}$ *mit Hilfe des Isomorphismus* α *und definieren wir*

$$\mathrm{i} := (0, 1),$$

so können wir jede komplexe Zahl $(a, b) \in \mathbf{C}$ *in der Gestalt*

$$(a, b) = a + b\mathrm{i} \qquad (a, b \in \mathbf{R})$$

schreiben, und es gilt

$$\mathrm{i}^2 + 1 = 0.$$

Der Körper $\mathbf{C}$ *ist eine minimale Erweiterung des Körpers* $\mathbf{R}$, *d. h., für jeden Teilkörper* $L \subseteq \mathbf{C}$ *folgt aus* $\mathbf{R} \subseteq L$ *entweder* $L = \mathbf{R}$ *oder* $L = \mathbf{C}$.

Beweis. Aus (2) und (3) folgt sofort, daß α ein Ringhomomorphismus ist. Offenbar gilt $\operatorname{Ker} \alpha = 0$, d. h., α ist injektiv und bildet $\mathbf{R}$ isomorph auf $\hat{\mathbf{R}}$ ab (Folgerung 1.1); hierbei ist $\hat{\mathbf{R}} = \{(a, 0) \mid a \in \mathbf{R}\}$. Offenbar ist $\hat{\mathbf{R}}$ ein Teilkörper von $\mathbf{C}$. Nach Ausführung der im Satz beschriebenen Identifikation folgt sofort $(a, b) = a + b\mathrm{i}$ und $\mathrm{i}^2 + 1 = 0$. Zum Beweis der Minimalität betrachten wir irgendeinen Teilkörper L mit $\mathbf{R} \subseteq L \subseteq \mathbf{C}$. Angenommen, es sei $\mathbf{R} \neq L$. Dann existiert ein Element $a + b\mathrm{i} \in L$ mit $b \neq 0$. Aus $a, b \in \mathbf{R} \subset L$ folgt $b\mathrm{i} = (a + b\mathrm{i}) - a \in L$ und $\mathrm{i} = b^{-1}(b\mathrm{i}) \in L$. Dann muß aber für beliebige $c, d \in \mathbf{R}$ auch $c + d\mathrm{i} \in L$ sein, d. h., es gilt $L = \mathbf{C}$. □

Definition 1. Der nach Satz 1 konstruierte Körper $\mathbf{C}$ heißt der *Körper der komplexen Zahlen*. Ist $z = a + b\mathrm{i}$ eine komplexe Zahl, so heißt $R(z) := a \in \mathbf{R}$ der *Realteil* und $I(z) := b \in \mathbf{R}$ der *Imaginärteil von* z. Die komplexen Zahlen mit $R(z) = 0$ heißen *imaginär*.

Wie schon in Satz 2 identifizieren wir im folgenden stets $\mathbf{R}$ mit dem Teilkörper $\hat{\mathbf{R}} \subset \mathbf{C}$ vermöge $a \in \mathbf{R} \mapsto \alpha(a) = a + 0\mathrm{i} = a \in \mathbf{C}$. Statt $z = (a, b)$ benutzt man im allgemeinen die Schreibweise $z = a + b\mathrm{i}$. Jetzt wollen wir zeigen, daß die im Satz 2 angegebenen Eigenschaften den Körper der komplexen Zahlen bis auf einen Isomorphismus eindeutig bestimmen.

Satz 3. *Es sei* K *eine Erweiterung des Körpers* $\mathbf{R}$, *die folgende Eigenschaften besitzt:*

1. *Es existiert ein* $j \in K$ *mit* $j^2 = -1$;

2. K *ist eine minimale Erweiterung von* $\mathbf{R}$, *d. h., ist* $L \subseteq K$ *ein Teilkörper mit* $\mathbf{R} \subseteq L$, *so gilt* $L = \mathbf{R}$ *oder* $L = K$.

Dann gibt es genau einen Isomorphismus $f: \mathbf{C} \to K$ *mit* $f \mid \mathbf{R} = \mathrm{id}_{\mathbf{R}}$ *und* $f(\mathrm{i}) = j$.

Beweis. Wenn $f: \mathbf{C} \to K$ ein derartiger Isomorphismus sein soll, muß notwendig $f(a + b\mathrm{i}) = f(a) + f(b) \cdot f(\mathrm{i}) = a + bj$ gelten, es gibt also höchstens einen derartigen Isomorphismus. Definieren wir f durch $f(a + b\mathrm{i}) := a + bj$, so folgt leicht $f(z_1 + z_2) = f(z_1) + f(z_2)$; wir prüfen die Multiplikativität nach:

$$\begin{aligned} f((a + b\mathrm{i})(c + d\mathrm{i})) &= f((ac - bd) + (ad + bc)\mathrm{i}) = (ac - bd) + (ad + bc)j \\ &= (a + bj)(c + dj) = f(a + b\mathrm{i}) \cdot f(c + d\mathrm{i}). \end{aligned}$$

Dabei haben wir $j^2=-1$ angewandt. Offenbar gilt $f \mid \mathbf{R}=\mathrm{id}_{\mathbf{R}}$ und $f(\mathrm{i})=j$, speziell also $\mathrm{Im}\, f \neq 0$. Daher wird $\mathbf{C}$ isomorph auf den Teilkörper $L:=\mathrm{Im}\, f \subseteq K$ abgebildet (Satz 2.2). Offenbar gilt $\mathbf{R} \subseteq L \subseteq K$ und $L \neq \mathbf{R}$, denn es ist $f(\mathrm{i})=j \in L \setminus \mathbf{R}$, weil $j^2=-1$ ist und die Gleichung (1) in $\mathbf{R}$ keine Lösung besitzt. Nach Eigenschaft 2 folgt $L=K$, und $f: \mathbf{C} \to K$ ist ein Isomorphismus. □

Wir wollen nun die einfachsten Eigenschaften des Körpers der komplexen Zahlen herleiten. Zuerst geben wir eine geometrische Interpretation an. Wir wählen in der Ebene ein festes, kartesisches Koordinatensystem (vgl. § 4.1). Der komplexen Zahl $z=a+bi \in \mathbf{C}$ ordnen wir den Punkt p mit den Koordinaten (a, b), $a, b \in \mathbf{R}$, zu. Offenbar erhalten wir so eine bijektive Abbildung von $\mathbf{C}$ auf die Ebene. Oft ist es zweckmäßig, statt der Punkte p der Ebene die entsprechenden Ortsvektoren $\overrightarrow{op}$ bezüglich des Ursprungs o zu betrachten. Bei dieser Abbildung gehen 1 und i in die auf den Koordinatenachsen liegenden Einheitsvektoren über (Abb. 1). Aus der

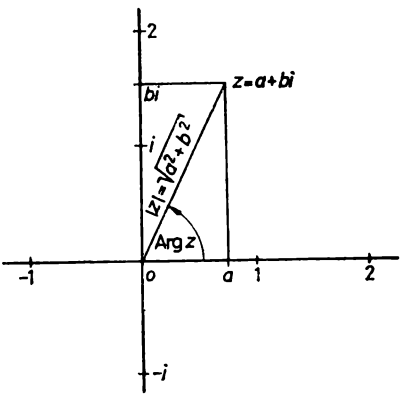


Abb. 1

elementaren Geometrie ist wohlbekannt, daß die Addition von zwei Ortsvektoren komponentenweise erfolgt. Wir können also feststellen, daß die Zuordnung $z \in \mathbf{C} \mapsto \overrightarrow{op} \in V$ ein Isomorphismus der additiven Gruppe von $\mathbf{C}$ auf die Gruppe V der Vektoren der Ebene ist (vgl. Beispiel 1.1.6). Damit erhalten wir eine geometrische Interpretation der Addition der komplexen Zahlen. Zur geometrischen Interpretation der Multiplikation müssen wir zunächst zwei neue Begriffe einführen:

Definition 2. Unter dem *Betrag* $|z|$ der komplexen Zahl z verstehen wir die Länge des z entsprechenden Ortsvektors:

$$z=a+bi \in \mathbf{C} \mapsto |z| := \sqrt{a^2+b^2} \in \mathbf{R}$$

(nach dem Satz von Pythagoras). Unter dem *Argument* von $z \in \mathbf{C}^*$ – Schreibweise $\mathrm{Arg}\, z$ – verstehen wir den Winkel zwischen der positiven Abszisse (der reellen Achse) und dem z entsprechenden Ortsvektor; $\mathrm{Arg}\, z$ ist bis auf ein ganzzahliges Vielfaches von 2π eindeutig bestimmt (vgl. Beispiel 0.2.17), falls $z \neq 0$ gilt; für $z=0$ wird $\mathrm{Arg}\, z$ nicht definiert.

Offenbar gilt

$$\cos(\operatorname{Arg} z) = a/|z|, \qquad \sin(\operatorname{Arg} z) = b/|z|,$$

also

$$z = |z|\,(\cos(\operatorname{Arg} z) + \mathrm{i}\sin(\operatorname{Arg} z)) \qquad (z \in \mathbf{C}^*).$$

Diese sogenannte trigonometrische Schreibweise der komplexen Zahlen ist eindeutig in dem folgenden Sinne: Ist $z \in \mathbf{C}^*$ und

$$z = r\,(\cos\varphi + \mathrm{i}\sin\varphi), \qquad r, \varphi \in \mathbf{R}, \qquad r \geqq 0, \tag{5}$$

so gilt $r = |z| > 0$ und $\varphi = \operatorname{Arg} z$, wie man sofort nachrechnet.

Eine geometrische Deutung der Multiplikation enthält der folgende

Satz 4. *Betrag und Argument besitzen folgende Eigenschaften:*

$$|zw| = |z| \cdot |w| \qquad (z, w \in \mathbf{C}), \tag{6}$$

$$\operatorname{Arg}(z \cdot w) = \operatorname{Arg} z + \operatorname{Arg} w \qquad (z, w \in \mathbf{C}^*). \tag{7}$$

Beweis. Für $z = 0$ oder $w = 0$ gilt (6) trivialerweise. Es seien also $z, w \in \mathbf{C}^*$, und es gelte

$$z = |z|\,(\cos\varphi + \mathrm{i}\sin\varphi), \qquad w = |w|\,(\cos\psi + \mathrm{i}\sin\psi)$$

mit $\varphi = \operatorname{Arg} z$, $\psi = \operatorname{Arg} w$. Multiplikation ergibt unter Berücksichtigung der Additionstheoreme für die Winkelfunktionen

$$zw = |z|\,|w|\,(\cos(\varphi + \psi) + \mathrm{i}\sin(\varphi + \psi)).$$

Aus der oben bereits bemerkten Eindeutigkeit der trigonometrischen Schreibweise folgen sofort (6) und (7). □

Aus Satz 4 erhält man sofort eine Möglichkeit zur geometrischen Konstruktion des Produkts zw: In Abb. 2 sind die Dreiecke $(0, 1, z)$ und $(0, w, zw)$ ähnlich.

Wir zeigen

Satz 5. *Für $z \in \mathbf{C}^*$ und $n \in \mathbf{Z}$ gilt*

$$|z^n| = |z|^n, \qquad \operatorname{Arg} z^n = n \operatorname{Arg} z.$$

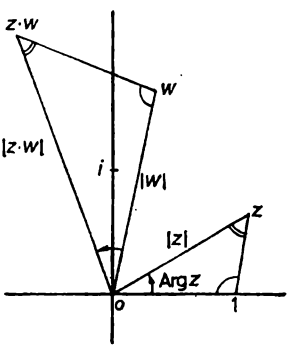


Abb. 2

Beweis. Für $n=0$ ist die Behauptung trivial. Für $n>0$ ergibt sie sich leicht durch Induktion aus Satz 4. Nach (4) gilt mit $\varphi = \operatorname{Arg} z$

$$z^{-1} = \frac{1}{|z|^2}(|z|\cos\varphi - \mathrm{i}\,|z|\sin\varphi) = \frac{1}{|z|}(\cos(-\varphi) + \mathrm{i}\sin(-\varphi));$$

das ist aber die Behauptung für $n=-1$. Ist schließlich $n \in \mathbf{Z}$ eine beliebige negative Zahl, so gilt $z^n = (z^{-1})^{|n|}$, und hieraus folgt

$$|z^n| = |z^{-1}|^{|n|} = (|z|^{-1})^{|n|} = |z|^n,$$

$$\operatorname{Arg} z^n = \operatorname{Arg}(z^{-1})^{|n|} = |n| \operatorname{Arg} z^{-1} = -|n| \operatorname{Arg} z = n \operatorname{Arg} z. \quad \square$$

Folgerung 1 (Formel von Moivre). *Gilt* $z = |z|(\cos\varphi + \mathrm{i}\sin\varphi)$ *und* $n \in \mathbf{Z}$, *so folgt*

$$z^n = |z|^n(\cos n\varphi + \mathrm{i}\sin n\varphi). \quad \square$$

Die bewiesenen Eigenschaften der Multiplikation der komplexen Zahlen gestatten eine gruppentheoretische Deutung. Zum Beispiel besagt die Gleichung (6), daß die Abbildung $\mu: z \in \mathbf{C}^* \mapsto |z| \in \mathbf{R}_+$ ein Homomorphismus der multiplikativen Gruppe $\mathbf{C}^*$ in die Gruppe $\mathbf{R}_+$ ist. Daher ist die erste Behauptung von Satz 5 einfach ein Spezialfall des Satzes 1.3.1 b). Nach Satz 1.2.12 ist der Kern $S^1 := \operatorname{Ker}\mu$ eine Untergruppe von $\mathbf{C}^*$; sie besteht aus allen $z \in \mathbf{C}$ mit $|z|=1$ und wird geometrisch als Kreis vom Radius 1 mit dem Zentrum 0 dargestellt.

Bemerkung. Aus der geometrischen Deutung der Addition folgt sofort, daß

$$|z+w| \leqq |z| + |w|$$

für alle $z, w \in \mathbf{C}$ gilt. Offenbar ist auch stets $|z| \geqq 0$, und es gilt $|z|=0$ dann und nur dann, wenn $z=0$ ist. Hieraus und aus (6) folgt, daß der Betrag alle Eigenschaften einer Norm (vgl. § 6.1) erfüllt.

Übung 1. Man beweise, daß die Abbildung

$$\lambda: z \in \mathbf{C}^* \mapsto d_{\operatorname{Arg} z} \in C$$

ein Homomorphismus von $\mathbf{C}^*$ auf die Gruppe C der Drehungen der Ebene um 0 ist (vgl. Beispiel 1.3.3). Man bestimme Ker λ und zeige, daß λ die Gruppe $S^1 = \operatorname{Ker}\mu \subset \mathbf{C}^*$ isomorph auf C abbildet.

Übung 2. Man benutze den Isomorphismus $S^1 \cong C$ von Übung 1, um die natürliche Wirkung von C über der Ebene mittels der Multiplikation komplexer Zahlen zu beschreiben.

Eine wichtige Rolle in der Theorie der komplexen Zahlen spielt die Abbildung

$$z = a + b\mathrm{i} \in \mathbf{C} \mapsto \bar{z} := a - b\mathrm{i} \in \mathbf{C} \qquad (a, b \in \mathbf{R}),$$

die jeder komplexen Zahl z ihre *konjugierte* $\bar{z}$ zuordnet. Geometrisch bedeutet die Abbildung $z \to \bar{z}$ die Spiegelung an der Abszissenachse. Offenbar gilt

$$|\bar{z}| = |z|, \qquad \operatorname{Arg}\bar{z} = -\operatorname{Arg} z.$$

Satz 6. *Die Abbildung* $z \in \mathbf{C} \mapsto \bar{z} \in \mathbf{C}$ *ist ein Automorphismus des Körpers* $\mathbf{C}$, *d. h., es gilt*

$$\overline{z+w} = \bar{z} + \bar{w}, \qquad \overline{zw} = \bar{z}\bar{w} \qquad (z, w \in \mathbf{C}) .$$

Beweis. Aus $\bar{\bar{z}} = z$ folgt, daß die Abbildung umkehrbar, also bijektiv ist. Die Vertauschbarkeit mit den Rechenoperationen ergibt sich unmittelbar aus den Definitionen. □

Übung 3. Es sei γ ein Endomorphismus des Körpers $\mathbf{C}$, der $\mathbf{R}$ in sich überführt. Man beweise: Dann gilt entweder $\gamma(z) = 0$ für alle $z \in \mathbf{C}$, oder es gilt $\gamma = \mathrm{id}_{\mathbf{C}}$ oder $\gamma(z) = \bar{z}$ für alle $z \in \mathbf{C}$. (Hinweis. Man wende Übung 1.3 an.)

Nach Satz 2 ist die Gleichung $x^2 + 1 = 0$ im Körper $\mathbf{C}$ lösbar. Wie wir später sehen werden, hat in $\mathbf{C}$ jedes Polynom Nullstellen. Wir wollen nun die Lösungen der Gleichung $x^n = c$ ($n \in \mathbf{N}$, $c \in \mathbf{C}$) bestimmen, die man die *n-ten Wurzeln aus c* nennt. Wenn $c = 1$ ist, spricht man von den *n-ten Einheitswurzeln*. Gilt $c = 0$, so gibt es nur die Lösung $x = 0$; es genügt also, den Fall $c \neq 0$ zu betrachten.

Satz 7. *Es gibt genau n verschiedene n-te Einheitswurzeln, nämlich*

$$\varepsilon_k := \cos(2\pi k/n) + \mathrm{i} \sin(2\pi k/n) \qquad (k = 0, 1, \ldots, n-1) .$$

Die Menge $K_n := \{\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}\}$ *ist eine zyklische Untergruppe von* $\mathbf{C}^*$, *die von* ε_1 *erzeugt wird.*

Beweis. Für $z \in \mathbf{C}$ gilt $z^n = 1$ genau dann, wenn $|z|^n = 1$ und $n \operatorname{Arg} z = 2\pi k$ gilt für ein gewisses $k \in \mathbf{Z}$ (Satz 5). Hieraus folgt $|z| = 1$ und $\operatorname{Arg} z = 2\pi k/n$ mit $k \in \mathbf{Z}$, d. h.

$$z = \varepsilon_k := \cos(2\pi k/n) + \mathrm{i} \sin(2\pi k/n) \qquad (k \in \mathbf{Z}) . \tag{8}$$

Die Gleichung (8) beschreibt also die Menge K_n. Offenbar gilt $\varepsilon_k = \varepsilon_1^k$ für $k \in \mathbf{Z}$, und somit ist K_n die von ε_1 erzeugte zyklische Untergruppe von $\mathbf{C}^*$. Nun gilt $o(\varepsilon_1) = n$; in der Tat ist $\varepsilon_1^n = 1$, während $0 < 2\pi l/n < 2\pi$ für $0 < l < n$ gilt, also $\varepsilon_1^l = \varepsilon_l \neq 1$. Nach Satz 1.3.2 sind die Zahlen ε_k, $k = 0, 1, \ldots, n-1$, paarweise verschieden, und ihre Vereinigung ist K_n. □

Folgerung 2. *Für jedes* $n \in \mathbf{N}$ *und* $c \in \mathbf{C}^*$ *existieren genau n verschiedene n-te Wurzeln aus c.*

Beweis. Wir setzen $\varphi := \operatorname{Arg} c$ und $b = \sqrt[n]{|c|}\,(\cos(\varphi/n) + \mathrm{i} \sin(\varphi/n))$. Nach Folgerung 1 gilt $b^n = c$. Daher existiert wenigstens eine Lösung der Gleichung $x^n = c$. Es sei nun $b_j := b\varepsilon_j$, $j = 0, 1, \ldots, n-1$. Diese Zahlen sind paarweise verschieden; denn aus $b_i = b_j$ folgt $\varepsilon_i = \varepsilon_j$, also $i = j$. Andererseits hat jede Wurzel aus c die Gestalt $b\varepsilon_j$; denn aus $a^n = c$ folgt $(a/b)^n = 1$, d. h. $a/b = \varepsilon_j$ für ein gewisses j. □

Übung 4. Man beweise, daß der Homomorphismus λ aus Übung 1 die Untergruppe K_n isomorph auf die Untergruppe $C_n \subset C$ abbildet (vgl. Beispiel 1.3.3).

Übung 5. Mit Hilfe des Ergebnisses von Übung 1.3.6 bestimme man die n-ten Einheitswurzeln ε_i, die K_n erzeugen: $[\varepsilon_i] = K_n$; sie heißen *primitive Einheitswurzeln*.

Übung 6. Man beweise, daß die n-ten Einheitswurzeln in der Ebene durch die Ecken eines regulären n-Ecks mit dem Zentrum 0 dargestellt werden; eine der Ecken ist 1.

Übung 7. Man beweise, daß die Menge $\{K_n\}_{n\in\mathbf{N}}$ alle endlichen Untergruppen von $\mathbf{C}^*$ enthält.

Übung 8. Man zeige, daß $\bigcup_{n=1}^{\infty} K_n$ eine abzählbare (überall dichte) Untergruppe in S^1 ist.

Zum Abschluß dieses Paragraphen wollen wir als ein interessantes Beispiel den Schiefkörper der Quaternionen einführen. Es sei $\mathbf{H} := \mathbf{C} \times \mathbf{C}$ die Menge der geordneten Paare (z, w) komplexer Zahlen. In $\mathbf{H}$ definieren wir die Addition wieder komponentenweise durch

$$(u, v) + (w, z) := (u + w, v + z) \tag{9}$$

und die Multiplikation durch

$$(u, v) \cdot (w, z) := (uw - \bar{z}v, zu + v\bar{w}) . \tag{10}$$

Offenbar ist $[\mathbf{H}, +, \cdot]$ ein Ring; wir werden sehen, daß er sogar ein Schiefkörper ist. Man nennt ihn den *Schiefkörper der Quaternionen.*

Übung 9. Man zeige, daß $\mathbf{H}$ assoziativ, aber nicht kommutativ ist; das Element $(1, 0)$ ist Einselement von $\mathbf{H}$.

Man erkennt leicht, daß die Abbildung $\beta: z \in \mathbf{C} \mapsto \beta(z) := (z, 0) \in \mathbf{H}$ ein injektiver Ringhomomorphismus ist. Daher können wir mittels β den Körper $\mathbf{C}$ mit dem Unterring aller Elemente der Form $(z, 0)$ von $\mathbf{H}$ identifizieren. Dabei wird $\mathbf{R}$ mit dem Unterring aller Elemente der Form $(a, 0)$, $a \in \mathbf{R}$, von $\mathbf{H}$ identifiziert. Wir definieren nun die sogenannten imaginären Einheiten

$$\mathrm{i} := (\mathrm{i}, 0), \qquad \mathrm{j} := (0, 1), \qquad \mathrm{k} := (0, \mathrm{i}) .$$

Übung 10. Man verifiziere die Gleichung

$$(a + b\mathrm{i}, c + d\mathrm{i}) = a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k} \qquad (a, b, c, d \in \mathbf{R})$$

und zeige, daß die Multiplikationstabelle der Elemente i, j, k folgendermaßen aussieht:

	i	j	k
i	-1	k	$-$j
j	$-$k	-1	i
k	j	$-$i	-1

Für ein beliebiges Quaternion $q = (z, w) = a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k}$ definieren wir den *Betrag* durch

$$|q| := \sqrt{|z|^2 + |w|^2} = \sqrt{a^2 + b^2 + c^2 + d^2}$$

und das *konjugierte Quaternion* $\bar{q}$ durch

$$\bar{q} := (\bar{z}, -w) = a - b\mathrm{i} - c\mathrm{j} - d\mathrm{k} .$$

Übung 11. Man beweise die folgenden Regeln:

$$\left.\begin{array}{ll} 1. & \overline{q_1 + q_2} = \overline{q_1} + \overline{q_2}, \\ 2. & \overline{q_1 q_2} = \overline{q_2}\,\overline{q_1}, \\ 3. & q\bar{q} = \bar{q}q = |q|^2, \\ 4. & |q_1 q_2| = |q_1|\,|q_2| \end{array}\right\} \quad (q, q_1, q_2 \in \mathbf{H}) .$$

Aus Übung 11 folgt unmittelbar, daß der Ring $\mathbf{H}$ ein Schiefkörper ist. In der Tat, für $q \in \mathbf{H}$ und $q \neq 0$ gilt $|q| > 0$; daher ist das Element $\bar{q}/|q|^2$ wohldefiniert, es ist invers zu q.

Übung 12. Man zeige, daß die Elemente $\pm 1, \pm i, \pm j, \pm k$ eine Untergruppe von $\mathbf{H}^*$ bilden.

Aus (9) und (10) ist ersichtlich, daß der Schiefkörper $\mathbf{H}$ aus dem Körper der komplexen Zahlen nach demselben Prinzip definiert wurde wie $\mathbf{C}$ aus dem Körper der reellen Zahlen. Wendet man dieses „Verdopplungsprinzip" noch einmal auf den Schiefkörper $\mathbf{H}$ an, so erhält man einen neuen Ring $\mathbf{O}$ mit Einselement, den Ring der *Oktaven*, auch *Cayleysche Zahlen* genannt. Für ihn gilt $\mathbf{O}^* = \mathbf{O} \setminus \{0\}$, aber er ist weder kommutativ noch assoziativ. Versucht man das Prinzip noch einmal anzuwenden, so erhält man schon keinen Ring mehr, in dem alle Elemente außer der Null umkehrbar wären; vgl. hierzu I. L. Kantor und A. S. Solodovnikov [1].

§ 4. Polynomringe

In diesem Paragraphen wollen wir Polynomringe mit Koeffizienten in einem Integritätsbereich definieren und untersuchen. Die Frage nach der Bestimmung der Nullstellen eines Polynoms wurde noch im vorigen Jahrhundert als Grundaufgabe der Algebra betrachtet. In der Algebra werden die Polynome nicht als Funktionen, wie in der Elementarmathematik üblich, definiert, sondern durch eine formale Konstruktion eines gewissen Ringes. In den wichtigsten klassischen Fällen sind beide Definitionen äquivalent; über endlichen Ringen, z. B. den Restklassenkörpern, ist die algebraische Definition reichhaltiger (vgl. Beispiel 1 weiter unten).

Definition 1. Es sei A ein Integritätsbereich. Unter einem *Polynom* über A verstehen wir eine unendliche Folge $\alpha = (a_0, a_1, ..., a_i, ...)$, $a_i \in A$ für alle $i \in \mathbf{N}_0$, in der alle bis auf endlich viele Glieder a_i gleich 0 sind. Das Polynom $0 = (0, 0, ..., 0, ...)$, in dem alle Glieder 0 sind, heißt das *Nullpolynom*. Ist $\alpha \neq 0$, so gibt es genau ein $n \in \mathbf{N}_0$ mit $a_n \neq 0$ und $a_i = 0$ für $i > n$; n heißt der *Grad des Polynoms* und wird mit $\operatorname{gr} \alpha$ bezeichnet. Für $\alpha = 0$ wird gr nicht definiert. Die Menge aller Polynome bezeichnen wir mit $A[x]$.

Bemerkung. Die von der üblichen abweichende Bezeichnung der Polynome ist nur zur Klärung der begrifflichen Zusammenhänge notwendig; nach Einführung der Unbestimmten x können wir durch (4) (siehe unten) zu der bekannten Schreibweise übergehen. Man beachte, daß x keine Variable ist! Offenbar hätten wir $A[x]$ auch als Menge aller endlichen Folgen $(a_0, a_1, ..., a_n)$, $a_n \neq 0$, $n \in \mathbf{N}_0$, definieren können; jedoch lassen sich die einzuführenden Operationen in der von uns bevorzugten *„formal unendlichen"* Schreibweise einfacher formulieren.

Wir wollen nun die Operationen der Addition und Multiplikation in $A[x]$ definieren. Es sei

$$\alpha = (a_0, a_1, ..., a_i, ...), \qquad \beta = (b_0, b_1, ..., b_i, ...).$$

Dann setzen wir

$$\alpha+\beta:=(a_0+b_0, a_1+b_1, ..., a_i+b_i, ...),$$
$$\alpha\cdot\beta:=(c_0, c_1, ..., c_i, ...) \quad \text{mit} \quad c_i:=\sum_{k+l=i} a_k b_l . \tag{1}$$

Man beweist leicht, daß $\alpha+\beta$, $\alpha\cdot\beta$ wieder Polynome sind.

Satz 1. *Es sei A ein Integritätsbereich. Die Menge $A[x]$ mit den durch* (1) *definierten Operationen ist dann wieder ein Integritätsbereich. Die Teilmenge der Polynome der Form $(a, 0, 0, ..., 0, ...)$, $a\in A$, ist ein zu A isomorpher Unterring von $A[x]$. Es gilt*

$$\operatorname{gr}(\alpha+\beta)\leqq\max(\operatorname{gr}\alpha, \operatorname{gr}\beta) \qquad (\alpha, \beta, \alpha+\beta\neq 0), \tag{2}$$

$$\operatorname{gr}(\alpha\cdot\beta)=\operatorname{gr}\alpha+\operatorname{gr}\beta \qquad (\alpha, \beta\neq 0). \tag{3}$$

Beweis. Man bemerkt sofort, daß $[A[x], +]$ eine abelsche Gruppe mit dem Polynom 0 als Nullelement ist. Die Kommutativität der Multiplikation ist ebenfalls leicht einzusehen. Wir beweisen die Assoziativität. Es seien α, β wie oben und $\gamma=(c_0, c_1, ..., c_i, ...)$. Wir setzen $(\alpha\beta)\gamma=(u_0, u_1, ...)$, $\alpha(\beta\gamma)=(v_0, v_1, ...)$. Nach (1) gilt

$$u_r=\sum_{l+k=r}\Big(\sum_{i+j=l} a_i b_j\Big)c_k=\sum_{i+j+k=r} a_i b_j c_k=\sum_{i+m=r} a_i \sum_{j+k=m} b_j c_k=v_r .$$

Der Beweis der Distributivität ist trivial. Somit ist $A[x]$ ein assoziativer, kommutativer Ring. Man prüft leicht nach, daß $(e, 0, ..., 0, ...)$ sein Einselement ist und daß die Abbildung $f: a\in A\mapsto(a, 0, ..., 0, ...)\in A[x]$ ein injektiver Homomorphismus ist, der A isomorph auf den im Satz angegebenen Unterring abbildet.

Die Verifikation von (2) ist trivial, wir beweisen (3). Es seien α, β und $\alpha\cdot\beta=(c_0, c_1, ..., c_i, ...)$ wie in (1) definiert, $n=\operatorname{gr}\alpha$, $m=\operatorname{gr}\beta$. Nach Definition (1) gilt $c_k=0$ für $k>n+m$, da in jedem Summanden von c_k wenigstens ein Faktor 0 ist. Weiter folgt $c_{n+m}=a_n\cdot b_m\neq 0$; denn A enthält keine Nullteiler. Somit ist $\operatorname{gr}\alpha\cdot\beta=m+n$. Hieraus folgt aber auch $\alpha\cdot\beta\neq 0$ für $\alpha\neq 0$ und $\beta\neq 0$, so daß $A[x]$ ebenfalls keine Nullteiler hat. □

Im weiteren werden wir das Element $a\in A$ mit dem Polynom

$$f(a)=(a, 0, ..., 0, ...)$$

identifizieren, so daß $A\subset A[x]$ ein Unterring ist. Wir bemerken noch, daß man den Ring $A[x]$ ebenso ausgehend von einem beliebigen Ring A definieren kann. Dann impliziert die Kommutativität, Assoziativität, Existenz eines Einselements bzw. Nullteilerfreiheit von A die entsprechende Eigenschaft des *Polynomringes* $A[x]$.

Folgerung 1. *Es gilt $A[x]^*=A^*$.*

Beweis. Da das Einselement $e\in A$ auch Einselement von $A[x]$ ist, gilt $A^*\subseteqq A[x]^*$. Es sei nun $\alpha\in A[x]^*$. Dann existiert ein $\alpha^{-1}\in A[x]$, so daß $\alpha\alpha^{-1}=e$ gilt. Aus (3) folgt $\operatorname{gr}\alpha+\operatorname{gr}\alpha^{-1}=\operatorname{gr} e=0$, und daher muß $\operatorname{gr}\alpha=0$, also $\alpha\in A$ sein; offenbar ist dann auch $\alpha\in A^*$. □

Wir definieren nun die *Unbestimmte* x durch

$$x := (0, e, 0, ..., 0, ...) .$$

Es gilt

$$x^k = (d_{0k}, d_{1k}, ..., d_{ik}, ...)$$

mit

$$d_{ik} = \begin{cases} 0 & \text{für } i \neq k, \\ e & \text{für } i = k \end{cases} \qquad i, k \in \mathbf{N} .$$

Zunächst gilt das für $k = 1$ wegen $x = x^1$, für $k > 1$ beweist man es durch vollständige Induktion nach k. Setzen wir schließlich noch

$$x^0 := e ,$$

so können wir jedes Polynom $\alpha = (a_0, a_1, ..., a_n, 0, ...)$ vom Grad $\operatorname{gr} \alpha \leqq n$ in der üblichen Form

$$\alpha = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + ... + a_n x^n \tag{4}$$

schreiben. Verlangen wir noch $\operatorname{gr} \alpha = n$, d. h. $a_n \neq 0$, so ist die Schreibweise (4) durch α eindeutig bestimmt. Im weiteren werden wir diese Bezeichnung benutzen. Die oben gegebenen Definitionen für die Addition und Multiplikation der Polynome sind weiter nichts als die bekannten Rechenregeln der Elementarmathematik für Ausdrücke der Gestalt (4).

Übung 1. Wir bezeichnen mit $A[[x]]$ die Menge aller Folgen $\alpha = (a_0, a_1, ..., a_i, ...)$ mit $a_i \in A$, A ein Integritätsbereich. Man beweise, daß die Operationen (1) $A[[x]]$ in einen Integritätsbereich verwandeln, der $A[x]$ als Unterring enthält. Ein Element $\alpha \in A[[x]]$ ist invertierbar genau dann, wenn $a_0 \in A^*$ gilt. $A[[x]]$ heißt der *Ring der formalen Potenzreihen über* A; seine Elemente schreibt man gewöhnlich in der Form

$$\alpha = \sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + ... + a_k x^k + ...$$

Wir wollen nun einige wichtige Eigenschaften der Polynomringe beweisen.

Satz 2 (Satz über die Division mit Rest). *Es sei A ein Integritätsbereich und $\alpha, \beta \in A[x]$, $\beta = b_0 + b_1 x + ... + b_n x^n$, $b_n \in A^*$. Dann existieren Polynome $\gamma, \delta \in A[x]$, so daß*

$$\alpha = \beta\gamma + \delta \quad \text{mit} \quad \delta = 0 \quad \text{oder} \quad \operatorname{gr} \delta < \operatorname{gr} \beta = n \tag{5}$$

gilt; die Polynome γ, δ sind hierdurch eindeutig bestimmt.

Beweis. Wir beweisen zuerst die Existenz einer Darstellung (5). Ist $\alpha = 0$, so kann man offenbar $\gamma = \delta = 0$ setzen. Für $\alpha \neq 0$ führen wir den Beweis durch Induktion nach $\operatorname{gr} \alpha$; dabei denken wir uns β fest. Angenommen, für alle α mit $\operatorname{gr} \alpha < m$ sei die Existenz bereits bewiesen. Es sei $\operatorname{gr} \alpha = m$ und $\alpha = a_0 + a_1 x + ... + a_m x^m$. Gilt $m < n$, so setzen wir einfach $\gamma = 0$, $\delta = \alpha$. Falls $m \geqq n$ ist, betrachten wir das Polynom

$$\tilde{\alpha} = \alpha - (a_m / b_n)\, x^{m-n} \beta .$$

Offenbar gilt $\operatorname{gr}\tilde{\alpha}<m$. Nach Induktionsannahme gibt es $\tilde{\gamma}, \tilde{\delta}\in A[x]$ mit $\tilde{\alpha}=\beta\tilde{\gamma}+\tilde{\delta}, \tilde{\delta}=0$ oder $\operatorname{gr}\tilde{\delta}<n$. Hieraus erhalten wir

$$\alpha=\tilde{\alpha}+(a_m/b_n)\,x^{m-n}\beta=\beta\,(\tilde{\gamma}+(a_m/b_n)\,x^{m-n})+\tilde{\delta}\,.$$

Setzen wir nun $\gamma=\tilde{\gamma}+(a_m/b_n)\,x^{m-n}$, $\delta=\tilde{\delta}$, so resultiert (5).

Wir zeigen nun die Eindeutigkeit der Darstellung. Angenommen, außer (5) gelte noch $\alpha=\beta\gamma_1+\delta_1$ mit $\delta_1=0$ oder $\operatorname{gr}\delta_1<n$. Dann folgt $\delta-\delta_1=\beta\,(\gamma_1-\gamma)$. Ist $\gamma_1=\gamma$, so folgt $\delta=\delta_1$. Gilt $\gamma_1\neq\gamma$, so ist $\operatorname{gr}(\beta\,(\gamma_1-\gamma))\geqq\operatorname{gr}\beta=n$ nach (3), während nach (2) $\operatorname{gr}(\beta\,(\gamma_1-\gamma))=\operatorname{gr}(\delta-\delta_1)<n$ gelten müßte, so daß wir einen Widerspruch bekämen. □

Definition 2. Das Polynom δ aus der Darstellung (5) heißt der *Rest* und das Polynom γ der *Quotient* bei Division von α durch β.

Offensichtlich gilt $\beta\mid\alpha$ genau dann, wenn $\delta=0$ gilt. Man bemerkt, daß der Beweis von Satz 2 einen Algorithmus zur Berechnung von γ und δ enthält, nämlich das aus der Elementarmathematik bekannte Verfahren zur Division zweier Polynome. Ist $\beta=x-c$, $c\in A$, so kann man die Division auch nach dem *Hornerschen Schema* durchführen, das wir nun beschreiben wollen.

Satz 3. *Es sei* $\alpha=a_0x^n+a_1x^{n-1}+\ldots+a_n$ *und* $\beta=x-c$, a_i, c *Elemente des Integritätsbereiches* A. *Dann lassen sich die Koeffizienten des Quotienten* $\gamma=c_0x^{n-1}+c_1x^{n-2}+\ldots+c_{n-1}$ *und der Rest* $r\in A$ *rekursiv nach den folgenden Formeln berechnen:*

$$\left.\begin{aligned} &c_0=a_0,\\ &c_1=cc_0+a_1,\\ &\cdots\cdots\cdots\cdots\\ &c_{n-1}=cc_{n-2}+a_{n-1},\\ &r=cc_{n-1}+a_n\,. \end{aligned}\right\} \tag{6}$$

Beweis. Nach Satz 2 gibt es eine Darstellung

$$\alpha=(x-c)\,\gamma+\delta \tag{7}$$

mit $\delta=0$ oder $\operatorname{gr}\delta=0$. Somit gilt $\delta=r\in A$. Vergleichen wir die Koeffizienten auf der rechten und linken Seite von (7) – man beachte die von (4) abweichende, ebenfalls gebräuchliche Numerierung der Koeffizienten –, so erhalten wir

$$\begin{aligned} &a_0=c_0\,,\\ &a_i=c_i-cc_{i-1}\qquad(i=1,\ldots,n-1)\,,\\ &a_n=r-cc_{n-1}\,, \end{aligned}$$

woraus (6) folgt. □

Wir wollen nun die Polynome von einem anderen Gesichtspunkt aus betrachten. Jedem Polynom $\alpha\in A[x]$ werden wir eine Funktion $c\in A\mapsto\alpha(c)\in A$ zuordnen; allerdings ist diese Zuordnung im allgemeinen weder injektiv noch surjektiv, speziell können verschiedene Polynome dieselbe Funktion ergeben (vgl. Beispiel 1 weiter unten).

Definition 3. Es sei $\alpha = a_0 + a_1 x + \ldots + a_n x^n \in A[x]$ und $c \in A$. Das Element

$$\alpha(c) := a_0 + a_1 c + \ldots + a_n c^n \in A$$

heißt der *Wert des Polynoms α an der Stelle c*. Ein Element $c \in A$ heißt eine *Nullstelle* des Polynoms α oder eine *Wurzel* der Gleichung $\alpha(x) = 0$, wenn $\alpha(c) = 0$ gilt.

Satz 4. *Es sei $c \in A$ fest. Dann ist die Abbildung $\alpha \in A[x] \mapsto \alpha(c) \in A$ ein Ringhomomorphismus von $A[x]$ auf A, dessen Einschränkung auf $A \subset A[x]$ die Identität ergibt.*

Beweis. Es ist zu zeigen, daß für beliebige $\alpha, \beta \in A[x]$ die Gleichungen

$$(\alpha + \beta)(c) = \alpha(c) + \beta(c), \qquad (\alpha\beta)(c) = \alpha(c) \cdot \beta(c)$$

gelten. Es seien $\alpha = \sum_i a_i x^i$, $\beta = \sum_j b_j x^j$. Die erste Beziehung ist trivial. Wir zeigen die zweite, die unmittelbar aus (1) folgt:

$$\alpha\beta(c) = \sum_k \Big(\sum_{i+j=k} a_i b_j \Big) c^k = \sum_{i,j} a_i b_j c^{i+j} = \Big(\sum_i a_i c^i \Big) \Big(\sum_j b_j c^j \Big) = \alpha(c)\, \beta(c) .$$

Die letzte Behauptung ist offensichtlich. □

Bemerkung. Satz 4 gilt für jeden assoziativen, kommutativen Ring A.

Satz 5 (Theorem von Bezout). *Es sei A ein Integritätsbereich, $\alpha \in A[x]$, $c \in A$. Dann ist der Wert $\alpha(c)$ gleich dem Rest von α bei Division durch $x - c$. Das Element c ist eine Nullstelle von α dann und nur dann, wenn $x - c \mid \alpha$ gilt.*

Beweis. Nach Satz 2 gilt (7) mit $\delta = r \in A$. Setzen wir hier $x = c$ ein, d. h., bestimmen wir auf der rechten und linken Seite den Wert des Polynoms an der Stelle c, so folgt aus Satz 4 $\alpha(c) = (c - c)\, \gamma(c) + \delta(c) = r$. Daher gilt $\alpha(c) = 0$ genau dann, wenn $r = 0$ ist, d. h., wenn $x - c \mid \alpha$ gilt. □

Definition 4. Die natürliche Zahl $k \in \mathbf{N}$ heißt *Vielfachheit der Nullstelle c des Polynoms α*, wenn $(x - c)^k \mid \alpha$ und $(x - c)^{k+1} \nmid \alpha$ gilt. Ist die Vielfachheit $k > 1$, so heißt c eine *mehrfache* und im Fall $k = 1$ eine *einfache* Nullstelle von α; formal zweckmäßig ist es, c eine Nullstelle der Vielfachheit 0 von α zu nennen, wenn $\alpha(c) \neq 0$ ist.

Es ist klar, daß für die Vielfachheit k einer Nullstelle von $\alpha \neq 0$ stets $k \leqq \operatorname{gr} \alpha$ gilt.

Satz 6. *Ein Element c des Integritätsbereichs A ist Nullstelle der Vielfachheit k des Polynoms α genau dann, wenn*

$$\alpha = (x - c)^k \beta \quad \textit{mit} \quad \beta(c) \neq 0 \tag{8}$$

gilt.

Beweis. Ist c Nullstelle der Vielfachheit k, so folgt aus der Definition, daß ein $\beta \in A[x]$ mit $\alpha = (x - c)^k \beta$ existiert. Wäre $\beta(c) = 0$, so erhielten wir $x - c \mid \beta$, d. h. $(x - c)^{k+1} \mid \alpha$, was nicht möglich ist. Gilt umgekehrt (8), so folgt $(x - c)^k \mid \alpha$, $x - c \nmid \beta$. Würde nun $(x - c)^{k+1}$ das Polynom α teilen, so gäbe es eine Darstellung der Form $\alpha = (x - c)^{k+1} \gamma$. Da $A[x]$ ein Integritätsbereich ist (Satz 1), folgt aus $(x - c)^{k+1} \gamma =$

$=(x-c)^k\beta$, daß $\beta=(x-c)\gamma$ ist (Kürzen durch $(x-c)^k$). Das wäre aber ein Widerspruch zu $\beta(c)\neq 0$. □

Satz 7. *Es sei A ein Integritätsbereich, $\alpha\in A[x]$, $\alpha\neq 0$, und c_i, $i=1, \ldots, r$, seien verschiedene Nullstellen von α; c_i habe die Vielfachheit k_i. Dann gibt es eine Darstellung*

$$\alpha=(x-c_1)^{k_1}\ldots(x-c_r)^{k_r}\beta \tag{9}$$

mit $\beta\in A[x]$, $\beta(c_i)\neq 0$ für $i=1, \ldots, r$. Ferner gilt

$$\sum_{i=1}^{r} k_i\leqq \operatorname{gr}\alpha;$$

ein Polynom $\alpha\neq 0$ kann also höchstens $\operatorname{gr}\alpha$ verschiedene Nullstellen besitzen.

Beweis. Wir führen den Beweis von Satz 7 durch Induktion nach r. Der Fall $r=1$ ist durch Satz 6 erledigt. Die Behauptung sei bereits für $r-1$ verschiedene Nullstellen bewiesen. Dann gilt

$$\alpha=(x-c_1)^{k_1}\ldots(x-c_{r-1})^{k_{r-1}}\bar{\beta},\qquad \bar{\beta}(c_i)\neq 0\qquad \text{für } i=1, \ldots, r-1\,.$$

Aus Satz 4 folgt

$$0=\alpha(c_r)=(c_r-c_1)^{k_1}\ldots(c_r-c_{r-1})^{k_{r-1}}\bar{\beta}(c_r)\,,$$

und da die Nullstellen alle verschieden sind, ergibt sich $\bar{\beta}(c_r)=0$. Es sei l die Vielfachheit der Nullstelle c_r für $\bar{\beta}$, d. h. $\bar{\beta}=(x-c_r)^l\beta$, $\beta(c_r)\neq 0$. Offenbar gilt auch $\beta(c_i)\neq 0$ für $i=1, \ldots, r-1$. Es bleibt $l=k_r$ zu zeigen. Jedenfalls gilt $\alpha=(x-c_r)^{k_r}\gamma$ mit $(x-c_r)\nmid\gamma$, also auch

$$(x-c_r)^{k_r}\gamma=(x-c_1)^{k_1}\ldots(x-c_{r-1})^{k_{r-1}}(x-c_r)^l\beta\,.$$

Da k_r die Vielfachheit der Nullstelle c_r ist, muß $l\leqq k_r$ gelten; wäre nun $l<k_r$, so kürzen wir die Gleichung durch $(x-c_r)^l$ und erhalten aus $(x-c_r)^{k_r-l}\gamma=(x-c_1)^{k_1}\ldots$ $\ldots(x-c_{r-1})^{k_{r-1}}\beta$ nach Einsetzen von c_r den Widerspruch $\beta(c_r)=0$. Damit ist (9) bewiesen. Aus (3) folgt

$$\operatorname{gr}\alpha=\sum_{i=1}^{r}k_i+\operatorname{gr}\beta\geqq\sum_{i=1}^{r}k_i\,.\quad\square$$

Folgerung 2. *Es sei A ein Integritätsbereich $\alpha, \beta\in A[x]$ und $r>\max(\operatorname{gr}\alpha, \operatorname{gr}\beta)$. Wenn r verschiedene Elemente $c_1, \ldots, c_r\in A$ existieren, für die $\alpha(c_i)=\beta(c_i)$, $i=1, \ldots, r$, gilt, ist $\alpha=\beta$.*

Beweis. Wir betrachten $\gamma=\alpha-\beta$. Nach Satz 4 gilt $\gamma(c_i)=0$ für $i=1, \ldots, r$. Daher muß $\gamma=0$ sein; denn sonst wäre $\operatorname{gr}\gamma\leqq\max(\operatorname{gr}\alpha, \operatorname{gr}\beta)<r$ und wir erhielten einen Widerspruch zu Satz 7. □

Folgerung 3. *Für einen unendlichen Integritätsbereich A ist die Abbildung $A[x]\to M(A)$, die jedem $\alpha\in A[x]$ die entsprechende Funktion $c\in A\mapsto\alpha(c)\in A$ zuordnet, injektiv.*

Beweis. Wenn $\alpha(c)=\beta(c)$ für alle $c\in A$ gilt, gilt diese Gleichung speziell für $r>\max(\operatorname{gr}\alpha, \operatorname{gr}\beta)$ Elemente, da ja A unendlich ist, und die Behauptung ergibt sich aus Folgerung 2. □

Betrachtet man $M(A)$ nach Beispiel 1.2 als Funktionenring, so erkennt man mit Hilfe von Satz 4 sofort, daß die in Folgerung 3 definierte Abbildung ein injektiver Ringhomomorphismus ist, der $A[x]$ in $M(A)$ einbettet.

Beispiel 1. Das folgende Beispiel zeigt, daß im Fall eines endlichen Ringes A ein Polynom nicht eindeutig durch die ihm entsprechende Funktion bestimmt wird: Es sei $A=\{c_1, ..., c_k\}$. Dann ist $\alpha_0=(x-c_1)\dots(x-c_k)\neq 0$, während $\alpha_0(c)=0$ für alle $c\in A$ gilt. Für $A=\mathbf{Z}_2$ gilt beispielsweise $\alpha_0=x^2-x=x^2+x$.

Übung 2. Man beweise, daß für einen endlichen Integritätsbereich A der Kern des oben betrachteten Ringhomomorphismus $A[x]\to M(A)$ gleich der Menge $\alpha_0 A[x]$ aller durch α_0 teilbaren Polynome ist.

Übung 3. Man zeige, daß jeder Ringhomomorphismus $f: A[x]\to A$ mit $f\mid A=\mathrm{id}_A$ von der Form $f(\alpha)=\alpha(c)$ ist, wobei $c\in A$ ein festes Element ist.

In der nächsten Übung, deren Durchführung wir dem Leser sehr empfehlen, behandeln wir zwei wichtige, klassische Interpolationsformeln.

Übung 4. Es sei A ein Körper, und $c_0, c_1, ..., c_n$ seien $n+1$ verschiedene Elemente aus A, ferner seien b_i, $i=0, 1, ..., n$, Elemente aus A. Man beweise: Es gibt ein Polynom $\alpha\in A[x]$ mit $\alpha(c_i)=b_i$ für $i=0, 1, ..., n$. (Hinweis. a) Eine Lösung stellt die *Interpolationsformel von Lagrange* dar:

$$\alpha=\sum_{i=0}^{n} b_i \frac{(x-c_0)(x-c_1)\dots(x-c_{i-1})(x-c_{i+1})\dots(x-c_n)}{(c_i-c_0)(c_i-c_1)\dots(c_i-c_{i-1})(c_i-c_{i+1})\dots(c_i-c_n)}.$$

b) Ein anderes Interpolationsverfahren geht von der *Newtonschen Interpolationsformel* aus:

$$\alpha=r_0+r_1(x-c_0)+r_2(x-c_0)(x-c_1)+\dots+r_n(x-c_0)(x-c_1)\dots(x-c_{n-1}),$$

für die die Koeffizienten rekursiv durch sukzessives Auswerten der Bedingung $\alpha(c_i)=b_i$ zu bestimmen sind. Aus $\alpha(c_0)=b_0$ folgt durch Einsetzen von $x=c_0$ sofort $r_0=b_0$. Sind $r_0, r_1, ..., r_{i-1}$ bereits bestimmt, so erhält man r_i sofort aus

$$\alpha(c_i)=b_i=r_0+r_1(c_i-c_0)+r_2(c_i-c_0)(c_i-c_1)+\dots+r_i(c_i-c_0)\dots(c_i-c_{i-1}).$$

Die angegebenen Interpolationsformeln haben wichtige Anwendungen in der numerischen Mathematik. Mit ihrer Hilfe läßt sich ein Polynom vom Grad $\leq n$ bestimmen, das für die Argumente $c_0, c_1, ..., c_n$ dieselben Werte wie eine Funktion φ annimmt, die nur an diesen Stellen bekannt ist. Man kann dann die Funktion φ mit einer gewissen Genauigkeit durch das Interpolationspolynom α ersetzen. Dieses Verfahren nennt man auch *parabolische Interpolation*.)

Wir wenden uns nun wieder Satz 7 zu und betrachten den Fall, daß $\sum_{i=1}^{r} k_i=\operatorname{gr}\alpha$ ist; nach (3) muß dann für den Faktor β aus (9) $\operatorname{gr}\beta=0$ gelten, d. h. $\beta=a\in A$. Dann wird α vollständig in *Linearfaktoren* $x-c_i$ zerlegt:

$$\alpha=a(x-c_1)^{k_1}\dots(x-c_r)^{k_r}, \qquad a\in A; \tag{10}$$

man nennt A in diesem Fall einen *Zerfällungsring* für das Polynom α. Wir wollen zeigen, daß die Zerlegung (10) bis auf die Reihenfolge der Faktoren eindeutig be-

stimmt ist. In der Tat, ist

$$\alpha = b\,(x-d_1)^{l_1} \dots (x-d_s)^{l_s} \tag{11}$$

irgendeine Zerlegung von α in Linearfaktoren, wobei $b, d_i \in A$ gilt und $d_1, \dots, d_s$ verschiedene Elemente sind, so ist d_i eine Nullstelle von α, muß also unter den c_j vorkommen. Setzen wir $\gamma_i := \alpha/(x-d_i)^{l_i}$, so gilt $\gamma_i(d_i) \neq 0$, d. h., l_i ist gleich der Vielfachheit von d_i. Das geht aber nur, wenn die Faktoren in (10) und (11) sich höchstens in der Reihenfolge unterscheiden. Betrachten wir noch die übliche Darstellung

$$\alpha = a_0 + a_1 x + \dots + a_n x^n$$

von α, $n = \operatorname{gr} \alpha$, so ergibt der Vergleich der höchsten Koeffizienten $a_n = a = b$, womit die Eindeutigkeit von (10) bewiesen ist. Es zeigt sich, daß man statt (10) auch

$$\alpha = a_n\,(x-c_1)^{k_1} \dots (x-c_r)^{k_r} \tag{12}$$

schreiben kann. Eine andere, oft nützliche Darstellung erhält man folgendermaßen: Es sei $b_1, \dots, b_n$ eine Folge von Nullstellen von α aus einem Zerfällungsring A, wobei in dieser Folge der Wert jeder Nullstelle von α so oft auftritt, wie ihre Vielfachheit angibt. Dann wird aus (12)

$$\alpha = a_n\,(x-b_1) \dots (x-b_n), \qquad a_n \in A,\ a_n \neq 0\,. \tag{13}$$

Satz 8 (Satz von VIETA). *Es sei A ein Zerfällungsring des Polynoms $\alpha = a_0 + a_1 x + \dots + a_n x^n$. Ist dann $b_1, \dots, b_n$ eine Folge von Nullstellen von α, in der jede Nullstelle so oft vorkommt, wie ihre Vielfachheit angibt, so gilt*

$$\left.\begin{aligned}
&a_{n-1} = -a_n\,(b_1 + \dots + b_n),\\
&a_{n-2} = a_n\,(b_1 b_2 + b_1 b_3 + \dots + b_{n-1} b_n),\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
&a_k = (-1)^{n-k} a_n\,(b_1 b_2 \dots b_{n-k} + b_1 b_2 \dots b_{n-k-1} b_{n-k+1}\\
&\qquad + \dots + b_{k+1} b_{k+2} \dots b_n),\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
&a_0 = (-1)^n a_n b_1 \dots b_n\,.
\end{aligned}\right\} \tag{14}$$

Der Beweis ergibt sich leicht durch Koeffizientenvergleich aus (13). □

Zum Abschluß dieses Paragraphen wollen wir noch die „Taylor-Entwicklung" eines Polynoms und den damit zusammenhängenden Begriff der Ableitung betrachten.

Satz 9. *Es sei A ein Integritätsbereich, $c \in A$ und $\alpha \in A[x]$. Dann gibt es eine und nur eine Darstellung von α in der Form*

$$\alpha = b_0 + b_1\,(x-c) + \dots + b_n\,(x-c)^n \tag{15}$$

mit $n = \operatorname{gr} \alpha$, $b_i \in A$.

Beweis. Die Existenz einer Zerlegung (15) beweisen wir durch vollständige Induktion nach $\operatorname{gr} \alpha$. Für $\alpha = 0$ oder $\operatorname{gr} \alpha = 0$ ist die Behauptung trivial. Angenom-

men, sie sei schon für alle Polynome vom Grade $\leqq n-1$ bewiesen, und es sei gr $\alpha = n$. Nach Satz 2 gibt es eine Darstellung $\alpha = (x-c)\,\beta + b_0$ mit $b_0 \in A$. Dann gilt gr $\beta = n-1$ (nach Satz 1), und wir können für β eine Darstellung der Form (15) finden:

$$\beta = b_1 + b_2\,(x-c) + \ldots + b_n\,(x-c)^{n-1}$$

mit $b_i \in A$. Hieraus folgt (15). Die Eindeutigkeit beweisen wir ebenfalls durch Induktion nach gr α. Ist α in der Form (15) dargestellt, so folgt wieder $\alpha = (x-c)\,\beta + b_0$, β wie oben. Nach Satz 2 sind β und b_0 durch α und c eindeutig bestimmt. Aus der Induktionsvoraussetzung folgt dann, daß die b_i, $i = 1, \ldots, n$, ebenfalls eindeutig bestimmt sind. □

Aus dem Beweis von Satz 9 ist ersichtlich, daß man die Koeffizienten b_i als Folge der Reste bei der Teilung von α durch $x-c$, dann bei Division des Quotienten β dieser Teilung durch $x-c$ usw. erhalten kann. Diese Divisionen lassen sich mittels des Hornerschen Schemas ausführen (Satz 3).

Folgerung 4. *Ein Element c des Integritätsbereiches A ist Nullstelle der Vielfachheit k des Polynoms $\alpha \in A[x]$, wenn in der Darstellung* (15) $b_0 = b_1 = \ldots = b_{k-1} = 0$ *und* $b_k \neq 0$ *gilt.* □

Definition 5. Unter der *Ableitung* α' des Polynoms

$$\alpha = \sum_{i \geqq 0} a_i x^i = a_0 + a_1 x + \ldots + a_n x^n$$

versteht man das Polynom

$$\alpha' := \sum_{i>0} i a_i x^{i-1} = a_1 + 2a_2 x + \ldots + n a_n x^{n-1}\,.$$

Wir setzen rekursiv $\alpha^{(i)} := \alpha^{(i-1)'}$, $\alpha^{(0)} := \alpha$ und nennen $\alpha^{(i)}$ die *i-te Ableitung* von α ($i \in \mathbf{N}_0$).

Satz 10. *Die Ableitung eines Polynoms hat folgende Eigenschaften:*

1. $(\alpha+\beta)' = \alpha' + \beta'$;
2. $(\alpha\beta)' = \alpha'\beta + \alpha\beta'$;
3. $(\alpha^k)' = k\alpha^{k-1}\alpha'$;
4. *Gilt* gr $\alpha > 0$, *so ist* gr $\alpha' \leqq (\text{gra}\ \alpha) - 1$ *oder* $\alpha' = 0$; *falls* char $A = 0$ *ist, gilt stets* gr $\alpha' = (\text{gr}\ \alpha) - 1$.

Beweis. Die Behauptung 1 ist trivial. Zum Beweis der zweiten Behauptung setzen wir $\alpha = \sum_i a_i x^i$, $\beta = \sum_j b_j x^j$. Dann gilt

$$\begin{aligned}(\alpha\beta)' &= \sum_{k>0} k \Big(\sum_{i+j=k} a_i b_j \Big) x^{k-1} = \sum_{k>0} \Big(\sum_{i+j=k} (i+j)\, a_i b_j \Big) x^{k-1} \\ &= \sum_{k>0} \Big(\sum_{i+j=k} i a_i b_j \Big) x^{k-1} + \sum_{k>0} \Big(\sum_{i+j=k} a_i j b_j \Big) x^{k-1} = \alpha'\beta + \alpha\beta'.\end{aligned}$$

Die Eigenschaft 3 erhält man leicht aus der Eigenschaft 2 durch vollständige Induktion. Schließlich folgt die Eigenschaft 4 aus Übung 1.5. □

Satz 11: *Für einen Integritätsbereich* A, $\alpha \in A[x]$, $c \in A$ *betrachten wir die Darstellung* (15). *Dann gilt*

$$\alpha^{(k)}(c) = k!\, b_k \qquad (k = 0, 1, \ldots). \tag{16}$$

Das Element c *ist mehrfache Wurzel von* α *genau dann, wenn* $\alpha(c) = \alpha'(c) = 0$ *gilt. Ist* $\operatorname{char} A = 0$, *so ist* c *Nullstelle der Vielfachheit* l *von* α *dann und nur dann, wenn* $\alpha^{(k)}(c) = 0$ *für* $k = 0, 1, \ldots, l-1$ *und* $\alpha^{(l)}(c) \neq 0$ *gilt. Ist* A *sogar ein Körper mit* $\operatorname{char} A = 0$, *so kann man* (15) *auch folgendermaßen schreiben:*

$$\alpha = \alpha(c) + \frac{\alpha'(c)}{1!}(x-c) + \ldots + \frac{\alpha^{(n)}(c)}{n!}(x-c)^n. \tag{17}$$

Beweis. Die Formel (16) ergibt sich leicht durch sukzessive Differentiation von (15) unter Anwendung von Satz 10. Die Behauptungen über die Vielfachheiten ergeben sich aus Folgerung 4. □

Die Formel (17) heißt die *Taylor-Entwicklung* des Polynoms α an der Stelle c.

§ 5. Euklidische Ringe

In diesem Paragraphen betrachten wir eine Klasse von Integritätsbereichen, in denen es ein Analogon der Division mit Rest gibt, die wir für die ganzen Zahlen und die Polynomringe über beliebigen Körpern bereits kennen. Viele Sätze der elementaren Arithmetik gelten in derartigen Ringen.

Definition 1. Ein Integritätsbereich A heißt ein *euklidischer Ring*, wenn für ihn eine Funktion $w: A \setminus \{0\} \to \mathbf{N}_0$ gegeben ist, die die folgenden Eigenschaften besitzt:

1. Sind $a, b \in A$ und ist $b \neq 0$, so gibt es Elemente $c, r \in A$ mit $a = bc + r$, wobei $r = 0$ oder $w(r) < w(b)$ gilt;

2. ist $b \neq 0$ und $a \mid b$, so gilt $w(a) \leqq w(b)$.

Beispiel 1. Es sei $A = \mathbf{Z}$. Wir setzen $w(a) := |a|$. Die Eigenschaft 1 folgt aus dem bekannten Satz über die *Division mit Rest* für die ganzen Zahlen, den man folgendermaßen formulieren kann: Sind $a, b \in \mathbf{Z}$ und gilt $b \neq 0$, so existieren (eindeutig bestimmte) Zahlen $c, r \in \mathbf{Z}$ mit $a = bc + r$, wobei $0 \leqq r < |b|$ gilt. Die Eigenschaft 2 ist offenbar erfüllt.

Beispiel 2. Es sei $A = K[x]$, K ein beliebiger Körper. Wir definieren für $\alpha \in K[x]$, $\alpha \neq 0$: $w(\alpha) := \operatorname{gr} \alpha$. Die Eigenschaft 1 folgt aus Satz 4.2, die Eigenschaft 2 aus Satz 4.1, (3).

Beispiel 3. Ein beliebiger Körper ist ein euklidischer Ring; es genügt, $w(a) := 1$ für $a \in K^*$ zu setzen.

Übung 1. Es sei A der Ring der *ganzen Gaußschen Zahlen*, d. h. der Unterring der Zahlen der Gestalt $a + bi$, $a, b \in \mathbf{Z}$, von $\mathbf{C}$. Wir definieren $w(z) := |z|^2$ für $z \in A$. Man zeige, daß A ein euklidischer Ring ist.

Übung 2. Man zeige, daß die Existenz eines Einselementes aus den übrigen Axiomen eines euklidischen Ringes folgt.

Satz 1. *Es sei A ein euklidischer Ring. Dann gibt es für beliebige Elemente $a, b \in A$ einen ggT.*

Beweis. Ist $a=b=0$, so ist offenbar $0=(0,0)$. Ist etwa $b \neq 0$, dann gilt

$$a = bc_1 + r_1 \quad \text{mit} \quad r_1 = 0 \quad \text{oder} \quad w(r_1) < w(b) .$$

Ist $r_1 \neq 0$, so erhalten wir

$$b = r_1 c_2 + r_2 \quad \text{mit} \quad r_2 = 0 \quad \text{oder} \quad w(r_2) < w(r_1) .$$

Gilt $r_2 \neq 0$, so können wir r_1 durch r_2 teilen und dieses Verfahren fortsetzen. Wir erhalten auf diese Weise eine Folge von Gleichungen

$$\left.\begin{aligned} a &= bc_1 + r_1 , \\ b &= r_1 c_2 + r_2 , \\ r_1 &= r_2 c_3 + r_3 , \\ &\cdots\cdots\cdots \\ r_{k-3} &= r_{k-2} c_{k-1} + r_{k-1} , \\ r_{k-2} &= r_{k-1} c_k + r_k , \end{aligned}\right\} \tag{1}$$

wobei $w(b) > w(r_1) > w(r_2) > \ldots > w(r_{k-1}) > w(r_k)$ gilt, falls $r_k \neq 0$ ist. Da $w(b) \in \mathbf{N}_0$ ist für $b \in A \setminus \{0\}$, muß das Verfahren nach endlich vielen Schritten abbrechen, d. h., einmal muß der Rest gleich 0 sein. Dies sei bei der $(k+1)$-ten Division der Fall, d. h., es gelte

$$r_{k-1} = r_k c_{k+1} . \tag{2}$$

Wir beweisen $r_k = (a, b)$. Nach (2) gilt $r_k \mid r_{k-1}$. Betrachten wir die Folge (1) und wenden Satz 2.4 an, so erhalten wir schrittweise $r_k \mid r_l$ für $l < k$ und schließlich $r_k \mid b$, $r_k \mid a$. Somit ist r_k ein gemeinsamer Teiler. Ist schließlich d irgendein gemeinsamer Teiler von a und b und schreiben wir (1) in der Gestalt

$$\left.\begin{aligned} r_1 &= a - bc_1 , \\ r_2 &= b - r_1 c_2 , \\ r_3 &= r_1 - r_2 c_3 , \\ &\cdots\cdots\cdots \\ r_{k-1} &= r_{k-3} - r_{k-2} c_{k-1} , \\ r_k &= r_{k-2} - r_{k-1} c_k , \end{aligned}\right\} \tag{3}$$

so folgt schrittweise $d \mid r_1, \ldots, d \mid r_k$, womit unsere Behauptung bewiesen ist. □

Das im Beweis von Satz 1 enthaltene Verfahren zur Bestimmung des ggT heißt der *euklidische Algorithmus.*

Folgerung 1. *Es seien $a, b \in A$ und $d=(a, b)$, wobei A ein euklidischer Ring ist. Dann gibt es $u, v \in A$ mit*

$$d = au + bv . \tag{4}$$

Beweis. Nach Satz 2.6 ist d assoziiert zu r_k. Daher genügt es, die Behauptung für r_k zu beweisen. Die letzte der Gleichungen (3) drückt r_k durch r_{k-1} und r_{k-2} aus. Setzen wir für r_{k-1} den Ausdruck aus der darüber stehenden Gleichung ein, so ist r_k aus r_{k-2} und r_{k-1} kombiniert. Durchlaufen wir auf diese Weise die Gleichungen (3) von unten nach oben, so erhalten wir die gesuchte Darstellung der Form (4). □

Satz 2. *Es sei A ein euklidischer Ring, $a, b, c \in A$ und $d=(a, b)$. Wir behaupten: Es gilt $d \mid c$ dann und nur dann, wenn $r, s \in A$ existieren mit*

$$c = ar + bs\,. \tag{5}$$

Gilt hierbei $b \neq 0$, so läßt sich r so wählen, daß $r=0$ oder $w(r) < w(b)$ ist.

Beweis. Aus Satz 2.4 folgt sofort: Wenn r und s existieren, für die (5) gilt, dann gilt auch $d \mid c$. Es sei umgekehrt $d \mid c$ und $c_1 = c/d$. Nach Folgerung 1 gibt es $u, v \in A$ mit (4). Multiplizieren wir (4) mit c_1, so erhalten wir

$$c = auc_1 + bvc_1\,.$$

Daher ist (5) mit $r = uc_1$, $s = vc_1$ erfüllt. Es seien nun r, s beliebig so gewählt, daß (5) gilt. Dann gibt es Elemente $r_1, q \in A$ mit $r = bq + r_1$, wobei $r_1 = 0$ oder $w(r_1) < w(b)$ gilt. Setzen wir die letzte Gleichung in (5) ein, so folgt

$$c = a(bq + r_1) + bs = ar_1 + b(s + aq)\,,$$

womit Satz 2 bewiesen ist. □

Folgerung 2. *Zwei Elemente a, b aus einem euklidischen Ring sind teilerfremd genau dann, wenn es $u, v \in A$ gibt mit $au + bv = e$.* □

Satz 3. *Es sei A ein euklidischer Ring, $a, b, c \in A$, und es gelte $c \mid ab$ und $(a, c) = e$. Dann folgt $c \mid b$.*

Beweis. Nach Folgerung 2 gibt es u und v mit $e = au + cv$. Multiplizieren wir diese Gleichung mit b, so folgt $b = (ab)u + cbv$. Wegen $c \mid ab$ erhalten wir die Behauptung aus Satz 2.4. □

Übung 3. Ein Element $m \in A$ heißt *kleinstes gemeinsame Vielfache* (kgV) von $a, b \in A$, wenn $a \mid m$ und $b \mid m$ und für alle m_1 mit $a \mid m_1$ und $b \mid m_1$ auch $m \mid m_1$ gilt. Man zeige: Ist A ein Integritätsbereich, so ist das kgV bis auf Assoziiertheit eindeutig bestimmt. Wenn A ein euklidischer Ring ist, existiert das kgV m für beliebige Elemente $a, b \in A$, und es gilt $ab \sim m(a, b)$.

Übung 4. Es sei $A = K[x]$, K ein Körper, $w = \mathrm{gr}$. Man beweise: Gilt unter Voraussetzung des zweiten Teiles von Satz 2 $\mathrm{gr}\, c < \mathrm{gr}\, a + \mathrm{gr}\, b$, so gilt auch $\mathrm{gr}\, s < \mathrm{gr}\, a$ oder $s = 0$.

Übung 5. Es seien die Bedingungen des zweiten Teils von Satz 2 erfüllt. Man beweise: Es gibt Elemente $r, s \in A$ so, daß (5) mit $r = 0$ oder $w(r) < w(b/d)$ gilt; ist K ein Körper und $A = K[x]$, so sind r, s hierdurch eindeutig bestimmt.

Wir wollen nun den Beweis dafür ansteuern, daß sich in einem euklidischen Ring jedes Element in Primfaktoren zerlegen läßt. Zur Vorbereitung beweisen wir zunächst Satz 4 und Lemma 1.

Satz 4. *Es seien $p, a_i \in A$ für $i=1, \ldots, s$, A ein euklidischer Ring, p prim, und es gelte $p \mid a_1 \ldots a_s$. Dann gilt auch $p \mid a_i$ für ein i.*

Beweis. Für $s=1$ ist die Behauptung trivial. Angenommen, sie sei schon für $s-1$ Faktoren bewiesen. Nach Satz 2.8 gilt $p \mid a_s$ oder $(p, a_s)=e$. Im ersten Fall sind wir fertig, im zweiten folgt aus Satz 3 $p \mid a_1 \ldots a_{s-1}$. Nach Induktionsvoraussetzung gilt $p \mid a_i$ für ein i mit $1 \leqq i \leqq s-1$. □

Lemma 1. *Es seien a, b von Null verschiedene Elemente des euklidischen Ringes A. Gilt $a \sim b$, so ist $w(a)=w(b)$. Falls $w(a)=w(b)$ und $a \mid b$ gilt, ist $a \sim b$.*

Beweis. Die erste Behauptung ist eine einfache Folgerung aus Bedingung 2 von Definition 1. Es sei nun $a \mid b$ und $w(a)=w(b)$. Wir zeigen, daß dann auch $b \mid a$ gilt, womit nach Satz 2.5 unsere Behauptung bewiesen ist. Dazu betrachten wir die Darstellung $a=bc+r$ mit $c, r \in A$, $r=0$ oder $w(r)<w(b)$. Falls $r \neq 0$ ist, erhalten wir aus $r=a-bc$ die Beziehung $a \mid r$, also $w(b)>w(r) \geqq w(a)$ im Widerspruch zu $w(a)=w(b)$. □

Satz 5 (Satz über die Zerlegung in Primfaktoren). *Es sei A ein euklidischer Ring. Jedes von 0 verschiedene Element $a \in A$ läßt sich als Produkt von Primelementen $p_i \in A$ darstellen:*

$$a=p_1 \ldots p_s . \tag{6}$$

Diese Darstellung ist eindeutig in dem folgenden Sinne: Ist

$$a=q_1 \ldots q_t \tag{7}$$

irgendeine Zerlegung von a in Primelemente q_j, so gilt $s=t$, und nach einer geeigneten Umnumerierung der Elemente q_j gilt $p_i \sim q_i$.

Bemerkung. Gilt $a \in A^*$, so sei $a=ae$ formal als Zerlegung in Primfaktoren verstanden. Wir benutzen die Verabredung, daß ein Produkt aus $s=0$ Faktoren gleich dem Einselement e ist.

Beweis. Die Existenz einer Zerlegung (6) zeigen wir durch Induktion nach $w(a)$. Angenommen, die Existenz sei schon für alle a' mit $w(a')<n$ gezeigt, und es sei $w(a)=n$. Ist a ein Primelement, so ist die Existenz von (6) trivial. Anderenfalls gilt $a=bc$ mit $b, c \notin A^*$. Nach Lemma 1 ist $w(b)<n$, $w(c)<n$, und wir können nach Induktionsvoraussetzung die Elemente b, c in Primfaktoren zerlegen: $b=p_1 \ldots p_r$, $c=p_{r+1} \ldots p_s$. Die Multiplikation dieser Zerlegungen ergibt (6).

Die Eindeutigkeit beweisen wir durch Induktion nach der Anzahl s der Faktoren von (6). Ist $s=1$, so ist a prim, und daher gilt $q_1 \sim a$, $q_2 \ldots q_t \in A^*$ bei geeigneter Numerierung der q_i. Wenn nun ein Element q ein invertierbares Element $c \in A^*$ teilt, muß es selbst invertierbar sein; denn wir haben $e=cc^{-1}=qbc^{-1}$, also $q^{-1}=bc^{-1}$. Da die q_i Primelemente sind, muß also $t=1$ und $a=p_1=q_1$ gelten. Angenommen, die Behauptung sei schon für Zerlegungen (6) mit $s-1$ Faktoren bewiesen. Aus (6) und (7) folgt $p_s \mid q_1 \ldots q_t$. Nach Satz 4 erhalten wir $p_s \mid q_t$ bei geeigneter Numerierung der Elemente q_j. Da $p_s \notin A^*$ und q_t prim ist, gilt $p_s \sim q_t$, also $q_t=p_s c$ mit $c \in A^*$.

Kürzen wir die Gleichung $p_1 \dots p_{s-1} p_s = q_1 \dots (q_{t-1} c)\, p_s$ durch p_s, so folgt $p_1 \dots p_{s-1} = q_1 \dots (q_{t-1} c)$. Weil nun $q_{t-1} c$ prim ist, können wir auf diese Zerlegungen die Induktionsvoraussetzung anwenden. Wir erhalten $t-1 = s-1$ und $p_i \sim q_i$ nach einer geeigneten Umnumerierung. □

Beispiel 4. Es sei A die Menge aller komplexen Zahlen der Form $z = a + b\sqrt{3}\,\mathrm{i}$, $a, b \in \mathbf{Z}$. Man prüft leicht nach, daß A ein Unterring von $\mathbf{C}$ ist; A ist offenbar ein Integritätsbereich. Wir wollen zeigen, daß es in A zwei Elemente gibt, die keinen ggT besitzen, und daß die Primfaktorzerlegung in A nicht eindeutig ist. Daraus folgt speziell, daß A kein euklidischer Ring sein kann. Wie man leicht erkennt, ist $A^* = \{-1, +1\}$ gleich der Menge aller $z \in A$ mit $|z| = 1$. Hieraus folgt: Gilt $z \in A$ und $|z| = 2$, so ist z ein Primelement. Bis auf Assoziierte sind das die Elemente 2 und $1 \pm \sqrt{3}\,\mathrm{i}$. Offenbar gilt $4 = 2 \cdot 2 = (1 + \sqrt{3}\,\mathrm{i})\,(1 - \sqrt{3}\,\mathrm{i})$, und folglich ist 4 nicht eindeutig in Primfaktoren zerlegbar. Die gemeinsamen Teiler der Elemente $z = 4\,(1 + \mathrm{i}\sqrt{3})$, $w = 4\,(1 - \mathrm{i}\sqrt{3})$ sind (bis auf Assoziierte) 2, $1 \pm \mathrm{i}\sqrt{3}$, 4, $2(1 \pm \mathrm{i}\sqrt{3})$. Wegen $2 \nmid 1 \pm \mathrm{i}\sqrt{3}$ besitzen z und w keinen ggT.

Übung 6. Man beweise, daß im Ring A von Beispiel 4 jedes $a \neq 0$ eine Zerlegung in Primfaktoren besitzt.

Übung 7. Es sei P die additive Halbgruppe der Zahlen $a/2^k$ mit $a, k \in \mathbf{N}_0$. Mit A bezeichnen wir den Unterring des Ringes $M(]0,\infty[, \mathbf{R})$ (vgl. Beispiel 1.2), der aus den Funktionen $\sum_{i=1}^{k} a_i x^{p_i}$, $a_i \in \mathbf{R}$, $p_i \in P$, $k \in \mathbf{N}_0$, besteht. Man beweise: a) A ist ein Integritätsbereich. — b) $A^* = \mathbf{R}^*$. — c) Alle Teiler f von $x \in A$ haben die Gestalt $f = a x^p$, $a \in \mathbf{R}^*$, $p \in P$, $p \geqq 1$. — d) Das Element $x \in A$ besitzt keine Zerlegung in Primfaktoren.

Es sei A ein euklidischer Ring, p ein Primelement und $a \in A$, $a \neq 0$. Unter der *Vielfachheit* von p in a verstehen wir diejenige Zahl $k \in \mathbf{N}_0$, für die $p^k \mid a$, aber $p^{k+1} \nmid a$ gilt.

Satz 6. *In einem euklidischen Ring sind folgende Aussagen äquivalent:*

1. *Die Vielfachheit des Primelementes p in a ist k.*
2. *$a = p^k b$, und es gilt $p \nmid b$.*
3. *In der Primfaktorzerlegung von a gibt es genau k Primfaktoren, die zu p assoziiert sind.*

Beweis. Es sei die erste Aussage erfüllt. Dann gilt $a = p^k b$. Wäre $p \mid b$, so hätten wir $p^{k+1} \mid a$, was der Aussage 1 widerspricht. Ist umgekehrt die zweite Aussage wahr, so gilt $p^k \mid a$. Wäre $p^{k+1} \mid a$, so hätten wir $a = p^k b = p^{k+1} c$ mit $c \in A$. Hieraus folgte $p \mid b$, was nicht möglich ist. Somit sind die Aussagen 1 und 2 äquivalent. Wir leiten die dritte Aussage aus der zweiten her. Es gilt $b = p_1 \dots p_s$, wobei die p_i prim sind. Wegen $p \nmid b$ folgt $p_i \not\sim p$ für $i = 1, \dots, s$. Folglich kommen in der Zerlegung $a = p^k p_1 \dots p_s$ genau k zu p assoziierte Faktoren vor. Der Beweis der zweiten Aussage aus der dritten ist trivial. □

Folgerung 3. *Jedes Element a des euklidischen Ringes A, $a \neq 0$, ist in der Form*

$$a = c p_1^{k_1} \dots p_r^{k_r}, \qquad r \geqq 0, \tag{8}$$

darstellbar, wobei $c \in A^*$ gilt, die p_i paarweise nicht assoziierte Primelemente und die k_i ihre Vielfachheiten in a sind. □

Beispiel 5. Aus Beispiel 2.4 folgt, daß im Fall $A = \mathbf{Z}$ in (8) $c = \pm 1$ und (8) die eindeutige Primfaktorzerlegung einer ganzen Zahl ist.

Beispiel 6. Es sei $A = K[x]$, wobei K irgendein Integritätsbereich ist. Ein Polynom $\varphi \in K[x]$ heißt *irreduzibel*, wenn $\operatorname{gr} \varphi > 0$ gilt und φ nicht echt zerlegbar ist, d. h., es gibt keine Darstellung $\varphi = \beta\gamma$ mit $\operatorname{gr} \beta > 0$, $\operatorname{gr} \gamma > 0$. Ist K ein Körper, so ist φ irreduzibel genau dann, wenn φ Primelement des Ringes $K[x]$ ist. Jedes Polynom vom Grad 1 ist irreduzibel. Für $c \in K$ ist die Vielfachheit des irreduziblen Polynoms $x - c$ in einem Polynom $\alpha \in K[x]$ gleich der Vielfachheit der Nullstelle c von α. Ist $\operatorname{gr} \varphi > 1$ und φ irreduzibel, so besitzt φ keine Nullstelle, wie sofort aus dem Satz von Bezout (Satz 4.5) folgt. Ist $\operatorname{gr} \varphi$ gleich 2 oder 3 und ist K ein Körper, so gilt hiervon auch die Umkehrung. Zum Beispiel ist das Polynom $x^2 + 1$ irreduzibel in $\mathbf{R}[x]$, also erst recht in $\mathbf{Q}[x]$ oder in $\mathbf{Z}[x]$. Das Polynom $x^3 - 2$ ist irreduzibel in $\mathbf{Q}[x]$, aber reduzibel in $\mathbf{R}[x]$.

Es sei nun wieder K ein Körper. Ein Polynom $\alpha \in K[x]$ heißt *reduziert*, wenn sein höchster Koeffizient $a_n = e$ ist. Offenbar ist jedes Polynom $\alpha \neq 0$ zu einem eindeutig bestimmten reduzierten Polynom assoziiert. Aus (8) folgt leicht, daß man jedes Polynom vom Grad n in der Form

$$\alpha = a_n p_1^{k_1} \dots p_r^{k_r} \tag{9}$$

darstellen kann, wobei die p_i verschiedene irreduzible reduzierte Polynome und die $k_i \in \mathbf{N}$ sind; diese Darstellung ist bis auf die Reihenfolge der Faktoren eindeutig. Wenn K ein Zerfällungskörper von α ist, stimmt die Zerlegung (9) mit der Darstellung (4.10) überein, deren Eindeutigkeit in § 4 auf andere Art bewiesen wurde.

Übung 8. Man beweise, daß ein euklidischer Ring dann und nur dann ein Körper ist, wenn er keine Primelemente enthält.

Übung 9. Man beweise, daß die Ringe $\mathbf{Z}$ und $K[x]$, K Körper, eine unendliche Menge nicht assoziierter Primelemente enthalten. (Hinweis. Man zeige: Sind $p_1, \dots, p_s \notin A^*$, so gilt $p_i \nmid p_1 \dots p_s + 1$ für $i = 1, \dots, s$.)

Wir wollen nun mit Hilfe der Primfaktoren und ihrer Vielfachheiten ein Teilbarkeitskriterium formulieren.

Satz 7. *Sind a, b von 0 verschiedene Elemente des euklidischen Ringes A, so gilt $a \mid b$ dann und nur dann, wenn für jedes Primelement $p \in A$ die Vielfachheit in a kleiner oder gleich der Vielfachheit in b ist.*

Beweis. Die Notwendigkeit der Bedingung ist klar; denn wenn k die Vielfachheit von p in a ist, gilt $p^k \mid a$, also auch $p^k \mid b$, und daher muß die Vielfachheit in b größer oder gleich k sein. Es sei nun umgekehrt $a = c p_1^{k_1} \dots p_r^{k_r}$. Nach Voraussetzung gilt $b = d p_1^{l_1} \dots p_r^{l_r} p_{r+1}^{l_{r+1}} \dots p_s^{l_s}$ mit $c, d \in A^*$, $k_i \leqq l_i$ für $i = 1, \dots, r$, $l_j > 0$ für $j > r$. Hieraus folgt $b = (d/c)\, a p_1^{l_1 - k_1} \dots p_r^{l_r - k_r} p_{r+1}^{l_{r+1}} \dots p_s^{l_s}$, d. h. $a \mid b$. □

Es sei nun P eine Menge von Primelementen des Ringes A, die aus jeder Klasse assoziierter Primelemente genau einen Vertreter enthält, beispielsweise die Menge aller positiven Primzahlen aus $\mathbf{Z}$ oder die Menge aller reduzierten irreduziblen Polynome aus $K[x]$. Für jedes Element $a \neq 0$ des euklidischen Ringes A bezeichnen wir mit $k_p(a)$ die Vielfachheit von p in a. Dann gilt $k_p(a) = 0$ für fast alle $p \in P$, und wir können statt (8) auch ein *formalunendliches* Produkt schreiben, in dem fast alle Faktoren 1 sind:

$$a = c \prod_{p \in P} p^{k_p(a)} \qquad (a \neq 0, c \in A^*) . \tag{10}$$

Satz 7 lautet dann:

$$a \mid b \leftrightarrow \text{für alle } p \in P \text{ gilt } k_p(a) \leqq k_p(b) .$$

Satz 8. *Es seien a, b von 0 verschiedene Elemente eines euklidischen Ringes. Dann gilt für ihren ggT*

$$(a, b) = \prod_{p \in P} p^{\min\{k_p(a), k_p(b)\}} . \tag{11}$$

Der Beweis folgt unmittelbar aus Satz 7. □

Folgerung 4. *Es gilt $(a, b) = e$ dann und nur dann, wenn a und b keine gemeinsamen Primfaktoren besitzen.* □

Hat der euklidische Ring A die Eigenschaft, daß für jedes $a \neq 0$, $a \in A$ nur endlich viele b mit $w(b) < w(a)$ existieren (z. B. für $A = \mathbf{Z}$ oder $A = K[x]$ für einen endlichen Körper K), so läßt sich aus Satz 8 ein Algorithmus zur Bestimmung des ggT gewinnen.

Übung 10. Man verallgemeinere Satz 8 auf den Fall von endlich vielen Elementen.

Übung 11. Man beweise (vgl. Übung 3)

$$\text{kgV}\,\{a, b\} = \prod_{p \in P} p^{\max\{k_p(a), k_p(b)\}}$$

für a, b aus einem euklidischen Ring A.

Abschließend betrachten wir noch einige spezielle Eigenschaften der Ringe $K[x]$, wenn K ein Körper ist. Ist $L \supseteq K$ eine Erweiterung des Körpers K, so ergibt sich eine natürliche Einbettung des Ringes $K[x]$ in den Ring $L[x]$.

Satz 9. *Ist L Erweiterungskörper von K, so ist $K[x]$ Unterring von $L[x]$. Sind $\alpha, \beta \in K[x]$, $\beta \neq 0$ und $\beta \mid \alpha$ in $L[x]$, so gilt $\alpha/\beta \in K[x]$, d. h. $\beta \mid \alpha$ in $K[x]$. Für $\gamma, \delta \in K[x]$ ist der ggT (γ, δ) in $K[x]$ gleich dem ggT (γ, δ) in $L[x]$.*

Beweis. Die erste Behauptung ist offensichtlich. Aus der Eindeutigkeitsaussage des Satzes 4.2 über die Division mit Rest folgt, daß das Ergebnis der Division von α durch β nicht davon abhängt, ob wir α und β als Polynom über K oder über L betrachten. Speziell folgt aus $\beta \mid \alpha$ über L auch $\alpha/\beta \in K[x]$. Die letzte Behauptung ergibt sich aus Satz 1, weil die Anwendung des euklidischen Algorithmus auf zwei Elemente γ, δ von $K[x]$ nicht aus $K[x]$ hinausführt. □

Für einen Körper K der Charakteristik 0 geben wir nun ein Verfahren zur Bestimmung der Vielfachheit eines irreduziblen Faktors in einem Polynom $\alpha \in K[x]$ an, das sich auf den Begriff der Ableitung stützt. Für irreduzible Faktoren ersten Grades haben wir das schon im Satz 4.11 getan.

Satz 10. *Es sei K ein Körper, $\alpha \in K[x]$, $\alpha' \neq 0$ und φ ein irreduzibles Polynom. Hat φ die Vielfachheit $k>0$ in α und die Vielfachheit k' in α', so ist $k' \geqq k-1$. Gilt* char $K=0$, *so ist $k'=k-1$.*

Beweis. Nach Satz 6 gilt $\alpha = \varphi^k \beta$, wobei $\varphi \nmid \beta$ ist. Nach Satz 4.10 ist

$$\alpha' = k\varphi^{k-1}\varphi'\beta + \varphi^k\beta' = \varphi^{k-1}(k\varphi'\beta + \varphi\beta').$$

Somit gilt $\varphi^{k-1} \mid \alpha'$, also $k' \geqq k-1$. Ist char $K=0$, so gilt $k\varphi'\beta = (ke)\,\varphi'\beta \sim \varphi'\beta$. Aus $\operatorname{gr}\varphi' < \operatorname{gr}\varphi$ folgt $\varphi \nmid \varphi'$. Nach Satz 4 gilt $\varphi \nmid k\varphi'\beta$ und daher auch $\varphi \nmid (k\varphi'\beta + \varphi\beta')$. Wenden wir wieder Satz 6 an, so ergibt sich unsere Behauptung. □

Folgerung 5. *Ist K ein Körper der Charakteristik 0, so ist die Vielfachheit des irreduziblen Polynoms φ in $\alpha \in K[x]$, $\alpha \neq 0$, gleich derjenigen Zahl k, für die $\varphi \mid \alpha^{(k-1)}$, aber $\varphi \nmid \alpha^{(k)}$ gilt.* □

Übung 12. Es sei K ein Körper, $\alpha \in K[x]$, $\alpha' \neq 0$. Man beweise: a) Ein irreduzibler Faktor φ von α hat eine Vielfachheit $k>1$ genau dann, wenn $\varphi \mid \alpha'$ gilt; b) das Polynom $\alpha/(\alpha, \alpha')$ hat keine mehrfachen irreduziblen Faktoren; seine irreduziblen Faktoren stimmen bis auf Assoziiertheit mit denen von α überein.

§ 6. Faktormonoide, Quotientenkörper

In diesem Paragraphen entwickeln wir ein Verfahren, einen beliebigen Integritätsbereich zu einem Körper, dem Quotientenkörper des Integritätsbereiches, zu erweitern. Als Modell für diese Konstruktion dient die Erweiterung des Ringes der ganzen Zahlen zum Körper der rationalen Zahlen. Zunächst wollen wir jedoch einen allgemeinen Begriff einführen, den wir auch im nächsten Kapitel benötigen.

Definition 1. Es sei $[M, *]$ ein Monoid und $\sim$ eine Äquivalenzrelation in M. Man sagt, die Äquivalenzrelation $\sim$ sei *verträglich mit der Operation* $*$, wenn aus $a_1 \sim a_2$ und $b_1 \sim b_2$ die Beziehung $a_1 * b_1 \sim a_2 * b_2$ folgt.

Wir setzen voraus, daß die Bedingungen der Definition 1 erfüllt sind, und definieren in der Faktormenge $\overline{M} := M/\sim$ eine Operation durch die Formel

$$\bar{a} * \bar{b} := \overline{a * b} \qquad (a, b \in M); \tag{1}$$

hierbei bezeichnet $\bar{a}$ die Äquivalenzklasse von $a \in M$ (vgl. (0.2.43)).

Satz 1. *Unter den Bedingungen der Definition 1 wird durch (1) eine algebraische Operation in $\overline{M}$ definiert. Die kanonische Abbildung $p\colon M \to \overline{M}$ ist ein Homomorphismus der Monoide. Ist $[M, *]$ assoziativ (bzw. kommutativ), so ist auch $[\overline{M}, *]$ assoziativ*

(*bzw. kommutativ*). *Enthält M ein Einselement e, so ist $\bar{e}$ Einselement von $\overline{M}$. Gilt $a \in M^*$, so ist $\bar{a} \in \overline{M}^*$, und es gilt* $(\bar{a})^{-1} = (\overline{a^{-1}})$.

Beweis. Aus Definition 1 folgt, daß die rechte Seite nur von den Äquivalenzklassen $\bar{a}$, $\bar{b}$ und nicht von der Wahl der Vertreter a, b abhängt. Somit ist $[\overline{M}, *]$ ein korrekt definiertes Monoid. Die Gleichung (1) kann man auch in der Form

$$p(a) * p(b) = p(a * b)$$

schreiben, die ausdrückt, daß p ein Homomorphismus der Monoide ist. Die übrigen Behauptungen ergeben sich unmittelbar aus der Definition. □

Definition 2. Das durch Satz 1 definierte Monoid $[\overline{M}, *]$ heißt das *Faktormonoid* von $[M, *]$ nach der Äquivalenzrelation $\sim$.

Als Beispiel für die Definition 2 erinnern wir an die Konstruktion der Restklassenringe $\mathbf{Z}_n$, vgl. Definition 2.9.

Es sei A ein Integritätsbereich. Wir betrachten die Menge $\hat{A} = A \times (A \setminus \{0\})$. In $\hat{A}$ definieren wir die folgende Relation:

$$(a_1, b_1) \sim (a_2, b_2), \quad \text{wenn } a_1 b_2 = a_2 b_1 \text{ ist.} \tag{2}$$

Diese Relation ist eine Äquivalenzrelation. Offenbar ist sie reflexiv und symmetrisch; wir zeigen die Transitivität. Gilt $(a_1, b_1) \sim (a_2, b_2)$ und $(a_2, b_2) \sim (a_3, b_3)$, so ist

$$a_1 b_2 = a_2 b_1 , \tag{3}$$

$$a_2 b_3 = a_3 b_2 . \tag{4}$$

Multiplizieren wir (3) mit b_3 und (4) mit b_1, so folgt $a_1 b_2 b_3 = a_3 b_2 b_1$. Weil $b_2 \neq 0$ ist, können wir diese Gleichung durch b_2 kürzen und erhalten $a_1 b_3 = a_3 b_1$, also $(a_1, b_1) \sim (a_3, b_3)$.

Wir bezeichnen mit $Q(A)$ die Faktormenge $\hat{A}/\sim$. In $Q(A)$ wollen wir die Operationen der Addition und Multiplikation so einführen, daß $Q(A)$ ein A erweiternder Körper wird. Dazu definieren wir zunächst zwei Operationen in $\hat{A}$, wobei wir uns an der elementaren Bruchrechnung orientieren ((a, b) entspricht a/b im Fall der ganzen Zahlen!):

$$(a, b) + (c, d) := (ad + bc, bd), \qquad (a, b) \cdot (c, d) := (ac, bd) . \tag{5}$$

Sind $b \neq 0$, $d \neq 0$, so ist auch $bd \neq 0$; daher sind die Definitionen (5) korrekt. Unmittelbar aus den Definitionen folgt, daß $[\hat{A}, +]$ und $[\hat{A}, \cdot]$ kommutative Halbgruppen mit dem Nullelement $(0, e)$ bzw. dem Einselement (e, e) sind. Wir beweisen, daß die Operationen (5) mit der Äquivalenzrelation $\sim$ verträglich sind. Dazu genügt es — wegen der Kommutativität der Operationen in $\hat{A}$ — zu zeigen, daß aus $(a, b) \sim (a', b')$

$$(a, b) + (c, d) \sim (a', b') + (c, d), \qquad (a, b) \cdot (c, d) \sim (a', b') \cdot (c, d) \tag{6}$$

folgt. Diese Formeln beweist man durch einfache Rechnungen, beispielsweise

$$(ad+bc)\,(b'd)=ab'd^2+bcb'd=a'bd^2+bcb'd=(a'd+b'c)\,(bd)\,.$$

Aus Satz 1 ergibt sich, daß die Operationen aus $\hat{A}$ auf $Q(A)$ übertragen werden. Nach (1) gelten für die Operationen in $Q(A)$ folgende Formeln:

$$\overline{(a,b)}+\overline{(c,d)}=\overline{(ad+bc,\,bd)},\qquad \overline{(a,b)}\cdot\overline{(c,d)}=\overline{(ac,\,bd)}\,. \tag{7}$$

Satz 2. *Ist A ein Integritätsbereich, so wird die Menge $Q(A)$ mit den Operationen (7) ein Körper.*

Beweis. Aus Satz 1 folgt, daß $[Q(A),+]$ und $[Q(A),\cdot]$ kommutative Halbgruppen mit dem Nullelement $\overline{(0,e)}$ bzw. dem Einselement $\overline{(e,e)}$ sind. Zum Beweis, daß $[Q(A),+]$ eine Gruppe ist, bemerken wir, daß

$$\overline{(a,b)}+\overline{(-a,b)}=\overline{(0,b^2)}=\overline{(0,e)}$$

gilt. Setzen wir nun voraus, daß $\overline{(a,b)}\neq\overline{(0,e)}$ ist, dann gilt $a\neq 0$, also $\overline{(b,a)}\in\hat{A}$. Wir erhalten

$$\overline{(a,b)}\cdot\overline{(b,a)}=\overline{(ab,\,ba)}=\overline{(e,e)}\,,$$

d. h., alle von 0 verschiedenen Elemente sind invertierbar. Es bleibt zu beweisen, daß das distributive Gesetz erfüllt ist. Nun gilt

$$\begin{aligned}&((a,b)+(c,d))\,(u,v)=(ad+bc,\,bd)\,(u,v)=((ad+bc)\,u,\,bdv)\,,\\&(a,b)\,(u,v)+(c,d)\,(u,v)=(au,\,bv)+(cu,\,dv)=(audv+cubv,\,bdv^2)\\&\qquad\qquad=((ad+bc)\,uv,\,bdv^2)\,.\end{aligned}$$

Da die beiden erhaltenen Paare offenbar äquivalent sind, ist unsere Behauptung bewiesen. □

Wir wollen nun zeigen, daß der konstruierte Körper $Q(A)$ den Integritätsbereich erweitert und aus den Quotienten der Elemente von A (in $Q(A)$) besteht. Dazu betrachten wir die Abbildung

$$f\colon a\in A\mapsto f(a):=\overline{(a,e)}\in Q(A)\,.$$

Satz 3. *Die Abbildung f bildet den Integritätsbereich A isomorph auf einen Unterring von $Q(A)$ ab. Identifiziert man A und* Im f *mit Hilfe der Abbildung f, so gilt $\overline{(a,b)}=a/b$ für $a,b\in A$, $b\neq 0$.*

Beweis. Wir zeigen, daß f ein Ringhomomorphismus ist. Es gilt

$$\begin{aligned}&f(a+b)=\overline{(a+b,e)}=\overline{(a,e)}+\overline{(b,e)}=f(a)+f(b)\,,\\&f(a\cdot b)=\overline{(ab,e)}\quad=\overline{(a,e)}\cdot\overline{(b,e)}=f(a)\cdot f(b)\,.\end{aligned}$$

Weiter ist Ker $f=0$. Ist nämlich $f(a)=\overline{(a,e)}=\overline{(0,e)}$, so gilt $a=0$. Nach Folgerung 1.1 bildet f den Ring A isomorph auf den Unterring Im f ab, der aus allen Klassen der Form $\overline{(a,e)}$ besteht. Identifizieren wir a und $\overline{(a,e)}$, dann gilt für $a,b\in A$, $b\neq 0$

$$a/b=ab^{-1}=\overline{(a,e)}\;\overline{(b,e)}^{-1}=\overline{(a,e)}\cdot\overline{(e,b)}=\overline{(a,b)}.\quad\square$$

Definition 3. Der Körper $Q(A)$ heißt der *Quotientenkörper* des Integritätsbereiches A. Diese Bezeichnung steht mit Definition 2.6 in Einklang. Gilt nämlich $a=bc$ für a, b, c in A, $b\neq 0$, so ist $c=a/b$ auch in $Q(A)$.

Der Körper $Q(A)$ ist ein *minimaler Körper*, der den Ring A enthält, d. h., gilt $A\subseteq K\subseteq Q(A)$ und ist K Teilkörper, so ist $K=Q(A)$. In der Tat, mit $a, b\in A$, $b\neq 0$ gilt $ab^{-1}\in K$, aber die Menge dieser Elemente ist schon $Q(A)$ (Satz 3). Wir wollen nun zeigen, daß diese Eigenschaft $Q(A)$ charakterisiert.

Satz 4. *Es sei L ein Körper, der den Integritätsbereich A als Unterring enthält; ferner gelte: Ist $K\subseteq L$ Teilkörper mit $A\subseteq K$, so ist $K=L$. Dann existiert ein Isomorphismus $f: Q(A)\to L$ mit $f \mid A=\mathrm{id}_A$, $\mathrm{Im}\, f=L$.*

Beweis. Wir definieren f durch $f(a/b):=a/b$ für $a, b\in A$, $b\neq 0$, wobei die Division rechts in L ausgeführt wird. Diese Definition hängt offenbar nicht von der Wahl der Darstellung des Quotienten ab: Ist $a'/b'=a/b$, so gilt $a=a'=0$ oder $a'=ac$, $b'=bc$ mit $a, a', b, b'\in A$, $c\in L$, also $f(a'/b')=f(a/b)$. f ist ein Homomorphismus:

$$f\left(\frac{a}{b}+\frac{c}{d}\right)=f\left(\frac{ad+bc}{bd}\right)=\frac{ad+bc}{bd}=\frac{a}{b}+\frac{c}{d},$$

analog für die Multiplikation. Offenbar gilt $f(a)=f\left(\frac{a}{e}\right)=a$ für $a\in A$. Somit ist $A\subseteq \mathrm{Im}\, f\neq 0$. Nach Satz 2.2 ist f injektiv und $\mathrm{Im}\, f$ ein Körper. Wegen $A\subseteq \mathrm{Im}\, f\subseteq L$ muß $\mathrm{Im}\, f=L$ gelten. □

Beispiel 1. Es gilt $Q(\mathbf{Z})=\mathbf{Q}$: Der Quotientenkörper des Ringes der ganzen Zahlen ist der Körper der rationalen Zahlen.

Beispiel 2. Es sei K ein beliebiger Körper. Dann heißt $K(x):=Q(K[x])$ der Körper der *rationalen Funktionen über K* (man beachte, daß im allgemeinen diese Bezeichnung irreführend ist, vgl. Definition 5 und Übung 5 weiter unten).

Übung 1. Man beweise: Ist K ein Körper, so gilt $Q(K)=K$.

Übung 2. Man beweise: Ist A ein Integritätsbereich, so gilt $Q(A[x])=Q(A)(x)$ (vgl. Beispiel 2).

Bis zum Schluß dieses Paragraphen werden wir Quotientenkörper $Q(A)$ von euklidischen Ringen A untersuchen, wobei wir vor allem die Beispiele 1 und 2 vor Augen haben.

Satz 5. *Es sei A ein euklidischer Ring. Dann kann man jedes $\varrho\in Q(A)$ in der Form*

$$\varrho=a/b, \qquad a, b\in A \text{ mit } (a, b)=e,\ b\neq 0, \tag{8}$$

darstellen; die Elemente a, b sind in A bis auf einen gemeinsamen invertierbaren Faktor eindeutig bestimmt.

Beweis. Es sei $\varrho=u/v$, $u, v\in A$, $v\neq 0$. Nach Satz 5.1 existiert der ggT $d=(u, v)$, und wegen $v\neq 0$ gilt $d\neq 0$. Die Elemente $a=u/d$, $b=v/d\neq 0$ des Ringes A sind teilerfremd (Übung 2.2), und es gilt offenbar $\varrho=a/b$. Ist nun $\varrho=a'/b'$ eine andere Dar-

stellung der Form (8), so folgt $ab' = a'b$. Hieraus ergibt sich nach Satz 5.3 $b \mid b'$ und $b' \mid b$. Nach Satz 2.5 ist daher $b' = bc$ mit $c \in A^*$, und wir erhalten $abc = a'b$. Kürzen durch $b \neq 0$ ergibt $a' = ac$. □

Definition 3. Eine Darstellung der Form (8) nennt man Darstellung von ϱ als *unkürzbarer Bruch.*

Definition 4. Es sei A ein euklidischer Ring. Ein Element $\varrho \in Q(A)$ heißt ein *einfacher Bruch* (oder *Partialbruch*), wenn ϱ in der Form

$$\varrho = u/p^k, \qquad u \neq 0\,, \tag{9}$$

darstellbar ist, wobei p ein Primelement von A, $k \in \mathbf{N}$ und $u \in A$ mit $w(u) < w(p)$ ist.

Man bemerke, daß der Bruch (9) unkürzbar ist. In der Tat gilt $p \nmid u$ wegen der Eigenschaft 2 aus Definition 5.1. Nach Folgerung 5.4 ist also $(p^k, u) = e$. Unser nächstes Ziel ist der Beweis des folgenden Satzes:

Satz 6. *Es sei A ein euklidischer Ring. Dann läßt sich jedes Element $\varrho \in Q(A)$ als Summe eines Elementes aus A und einiger einfacher Brüche mit paarweise nicht assoziierten Nennern darstellen.*

Beweis. Für ein von 0 verschiedenes Element $c \in A$ bezeichne $\lambda(c)$ die Anzahl der Primfaktoren in der Primfaktorzerlegung des Elementes c; für $c \in A^*$ setzen wir $\lambda(c) = 0$. Wir beweisen die Existenz der geforderten Darstellung durch Induktion nach $\lambda(b)$, wenn $\varrho = a/b$ eine Darstellung von ϱ als unkürzbarer Bruch ist. Dabei wird sich herausstellen, daß die Nenner der einfachen Brüche unserer gesuchten Darstellung Teiler von b sind.

Für $\lambda(b) = 0$ ist unsere Behauptung offenbar erfüllt. Angenommen, sie sie schon für alle ϱ mit $\lambda(b) < n$ bewiesen. Wir betrachten ein ϱ mit $\lambda(b) = n$. Es sei p ein Primteiler von b mit der Vielfachheit $k > 0$. Dann gilt $b = p^k c$ mit $(p, c) = e$. Nach Satz 5.2 existieren $u, v \in A$ mit

$$a = cu + pv\,,$$

wobei $u = 0$ oder $w(u) < w(p)$ gilt. Da $\varrho = a/b$ ein unkürzbarer Bruch ist, haben wir $p \nmid a$, so daß $u \neq 0$ sein muß. Multiplizieren wir diese Gleichung mit b^{-1}, so folgt

$$\varrho = a/b = u/p^k + v/(p^{k-1}c)\,.$$

Der erste Summand ist ein einfacher Bruch. Es sei $\varrho' = v/p^{k-1}c = a'/b'$ eine Darstellung des zweiten Summanden als unkürzbarer Bruch. Aus dem Beweis von Satz 5 erkennt man, daß $b' = p^{k-1}c/(v, p^{k-1}c)$ gilt; also ist $\lambda(b') \leqq \lambda(p^{k-1}c) = n - 1$. Folglich können wir ϱ' nach Induktionsvoraussetzung als Summe eines Elementes von A und gewisser einfacher Brüche darstellen, die paarweise nicht assoziierte Nenner haben, welche b' und folglich auch b teilen. Diese Nenner können nicht zu p^k assoziiert sein; denn es gilt $p^k \nmid b'$. □

Satz 7. *Es sei $A = K[x]$, K ein Körper. Dann ist die in Satz 6 beschriebene Darstellung der Elemente des Körpers $Q(A) = K(x)$ eindeutig.*

Beweis. Angenommen, wir hätten zwei verschiedene Darstellungen des Elementes ϱ. Bringen wir alle Glieder auf eine Seite und fassen die einfachen Brüche mit

assoziierten Nennern zusammen – hierbei entsteht nach Satz 4.1 entweder 0 oder ein einfacher Bruch mit demselben Nenner –, so erhalten wir eine nichttriviale Darstellung der Null in der Form

$$\alpha+\varrho_1+\ldots+\varrho_k=0\,, \tag{10}$$

wobei $\alpha\in K[x]$ und die ϱ_i einfache Brüche mit paarweise nicht assoziierten Nennern sind. Es seien $p_1, \ldots, p_s$ alle paarweise nicht assoziierten Primelemente, die in den Nennern der ϱ_i auftreten, und $k_1, \ldots, k_s$ ihre höchsten vorkommenden Potenzen. Speziell sei $\varrho_1=u/p_1^{k_1}$ mit $\operatorname{gr} u<\operatorname{gr} p_1$. Multiplizieren wir (10) mit $p_1^{k_1-1}p_2^{k_2}\ldots p_s^{k_s}$, so erhalten wir eine Gleichung der Gestalt

$$\frac{up_2^{k_2}\ldots p_s^{k_s}}{p_1}+\beta=0\,,$$

für die $\beta\in K[x]$ gilt. Somit müßte $p_1 \mid up_2^{k_2}\ldots p_s^{k_s}$ gelten, was Satz 5.4 widerspricht. □

Wir bemerken, daß man die in Satz 6 beschriebene Zerlegung im Fall $K(x)$ auch *Partialbruchzerlegung der rationalen Funktionen* nennt. Sie hat viele Anwendungen, z. B. für $K=\mathbf{R}$ bei der Integration der rationalen Funktionen.

Übung 3. Für den Körper der rationalen Zahlen ist die Zerlegung in einfache Brüche nicht eindeutig; z. B. gilt $2/9=1/3+(-1)/9$. Man kann die Eindeutigkeit jedoch erzwingen, indem man nur positive einfache Brüche, also solche mit $0<u<p$, zuläßt. Man beweise, daß jede rationale Zahl eindeutig als Summe einer ganzen Zahl und einiger positiver einfacher Brüche mit verschiedenen positiven Nennern dargestellt werden kann.

Übung 4. Es sei K ein Körper. Man beweise, daß jedes Element $\varrho\in K(x)$ als Summe $\varrho=\varrho_0+\varrho_1$ darstellbar ist, wobei $\varrho_0\in K[x]$ gilt und ϱ_1 die Form $\varrho_1=\alpha/\beta$ mit $\alpha, \beta\in K[x]$ und $\alpha=0$ oder $\operatorname{gr}\alpha<\operatorname{gr}\beta$ besitzt. Eine solche Darstellung ist eindeutig. Man formuliere und beweise eine analoge Eigenschaft für den Körper $\mathbf{Q}$.

Wenn der Körper K unendlich ist, kann man die in Beispiel 2 angegebene algebraische Konstruktion von $K(x)$ vermeiden und den Körper der rationalen „Funktionen" als Menge von wirklichen Funktionen definieren.

Definition 5. Eine Funktion ϱ, deren Definitionsbereich und Wertemenge in K liegen, heißt *rational*, wenn es Polynome $\alpha, \beta\in K[x]$ gibt, so daß ϱ für alle $c\in K$ mit $\beta(c)\neq 0$ definiert ist und

$$\varrho(c)=\alpha(c)/\beta(c) \quad \text{für} \quad c\in K,\ \beta(c)\neq 0\,, \tag{11}$$

gilt. Zwei rationale Funktionen werden als gleich betrachtet, wenn sie auf dem Durchschnitt ihrer Definitionsbereiche übereinstimmen. Man definiert die Operationen der Addition und der Multiplikation der rationalen Funktionen elementweise für alle die $c\in K$, die im Durchschnitt der Definitionsbereiche der beiden Summanden bzw. Faktoren liegen.

Übung 5. Man beweise, daß für einen unendlichen Körper K die rationalen Funktionen im Sinne der Definition 5 einen Körper bilden. Ist K unendlich, so ist die Zuordnung $\varphi\mapsto\alpha/\beta\in K(x)$, α, β nach (11), ein Isomorphismus dieses Körpers auf den im Beispiel 2 beschriebenen Quotientenkörper $K(x)$.

§ 7. Polynome in mehreren Unbestimmten. Symmetrische Polynome

Es sei A ein Integritätsbereich. In § 4 konstruierten wir den zu A gehörenden Polynomring $A[x]$, der wiederum ein Integritätsbereich ist. Wiederholen wir mit diesem Integritätsbereich dieselbe Konstruktion, so erhalten wir einen neuen Integritätsbereich $A[x, y] := A[x][y]$. Verallgemeinern wir dieses Verfahren, so kommen wir auf folgende rekursive Definition:

Definition 1. 1. Es sei $A[x_1]$ der zum Integritätsbereich A gehörende Polynomring. 2. Für $n = 2, 3, \ldots$ sei

$$A[x_1, \ldots, x_n] := A[x_1, \ldots, x_{n-1}][x_n] .$$

Der Integritätsbereich $A[x_1, \ldots, x_n]$ heißt *Polynomring in n Unbestimmten* $x_1, \ldots, x_n$ *über* A.

Aus Satz 4.1 und Folgerung 4.1 erhält man leicht durch vollständige Induktion:

Satz 1. *Ist A ein Integritätsbereich, so ist auch $A[x_1, \ldots, x_n]$ ein Integritätsbereich. Es gibt kanonische Einbettungen*

$$A \subset A[x_1] \subset A[x_1, x_2] \subset \ldots \subset A[x_1, \ldots, x_n] \subset \ldots .$$

Ferner gilt

$$A[x_1, \ldots, x_n]^* = A^* . \quad \square$$

Speziell zeigt die Relation

$$A[x_1, \ldots, x_{i-1}][x_i] = A[x_1, \ldots, x_i] \subset A[x_1, \ldots, x_n] ,$$

daß man x_i, $1 \leqq i \leqq n$, als Element des Ringes $A[x_1, \ldots, x_n]$ betrachten kann. Jedes n-Tupel $(k_1, \ldots, k_n)$ von Zahlen $k_i \in \mathbf{N}_0$ bestimmt ein Element

$$x_1^{k_1} \ldots x_n^{k_n} \in A[x_1, \ldots, x_n] .$$

Satz 2. *Jedes Element $\alpha \in A[x_1, \ldots, x_n]$ läßt sich eindeutig in der Form*

$$\alpha = \sum_{k_1, \ldots, k_n} a_{k_1 \ldots k_n} x_1^{k_1} \ldots x_n^{k_n} \tag{1}$$

darstellen, wobei $a_{k_1 \ldots k_n} \in A$ gilt, $(k_1, \ldots, k_n)$ die Menge $\mathbf{N}_0^n$ durchläuft und höchstens endlich viele der Koeffizienten $a_{k_1 \ldots k_n}$ von 0 verschieden sind.

Beweis. Wir zeigen die Existenz der Darstellung (1) durch Induktion nach n. Für $n = 1$ ergibt sich die Behauptung aus (4.4). Angenommen, sie sei schon für $A[x_1, \ldots, x_{n-1}]$ bewiesen. Wir stellen das Polynom $\alpha \in A[x_1, \ldots, x_{n-1}][x_n]$ in der Form (4.4) dar:

$$\alpha = \sum_{k_n = 0}^{m} \alpha_{k_n} x_n^{k_n} ,$$

wobei $\alpha_{k_n} \in A[x_1, \ldots, x_{n-1}]$ ist. Nach Induktionsvoraussetzung gilt

$$\alpha_{k_n} = \sum_{k_1, \ldots, k_{n-1}} a_{k_1 \ldots k_{n-1} k_n} x_1^{k_1} \ldots x_{n-1}^{k_{n-1}} ,$$

wo nur endlich viele $a_{k_1 \dots k_{n-1} k_n}$ ungleich 0 sind. Durch Einsetzen in die vorstehende Formel erhalten wir die gesuchte Darstellung.

Die Eindeutigkeit der Darstellung (1) beweisen wir ebenfalls durch Induktion nach n. Für $n=1$ ist die Behauptung offensichtlich (vgl. § 4). Angenommen, sie sei schon für $n-1$ bewiesen, und es sei

$$\alpha = \sum_{k_1,\dots,k_n} b_{k_1 \dots k_n} x_1^{k_1} \dots x_n^{k_n}$$

eine neben (1) existierende Darstellung von α. Dann gilt

$$\sum_{k_n} \Big(\sum_{k_1,\dots,k_{n-1}} a_{k_1 \dots k_{n-1} k_n} x_1^{k_1} \dots x_{n-1}^{k_{n-1}} \Big) x_n^{k_n}$$
$$= \sum_{k_n} \Big(\sum_{k_1,\dots,k_{n-1}} b_{k_1 \dots k_{n-1} k_n} x_1^{k_1} \dots x_{n-1}^{k_{n-1}} \Big) x_n^{k_n}.$$

Hieraus folgt, daß die rechts und links stehenden inneren Summen für alle k_n entsprechend gleich sein müssen:

$$\sum_{k_1,\dots,k_{n-1}} a_{k_1 \dots k_{n-1} k_n} x_1^{k_1} \dots x_{n-1}^{k_{n-1}} = \sum_{k_1,\dots,k_{n-1}} b_{k_1 \dots k_{n-1} k_n} x_1^{k_1} \dots x_{n-1}^{k_{n-1}},$$

und nach Induktionsvoraussetzung ist $a_{k_1 \dots k_{n-1} k_n} = b_{k_1 \dots k_{n-1} k_n}$ für alle $k_1, \dots, k_{n-1}, k_n$. □

Definition 2. Ein Element der Gestalt

$$\mu = a x_1^{k_1} \dots x_n^{k_n}, \qquad a \in A,\ a \neq 0,$$

heißt ein *Monom*. Unter dem *Grad des Monoms* versteht man die Zahl

$$\operatorname{gr} \mu = k_1 + \dots + k_n .$$

Monome mit demselben n-Tupel $(k_1, \dots, k_n)$ heißen *ähnlich*. Die in der Darstellung (1) vorkommenden Monome heißen die *Glieder* des Polynoms α. Ein Polynom α heißt *homogen vom Grad m*, wenn alle seine Glieder denselben Grad m haben. Im allgemeinen Fall versteht man unter dem *Grad* des beliebigen Polynoms $\alpha \neq 0$

$$\operatorname{gr} \alpha := \max \operatorname{gr} \mu ,$$

wobei μ alle Glieder des Polynoms α durchläuft.

Übung 1. Es sei A ein Integritätsbereich. Man beweise für $\alpha, \beta \in A[x_1, \dots, x_n]$

$$\operatorname{gr} (\alpha \cdot \beta) = \operatorname{gr} \alpha + \operatorname{gr} \beta \qquad (\alpha \neq 0, \beta \neq 0) .$$

Übung 2. Man beweise, daß jedes Polynom eindeutig als Summe homogener Polynome verschiedener Grade dargestellt werden kann.

Für $n=1$ sind die Glieder eines Polynoms durch ihren Grad in natürlicher Weise geordnet. Ist jedoch $n>1$, so reicht der Grad nicht aus, um eine Reihenfolge der Glieder festzulegen. Im weiteren werden wir die sogenannte lexikographische Ordnung benötigen, die wir nun beschreiben wollen.

Definition 3. Es sei $\mathbf{N}_0^n$ die Menge aller n-Tupel $(k_1, \dots, k_n)$ mit $k_i \in \mathbf{N}_0$, $i=1, \dots, n$. Die *lexikographische Ordnung in* $\mathbf{N}_0^n$ wird folgendermaßen definiert: Es

gelte

$$(k_1, ..., k_n) > (l_1, ..., l_n),$$

wenn ein i existiert, so daß $k_1 = l_1, ..., k_{i-1} = l_{i-1}$ und $k_i > l_i$ gilt. Die entsprechende Ordnung der Monome heißt ebenfalls *lexikographisch.*

Satz 3. *Die lexikographische Ordnung in* $\mathbf{N}_0^n$ *ist eine lineare Ordnung, d. h., es gelten*

1. *Für zwei n-Tupel* $\sigma_n, \tau_n \in \mathbf{N}_0^n$ *gilt eine und nur eine der Relationen* $\sigma_n > \tau_n$, $\sigma_n = \tau_n$ *oder* $\tau_n > \sigma_n$.

2. *Ist* $\varrho_n > \sigma_n$ *und* $\sigma_n > \tau_n$ *für* $\varrho_n, \sigma_n, \tau_n \in \mathbf{N}_0^n$, *so gilt auch* $\varrho_n > \tau_n$ (*Transitivität*).

Beweis. Die Eigenschaft 1 folgt unmittelbar aus der Definition und der linearen Ordnung der natürlichen Zahlen. Wir beweisen die Eigenschaft 2. Es sei $\varrho_n = (r_1, ..., r_n)$, $\sigma_n = (s_1, ..., s_n)$ und $\tau_n = (t_1, ..., t_n)$. Dann gibt es nach Voraussetzung solche natürlichen Zahlen i, j, $1 \leqq i, j \leqq n$, mit

$$r_1 = s_1, ..., r_{i-1} = s_{i-1}, \qquad r_i > s_i,$$

$$s_1 = t_1, ..., s_{j-1} = t_{j-1}, \qquad s_j > t_j.$$

Es sei $k = \min(i, j)$. Offenbar gilt $r_1 = s_1 = t_1, ..., r_{k-1} = s_{k-1} = t_{k-1}$ und $r_k \geqq s_k \geqq t_k$, wobei in wenigstens einer der letzten beiden Ungleichungen das Zeichen $>$ stehen muß. Folglich ist $r_1 = t_1, ..., r_{k-1} = t_{k-1}$ und $r_k > t_k$, d. h. $\varrho_n > \tau_n$. □

Folgerung 1. *In jeder nichtleeren, endlichen Teilmenge von* $\mathbf{N}_0^n$ *existiert ein im Sinne der lexikographischen Ordnung größtes Element. Analog gibt es in jedem von 0 verschiedenen Polynom ein lexikographisch höchstes Monom.* □

Satz 4. *Es seien* $\mu_1, \mu_2, \nu_1, \nu_2 \in A[x_1, ..., x_n]$ *Monome, und es gelte* $\mu_1 > \mu_2$ *und entweder* $\nu_1 > \nu_2$ *oder es seien* ν_1, ν_2 *ähnlich. Dann gilt auch* $\mu_1\nu_1 > \mu_2\nu_2$. *Das höchste Glied des Produktes zweier von 0 verschiedener Polynome ist gleich dem Produkt ihrer höchsten Glieder.*

Beweis. Es seien $\mu_1 = c_1 x_1^{k_1} ... x_n^{k_n}$, $\mu_2 = c_2 x_1^{l_1} ... x_n^{l_n}$, $\nu_1 = d_1 x_1^{p_1} ... x_n^{p_n}$, $\nu_2 = d_2 x_1^{q_1} ... x_n^{q_n}$. Dann gilt

$$\mu_1\nu_1 = c_1 d_1 x_1^{k_1+p_1} ... x_n^{k_n+p_n} \quad \text{und} \quad \mu_2\nu_2 = c_2 d_2 x_1^{l_1+q_1} ... x_n^{l_n+q_n}.$$

Eine einfache Abschätzung unter Beachtung von $(k_1, ..., k_n) > (l_1, ..., l_n)$, $(p_1, ..., p_n) \geqq (q_1, ..., q_n)$ ergibt die erste Behauptung. Zum Beweis der zweiten Behauptung zerlegen wir die Polynome $\alpha, \beta \in A[x_1, ..., x_n]$ in paarweise nicht ähnliche Monome

$$\alpha = \mu_0 + \mu_1 + ... + \mu_u, \qquad \beta = \nu_0 + \nu_1 + ... + \nu_v,$$

wobei $\mu_0 > \mu_i$ für $i = 1, ..., u$ und $\nu_0 > \nu_j$ für $j = 1, ..., v$ gelte. Es folgt

$$\alpha\beta = \mu_0\nu_0 + \sum_{i=1}^{u} \mu_i\nu_0 + \sum_{j=1}^{v} \mu_0\nu_j + \sum_{i=1}^{u} \sum_{j=1}^{v} \mu_i\nu_j. \tag{2}$$

Die Zerlegung des Polynoms $\alpha\beta$ in paarweise nicht ähnliche Monome erhält man durch Zusammenfassen der ähnlichen Glieder in (2). Aus dem ersten Teil des Satzes folgt, daß $\mu_0\nu_0$ höher ist als alle übrigen Summanden in (2). □

Man beachte, daß die lexikographische Ordnung der Glieder eines Polynoms nicht unmittelbar mit seinem Grad zusammenhängt. Das höchste Glied eines Polynoms α kann einen kleineren Grad als α haben.

Analog wie bei den Polynomen in einer Unbestimmten kann man jedem Polynom $\alpha \in A[x_1, ..., x_n]$ eine Funktion der Variablen $x_1, ..., x_n$, die den Ring A durchlaufen, mit Werten in A zuordnen. Es ist jedoch nützlich, eine etwas allgemeinere Situation zu betrachten. Es sei B ein assoziativer und kommutativer Ring, der A als Unterring enthält, beispielsweise $B = A$ oder B ein Polynomring über A, und $b_1, ..., b_n \in B$. Hat α die Gestalt (1), so setzen wir

$$\alpha(b_1, ..., b_n) := \sum_{k_1,...,k_n} a_{k_1...k_n} b_1^{k_1} ... b_n^{k_n} . \tag{3}$$

Satz 5. *Es sei $A \subseteq B$ Unterring, B assoziativer und kommutativer Ring, $c_1, ..., c_n \in B$ feste Elemente. Dann ist die Abbildung*

$$\alpha \in A[x_1, ..., x_n] \mapsto \alpha(c_1, ..., c_n) \in B$$

ein Ringhomomorphismus, dessen Einschränkung auf A die Identität ist. Umgekehrt gibt es für einen beliebigen Ringhomomorphismus $f: A[x_1, ..., x_n] \mapsto B$ mit $f \mid A = \mathrm{id}_A$ eindeutig bestimmte Elemente $c_1, ..., c_n \in B$ so, daß

$$f(\alpha) = \alpha(c_1, ..., c_n) \qquad (\alpha \in A[x_1, ..., x_n])$$

gilt.

Beweis. Es sei

$$\beta = \sum_{l_1,...,l_n} b_{l_1...l_n} x_1^{l_1} ... x_n^{l_n}$$

ebenfalls ein Polynom aus $A[x_1, ..., x_n]$. Dann gilt

$$\alpha \cdot \beta = \sum_{m_1,...,m_n} \left(\sum_{\substack{k_1+l_1=m_1 \\ \cdots\cdots\cdots \\ k_n+l_n=m_n}} a_{k_1...k_n} b_{l_1...l_n} \right) x_1^{m_1} ... x_n^{m_n} .$$

Nach (3) ist für $c_i \in B$ fest, $i = 1, ..., n$:

$$\begin{aligned} \alpha \cdot \beta(c_1, ..., c_n) &= \sum_{m_1,...,m_n} \left(\sum_{\substack{k_1+l_1=m_1 \\ \cdots\cdots\cdots \\ k_n+l_n=m_n}} a_{k_1...k_n} b_{l_1...l_n} \right) c_1^{m_1} ... c_n^{m_n} \\ &= \sum_{\substack{k_1,...,k_n \\ l_1,...,l_n}} a_{k_1...k_n} b_{l_1...l_n} c_1^{k_1+l_1} ... c_n^{k_n+l_n} \\ &= \alpha(c_1, ..., c_n) \cdot \beta(c_1, ..., c_n) . \end{aligned}$$

Ähnlich beweist man $(\alpha + \beta)(c_1, ..., c_n) = \alpha(c_1, ..., c_n) + \beta(c_1, ..., c_n)$.

Bezeichnen wir mit $g: A[x_1, ..., x_n] \to B$ den gerade betrachteten Homomorphismus, so gilt $g(x_i) = c_i$; die Elemente c_i sind also durch g eindeutig bestimmt.

Es sei nun umgekehrt ein Homomorphismus $f: A[x_1, ..., x_n] \to B$ mit $f \mid A = \mathrm{id}_A$ gegeben. Wir setzen $c_i := f(x_i) \in B$, $i = 1, ..., n$. Ist $\alpha \in A[x_1, ..., x_n]$ durch (1) gegeben,

so folgt

$$f(\alpha) = \sum_{k_1,\ldots,k_n} f(a_{k_1\ldots k_n})\, f(x_1)^{k_1} \ldots f(x_n)^{k_n}$$
$$= \sum_{k_1,\ldots,k_n} a_{k_1\ldots k_n} c_1^{k_1} \ldots c_n^{k_n} = \alpha(c_1, \ldots, c_n)\,. \quad \square$$

Übung 3. Es sei B ein beliebiger assoziativer und kommutativer Ring und $\varphi\colon A \to B$ ein Ringhomomorphismus. Man beweise, daß für beliebige $c_1, \ldots, c_n \in B$ ein und nur ein Ringhomomorphismus $f\colon A[x_1, \ldots, x_n] \to B$ existiert, für den $f \mid A = \varphi$ und $f(x_i) = c_i$, $i = 1, \ldots, n$, gilt.

Übung 4. Es seien B und C zwei assoziative und kommutative Ringe, die A als Unterring enthalten. Ferner sei $\varphi\colon B \to C$ ein Ringhomomorphismus mit $\varphi \mid A = \mathrm{id}_A$. Man beweise: Für alle $c_1, \ldots, c_n \in B$ und $\alpha \in A[x_1, \ldots, x_n]$ gilt

$$\varphi(\alpha(c_1, \ldots, c_n)) = \alpha(\varphi(c_1), \ldots, \varphi(c_n))\,.$$

Satz 6. *Der Integritätsbereich A sei unendlich, und es seien $\alpha, \beta \in A[x_1, \ldots, x_n]$. Gilt dann $\alpha(c_1, \ldots, c_n) = \beta(c_1, \ldots, c_n)$ für beliebige $c_1, \ldots, c_n \in A$, so ist $\alpha = \beta$.*

Beweis. Nach Satz 5 genügt es zu zeigen, daß $\alpha = 0$ aus $\alpha(c_1, \ldots, c_n) = 0$ für alle $c_1, \ldots, c_n \in A$ folgt. Wir führen den Beweis durch Induktion nach n. Für $n = 1$ ist unsere Behauptung durch Folgerung 4.3 bewiesen. Angenommen, sie sei für den Ring $A[x_1, \ldots, x_{n-1}]$ gültig. Wir schreiben $\alpha \in A[x_1, \ldots, x_n]$ in der Gestalt

$$\alpha = \sum_{i=0}^{m} \alpha_i x_n^i$$

mit $\alpha_i \in A[x_1, \ldots, x_{n-1}]$. Aus Satz 5 folgt

$$\alpha(c_1, \ldots, c_n) = \sum_{i=0}^{m} \alpha_i(c_1, \ldots, c_{n-1})\, c_n^i = 0$$

für alle $c_1, \ldots, c_n \in A$. Wir fixieren nun $c_1, \ldots, c_{n-1} \in A$ und betrachten das von diesen Elementen abhängende Polynom der einen Unbestimmten x_n:

$$\beta = \sum_{i=0}^{m} \alpha_i(c_1, \ldots, c_{n-1})\, x_n^i\,.$$

Offenbar gilt $\beta(c) = 0$ für alle $c \in A$, so daß $\beta = 0$ gilt. Daraus folgt $\alpha_i(c_1, \ldots, c_{n-1}) = 0$ für $i = 0, 1, \ldots, m$ und beliebige $c_1, \ldots, c_{n-1} \in A$. Nach Induktionsvoraussetzung muß $\alpha_i = 0$, $i = 0, 1, \ldots, m$, also auch $\alpha = 0$ gelten. $\square$

Der letzte Teil dieses Paragraphen ist der wichtigen Klasse der symmetrischen Polynome gewidmet. Beispiele solcher Polynome haben wir schon in § 4 kennengelernt; sie stehen auf der rechten Seite der Formel (4.14) von VIETA. Um die symmetrischen Polynome zu definieren, betrachten wir zuerst eine natürliche Wirkung der symmetrischen Gruppe S_n über $A[x_1, \ldots, x_n]$, nämlich die Permutation der Unbestimmten x_i:

Für beliebige $s \in S_n$ und $\alpha \in A[x_1, \ldots, x_n]$ definieren wir

$$s\alpha := \alpha(x_{s(1)}, \ldots, x_{s(n)}) \in A[x_1, \ldots, x_n]\,. \tag{4}$$

Nach (3) erhalten wir also $s\alpha$ aus α, indem wir die Unbestimmte x_i durch $x_{s(i)}$ ersetzen. (Hier ist $B = A[x_1, ..., x_n]$, $b_i = x_{s(i)}$.)

Satz 7. *Die Formel* (4) *definiert eine Wirkung der Gruppe* S_n *über* $A[x_1, ..., x_n]$. *Für jedes* $s \in S_n$ *ist die Abbildung* $\alpha \mapsto s\alpha$ *ein Automorphismus des Ringes* $A[x_1, ..., x_n]$.

Beweis. Es seien $s, t \in S_n$, $\alpha \in A[x_1, ..., x_n]$. Dann gilt

$$s(t\alpha) = s(\alpha(x_{t(1)}, ..., x_{t(n)})) = (\alpha(x_{t(1)}, ..., x_{t(n)}))\,(x_{s(1)}, ..., x_{s(n)})$$
$$= \alpha(x_{s(t(1))}, ..., x_{s(t(n))}) = \alpha(x_{s\circ t(1)}, ..., x_{s\circ t(n)}) = (s \circ t)\,\alpha\,.$$

Offenbar gilt $e\alpha = \alpha$. Somit sind alle Bedingungen der Definition 1.4.1 erfüllt.

Nach Satz 5 ist die Abbildung $t_s : \alpha \mapsto s\alpha$ für beliebige $s \in S_n$ ein Endomorphismus des Ringes $A[x_1, ..., x_n]$. Wie in § 1.4 gezeigt wurde, ist t_s bijektiv und daher ein Automorphismus. □

Definition 4. Ein Polynom $\alpha \in A[x_1, ..., x_n]$ heißt *symmetrisch*, wenn $s\alpha = \alpha$ für alle $s \in S_n$ gilt. Die Menge aller symmetrischen Polynome wird mit $A[x_1, ..., x_n]_{S_n}$ bezeichnet.

Folgerung 2. *Das Polynom* α *ist symmetrisch dann und nur dann, wenn* $s\alpha = \alpha$ *für jede Transposition* $s \in S_n$ *gilt.*

Der Beweis ergibt sich unmittelbar aus Satz 7 und Satz 1.2.3. □

Folgerung 3. *Die symmetrischen Polynome bilden einen Unterring von* $A[x_1, ..., x_n]$, *der* A *enthält.*

Beweis. Offenbar gilt $A \subseteq A[x_1, ..., x_n]_{S_n}$. Es seien nun α und β symmetrisch und $s \in S_n$. Nach Satz 5 ist $s(\alpha + \beta) = s\alpha + s\beta = \alpha + \beta$, $s(\alpha\beta) = s\alpha \cdot s\beta = \alpha \cdot \beta$. Somit sind $\alpha + \beta$ und $\alpha \cdot \beta$ symmetrisch; wegen $s(-\alpha) = -s\alpha$ ist mit α auch $-\alpha$ symmetrisch. □

Unsere Aufgabe besteht nun darin, die Struktur des Ringes der symmetrischen Polynome zu untersuchen.

Definition 5. Unter den *elementarsymmetrischen Polynomen* aus $A[x_1, ..., x_n]$ versteht man die folgenden n Polynome:

$$\sigma_1 := x_1 + x_2 + ... + x_n\,,$$
$$\sigma_2 := x_1x_2 + x_1x_3 + ... + x_2x_3 + ... + x_{n-1}x_n\,,$$
$$\sigma_3 := x_1x_2x_3 + x_1x_2x_4 + ... + x_{n-2}x_{n-1}x_n\,,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\sigma_{n-1} := x_1x_2 \ldots x_{n-1} + x_1x_2 \ldots x_{n-2}x_n + ... + x_2x_3 \ldots x_n\,,$$
$$\sigma_n := x_1x_2 \ldots x_n\,.$$

Eine allgemeine Formel für die Definition der elementarsymmetrischen Polynome ist

$$\sigma_k := \sum_{1 \leq i_1 < ... < i_k \leq n} x_{i_1} \ldots x_{i_k}\,, \qquad k = 1, ..., n\,.$$

Man überzeugt sich leicht davon, daß die Polynome σ_k alle symmetrisch sind. Mit Hilfe der σ_k kann man die Formel (4.14) von VIETA in der Gestalt

$$a_k = a_n(-1)^{n-k}\,\sigma_{n-k}(b_1, \ldots, b_n), \qquad k = 0, 1, \ldots, n-1\,, \tag{5}$$

schreiben.

Aus Folgerung 3 ist offensichtlich, daß jeder Ausdruck, den man aus $\sigma_1, \ldots, \sigma_n$ und Elementen von A durch die Operationen der Addition und Multiplikation bildet, wieder ein symmetrisches Polynom ist. Anders gesagt: Ist $\beta \in A[x_1, \ldots, x_n]$, so gilt $\beta(\sigma_1, \ldots, \sigma_n) \in A[x_1, \ldots, x_n]_{S_n}$.

Satz 8 (Hauptsatz über symmetrische Polynome). *Jedes symmetrische Polynom α in n Unbestimmten über A kann man eindeutig als Polynom in den elementarsymmetrischen Polynomen $\sigma_1, \ldots, \sigma_n$ schreiben. Anders ausgedrückt, die Abbildung*

$$\beta \in A[x_1, \ldots, x_n] \mapsto \beta(\sigma_1, \ldots, \sigma_n) \in A[x_1, \ldots, x_n]_{S_n}$$

ist ein Isomorphismus dieser Ringe.

Beweis. Wir führen den Beweis über zwei Hilfssätze.

Lemma 1. *Es sei $\mu = c x_1^{k_1} \ldots x_n^{k_n}$ das höchste Glied eines symmetrischen Polynoms α. Dann gilt $k_1 \geqq \ldots \geqq k_n$.*

Beweis. Angenommen, es existiert ein i mit $k_i < k_{i+1}$. Wir nehmen die Transposition $(i\ i+1)$ und bilden $\alpha = (i\ i+1)\,\alpha$. Folglich muß α auch das Glied

$$(i\ i+1)\,\mu = c x_1^{k_1} \ldots x_{i+1}^{k_i} x_i^{k_{i+1}} \ldots x_n^{k_n} = c x_1^{k_1} \ldots x_i^{k_{i+1}} x_{i+1}^{k_i} \ldots x_n^{k_n}$$

enthalten. Aus unserer Annahme folgt $(i\ i+1)\,\mu > \mu$, und μ kann nicht das höchste Glied sein. □

Lemma 2. *Das höchste Glied des Polynoms $\sigma_1^{l_1} \ldots \sigma_n^{l_n}$, $l_i \in \mathbf{N}_0$, $i = 1, \ldots, n$, hat die Gestalt $x_1^{l_1+l_2+\ldots+l_n} x_2^{l_2+\ldots+l_n} \ldots x_n^{l_n}$; es bestimmt eindeutig die Zahlen $l_1, \ldots, l_n$.*

Beweis. Offensichtlich ist das höchste Glied von σ_i das Element $x_1 \ldots x_i$. Nun wendet man Satz 4 an und erhält die erste Behauptung. Die zweite Behauptung folgt aus der Tatsache, daß das Gleichungssystem

$$\begin{aligned} l_1 + l_2 + \ldots + l_n &= k_1\,, \\ l_2 + \ldots + l_n &= k_2\,, \\ &\cdots\cdots\cdots \\ l_n &= k_n \end{aligned}$$

die eindeutig bestimmte Lösung

$$l_i = k_i - k_{i+1} \qquad (i = 1, \ldots, n-1), \qquad l_n = k_n$$

besitzt. □

Wir beweisen nun Satz 8. Es sei $\alpha \neq 0$ und $c x_1^{k_1} \ldots x_n^{k_n}$ das höchste Glied von α. Nach Lemma 1 gilt $k_i \geqq k_{i+1}$. Für das symmetrische Polynom

$$\gamma_1 = c\sigma_1^{k_1 - k_2} \ldots \sigma_{n-1}^{k_{n-1} - k_n} \sigma_n^{k_n}$$

stimmt das höchste Glied mit dem höchsten Glied des Polynoms α überein. Also ist $\alpha_1 = \alpha - c\gamma_1$ ein symmetrisches Polynom, das 0 ist oder dessen höchstes Glied niedriger als das von α ist. Gilt $\alpha_1 \neq 0$, so können wir diese Überlegung wiederholen; wir kommen in endlich vielen Schritten zum Ende des Verfahrens, wenn wir zeigen können, daß nur endlich viele $(m_1, ..., m_n) \in \mathbf{N}_0^n$ existieren mit $m_1 \geqq ... \geqq m_n$ und $(m_1, ..., m_n) \prec (k_1, ..., k_n)$. Aber für derartige n-Tupel gilt $m_i \leqq m_1 \leqq k_1$, $i = 1, ..., n$. Somit gibt es höchstens $(k_1+1)^n$ derartige Tupel. Aus dem Beweis ist klar, daß es endlich viele Monome $\mu_1, ..., \mu_r \in A[x_1, ..., x_n]$ gibt mit

$$\alpha - \mu_1(\sigma_1, ..., \sigma_n) - ... - \mu_r(\sigma_1, ..., \sigma_n) = 0 .$$

Setzen wir $\beta = \mu_1 + ... + \mu_r$, so folgt $\alpha = \beta(\sigma_1, ..., \sigma_n)$.

Es bleibt die Eindeutigkeit zu zeigen, d. h., die Injektivität des Homomorphismus $\beta \mapsto \beta(\sigma_1, ..., \sigma_n)$ soll nachgewiesen werden. Wir zeigen, daß der Kern 0 ist. Es sei $\beta \in A[x_1, ..., x_n]$ ein Element des Kerns, d. h. $\beta(\sigma_1, ..., \sigma_n) = 0$. Angenommen, es ist $\beta \neq 0$. Wir schreiben nun β als Summe paarweise nicht ähnlicher Monome $\beta = \mu_1 + ... + \mu_k$. Dann gilt

$$\beta(\sigma_1, ..., \sigma_n) = \mu_1(\sigma_1, ..., \sigma_n) + ... + \mu_k(\sigma_1, ..., \sigma_n) .$$

Nach Lemma 2 sind die höchsten Glieder der Polynome $\mu_i(\sigma_1, ..., \sigma_n)$ ebenfalls paarweise nicht ähnlich. Nach Folgerung 1 gibt es unter diesen Gliedern ein höchstes. Folglich enthält das Polynom $\beta(\sigma_1, ..., \sigma_n)$ ein von 0 verschiedenes Glied, was unmöglich ist, es muß also $\beta = 0$ sein. □

Folgerung 4. *Es sei $\varphi \in K[x]$, K ein Körper,* gr $\varphi > 1$, *und L ein Erweiterungskörper von K, über dem φ zerfällt. Es seien $c_1, ..., c_n \in L$ die Nullstellen von φ, wobei jede Nullstelle so oft auftritt, wie ihre Vielfachheit angibt. Dann gilt für jedes symmetrische Polynom $\alpha \in K[x_1, ..., x_n]_{S_n}$*

$$\alpha(c_1, ..., c_n) \in K.$$

Beweis. Nach Satz 8 gibt es ein $\beta \in K[x_1, ..., x_n]$ mit $\alpha = \beta(\sigma_1, ..., \sigma_n)$. Hieraus folgt leicht (vgl. Satz 5 oder Übung 3) $\alpha(c_1, ..., c_n) = \beta(\sigma_1(c_1, ..., c_n), ..., \sigma_n(c_1, ..., c_n))$. Nach (5) gilt $\sigma_i(c_1, ..., c_n) \in K$ und somit auch $\alpha(c_1, ..., c_n) \in K$. □

Beispiel 1. Wir betrachten das Polynom

$$\delta = \prod_{1 \leqq i < j \leqq n} (x_i - x_j)^2.$$

Man prüft leicht nach (vgl. Übung 1.2.3), daß δ symmetrisch ist. Aus Satz 8 folgt die Existenz eines Polynoms $\Delta \in \mathbf{Z}[x_1, ..., x_n]$, für das

$$\delta = \Delta(-\sigma_1, \sigma_2, ..., (-1)^n \sigma_n)$$

gilt. Die Polynome δ und Δ kann man auch als Elemente des Ringes $A[x_1, ..., x_n]$ über einen beliebigen Integritätsbereich A ansehen. Betrachten wir das Polynom

$$\varphi = x^n + c_1 x^{n-1} + ... + c_n \tag{6}$$

mit den Nullstellen $b_1, ..., b_n$ aus einem Zerfällungsring A von φ, so folgt aus (5)

$$\Delta(c_1, ..., c_n) = \delta(b_1, ..., b_n) = \prod_{i<j} (b_i - b_j)^2. \tag{7}$$

(Man beachte die von Satz 4.8 abweichende Bezeichnung der Koeffizienten von φ in (6).) Das Element (7) des Ringes A heißt die *Diskriminante* des Polynoms φ. Offensichtlich gilt $\Delta(c_1, ..., c_n)=0$ genau dann, wenn φ mehrfache Nullstellen besitzt.

Übung 5. Man berechne das Polynom Δ für $n=2$ und $n=3$.

Übung 6. Die symmetrischen Polynome

$$s_k := x_1^k + ... + x_n^k, \qquad k=1, 2, ...,$$

heißen die *Potenzsummen*. a) Man beweise die folgenden *Newtonschen Formeln:*

$$s_k - s_{k-1}\sigma_1 + s_{k-2}\sigma_2 - ... + (-1)^{k-1} s_1\sigma_{k-1} + (-1)^k k\sigma_k = 0 \quad \text{für} \quad k \leqq n,$$
$$s_k - s_{k-1}\sigma_1 + s_{k-2}\sigma_2 - ... + (-1)^n s_{k-n}\sigma_n = 0 \quad \text{für} \quad k > n.$$

b) Man drücke mit Hilfe dieser Formeln die Potenzsummen s_2 und s_3 durch die elementarsymmetrischen Polynome aus. — c) Es sei K ein Körper der Charakteristik 0. Man beweise: Die Abbildung

$$\beta \in K[x_1, ..., x_n] \mapsto \beta(s_1, ..., s_n) \in K[x_1, ..., x_n]_{S_n}$$

ist ein Isomorphismus, d. h., Satz 8 bleibt über dem Körper K bei Ersetzung der σ_i durch die s_i, $i=1, ..., n$, gültig.

Beispiel 2. Es sei K ein Körper. Dann wird der Quotientenkörper des Polynomringes $K[x_1, ..., x_n]$,

$$K(x_1, ..., x_n) := Q(K[x_1, ..., x_n]), \tag{8}$$

der nach Satz 1 und Satz 6.2 definiert ist, der *Körper der rationalen Funktionen in den n Unbestimmten* $x_1, ..., x_n$ *über* K genannt. Für $n=1$ stimmt diese Definition mit Beispiel 6.2 überein. Die folgende Übung verallgemeinert Übung 6.5:

Übung 7. Es sei K ein unendlicher Körper und $f \in K(x_1, ..., x_n)$. Wir ordnen f folgendermaßen eine Funktion $\tilde{f}$ zu: Der Definitionsbereich von $\tilde{f}$ sei

$$D_f := \{(c_i) \in K^n \mid \text{es gibt } \alpha, \beta \in K[x_1, ..., x_n] \text{ mit } f = \alpha/\beta \text{ und } \beta(c_1, ..., c_n) \neq 0\}; \tag{9}$$

für jedes $(c_i) \in D_f$ setzen wir $\tilde{f}(c_1, ..., c_n) = \alpha(c_1, ..., c_n)/\beta(c_1, ..., c_n)$. Man beweise: a) $\tilde{f}(c_1, ..., c_n)$ hängt nicht von der Wahl der Darstellung (9) ab. — b) Für beliebige f, $g \in K(x_1, ..., x_n)$ gelten

$$\emptyset \neq D_f \cap D_g = D_{f \cdot g} \subseteq D_{f+g}, \tag{10}$$
$$D_{1/f} = K^n \setminus \tilde{f}^{-1}(0). \tag{11}$$

c) Bei Einschränkung auf geeignete Definitionsbereiche der Gestalt D_h, $h \in K(x_1, ..., x_n)$, gelten

$$\widetilde{f \pm g} = \tilde{f} \pm \tilde{g}, \qquad \widetilde{f \cdot g} = \tilde{f} \cdot \tilde{g}, \qquad \widetilde{(1/f)} = 1/\tilde{f}. \tag{12}$$

Dabei ist $\tilde{f}=0$ genau dann, wenn $f=0$ ist, und offenbar gilt $\tilde{1}=1$. Im Sinne von b) ist also die Zuordnung $f \mapsto \tilde{f}$ für unendliche Körper ein Isomorphismus von $K(x_1, ..., x_n)$ auf den Körper der rationalen Funktionen aus K^n in K.

Übung 8. Man verallgemeinere (4) und Definition 4 auf $K(x_1, ..., x_n)$ und zeige: Gilt char $K=0$, so ist $K(x_1, ..., x_n)_{S_n}$ kanonisch isomorph zu $Q(K[x_1, ..., x_n]_{S_n})$. Hieraus folgt: Jede symmetrische rationale Funktion $f \in K(x_1, ..., x_n)_{S_n}$ läßt sich als rationale Funktion der elementarsymmetrischen Polynome $\sigma_1, ..., \sigma_n$ schreiben.

§ 8. Polynome über den Körpern der komplexen und reellen Zahlen

In diesem Paragraphen betrachten wir den Ring $K[x]$ mit $K = \mathbf{C}$ oder $K = \mathbf{R}$. Hier lassen sich die irreduziblen Polynome vollständig beschreiben. Grundlage dafür ist der sogenannte „Fundamentalsatz der Algebra" von C. F. GAUSS:

Satz 1. *Jedes Polynom $\alpha \in \mathbf{C}[x]$ mit $\operatorname{gr} \alpha > 0$ besitzt im Körper $\mathbf{C}$ eine Nullstelle.*

Einen Beweis dieses Satzes werden wir im nächsten Kapitel geben. Wir wollen jetzt einige wichtige Folgerungen aus ihm herleiten.

Folgerung 1. *Der Körper $\mathbf{C}$ ist Zerfällungsring für jedes Polynom $\alpha \in \mathbf{C}[x]$ mit $\operatorname{gr} \alpha > 0$.*

Beweis. Es seien $c_1, \ldots, c_r$ alle verschiedenen Nullstellen des Polynoms α, $k_1, \ldots, k_r$ ihre Vielfachheiten. Wir betrachten die Darstellung (4.9) von α. Offenbar kann β keine Nullstellen haben. Nach Satz 1 ist also $\operatorname{gr} \beta = 0$, und es gilt (4.10). □

Folgerung 2. *Jedes Polynom $\alpha \in \mathbf{C}[x]$, $\alpha \neq 0$, ist eindeutig (bis auf die Reihenfolge der Faktoren) in der Form*

$$\alpha = a\,(x - c_1)^{k_1} \ldots (x - c_r)^{k_r}, \qquad c_i \neq c_j \quad \text{für} \quad i \neq j\,,$$

darstellbar; hier bezeichnet $a \in \mathbf{C}$ den höchsten Koeffizienten von α, $c_i \in \mathbf{C}$ sind die verschiedenen Nullstellen von α und $k_i \in \mathbf{N}$ ihre Vielfachheiten, $i = 1, \ldots, r$, $r \in \mathbf{N}_0$. □

Folgerung 3. *Ein Polynom über dem Körper $\mathbf{C}$ ist irreduzibel genau dann, wenn sein Grad 1 ist.* □

Folgerung 4. *Die einfachen Brüche des Körpers $\mathbf{C}(x)$ haben die Gestalt $a\,(x-c)^{-k}$ mit $a, c \in \mathbf{C}$, $a \neq 0$, $k \in \mathbf{N}$.* □

Wir wollen nun Polynome mit reellen Koeffizienten betrachten. Aus der Einbettung $\mathbf{R}[x] \subset \mathbf{C}[x]$ ergibt sich folgende wichtige Eigenschaft ihrer Nullstellen:

Satz 2. *Es sei $\alpha \in \mathbf{R}[x]$ und $c \in \mathbf{C}$ eine Nullstelle von α. Dann ist ihre konjugierte Zahl $\bar{c}$ ebenfalls eine Nullstelle von α.*

Beweis. Sind a_j die Koeffizienten von α, so gilt

$$0 = \alpha(c) = a_0 + a_1 c + \ldots + a_n c^n.$$

Aus Satz 3.6 folgt

$$0 = \bar{0} = \overline{\alpha(c)} = \bar{a}_0 + \bar{a}_1 \bar{c} + \ldots + \bar{a}_n \bar{c}^n = a_0 + a_1 \bar{c} + \ldots + a_n \bar{c}^n;$$

denn wegen $a_j \in \mathbf{R}$ ist $a_j = \bar{a}_j$. □

Satz 3. *Ein Polynom $\alpha \in \mathbf{R}[x]$ ist irreduzibel dann und nur dann, wenn es entweder ein Polynom ersten Grades ist oder wenn α ein Polynom zweiten Grades ist, das keine reellen Nullstellen besitzt.*

Beweis. Daß die angegebenen Polynome irreduzibel sind, wurde bereits in Beispiel 5.6 bewiesen. Es sei umgekehrt $\alpha \in \mathbf{R}[x]$ irreduzibel. Wegen $\operatorname{gr} \alpha > 0$ hat α

nach Satz 1 eine Nullstelle $c \in \mathbf{C}$. Gilt $c \in \mathbf{R}$, so folgt aus Satz 4.5

$$\alpha = (x-c)\,\beta, \qquad \beta \in \mathbf{R}[x]\,. \tag{1}$$

Da α irreduzibel ist, muß $\operatorname{gr}\beta = 0$ sein. Im Fall $c \notin \mathbf{R}$ ist $\bar{c} \neq c$ eine weitere Nullstelle von α in $\mathbf{C}$. Daher gilt

$$\alpha = (x-c)\,(x-\bar{c})\,\gamma, \qquad \gamma \in \mathbf{C}[x]\,,$$

$$\alpha = (x^2-(c+\bar{c})\,x+c\bar{c})\,\gamma\,.$$

Wegen $c+\bar{c} = 2R(c) \in \mathbf{R}$ und $c\bar{c} = |c|^2 \in \mathbf{R}$ liegt das Polynom $x^2-(c+\bar{c})\,x+c\bar{c}$ in $\mathbf{R}[x]$, und nach Satz 5.9 gilt daher auch $\gamma \in \mathbf{R}[x]$. Weil α irreduzibel ist, muß $\operatorname{gr}\gamma = 0$, d. h. α ein Polynom zweiten Grades ohne reelle Nullstellen sein. □

Folgerung 5. *Jedes Polynom $\alpha \in \mathbf{R}[x]$, $\alpha \neq 0$, ist eindeutig (bis auf die Reihenfolge der Faktoren) in der Form*

$$\alpha = a\,(x-c_1)^{k_1} \ldots (x-c_r)^{k_r}\,(x^2+p_1x+q_1)^{l_1} \ldots (x^2+p_sx+q_s)^{l_s}$$

darstellbar; hierbei bezeichnen $a \in \mathbf{R}$, $a \neq 0$, den höchsten Koeffizienten, $r \in \mathbf{N}_0$ die Anzahl der verschiedenen reellen Nullstellen, $s \in \mathbf{N}_0$ die Anzahl der verschiedenen irreduziblen Teiler zweiten Grades, $k_j, l_j \in \mathbf{N}$ ihre Vielfachheiten, und es gilt $c_i, p_j, q_j \in \mathbf{R}$, $p_j^2 < 4q_j$ für $j = 1, \ldots, s$. □

Folgerung 6. *Die einfachen Brüche des Körpers $\mathbf{R}(x)$ haben die Gestalt*

$$\frac{a}{(x-c)^k} \quad \text{oder} \quad \frac{ax+b}{(x^2+px+q)^k} \quad \text{mit} \quad k \in \mathbf{N},\ a, b, c, p, q \in \mathbf{R}$$

und $p^2 < 4q$; hierbei ist $a \neq 0$ bzw. $ax+b \neq 0$. □

Die Berechnung der Nullstellen eines reellen oder komplexen Polynoms ist eine für die Anwendungen sehr wichtige, aber keineswegs immer einfache Aufgabe. Für $n = 2, 3, 4$ gibt es explizite Formeln, die wir hier nicht herleiten wollen. Für $n = 2$ sind sie aus der Elementarmathematik bekannt (siehe auch Lemma 3.5.1), für $n = 3$ gelten die Formeln von CARDANO und für $n = 4$ die von FERRARI. Für Polynome vom Grad ≥ 5 kann man mit Hilfe der Theorie von E. GALOIS (vgl. etwa R. KOCHENDÖRFFER [1]) beweisen, daß keine expliziten Formeln existieren, die es gestatten, die Nullstellen eines allgemeinen Polynoms mit Hilfe von Radikalen (Wurzelausdrücken) zu berechnen; in der Praxis werden für $n \geq 3$ meist Näherungsmethoden zur Berechnung der Nullstellen angewandt (vgl. I. S. BERESIN und N. P. SHIDKOW [1]). In diesem Paragraphen wollen wir nur einige einfache Sätze über die Lage der reellen Nullstellen eines reellen Polynoms herleiten, die für die Bestimmung der Nullstellen nützlich sein können.

Satz 4. *Es sei $\varphi = a_0 + a_1x + \ldots + a_nx^n$ ein reelles Polynom, $a_i \in \mathbf{R}$, $a_n > 0$ und wenigstens ein $a_i < 0$. Mit A bezeichnen wir das Maximum der Beträge der negativen Koeffizienten von φ und mit k die größte Zahl, für die $a_k < 0$ gilt. Dann ist jede reelle Nullstelle von φ kleiner als*

$$M := 1 + \sqrt[n-k]{A/a_n}\,.$$

Beweis. Wir ersetzen die Koeffizienten $a_0, a_1, \ldots, a_k$ durch $-A$ und die $a_{k+1}, \ldots, a_{n-1}$ durch 0. Dann gilt für jedes $c>1$

$$\varphi(c) \geqq -A\,(1+c+\ldots+c^k)+a_n c^n$$
$$\geqq a_n c^n - A\,\frac{c^{k+1}-1}{c-1} = a_n c^n - \frac{Ac^{k+1}}{c-1} + \frac{A}{c-1}\,.$$

Für $c>1$ folgt durch Streichen des letzten Summanden

$$\varphi(c) > a_n c^n - \frac{Ac^{k+1}}{c-1} = c^{k+1}\left(a_n c^{n-k-1} - \frac{A}{c-1}\right)$$
$$> c^{k+1}\left(a_n\,(c-1)^{n-k-1} - \frac{A}{c-1}\right) = \frac{c^{k+1}}{c-1}\,(a_n\,(c-1)^{n-k} - A)\,.$$

Ist nun $c \geqq M$, so gilt $c>1$ und $(c-1)^{n-k} \geqq A/a_n$, also $\varphi(c)>0$. □

Satz 5. *Es sei* $\varphi \in \mathbf{R}[x]$ *und* $n = \operatorname{gr}\varphi$. *Für ein gewisses* $M \in \mathbf{R}$, $M>0$, *gelte* $\varphi^{(k)}(M) \geqq 0$, $k=0, 1, \ldots, n-1$, *und* $\varphi^{(n)}(M)>0$ (*d. h.* $a_n>0$). *Dann ist jede reelle Nullstelle des Polynoms* φ *kleiner oder gleich* M.

Beweis. Aus der Taylor-Entwicklung (4.17) im Punkt M ersieht man unmittelbar, daß $\varphi(c)>0$ für $c>M$ gilt. □

Bemerkung. Will man eine untere Schranke für die reellen Nullstellen des Polynoms φ finden, so betrachtet man das Polynom $\varphi(-x)$ und bestimmt für dieses eine obere Schranke M'; um die Sätze 4 oder 5 anwenden zu können, muß man eventuell $\varphi(-x)$ mit -1 multiplizieren, wodurch die Nullstellen nicht geändert werden. Dann ist offenbar $m=-M'$ eine untere Schranke.

Übung 1. Es sei $M>0$ größer als alle reellen Nullstellen des Polynoms $\varphi = a_0 + a_1 x + \ldots + a_n x^n$ und $M_1>0$ größer als alle Nullstellen des Polynoms $\psi = a_n + a_{n-1}x + \ldots + a_0 x^n$. Man beweise, daß alle positiven Nullstellen des Polynoms φ in dem offenen Intervall $]M_1^{-1}, M[$ liegen.

Der folgende Satz gibt eine einfache Abschätzung für die Anzahl der positiven Nullstellen eines reellen Polynoms. Dabei verstehen wir unter „*Anzahl der Nullstellen*“ – im Unterschied zu „Anzahl der verschiedenen Nullstellen“ – stets, daß jede Nullstelle so oft gezählt wird, wie ihre Vielfachheit angibt.

Satz 6 (Zeichenregel von Descartes). *Es sei* $\varphi = a_0 + a_1 x + \ldots + a_n x^n$, $a_i \in \mathbf{R}$, $a_n \neq 0$, *ein reelles Polynom,* $p(\varphi)$ *die Anzahl der positiven Nullstellen des Polynoms* φ *und* $q(\varphi)$ *die Anzahl der Vorzeichenwechsel in der Folge seiner Koeffizienten* $(a_0, a_1, \ldots, a_n)$. *Dann gilt* $p(\varphi) \leqq q(\varphi)$, *und* $q(\varphi) - p(\varphi)$ *ist eine gerade Zahl.*

Beweis. Offenbar gilt $p(-\varphi) = p(\varphi)$ und $q(-\varphi) = q(\varphi)$; daher können wir $a_n>0$ voraussetzen. Wir nehmen ferner an, daß die Zahl 0 eine k-fache ($k \geqq 0$) Nullstelle von φ sei. Dann gilt $a_0 = a_1 = \ldots = a_{k-1} = 0$, $a_k \neq 0$, und $\varphi = x^k \psi$, wobei $\psi = a_k + a_{k+1}x + \ldots + a_n x^{n-k}$ ist. Offensichtlich ist wieder $p(\varphi) = p(\psi)$ und $q(\varphi) = q(\psi)$, so daß wir o. B. d. A. $a_0 = \varphi(0) \neq 0$ voraussetzen können. Zuerst zeigen wir, daß $p(\varphi)$ und $q(\varphi)$ beide gerade oder beide ungerade sind. Wegen $a_n>0$ gilt $\varphi(c)>0$ für

genügend großes c. Hieraus folgt: $q(\varphi)$ ist gerade genau dann, wenn $\varphi(0)=a_0>0$ gilt, und das ist dann und nur dann der Fall, wenn die Funktion φ auf $]0,\infty[$ eine gerade Anzahl Mal das Vorzeichen ändert. Da ein Polynom stetig ist (hier machen wir von speziellen Eigenschaften der reellen Zahlen Gebrauch, die in der Analysis bewiesen werden) kann eine Vorzeichenänderung nur an einer Nullstelle eintreten. Es sei also b eine Nullstelle der Vielfachheit k. Dann gilt $\varphi=(x-b)^k\,\beta$ und $\beta(b)\neq 0$. Hieraus erkennt man: φ ändert an der Nullstelle b sein Vorzeichen genau dann, wenn k ungerade ist. Somit ist $p(\varphi)$ gerade genau dann, wenn φ die positive x-Achse $]0,\infty[$ eine gerade Anzahl Mal schneidet.

Wir beweisen nun $p(\varphi)\leqq q(\varphi)$ durch Induktion nach $n=\operatorname{gr}\varphi$. Angenommen, dies sei schon für alle Polynome vom Grad $\leqq n-1$ bewiesen, und es sei $\operatorname{gr}\varphi=n$. Dann gilt für die Ableitung $\operatorname{gr}\varphi'=n-1$, und aus der Induktionsvoraussetzung folgt $p(\varphi')\leqq q(\varphi')$. Es seien nun $c_1<c_2<\ldots<c_r$ alle verschiedenen, positiven Nullstellen von φ und k_i, $i=1,\ldots,r$, ihre Vielfachheiten. Aus Satz 4.11 ergibt sich, daß die Nullstelle c_i eine Nullstelle der Vielfachheit k_i-1 von φ' ist. Ferner erhält man aus dem in der Analysis bekannten Satz von Rolle, daß zwischen zwei Nullstellen von φ wenigstens eine Nullstelle von φ' liegen muß. Also gilt

$$p(\varphi')\geqq\sum_{i=1}^{r}(k_i-1)+r-1=p(\varphi)-1\,.$$

Aus der Gestalt des Polynoms φ' folgt $q(\varphi')\leqq q(\varphi)$. Somit erhalten wir

$$p(\varphi)-1\leqq p(\varphi')\leqq q(\varphi')\leqq q(\varphi)\,.$$

Aus $p(\varphi)\leqq q(\varphi)+1$ ergibt sich nun $p(\varphi)\leqq q(\varphi)$; denn nach dem zuerst Bewiesenen kann der Fall $p(\varphi)=q(\varphi)+1$ nicht eintreten. □

Folgerung 7. *Die Anzahl der negativen Nullstellen eines reellen Polynoms φ ist nicht größer als $q(\psi)$, wobei $\psi:=\varphi(-x)$ gesetzt wurde; diese Anzahl ist gerade genau dann, wenn $q(\psi)$ gerade ist.* □

Satz 7. *Ist* $\mathbf{R}$ *ein Zerfällungskörper des Polynoms φ, so gilt $p(\varphi)=q(\varphi)$, und die Anzahl der negativen Nullstellen ist gleich $q(\psi)$ mit $\psi:=\varphi(-x)$.*

Beweis. Wie beim Beweis von Satz 6 können wir wieder $\varphi(0)\neq 0$ annehmen. Dann gilt $p(\varphi)+p(\psi)=n$, $n:=\operatorname{gr}\varphi$. Aus Satz 6 und Folgerung 7 erhalten wir $q(\varphi)+q(\psi)\geqq n$. Aber andererseits muß $q(\varphi)+q(\psi)\leqq n$ gelten; schreibt man nämlich in den für die Bestimmung von $q(\varphi)$ bzw. $q(\psi)$ maßgeblichen Folgen

$$a_0, a_1, \ldots, a_n \tag{2}$$

bzw.

$$a_0, -a_1, a_2, \ldots, (-1)^n a_n \tag{3}$$

für die a_j, die 0 sind, irgendeine von 0 verschiedene Zahl hin, so kann sich die Anzahl der Vorzeichenwechsel höchstens vergrößern. Wir können daher $a_i\neq 0$ für $i=0,1,\ldots,n$ annehmen. Nun ändert sich in (2) beim i-ten Übergang das Vorzeichen genau dann, wenn es sich in (3) nicht ändert, so daß in diesem Fall $q(\varphi)+q(\psi)=n$ gilt. Somit folgt $q(\varphi)+q(\psi)=n$ allgemein, und es muß nach Satz 6 $p(\varphi)=q(\varphi)$ und $p(\psi)=q(\psi)$ sein. □

Der folgende Satz gibt die Möglichkeit, die Anzahl der verschiedenen reellen Nullstellen eines reellen Polynoms $\varphi \in \mathbf{R}[x]$ zu ermitteln.

Satz 8 (Satz von STURM). *Es sei* $\varphi \in \mathbf{R}[x]$, $\varphi \neq 0$. *Wir setzen* $\varphi_0 := \varphi$, $\varphi_1 := \varphi'$ *und bestimmen mit Hilfe des euklidischen Algorithmus* (§ 5) *eine endliche Folge von Polynomen* φ_j *aus*

$$\varphi_0 = \gamma_1 \varphi_1 - \varphi_2, \qquad \varphi_1 = \gamma_2 \varphi_2 - \varphi_3, \ \ldots, \ \varphi_{k-1} = \gamma_k \varphi_k . \tag{4}$$

Für $a \in \mathbf{R}$ *mit* $\varphi(a) \neq 0$ *sei* $w(a)$ *die Anzahl der Vorzeichenwechsel in der Folge* $(\varphi_j(a))$, $j = 0, \ldots, k$, *in der die Nullen* $\varphi_j(a) = 0$ *fortzulassen sind. Dann gilt: Für jedes Intervall* $I = \{x \in \mathbf{R} \mid b \leqq x \leqq c\}$, *für das* $\varphi(b) \neq 0$ *und* $\varphi(c) \neq 0$ *gelten, ist die Anzahl der verschiedenen, in I liegenden Nullstellen von* φ *gleich* $w(b) - w(c)$.

Beweis. Nach dem Beweis von Satz 5.1 ist φ_k der ggT von φ und φ'; φ_k teilt somit alle φ_j. (Dabei stört es nicht, daß wir die Reste in (4) mit entgegengesetztem Vorzeichen genommen haben.) Somit ist wegen $\varphi(a) \neq 0$ die Anzahl $w(a)$ der Vorzeichenwechsel in der Folge $(\varphi_j(a))$ und in der Folge $(\mu_j(a))$ mit $\mu_j := \varphi_j / \varphi_k$ dieselbe, und es gilt $\varphi_j(a) = 0$ genau dann, wenn $\mu_j(a) = 0$ gilt, $j = 0, \ldots, k-1$; ferner ist $\mu_k = 1$. Wir betrachten die Folge $(\mu_j(a))$ in Abhängigkeit von a. Aus der Analysis ist bekannt, daß jedes Polynom eine stetige Funktion ist; daher ändert $\mu_j(x)$ sein Vorzeichen höchstens an einer Nullstelle von μ_j. Die sämtlichen Nullstellen der Polynome μ_j teilen $\mathbf{R}$ in endlich viele Intervalle ein, und die Anzahl $w(a)$ kann sich höchstens dann ändern, wenn a eine dieser Nullstellen überstreicht. Es sei etwa $\mu_0(a) \neq 0$ und $\mu_j(a) = 0$ für ein j mit $0 < j < k$. Dann müssen $\varphi_j(a) = 0$ und sowohl $\varphi_{j-1}(a) \neq 0$ als auch $\varphi_{j+1}(a) \neq 0$ sein; wäre das nicht so, so wären wegen (4) alle $\varphi_l(a)$ mit $l \leqq j$ gleich 0, was zu dem Widerspruch $\varphi(a) = 0$ führen würde. Daher sind auch in der Folge $(\mu_j(a))$, $j = 0, \ldots, k$, niemals zwei benachbarte Glieder gleichzeitig 0. Da aus (4) bei Division durch φ_k speziell $\mu_{j-1}(a) = -\mu_{j+1}(a)$ folgt, ändert sich $w(a)$ an einer Nullstelle a von μ_j, für die $\varphi(a) \neq 0$ gilt, nicht. Es bleibt der Fall zu betrachten, daß $\varphi(a) = \mu_0(a) = 0$ gilt. Dann ist a eine Nullstelle einer gewissen Ordnung $p \in \mathbf{N}$ von φ. Nach Division von

$$\varphi_0 = (x-a)^p \beta, \qquad \varphi_1 = p\,(x-a)^{p-1} \beta + (x-a)^p \beta'$$

durch φ_k folgt

$$\mu_0 = (x-a)\,\beta_1, \qquad \mu_1 = p\beta_1 + (x-a)\,\beta_2$$

mit $\beta_1(a) \neq 0$, also auch $\mu_1(a) \neq 0$. Unabhängig vom Vorzeichen von $\beta_1(a)$ folgt hieraus $w(a-\varepsilon) = w(a+\varepsilon) + 1$ für genügend kleines $\varepsilon > 0$; denn die Werte der $\mu_j(a)$ für $j > 0$ tragen nicht zur Änderung von w bei, was wegen $\mu_1(a) \neq 0$ genauso wie im Fall $\mu_0(a) \neq 0$ folgt. Daraus ergibt sich sofort die Behauptung. □

Bemerkung. Die konstruierte Folge (φ_j), $j = 0, \ldots, k$, wird auch eine *Sturmsche Reihe* für φ genannt. Interessiert man sich für die Anzahl aller verschiedenen reellen Nullstellen von φ, so genügt es, die höchsten Koeffizienten der Polynome

$$\varphi_j = a_j x^{n_j} + \ldots$$

zu betrachten. Weil für genügend große $c \in \mathbf{R}$ das Vorzeichen von $\varphi_j(c)$ gleich dem von a_j ist, erhält man $w(c)$ als Anzahl der Vorzeichenwechsel in der Folge $(a_0, a_1, \ldots, a_k)$ und analog $w(b)$ für genügend kleine negative b als Anzahl der Vorzeichenwechsel in der Folge $(a_0(-1)^{n_0}, a_1(-1)^{n_1}, \ldots, a_k(-1)^{n_k})$, so daß sich die Berechnung spezieller Werte $\varphi_j(b)$, $\varphi_j(c)$ erübrigt.

§ 9. Lineare Gleichungssysteme. Gaußscher Algorithmus

Das Thema dieses Paragraphen ist die Untersuchung linearer Gleichungssysteme. Diese Gleichungssysteme sind für die Anwendungen von großer Wichtigkeit; viele Verfahren der numerischen Mathematik führen auf die Lösung derartiger Systeme. Ihre Theorie ist ein wichtiger Teil der linearen Algebra, die wir in den Kapiteln 4 bis 6 im Zusammenhang mit der Geometrie darstellen wollen. Der in diesem Paragraphen zu beschreibende Gaußsche Algorithmus jedoch ist eine rein algebraische Angelegenheit; er stützt sich allein auf die Rechenregeln in einem Körper.

Definition 1. Es sei K ein *Körper*. Ein *lineares Gleichungssystem aus m Gleichungen mit n Unbekannten* hat die Form

$$\left.\begin{aligned} &a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ &a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m\,, \end{aligned}\right\} \tag{1}$$

wobei $a_{ij}, b_i \in K$ gilt für $i = 1, \ldots, m$, $j = 1, \ldots, n$ und die x_j, $j = 1, \ldots, n$, Unbestimmte sind. Das System (1) heißt *homogen*, wenn alle b_i gleich 0 sind. Die Matrix (vgl. (0.2.39))

$$(a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}$$

heißt die *Matrix des Systems* (1), und die Matrix

$$(a_{ij}\ b_i) = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} & b_1 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} & b_m \end{pmatrix}$$

seine *erweiterte Matrix*. Ein n-Tupel $(c_j) = (c_1, \ldots, c_n) \in K^n$ von Elementen $c_i \in K$ heißt eine *Lösung* des Systems (1), wenn bei Einsetzen $x_j = c_j$, $j = 1, \ldots, n$, die Gleichungen

$$\sum_{j=1}^{n} a_{ij}c_j = b_i\,, \qquad i = 1, \ldots, m\,, \tag{2}$$

erfüllt sind. Das System (1) heißt *lösbar*, wenn wenigstens eine Lösung $(c_j) \in K^n$ existiert, und *unlösbar* sonst.

Beispiel 1. Ein homogenes System ist stets lösbar; denn es besitzt die *triviale Lösung* $c_j = 0$, $j = 1, \ldots, n$.

Offenbar ist ein lineares Gleichungssystem durch Angabe seiner erweiterten Matrix vollständig bestimmt; die Gleichungen entsprechen den Zeilen der Matrix, die Koeffizienten bei derselben Unbekannten (man sagt hier aus naheliegenden Gründen „Unbekannte" statt „Unbestimmte") füllen jeweils eine Spalte, und die rechte Seite füllt die letzte, $(n+1)$-te Spalte. Im folgenden werden wir mit den Gleichungen elementare Operationen ausführen. Diese übertragen sich entsprechend auf die Zeilen der Matrix (und umgekehrt). Die Matrixschreibweise ist oft kürzer und übersichtlicher.

Definition 2. Zwei lineare Gleichungssysteme mit n Unbekannten über dem Körper K heißen *äquivalent*, wenn sie dieselbe Lösungsmenge besitzen.

Speziell sind alle unlösbaren Gleichungssysteme mit n Unbekannten äquivalent. Der Gaußsche Algorithmus besteht nun darin, das gegebene Gleichungssystem (1) durch elementare Umformungen in ein äquivalentes Gleichungssystem zu verwandeln, dessen Lösungsmenge man unmittelbar angeben kann.

Definition 3. Unter einer *elementaren Umformung* eines linearen Gleichungssystems (bzw. einer Matrix mit Elementen aus K) versteht man jede der folgenden Operationen:

I. Vertauschung zweier Gleichungen (bzw. Zeilen);

II. Multiplikation der l-ten Gleichung (bzw. aller Elemente der l-ten Zeile) mit $c \in K$ und Addition zur i-ten Gleichung (bzw. zum entsprechenden Element der i-ten Zeile) für $i \neq l$. Für die neue i-te Gleichung (bzw. Zeile) gilt also

$$\hat{a}_{ij} = a_{ij} + ca_{lj}\,, \qquad \hat{b}_i = b_i + cb_l\,, \qquad i \neq l; \tag{3}$$

alle übrigen Gleichungen (bzw. Zeilen), auch die l-te, bleiben ungeändert.

III. Die Multiplikation einer Gleichung (bzw. aller Elemente einer Zeile) mit $c \in K^*$.

Satz 1. *Bei einer elementaren Umformung geht ein lineares Gleichungssystem* (1) *in ein äquivalentes System über.*

Beweis. Für die Umformungen vom Typ I oder III ist die Behauptung trivial. Wir betrachten eine Umformung vom Typ II. Es sei $(c_1, \ldots, c_n)$ eine Lösung von (1). Denken wir uns die c_j eingesetzt, multiplizieren die l-te Gleichung mit c und addieren sie zur i-ten, so folgt

$$\sum_{j=1}^{n} \hat{a}_{ij}c_j = \sum_{j=1}^{n} a_{ij}c_j + c\sum_{j=1}^{n} a_{lj}c_j = b_i + cb_l = \hat{b}_i\,.$$

Somit erfüllt (c_j) auch das umgeformte System. Daß jede Lösung des neuen Systems auch Lösung des ursprünglichen ist, folgt ebenso; denn wegen $i \neq l$ erhalten wir durch $a_{ij} = \hat{a}_{ij} - ca_{lj}$, $b_i = \hat{b}_i - cb_l$ das alte System aus dem neuen wiederum durch eine Operation vom Typ II. □

Wir wenden nun die elementaren Umformungen mit dem Ziel an, die linke Seite von (1) auf eine einfache Gestalt zu bringen. Der Kürze halber schreiben wir nur die Matrix des Systems hin; man beachte jedoch, daß bei der praktischen Durchführung alle Operationen mit der erweiterten Matrix auszuführen sind.

Definition 4. Eine Matrix vom Typ m, n mit Elementen aus K heißt eine *Stufenmatrix*, wenn sie die Gestalt

$$\begin{bmatrix} 0 \dots c_{1k_1} & c_{1,k_1+1} \cdots c_{1k_2} & c_{1,k_2+1} \cdots c_{1k_r} & c_{1,k_r+1} \cdots c_{1n} \\ 0 \dots 0 \quad 0 & \cdots c_{2k_2} & c_{2,k_2+1} \cdots c_{2k_r} & c_{2,k_r+1} \cdots c_{2n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ 0 \dots 0 \quad 0 & \dots 0 \quad 0 & \cdots c_{rk_r} & c_{r,k_r+1} \cdots c_{rn} \\ 0 \dots 0 \quad 0 & \dots 0 \quad 0 & \dots 0 \quad 0 & \dots 0 \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ 0 \dots 0 \quad 0 & \dots 0 \quad 0 & \dots 0 \quad 0 & \dots 0 \end{bmatrix} \tag{4}$$

mit $1 \leqq k_1 < \dots < k_r \leqq n$, $0 \leqq r \leqq m$ und $c_{ik_i} \neq 0$ für $i = 1, \dots, r$ besitzt. Sie heißt eine *spezielle Stufenmatrix*, wenn außerdem noch

$$c_{lk_i} = 0 \quad \text{für} \quad l < i \quad \text{und} \quad c_{ik_i} = 1$$

gilt.

Satz 2. *Jede Matrix mit Elementen aus K kann durch elementare Umformungen in eine spezielle Stufenmatrix verwandelt werden.*

Beweis. Wir zeigen zuerst, daß wir die Matrix (a_{ij}) durch elementare Umformungen in eine Stufenmatrix verwandeln können. Wenn alle Elemente der Matrix 0 sind, ist sie spezielle Stufenmatrix mit $r = 0$. Andernfalls sei k_1 die kleinste Spaltennummer, für die ein $a_{ik_1} \neq 0$ vorhanden ist. Durch eine Zeilenvertauschung können wir erreichen, daß $a_{1k_1} \neq 0$ gilt. Multiplizieren wir nun nacheinander die erste Zeile mit $-a_{jk_1}/a_{1k_1}$ und addieren sie jeweils elementweise zur j-ten, $j > 1$, so erhalten wir eine Matrix der Gestalt

$$\begin{pmatrix} 0 \dots 0 & a_{1k_1} & a_{1,k_1+1} \cdots a_{1n} \\ 0 \dots 0 \quad 0 & \tilde{a}_{2,k_1+1} \cdots \tilde{a}_{2n} \\ \cdots\cdots & \cdots\cdots \\ 0 \dots 0 \quad 0 & \tilde{a}_{m,k_1+1} \cdots \tilde{a}_{mn} \end{pmatrix} = (\tilde{a}_{ij}) .$$

Mit der Matrix, die aus den letzten $m-1$ Zeilen von $(\tilde{a}_{ij})$ besteht, verfahren wir analog. Nach endlich vielen Schritten kommen wir zu einer Stufenmatrix, wie man durch vollständige Induktion nach der Anzahl m der Zeilen sofort erkennt.

Um nun aus einer Matrix der Form (4) eine spezielle Stufenmatrix herzustellen, wenden wir folgende elementare Umformungen an: Wir multiplizieren die r-te Zeile mit $-c_{lk_r}/c_{rk_r}$ und addieren sie zur l-ten für alle $l < r$; hierdurch stehen in der k_r-ten Spalte außer c_{rk_r} nur Nullen. Multiplizieren wir die r-te Zeile mit $c_{rk_r}^{-1}$, so geht c_{rk_r} in $\hat{c}_{rk_r} = 1$ über. Danach verfahren wir analog mit der k_{r-1}-ten Spalte usw. □

Wir wenden uns nun wieder den linearen Gleichungssystemen zu. Da sich bei elementaren Umformungen, d. h. bei dem im Beweis von Satz 2 beschriebenen *Gaußschen Algorithmus*, die Lösungsmenge nicht ändert, können wir die Matrix des Systems in eine spezielle Stufenmatrix überführen und das so entstehende äquivalente System lösen. Es ergibt sich

Satz 3. *Es sei ein lineares Gleichungssystem* (1) *aus m Gleichungen mit n Unbekannten und Koeffizienten aus einem Körper K gegeben. Dann können wir es durch Anwendung elementarer Umformungen nach dem im Beweis von Satz 2 beschriebenen Gaußschen Algorithmus in ein äquivalentes Gleichungssystem verwandeln, dessen Matrix spezielle Stufenform hat.*

Für die Lösung eines derartigen linearen Gleichungssystems mit der erweiterten Matrix

$$\left[\begin{array}{cccccccccccc}
0 & \dots & 1 & a_{1,k_1+1} & \dots & 0 & a_{1,k_2+1} & \dots & 0 & a_{1,k_r+1} & \dots & a_{1n} & b_1 \\
0 & \dots & 0 & 0 & \dots & 1 & a_{2,k_2+1} & \dots & 0 & a_{2,k_r+1} & \dots & a_{2n} & b_2 \\
\multicolumn{13}{c}{\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots} \\
0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 1 & a_{r,k_r+1} & \dots & a_{rn} & b_r \\
0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & b_{r+1} \\
\multicolumn{13}{c}{\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots} \\
0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & b_m
\end{array}\right] \tag{5}$$

gibt es folgende Möglichkeiten:

a) *Es gibt ein* $b_l \neq 0$, $l > r$. *Dann ist das System unlösbar.*

b) *Es gilt* $b_{r+1} = \dots = b_m = 0$. *Dann schreiben wir das System in der Gestalt*

$$\left.\begin{array}{l}
x_{k_1} = b_1 - a_{1,k_1+1}x_{k_1+1} - \dots - a_{1,k_2+1}x_{k_2+1} - \dots - a_{1,k_r+1}x_{k_r+1} - \dots - a_{1n}x_n , \\
x_{k_2} = b_2 \qquad\qquad - a_{2,k_2+1}x_{k_2+1} - \dots - a_{2,k_r+1}x_{k_r+1} - \dots - a_{2n}x_n , \\
\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\
x_{k_r} = b_r \qquad\qquad\qquad\qquad - a_{r,k_r+1}x_{k_r+1} - \dots - a_{rn}x_n .
\end{array}\right\} \tag{6}$$

Setzt man für die links nicht vorkommenden Unbekannten x_j, $j \neq k_1, \dots, k_r$, *beliebige Werte* $c_j \in K$ *ein, so erhält man aus* (6) *die Werte der übrigen Unbekannten* $x_{k_l} = c_{k_l}$, $l = 1, \dots, r$. *Die Menge aller derart entstehenden n-Tupel* $(c_j) \in K^n$ *ist die Lösungsmenge des Systems. Die Lösung ist eindeutig bestimmt dann und nur dann, wenn* $r = n$ *ist.* □

Folgerung 1. *Gilt in* (1) $m < n$, *so ist das System* (1) *unlösbar oder es gibt mehr als eine Lösung. Speziell hat jedes homogene System mit* $m < n$ *wenigstens eine nichttriviale Lösung.* □

Die willkürlich wählbaren Unbekannten x_j, $j \neq k_1, \dots, k_r$, nennt man auch *freie Unbekannte* oder *Parameter*.

Übung 1. Man beweise: Ist K ein unendlicher Körper und hat (1) mehr als eine Lösung, so hat (1) unendlich viele Lösungen. Falls K endlich ist, bestimme man für ein lösbares System (1) die Anzahl der Lösungen in Abhängigkeit von n und r.

3. Faktorgruppen und Faktorringe

In diesem Kapitel wollen wir die Theorie der Gruppen, Ringe und Körper fortsetzen. Die wesentlichen, hier einzuführenden Grundbegriffe sind die der Faktorgruppe und des Faktorringes; sie hängen eng mit den Homomorphismen der Gruppen und Ringe zusammen, vgl. die Homomorphiesätze in § 1 und § 3. Mittels der Faktorringe kann man insbesondere Erweiterungen eines Körpers konstruieren, in welchen ein über diesem Körper gegebenes Polynom zerfällt. Auf diesem Wege werden wir einen Beweis des Fundamentalsatzes der Algebra (Satz 2.8.1) erhalten, den wir ja nachzutragen haben. Wir betrachten weiter die wichtige Klasse der Hauptidealringe, welche die euklidischen Ringe als Teilklasse enthält.

§ 1. Nebenklassen nach einer Untergruppe. Faktorgruppen

Es sei G eine beliebige Gruppe und $H \subseteq G$ eine Untergruppe. Mit Hilfe von H wollen wir nun zwei im allgemeinen verschiedene Äquivalenzrelationen auf G definieren. Für $a, b \in G$ setzen wir

$$a =_H b, \quad \text{falls} \quad b^{-1}a \in H;$$
$$a \ {}_H= b, \quad \text{falls} \quad ab^{-1} \in H.$$

Satz 1. *Die Relationen* $=_H$ *und* ${}_H=$ *sind Äquivalenzrelationen auf* G.

Beweis. Wir ordnen jedem $h \in H$ die Transformation $t_h := r_{h^{-1}}$ der Gruppe G zu. Da $t_{h_1 h_2} = t_{h_1} \circ t_{h_2}$ gilt, erhalten wir eine Wirkung von H über der Menge G, vgl. Beispiel 1.4.4. Die Beschreibung der mit dieser Wirkung verknüpften Äquivalenzrelation nach (1.4.9) stimmt mit der Definition von $=_H$ überein; in der Tat, $a =_H b$ gilt genau dann, wenn ein $h \in H$ mit $b^{-1}a = h$ existiert, d. h., wenn $a = bh = t_h^{-1}(b)$ gilt. Analog ist ${}_H=$ die Äquivalenzrelation, die zu der durch $t_h = l_h$, $h \in H$, definierten Wirkung von H über G gehört. □

Nach Satz 1 zerfällt also G in die Äquivalenzklassen nach der Relation $=_H$ (und analog nach der Relation ${}_H=$). Die Äquivalenzklasse des Elementes $a \in G$ bezüglich

$=_H$ ist gleich dem Orbit von a unter der Wirkung der Rechtstranslationen r_h, $h \in H$, d. h. gleich der Menge $aH := \{ah\}_{h \in H}$, in Übereinstimmung mit der in § 1.2 eingeführten Bezeichnung.

Definition 1. Die Menge aH heißt die *Linksnebenklasse* des Elementes $a \in G$ nach der Untergruppe H. Die Menge aller Linksnebenklassen, d. h. die Faktormenge $G/=_H$, wird mit G/H bezeichnet und die *Faktormenge von G nach H* genannt. Analog werden die *Rechtsnebenklassen* Ha definiert, die die Äquivalenzklassen der Relation $_H=$ sind; die Menge der Rechtsnebenklassen wird mitunter mit $H\backslash G$ bezeichnet. Ist G/H endlich, so nennt man die Anzahl $|G/H|$ den *Index* der Untergruppe H in G und schreibt $(G : H) := |G/H|$.

Beispiel 1. Es sei $G = \mathbf{Z}$, $H = n\mathbf{Z}$, wobei $n \in \mathbf{N}$ eine feste natürliche Zahl ist. Die Relationen $=_H$ und $_H=$ stimmen hier überein, da $\mathbf{Z}$ abelsch ist; sie fallen mit der Relation $\equiv \bmod n$ zusammen (§ 2.2). Daher gilt $G/H = \mathbf{Z}_n$ und $(G : H) = n$.

Beispiel 2. Es sei $G = S_n$, $H = A_n$. Aus Satz 1.2.5 folgt, daß für $s, t \in S_n$ die Relation $s =_H t$ (oder $s\ _H= t$) dann und nur dann erfüllt ist, wenn $\operatorname{sgn} s = \operatorname{sgn} t$ gilt, wenn also s und t entweder beide gerade oder beide ungerade sind. Daher besteht S_n/A_n aus zwei Elementen: der Klasse der geraden Permutationen und der der ungeraden. Es gilt $(S_n : A_n) = 2$.

Beispiel 3. Es sei $G = \mathbf{C}^*$ und K_n die Gruppe der n-ten Einheitswurzeln (vgl. Satz 2.3.7). Die Nebenklasse wK_n eines beliebigen Elementes $w \in \mathbf{C}^*$ ist die Menge der n-ten Wurzeln aus w^n.

Wir betrachten im folgenden hauptsächlich die Linksnebenklassen einer Gruppe G nach einer Untergruppe H. Es bezeichne $p : g \in G \to gH \in G/H$ die kanonische Abbildung. Für jedes $g \in G$ definieren wir eine Abbildung $\bar{l}_g : G/H \to G/H$ so, daß das Diagramm

$$\begin{array}{ccc} G & \xrightarrow{l_g} & G \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle p} \\ G/H & \xrightarrow[\bar{l}_g]{} & G/H \end{array}$$

kommutativ wird, d. h., wir setzen

$$\bar{l}_g(aH) := (ga)\,H\,. \tag{1}$$

Satz 2. *Die Abbildung $g \in G \mapsto \bar{l}_g \in S(G/H)$ definiert eine transitive Wirkung von G auf der Menge G/H. Die stationäre Untergruppe des Elementes $eH = H \in G/H$ ist die Untergruppe H. Das oben angegebene Diagramm ist kommutativ.*

Beweis. Offenbar gilt $\bar{l}_e = \mathrm{id}_{G/H}$ und $\bar{l}_{dg} = \bar{l}_d \circ \bar{l}_g$. Zum Beweis der Transitivität bemerken wir, daß für beliebiges $a \in G$ die Beziehung $aH = \bar{l}_a(H)$ gilt, d. h., jedes $aH \in G/H$ liegt im Orbit von $eH = H$. Weiter gilt $\bar{l}_g(H) = H$ dann und nur dann, wenn $gH = H$, also wenn $g \in H$ ist. Die letzte Behauptung folgt unmittelbar aus der Definition. □

Als Folgerung aus diesen allgemeinen Betrachtungen beweisen wir einen klassischen Satz über endliche Gruppen:

Satz 3 (Satz von LAGRANGE). *Es sei G eine endliche Gruppe und $H \subseteq G$ eine Untergruppe. Dann gilt*

$$|G| = (G:H) \cdot |H| .$$

Beweis. Wir betrachten die Zerlegung von G in die Linksnebenklassen nach H. Da $aH = l_a(H)$ und l_a bijektiv ist, folgt $|aH| = |H|$, d. h., alle Linksnebenklassen haben dieselbe Anzahl von Elementen. Aus der Definition von $(G:H)$ ergibt sich die Behauptung. □

Folgerung 1. *Ist G eine endliche Gruppe und $g \in G$, so gilt $o(g) \mid |G|$.*

Beweis. Nach Satz 1.3.2 gilt $o(g) = |[g]|$, und aus Satz 3 folgt $|[g]| \mid |G|$. □

Folgerung 2. *Jede endliche Gruppe G von Primzahlordnung ist zyklisch.*

Beweis. Die Primzahl p sei die Ordnung von G. Es sei $a \neq e$ ein Element von G. Dann gilt $o(a) > 1$ und $o(a) \mid p$, also $o(a) = p$. Daher ist $|[a]| = |G| = p$, und somit $[a] = G$. □

Übung 1. Man definiere mit Hilfe der Inversion $a \mapsto a^{-1}$ von G eine bijektive Abbildung von G/H auf $H\backslash G$. Ist speziell G/H endlich, so gilt $|H\backslash G| = |G/H| = (G:H)$.

Übung 2. Es sei $p \in \mathbf{N}$ eine Primzahl. Man beweise, daß alle von 0 verschiedenen Elemente des Körpers $\mathbf{Z}_p$ (und nur diese) Nullstellen des Polynoms $x^{p-1} - 1$ über $\mathbf{Z}_p$ sind. Hieraus leite man den *„Kleinen Satz von Fermat"* ab:

$$p \mid a^{p-1} - 1 \quad \text{für alle} \quad a \in \mathbf{Z} \quad \text{mit} \quad (a, p) = 1 .$$

Ferner beweise man den *Satz von Wilson*: $p \mid (p-1)! + 1$. (Hinweis. Man schließe über die Nullstellen von $x^{p-1} - 1 \in \mathbf{Z}_p[x]$.)

Im Fall $G = \mathbf{Z}$, $H = n\mathbf{Z}$ haben wir in § 2.2 die Menge $\mathbf{Z}_n = \mathbf{Z}/n\mathbf{Z}$ in eine Gruppe (sogar einen Ring) verwandelt, indem wir die Operationen aus $\mathbf{Z}$ mit Hilfe der kanonischen Abbildung auf $\mathbf{Z}_n$ übertrugen. Dieses Verfahren haben wir in § 2.6, Definition 2.6.1 und Satz 2.6.1, auf beliebige Monoide verallgemeinert. Wir wollen nun die analoge Frage für eine Gruppe G und eine Äquivalenzrelation $=_H$ untersuchen. Es erweist sich, daß diese Relation im allgemeinen nicht mit der Gruppenoperation verträglich ist; nur für gewisse Untergruppen, die sogenannten Normalteiler, ist das der Fall.

Definition 2. Eine Untergruppe $H \subseteq G$ heißt ein *Normalteiler von G*, wenn für alle $h \in H$ sämtliche zu h konjugierten Elemente wieder zu H gehören, d. h., für alle $h \in H$ und alle $g \in G$ gilt $ghg^{-1} \in H$.

Satz 4. *Für eine Untergruppe $H \subseteq G$ sind die folgenden Eigenschaften äquivalent:*

1. *H ist Normalteiler;*
2. *für alle $g \in G$ gilt $\alpha_g(H) = H$;*
3. *es gilt $gH = Hg$ für alle $g \in G$;*
4. *die Äquivalenzrelationen $\ _H\!=$ und $=_H$ stimmen überein;*
5. *die Äquivalenzrelation $=_H$ ist mit der Gruppenoperation in G verträglich.*

Beweis. Zunächst bemerken wir, daß H genau dann Normalteiler ist, wenn H bei allen inneren Automorphismen α_g, $g \in G$, invariant bleibt:

$$\alpha_g(H) = gHg^{-1} = H;$$

aus der Definition folgt nämlich $gHg^{-1} \subseteq H$ für alle g; wenden wir hierauf den inversen Automorphismus an, so ergibt sich $H \subseteq g^{-1}Hg$ für alle g, also auch für g^{-1}, was $H \subseteq gHg^{-1}$ und somit $gHg^{-1} = H$ ergibt. Die Umkehrung ist trivial. Offenbar ist die Eigenschaft 2 äquivalent zu der Eigenschaft 3; denn es gilt $gHg^{-1} = H$ für alle g genau dann, wenn $gH = Hg$ für alle g erfüllt ist; man braucht nur die Rechtstranslation r_g bzw. r_g^{-1} anzuwenden. Die Äquivalenz der Eigenschaften 3 und 4 folgt unmittelbar, da zwei Äquivalenzrelationen genau dann übereinstimmen, wenn sie dieselbe Einteilung in Äquivalenzklassen definieren.

Wir zeigen nun, daß die Eigenschaft 5 aus der Eigenschaft 3 folgt. Es sei $a_1 =_H b_1$ und $a_2 =_H b_2$. Dann existieren $h_1, h_2 \in H$ derart, daß $a_1 = b_1 h_1$ und $a_2 = b_2 h_2$ gilt. Hieraus ergibt sich $a_1 a_2 = b_1(h_1 b_2)\, h_2$. Nun ist $h_1 b_2 \in Hb_2 = b_2 H$; also gibt es ein $h_3 \in H$ mit $h_1 b_2 = b_2 h_3$. Setzen wir das in unser Produkt ein, so resultiert $a_1 a_2 = b_1 b_2 (h_3 \cdot h_2)$, und es gilt $h_3 \cdot h_2 \in H$, d. h. $a_1 a_2 =_H b_1 b_2$. Umgekehrt folgt die Eigenschaft 1 aus der Eigenschaft 5; denn multiplizieren wir für $g \in G$, $h \in H$ die beiden Äquivalenzen $gh =_H g$, $g^{-1} =_H g^{-1}$, so erhalten wir $ghg^{-1} =_H e$, d. h. $ghg^{-1} \in H$. □

Wegen der Eigenschaft 2 werden die Normalteiler mitunter auch *invariante Untergruppen* genannt.

Nach Satz 2.6.1 und der Eigenschaft 5 der Normalteiler ist in der Faktormenge G/H eine Operation erklärt, die wir genauso wie die Operation in G bezeichnen; bei multiplikativer Schreibweise gilt also für das Produkt in G/H

$$(aH)\,(bH) = abH\,. \tag{2}$$

Aus Satz 2.6.1 folgt ebenfalls, daß *das Monoid* $[G/H, \cdot]$ *eine Gruppe ist*; ihr *Einselement* ist $eH = H$, und das *zu* aH *inverse Element* ist

$$(aH)^{-1} = a^{-1}H\,.$$

Die kanonische Abbildung $p\colon G \to G/H$ *ist ein Homomorphismus.*

Definition 2. Es sei H ein Normalteiler der Gruppe G. Dann heißt die durch (2) erklärte Gruppe $[G/H, \cdot]$ die *Faktorgruppe von* G *nach* H.

Beispiel 4. In einer beliebigen Gruppe G sind die Untergruppen $\{e\}$ und G Normalteiler. Man erkennt leicht, daß die Nebenklassen nach der trivialen Untergruppe $\{e\}$ die einelementigen Teilmengen von G sind. Daher kann man G und $G/\{e\}$ mittels der kanonischen Abbildung identifizieren. Die Faktormenge G/G dagegen enthält nur ein Element.

Beispiel 5. In einer abelschen Gruppe G ist jede Untergruppe ein Normalteiler und bestimmt daher eine ebenfalls abelsche Faktorgruppe G/H. Als Beispiel erwähnen wir die in § 2.2 definierten additiven Gruppen $\mathbf{Z}_n = \mathbf{Z}/n\mathbf{Z}$. Schreibt man die Gruppenoperation in G als Addition, so wird auch in G/H die additive Schreibweise benutzt; anstelle von aH schreibt man entsprechend $a + H$.

Übung 3. Man beweise, daß die Untergruppe $H \subsetneq S_n$, die aus allen den Permutationen s mit $s(n)=n$ besteht, für $n>2$ kein Normalteiler ist.

Übung 4. Man bestimme alle Untergruppen von S_3 und stelle fest, welche von diesen Normalteiler sind.

Übung 5. Man zeige, daß die Kleinsche Vierergruppe V (vgl. Übung 1.3.8) Normalteiler in S_4 ist.

Übung 6. Man beweise: Ist H Untergruppe in G und gilt $(G:H)=2$, so ist H ein Normalteiler.

Übung 7. Man zeige: Ist H Normalteiler in G, so stimmt das Produkt der Nebenklassen im Sinne der Formel (2) mit dem Produkt der Teilmengen aH, bH nach der in § 1.2 vor Satz 1.2.8 gegebenen Definition überein.

Übung 8. Unter dem *Kommutator* $[a,b]$ zweier Elemente a, b einer beliebigen Gruppe G versteht man das Element $[a,b]:=aba^{-1}b^{-1}\in G$; die *Kommutatorgruppe* $K\subsetneq G$ wird als die von allen möglichen Kommutatoren erzeugte Untergruppe definiert. Man beweise, daß K ein Normalteiler in G ist. Ist $N\subsetneq G$ ein beliebiger Normalteiler von G, so ist die Faktorgruppe G/N abelsch dann und nur dann, wenn $K\subsetneq N$ gilt.

Übung 9. Man beweise, daß A_n die Kommutatorgruppe von S_n und V die Kommutatorgruppe von A_4 ist.

Satz 5. *Es sei $f: G\to H$ ein surjektiver Homomorphismus. Ist N Normalteiler in G, so ist $f(N)$ Normalteiler in H. Eine Untergruppe $B\subsetneq H$ ist Normalteiler in H dann und nur dann, wenn $f^{-1}(B)$ Normalteiler in G ist.*

Beweis. Ist $N\subsetneq G$ Untergruppe, so ist auch $f(N)\subsetneq H$ eine Untergruppe, vgl. Satz 1.2.12. Da f surjektiv ist, existiert für jedes Element $h\in H$ ein $g\in G$ mit $h=f(g)$. Für $a\in N$ gilt

$$hf(a)\,h^{-1}=f(g)\,f(a)\,f(g)^{-1}=f(gag^{-1})\in f(N)\,,$$

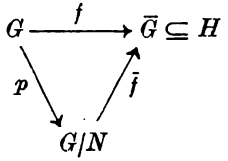
weil $gag^{-1}\in N$ ist. Es sei nun $B\subsetneq H$ ein Normalteiler in H. Wieder nach Satz 1.2.12 ist $f^{-1}(B)\subsetneq G$ eine Untergruppe. Ist $f^{-1}(B)$ ein Normalteiler, so ist auch $B=f(f^{-1}(B))$ ein Normalteiler nach dem eben Bewiesenen. Es sei umgekehrt B ein Normalteiler in H, $g\in G$ und $a\in f^{-1}(B)$. Dann gilt

$$f(gag^{-1})=f(g)\,f(a)\,f(g)^{-1}\in B\,,$$

da $f(a)\in B$ ist. Also ist $gag^{-1}\in f^{-1}(B)$, d. h., $f^{-1}(B)$ ist Normalteiler in G. □

Der Zusammenhang zwischen Homomorphismen und Faktorgruppen wird durch den folgenden einfachen, aber sehr wichtigen Satz hergestellt:

Satz 6 (Homomorphiesatz). *Es sei $f: G\to H$ ein Gruppenhomomorphismus und $N=\operatorname{Ker} f$, $\bar{G}=\operatorname{Im} f$. Dann ist N ein Normalteiler in G, und es gibt einen eindeutig bestimmten Isomorphismus $\bar{f}: G/N\to\bar{G}$, für den das Diagramm*



(3)

kommutativ wird, d. h., $f=\bar{f}\circ p$ gilt.

Beweis. Betrachten wir f als Homomorphismus von G in $\bar{G}$, so ist f surjektiv. Daher können wir Satz 5 auf den Normalteiler $\{e\} \subseteq \bar{G}$ anwenden; es folgt, daß $N = f^{-1}(e)$ Normalteiler in G ist. Wenn nun überhaupt ein Homomorphismus $\bar{f}$ existiert, der (3) kommutativ macht, dann muß

$$\bar{f}(gN) = f(g) \tag{4}$$

gelten; denn $p: G \to G/N$ ist ja die kanonische Abbildung. Damit ist die eindeutige Bestimmtheit von $\bar{f}$ gezeigt. Wir wollen nun (4) als Definition von $\bar{f}$ betrachten. Dann ist zuerst zu zeigen, daß $\bar{f}$ nicht von der Wahl des Repräsentanten $g \in gN$ abhängt. In der Tat, es gilt $gN = g'N$ dann und nur dann, wenn ein $a \in N$ mit $g = g'a$ existiert, und das ist dann und nur dann der Fall, wenn $g'^{-1}g \in N$, d. h. $f(g'^{-1}g) = e$, also $f(g') = f(g)$ gilt. Damit ist auch die Injektivität von $\bar{f}$ bewiesen: Aus $\bar{f}(aN) = \bar{f}(bN)$ folgt $f(a) = f(b)$, d. h. $b^{-1}a \in f^{-1}(e) = N$, also $aN = bN$. Da $\bar{f}(G/N) = f(G) = \bar{G}$ gilt, ist $\bar{f}$ surjektiv. Es bleibt zu zeigen, daß $\bar{f}$ ein Gruppenhomomorphismus ist:

$$\bar{f}((aN) \cdot (bN)) = \bar{f}(abN) = f(ab) = f(a) \cdot f(b) = \bar{f}(aN) \cdot \bar{f}(bN) . \quad \square$$

Folgerung 3. *Die Untergruppe $N \subseteq G$ ist Normalteiler dann und nur dann, wenn sie Kern eines Homomorphismus ist.* $\square$

Folgerung 4 (2. Isomorphiesatz[1]). *Es sei $f: G \to H$ ein surjektiver Gruppenhomomorphismus und K ein Normalteiler in H. Dann existiert ein eindeutig bestimmter Isomorphismus $\bar{f}: G/f^{-1}(K) \to H/K$ derart, daß das Diagramm*

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle p'} \\ G/f^{-1}(K) & \xrightarrow{\bar{f}} & H/K \end{array}$$

kommutativ wird; hier bezeichnen p und p' die kanonischen Abbildungen.

Beweis. Die Kommutativität bedeutet $p' \circ f = \bar{f} \circ p$. Wir setzen $f_1 := p' \circ f$. Dann ist f_1 ein Homomorphismus, und es gilt $\operatorname{Ker} f_1 = f^{-1}(K)$; in der Tat gilt $\operatorname{Ker} f_1 = f^{-1}(\operatorname{Ker} p') = f^{-1}(K)$. Da f und p' surjektiv sind, muß auch f_1 surjektiv sein. Nach Satz 6 gibt es genau einen Isomorphismus $\bar{f}$ mit $p' \circ f = f_1 = \bar{f} \circ p$. $\square$

Es sei bemerkt, daß man Satz 6 und Folgerung 4 häufig benutzt, um sich Modelle für Faktorgruppen zu beschaffen. Ist nämlich $N \subseteq G$ ein Normalteiler und $f: G \to H$ ein Homomorphismus mit $\operatorname{Ker} f = N$, so gilt $G/N \cong \operatorname{Im} f$.

Beispiel 6. Mit Hilfe des Homomorphismus sgn: $S_n \to \{-1, 1\}$ erhält man aus Satz 6 leicht, daß A_n Normalteiler in S_n ist und die Isomorphie $S_n/A_n \cong \{-1, 1\}$ besteht (vgl. Beispiel 2).

Übung 10. Man zeige, daß folgende Isomorphien bestehen (Bezeichnungen nach § 2.3):

$$\mathbf{C}^*/S^1 \cong \mathbf{R}_+; \qquad \mathbf{C}^*/\mathbf{R}_+ \cong S^1; \qquad \mathbf{C}^*/\mathbf{R}^* \cong S^1;$$
$$\mathbf{C}^*/K_n \cong \mathbf{C}^*; \qquad S^1/K_n \cong S^1; \qquad K_{n \cdot m}/K_n \cong K_m .$$

[1]) Der unter dem Namen „1. Isomorphiesatz" bekannte Satz wird auf S. 121 f. formuliert und bewiesen.

Zum Abschluß des Paragraphen wollen wir ein Analogon von Satz 6 beweisen, das eine allgemeine Beschreibung der transitiven Transformationsgruppen ergibt. Es sei G eine Gruppe. Nach Satz 2 gehört zu jeder Untergruppe $H \subseteq G$ eine transitive Wirkung von G auf der Faktormenge G/H. Wir wollen jetzt zeigen, daß sich jede transitive Wirkung auf diese Weise darstellen läßt.

Satz 7. *Es seien $[G, X]$ eine transitive Transformationsgruppe, $x_0 \in X$ ein beliebiger, fest gewählter Punkt, $H = G_{x_0}$ seine stationäre Untergruppe und $p_{x_0}: g \in G \mapsto gx_0 \in X$ die bereits durch* (1.4.10) *definierte Abbildung. Dann existiert eine bijektive Abbildung $\bar{p}_{x_0}: G/H \to X$, so daß das Diagramm*

$$\begin{array}{ccc} G & \xrightarrow{p_{x_0}} & X \\ & {\scriptstyle p}\searrow \quad \nearrow{\scriptstyle \bar{p}_{x_0}} & \\ & G/H & \end{array} \tag{5}$$

kommutativ wird (p — kanonische Abbildung). Bezeichnet l_g die Transformation in G/H und t_g die Transformation in X, so ist für jedes $g \in G$ das Diagramm

$$\begin{array}{ccc} G/H & \xrightarrow{l_g} & G/H \\ {\scriptstyle \bar{p}_{x_0}}\downarrow & & \downarrow{\scriptstyle \bar{p}_{x_0}} \\ X & \xrightarrow{t_g} & X \end{array} \tag{6}$$

kommutativ.

Beweis. Wir betrachten die Abbildung $p_{x_0}: G \to X$ und zeigen, daß die Urbilder $p_{x_0}^{-1}(x)$ der Punkte $x \in X$ gerade die Linksnebenklassen von G nach H sind. Da G auf X transitiv wirkt, ist p_{x_0} surjektiv (Satz 1.4.5). Es genügt also zu zeigen, daß $p_{x_0}(a) = p_{x_0}(b)$ dann und nur dann gilt, wenn $a =_H b$ ist. Nun ist $p_{x_0}(a) = p_{x_0}(b)$ genau dann, wenn $ax_0 = bx_0$, d. h. $b^{-1}ax_0 = x_0$, also $b^{-1}a \in G_{x_0} = H$ gilt. Danach ist klar, daß p_{x_0} die bijektive Abbildung $\bar{p}_{x_0}$ durch $\bar{p}_{x_0}(aH) := ax_0$ eindeutig bestimmt, wobei das Diagramm (5) offenbar kommutativ wird. Die Kommutativität von (6) ergibt sich aus (1) und (1.4.11) durch eine einfache Rechnung: Für alle $a \in G$, $g \in G$ gilt

$$\bar{p}_{x_0} \circ l_g(aH) = \bar{p}_{x_0}(gaH) = (ga)\, x_0 = g(ax_0) = t_g \circ \bar{p}_{x_0}(aH)\,. \quad \square$$

Satz 7 zeigt: Man kann G/H und X durch $\bar{p}_{x_0}$ identifizieren, wobei diese Identifikation nur von der Wahl des Punktes x_0 abhängt; wegen der Kommutativität des Diagramms (6) geht dabei die Wirkung von G auf G/H in die Wirkung von G auf X über. In diesem Sinne ist $\bar{p}_{x_0}$ als Isomorphismus der G-Transformationsgruppen $[G, G/H]$ und $[G, X]$ anzusehen, vgl. die Beispiele 1.5.3., 1.5.4 und Übung 1.5.1.

Übung 11. Es sei $[G, X]$ eine transitive Transformationsgruppe und $H = G_{x_0}$ die stationäre Untergruppe des Punktes x_0. Man beweise: Die Nebenklasse aH besteht aus allen den $g \in G$, für die $g \cdot x_0 = a \cdot x_0$ gilt, und die Nebenklasse Ha ist die Menge aller derjenigen $g \in G$, für die $g(a^{-1}x_0) = x_0$, d. h. $g^{-1}x_0 = a^{-1}x_0$ gilt.

Übung 12. Man beweise, daß der Nichteffektivitätskern (Definition 1.4.2) einer Transformationsgruppe $[G, X]$ ein Normalteiler in G ist. Speziell ist das Zentrum Z_G einer Gruppe G (Beispiel 1.4.7) ein Normalteiler in G. Man beweise $G/Z_G \cong \mathrm{Int}\, G$ (vgl. Satz 1.4.1).

Übung 13. Unter den Voraussetzungen der Übung 11 beweise man, daß der Nichteffektivitätskern der größte Normalteiler der Gruppe G ist, der in G_{x_0} enthalten ist.

Übung 14. Es seien G eine Gruppe und $H_1, H_2 \subseteqq G$ Untergruppen. Man beweise die Äquivalenz der folgenden Bedingungen: 1. Die Untergruppe $H_1 \subseteqq G$ wirkt transitiv auf G/H_2. — 2. $G = H_1 \cdot H_2$. — 3. $G = H_2 H_1$. — 4. Die Untergruppe $H_2 \subseteqq G$ wirkt transitiv auf G/H_1.

Übung 15. Es sei $Y \subseteqq \{1, \ldots, n\}$ eine nichtleere Teilmenge und S_n^Y die Menge aller derjenigen $s \in S_n$, für die $s(b) = b$ für alle $b \notin Y$ gilt. Man zeige, daß S_n^Y eine Untergruppe von S_n ist und daß $S_n^Y \cong S(Y) \cong S_{|Y|}$ gilt. Für eine beliebige natürliche Zahl k mit $0 < k < n$ bezeichne $\mathfrak{A}_{n,k}$ die Menge aller geordneten Kombinationen zu je k aus der Menge $\{1, \ldots, n\}$. Man betrachte die in naheliegender Weise zu definierende Transformationsgruppe $[S_n, \mathfrak{A}_{n,k}]$, zeige, daß sie transitiv ist und folgere hieraus $|\mathfrak{A}_{n,k}| = n!/(n-k)!$.

Übung 16. Es sei G eine endliche Gruppe. Für $a \in G$ bezeichne K_a die Klasse der zu a konjugierten Elemente. Man beweise $|K_a| \mid |G|$. Hieraus leite man ab: Wenn $|G| = p^k$ gilt mit p Primzahl und $k > 0$, so ist das Zentrum $Z_G \neq \{e\}$.

Übung 17. Es sei G eine endliche Gruppe und $G = \bigcup_{i=1}^{r} K_i$ die Zerlegung von G in die verschiedenen Klassen konjugierter Elemente. Aus jeder Klasse K_i wählen wir einen Vertreter a_i und bezeichnen mit $m_i := |Z_{a_i}|$ die Ordnung des Zentralisators von a_i, $i = 1, \ldots, r$. Man beweise, daß $\sum_{i=1}^{r} 1/m_i = 1$ gilt.

Übung 18. Es seien $[G, X]$ eine Transformationsgruppe, G und X endlich, und $X_g := \{x \in X \mid gx = x\}$. Man beweise die *Formel von Cauchy-Burnside* für die Anzahl der Orbits:

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X_g| \,. \tag{7}$$

(Hinweis. Sind $Y, Z \subset X$ invariante Teilmengen mit $X = Y \cup Z$, $Y \cap Z = \emptyset$, und gilt (7) für die Transformationsgruppen $[G, Y]$, $[G, Z]$, so gilt (7) auch für $[G, X]$. Hierdurch kann man die Aufgabe auf den transitiven Fall zurückführen, auf den Satz 7 anwendbar ist.)

§ 2. Produkte von Untergruppen. Direkte Produkte

Es seien G eine Gruppe und $H, N \subseteqq G$ Untergruppen. Dann ist das Produkt $H \cdot N \subseteqq \subseteqq G$ eine Teilmenge, aber im allgemeinen keine Untergruppe von G. Andererseits kann man die von den Untergruppen H und N erzeugte Untergruppe $[H \cup N]$ bilden, vgl. § 1.2. Satz 1.2.8 besagt, daß für abelsche Gruppen $H \cdot N$ und $[H \cup N]$ übereinstimmen. Wir wollen nun eine allgemeine Situation beschreiben, in der diese Gleichheit ebenfalls gilt.

Satz 1 (1. Isomorphiesatz). *Es seien H eine Untergruppe und N ein Normalteiler der Gruppe G. Dann gilt $[H \cup N] = H \cdot N$. Die Untergruppe $H \cap N$ ist Normalteiler in H, und es besteht die Isomorphie*

$$H/H \cap N \cong HN/N \,. \tag{1}$$

Beweis. Nach Satz 1.4 gilt $gN=Ng$ für alle $g\in G$. Hieraus folgt $HN=NH$ für eine beliebige Teilmenge $H\subseteq G$. Offenbar ist $H\subseteq HN$, $N\subseteq HN$. Nach Satz 1.2.6 genügt es, für den Beweis von $[H\cup N]=HN$ zu zeigen, daß HN eine Untergruppe ist; denn offenbar gilt $HN\subseteq[H\cup N]$. Es seien $h_1, h_2\in H$ und $a_1, a_2\in N$. Nach Satz 1.4 gibt es ein $a_3\in N$ mit $a_1h_2=h_2a_3$. Daher gilt $(h_1a_1)(h_2a_2)=h_1h_2a_3a_1\in HN$. Weiter ist $(h_1a_1)^{-1}=a_1^{-1}h_1^{-1}\in NH=HN$. Damit ist die erste Behauptung bewiesen. Zum Beweis der zweiten Behauptung betrachten wir den kanonischen Homomorphismus $p: G\to G/N$. Seine Einschränkung $\tilde{p}:=p\mid H$ ist ein im allgemeinen nicht surjektiver Homomorphismus von H in G/N. Offenbar gilt $\operatorname{Ker}\tilde{p}=H\cap\operatorname{Ker}p=H\cap N$. Nach Satz 1.6 ist $H\cap N$ Normalteiler in H, und es gilt $\operatorname{Im}\tilde{p}=\{hN\}_{h\in H}\cong H/H\cap N$. Weiter sei $q:=p\mid HN$. Dann ist $q: HN\to G/N$ ein Homomorphismus mit $\operatorname{Im}q=\operatorname{Im}\tilde{p}$ und $\operatorname{Ker}q=\operatorname{Ker}p=N\subseteq HN$. Somit folgt analog $\operatorname{Im}\tilde{p}\cong HN/N$, d. h. (1). □

Wir betrachten nun eine beliebige, nicht notwendig endliche Familie $(H_i)_{i\in I}$ von Untergruppen einer Gruppe G. Unter der Voraussetzung, daß alle H_i Normalteiler sind, bezeichnen wir mit $\prod_{i\in I} H_i$ die Menge aller derjenigen Elemente $g\in G$, die als endliche Produkte der Form $g=g_{i_1}\dots g_{i_k}$ mit $k\in\mathbf{N}$, $g_{i_\alpha}\in H_{i_\alpha}$, $i_\alpha\neq i_\beta$ für $\alpha\neq\beta$, $1\leqq\alpha, \beta\leqq k$, darstellbar sind. Der folgende Satz verallgemeinert Satz 1.2.8:

Satz 2. *Die Menge $\prod_{i\in I} H_i$ ist ein Normalteiler der Gruppe G. Sie stimmt mit der Untergruppe überein, die von der Familie $(H_i)_{i\in I}$ erzeugt wird. Ist $I=\{1,\dots,m\}$ endlich, so gilt*

$$\prod_{i\in I} H_i=\prod_{i=1}^{m} H_i=H_1\dots H_m.$$

Beweis. Wir betrachten zuerst den Fall $I=\{1,\dots,m\}$ endlich. Da $H_1\dots H_m=(H_1\dots H_{m-1})\cdot H_m$ gilt, erhält man aus Satz 1 leicht durch vollständige Induktion, daß $H_1\dots H_m$ eine Untergruppe von G ist. Wir bemerken, daß für eine beliebige Permutation $s\in S_m$ die Identität $H_{s(1)}\dots H_{s(m)}=H_1\dots H_m$ gilt. In der Tat können wir jede Permutation als Produkt von Transpositionen benachbarter Zahlen darstellen (Übung 1.2.7), und nach Satz 1 hängt das Produkt zweier benachbarter Normalteiler nicht von ihrer Reihenfolge ab.

Wir kommen nun zum allgemeinen Fall. Es seien $a, b\in\prod_{i\in I} H_i$, $a=a_{i_1}\dots a_{i_k}$, $b=b_{j_1}\dots b_{j_l}$, wobei $a_{i_\alpha}\in H_{i_\alpha}$, $b_{j_\beta}\in H_{j_\beta}$ gilt und alle i_α (und j_β) voneinander verschieden sind. Durch Hinzufügen von Faktoren, die gleich e sind, können wir stets erreichen, daß $k=l$ gilt und $\{i_1,\dots,i_k\}=\{j_1,\dots,j_k\}$ ist. Dann ist $a\in H_{i_1}\dots H_{i_k}$, $b\in H_{j_1}\dots H_{j_k}$ und nach dem eben Bewiesenen $H_{i_1}\dots H_{i_k}=H_{j_1}\dots H_{j_k}$ eine Untergruppe von G. Daher gilt $ab\in H_{i_1}\dots H_{i_k}\subseteq\prod_{i\in I} H_i$. Aus demselben Grunde ist auch $a^{-1}\in H_{i_1}\dots H_{i_k}\subseteq\prod_{i\in I} H_i$ (vgl. Satz 1.1.3). Somit genügt $\prod_{i\in I} H_i$ den Bedingungen von Satz 1.2.1 und ist eine Untergruppe. Weil diese Untergruppe alle H_i, $i\in I$, enthält und in der von der Familie $(H_i)_{i\in I}$ erzeugten Untergruppe enthalten ist, muß sie gleich dieser Untergruppe sein (vgl. Satz 1.2.6). Um zu zeigen, daß die Untergruppe

$\prod_{i\in I} H_i$ ein Normalteiler ist, betrachten wir den zu einem beliebigen Element $g\in G$ gehörenden inneren Automorphismus α_g. Da alle H_i Normalteiler sind, gilt für $a=a_{i_1}\dots a_{i_k}\in\prod_{i\in I} H_i$, $a_{i_\alpha}\in H_{i_\alpha}$, daß

$$\alpha_g(a)=\alpha_g(a_{i_1})\dots\alpha_g(a_{i_k})\in H_{i_1}\dots H_{i_k}\subseteq\prod_{i\in I} H_i$$

ist; denn es gilt $\alpha_g(a_i)\in\alpha_g(H_i)=H_i$ für alle $i\in I$. □

Wir wollen nun den Begriff des direkten Produktes von Normalteilern einführen. Dabei können wir annehmen, daß das Produkt die ganze Gruppe G ist; sonst ließe sich anstelle von G die von der Familie $(H_i)_{i\in I}$ erzeugte Untergruppe betrachten.

Definition 1. Es sei G eine Gruppe und $(G_i)_{i\in I}$ eine Familie von Untergruppen $G_i\subseteq G$. Man sagt, daß G *Produkt* der Untergruppen G_i sei, wenn alle G_i Normalteiler in G sind und $G=\prod_{i\in I} G_i$ ist. Die Gruppe G heißt *direktes Produkt* der Familie $(G_i)_{i\in I}$ von Untergruppen $G_i\subseteq G$, wenn folgende Bedingungen erfüllt sind:

1. Es ist $ab=ba$ für alle $a\in G_i$, $b\in G_j$, $i\neq j$, $i, j\in I$;

2. jedes $g\in G$ läßt sich bis auf die Reihenfolge der Faktoren eindeutig als formal unendliches Produkt $g=\prod_{i\in I} g_i$ darstellen, wobei $g_i\in G_i$ gilt und $g_i=e$ für fast alle $i\in I$ ist.

Der folgende Satz zeigt, daß die Zerlegung in ein direktes Produkt von Untergruppen auch ein Produkt von Normalteilern ist. Er enthält ein Kriterium dafür, daß eine Gruppe in ein direktes Produkt einer gegebenen Familie von Untergruppen zerfällt.

Satz 3. *Es sei $(G_i)_{i\in I}$ eine Familie von Untergruppen der Gruppe G. Dafür daß G direktes Produkt der Familie $(G_i)_{i\in I}$ ist, sind die folgenden Bedingungen* 1, 2 *und eine der Bedingungen* 3a), 3b) *notwendig und hinreichend:*

1. *Jedes G_i, $i\in I$, ist Normalteiler in G;*

2. *G wird durch die Familie der Untergruppen $(G_i)_{i\in I}$ erzeugt;*

3a). *Ist $e=g_{i_1}\dots g_{i_k}$ mit $g_{i_\alpha}\in G_{i_\alpha}$, $i_\alpha\neq i_\beta$ für $\alpha\neq\beta$, $\alpha, \beta=1, \dots, k$, so gilt $g_{i_\alpha}=e$ für $\alpha=1, \dots, k$.*

3b). *Für alle $j\in I$ gilt $G_j\cap\prod_{i\neq j} G_i=\{e\}$.*

Beweis. Es sei G direktes Produkt der Untergruppen G_i. Dann ist die Eigenschaft 2 offensichtlich. Zum Beweis der Eigenschaft 1 genügt es, $\alpha_g(G_i)\subseteq G_i$ für alle $g\in G$ und $i\in I$ zu zeigen. Wegen einer Eigenschaft der inneren Automorphismen α_g (vgl. Beispiel 1.4.5) und der schon bewiesenen Eigenschaft 2 genügt es, die Inklusion $\alpha_g(G_i)\subseteq G_i$ für alle $g\in G_j$, $j\in I$, zu beweisen. Für diesen Fall folgt sie aber sofort aus der Bedingung 1 von Definition 1. Die Eigenschaft 3a) schließlich ist ein Spezialfall der Eindeutigkeitsaussage von Definition 1.

Wir beweisen, daß aus den Eigenschaften 1 und 3a) die Eigenschaft 3b) folgt. Es sei $g\in G_j\cap\prod_{i\neq j} G_i$. Dann gilt $g=g_{i_1}\dots g_{i_k}$, wobei die $i_\alpha\neq j$ und voneinander ver-

schieden sind und $g_{i_\alpha} \in G_{i_\alpha}$, $\alpha = 1, \ldots, k$, gilt. Hieraus folgt $e = g_{i_1} \ldots g_{i_k} g^{-1}$ mit $g^{-1} \in G_j$. Dann muß aber nach 3a) $g = e$ gelten.

Es seien nun die Bedingungen 1, 2 und 3b) erfüllt. Aus Satz 2 folgt dann $G = \prod_{i \in I} G_i$. Wir beweisen die Bedingung 1 von Definition 1. Zunächst erhalten wir aus der Bedingung 3b) die Beziehung $G_i \cap G_j = \{e\}$ für $i \neq j$. Für $a \in G_i$, $b \in G_j$, $i \neq j$, betrachten wir den Kommutator $c = aba^{-1}b^{-1}$. Weil G_j ein Normalteiler ist, erhalten wir $c = (aba^{-1})\, b^{-1} \in G_j$; analog ist $c = a(ba^{-1}b^{-1}) \in G_i$, also $c \in G_i \cap G_j$ und somit $c = e$. Das bedeutet aber $ab = ba$.

Aus dem Bewiesenen folgt, daß jedes $g \in G$ in Form eines formal unendlichen Produktes $g = \prod_{i \in I} g_i$, $g_i \in G_i$, darstellbar ist, das nicht von der Reihenfolge der Faktoren abhängt. Es bleibt die Eindeutigkeit dieser Darstellung zu zeigen. Hierzu sei $g = \prod_{i \in I} g_i'$, $g_i' \in G_i$, ebenfalls eine formal unendliche Darstellung von g. Da die Elemente verschiedener Untergruppen G_i miteinander kommutieren, erhalten wir die Gleichung $g_j' g_j^{-1} = \prod_{i \neq j} (g_i'^{-1} g_i)$. Nach der Bedingung 3b) muß somit $g_j' g_j^{-1} = e$, d. h. $g_j = g_j'$ für alle $j \in I$ gelten. □

Bemerkung. Ist $I = \{1, \ldots, m\}$ endlich, so läßt sich die Bedingung 3b) zu der folgenden Bedingung abschwächen:

3c). *Es gilt* $G_j \cap \prod_{i=1}^{j-1} G_i = \{e\}$ *für alle* $j = 2, \ldots, m$.

In der Tat, aus der Bedingung 3c) folgt ebenfalls, daß $G_i \cap G_j = \{e\}$ für $i \neq j$ ist, und daraus erhält man wie oben die Bedingung 1 von Definition 1. Es bleibt die Eindeutigkeit der Produktdarstellung zu zeigen. Angenommen, es sei $g = \prod_{i=1}^{m} g_i = \prod_{i=1}^{m} g_i'$ und es gäbe ein j, $1 \leqq j \leqq m$, mit $g_j \neq g_j'$ und $g_i = g_i'$ für $i = j+1, \ldots, m$. Dann folgt $g_1 \ldots g_j = g_1' \ldots g_j'$ und $g_j \neq g_j'$. Folglich muß $j > 1$ sein. In diesem Fall erhalten wir aber durch $e = g_j' g_j^{-1} = \prod_{i=1}^{j-1} (g_i'^{-1} g_i)$ einen Widerspruch zu der Bedingung 3c).

Folgerung 1. *Ist* $G = G_1 \cdot G_2$ *ein direktes Produkt, so gilt* $G/G_1 \cong G_2$.

Beweis. Da G_1 Normalteiler ist, können wir Satz 1 anwenden. Aus $G_1 \cap G_2 = \{e\}$ folgt $G/G_1 \cong G_2/\{e\} = G_2$. □

Beispiel 1. Die Gruppe $\mathbf{R}^*$ ist das direkte Produkt

$$\mathbf{R}^* = \mathbf{R}_+ \cdot \{-1, 1\}.$$

Beispiel 2. Die Eindeutigkeit der Darstellung $z = \varrho e^{i\varphi}$ für $z \in \mathbf{C}^*$ (§ 2.3) ergibt sofort das direkte Produkt

$$\mathbf{C}^* = \mathbf{R}_+ \cdot S^1.$$

Beispiel 3. Für abelsche, additiv geschriebene Gruppen spricht man auch von der *Summe* (bzw. der *direkten Summe*) der Untergruppen G_i und schreibt (vgl. § 1.2)

$$G = G_1 + \ldots + G_r = \sum_{i=1}^{r} G_i \quad \text{bzw.} \quad G = \sum_{i \in I} G_i.$$

Um auszudrücken, daß eine Summe direkt ist, benutzt man das Symbol $\oplus$:

$$G = G_1 \oplus \ldots \oplus G_r = \bigoplus_{i=1}^{r} G_i \quad \text{bzw.} \quad G = \bigoplus_{i \in I} G_i .$$

Zum Beispiel ist die Gruppe V der Vektoren der Ebene (Beispiel 1.1.6) gleich der direkten Summe $V = L_1 \oplus L_2$, wobei L_i die Untergruppe derjenigen Vektoren ist, die zu einer Geraden H_i durch o gehören, $H_1 \neq H_2$, o der Koordinatenursprung.

Übung 1. Es seien G eine Gruppe und $G_i \subseteq G$, $i = 1, \ldots, r$, Untergruppen, die alle mit eventueller Ausnahme einer einzigen Normalteiler in G sind. Man beweise, daß dann $\left[\bigcup_{i=1}^{r} G_i\right] = G_1 \ldots G_r$ gilt.

Übung 2. Man zeige, daß die Normalteiler einer beliebigen Gruppe G bezüglich der Ordnung $\subseteq$ einen vollständigen Verband (Teilverband des Verbandes aller Untergruppen) bilden; vgl. Satz 1.2.7 und die darauf folgende Bemerkung.

Übung 3. Es seien $G = H \cdot N$, H eine Untergruppe, N ein Normalteiler in G. Sind die Elemente $g \in G$ eindeutig in der Form $g = ha$, $h \in H$, $a \in N$, darstellbar (was zur Bedingung $H \cap N = \{e\}$ gleichwertig ist), so heißt G ein *halbdirektes Produkt* von H und N. Aus Satz 1 folgt in diesem Fall $H \cong G/N$. Man zeige, daß $S_4 = H \cdot V$, H die stationäre Untergruppe des Elementes 4, V die Kleinsche Vierergruppe, ein halbdirektes Produkt ist. Hieraus leite man $S_4/V \cong S_3$ her.

Der Begriff eines direkten Produktes gestattet noch einen anderen Zugang, den wir jetzt darlegen wollen.

Definition 2. Es seien $[M_i, \cdot]$, $i = 1, \ldots, r$, beliebige Monoide. Unter dem *direkten Produkt der Monoide* $M_1, \ldots, M_r$ versteht man die Menge $M := \bigtimes_{i=1}^{r} M_i = M_1 \times \ldots \times M_r$, versehen mit der folgenden Operation:

$$(x_1, \ldots, x_r) \cdot (y_1, \ldots, y_r) := (x_1 \cdot y_1, \ldots, x_r \cdot y_r) .$$

Zum Monoid $[M, \cdot]$ gehören die *i-ten Projektionen*

$$\pi_i : (x_1, \ldots, x_r) \in M \mapsto \pi_i(x_1, \ldots, x_r) := x_i , \qquad i = 1, \ldots, r .$$

Besitzt jedes Monoid M_i ein Einselement e, so können wir noch die i-ten *Injektionen* ι_i definieren:

$$\iota_i : x_i \in M_i \mapsto \iota_i(x_i) := (e, \ldots, e, x_i, e, \ldots, e) \in M, \qquad i = 1, \ldots, r;$$

hier steht x_i an der i-ten Stelle des r-Tupels.

Satz 4. *Sind die* $[M_i, \cdot]$ *Monoide, so sind die Projektionen* $\pi_i : M \to M_i$ *(nach Definition 2) Homomorphismen. Sind alle* M_i *kommutativ oder assoziativ, so besitzt auch* M *die entsprechende Eigenschaft. Besitzen alle* M_i *Einselemente* e, *so ist* $(e, \ldots, e)$ *das Einselement von* M, *und es gilt* $M^* = \bigtimes_{i=1}^{r} M_i^*$ *sowie*

$$(x_1, \ldots, x_r)^{-1} = (x_1^{-1}, \ldots, x_r^{-1}) .$$

Unter diesen Voraussetzungen sind die Abbildungen ι_i *injektive Homomorphismen. Sind schließlich alle* M_i *Gruppen, so ist auch* M *eine Gruppe.*

Den sehr einfachen Beweis überlassen wir dem Leser. □

Beispiel 4. Die additive Gruppe $[\mathbf{C}, +]$ der komplexen Zahlen ist direktes Produkt zweier reeller additiver Gruppen $[\mathbf{R}, +]$.

Wir wollen nun zeigen, daß für Gruppen G_i die Begriffe der direkten Produkte nach Definition 1 und Definition 2 im wesentlichen übereinstimmen.

Satz 5. *Es seien* G_i, $i=1, \ldots, r$, *Gruppen. Dann ist* $G := \bigtimes_{i=1}^{r} G_i$ *das direkte Produkt (im Sinne von Definition* 1*) der Untergruppen* $\bar{G}_i := \iota_i(G_i) \subseteq G$, $i=1, \ldots, r$. *Ist umgekehrt* G *direktes Produkt seiner Untergruppen* H_i, $i=1, \ldots, r$, *im Sinne der Definition* 1, *so gibt es einen und nur einen Isomorphismus* $\varphi: G \to H = \bigtimes_{i=1}^{r} H_i$ *mit* $\varphi \mid H_i = \iota_i$.

Beweis. Offenbar gilt $(g_1, \ldots, g_r) = (g_1, e, \ldots, e) \cdot (e, g_2, e, \ldots, e) \ldots (e, e, \ldots, e, g_r) = \iota_1(g_1) \ldots \iota_r(g_r)$. Folglich ist $G = \bar{G}_1 \ldots \bar{G}_r$. Es ist klar, daß alle Elemente $a \in \bar{G}_i$, $b \in \bar{G}_j$, $i \neq j$, kommutieren, d. h. $ab = ba$ erfüllen. Sind nun $h_i \in \bar{G}_i$ so beschaffen, daß $(g_1, \ldots, g_r) = h_1 \ldots h_r$ ist, so haben die h_i die Gestalt $h_i = (e, \ldots, e, a_i, e, \ldots, e)$ mit $a_i \in G_i$, und es folgt $(g_1, \ldots, g_r) = (a_1, \ldots, a_r)$, also $a_i = g_i$. Die Darstellung ist also eindeutig, und die $\bar{G}_1, \ldots, \bar{G}_r$ erfüllen alle Bedingungen der Definition 1.

Es sei nun umgekehrt $G = H_1 \ldots H_r$ ein direktes Produkt. Soll φ ein Isomorphismus mit $\varphi \mid H_i = \iota_i$ sein, so muß notwendig $\varphi(g) := (g_1, \ldots, g_r)$ für $g = g_1 \ldots g_r$, $g_i \in H_i$, gesetzt werden, wie unmittelbar aus der Definition eines Homomorphismus folgt. Aus der Eindeutigkeit der Darstellungen ergibt sich sofort die Bijektivität von φ; die Homomorphie-Eigenschaft folgt aus

$$\begin{aligned}\varphi(gh) &= \varphi(g_1 \ldots g_r \cdot h_1 \ldots h_r) = \varphi(g_1 h_1 \ldots g_r h_r) \\ &= (g_1 h_1, \ldots, g_r h_r) = (g_1, \ldots, g_r) \cdot (h_1, \ldots, h_r) = \varphi(g) \cdot \varphi(h) \,. \quad \square\end{aligned}$$

Übung 4. Es seien G_i, $i=1, \ldots, r$, Gruppen und $H_i \subseteq G_i$ Normalteiler in G_i. Man beweise, daß $H = \bigtimes_{i=1}^{r} H_i$ ein Normalteiler in $G = \bigtimes_{i=1}^{r} G_i$ ist und $G/H \cong \bigtimes_{i=1}^{r} G_i/H_i$ gilt.

Übung 5. Es seien H_1, H_2 endliche Untergruppen einer beliebigen Gruppe G. Man beweise: $|H_1 H_2| = |H_1| \cdot |H_2| / |H_1 \cap H_2|$. (Hinweis. Man betrachte die Wirkung der Gruppe $H_1 \times H_2$ auf G mit Hilfe der Transformationen $t_{(h_1, h_2)} = l_{h_1} \circ r_{h_2}^{-1}$, $h_i \in H_i$, $i=1, 2$.)

Übung 6. Es seien G eine endliche Gruppe und $H_i \subseteq G$, $i=1, \ldots, r$, Normalteiler in G; dabei gelte $G = \prod_{i=1}^{r} H_i$. Man beweise: Dieses Produkt ist direkt dann und nur dann, wenn $|G| = \prod_{i=1}^{r} |H_i|$ gilt.

Übung 7. Es seien G_1, G_2 Gruppen, $g_i \in G_i$, $i=1, 2$, $g = (g_1, g_2) \in G_1 \times G_2$. Man zeige: $o(g)$ ist endlich dann und nur dann, wenn $o(g_1)$ und $o(g_2)$ endlich sind; in diesem Fall ist $o(g)$ das kleinste gemeinsame Vielfache von $o(g_1)$ und $o(g_2)$.

Übung 8. Es seien G_1, G_2 nichttriviale Gruppen. Man beweise, daß die Gruppe $G_1 \times G_2$ genau dann zyklisch ist, wenn G_1 und G_2 endliche zyklische Gruppen mit zueinander teilerfremden Ordnungen sind. Hieraus leite man ab: Ist $n = p_1^{k_1} \ldots p_r^{k_r}$ die Zerlegung von $n \in \mathbf{N}$ in seine Primfaktoren, $p_i \neq p_j$ für $i \neq j$, so gilt die Isomorphie der additiven Gruppen der Restklassenringe

$$\mathbf{Z}_n \cong \mathbf{Z}_{p_1^{k_1}} \times \ldots \times \mathbf{Z}_{p_r^{k_r}} \,.$$

(Bemerkung. Da zyklische Gruppen derselben Ordnung isomorph sind (Satz 1.3.3), gilt diese Isomorphie auch für beliebige zyklische Gruppen der entsprechenden Ordnungen, vgl. Übung 2.2.3.)

Übung 9. Es sei G eine gewisse Gruppe, $H \subseteq Z_G$ eine im Zentrum von G liegende zyklische Untergruppe der Ordnung n und G/H eine zyklische Gruppe der Ordnung m. Man beweise: Sind m und n teilerfremd, so ist G zyklisch. Hieraus leite man ab, daß eine beliebige abelsche Gruppe der Ordnung $p_1 \dots p_r$, wobei die p_i verschiedene Primzahlen sind, zyklisch ist.

Übung 10. Es sei p eine Primzahl. Man beweise: Ist G eine beliebige Gruppe der Ordnung p^2, so ist G abelsch und dabei entweder zyklisch oder direktes Produkt zweier zyklischer Untergruppen der Ordnung p. (Hinweis. Mit Hilfe von Übung 1.16 zeige man, daß ein $a \in Z_G$ existiert mit $o(a) = p$; auf $G/[a]$ wende man dann Folgerung 1.2 an. Wir bemerken, daß Übung 2.3.12 ein Beispiel einer nichtabelschen Gruppe der Ordnung 8 enthält.)

Übung 11. Wir betrachten eine Zerlegung $\{1, \dots, n\} = \bigcup_{i=1}^{r} Y_i$ in nichtleere, paarweise disjunkte Teilmengen Y_i. Mit $S_n^{Y_1,\dots,Y_r}$ bezeichnen wir die Menge aller derjenigen $s \in S_n$, für die $s(Y_i) = Y_i$, $i = 1, \dots, r$, gilt. Man beweise, daß $S_n^{Y_1,\dots,Y_r}$ eine Untergruppe von S_n ist, die eine Darstellung als direktes Produkt

$$S_n^{Y_1,\dots,Y_r} = \prod_{i=1}^{r} S_n^{Y_i}$$

(vgl. Übung 1.15) besitzt. Man bestimme $|S_n^{Y_1,\dots,Y_r}|$.

Übung 12. Es sei $n = \sum_{i=1}^{r} n_i$, $n_i \in \mathbf{N}$. Wir bezeichnen mit $\mathfrak{X}_{n_1,\dots,n_r}$ die Menge aller möglichen Zerlegungen der Menge $\{1, \dots, n\}$ der Form

$$\{1, \dots, n\} = \bigcup_{i=1}^{r} Y_i, \qquad |Y_i| = n_i, \qquad i = 1, \dots, r.$$

Man betrachte S_n als transitive Transformationsgruppe der Menge $\mathfrak{X}_{n_1,\dots,n_r}$ und beweise

$$|\mathfrak{X}_{n_1,\dots,n_r}| = \frac{n!}{n_1! \dots n_r!}.$$

Übung 13. Es seien G, H Gruppen. Man beweise, daß eine Abbildung $f: G \to H$ genau dann ein Homomorphismus ist, wenn ihr Graph $\Gamma_f := \{(g, f(g))\}_{g \in G}$ eine Untergruppe von $G \times H$ ist.

§ 3. Ideale und Faktorringe

In diesem Paragraphen wollen wir für die Theorie der Ringe ein Analogon des in § 1 für die Gruppen Dargelegten entwickeln. Die Rolle der Normalteiler übernehmen hier Unterringe spezieller Art, die Ideale, die wir nun definieren:

Definition 1. Eine Teilmenge B des Ringes A heißt ein *Ideal*, wenn 1. B eine Untergruppe der additiven Gruppe von A ist und 2. für beliebige $a \in A$ und $b \in B$ stets $ab \in B$ und $ba \in B$ gilt.

Offenbar ist jedes Ideal ein Unterring; denn wegen der Bedingung 2 ist natürlich $B \cdot B \subseteq B$.

Beispiel 1. Es sei A ein assoziativer und kommutativer Ring und $a \in A$. Dann ist die Menge aA aller durch a teilbaren Elemente von A ein Ideal, wie man leicht mit Hilfe von Satz 2.2.4 beweist. Dieses Ideal wird das *von a erzeugte Hauptideal* des Ringes A genannt, a heißt ein *erzeugendes Element* von aA. Ist A ein Ring mit Einselement, so gilt $a \in aA$. Aus Satz 2.2.5 folgt, daß in einem Integritätsbereich das erzeugende Element eines Hauptideals bis auf Assoziiertheit eindeutig bestimmt ist.

Beispiel 2. Es sei $A = \mathbf{Z}[x]$. Man überprüft leicht, daß die Menge B aller Polynome der Form $a_0 + a_1 x + \ldots + a_n x^n$ mit $2 \mid a_0$ ein Ideal in A ist. Dieses Ideal ist kein Hauptideal. Wäre nämlich $B = \alpha A$ mit $\alpha \in A$, so müßte $\alpha \mid 2$ gelten; denn es ist $2 \in B$. Nach Satz 2.4.1 müßte daher $\operatorname{gr} \alpha = 0$ sein, also $\alpha = \pm 1$ oder ± 2. Das führt jedoch auf einen Widerspruch.

Beispiel 3. Es sei A der Ring aller stetigen Funktionen auf dem Intervall $[a, b]$ mit Werten in $\mathbf{R}$. Für $c \in [a, b]$ ist die Menge B aller Funktionen $f \in A$ mit $f(c) = 0$ ein Ideal in A.

Beispiel 4. In einem beliebigen Ring A sind die Teilmengen $\{0\}$ und A Ideale. Ist A ein Körper, so gibt es außer diesen beiden keine anderen Ideale. Ist nämlich $I \subseteq A$ Ideal des Körpers A und existiert ein $a \neq 0$ in I, dann ist auch $b = (b/a)\, a \in I$ für alle $b \in A$; und somit gilt $I = A$.

Satz 1. *Es sei A ein Ring und B eine Untergruppe der additiven Gruppe von A. Dann ist die Relation $=_B$ mit der Multiplikation in A verträglich dann und nur dann, wenn B ein Ideal in A ist.*

Beweis. Es sei B ein Ideal. Dann folgt aus $a_1 =_B b_1$ und $a_2 =_B b_2$, d. h. also mit $c_i := a_i - b_i \in B$,

$$a_1 \cdot a_2 = (b_1 + c_1)(b_2 + c_2) = b_1 b_2 + (b_1 + c_1) c_2 + c_1 b_2 .$$

Nach Definition eines Ideals gilt $(b_1 + c_1) c_2 + c_1 b_2 \in B$, also $a_1 a_2 =_B b_1 b_2$. Umgekehrt sei nun $=_B$ mit der Multiplikation in A verträglich. Für $a \in A$ und $b \in B$ folgt dann $a =_B a$ und $b =_B 0$, also $ab =_B a0 = 0$ und $ba =_B 0a = 0$. Daher liegen ab und ba in B, B ist somit ein Ideal. □

Für jedes Ideal B des Ringes A ist nach Satz 1 und Satz 2.6.1 in der Faktorgruppe A/B eine Multiplikation durch

$$(a_1 + B) \cdot (a_2 + B) := a_1 a_2 + B \tag{1}$$

erklärt, und es gilt

Satz 2. *Es sei A ein Ring und $B \subseteq A$ ein Ideal. Die Multiplikation* (1) *und die Addition der Faktorgruppe A/B verwandeln A/B in einen Ring. Die kanonische Abbildung $p\colon A \to A/B$ ist ein Ringhomomorphismus. Wenn A assoziativ oder kommutativ ist, besitzt auch A/B diese Eigenschaft. Ist A ein Ring mit Einselement e, so ist $e + B$ Einselement des Ringes A/B.*

Beweis. Für beliebige $a_1, a_2 \in A$ gilt $(a_1+B)+(a_2+B)=(a_1+a_2)+B$. Für $b \in A$ folgt dann nach (1)

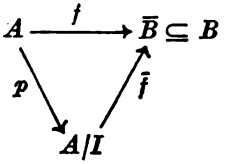
$$\begin{aligned}((a_1+B)+(a_2+B))\,(b+B) &= (a_1+a_2)\,b+B = a_1b+a_2b+B \\ &= (a_1b+B)+(a_2b+B) \\ &= (a_1+B)\,(b+B)+(a_2+B)\,(b+B)\,.\end{aligned}$$

Analog beweist man die andere Distributivitätsbedingung. Der Rest der Behauptung ergibt sich aus Satz 2.6.1. □

Definition 2. Ist B ein Ideal des Ringes A, so heißt der nach Satz 2 gegebene Ring $[A/B, +, \cdot]$ der *Faktorring* von A nach B.

Beispiel 5. Der Faktorring $\mathbf{Z}/n\mathbf{Z}$, $n \in \mathbf{N}$, ist der Restklassenring $\mathbf{Z}_n$ modulo n (vgl. Definition 2.2.9).

Satz 3 (Homomorphiesatz für Ringe). *Es sei $f\colon A \to B$ ein Ringhomomorphismus, $I = \operatorname{Ker} f$ und $\bar{B} = \operatorname{Im} f$. Dann ist I ein Ideal in A, und es gibt einen eindeutig bestimmten Ringisomorphismus $\bar{f}\colon A/I \to \bar{B}$, für den das Diagramm*



kommutativ ist.

Beweis. Offenbar ist I eine Untergruppe von $[A, +]$; wegen $f(a \cdot b) = f(a) \cdot f(b) = 0$ für $a \in A$ und $b \in I$ und der analogen Beziehung $f(ba) = 0$ folgt, daß I ein Ideal ist. Wenn das obige Diagramm kommutativ sein soll, muß $\bar{f}$ mit dem schon in Satz 1.6 definierten Gruppenisomorphismus übereinstimmen:

$$\bar{f}(a+I) = f(a) \qquad (a \in A)\,.$$

Es bleibt nur zu zeigen, daß $\bar{f}$ auch ein Homomorphismus für die Multiplikation ist:

$$\begin{aligned}\bar{f}((a_1+I)\,(a_2+I)) &= \bar{f}(a_1a_2+I) = f(a_1 \cdot a_2) = f(a_1) \cdot f(a_2) \\ &= \bar{f}(a_1+I) \cdot \bar{f}(a_2+I)\,.\end{aligned}$$ □

Übung 1. Man formuliere und beweise für Ringe die Analoga von Satz 1.5 und Folgerung 1.4.

Übung 2. Es sei A ein assoziativer und kommutativer Ring mit Einselement. Man beweise: Gibt es in A keine Ideale außer $\{0\}$ und A, so ist A ein Körper. Ferner zeige man: Ist $I \neq A$ ein *maximales, echtes Ideal* von A, d. h., folgt aus $I \subseteq I_1 \subseteq A$, I_1 Ideal, daß $I_1 = I$ oder $I_1 = A$ gilt, so ist der Faktorring A/I ein Körper, und umgekehrt.

Übung 3. Es seien A ein Ring, B ein Unterring und I ein Ideal in A. Man beweise das folgende Analogon von Satz 2.1: $B+I$ ist ein Unterring in A, $I \cap B$ ist ein Ideal in B, und es gilt $B/I \cap B \cong (B+I)/I$.

Übung 4. Man beweise, daß die Ideale eines beliebigen Ringes einen vollständigen Verband bilden.

Übung 5. Man beweise den folgenden *Homomorphiesatz für Monoide*: Es sei $f: M \to N$ ein Homomorphismus der Monoide und $\sim$ die durch die Abbildung f in M definierte Äquivalenzrelation. Dann ist die Relation $\sim$ mit der Operation in M verträglich, und es gibt einen eindeutig bestimmten Isomorphismus $\bar{f}: M/\sim \to N = \mathrm{Im}\, f$, für den $\bar{f} \circ p = f$ gilt; hierbei bezeichnet $p: M \to M/\sim$ die kanonische Abbildung.

Zum Abschluß dieses Paragraphen wollen wir noch kurz die Begriffe „direktes Produkt" und „direkte Summe" für Ringe beschreiben.

Definition 3. Es sei $(A_i)_{i\in I}$ eine Familie von Unterringen des Ringes A. Man sagt, A sei *direkte Summe der Unterringe* A_i, wenn 1. $A = \bigoplus_{i\in I} A_i$ eine Zerlegung der additiven Gruppe von A in die direkte Summe der additiven Untergruppen A_i ist und 2. stets $ab = 0$ gilt für $a \in A_i$, $b \in A_j$ und $i \neq j$, $i, j \in I$.

Übung 6. Es sei $A = \bigoplus_{i=1}^{r} A_i$ eine Zerlegung der additiven Gruppe des Ringes A in eine direkte Summe von Untergruppen. Man beweise, daß diese Zerlegung eine direkte Summe von Unterringen dann und nur dann ist, wenn alle A_i Ideale in A sind.

Es seien nun $A_1, \ldots, A_r$ beliebige Ringe. Wir betrachten das direkte Produkt $A := \bigtimes_{i=1}^{r} A_i$ der additiven Gruppen A_i. Nach Definition 2.2 wird durch die Multiplikationen in den Ringen A_i eine Multiplikation in A bestimmt. Man prüft leicht nach, daß $[A, +, \cdot]$ ein Ring ist. Dieser Ring heißt das *direkte Produkt* der Ringe A_i, $i = 1, \ldots, r$. Die in § 2 definierten Abbildungen $\iota_k: A_k \to A$ sind injektive Ringhomomorphismen; ι_k bildet also den Ring A_k isomorph auf den Unterring $\tilde{A}_k = \{(0, \ldots, 0, a_k, 0, \ldots, 0) \mid a_k \in A_k\} \subseteq A$ ab.

Übung 7. Man beweise, daß der Ring $A = \bigtimes_{i=1}^{r} A_i$ in die direkte Summe der Unterringe $\tilde{A}_i$, $i = 1, \ldots, r$, zerfällt. Umgekehrt, zerfällt ein Ring A in eine direkte Summe seiner Unterringe $B_1, \ldots, B_r$, so gibt es einen eindeutig bestimmten Ringisomorphismus $\varphi: A \to B := \bigtimes_{i=1}^{r} B_i$, so daß $\varphi \mid B_k = \iota_k$ für $k = 1, \ldots, r$ gilt.

Übung 8. Man beweise, daß ein direktes Produkt zweier von $\{0\}$ verschiedener Ringe stets Nullteiler besitzt (vgl. Übung 2.2.8).

Übung 9. Es sei X eine Menge aus $n > 0$ Elementen und A ein beliebiger Ring. Man beweise, daß der Ring $M(X, A)$ (vgl. Beispiel 2.1.2) isomorph zum direkten Produkt von n Exemplaren des Ringes A ist.

Übung 10. Man beweise, daß die in Übung 2.8 festgestellte Isomorphie der additiven Gruppen der Restklassenringe sogar eine Ringisomorphie ist.

§ 4. Hauptidealringe

In diesem Paragraphen betrachten wir die wichtige Klasse der Hauptidealringe, die Verallgemeinerungen der euklidischen Ringe sind.

Definition 1. Unter einem *Hauptidealring* versteht man einen Integritätsbereich, dessen Ideale sämtlich Hauptideale sind.

Beispiel 1. *Jeder euklidische Ring A ist ein Hauptidealring.* In der Tat, sei $I \subseteq A$ ein Ideal, $I \neq \{0\}$, dann gibt es in I ein Element $a_0 \neq 0$, so daß $w(a_0) \leqq w(a)$ für alle $a \in I$, $a \neq 0$, gilt. Aus der Definition eines Ideals folgt unmittelbar $a_0 A \subseteq I$. Andererseits sei $b \in I$. Da A ein euklidischer Ring ist, gibt es $q, r \in A$, so daß $b = a_0 q + r$ gilt mit $r = 0$ oder $w(r) < w(a_0)$. Nun ist $r = b - a_0 q \in I$, und deshalb kann $w(r) < w(a_0)$ nicht eintreten; es gilt also $b = q a_0 \in a_0 A$.

Beispiel 2. Der Ring $\mathbf{Z}[x]$ ist ein Integritätsbereich, aber kein Hauptidealring, vgl. Beispiel 3.2.

Wir wollen als erstes beweisen, daß in einem Hauptidealring der ggT (größte gemeinsame Teiler) stets existiert. Es sei zunächst A ein beliebiger, assoziativer und kommutativer Ring, und es seien $a_1, \ldots, a_r \in A$. Wir definieren die Untergruppe

$$I := a_1 A + \ldots + a_r A$$

der additiven Gruppe von A. Die Untergruppe I besteht aus allen Elementen der Form $a_1 b_1 + \ldots + a_r b_r$, $b_i \in A$. Man prüft leicht nach, vgl. Übung 3.4, daß I ein Ideal in A ist. Wenn A ein Einselement enthält, gilt $a_i \in I$ für $i = 1, \ldots, r$.

Satz 1. *Es sei A ein Hauptidealring. Dann gibt es zu je r Elementen $a_1, \ldots, a_r \in A$ einen ggT $d = (a_1, \ldots, a_r)$, $r \in \mathbf{N}$. Dabei ist d das bis auf Assoziiertheit eindeutig bestimmte erzeugende Element des Ideals $I = a_1 A + \ldots + a_r A$. Es gibt also $b_i \in A$ so, daß*

$$d = a_1 b_1 + \ldots + a_r b_r$$

gilt.

Beweis. Da I ein Ideal ist, gibt es ein $d \in A$ mit $I = dA$. Wegen $a_i \in I$ folgt $d \mid a_i$. Ist andererseits $d_1 \in A$ und gilt $d_1 \mid a_i$ für $i = 1, \ldots, r$, so teilt d_1 jedes Element aus I, also gilt auch $d_1 \mid d$ (vgl. Satz 2.2.4). Die Eindeutigkeitsaussage folgt aus Beispiel 3.1. □

Folgerung 1. *Die Elemente $a_1, \ldots, a_r$ sind teilerfremd dann und nur dann, wenn $b_1, \ldots, b_r \in A$ existieren, so daß*

$$a_1 b_1 + \ldots + a_r b_r = e$$

gilt.

Beweis. Ist $e = (a_1, \ldots, a_r)$, so gibt es nach Satz 1 eine Darstellung der geforderten Art. Ist umgekehrt $(a_1, \ldots, a_r) = d \nsim e$, so gilt $d \nmid e$, also $e \notin I$, d. h., eine solche Darstellung existiert nicht. □

Folgerung 2. *Es sei A ein Hauptidealring, und es seien $a, b, c \in A$, $(a, c) = e$ und $c \mid ab$. Dann gilt $c \mid b$.* □

Folgerung 3. *Es sei A ein Hauptidealring und $p \in A$ ein Primelement. Gilt $p \mid a_1 \ldots a_r$ für gewisse Elemente $a_1, \ldots, a_r \in A$, so gibt es ein i mit $p \mid a_i$.*

Der Beweis dieser Folgerungen ist wörtlich der von Satz 2.5.3 bzw. 2.5.4.

Satz 2. *Es sei A ein Hauptidealring. Dann gibt es für jedes $a \in A$, $a \neq 0$, $a \notin A^*$, eine Darstellung als Produkt von Primelementen des Ringes A. Diese Darstellung ist bis auf die Reihenfolge der Faktoren und bis auf Assoziiertheit eindeutig.*

Beweis. Die erste Behauptung beweisen wir indirekt. Angenommen, es gibt ein Element $a_0 \in A \setminus A^*$, $a_0 \neq 0$, so daß für a_0 keine Zerlegung in Primfaktoren existiert. Dann kann a_0 nicht Primelement sein, es besitzt daher eine echte Zerlegung $a_0 = a_1 b$, $a_1, b \in A \setminus A^*$, $a_1 \neq 0$, $b \neq 0$. Würde nun für a_1 und b eine Zerlegung in Primfaktoren existieren, so ergäbe das sofort eine Primfaktorzerlegung von a_0. Also sei etwa a_1 nicht in Primfaktoren zerlegbar. Da a_0 und a_1 nicht assoziiert sind, gilt $a_0 A \subset a_1 A$. Setzen wir diese Überlegung fort, so erhalten wir eine unendliche, monoton aufsteigende Kette von Hauptidealen

$$a_0 A \subset a_1 A \subset \ldots \subset a_i A \subset a_{i+1} A \subset \ldots \tag{1}$$

Es sei $I := \bigcup_{i=0}^{\infty} a_i A$. Man prüft leicht nach, daß I ein Ideal ist. Daher gibt es ein $d \in I$ mit $I = dA$. Dann muß aber auch ein i existieren mit $d \in a_i A$, so daß $I = dA \subseteq a_i A \subseteq I$ gilt, also $I = a_i A$. Das ist aber ein Widerspruch zur Unendlichkeit der Kette (1). Die Eindeutigkeitsaussage beweist man ebenso wie für Satz 2.5.5, wobei man Folgerung 3 benutzt. □

Übung 1. Man beweise, daß der Ring der formalen Potenzreihen $K[[x]]$ über einem Körper K (Übung 2.4.1) ein Hauptidealring ist. Weiter bestimme man alle Primelemente von $K[[x]]$ und gebe für beliebiges $\alpha \in K[[x]]$ die Zerlegung in Primfaktoren an.

Übung 2. Man beweise, daß ein Hauptidealring ein Körper ist dann und nur dann, wenn er keine Primelemente enthält.

Satz 3. *Es sei A ein Hauptidealring und $a \in A$, $a \neq 0$. Dann sind folgende Aussagen äquivalent:*

1. *a ist ein Primelement;*
2. *A/aA ist ein Körper;*
3. *A/aA ist ein Integritätsbereich.*

Beweis. Wir zeigen zuerst, daß die zweite Aussage aus der ersten folgt. Nach Satz 3.2 ist A/aA ein assoziativer und kommutativer Ring mit Einselement, hierbei gilt $e + aA \neq 0 + aA$; wäre nämlich $e =_{aA} 0$, so wäre $e \in aA$, also $a \mid e$, d. h. $a \in A^*$, a wäre kein Primelement. Wir zeigen, daß jedes von 0 verschiedene Element aus A/aA invertierbar ist. Es sei also $b \in A$, $b + aA \neq aA$. Dann gilt $a \nmid b$, und da a prim ist, folgt $(a, b) = e$ (Satz 2.2.8). Nach Folgerung 1 existieren $u, v \in A$ mit $bu + av = e$, also $bu + av =_{aA} bu =_{aA} e$. Somit gilt $u + aA = (b + aA)^{-1}$.

Der Schluß von der zweiten auf die dritte Aussage ist trivial. Es bleibt zu zeigen, daß die erste Aussage aus der dritten folgt. Es sei also A/aA ein Integritätsbereich. Dann enthält A/aA ein von 0 verschiedenes Element, und es folgt $a \notin A^*$. Angenommen, wir hätten eine Zerlegung $a = bc$ mit $b, c \in A$. Dann gilt $0 =_{aA} bc$, und da A/aA Integritätsbereich ist, muß $b =_{aA} 0$ oder $c =_{aA} 0$ sein. Es sei etwa $b =_{aA} 0$, d. h. $b \in aA$. Dann gilt $a \mid b$, und wegen $b \mid a$ ist $a \sim b$ und $c \in A^*$. Daher ist a ein Primelement. □

Für $A = \mathbf{Z}$ sind Satz 3 und Satz 2.2.10 identisch. Ein anderer wichtiger Spezialfall, nämlich $A = K[x]$, K ein Körper, wird im nächsten Paragraphen behandelt.

Übung 3. Es sei A ein Integritätsbereich. Man beweise, daß $A[x]$ ein Hauptidealring ist dann und nur dann, wenn A ein Körper ist.

§ 5. Adjunktion der Nullstellen eines Polynoms. Beweis des Gaußschen Fundamentalsatzes der Algebra

Es sei K ein Körper und $\varphi \in K[x]$ ein irreduzibles Polynom. Gilt $\operatorname{gr} \varphi > 1$, so hat φ keine Nullstellen in K. Mit Hilfe der Ergebnisse von § 4 wollen wir nun eine Erweiterung L des Körpers K konstruieren, in der φ eine Nullstelle besitzt. Als Anwendung beweisen wir den Gaußschen Satz, daß jedes Polynom über $\mathbf{C}$ eine Nullstelle in $\mathbf{C}$ besitzt.

Satz 1. *Es sei K ein Körper und $\varphi \in K[x]$ ein irreduzibles Polynom, $n = \operatorname{gr} \varphi > 1$. Dann existiert ein Erweiterungskörper $L \supset K$ und ein Element $\zeta \in L$ mit folgenden Eigenschaften:*

1. $\varphi(\zeta) = 0$.
2. *Jedes Element $b \in L$ ist eindeutig in der Gestalt*

$$b = b_0 + b_1\zeta + \ldots + b_{n-1}\zeta^{n-1} \tag{1}$$

mit $b_i \in K$, $i = 0, \ldots, n-1$, darstellbar.

3. *Ist $L_1 \subseteq L$ ein Unterring mit $K \cup \{\zeta\} \subseteq L_1$, so gilt $L_1 = L$.*

Beweis. Da φ ein Primelement ist, muß nach Satz 4.3 der Ring $L := K[x]/I$ mit $I := \varphi K[x]$ ein Körper sein. Offenbar gilt für alle $\alpha \in I, \alpha \neq 0$, daß $\operatorname{gr} \alpha \geqq n > 1$ ist; also ist $K \cap I = \{0\}$. Daher induziert der kanonische Homomorphismus $p\colon K[x] \to L$ den injektiven Homomorphismus $p \mid K$. Sein Bild $p(K)$ besteht aus allen Klassen der Form $a + I$ mit $a \in K$; es ist ein Teilkörper von L. Identifizieren wir $a \in K$ mit $a + I \in L$ für alle $a \in K$, so wird L eine Erweiterung von K. Daher ist auch $K[x] \subseteq L[x]$, und wir können φ als Polynom über L betrachten. Nach dieser Identifizierung können wir sehr einfach den kanonischen Homomorphismus $p\colon K[x] \to L$ beschreiben. Es sei nämlich $p(x) = \zeta$. Dann gilt für $\beta = \sum_\nu b_\nu x^\nu$ offenbar

$$p(\beta) = \sum_\nu p(b_\nu)\, p(x)^\nu = \sum_\nu b_\nu \zeta^\nu \in L\,,$$

also

$$\beta(\zeta) = p(\beta) = \beta + I, \qquad \beta \in K[x]\,. \tag{2}$$

Speziell ist $0 = p(\varphi) = \varphi(\zeta)$. Daher ist ζ eine Nullstelle von φ über L, d. h., es gilt Eigenschaft 1.

Die zweite Behauptung ergibt sich sofort durch Division mit Rest in $K[x]$ (Satz 2.4.2). Es sei $b = p(\beta) \in L$. Für $\beta \in K[x]$ erhalten wir nach Division durch φ: $\beta = \alpha \cdot \varphi + \gamma$ mit $\alpha, \gamma \in K[x]$, $\gamma = 0$ oder $\operatorname{gr} \gamma < n$. Somit gilt wegen $p(\varphi) = 0$

$$b = p(\beta) = p(\gamma) = \sum_{i=0}^{n-1} c_i \zeta^i;$$

das ist aber eine Darstellung der Form (1). Angenommen, wir hätten zwei derartige Darstellungen, etwa (1) und die eben angegebene. Dann gilt

$$0 = b_0 - c_0 + (b_1 - c_1)\,\zeta + \ldots + (b_{n-1} - c_{n-1})\,\zeta^{n-1}\,.$$

Wir hätten also ein Polynom

$$\psi = \sum_{i=0}^{n-1} (b_i - c_i)\, x^i \in K[x]$$

mit $p(\psi) = \psi(\zeta) = 0$, also $\psi \in I = \varphi K[x]$, d. h. $\varphi \mid \psi$. Wäre $\psi \neq 0$, so erhielten wir einen Widerspruch zu $\operatorname{gr} \varphi > \operatorname{gr} \psi$. Also muß $\psi = 0$, d. h. $b_i = c_i$ für $i = 0, \ldots, n-1$, sein. Die dritte Behauptung folgt unmittelbar aus der zweiten. □

Definition 1. Der im Beweis von Satz 1 konstruierte Körper L heißt der durch *Adjunktion einer Nullstelle von φ entstehende Erweiterungskörper von K.*

Wir wollen nun Satz 1 durch die folgende Eindeutigkeitsaussage ergänzen:

Satz 2. *Es seien K ein Körper, $\varphi \in K[x]$ ein irreduzibles Polynom vom Grade $n > 1$, M ein Erweiterungskörper von K, der eine Nullstelle c von φ enthalte. Dann gibt es einen Isomorphismus der in Satz 1 angegebenen Erweiterung L von K auf einen Teilkörper $L_1 \subseteq M$ mit den folgenden Eigenschaften:*

1. *Es gilt $f \mid K = \mathrm{id}_K$.*
2. *$f(\zeta) = c$.*
3. *Jedes Element $b \in L_1$ besitzt eine und nur eine Darstellung der Form $b = b_0 + b_1 c + \ldots + b_{n-1} c^{n-1}$ mit $b_i \in K$.*
4. *Enthält M keinen echten Teilkörper, der K und c umfaßt, so gilt $L_1 = M$.*

Beweis. Nach Satz 2.4.4 ist die Abbildung

$$g: \alpha \in K[x] \mapsto g(\alpha) := \alpha(c) \in M$$

ein Ringhomomorphismus. Wir wollen zeigen, daß $\operatorname{Ker} g = I := \varphi K[x]$ gilt. Aus $\varphi(c) = 0$ folgt $\varphi \in \operatorname{Ker} g$ und somit $I \subseteq \operatorname{Ker} g$. Da nun L ein Körper ist, erhielten wir aus $I \neq \operatorname{Ker} g$, weil $p(\operatorname{Ker} g) \neq \{0\}$ ein Ideal in L ist, daß $p(\operatorname{Ker} g) = L$ gelten muß (Beispiel 3.4). Dann gibt es zu jedem $\alpha \in K[x]$ ein $\beta \in \operatorname{Ker} g$ mit $p(\alpha) = p(\beta)$, also ein $\gamma \in I$ mit $\alpha = \beta + \gamma$, und aus $I \subseteq \operatorname{Ker} g$ erhielten wir $g(\alpha) = 0$ für alle $\alpha \in K[x]$, was jedoch $g(\alpha) = a$ für $\alpha = a \in K$ widerspricht. Somit muß $I = \operatorname{Ker} g$ gelten. Nach dem Homomorphiesatz 3.3 ist die durch $f := \bar{g}$, d. h.

$$\alpha + I \in L \mapsto f(\alpha + I) := g(\alpha) = \alpha(c), \qquad \alpha \in K[x],$$

definierte Abbildung ein Isomorphismus auf $L_1 := \operatorname{Im} g$. Wegen der Identifizierung $a = a + I$ für $a \in K$ gilt $f(a) = a(c) = a$, womit die erste Behauptung bewiesen ist. Aus $f(\zeta) = f(x + I) = x(c) = c$ ergibt sich die Eigenschaft 2. Die Behauptung 3 folgt aus der Eigenschaft 2 von Satz 1, und die Behauptung 4 ist offensichtlich. □

Beispiel 1. Es sei $K = \mathbf{R}$ und $\varphi = x^2 + 1$. Durch Satz 1 erhalten wir ein von dem in § 2.3 angegebenen verschiedenes Verfahren zur Konstruktion von $\mathbf{C}$. Den Satz 2 kann man als eine Verallgemeinerung von Satz 2.3.3 betrachten.

Übung 1. Unter Anwendung von Satz 1 konstruiere man Körper mit 4, 8 und 9 Elementen.

Satz 3. *Es sei K ein Körper und $\alpha \in K[x]$ ein beliebiges Polynom mit $\operatorname{gr} \alpha > 0$. Dann gibt es einen Erweiterungskörper von K, über dem α zerfällt.*

Beweis. Wir führen den Beweis durch vollständige Induktion nach $\operatorname{gr}\alpha$. Für $\operatorname{gr}\alpha=1$ ist K selbst Zerfällungskörper für α. Die Behauptung sei schon für Polynome vom Grad $n-1$ bewiesen, und es sei $\operatorname{gr}\alpha=n$. Nach Satz 2.5.5 (oder 4.2) gibt es eine Darstellung von α als Produkt von Primfaktoren $\alpha=\varphi_1 \dots \varphi_r$. Nach Satz 1 konstruieren wir eine Erweiterung $L\supseteq K$, indem wir, falls $\operatorname{gr}\varphi_1>1$ ist, eine Nullstelle ζ von φ_1 adjungieren. Offenbar gilt $\alpha(\zeta)=0$, also $\alpha=(x-\zeta)\,\beta$ mit $\beta\in L[x]$, $\operatorname{gr}\beta=n-1$ (vgl. Satz 2.4.5). Nach Induktionsvoraussetzung gibt es nun eine Erweiterung M von L, in der β zerfällt. Offenbar zerfällt dann auch α in M. □

Abschließend wollen wir nun den „Fundamentalsatz der Algebra" von C. F. Gauss (Satz 2.8.1) beweisen. Der Beweis wird über zwei Hilfssätze geführt.

Lemma 1. *Jedes Polynom vom Grad* 2 *über* $\mathbf{C}$ *hat zwei komplexe Nullstellen.*

Beweis. Wir können $\alpha=x^2+px+q$ setzen. Im Fall $4q=p^2$ ist $\alpha=\left(x+\frac{1}{2}p\right)^2$; es hat daher eine Nullstelle der Vielfachheit 2. Falls $p^2-4q\neq 0$ ist, bezeichne $\sqrt{p^2-4q}$ eine der nach Folgerung 2.3.2 existierenden beiden komplexen Quadratwurzeln aus p^2-4q. Dann gilt offenbar

$$\alpha=\left(x+\frac{p}{2}-\frac{1}{2}\sqrt{p^2-4q}\right)\left(x+\frac{p}{2}+\frac{1}{2}\sqrt{p^2-4q}\right). \quad \square$$

Lemma 2. *Jedes Polynom* $\alpha\in\mathbf{R}[x]$ *vom Grad* $\operatorname{gr}\alpha>0$ *besitzt eine Nullstelle in* $\mathbf{C}$.

Beweis. Es sei $n=\operatorname{gr}\alpha=2^k p$, wobei $k\geqq 0$ und p eine ungerade Zahl ist. Wir beweisen das Lemma durch Induktion nach k. Es sei zuerst $k=0$, d. h. n ungerade. Dann hat α sogar eine reelle Nullstelle: Ist etwa das höchste Glied $a_n>0$, so nimmt α für genügend große c positive Werte $\alpha(c)$ und für genügend kleine c negative Werte an; da α eine auf $\mathbf{R}$ stetige Funktion bestimmt, muß sie auch für ein gewisses $c_0\in\mathbf{R}$ den Wert 0 annehmen.

Nehmen wir nun an, daß Lemma 2 schon für alle Polynome mit einem Grad der Form $2^{k-1}p$, p ungerade, bewiesen sei. Es sei $\alpha\in\mathbf{R}[x]$ ein Polynom mit $\operatorname{gr}\alpha=2^k p$, das wir auch als Polynom über $\mathbf{C}$ betrachten können. Nach Satz 3 existiert eine Erweiterung $K\supseteq\mathbf{C}\supseteq\mathbf{R}$, in der α zerfällt. Es seien $u_1, \dots, u_n$, $n=2^k p$, die Nullstellen von α in K. Für ein beliebiges, aber festes $c\in\mathbf{R}$ definieren wir die Elemente

$$v_{ij}:=u_i u_j+c\,(u_i+u_j)\in K, \qquad 1\leqq i<j\leqq n\,.$$

Wir betrachten nun den Ring $\mathbf{R}[y_{12}, \dots, y_{n-1,n}]$ der reellen Polynome in den $\frac{1}{2}n\,(n-1)$ Unbestimmten $y_{12}, \dots, y_{n-1,n}$ und wollen zuerst folgende Behauptung beweisen: Ist $\gamma\in\mathbf{R}[y_{12}, \dots, y_{n-1,n}]_{S_{n(n-1)/2}}$ ein symmetrisches Polynom, so gilt $\gamma(v_{12}, \dots, v_{n-1,n})\in\mathbf{R}$. Zu diesem Zweck betrachten wir den Homomorphismus

$$f\colon \mathbf{R}[y_{12}, \dots, y_{n-1,n}]\to\mathbf{R}[x_1, \dots, x_n]\,,$$

der durch die Bedingungen

$$f(a)=a \quad \text{für} \quad a\in\mathbf{R} \quad \text{und} \quad f(y_{ij})=z_{ij}:=x_i x_j+c\,(x_i+x_j)$$

bestimmt wird (vgl. Satz 2.7.5). Ist nun γ ein symmetrisches Polynom der y_{ij}, so ist $f(\gamma)$ ein symmetrisches Polynom in den x_i; in der Tat, ist $(k\ l) \in S_n$ eine Transposition, so bestimmt sie eine Permutation der z_{ij}, also eine Permutation $s_{kl} \in S_{n(n-1)/2}$. Man erkennt leicht, z. B. aus Übung 2.7.4, daß

$$(k\ l)\, f(\gamma) = f(s_{kl}\gamma), \qquad \gamma \in \mathbf{R}[y_{12}, \ldots, y_{n-1,n}],$$

gilt. Ist also γ symmetrisch, so erhalten wir $(k\ l)\, f(\gamma) = f(\gamma)$, und aus Folgerung 2.7.2 ergibt sich, daß $f(\gamma)$ symmetrisch ist.

Offenbar gilt für ein beliebiges $\gamma \in \mathbf{R}[y_{12}, \ldots, y_{n-1,n}]$

$$\gamma(v_{12}, \ldots, v_{n-1,n}) = f(\gamma)\,(u_1, \ldots, u_n),$$

vgl. wieder Übung 2.7.4. Mit γ ist auch $f(\gamma)$ symmetrisch, also ist $f(\gamma)\,(u_1, \ldots, u_n)$ reell, da die u_i Nullstellen des reellen Polynoms α sind, vgl. Folgerung 2.7.4.

Nun betrachten wir das Polynom

$$\beta := \prod_{1 \leqq i < j \leqq n} (x - v_{ij})$$

über K. Nach Satz 2.4.8 haben seine Koeffizienten die Gestalt $(-1)^k \sigma_k(v_{12}, \ldots, v_{n-1,n})$, wobei σ_k die elementarsymmetrischen Polynome in den Unbestimmten y_{ij} sind. Nach dem eben Bewiesenen sind diese Koeffizienten reell, d. h., es gilt $\beta \in \mathbf{R}[x]$. Für den Grad von β erhalten wir

$$\operatorname{gr} \beta = \frac{n(n-1)}{2} = \frac{1}{2}\,(2^k p\,(2^k p - 1)) = 2^{k-1} q,$$

wobei q eine ungerade Zahl ist. Also hat β nach Induktionsvoraussetzung wenigstens eine komplexe Nullstelle. Damit finden wir für jede reelle Zahl c wenigstens ein Paar (i, j), $i < j$, mit $v_{ij} \in \mathbf{C}$. Da die Anzahl dieser Paare endlich ist, gibt es c, $c' \in \mathbf{R}$, $c \neq c'$, derart, daß (bei geeigneter Numerierung)

$$v_{12}(c) = u_1 u_2 + c\,(u_1 + u_2) \in \mathbf{C},$$
$$v_{12}(c') = u_1 u_2 + c'\,(u_1 + u_2) \in \mathbf{C}$$

gilt. Hieraus folgt leicht $a := u_1 + u_2 \in \mathbf{C}$ und $b := u_1 u_2 \in \mathbf{C}$; die u_1, u_2 sind also Nullstellen des komplexen Polynoms $\varphi = (x - u_1)\,(x - u_2) = x^2 - ax + b \in \mathbf{C}[x]$. Da φ nach Lemma 1 bereits zwei komplexe Nullstellen hat, müssen diese nach Satz 2.4.7 mit u_1, u_2 übereinstimmen, d. h., es gilt u_1, $u_2 \in \mathbf{C}$. □

Nun können wir leicht den Fundamentalsatz beweisen. Es sei $\alpha = \sum_{i=0}^{n} a_i x^i$ ein beliebiges Polynom aus $\mathbf{C}[x]$. Wir betrachten gleichzeitig das Polynom

$$\bar{\alpha} := \sum_{i=0}^{n} \bar{a}_i x^i$$

und setzen $\beta := \alpha\bar{\alpha}$. Dann gilt $\beta \in \mathbf{R}[x]$, wie man sofort aus der Formel für die Koeffizienten eines Produktes erkennt,

$$b_k = \sum_{i+j=k} a_i \bar{a}_j.$$

Nach Satz 2.3.6 ist

$$b_k = \sum_{i+j=k} \bar{a}_i \bar{\bar{a}}_j = \sum_{i+j=k} \bar{a}_i a_j = b_k \,.$$

Aus Lemma 2 ergibt sich die Existenz einer komplexen Nullstelle c von β. Nun gilt aber $\beta(c) = \alpha(c)\,\bar{\alpha}(c) = 0$. Ist $\alpha(c) = 0$, so sind wir fertig, andernfalls gilt $\bar{\alpha}(c) = 0$. Dann ist aber $\bar{c}$ eine Nullstelle von α; denn es gilt

$$\alpha(\bar{c}) = a_0 + a_1\bar{c} + \ldots + a_n\bar{c}^n = \overline{\bar{a}_0 + \bar{a}_1 c + \ldots + \bar{a}_n c^n} = \overline{\bar{\alpha}(c)} = 0 \,. \quad \square$$

4. Punkt- und Vektorräume

In diesem Kapitel beginnen wir mit dem Aufbau der affinen Geometrie. Wichtige Begriffe der affinen Geometrie sind Punkte, Geraden, Ebenen, Vektoren, Skalare (das sind Elemente eines vorgegebenen Körpers K), Parallelität u. a. m. Begriffe wie Längen und Winkel, die enger mit den reellen Zahlen zusammenhängen, werden erst in der euklidischen Geometrie in Kapitel 6 behandelt, das jedoch sehr stark auf der affinen Geometrie aufbaut. Bei der von uns gewählten Axiomatik erscheint die affine Geometrie als eine Transformationsgruppe, bei der die Vektoren als Translationen (Parallelverschiebungen) über dem affinen Punktraum wirken. Daher wird zunächst in den §§ 1 und 2 der Begriff des Vektorraumes entwickelt, der nicht nur für die Geometrie, sondern auch für die Algebra und die moderne Analysis von grundlegender Bedeutung ist. In § 3 werden dann die affinen Punkträume axiomatisch charakterisiert, die Geraden werden definiert, und erste geometrische Ergebnisse wie der Strahlensatz und die Beschreibung der Homothetien werden entwickelt. Mit der Einführung der Dimension in § 4 schließen wir die Axiomatik der affinen Geometrie ab; wir betrachten natürlich wegen der wichtigen Anwendungen von vornherein n-dimensionale affine Punkt- und Vektorräume über einem beliebigen Körper K; dem Anfänger sei empfohlen, sich zunächst alles für den Fall $K = \mathbf{R}$ und $n = 3$ vorzustellen. Nach Definition der Punkt- und Vektorkoordinaten in § 4 werden schließlich in den §§ 5 und 6 die k-dimensionalen Ebenen und ihre Lageeigenschaften untersucht. Besonders an den Dimensionssätzen des § 6 wird klar, daß es keine Schwierigkeiten bereitet, sich mit Hilfe algebraischer Methoden die n-dimensionalen Räume zu veranschaulichen. Die §§ 7 und 8 sind dem Volumen- und Determinantenbegriff gewidmet. Die Determinanten besitzen wichtige Anwendungen in allen Zweigen der Mathematik. Als ein erstes Anwendungsbeispiel beweisen wir die Cramersche Regel für die Auflösung eines linearen Gleichungssystems.

§ 1. Translationen. Dehnungen. Vektoren

In diesem einleitenden Paragraphen wollen wir an einige anschauliche Tatsachen aus der elementaren Geometrie erinnern, die uns als Ausgangspunkt für den axiomatischen Aufbau der Punkt- und Vektorräume dienen sollen. Ziel der Betrachtungen ist die Herausarbeitung des Begriffes eines Vektorraumes über einem Körper K. Die Elementargeometrie ist für uns nur ein heuristisches Hilfsmittel, um den Begriff des Vektorraumes zu motivieren; ist dieser Begriff einmal gewonnen, so läßt sich aus ihm umgekehrt die gesamte Geometrie und viele ihrer Verallgemeinerungen herleiten, was zum Teil im folgenden ausgeführt wird.

Mit $\boldsymbol{A}^n$ bezeichnen wir den *Punktraum*, dessen Geometrie wir beschreiben wollen; die natürliche Zahl n ist dabei kein Exponent, sondern nur ein oberer Index, der die *Dimension* des betrachteten Raumes angibt. Für uns sind im Moment nur die folgenden Fälle wichtig: Der nulldimensionale Raum $\boldsymbol{A}^0$ besteht aus einem einzigen Punkt $\boldsymbol{A}^0 = \{o\}$, der eindimensionale Raum ist eine Gerade, der zweidimensionale Raum eine Ebene, und der dreidimensionale Raum ist unser Anschauungsraum. Mit $a, b, \ldots, x, y, z \in \boldsymbol{A}^n$ bezeichnen wir die Elemente dieser Räume, die wir *Punkte* nennen.

Die Dimension n drückt dabei nur die folgende, für das weitere wichtige Tatsache aus: Es gibt sogenannte *kartesische Koordinatensysteme*, d. h. bijektive Abbildungen

$$\varphi: x \in \boldsymbol{A}^n \mapsto \varphi(x) = (\xi_1, \ldots, \xi_n) \in \mathbf{R}^n, \tag{1}$$

die jedem Punkt $x \in \boldsymbol{A}^n$ ein n-Tupel reeller Zahlen $\xi_i \in \mathbf{R}$, $i = 1, \ldots, n$, zuordnen und in den uns interessierenden Fällen folgendermaßen definiert sind: Für $n = 0$ setzen wir $\mathbf{R}^0 = \{0\}$ und wählen für φ die Abbildung $\varphi(o) = 0$; für $n = 1$ wählen wir einen Punkt $o \in \boldsymbol{A}^1$, dem wir die Zahl $0 \in \mathbf{R}$ zuordnen, einen Punkt $a \in \boldsymbol{A}^1$, $a \neq o$, dem wir die 1 zuordnen, und definieren die Funktion φ, indem wir durch Streckenabtragen und Teilen die *Skala* mit den Grundpunkten o, a auf der Geraden $\boldsymbol{A}^1$ konstruieren („Zahlenstrahl"); im Fall $n = 2$ wählen wir einen Punkt $o \in \boldsymbol{A}^2$ und zwei durch ihn gehende Geraden, auf denen wir Skalen mit den Grundpunkten o und a_1 bzw. a_2 konstruieren; die Koordinate ξ_i des Punktes $x \in \boldsymbol{A}^2$ ist dann der Skalenwert seiner Parallelprojektion auf die ξ_i-Achse ($i = 1, 2$) (Abb. 3). Ähnlich definiert man die

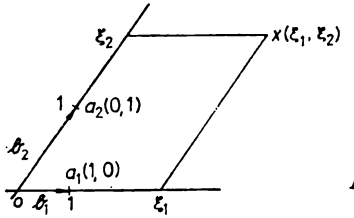


Abb. 3

Koordinaten im $\boldsymbol{A}^3$, indem man wieder von einem *Ursprung* $o \in \boldsymbol{A}^3$ ausgeht, durch ihn drei verschiedene Geraden, die *Achsen* des Systems, zieht und auf diesen je eine Skala einführt; dabei sollen diese drei Geraden nicht in einer Ebene liegen. Dann bestimmen je zwei der Geraden eine Ebene durch o, die wir entsprechend die ξ_1, ξ_2-

Ebene usw. nennen. Ziehen wir nun durch den beliebigen Punkt $x \in A^3$ die zur ξ_1, ξ_2-Ebene parallele Ebene und schneiden sie mit der ξ_3-Achse, so erhalten wir als Skalenwert des Schnittpunktes die dritte Koordinate ξ_3 von x und analog die anderen Koordinaten (Abb. 4).

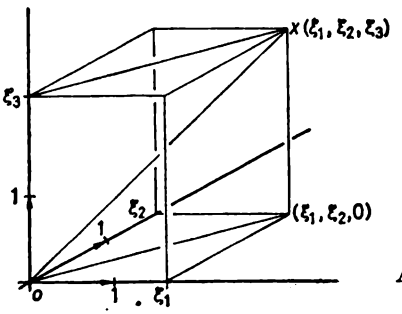


Abb. 4

Für den Rest dieses Paragraphen denken wir uns nun ein beliebiges Koordinatensystem, etwa in der Ebene A^2, gegeben. Dann können wir alle geometrischen Operationen und Überlegungen auf Rechnungen mit den n-Tupeln $\varphi(x) = (\xi_i) \in \mathbf{R}^n$ zurückführen. Wir erinnern daran, daß $[\mathbf{R}^n, +]$ als direktes Produkt von abelschen Gruppen selbst wieder eine abelsche Gruppe ist, vgl. Beispiel 3.2.3. Die Addition erfolgt dabei „komponentenweise“:

$$(\xi_1, \ldots, \xi_n) + (\eta_1, \ldots, \eta_n) = (\xi_1 + \eta_1, \ldots, \xi_n + \eta_n) \,. \tag{2}$$

Wir können, da wir das Koordinatensystem festhalten, die Ebene direkt mit $\mathbf{R}^2$ identifizieren, indem wir $x = \varphi(x) = (\xi_1, \xi_2)$ setzen. Weil die Gruppe $\mathbf{R}^2$ abelsch ist, ist jede Rechtstranslation auch eine Linkstranslation (vgl. § 1.4), und wir sprechen einfach von den Translationen der Gruppe. Somit wirkt $\mathbf{R}^2$ über $A^2 = \mathbf{R}^2$ einfach transitiv als Gruppe der durch die Operation + definierten Translationen, und diese Translationen stimmen mit den in der Geometrie auch als Parallelverschiebungen bezeichneten Transformationen der Ebene überein.

Die Translationen nennt man häufig auch „Vektoren des A^n“. Statt „Ausführen der Translation“ sagt man dann „Abtragen des Vektors“. Eine Translation veranschaulicht man sich durch einen von x nach $t(x)$ gezogenen Pfeil. Der Hintereinanderausführung der Translationen entspricht die „geometrische Addition der Vektoren“, die natürlich wieder abelsch ist. Mit diesen Bezeichnungen können wir das bisher Festgestellte folgendermaßen zusammenfassen:

Die Vektoren bilden eine abelsche Gruppe, die einfach transitiv auf dem A^n ($n = 2$) wirkt.

Für viele geometrische Anwendungen benötigt man noch die *Multiplikation eines Vektors mit einer Zahl.* Zum Beispiel definiert man eine Dehnung d_λ um den Faktor $\lambda \neq 0$ mit dem Fixpunkt o, dem „Dehnungszentrum“, mit Hilfe der Koordinaten folgendermaßen:

$$x = (\xi_1, \xi_2) \in A^2 \mapsto x' = d_\lambda(x) := (\xi_1 \lambda, \xi_2 \lambda) \in A^2.$$

Hierbei geht jede Strecke (a, b) in eine parallele Strecke (a', b') über und wird dabei um den Faktor λ gedehnt. Es ist nun zweckmäßig, die Multiplikation der einzelnen Koordinaten mit λ als Multiplikation des Vektors (ξ_i) mit der Zahl λ aufzufassen, was auf folgende Definition führt:

$$((\xi_i), \lambda) \in \mathbf{R}^n \times \mathbf{R} \mapsto (\xi_i)\,\lambda := (\xi_i \lambda) \in \mathbf{R}^n \tag{3}$$

(*komponentenweise Multiplikation eines n-Tupelvektors mit einer Zahl*). Man prüft leicht nach, daß für sie die folgenden Rechenregeln gelten:

$$((\xi_i) + (\eta_i))\,\lambda = (\xi_i)\,\lambda + (\eta_i)\,\lambda\,, \tag{4}$$

$$(\xi_i)\,(\lambda + \mu) \quad = (\xi_i)\,\lambda + (\xi_i)\,\mu\,, \tag{5}$$

$$((\xi_i)\,\lambda)\,\mu \quad = (\xi_i)\,(\lambda \cdot \mu)\,, \tag{6}$$

$$(\xi_i)\,1 \quad = (\xi_i) \tag{7}$$

für alle $(\xi_i), (\eta_i) \in \mathbf{R}^n$ und $\lambda, \mu \in \mathbf{R}$. Zusammenfassend können wir feststellen:

Im Raum $\mathbf{R}^n$ *der n-Tupelvektoren* (ξ_i) *ist eine komponentenweise Addition + durch* (2) *erklärt, bezüglich der* $[\mathbf{R}^n, +]$ (*als direktes Produkt abelscher Gruppen*) *eine abelsche Gruppe ist. Bei komponentenweiser Definition der Multiplikation eines n-Tupelvektors* $(\xi_i) \in \mathbf{R}^n$ *mit einer Zahl* $\lambda \in \mathbf{R}$ *nach* (3) *gelten die Rechenregeln* (4) *bis* (7).

Übung 1. Es sei D ein assoziativer Ring mit Einselement und D^n der Raum der n-Tupel (ξ_i), $\xi_i \in D$, $i = 1, ..., n$. Man zeige: a) Wird die Addition in D^n durch (2) definiert, so wird $[D^n, +]$ eine abelsche Gruppe. — b) Definiert man die Multiplikation mit Elementen $\lambda \in D$ analog (3), so sind die Regeln (4) bis (7) erfüllt.

Übung 2. Unter den Voraussetzungen von Übung 1 bezeichne D^* die multiplikative Gruppe von D. Wir definieren für $\lambda \in D^*$ die Dehnungen $r_\lambda: D^n \to D^n$ durch $r_\lambda(\xi_i) := (\xi_i)\,\lambda^{-1}$. a) Man beweise: Die Zuordnung $\lambda \in D^* \mapsto r_\lambda \in S(D^n)$ definiert für $n \geqq 1$ eine effektive Transformationsgruppe $[D^*, D^n]$ (vgl. Definition 1.4.2). — b) Weil $0 = (0, ..., 0) \in D^n$ Fixpunkt für alle r_λ ist, gilt $D^*(0) = \{0\}$. Folglich ist auch $[D^*, D^n \setminus \{0\}]$ eine Transformationsgruppe. Man beweise: Ist D ein Integritätsbereich, so wirkt D^* frei über $D^n \setminus \{0\}$. Schließlich gebe man ein Beispiel dafür an, daß D^* nicht frei über $D^n \setminus \{0\}$ wirkt.

§ 2. Vektorräume

In diesem Paragraphen wollen wir nun die in § 1 in einem anschaulichen Spezialfall beschriebene Vektoralgebra wesentlich verallgemeinern und vor allem durch ein Axiomensystem beschreiben. Wie die unten angeführten Beispiele zeigen, erhält sie dadurch einen bedeutend erweiterten Anwendungsbereich, der so geometrisch-anschaulichen Betrachtungen zugänglich wird. Im nächsten Paragraphen werden wir dann mit Hilfe des Vektorbegriffes die affine Geometrie begründen.

Definition 1. Ein Tripel $[V, +, K]$ heißt ein *Vektorraum über dem Körper* K wenn die folgenden Eigenschaften erfüllt sind:

(V 1) Das Paar $[V, +]$ ist eine abelsche Gruppe (Definition 1.1.6);

(V 2) K ist ein Körper (vgl. § 2.2), und es ist eine Operation

$$(\mathfrak{x}, \lambda) \in \boldsymbol{V} \times K \mapsto \mathfrak{x}\lambda \in \boldsymbol{V} \tag{1}$$

gegeben, die den folgenden Bedingungen genügt:

$$(\mathfrak{x}+\mathfrak{y})\,\lambda = \mathfrak{x}\lambda + \mathfrak{y}\lambda\,, \tag{2}$$

$$\mathfrak{x}\,(\lambda+\mu) = \mathfrak{x}\lambda + \mathfrak{x}\mu\,, \tag{3}$$

$$(\mathfrak{x}\lambda)\,\mu \;\; = \mathfrak{x}(\lambda\mu)\,, \tag{4}$$

$$\mathfrak{x}\,1 \;\; = \mathfrak{x} \tag{5}$$

für alle $\mathfrak{x}, \mathfrak{y} \in \boldsymbol{V}$ und $\lambda, \mu \in K$.

Wir bemerken, daß wir in dieser Definition und im folgenden das Einselement des gerade betrachteten Körpers K mit dem Symbol 1 bezeichnen; Verwechslungen mit der natürlichen Zahl 1 sind nicht zu befürchten.

Beispiel 1. Es sei K ein beliebiger Körper. Dann ist der Raum der n-Tupel $(\xi_i) \in K^n$ als n-fache direkte Summe

$$\underbrace{K \oplus K \oplus \ldots \oplus K}_{n\text{-mal}} \tag{6}$$

der abelschen additiven Gruppe $[K, +]$ des Körpers wieder eine abelsche Gruppe. Definiert man analog zu (1.3) (mit K anstatt $\mathbf{R}$) eine Operation (1), so gelten wieder die Regeln (1.4) bis (1.7), die hier mit (2) bis (5) übereinstimmen. Daher ist K^n ein Vektorraum über K, den wir den *n-Tupel-Raum über K* nennen.

Beispiel 2. Ist $\boldsymbol{V} = \{\mathfrak{o}\}$ die nur aus dem Nullelement bestehende triviale abelsche Gruppe, so erfüllt $\mathfrak{o}\lambda = \mathfrak{o}$ die Bedingungen (2) bis (5), und wir erhalten den *trivialen Vektorraum* K^0 über K, der nur aus dem Nullvektor $\mathfrak{o}$ besteht. Somit ist K^n für alle natürlichen Zahlen $n \geqq 0$ definiert.

Beispiel 3. Als Spezialfall von Beispiel 1 haben wir: *Jeder Körper $K = K^1$ kann als Vektorraum über sich selbst betrachtet werden.*

Beispiel 4. Es sei $M \neq \emptyset$ eine nichtleere Menge, K ein Körper und K^M die Menge aller Abbildungen von M in K (vgl. Beispiel 0.2.11). Definieren wir die Addition zweier Abbildungen $f, g \in K^M$ bzw. die Multiplikation von $f \in K^M$ mit einem $\lambda \in K$ wie üblich argumentweise durch

$$(f+g)\,(x) := f(x) + g(x)\,, \tag{7}$$

$$(f\lambda)\,(x) := f(x)\,\lambda \tag{8}$$

für alle $x \in M$, so wird $[K^M, +, K]$ ein Vektorraum über K. Beachtet man, daß ein n-Tupel $(\xi_i) \in K^n$ als Abbildung $i \mapsto \xi_i$ der Menge $\{1, 2, \ldots, n\}$ in K aufgefaßt werden kann und daß hierbei die Operationen (7) und (8) mit den entsprechenden Operationen für n-Tupel übereinstimmen, so erkennt man, daß die n-Tupel-Vektorräume Spezialfälle von Beispiel 4 sind.

Beispiel 5. Nimmt man als $[V,+]$ die additive Gruppe des Polynomringes $K[x]$ über dem Körper K und als Operation von K über $K[x]$ die Multiplikation

$$(\sum a_\nu x^\nu, \lambda) \in K[x] \times K \to \sum a_\nu \lambda x^\nu \in K[x], \tag{9}$$

so wird $K[x]$ ein Vektorraum über K.

Für die Addition $+$ eines Vektorraumes gelten natürlich alle Rechenregeln einer abelschen Gruppe. Aus den Distributivgesetzen (2), (3) erhält man leicht durch vollständige Induktion

$$\left(\sum_{i=1}^{n} \mathfrak{x}_i\right) \lambda = \sum_{i=1}^{n} (\mathfrak{x}_i \lambda), \tag{10}$$

$$\mathfrak{x} \sum_{i=1}^{n} \lambda_i = \sum_{i=1}^{n} (\mathfrak{x} \lambda_i). \tag{11}$$

Satz 1. *Ist* $[V,+,K]$ *ein Vektorraum,* $\mathfrak{x} \in V, \lambda \in K$, *so gilt* $\mathfrak{x}\lambda = \mathfrak{o}$ *genau dann, wenn* $\mathfrak{x} = \mathfrak{o}$ *oder* $\lambda = 0$ *ist.*

Beweis. Für beliebige $\mathfrak{x} \in V$ und $\lambda \in K$ gilt $\mathfrak{x}\lambda = (\mathfrak{x} + \mathfrak{o})\lambda = \mathfrak{x}\lambda + \mathfrak{o}\lambda$ nach (2); durch Subtraktion von $\mathfrak{x}\lambda$ folgt $\mathfrak{o}\lambda = \mathfrak{o}$. Analog beweist man aus (3) $\mathfrak{x}0 = \mathfrak{o}$. Ist umgekehrt $\mathfrak{x}\lambda = \mathfrak{o}$ und $\lambda \neq 0$, so folgt nach dem eben Bewiesenen unter Anwendung von (4) und (5) $\mathfrak{o} = \mathfrak{o}\lambda^{-1} = (\mathfrak{x}\lambda)\lambda^{-1} = \mathfrak{x}\,1 = \mathfrak{x}$, also $\mathfrak{x} = \mathfrak{o}$. □

Definition 2. Eine Teilmenge W des Vektorraumes V heißt ein *Unterraum von* V, wenn W eine Untergruppe von $[V,+]$ ist und mit $\mathfrak{x} \in W$ und $\lambda \in K$ stets $\mathfrak{x}\lambda \in W$ gilt. Ein Unterraum W ist also eine in bezug auf die Vektoroperationen abgeschlossene, nicht leere Teilmenge; W ist natürlich selbst wieder ein Vektorraum über K. Man beweist leicht

Satz 2. Ist $(W_\iota)_{\iota \in I}$ *eine Familie von Unterräumen des Vektorraumes* V, *so ist auch der Durchschnitt* $\bigcap_{\iota \in I} W_\iota$ *ein Unterraum von* V. □

Der *triviale Unterraum* $\{\mathfrak{o}\}$ besteht nur aus dem Nullvektor. Jeder Vektorraum V ist natürlich Unterraum von sich. Betrachten wir das Beispiel 4 für den Fall $K = \mathbf{R}$ oder $\mathbf{C}$ und M etwa ein Intervall von $\mathbf{R}$, so folgt aus elementaren Sätzen der Analysis, daß die Menge der stetigen (bzw. differenzierbaren) Funktionen ein Unterraum des Vektorraumes aller Funktionen auf dem Intervall M ist. Die Menge der Polynome vom Grad $\leqq n$ ist ein Unterraum des Vektorraumes aller Polynome über K (Beispiel 5).

Definition 3. Es sei M eine beliebige Teilmenge des Vektorraumes V. Unter der *linearen Hülle* $\mathfrak{L}(M)$ *von* M verstehen wir den Durchschnitt des Systems aller der Unterräume $W \subseteqq V$, die M enthalten:

$$\mathfrak{L}(M) := \bigcap_{\substack{M \subseteqq W \\ W \text{ Unterraum}}} W. \tag{12}$$

Satz 3. *Die lineare Hülle* $\mathfrak{L}(M)$ *von* M *ist der kleinste Unterraum von* V, *der* M *enthält. Die Zuordnung* $M \in \mathfrak{P}(V) \mapsto \mathfrak{L}(M) \in \mathfrak{P}(V)$ *ist ein Hüllenoperator, d. h., es*

gelten die Beziehungen

$$M \subseteq \mathfrak{L}(M)\,, \tag{13}$$

$$\textit{aus } M \subseteq N \textit{ folgt } \mathfrak{L}(M) \subseteq \mathfrak{L}(N)\,, \tag{14}$$

$$\mathfrak{L}(\mathfrak{L}(M)) = \mathfrak{L}(M)\,. \tag{15}$$

Beweis. Nach Satz 2 ist $\mathfrak{L}(M)$ stets ein Unterraum, und aus der Definition 3 ergibt sich sofort (13). Bezeichnet $\mathfrak{W}(M)$ das System aller Unterräume von $\boldsymbol{V}$, die M enthalten, so gilt offenbar: Aus $M \subseteq N$ folgt $\mathfrak{W}(M) \supseteq \mathfrak{W}(N)$, und hieraus ergibt sich (14). Wegen (13) gilt $\mathfrak{L}(M) \subseteq \mathfrak{L}(\mathfrak{L}(M))$, und weil $\mathfrak{L}(M)$ selbst ein Unterraum ist, gilt $\mathfrak{L}(M) \in \mathfrak{W}(\mathfrak{L}(M))$; aus Definition 3 erhält man daher

$$\mathfrak{L}(\mathfrak{L}(M)) = \bigcap_{\boldsymbol{W} \in \mathfrak{W}(\mathfrak{L}(M))} \boldsymbol{W} \subseteq \mathfrak{L}(M)\,.$$

Aus den letzten beiden Relationen ergibt sich (15). Ist $\boldsymbol{W}$ irgendein Unterraum, der M enthält, d. h. $\boldsymbol{W} \in \mathfrak{W}(M)$, so gilt natürlich $\mathfrak{L}(M) \subseteq \boldsymbol{W}$, da $\mathfrak{L}(M)$ der Durchschnitt aller derartigen $\boldsymbol{W}$ ist; weil $\mathfrak{L}(M)$ selbst ein Unterraum ist, ist also $\mathfrak{L}(M)$ der kleinste Unterraum, der M enthält. □

Folgerung 1. *Eine Teilmenge $M \subseteq \boldsymbol{V}$ ist ein Unterraum genau dann, wenn $M = \mathfrak{L}(M)$ gilt.* □

Wir wollen nun die lineare Hülle mit Hilfe der Linearkombinationen beschreiben. Es sei $M \subseteq \boldsymbol{V}$ eine beliebige Menge von Vektoren. Ein Vektor $\mathfrak{x}$ heißt *Linearkombination aus M*, wenn es endlich viele Elemente $\lambda_i \in K$ und Vektoren $\mathfrak{m}_i \in M$ gibt, so daß

$$\mathfrak{x} = \sum_{i=1}^{k} \mathfrak{m}_i \lambda_i \tag{16}$$

gilt. Benutzen wir die Menge M als Indexmenge und betrachten nur die Familien $(\lambda_\mathfrak{m})_{\mathfrak{m} \in M} \in K^M$, für die alle bis auf endlich viele $\lambda_\mathfrak{m}$ gleich 0 sind, so können wir jede Linearkombination aus M auch in Gestalt einer *formal unendlichen Summe*

$$\mathfrak{x} = \sum_{\mathfrak{m} \in M} \mathfrak{m} \lambda_\mathfrak{m}\,, \qquad \lambda_\mathfrak{m} = 0 \text{ für fast alle } \mathfrak{m} \in M\,, \tag{17}$$

schreiben. Wir beweisen

Satz 4. *Die lineare Hülle $\mathfrak{L}(M)$ ist gleich der Menge aller Linearkombinationen aus M.*

Beweis. Für den Beweis bezeichne M' die Menge aller Linearkombinationen aus M. Ist $\boldsymbol{W} \subseteq \boldsymbol{V}$ ein Unterraum, der M enthält, so gilt auch $M' \subseteq \boldsymbol{W}$; denn die Vektoroperationen führen nicht aus $\boldsymbol{W}$ hinaus. Speziell gilt $M' \subseteq \mathfrak{L}(M)$. Andererseits gilt $M \subseteq M'$, denn jedes $\mathfrak{x} \in M$ ist Linearkombination $\mathfrak{x} = \mathfrak{x}\,1$ aus M. Folglich gilt $\mathfrak{L}(M) \subseteq \mathfrak{L}(M')$. Wir zeigen nun, daß M' selbst ein Unterraum ist; nach Folgerung 1 gilt dann $\mathfrak{L}(M') = M'$, und unser Satz ist bewiesen. Zunächst einmal gilt $M' \neq \emptyset$, denn es ist stets $\mathfrak{o} \in M'$, wie man erkennt, wenn man in (17) alle $\lambda_\mathfrak{m} = 0$ setzt. Ferner gilt: Ist

$$\mathfrak{x} = \sum \mathfrak{m} \lambda_\mathfrak{m} \in M' \quad \text{und} \quad \mathfrak{y} = \sum \mathfrak{m} \mu_\mathfrak{m} \in M',$$

so ist auch

$$\mathfrak{x}+\mathfrak{y}=\sum \mathfrak{m}\,(\lambda_{\mathfrak{m}}+\mu_{\mathfrak{m}})\in M',$$

und mit $\alpha\in K$ ist auch

$$\mathfrak{x}\alpha=\sum \mathfrak{m}(\lambda_{\mathfrak{m}}\alpha)\in M'.$$

Aus dem folgenden Lemma ergibt sich sofort die Behauptung.

Lemma 1. *Es sei V ein Vektorraum über K und $M\subset V$ eine Teilmenge. M ist Unterraum von V dann und nur dann, wenn folgende drei Bedingungen erfüllt sind:*

1⁰. $M\neq\emptyset$.

2⁰. *Mit* $\mathfrak{x},\mathfrak{y}\in M$ *gilt auch* $\mathfrak{x}+\mathfrak{y}\in M$.

3⁰. *Ist* $\mathfrak{x}\in M$ *und* $\alpha\in K$, *so gilt* $\mathfrak{x}\alpha\in M$.

Beweis. Die Notwendigkeit dieser Bedingungen ist offensichtlich. Für die Umkehrung bleibt wegen 3⁰ nur zu zeigen, daß M eine Untergruppe von $[V,+]$ ist. Nach 1⁰ und 2⁰ genügt es hierzu zu beweisen, daß mit $\mathfrak{x}\in M$ auch $-\mathfrak{x}\in M$ gilt. Wegen $\mathfrak{x}+\mathfrak{x}(-1)=\mathfrak{x}\,(1-1)=\mathfrak{x}\,0=\mathfrak{o}$ hat man

$$\mathfrak{x}(-1)=-\mathfrak{x}\,, \tag{18}$$

und die Behauptung resultiert aus 3⁰. □

Wir betrachten nun das System $\mathfrak{U}$ aller Unterräume des Vektorraumes V. Die mengentheoretische Enthaltenseinsrelation $\subseteq$ definiert eine Ordnung in $\mathfrak{U}$, bezüglich der der triviale Unterraum $\mathfrak{o}$ ($=\{\mathfrak{o}\}$; Abkürzung) das *kleinste* und V selbst das *größte Element* ist. Nach Satz 2 ist in $\mathfrak{U}$ eine Operation $\cap$ definiert, die jeder Familie $(\boldsymbol{W}_i)_{i\in I}$, $\boldsymbol{W}_i\in\mathfrak{U}$, den *Durchschnitt* $\bigcap\limits_{i\in I}\boldsymbol{W}_i\in\mathfrak{U}$ zuordnet; dieses ist nach der bekannten Durchschnittseigenschaft das *eindeutig bestimmte größte Element aus* $\mathfrak{U}$, *das kleiner oder gleich allen Elementen $\boldsymbol{W}_i$ der Familie* ist. Wie man sich leicht an Beispielen, etwa in K^n, klarmacht, ist die Vereinigung zweier Unterräume im allgemeinen kein Unterraum. Mit Hilfe der linearen Hülle kann man sich jedoch ein Analogon für die Vereinigung verschaffen, was in der folgenden Definition geschieht:

Definition 4. Es sei V ein Vektorraum und $(\boldsymbol{W}_i)_{i\in I}$ eine Familie von Unterräumen $\boldsymbol{W}_i\subset V$. Unter der *Summe der Familie* $(\boldsymbol{W}_i)_{i\in I}$ versteht man den Unterraum

$$\sum_{i\in I}\boldsymbol{W}_i:=\mathfrak{L}\Big(\bigcup_{i\in I}\boldsymbol{W}_i\Big)\,. \tag{19}$$

Nach Satz 3 ist $\sum\limits_{i\in I}\boldsymbol{W}_i$ *der kleinste Unterraum, der alle Unterräume der Familie* $(\boldsymbol{W}_i)_{i\in I}$ *enthält*. In Analogie zum Verband der Untergruppen einer Gruppe G (vgl. § 1.2) kann man das über $\mathfrak{U}$ Bewiesene auch in dem folgenden Satz zusammenfassen:

Satz 5. *Das System $\mathfrak{U}$ der Unterräume eines Vektorraumes V ist bezüglich der Ordnung $\subseteq$ ein vollständiger Verband.* □

Übung 1. Es sei V ein Vektorraum über K und $M \subset V$. Man beweise

$$-\sum_{\mathfrak{m}\in M} \mathfrak{m}\lambda_{\mathfrak{m}} = \sum_{\mathfrak{m}\in M} \mathfrak{m}\,(-\lambda_{\mathfrak{m}})\,, \tag{20}$$

$$\sum_{\mathfrak{m}\in M} \mathfrak{m}\lambda_{\mathfrak{m}} + \sum_{\mathfrak{m}\in M} \mathfrak{m}\mu_{\mathfrak{m}} = \sum_{\mathfrak{m}\in M} \mathfrak{m}\,(\lambda_{\mathfrak{m}}+\mu_{\mathfrak{m}})\,, \tag{21}$$

$$k\left(\sum_{\mathfrak{m}\in M} \mathfrak{m}\lambda_{\mathfrak{m}}\right)\alpha = \sum_{\mathfrak{m}\in M} \mathfrak{m}(k\lambda_{\mathfrak{m}}\alpha), \qquad \alpha\in K, \qquad k\in \mathbf{Z}\,. \tag{22}$$

(Man gehe auf (16) zurück und wende vollständige Induktion an.)

Übung 2. Es sei M eine beliebige Menge, $M \neq \emptyset$, und K ein Körper. Man beweise, daß die folgenden Teilmengen Unterräume von K^M sind:

a) $\boldsymbol{W} := \{(\lambda_i)_{i\in M} \mid (\lambda_i)\in K^M$ und $\lambda_i = 0$ für fast alle $i \in M\}$;

b) für $N \subset M$ sei $\boldsymbol{W}(N) := \{(\lambda_i) \mid (\lambda_i)\in K^M$ und $\lambda_i = 0$ für alle $i \in N\}$.

Übung 3. Wir betrachten den Polynomring $K[x]$ über dem Körper K. Es sei $g \in K[x]$ und $(g) := \{h \mid h \in K[x]$ und g teilt $h\}$. Man beweise, daß (g) ein Unterraum des Vektorraumes $K[x]$ ist; (g) ist auch ein Unterring ohne Einselement. Gibt es auch Unterringe z. B. von $\mathbf{R}[x]$, die keine Unterräume sind?

Übung 4. Es sei $(\boldsymbol{W}_i)_{i\in I}$ eine Familie von Unterräumen $\boldsymbol{W}_i \subset V$. Man beweise: $\sum_{i\in I} \boldsymbol{W}_i$ ist die Menge aller derjenigen $\mathfrak{x} \in V$, die eine Darstellung als formal unendliche Summe $\mathfrak{x} = \sum_{i\in I} \mathfrak{w}_i$, $\mathfrak{w}_i \in \boldsymbol{W}_i$, $\mathfrak{w}_i = \mathfrak{o}$ für fast alle $i \in I$, besitzen; mit anderen Worten, die Definition (19) stimmt mit dem Begriff der Summe der additiven Untergruppen $[\boldsymbol{W}_i, +]$ überein, vgl. § 1.2. Für endlich viele Vektorräume bezeichnet man die Summe oft auch mit

$$\sum_{i=1}^{k} \boldsymbol{W}_i = \boldsymbol{W}_1 + \ldots + \boldsymbol{W}_k\,. \tag{23}$$

Übung 5. Wir betrachten das System $[\mathfrak{U}, +, \cap]$ der Unterräume eines Vektorraumes $\boldsymbol{V}$ mit den Operationen der Addition $+$ und der Durchschnittsbildung $\cap$. Man beweise, daß die Operationen $+, \cap$ assoziativ und kommutativ sind und ein Null- bzw. Einselement besitzen. Nur die neutralen Elemente besitzen ein Inverses. Anhand von Beispielen zeige man, daß keines der beiden denkbaren Distributivgesetze gilt. Man erkennt jedoch sofort

$$(\boldsymbol{W}_0 + \boldsymbol{U}) \cap (\boldsymbol{W}_1 + \boldsymbol{U}) \supseteq (\boldsymbol{W}_0 \cap \boldsymbol{W}_1) + \boldsymbol{U}\,, \tag{24}$$

$$(\boldsymbol{W}_0 \cap \boldsymbol{U}) + (\boldsymbol{W}_1 \cap \boldsymbol{U}) \subseteq (\boldsymbol{W}_0 + \boldsymbol{W}_1) \cap \boldsymbol{U}\,. \tag{25}$$

Übung 6. Es sei $\boldsymbol{V}$ ein Vektorraum, $\boldsymbol{M} \subseteq \boldsymbol{V}$ und $\boldsymbol{N} \subseteq \boldsymbol{V}$. Man beweise: Es gilt $\boldsymbol{N} \subseteq \mathfrak{L}(\boldsymbol{M})$ dann und nur dann, wenn $\mathfrak{L}(\boldsymbol{M}) = \mathfrak{L}(\boldsymbol{M} \cup \boldsymbol{N})$ erfüllt ist. Hieraus folgt: Es ist für Unterräume $\boldsymbol{W}, \boldsymbol{U} \subseteq \boldsymbol{V}$ die Gleichung $\boldsymbol{W} + \boldsymbol{U} = \boldsymbol{U}$ genau dann erfüllt, wenn $\boldsymbol{W} \subseteq \boldsymbol{U}$ gilt.

Übung 7. Man beweise: Ist $\boldsymbol{V}$ ein Vektorraum über K und K ein Erweiterungskörper von L, so ist $[\boldsymbol{V}, +, L]$ mit derselben Addition und der wegen $L \subseteq K$ definierten Multiplikation $(\mathfrak{x}, \lambda) \in \boldsymbol{V} \times L \mapsto \mathfrak{x}\lambda \in \boldsymbol{V}$ ein Vektorraum über L. Speziell ist K ein Vektorraum über L; z. B. ist $\mathbf{C}$ ein Vektorraum über $\mathbf{R}$ und $\mathbf{R}$ ein Vektorraum über $\mathbf{Q}$. Entsteht $[\boldsymbol{V}, +, L]$ auf die beschriebene Weise aus $[\boldsymbol{V}, +, K]$, so sagt man, $[\boldsymbol{V}, +, L]$ werde durch *Einschränkung auf* L aus $[\boldsymbol{V}, +, K]$ gebildet. Ist speziell $K = \mathbf{C}$ und $L = \mathbf{R}$, so heißt $[\boldsymbol{V}, +, \mathbf{R}]$ die *Reellifizierung* von $[\boldsymbol{V}, +, \mathbf{C}]$; die Reellifizierung von $\boldsymbol{V}$ wird mit $r\boldsymbol{V}$ bezeichnet.

§ 3. Axiome der affinen Geometrie

Bei den Überlegungen in § 1 haben wir uns auf gewisse Fakten aus der Elementargeometrie, nämlich die Existenz von Koordinatensystemen, gestützt, die wir bisher nicht streng begründet haben. Für die axiomatische Begründung der Geometrie gibt es zwei methodisch ganz verschiedene Wege, die unter den Bezeichnungen „synthetische" und „analytische" Geometrie bekannt sind. Während man in der synthetischen Geometrie von den geometrischen Grundbegriffen Punkt, Gerade, Ebene ausgeht und deren Schnitt- und Lageeigenschaften axiomatisiert, woraus man dann die „Zahlen" durch eine geometrische Konstruktion einer Skala auf einer Geraden und damit auch die Existenz von Koordinatensystemen herleitet, geht man in der analytischen Geometrie von einem gegebenen Körper K aus, dessen Elemente $\alpha, \beta, \ldots, \zeta \in K$ die Zahlen oder „Skalare" der Geometrie sind. Für die Geometrie des Anschauungsraumes ist für K der Körper der reellen Zahlen zu nehmen; um jedoch die aus der geometrischen Anschauung gewonnenen Erkenntnisse auch in mehr abstrakte Bereiche der Algebra und Analysis zu übertragen, ist es zweckmäßig, von einem beliebigen Körper K auszugehen und sich nicht auf das Dreidimensionale zu beschränken. Wir gehen hier den analytischen Weg (der besser der „algebraische" heißen sollte; jedoch ist die „algebraische" Geometrie eine zwar verwandte, jedoch viel tiefer liegende und andere mathematische Disziplin), der kürzer ist und schneller zu den Anwendungen hinführt. Entsprechend den lediglich der Motivierung dienenden Überlegungen von § 1 gehen wir dabei von den Grundbegriffen *Punkt, Vektor* und *Skalar* aus; die Vektoren sind als Translationen des Punktraumes zu interpretieren, und der Körper der Skalare geht in den Begriff des Vektorraumes ein.

Definition 1. Unter einer *affinen Geometrie* versteht man ein Tripel $[\boldsymbol{A}, \boldsymbol{V}, K]$ von drei Grundmengen, für die die folgenden Axiome erfüllt sind:

(I) In K sind zwei Operationen $+$ und $\cdot$ erklärt, bezüglich derer K ein *Körper* ist (vgl. § 2.2).

(II) $\boldsymbol{V}$ ist ein *Vektorraum über dem Körper* K; dabei mögen die Bezeichnungen und Axiome von Definition 2.1 erfüllt sein.

(III) Das Paar $[\boldsymbol{V}, \boldsymbol{A}]$ ist eine *einfach transitive Transformationsgruppe* (vgl. § 1.4). $\boldsymbol{A}$ heißt *affiner Punktraum*, seine Elemente $a, b, c, \ldots, z \in \boldsymbol{A}$ die *Punkte* der affinen Geometrie.

Im Unterschied zu Definition 1.4.1 ist für die Wirkung von $\boldsymbol{V}$ über $\boldsymbol{A}$ eine abweichende Schreibweise üblich und zweckmäßig, die wir nun erläutern wollen. Da $[\boldsymbol{V}, +]$ abelsch ist, schreiben wir auch die Wirkung additiv, und zwar von rechts. Es ist also eine Abbildung

$$+ : (x, \mathfrak{x}) \in \boldsymbol{A} \times \boldsymbol{V} \mapsto y = x + \mathfrak{x} \in \boldsymbol{A} \tag{1}$$

gegeben, für die nach Definition 1.4.1 gilt:

$$1.\ (x+\mathfrak{a})+\mathfrak{b} = x+(\mathfrak{a}+\mathfrak{b}), \qquad x \in \boldsymbol{A}, \qquad \mathfrak{a}, \mathfrak{b} \in \boldsymbol{V}, \tag{2}$$

$$2.\ x+\mathfrak{o} = x, \qquad x \in \boldsymbol{A}; \tag{3}$$

hier ist $\mathfrak{o} \in \boldsymbol{V}$ der Nullvektor. Die Ausführung der Operation (1) nennt man auch *Abtragen des Vektors* $\mathfrak{x}$ *am Punkt* x. Wegen der einfachen Transitivität (Definition 1.4.5) hat die Wirkung von $\boldsymbol{V}$ über $\boldsymbol{A}$ noch die folgende Eigenschaft:

Zu jedem geordneten Paar $(x, y) \in \boldsymbol{A} \times \boldsymbol{A}$ *gibt es genau einen Vektor* $\mathfrak{x} \in \boldsymbol{V}$, *so daß* $y = x + \mathfrak{x}$ *gilt*; mit anderen Worten: Wir haben eine Abbildung

$$(x, y) \in \boldsymbol{A} \times \boldsymbol{A} \mapsto \mathfrak{x} = \vec{xy} \in \boldsymbol{V} \quad \text{mit} \quad y = x + \vec{xy}\,, \tag{4}$$

die jedem geordneten Paar $(x, y) \in \boldsymbol{A} \times \boldsymbol{A}$ den *Ortsvektor* $\vec{xy}$ *von* x *nach* y zuordnet.

Man beachte, daß durch Definition 1 dem Zeichen + eine dreifache Bedeutung zugeordnet wird. Durch die verschiedenartige Bezeichnung der Elemente der Grundmengen $\boldsymbol{A}$, $\boldsymbol{V}$, K werden Verwechslungen ausgeschlossen. Wie die nachfolgenden Rechenregeln zeigen, ist diese Bezeichnungsweise sehr zweckmäßig.

Für jedes $\mathfrak{a} \in \boldsymbol{V}$ wird durch

$$t_{\mathfrak{a}} : x \in \boldsymbol{A} \mapsto t_{\mathfrak{a}}(x) := x + \mathfrak{a} \in \boldsymbol{A} \tag{5}$$

eine bijektive Abbildung von $\boldsymbol{A}$ auf sich definiert, die die *Translation* $t_{\mathfrak{a}}$ um den Vektor $\mathfrak{a}$ heißt. Aus den Grundeigenschaften einer Transformationsgruppe § 1.4, (1), (2), ergibt sich sofort

$$t_{\mathfrak{a}} \circ t_{\mathfrak{b}} = t_{\mathfrak{a}+\mathfrak{b}}\,, \qquad t_{\mathfrak{o}} = \mathrm{id}_{\boldsymbol{A}}\,, \qquad t_{\mathfrak{a}}^{-1} = t_{-\mathfrak{a}}\,, \tag{6}$$

und wegen der Kommutativität der Addition in $\boldsymbol{V}$ folgt

$$t_{\mathfrak{a}+\mathfrak{b}} = t_{\mathfrak{b}+\mathfrak{a}}\,. \tag{7}$$

Weiter gilt:

$$\textit{Aus } t_{\mathfrak{a}} = \mathrm{id}_{\boldsymbol{A}} \textit{ folgt } \mathfrak{a} = \mathfrak{o}\,, \tag{8}$$

d. h., die Gruppe $\boldsymbol{V}$ der Vektoren wirkt *effektiv* über $\boldsymbol{A}$. Aus $t_{\mathfrak{a}} = \mathrm{id}_{\boldsymbol{A}}$ folgt für ein beliebiges $x \in \boldsymbol{A}$ die Beziehung $x = x + \mathfrak{a}$; wegen (3) und der Eindeutigkeit des Ortsvektors ist $\mathfrak{a} = \vec{xx} = \mathfrak{o}$. Aus (6) und (8) folgt

Satz 1. *Die durch* (5) *definierte Zuordnung* $\mathfrak{a} \mapsto t_{\mathfrak{a}}$ *ist ein Isomorphismus der additiven Gruppe des Vektorraumes* $\boldsymbol{V}$ *auf eine Untergruppe der Gruppe aller Transformationen von* $\boldsymbol{A}$, *die man die Translationsgruppe* $\mathfrak{T}(\boldsymbol{A}) := \{t_{\mathfrak{a}}\}_{\mathfrak{a} \in \boldsymbol{V}}$ *nennt.* □

Bemerkung. $\boldsymbol{V}$ wirkt *frei* über $\boldsymbol{A}$, d. h., wenn eine Translation $t_{\mathfrak{a}}$ einen *Fixpunkt* x_0, $t_{\mathfrak{a}}(x_0) = x_0$, besitzt, ist $\mathfrak{a} = \mathfrak{o}$ (vgl. Definition 1.4.4):

$$y = x + \mathfrak{a} \Leftrightarrow \vec{xy} = \mathfrak{a}\,, \tag{9}$$

$$x = x + \mathfrak{a} \Leftrightarrow \vec{xx} = \mathfrak{a} = \mathfrak{o}\,. \tag{10}$$

Man beweist leicht die folgenden Rechenregeln für die Bildung der Ortsvektoren:

$$\vec{p_1p_2} + \vec{p_2p_3} + \ldots + \vec{p_{k-2}p_{k-1}} + \vec{p_{k-1}p_k} = \vec{p_1p_k}\,, \tag{11}$$

$$\vec{qp} = -\vec{pq}\,, \tag{12}$$

$$\vec{(p+\mathfrak{a})\,(q+\mathfrak{b})} = \vec{pq} + \mathfrak{b} - \mathfrak{a}\,. \tag{13}$$

Aus der einfachen Transitivität von $\boldsymbol{V}$ über $\boldsymbol{A}$ folgt sofort

Satz 2. *Es sei $o \in \boldsymbol{A}$ ein beliebiger, fester Punkt. Dann definiert*

$$\Phi_0 : x \in \boldsymbol{A} \mapsto \Phi_0(x) := \overrightarrow{ox} \in \boldsymbol{V} \tag{14}$$

eine bijektive Abbildung; die Umkehrung von Φ_0 ist

$$\Phi_0^{-1} : \mathfrak{x} \in \boldsymbol{V} \mapsto \Phi_0^{-1}(\mathfrak{x}) = o + \mathfrak{x} \in \boldsymbol{A}. \quad \square \tag{15}$$

Beispiel 1. Satz 2 legt folgendes Beispiel einer affinen Geometrie nahe: Es sei $\boldsymbol{V}$ ein Vektorraum über K. Wir setzen $\boldsymbol{A} = \boldsymbol{V}$ und betrachten das Tripel $[\boldsymbol{V}, \boldsymbol{V}, K]$. Die Axiome (I), (II) der Definition einer affinen Geometrie sind offenbar erfüllt; um (III) zu gewährleisten, definieren wir die Abbildung (1) mittels der Addition in $\boldsymbol{V}$:

$$+ : (\mathfrak{x}, \mathfrak{y}) \in \boldsymbol{A} \times \boldsymbol{V} = \boldsymbol{V} \times \boldsymbol{V} \mapsto \mathfrak{x} + \mathfrak{y} \in \boldsymbol{A} = \boldsymbol{V}. \tag{16}$$

Da die Gleichung $\mathfrak{b} = \mathfrak{a} + \mathfrak{x}$ in $\boldsymbol{V}$ eindeutig lösbar ist – $[\boldsymbol{V}, +]$ ist eine Gruppe –, ist die durch (16) definierte Wirkung von $\boldsymbol{V}$ über sich einfach transitiv. Als Spezialfälle erhalten wir die affinen Geometrien $[K^n, K^n, K]$ für jeden Körper K und alle natürlichen Zahlen $n = 0, 1, \ldots$ Für $K = \mathbf{R}$ haben wir diese Geometrien schon in § 1 betrachtet.

Zum Abschluß dieses Paragraphen wollen wir noch einige geometrische Grundbegriffe behandeln, für die die „Dimension" des affinen Raumes, die wir erst im nächsten Paragraphen einführen werden, nicht wesentlich ist.

Definition 2. Es seien $a \in \boldsymbol{A}$ und $\mathfrak{a} \in \boldsymbol{V}$, $\mathfrak{a} \neq \mathfrak{o}$, feste, beliebige Elemente. Unter der *Geraden $\boldsymbol{H} = \boldsymbol{H}(a, \mathfrak{a})$ durch den Punkt a in Richtung des Vektors $\mathfrak{a}$* verstehen wir die Punktmenge

$$\boldsymbol{H}(a, \mathfrak{a}) := \{x \mid x = a + \mathfrak{a}\tau, \tau \in K\}. \tag{17}$$

Wir erhalten also die Gerade $\boldsymbol{H}(a, \mathfrak{a})$, indem wir den vom Vektor $\mathfrak{a}$ erzeugten Unterraum $\mathfrak{L}(\{\mathfrak{a}\})$ an dem Punkt a antragen. Es gilt

Lemma 1. *Die Abbildung*

$$\tau \in K \mapsto x(\tau) = a + \mathfrak{a}\tau \in \boldsymbol{H} \tag{18}$$

ist eine bijektive Abbildung des Körpers K auf die Gerade $\boldsymbol{H}$.

Beweis. Nach Definition von $\boldsymbol{H}$ ist die Abbildung surjektiv. Aus $x = a + \mathfrak{a}\tau_1 = a + \mathfrak{a}\tau_2$ folgt $\mathfrak{a}\tau_1 = \mathfrak{a}\tau_2 = \overrightarrow{ax}$, also $\mathfrak{a}\tau_2 - \mathfrak{a}\tau_1 = \mathfrak{a}(\tau_2 - \tau_1) = \mathfrak{o}$. Wegen $\mathfrak{a} \neq \mathfrak{o}$ erhalten wir aus Satz 2.1 $\tau_2 = \tau_1$, und somit ist (18) auch injektiv. $\square$

Die Abbildung (18) nennt man eine *Parameterdarstellung* der Geraden $\boldsymbol{H}$ mit dem *affinen Parameter* $\tau \in K$; denkt man sich an jeden Punkt $x \in \boldsymbol{H}$ seinen Parameter angeschrieben, so entsteht die *affine Skala* auf $\boldsymbol{H}$ mit dem *Nullpunkt* $a = x(0)$ und dem *Einheitspunkt* $a + \mathfrak{a} = x(1)$.

Satz 3. *Durch zwei verschiedene Punkte $a_0, a_1 \in \boldsymbol{A}$ geht genau eine Gerade, nämlich*

$$\boldsymbol{H}(a_0, a_1) := \boldsymbol{H}(a_0, \overrightarrow{a_0 a_1}). \tag{19}$$

Beweis. Wählen wir auf der Geraden (19) den affinen Parameter entsprechend (18), so werden a_0, a_1 Null- bzw. Einheitspunkt der affinen Skala auf $\boldsymbol{H}$ und liegen daher auf $\boldsymbol{H}$, womit die Existenz bewiesen ist. Es sei nun $\boldsymbol{H}_0=\boldsymbol{H}(b, \mathfrak{b})$ irgendeine Gerade mit $a_i \in \boldsymbol{H}_0$, $i=0, 1$, und $\boldsymbol{H}$ die durch (19) definierte Gerade. Wir zeigen zuerst $\boldsymbol{H} \subseteq \boldsymbol{H}_0$. Wegen $a_i \in \boldsymbol{H}_0$ gibt es Elemente $\alpha_i \in K$, so daß $a_i=b+\mathfrak{b}\alpha_i$ gilt. Hieraus folgt $\overrightarrow{a_0a_1}=\mathfrak{b}(\alpha_1-\alpha_0)=\mathfrak{b}\gamma$ mit $\gamma=\alpha_1-\alpha_0 \neq 0$ wegen $a_0 \neq a_1$. Für beliebiges $x \in \boldsymbol{H}$ gilt $x=a_0+\overrightarrow{a_0a_1}\tau=b+\mathfrak{b}(\alpha_0+\gamma\tau) \in \boldsymbol{H}_0$. Andererseits ist $\mathfrak{b}=\overrightarrow{a_0a_1}\gamma^{-1}$ und daher $b=a_0-\overrightarrow{a_0a_1}\gamma^{-1}\alpha_0 \in \boldsymbol{H}$. Hieraus ergibt sich analog zu dem eben Bewiesenen $\boldsymbol{H}_0 \subseteq \boldsymbol{H}$. □

Aus dem Beweis ersehen wir, daß sich $\boldsymbol{H}$ und $\boldsymbol{H}_0$ als Punktmengen nicht unterscheiden; definieren wir auf ihnen den durch ihre erzeugenden Elemente bestimmten affinen Parameter, so erhalten wir lediglich zwei Parameterdarstellungen derselben Geraden. Allgemein gilt

Satz 4. *Sind τ, σ die dem Punkt $x \in \boldsymbol{H}(a, \mathfrak{a})=\boldsymbol{H}(b, \mathfrak{b})$ bezüglich der durch $a, \mathfrak{a}$ bzw. $b, \mathfrak{b}$ bestimmten affinen Skalen zugeordneten Werte der affinen Parameter:*

$$x=a+\mathfrak{a}\tau=b+\mathfrak{b}\sigma, \qquad \tau, \sigma \in K, \tag{20}$$

so gibt es von $x \in \boldsymbol{H}$ unabhängige Skalare α, $\gamma \in K$ mit

$$\sigma=\gamma\tau+\alpha, \qquad \gamma \neq 0. \tag{21}$$

Dabei ist $\alpha=\sigma(a)$ der Parameterwert von a in der σ-Skala, und $\gamma \neq 0$ ist durch $\mathfrak{a}=\mathfrak{b}\gamma$ bestimmt.

Beweis. Wegen $a \in \boldsymbol{H}$ gibt es nach Lemma 1 genau ein $\alpha \in K$ mit $a=b+\mathfrak{b}\alpha$. Hieraus folgt $\overrightarrow{ab}=-\mathfrak{b}\alpha$. Analog gibt es wegen $a+\mathfrak{a} \in \boldsymbol{H}$ genau ein $\beta \in K$ mit $a+\mathfrak{a}=b+\mathfrak{b}\beta$. Somit gilt

$$\mathfrak{a}=\overrightarrow{ab}+\mathfrak{b}\beta=\mathfrak{b}(\beta-\alpha)=\mathfrak{b}\gamma$$

mit $\gamma \neq 0$ wegen $\mathfrak{a} \neq \mathfrak{o}$. Setzen wir die gefundenen Ausdrücke für a und $\mathfrak{a}$ in die erste der Gleichungen (20) ein, so folgt $x=b+\mathfrak{b}(\gamma\tau+\alpha)=b+\mathfrak{b}\sigma$, und nach Lemma 1 gilt (21). Die durch (21) gegebene Zuordnung zwischen zwei affinen Skalen ist bijektiv; man nennt sie eine *affine Parametertransformation*. □

Drei Punkte $x, y, z \in \boldsymbol{A}$ heißen *kollinear*, wenn es eine Gerade $\boldsymbol{H} \subset \boldsymbol{A}$ gibt mit $\{x, y, z\} \subseteq \boldsymbol{H}$. Wenn es in $\boldsymbol{A}$ wenigstens zwei Punkte gibt und je drei Punkte kollinear sind, ist $\boldsymbol{A}$ selbst eine Gerade. Ein geordnetes Paar (a, b) von Punkten heißt eine *Strecke*, ein $(k+1)$-Tupel $(p_0, p_1, \ldots, p_k)$ heißt ein *Streckenzug* mit den *Ecken* p_i und den *Endpunkten* p_0, p_k; die Strecken (p_i, p_{i+1}), $i=0, 1, \ldots, k-1$, sind die Strecken des Streckenzuges und die Geraden $\boldsymbol{H}(p_i, p_{i+1})$ seine *Seiten*; dabei haben wir stillschweigend vorausgesetzt, daß $p_i \neq p_{i+1}$ gilt; eine Strecke, deren beide Punkte zusammenfallen, heißt auch *ausgeartet*. Ein Streckenzug mit $p_0=p_k$ heißt ein k-Eck oder ein *Polygon*.

Bemerkung. Im Fall $K=\mathbf{R}$ ist neben den Körperoperationen noch eine Ordnung $\leqq$ gegeben. In diesem Fall definiert man eine Strecke (a, b) meist als die Menge $\{x \mid x=a+\overrightarrow{ab}\tau, 0 \leqq \tau \leqq 1\}$ derjenigen Punkte x der Geraden $\boldsymbol{H}(a, b)$, die *zwischen* a

und b liegen. Bei einem beliebigen Körper, z. B. im Fall $K=\mathbf{C}$, wäre eine derartige Definition sinnlos. Auch Skizzen sind streng genommen nur auf den Fall $K=\mathbf{R}$ anwendbar; sie können bei beliebigem K nur als Schemata angesehen werden.

Definition 3. Zwei Punktmengen $M, N \subseteq \boldsymbol{A}$ heißen *parallel*, in Zeichen $M \parallel N$, wenn es einen Vektor $\mathfrak{b} \in \boldsymbol{V}$ gibt mit

$$N = t_{\mathfrak{b}}(M) = M + \mathfrak{b} := \{x + \mathfrak{b}\}_{x \in M}\,, \tag{22}$$

wobei die letzte Gleichung nur die anschauliche Schreibweise $M+\mathfrak{b}$ definieren möge. Zwei Streckenzüge $(p_0, p_1, \ldots, p_k)$, $(q_0, q_1, \ldots, q_k)$ heißen *parallel*, wenn es ein $\mathfrak{b} \in \boldsymbol{V}$ gibt mit $q_i = p_i + \mathfrak{b}$ für $i = 0, 1, \ldots, k$. Aus Axiom (III) folgt sofort, daß die Relation $\parallel$ eine Äquivalenzrelation ist.

Definition 4. In $\boldsymbol{A}$ gebe es wenigstens drei nicht kollineare Punkte, d. h., $\boldsymbol{A}$ enthalte wenigstens zwei Geraden. Eine Abbildung $f\colon \boldsymbol{A} \to \boldsymbol{A}$ heißt eine *Homothetie*, wenn $f(\boldsymbol{H}) \parallel \boldsymbol{H}$ für jede Gerade $\boldsymbol{H} \subset \boldsymbol{A}$ gilt.

Ist $\boldsymbol{H}$ eine Gerade und $\boldsymbol{H}' \parallel \boldsymbol{H}$, so ist auch $\boldsymbol{H}'$ eine Gerade; in der Tat, hat $\boldsymbol{H}$ die Parameterdarstellung (18), gilt $\boldsymbol{H}' = t_{\mathfrak{b}}(\boldsymbol{H})$ und $x = a + \mathfrak{a}\tau \in \boldsymbol{H}$, so folgt

$$t_{\mathfrak{b}}(x) = (a + \mathfrak{a}\tau) + \mathfrak{b} = (a + \mathfrak{b}) + \mathfrak{a}\tau = t_{\mathfrak{b}}(a) + \mathfrak{a}\tau \in \boldsymbol{H}(t_{\mathfrak{b}}(a), \mathfrak{a})\,,$$

also $\boldsymbol{H}' = t_{\mathfrak{b}}(\boldsymbol{H}) \subseteq \boldsymbol{H}(t_{\mathfrak{b}}(a), \mathfrak{a})$; analog gilt

$$t_{-\mathfrak{b}}(\boldsymbol{H}(t_{\mathfrak{b}}(a), \mathfrak{a})) \subseteq \boldsymbol{H}(a, \mathfrak{a}) = \boldsymbol{H}\,.$$

Wenden wir hierauf $t_{\mathfrak{b}}$ an, so folgt $\boldsymbol{H}(t_{\mathfrak{b}}(a), \mathfrak{a}) \subseteq t_{\mathfrak{b}}(\boldsymbol{H}) = \boldsymbol{H}'$, also

$$t_{\mathfrak{b}}(\boldsymbol{H}(a, \mathfrak{a})) = \boldsymbol{H}(t_{\mathfrak{b}}(a), \mathfrak{a})\,.$$

Somit führt jede Homothetie Geraden wieder in Geraden über. Wir betrachten außer den Translationen noch die *Dehnungen* $d_{a,\lambda}$ mit dem Fixpunkt $a \in \boldsymbol{A}$ und dem Dehnungsfaktor $\lambda \in K$, $\lambda \neq 0$:

$$d_{a,\lambda}\colon x \in \boldsymbol{A} \mapsto d_{a,\lambda}(x) := a + \vec{ax}\lambda \in \boldsymbol{A}\,. \tag{23}$$

Man zeigt leicht, etwa mit Hilfe des unten bewiesenen Lemmas 2, daß Translationen und Dehnungen Homothetien sind. Wie wir sehen werden, ist umgekehrt jede Homothetie eine Translation oder eine Dehnung.

Lemma 2. *Die Geraden* $\boldsymbol{H} = \boldsymbol{H}(a, \mathfrak{a})$ *und* $\boldsymbol{H}_0 = \boldsymbol{H}(b, \mathfrak{b})$ *sind parallel genau dann, wenn es ein* $\lambda \in K$ *gibt mit* $\mathfrak{a} = \mathfrak{b}\lambda$.

Beweis. Es sei $\mathfrak{c} \in \boldsymbol{V}$ mit $t_{\mathfrak{c}}(\boldsymbol{H}) = \boldsymbol{H}_0$. Die Bilder des Null- und des Einheitspunktes der affinen Skala von $\boldsymbol{H}$ liegen in $\boldsymbol{H}_0$; daher gibt es Elemente $\alpha, \beta \in K$ mit $a + \mathfrak{c} = b + \mathfrak{b}\alpha$ und $a + \mathfrak{a} + \mathfrak{c} = b + \mathfrak{b}\beta$ mit $\alpha \neq \beta$, weil $t_{\mathfrak{c}}$ bijektiv ist. Hieraus folgt $b + \mathfrak{b}\beta = b + \mathfrak{b}\alpha + \mathfrak{a}$, also $\mathfrak{a} = \mathfrak{b}(\beta - \alpha)$. Es sei umgekehrt $\mathfrak{a} = \mathfrak{b}\lambda$. Wir setzen $\mathfrak{c} = \vec{ab}$ und behaupten $t_{\mathfrak{c}}(\boldsymbol{H}) = \boldsymbol{H}_0$. In der Tat gilt für $x \in \boldsymbol{H}$

$$t_{\mathfrak{c}}(x) = a + \mathfrak{a}\tau + \mathfrak{c} = b + \mathfrak{b}\lambda\tau \in \boldsymbol{H}_0\,.$$

Somit ist $t_{\mathfrak{c}}(\boldsymbol{H}) \subseteq \boldsymbol{H}_0$; wegen $\mathfrak{a} \neq \mathfrak{o}$ ist aber auch $\lambda \neq 0$, und daher ist jeder Punkt von $\boldsymbol{H}_0$ Bild eines Punktes von $\boldsymbol{H}$. □

Folgerung 1. *Durch jeden Punkt $b \in \boldsymbol{A}$ geht genau eine zu $\boldsymbol{H} = \boldsymbol{H}(a, \mathfrak{a})$ parallele Gerade, nämlich $\boldsymbol{H}(b, \mathfrak{a})$; zwei zueinander parallele Geraden $\boldsymbol{H}, \boldsymbol{H}_0, \boldsymbol{H} \parallel \boldsymbol{H}_0$, mit $\boldsymbol{H} \cap \boldsymbol{H}_0 \neq \emptyset$ sind gleich.* □

Lemma 3. *Drei Punkte $x, y, z \in \boldsymbol{A}$ sind kollinear genau dann, wenn es zwei Elemente $\alpha, \beta \in K$ gibt mit $\alpha \neq 0$ oder $\beta \neq 0$, so daß*

$$\vec{xy}\alpha + \vec{xz}\beta = \mathfrak{o} \tag{24}$$

gilt.

Beweis. Es seien $x, y, z \in \boldsymbol{H}(a, \mathfrak{a})$ kollinear. Ist etwa $x = z$, so gilt $\vec{xy} \cdot 0 + \vec{xz} \cdot 1 = \mathfrak{o}$, und (24) ist mit $\beta = 1 \neq 0$ erfüllt. Wir können also annehmen, daß alle drei Punkte verschieden sind. Dann gibt es drei verschiedene Elemente $\xi, \eta, \zeta \in K$ mit $x = a + \mathfrak{a}\xi$, $y = a + \mathfrak{a}\eta$, $z = a + \mathfrak{a}\zeta$. Durch eine leichte Rechnung folgt $\vec{xy}\,(\eta - \xi)^{-1} + \vec{xz}\,(\xi - \zeta)^{-1} = \mathfrak{o}$. Ist umgekehrt (24) erfüllt und etwa $\beta \neq 0$, so gilt $\vec{xz} = -\vec{xy}\,\alpha\beta^{-1}$, also $z = x - \vec{xy}\,\alpha\beta^{-1} \in \in \boldsymbol{H}(x, y)$, falls $x \neq y$ ist; der Fall $x = y$ ist trivial. □

Es sei $f: \boldsymbol{A} \to \boldsymbol{A}$ eine Homothetie und $x, y, z \in \boldsymbol{A}$ seien nicht kollinear. Aus der Definition 4 der Homothetien und Lemma 2 folgt die Existenz von drei Skalaren $\lambda, \mu, \nu \in K$ mit

$$\overrightarrow{f(x)\,f(z)} = \vec{xz}\lambda, \qquad \overrightarrow{f(y)\,f(z)} = \vec{yz}\mu, \qquad \overrightarrow{f(x)\,f(y)} = \vec{xy}\nu\,. \tag{25}$$

Wegen $\overrightarrow{f(x)\,f(z)} = \overrightarrow{f(x)\,f(y)} + \overrightarrow{f(y)\,f(z)}$ erhalten wir

$$\vec{xz}\lambda = \vec{xy}\nu + \vec{yz}\mu = (\vec{xy} + \vec{yz})\,\lambda\,.$$

Hieraus folgt $\vec{xy}\,(\lambda - \nu) + \vec{yz}\,(\lambda - \mu) = \mathfrak{o}$. Da die Punkte x, y, z nicht kollinear sind, muß nach Lemma 3 in (25) $\lambda = \mu = \nu$ gelten. Wenn andererseits $x, y, z \in \boldsymbol{H}$ kollinear sind, wählen wir in $\boldsymbol{A}$ einen Punkt a mit $a \notin \boldsymbol{H}$ und betrachten die nicht kollinearen Tripel (x, y, a), (a, y, z). Da in beiden Tripeln die Punkte a, y vorkommen, müssen die „Dehnungsfaktoren" beider Tripel übereinstimmen. Wir bemerken noch, daß der gemeinsame Dehnungsfaktor $\lambda = \mu = \nu$ von (25) von 0 verschieden sein muß; sonst würde $f(\boldsymbol{A})$ in einen Punkt ausarten, und das Bild keiner Geraden könnte eine Gerade sein. Damit ist bewiesen:

Lemma 4. *Im affinen Raum $\boldsymbol{A}$ mögen drei nicht kollineare Punkte existieren. Dann gehört zu jeder Homothetie $f: \boldsymbol{A} \to \boldsymbol{A}$ ein eindeutig bestimmter Dehnungsfaktor $\lambda \neq 0$, $\lambda \in K$, so daß für $x, y \in \boldsymbol{A}$ stets*

$$\overrightarrow{f(x)\,f(y)} = \vec{xy}\lambda \tag{26}$$

gilt. □

Folgerung 2. *Eine Homothetie $f: \boldsymbol{A} \to \boldsymbol{A}$ ist durch Angabe ihres Dehnungsfaktors $\lambda \neq 0$, $\lambda \in K$, und des Bildes $f(a)$ eines einzigen Punktes $a \in \boldsymbol{A}$ eindeutig bestimmt; nach (26) gilt dann nämlich für beliebiges $x \in \boldsymbol{A}$*

$$f(x) = f(a) + \vec{ax}\lambda\,. \quad \square \tag{27}$$

Folgerung 3. *Die Homothetien sind bijektiv; sie bilden bezüglich der Verknüpfung $\circ$ von Abbildungen eine Gruppe von Transformationen von $\boldsymbol{A}$.*

Beweis. Setzen wir in (27) $y=f(x)$, $b=f(a)$, so erhalten wir für die inverse Abbildung f^{-1}

$$f^{-1}(y)=x=a+\vec{by}\lambda^{-1}, \qquad a=f^{-1}(b)\,. \tag{28}$$

Diese Formel hat dieselbe Gestalt wie (27); es genügt also zu zeigen, daß jede Zuordnung $f: \boldsymbol{A}\to\boldsymbol{A}$ der Form (27) mit $\lambda\neq 0$ eine Homothetie ist. In der Tat gilt

$$f=t_{\vec{ab}}\circ d_{a,\lambda}\,, \qquad f^{-1}=t_{-\vec{ab}}\circ d_{b,\lambda^{-1}}\,, \tag{29}$$

und diese Abbildungen sind als Verknüpfung einer Dehnung und einer Translation Homothetien. Aus Definition 4 erhält man nun unmittelbar die Gruppeneigenschaft. □

Die Beziehung (29) zeigt, daß man jede Homothetie als Verknüpfung einer Dehnung und einer Translation darstellen kann; um unser Ziel zu erreichen, fragen wir nach den Fixpunkten c, $f(c)=c$, der Homothetie f. Es sei zunächst $\lambda=1$. Dann gilt nach (27)

$$f(x)=b+\vec{ax}=a+\vec{ab}+\vec{ax}=x+\vec{ab}=t_{\vec{ab}}(x)\,,$$

d. h., *f ist eine Translation.* Wenn diese einen Fixpunkt hat, ist sie nach (10) die Identität. Es sei nun $\lambda\neq 1$. Aus

$$\begin{aligned} c=f(c)=b+\vec{ac}\lambda &\Leftrightarrow \vec{ac}=\vec{ab}+\vec{ac}\lambda \\ &\Leftrightarrow \vec{ac}\,(1-\lambda)=\vec{ab} \Leftrightarrow c=a+\vec{ab}\,(1-\lambda)^{-1} \end{aligned}$$

folgt, daß f in diesem Fall genau einen Fixpunkt c besitzt. Wenden wir Folgerung 2 für $a=c$ an, so erhalten wir $f(x)=c+\vec{cx}\lambda$, d. h. $f=d_{c,\lambda}$. Damit ist der folgende Satz bewiesen:

Satz 5. *In $\boldsymbol{A}$ mögen drei nicht kollineare Punkte existieren. Dann ist jede Homothetie von $\boldsymbol{A}$ eine Translation oder eine Dehnung; sie ist eine Translation genau dann, wenn ihr Dehnungsfaktor gleich* 1 *ist.* □

Zwei nicht ausgeartete Strecken (a, b), (a', b') heißen *homothetisch,* wenn es eine Homothetie $f: \boldsymbol{A}\to\boldsymbol{A}$ gibt mit $f(a)=a'$, $f(b)=b'$. In Analogie zu Definition 3 ist auch klar, was man unter *homothetischen Mengen* oder *homothetischen Streckenzügen* zu verstehen hat. Wenn (a, b) zu (a', b') homothetisch ist, müssen die Geraden $\boldsymbol{H}(a, b)$, $\boldsymbol{H}(a', b')$ zueinander parallel sein, und nach Lemma 2 gibt es dann ein $\lambda\in K$, $\lambda\neq 0$, mit $\vec{a'b'}=\vec{ab}\lambda$. Gilt umgekehrt diese Relation, so ist $x\in\boldsymbol{A}\mapsto f(x):=$ $:=a'+\vec{ax}\lambda\in\boldsymbol{A}$ die Definition einer Homothetie, die (a, b) in (a', b') überführt; nach Folgerung 2 ist sie eindeutig bestimmt. Also gilt

Lemma 5. *Zwei nicht ausgeartete Strecken (a, b), (a', b') sind genau dann homothetisch, wenn ein $\lambda\in K$, $\lambda\neq 0$, existiert mit $\vec{a'b'}=\vec{ab}\lambda$.* □

Ist $a\neq b$, so ist der Skalar λ offenbar eindeutig bestimmt. Wir nennen ihn das *Streckenverhältnis der homothetischen Strecken* und schreiben

$$\lambda=(a', b')/(a, b)=\vec{a'b'}/\vec{ab}\,. \tag{30}$$

Man beachte, daß das Streckenverhältnis nur für homothetische Strecken definiert ist; es hat in der affinen Geometrie keinen Sinn, von der „Länge" einer Strecke zu sprechen. Die Gleichung (30) bleibt für $a'=b'$ sinnvoll; dieser Fall wird durch $\lambda=0$ charakterisiert. Ist $\mathfrak{a}\neq\mathfrak{o}$ und $\mathfrak{b}\in\mathfrak{L}(\{\mathfrak{a}\})$, so gibt es einen eindeutig bestimmten Skalar $\lambda\in K$ mit $\mathfrak{b}=\mathfrak{a}\lambda$; man schreibt dann auch $\lambda=\mathfrak{b}/\mathfrak{a}$ und spricht vom *Verhältnis der Vektoren* $\mathfrak{b}$, $\mathfrak{a}$. Mit Hilfe der so erklärten Begriffe können wir den folgenden „*Strahlensatz*" beweisen:

Satz 6. *Es seien* a, x_0, x_1, y_0, $y_1\in\boldsymbol{A}$ *fünf verschiedene Punkte,* $x_1\in\boldsymbol{H}(a, x_0)=\boldsymbol{H}$, $y_1\in\boldsymbol{H}(a, y_0)=\boldsymbol{H}'$, $\boldsymbol{H}\neq\boldsymbol{H}'$. *Dann sind die folgenden drei Aussagen äquivalent:*

a) $\boldsymbol{H}(x_0, y_0)\parallel\boldsymbol{H}(x_1, y_1)$.

b) *Die Strecken* (x_0, y_0), (x_1, y_1) *sind homothetisch, d. h., es gibt ein* $\lambda\in K$ *mit* $\overrightarrow{x_1y_1}=\overrightarrow{x_0y_0}\lambda$.

c) *Es gilt* $(a, x_1)/(a, x_0)=(a, y_1)/(a, y_0)$.

Ist eine dieser Aussagen erfüllt, so gilt

$$(x_1, y_1)/(x_0, y_0)=(a, x_1)/(a, x_0)=(a, y_1)/(a, y_0)=\lambda\,. \tag{31}$$

Beweis. Die Äquivalenz von a) und b) folgt unmittelbar aus Lemma 2 und Lemma 5. Wir beweisen b)⇒c). Wegen $x_1\in\boldsymbol{H}(a, x_0)$, $y_1\in\boldsymbol{H}(a, y_0)$ gibt es $\sigma, \tau\in K$ mit $x_1=a+\overrightarrow{ax_0}\sigma$, $y_1=a+\overrightarrow{ay_0}\tau$, d. h. $\sigma=(a, x_1)/(a, x_0)$, $\tau=(a, y_1)/(a, y_0)$. Aus b) folgt

$$\overrightarrow{x_1y_1}=\overrightarrow{x_0y_0}\lambda=\overrightarrow{x_1a}+\overrightarrow{ay_1}=(\overrightarrow{x_0a}+\overrightarrow{ay_0})\lambda=\overrightarrow{x_0a}\,\sigma+\overrightarrow{ay_0}\tau\,.$$

Also gilt auch $\overrightarrow{ax_0}\,(\sigma-\lambda)=\overrightarrow{ay_0}\,(\tau-\lambda)$. Weil die Geraden $\boldsymbol{H}$, $\boldsymbol{H}'$ nach Voraussetzung verschieden sind, sind die Punkte a, x_0, y_0 nicht kollinear, und nach Lemma 3 muß daher $\lambda=\sigma=\tau$ gelten. Damit ist c) bewiesen und gleichzeitig, daß aus b) die Gleichung (31) folgt. Es bleibt c) ⇒ b) zu zeigen. Nach c) gelten für ein gewisses $\lambda\in K$ die Gleichungen $\overrightarrow{ax_1}=\overrightarrow{ax_0}\lambda$ und $\overrightarrow{ay_1}=\overrightarrow{ay_0}\lambda$. Durch Subtraktion der ersten von der zweiten dieser Gleichungen folgt $\overrightarrow{x_1y_1}=\overrightarrow{x_0y_0}\lambda$, d. h. die Aussage b). □

Übung 1. Ist $a\neq b$, $x\in\boldsymbol{H}(a, b)$, so ist $\tau(x)=(a, x)/(a, b)$ der affine Parameter von $\boldsymbol{H}$ mit $\tau(a)=0$ und $\tau(b)=1$ (Deutung des affinen Parameters als Streckenverhältnis).

Übung 2. Ein Viereck (s, p, q, r, s) heißt *eigentlich*, wenn je drei seiner Eckpunkte nicht kollinear sind; es heißt ein *Parallelogramm*, wenn $\overrightarrow{pq}+\overrightarrow{rs}=\mathfrak{o}$ gilt; die Geraden $\boldsymbol{H}(p, r)$, $\boldsymbol{H}(q, s)$ heißen die *Diagonalen* des eigentlichen Vierecks. Man beweise: a) Das Viereck ist ein Parallelogramm genau dann, wenn $\overrightarrow{qr}+\overrightarrow{sp}=\mathfrak{o}$ gilt. — b) Es sei char $K\neq 2$. Ein eigentliches Viereck ist ein Parallelogramm genau dann, wenn der Schnittpunkt $a:=\boldsymbol{H}(p, r)\cap\boldsymbol{H}(q, s)$ der Diagonalen existiert und die Strecken (p, r), (q, s) halbiert, d. h., wenn die Gleichungen $\overrightarrow{pr}=2\overrightarrow{pa}$ und $\overrightarrow{qs}=2\overrightarrow{qa}$ gelten.

Übung 3. Es sei wieder $[\boldsymbol{A}, \boldsymbol{V}, K]$ eine beliebige affine Geometrie. Man beweise: Eine Abbildung $f\colon\boldsymbol{A}\to\boldsymbol{A}$ ist eine Translation dann und nur dann, wenn $(a, b)\parallel(f(a), f(b))$ für alle Strecken (a, b) von $\boldsymbol{A}$, $a\neq b$, gilt. Jede Translation ist durch das Bild eines einzigen Punktes eindeutig bestimmt.

Übung 4. Es seien $D=(p_1, p_2, p_3)$ und $D'=(q_1, q_2, q_3)$ zwei Dreiecke des affinen Raumes $\boldsymbol{A}$ aus je drei nicht kollinearen Punkten, deren Seiten (p_i, p_j), (q_i, q_j) homothetisch sind für $1\leqq i<j\leqq 3$. Man zeige: Es gibt eine Homothetie $f\colon\boldsymbol{A}\to\boldsymbol{A}$ mit $f(D)=D'$.

Übung 5. Es bezeichne $\mathfrak{H}(A)$ die Gruppe der Homothetien eines affinen Raumes A, in dem drei nicht kollineare Punkte existieren; der Körper K der affinen Geometrie möge wenigstens drei Elemente enthalten. Es sei $o \in A$ ein fester Punkt, und $d_\lambda: A \to A$ bezeichne die Dehnung mit dem Fixpunkt o und dem Faktor $\lambda \in K^*$. Man beweise: a) Die Menge der Dehnungen $\mathfrak{D}_0 := \{d_\lambda\}_{\lambda \in K^*} \subset \mathfrak{H}(A)$ ist eine Untergruppe von $\mathfrak{H}(A)$. — b) Die Menge der Translationen $\mathfrak{T}(A) \subset \mathfrak{H}(A)$ ist ein Normalteiler von $\mathfrak{H}(A)$. — c) Die Gruppe $\mathfrak{H}(A)$ ist ein halbdirektes Produkt $\mathfrak{H}(A) = \mathfrak{T}(A) \cdot \mathfrak{D}_0$ (vgl. Übung 3.2.3). — d) Die Untergruppe $\mathfrak{D}_0$ ist kein Normalteiler von $\mathfrak{H}(A)$. — e) Die Kommutatorgruppe von $\mathfrak{H}(A)$ ist gleich $\mathfrak{T}(A)$ (vgl. Übung 3.1.8). — f) Man bestimme für beliebiges $f \in \mathfrak{H}(A)$ den Zentralisator Z_f von f und zeige, daß das Zentrum $Z_{\mathfrak{H}(A)}$ trivial ist (vgl. Beispiel 1.4.7). — g) Die Gruppen K^*, $\mathfrak{D}_0$ und $\mathfrak{H}(A)/\mathfrak{T}(A)$ sind isomorph (vgl. Satz 3.1.6). — h) Die Transformationsgruppen $[\mathfrak{H}(A), A]$ und $[\mathfrak{H}(A), \mathfrak{H}(A)/\mathfrak{D}_0]$ sind isomorph (vgl. Satz 3.1.7).

§ 4. Lineare Unabhängigkeit. Dimension

Unsere nächste Aufgabe ist es, den Begriff der Dimension, der in § 1 nur anschaulich betrachtet wurde, in die Axiomatik der affinen Geometrie einzufügen. Dazu genügt es, die Dimension eines Vektorraumes zu definieren. Zuerst formulieren wir eine sehr leicht einzusehende Eigenschaft der Vektorräume der n-Tupel K^n:

Lemma 1. *Es sei K^n der Vektorraum der n-Tupel über einem Körper K, $n \in \mathbf{N}_0$. Dann gibt es n Vektoren, nämlich*

$$\mathfrak{e}_i = (0, \ldots, 0, \underset{i}{1}, 0, \ldots, 0) \in K^n, \qquad i = 1, \ldots, n, \tag{1}$$

mit den folgenden Eigenschaften:

1. *Jeder Vektor $\mathfrak{x} = (\xi_i) \in K^n$ besitzt eine Darstellung als Linearkombination der $\mathfrak{e}_i$:*

$$\mathfrak{x} = \sum_{i=1}^{n} \mathfrak{e}_i \xi_i . \tag{2}$$

2. *Ist $\mathfrak{x} = \sum \mathfrak{e}_i \eta_i = \sum \mathfrak{e}_i \xi_i$, so gilt $\xi_i = \eta_i$ für $i = 1, \ldots, n$, d. h., die Koeffizienten ξ_i der Linearkombination sind eindeutig bestimmt.*

Beweis. Nach Beispiel 2.1 und (1.3) gilt

$$\mathfrak{e}_i \xi_i = (0, .., 0, \xi_i, 0, \ldots, 0) . \tag{3}$$

Die Behauptung folgt nun aus dem Additionsgesetz (1.2) in K^n. □

Die Frage nach der Existenz und Eindeutigkeit von Darstellungen der Gestalt (2) in beliebigen Vektorräumen führt uns auf die folgenden Definitionen:

Definition 1. Es sei V ein Vektorraum über K. Die Menge $M \subseteq V$ heißt eine *erzeugende Menge von V*, wenn die lineare Hülle $\mathfrak{L}(M) = V$ ist.

Ist M erzeugende Menge, so ist auch jede größere Menge $M' \supseteq M$ erzeugend.

Definition 2. Eine Teilmenge $M \subseteq V$ heißt *linear unabhängig*, wenn für jedes $\mathfrak{x} \in \mathfrak{L}(M)$ genau eine Darstellung

$$\mathfrak{x} = \sum_{\mathfrak{m} \in M} \mathfrak{m} \xi_{\mathfrak{m}} \tag{4}$$

als formal unendliche Linearkombination aus M existiert; für $\mathfrak{x} \in \mathfrak{L}(M)$ sind also die Koeffizienten $\xi_{\mathfrak{m}}$ eindeutig bestimmt. Offenbar gilt: Ist $M' \subseteq M$ und M linear unabhängig, so ist auch M' linear unabhängig.

Lemma 2. *Eine Menge $M \subset V$ ist linear unabhängig genau dann, wenn der Nullvektor nur trivial aus M linear kombinierbar ist, d. h., wenn aus $\mathfrak{o} = \sum_{\mathfrak{m} \in M} \mathfrak{m}\lambda_{\mathfrak{m}}$ stets $\lambda_{\mathfrak{m}} = 0$ für alle $\mathfrak{m} \in M$ folgt.*

Beweis. Wenn M linear unabhängig ist, besitzt jeder Vektor aus $\mathfrak{L}(M)$ genau eine Darstellung (4); für den Nullvektor muß das also die triviale Darstellung mit $\lambda_{\mathfrak{m}} = 0$ für alle $\mathfrak{m} \in M$ sein. Ist umgekehrt M linear abhängig, so gibt es einen Vektor $\mathfrak{x} \in \mathfrak{L}(M)$, der zwei verschiedene Darstellungen $\mathfrak{x} = \sum \mathfrak{m}\eta_{\mathfrak{m}} = \sum \mathfrak{m}\xi_{\mathfrak{m}}$ besitzt. Da $\eta_{\mathfrak{m}} \neq \xi_{\mathfrak{m}}$ für wenigstens ein $\mathfrak{m} \in M$ gelten muß, ergibt sich durch Subtraktion eine nichttriviale Darstellung des Nullvektors

$$\mathfrak{o} = \sum_{\mathfrak{m} \in M} \mathfrak{m}(\eta_{\mathfrak{m}} - \xi_{\mathfrak{m}}) . \quad \square$$

Beispiel 1. Die Menge $M = \{\mathfrak{e}_i \mid i = 1, \ldots, n\} \subset K^n$ ist nach Lemma 1 eine linear unabhängige erzeugende Menge. Für einen beliebigen Vektorraum V ist die leere Menge stets linear unabhängig. Eine Einermenge $M = \{\mathfrak{m}\}$ ist genau dann linear abhängig, wenn $\mathfrak{m} = \mathfrak{o}$ ist. Nach Lemma 3.3 und Lemma 2 sind die drei Punkte $x, y, z \in A$ genau dann kollinear, wenn die Menge $\{\vec{xy}, \vec{xz}\}$ linear abhängig ist. Nach Lemma 3.2 sind die Geraden $H(a, \mathfrak{a})$, $H(b, \mathfrak{b})$ parallel genau dann, wenn $\{\mathfrak{a}, \mathfrak{b}\}$ linear abhängig ist. Aus Lemma 2 folgt

Folgerung 1. *Eine Menge $M \subseteq V$, die mehr als ein Element enthält, ist genau dann linear abhängig, wenn sich einer der Vektoren $\mathfrak{m} \in M$ durch die anderen linear kombinieren läßt.* $\square$

Satz 1. *Es sei V ein Vektorraum über K, $M \subseteq V$. Die Menge M ist eine maximale linear unabhängige Menge genau dann, wenn M eine minimale erzeugende Menge ist.*

Beweis. Es sei M maximale linear unabhängige Menge. Wegen $M \subseteq \mathfrak{L}(M)$ genügt es, für jedes $\mathfrak{x} \in V \setminus M$ zu zeigen, daß $\mathfrak{x} \in \mathfrak{L}(M)$ gilt. Da M maximale linear unabhängige Menge ist, ist $M' = M \cup \{\mathfrak{x}\}$ linear abhängig. Daher gibt es eine nichttriviale Darstellung des Nullvektors

$$\mathfrak{o} = \mathfrak{x}\xi + \sum_{\mathfrak{m} \in M} \mathfrak{m}\lambda_{\mathfrak{m}} .$$

Hier muß aber $\xi \neq 0$ sein, weil $\mathfrak{o}$ sonst schon nichttrivial aus M linear kombinierbar wäre, was der linearen Unabhängigkeit von M widerspricht. Somit gilt

$$\mathfrak{x} = -\sum_{\mathfrak{m} \in M} \mathfrak{m}\lambda_{\mathfrak{m}}\xi^{-1}, \tag{5}$$

d. h., M ist eine erzeugende Menge. Wäre M nicht minimal, so gäbe es eine erzeugende Menge $M_0 \subset M$. Dann wäre jedes $\mathfrak{a} \in M \setminus M_0$ schon aus M_0 linear kombinierbar, und nach Folgerung 1 wäre M linear abhängig im Widerspruch zur Voraussetzung. Es sei nun umgekehrt M eine minimale erzeugende Menge. Wäre M linear

abhängig, so könnte man nach Folgerung 1 einen der Vektoren $\mathfrak{c} \in M$ durch die übrigen linear ausdrücken. Setzt man in jeder Linearkombination (4) für $\mathfrak{c}$ diesen Ausdruck ein, so erkennt man, daß schon $M \setminus \{\mathfrak{c}\}$ eine erzeugende Menge wäre, was der Minimalität von M widerspricht. Somit ist M linear unabhängig. Wäre M nun nicht maximale linear unabhängige Menge, so gäbe es einen Vektor $\mathfrak{b} \in V \setminus M$ mit $M \cup \{\mathfrak{b}\}$ linear unabhängig; nach Folgerung 1 ließe sich dann $\mathfrak{b}$ nicht aus M linear kombinieren, und M könnte entgegen der Voraussetzung keine erzeugende Menge sein. □

Definition 3. Eine minimale erzeugende Menge oder, was dasselbe ist, eine maximale linear unabhängige Menge heißt eine *Basis des Vektorraumes* V. Ein Vektorraum V heißt *endlichdimensional*, wenn er eine Basis aus endlich vielen Elementen besitzt, und *unendlichdimensional* andernfalls.

Wir übergehen die Frage nach der Existenz einer Basis in einem beliebigen Vektorraum (vgl. Übung 7) und beweisen

Satz 2. *Es sei V ein endlichdimensionaler Vektorraum über K, $B = \{\mathfrak{b}_1, \ldots, \mathfrak{b}_n\}$ eine Basis von V und $M = \{\mathfrak{c}_1, \ldots, \mathfrak{c}_k\}$ eine linear unabhängige Menge. Dann gilt $k \leqq n$. Jede Basis von V enthält dieselbe Anzahl n von Elementen.*

Beweis. Wir zeigen $k \leqq n$. Hieraus erhält man sofort die zweite Behauptung; denn wenn M ebenfalls eine Basis ist, dann muß auch $n \leqq k$, also $n = k$ gelten. Da B eine Basis ist, können wir jedes $\mathfrak{c}_\alpha \in M$ durch die $\mathfrak{b}_i$ linear kombinieren:

$$\mathfrak{c}_\alpha = \sum_{i=1}^{n} \mathfrak{b}_i \gamma_{i\alpha} . \tag{6}$$

Setzen wir diese Ausdrücke in eine Linearkombination des Nullvektors aus den $\mathfrak{c}_\alpha$ ein, so folgt

$$\mathfrak{o} = \sum_{\alpha=1}^{k} \mathfrak{c}_\alpha \xi_\alpha = \sum_{i=1}^{n} \mathfrak{b}_i \sum_{\alpha=1}^{k} \gamma_{i\alpha} \xi_\alpha$$

genau dann, wenn

$$\sum_{\alpha=1}^{k} \gamma_{i\alpha} \xi_\alpha = 0 \quad \text{für} \quad i = 1, \ldots, n \tag{7}$$

gilt. Wäre nun die Anzahl k der Unbekannten ξ_α größer als die Anzahl n der Gleichungen, so hätte das homogene lineare Gleichungssystem (7) nach dem Gaußschen Algorithmus wenigstens eine nichttriviale Lösung (vgl. Folgerung 2.9.1), was der vorausgesetzten linearen Unabhängigkeit von M widerspräche. Also ist $k \leqq n$. □

Bemerkung. Einen anderen Beweis dieses Satzes, der vom Gaußschen Algorithmus nicht Gebrauch macht, erhält man leicht aus dem Steinitzschen Austauschsatz (vgl. § 6).

Definition 4. Es sei V ein endlichdimensionaler Vektorraum über K. Enthält eine Basis von V genau n Elemente, so nennen wir V *n-dimensional* und schreiben $\dim V = n$ oder $V = V^n$. Ist V unendlichdimensional, so schreiben wir $\dim V = \infty$.

Auf Grund von Satz 2 hängt dim V nicht von der Wahl der Basis von V ab. Eine affine Geometrie $[A, V, K]$ bzw. ein affiner Raum $A\,(=A^n)$ heißt *n-dimensional*, wenn der zugehörige Vektorraum n-dimensional ist. Häufig drückt man die Forderung, daß ein Vektorraum n-dimensional sei, auch durch ein *Dimensionsaxiom* aus, das folgendermaßen lautet:

Dimensionsaxiom. a) *In V^n gibt es eine Menge $\{\mathfrak{b}_1, ..., \mathfrak{b}_n\}$ aus n linear unabhängigen Vektoren.* b) *Jede Menge, die mehr als n Vektoren enthält, ist linear abhängig.*

Folgerung 2. *Ein Vektorraum V erfüllt genau dann das Dimensionsaxiom mit der Dimension n, wenn er eine Basis aus n Elementen besitzt.*

Beweis. Wenn V das Dimensionsaxiom erfüllt, ist die Menge $\{\mathfrak{b}_1, ..., \mathfrak{b}_n\}$ eine maximale linear unabhängige Menge, d. h. eine Basis aus n Elementen. Wenn umgekehrt eine Basis aus n Elementen existiert, ist Teil a) des Dimensionsaxioms erfüllt. Nach Satz 2 kann es aber keine linear unabhängige Menge mit mehr als n Elementen geben, und somit gilt auch b). □

Folgerung 3. *Es sei V ein beliebiger Vektorraum über K. Eine Teilmenge $B \subseteq V$ ist Basis genau dann, wenn sie eine linear unabhängige erzeugende Menge ist.*

Beweis. Auf Grund von Definition 3 und Satz 1 ist die Bedingung notwendig. Ist andererseits B linear unabhängige erzeugende Menge, so muß B auch minimale erzeugende Menge, d. h. Basis sein; denn wenn es eine kleinere erzeugende Menge $B_0 \subset B$ gäbe, müßte sich einer der Vektoren aus B durch die anderen linear ausdrücken lassen, was wegen Folgerung 1 unmöglich ist. □

Aus Lemma 1 erhält man sofort

Folgerung 4. *Die Menge $\{\mathfrak{e}_1, ..., \mathfrak{e}_n\}$ des Vektorraumes K^n, $\mathfrak{e}_i$ definiert durch* (1), *ist eine Basis, die wir die Standardbasis von K^n nennen. Daher gilt*

$$\dim K^n = n\,. \quad \square$$

Wir können nun leicht Vektorkoordinaten in einem Vektorraum V^n definieren. Unter einem *n-Bein* (oder *Repère*) *von* V^n verstehen wir eine geordnete Basis $(\mathfrak{b}_1, ..., \mathfrak{b}_n)$, d. h. eine Folge aus n linear unabhängigen Vektoren; häufig sagt man statt „n-Bein" ebenfalls „Basis". Ist K der zugrunde liegende Körper, so wird durch

$$\varphi\colon \mathfrak{x} = \sum_{i=1}^{n} \mathfrak{b}_i \xi_i \in V^n \mapsto (\xi_i) \in K^n \tag{9}$$

eine bijektive Abbildung definiert, die jedem Vektor $\mathfrak{x} \in V^n$ *das n-Tupel* $(\xi_i) \in K^n$ *seiner Vektorkoordinaten bezüglich des n-Beins* $(\mathfrak{b}_i)$ *zuordnet.* Man beachte, daß die Koordinaten nicht nur von der Basis, sondern auch von der gewählten Anordnung, d. h. von dem n-Bein abhängen.

Im Fall des n-dimensionalen affinen Punktraumes A^n verstehen wir unter einem *n-Bein* oder *Repère* ein Tupel $(o; \mathfrak{b}_1, ..., \mathfrak{b}_n)$, bestehend aus einem beliebigen fest gewählten Punkt $o \in A^n$ und einem n-Bein des zugehörigen Vektorraumes V^n. Nach Satz 3.2 gehört zu dem Punkt o eine bijektive Abbildung $\Phi_0\colon A^n \to V^n$. Verknüpfen

wir sie mit der Abbildung (9), so erhalten wir die Abbildung $\psi = \varphi \circ \Phi_0 \colon \boldsymbol{A}^n \to K^n$,

$$\psi \colon x = o + \sum_{i=1}^{n} \mathfrak{b}_i \xi_i \in \boldsymbol{A}^n \mapsto \psi(x) := (\xi_i) \in K^n, \tag{10}$$

die jedem Punkt $x \in \boldsymbol{A}^n$ das n-Tupel $(\xi_i) \in K^n$ seiner *Punktkoordinaten bezüglich des n-Beins* $(o; \mathfrak{b}_1, \ldots, \mathfrak{b}_n)$ zuordnet. Die Punktkoordinaten von x sind also gleich den Vektorkoordinaten des Ortsvektors $\overrightarrow{ox}$. Die Punkte o, $a_i := o + \mathfrak{b}_i$, $i = 1, \ldots, n$, heißen die *Grundpunkte des Koordinatensystems*, o sein *Ursprung* und die Geraden $\boldsymbol{H}_i = \boldsymbol{H}(o, a_i)$ seine *Achsen* (vgl. Abb. 3). Man nennt die so definierten Koordinatensysteme auch *affin* oder *kartesisch*. Damit haben wir den in § 1 aus der Anschauung gewonnenen kartesischen Koordinaten eine präzise axiomatische Grundlage gegeben und die Axiomatik der affinen Geometrie abgeschlossen.

Beispiel 2. Wir betrachten einen eindimensionalen Vektorraum $\boldsymbol{V}^1$. Ist $\mathfrak{a} \neq \mathfrak{o}$, so ist $\{\mathfrak{a}\}$ eine Basis von $\boldsymbol{V}^1$ (vgl. Beispiel 1), und die einzige Koordinate ξ eines beliebigen Vektors $\mathfrak{x} \in \boldsymbol{V}$ ist gleich dem Vektorverhältnis $\xi = \mathfrak{x}/\mathfrak{a}$. Es sei nun $\boldsymbol{A}^1$ ein eindimensionaler affiner Raum mit dem Vektorraum $\boldsymbol{V}^1$, $a \in \boldsymbol{A}^1$ ein beliebiger Punkt. Dann ist $\boldsymbol{A}^1 = \boldsymbol{H}(a, \mathfrak{a})$, und die einzige Punktkoordinate des beliebigen Punktes $x \in \boldsymbol{A}^1$ ist gleich seinem affinen Parameter bezüglich der durch a und $a + \mathfrak{a}$ bestimmten affinen Skala; die durch (3.18) beschriebene Abbildung ist die Inverse der Koordinatenabbildung ψ im Fall $n = 1$.

Als Spezialisierung des Begriffes der direkten Summe einer Familie von Untergruppen einer abelschen Gruppe (vgl. Beispiel 3.2.3) behandeln wir noch die direkte Summe von Unterräumen eines Vektorraumes:

Definition 5. Es sei $\boldsymbol{V}$ ein Vektorraum und $(\boldsymbol{W}_\iota)_{\iota \in I}$ eine Familie von Unterräumen von $\boldsymbol{V}$. Man sagt, $\boldsymbol{V}$ sei *direkte Summe der* $(\boldsymbol{W}_\iota)_{\iota \in I}$ und schreibt hierfür

$$\boldsymbol{V} = \bigoplus_{\iota \in I} \boldsymbol{W}_\iota, \tag{11}$$

wenn $\boldsymbol{V} = \sum_{\iota \in I} \boldsymbol{W}_\iota$ die Summe der $\boldsymbol{W}_\iota$ ist (vgl. (2.19) und Übung 2.4) und jedes $\mathfrak{x} \in \boldsymbol{V}$ höchstens eine Darstellung als formal unendliche Summe

$$\mathfrak{x} = \sum_{\iota \in I} \mathfrak{x}_\iota \quad \text{mit} \quad \mathfrak{x}_\iota \in \boldsymbol{W}_\iota \tag{12}$$

besitzt. Das durch $\mathfrak{x} \in \boldsymbol{V}$ eindeutig bestimmte Element $\mathfrak{x}_\iota = \mathfrak{x}_\iota(\mathfrak{x}) \in \boldsymbol{W}_\iota$ heißt die *Komponente von $\mathfrak{x}$ in $\boldsymbol{W}_\iota$* bei der direkten Summenzerlegung (11). Für endliche Familien schreibt man statt (11)

$$\boldsymbol{V} = \boldsymbol{W}_1 \oplus \ldots \oplus \boldsymbol{W}_k. \tag{13}$$

Den folgenden Satz kann man auch aus Satz 3.2.3 herleiten:

Satz 3. *Es sei $(\boldsymbol{W}_\iota)_{\iota \in I}$ eine Familie von Unterräumen von $\boldsymbol{V}$ und $\boldsymbol{V} = \sum_{\iota \in I} \boldsymbol{W}_\iota$. Diese Summe ist direkt dann und nur dann, wenn*

$$\boldsymbol{W}_\varkappa \cap \sum_{\substack{\iota \in I \\ \iota \neq \varkappa}} \boldsymbol{W}_\iota = \{\mathfrak{o}\} \quad \textit{für alle} \quad \varkappa \in I \tag{14}$$

gilt.

Beweis. Ist die Summe nicht direkt, so gibt es ein $\mathfrak{x} \in \boldsymbol{V}$, das zwei verschiedene Darstellungen $\mathfrak{x} = \sum_{\iota \in I} \mathfrak{x}_\iota = \sum_{\iota \in I} \hat{\mathfrak{x}}_\iota$ besitzt. Es sei etwa $\mathfrak{x}_\varkappa \neq \hat{\mathfrak{x}}_\varkappa$. Dann gilt

$$\mathfrak{o} \neq \mathfrak{x}_\varkappa - \hat{\mathfrak{x}}_\varkappa \in \boldsymbol{W}_\varkappa \cap \sum_{\substack{\iota \in I \\ \iota \neq \varkappa}} \boldsymbol{W}_\iota ,$$

und daher gilt (14) nicht. Ist umgekehrt (14) nicht erfüllt, so gibt es ein $\varkappa \in I$ und ein $\mathfrak{x} \neq \mathfrak{o}$ mit

$$\mathfrak{x} \in \boldsymbol{W}_\varkappa \cap \sum_{\substack{\iota \in I \\ \iota \neq \varkappa}} \boldsymbol{W}_\iota ,$$

und dieses $\mathfrak{x}$ besitzt gewiß zwei verschiedene Darstellungen $\mathfrak{x} = \mathfrak{x}_\varkappa$ und $\mathfrak{x} = \sum_{\iota \neq \varkappa} \mathfrak{x}_\iota$. □

Beispiel 3. Es sei $(\mathfrak{a}_i)$, $i = 1, \ldots, n$, eine Basis von $\boldsymbol{V}^n$. Dann ist $\boldsymbol{V}^n$ direkte Summe der zugehörigen Koordinatenachsen:

$$\boldsymbol{V}^n = \bigoplus_{i=1}^{n} \mathfrak{L}(\{\mathfrak{a}_i\}) . \tag{15}$$

Bemerkung. Gilt bei einer direkten Summenzerlegung (12) und analog $\mathfrak{y} = \sum \mathfrak{y}_\iota$, so folgt $\mathfrak{x}\lambda = \sum (\mathfrak{x}_\iota \lambda)$ und $\mathfrak{x} + \mathfrak{y} = \sum (\mathfrak{x}_\iota + \mathfrak{y}_\iota)$. Bei einer direkten Summendarstellung erfolgen die Vektoroperationen also komponentenweise.

Folgerung 5. *Ist* $\dim \boldsymbol{V} = n < \infty$ *und gilt* $\boldsymbol{V} = \bigoplus_{\iota \in I} \boldsymbol{W}_\iota$, *so ist*

$$\dim \boldsymbol{V} = \sum_{\iota \in I} \dim \boldsymbol{W}_\iota . \tag{16}$$

Beweis. Es genügt, nur die nichttrivialen Summanden $\boldsymbol{W}_\iota \neq \{0\}$ zu betrachten. Wegen der Existenz und Eindeutigkeit der Darstellungen (12) ergibt sich sofort, daß die Vereinigungsmenge der Basen der $\boldsymbol{W}_\iota$ eine Basis von $\boldsymbol{V}$ ist. Da wegen (14) diese Basen der $\boldsymbol{W}_\iota$ paarweise disjunkt sein müssen, folgt (16). □

Übung 1. Man beweise, daß die durch (9) definierte Abbildung φ linear ist, d. h., sie besitzt die folgenden Eigenschaften:

$$\varphi(\mathfrak{a} + \mathfrak{b}) = \varphi(\mathfrak{a}) + \varphi(\mathfrak{b}), \qquad \varphi(\mathfrak{a}\lambda) = \varphi(\mathfrak{a})\,\lambda .$$

Übung 2. Es sei $\boldsymbol{V}$ ein Vektorraum über dem kleinsten Körper $K = \{0, 1\}$. Man beweise: Eine Menge $M = \{\mathfrak{a}, \mathfrak{b}\} \subseteq \boldsymbol{V}$ aus zwei Elementen ist genau dann linear unabhängig, wenn sie nicht den Nullvektor enthält.

Eine leichte, aber nicht unwichtige Verallgemeinerung der Definition einer linear unabhängigen Menge ist

Definition 6. Es sei $\boldsymbol{V}$ ein Vektorraum über K, I eine Indexmenge. Die Vektorfamilie $(\mathfrak{c}_\iota)_{\iota \in I}$, $\mathfrak{c}_\iota \in \boldsymbol{V}$, heißt *linear unabhängig*, wenn jeder Vektor $\mathfrak{x} \in \boldsymbol{V}$ höchstens eine Darstellung als (formal unendliche) Linearkombination der Gestalt $\mathfrak{x} = \sum_{\iota \in I} \mathfrak{c}_\iota \xi_\iota$ besitzt.

Übung 3. Man beweise: a) Jede Teilfamilie $(\mathfrak{c}_\varkappa)_{\varkappa \in J}$, $J \subseteq I$, einer linear unabhängigen Familie ist selbst linear unabhängig. — b) Gilt $\mathfrak{c}_\iota = \mathfrak{c}_\lambda$ für ein Paar $\iota \neq \lambda$, so ist $(\mathfrak{c}_\iota)_{\iota \in I}$ linear

abhängig. – c) Ist die Familie $(\mathfrak{c}_\iota)_{\iota\in I}$ linear unabhängig, so ist es auch die Menge $\{\mathfrak{c}_\iota\}_{\iota\in I}$. – d) Man zeige an einem Beispiel, daß die Umkehrung von c) nicht gilt. – e) Man formuliere und beweise die Analoga von Lemma 2 und Folgerung 1 für Familien von Vektoren.

Übung 4. Man zeige: Der Vektorraum K^M von Beispiel 2.4 ist n-dimensional genau dann, wenn $|M|=n$ gilt, und unendlichdimensional, falls M unendlich ist.

Übung 5. Man zeige: Die Menge $\{x^k \mid k\in \mathbf{N}_0\}$ ist eine Basis des Vektorraumes $K[x]$, vgl. Beispiel 2.5; es gilt also $\dim K[x]=\infty$.

Übung 6. Es sei $K[[x]]$ der Ring der formalen Potenzreihen über einem Körper K, vgl. Übung 2.4.1. Man beweise: $K[[x]]$ ist ein unendlichdimensionaler Vektorraum über K.

Übung 7. Es sei V ein Vektorraum über K, $M\subseteq D\subseteq V$, M linear unabhängig, und D eine erzeugende Menge. Mit $\mathfrak{T}$ bezeichnen wir das System der linear unabhängigen Mengen L mit $M\subseteq L\subseteq D$. Man zeige: a) $\mathfrak{T}$ ist bezüglich der Ordnung $\subseteq$ *induktiv*, genauer: Ist $\mathfrak{T}_0\subseteq\mathfrak{T}$ und $\mathfrak{T}_0$ linear geordnet, so ist auch $\bigcup_{L\in\mathfrak{T}_0} L\in\mathfrak{T}$. – b) Nach dem Lemma von Zorn (Satz von Kuratowski-Zorn; vgl. etwa A. G. Kuroš [2] oder S. Lang [1]) folgt aus a), daß in $\mathfrak{T}$ ein maximales Element B existiert. Man beweise: B ist eine Basis von V. – c) Folgerung. Für $M=\emptyset$ und $D=V$ ergibt sich: In V existiert eine Basis. – d) Man beweise: Zwei Basen B_1, B_2 von V haben stets die gleiche Mächtigkeit. (Hinweis. Für unendliche Mächtigkeiten schließe man indirekt. Ist $|B_1|<|B_2|$, so stelle man jedes $\mathfrak{b}\in B_1$ mittels einer endlichen Menge $M_\mathfrak{b}\subseteq B_2$ dar. Die Vereinigung $\bigcup_{\mathfrak{b}\in B_1} M_\mathfrak{b}\subseteq B_2$ hat dieselbe Mächtigkeit wie B_1 und ist erzeugende Menge.)

Übung 8. Ein Körper K heißt *endliche Erweiterung* des Körpers L, wenn $K\supseteq L$ eine Erweiterung und $\dim_L K$ endlich ist; dabei bedeutet $\dim_L K$ die Dimension von K, betrachtet als Vektorraum über L (vgl. Übung 2.7); $\dim_L K$ wird auch der *Körpergrad von K über L* genannt. Man beweise: Ist V ein endlichdimensionaler Vektorraum über K und K eine endliche Erweiterung von L, so ist V auch ein endlichdimensionaler Vektorraum über L, und es gilt

$$\dim_L V=\dim_K V\cdot\dim_L K\,.$$

Ist beispielsweise V ein n-dimensionaler Vektorraum über $\mathbf{C}$, so ist seine Reellifizierung rV ein $2n$-dimensionaler Vektorraum über $\mathbf{R}$; aus einer Basis $\{a_k\}$, $k=1,\ldots,n$, von V über $\mathbf{C}$ erhalten wir durch $\{a_k, a_k i\}$, $k=1,\ldots,n$, $i=\sqrt{-1}$, eine Basis von rV.

Übung 9. Man beweise: Ist K ein endlicher Körper, d. h. $|K|\in\mathbf{N}$, und $\operatorname{char} K=p$, so gibt es ein $k\in\mathbf{N}$ mit $|K|=p^k$: Die Mächtigkeit eines endlichen Körpers ist eine Potenz seiner Charakteristik.

§ 5. k-Ebenen

Die Definition 3.2 einer Geraden kann man auch so beschreiben: Man bilde den von einem Vektor $\mathfrak{a}\in V$, $\mathfrak{a}\neq\mathfrak{o}$, erzeugten eindimensionalen Vektorraum $W^1=\mathfrak{L}(\{\mathfrak{a}\})$ und mit ihm den W^1-Orbit des Punktes $a\in A$, für den folgende Bezeichnung vereinbart wird:

$$a+W:=\{x \mid x\in A \text{ und } x=a+\mathfrak{w},\ \mathfrak{w}\in W\}\,. \tag{1}$$

Diese Definition (1) ist für jeden Punkt $a\in A$ und sogar für jede Vektormenge $W\subset V$ sinnvoll; denkt man sich z. B. für W einen zweidimensionalen Vektorraum

des dreidimensionalen Anschauungsraumes (§ 1) eingesetzt, so erhält man eine Ebene. Die Definition einer allgemeinen Ebene ist

Definition 1. Es sei $[\boldsymbol{A}, \boldsymbol{V}, K]$ eine affine Geometrie. Eine nichtleere Punktmenge $\boldsymbol{H} \subset \boldsymbol{A}$ heißt eine *Ebene*, wenn es einen Unterraum $\boldsymbol{W} \subset \boldsymbol{V}$ gibt, so daß $\boldsymbol{H}$ der $\boldsymbol{W}$-Orbit (1) eines seiner Punkte $a \in \boldsymbol{H}$ ist. Wir verwenden statt (1) auch die folgenden Bezeichnungen:

$$\boldsymbol{H}(a, \boldsymbol{W}) := a + \boldsymbol{W}, \qquad \boldsymbol{H}(a; \mathfrak{c}_1, \ldots, \mathfrak{c}_k) := a + \mathfrak{L}(\{\mathfrak{c}_1, \ldots, \mathfrak{c}_k\})$$

und nennen $\boldsymbol{H}$ die von a und $\boldsymbol{W}$ bzw. die von a und $\{\mathfrak{c}_\varkappa\}_{\varkappa=1,\ldots,k}$ *aufgespannte Ebene*.

Beispiel 1. Ist $\boldsymbol{W} = \{\mathfrak{o}\}$ der triviale Unterraum, so gilt $a + \boldsymbol{W} = \{a\}$. Für $\boldsymbol{W} = \mathfrak{L}(\{\mathfrak{a}\})$, $\mathfrak{a} \neq \mathfrak{o}$, erhalten wir die Geraden

$$\boldsymbol{H}(a, \mathfrak{a}) = a + \mathfrak{L}(\{\mathfrak{a}\}) \qquad (\mathfrak{a} \neq \mathfrak{o}) . \tag{2}$$

Setzt man $\boldsymbol{W} = \boldsymbol{V}$, so gilt für alle $a \in \boldsymbol{A}$ die Beziehung $\boldsymbol{A} = a + \boldsymbol{V}$; der affine Raum ist also selbst eine Ebene. Man beachte, daß in Definition 1 von der Dimension abstrahiert wird (vgl. Definition 2 und die darauf folgende Bemerkung).

Lemma 1. *Es seien $a, b \in \boldsymbol{A}$ und $\boldsymbol{U}, \boldsymbol{W}$ Unterräume von $\boldsymbol{V}$. Dann gilt $a + \boldsymbol{W} = b + \boldsymbol{U}$ dann und nur dann, wenn $\boldsymbol{W} = \boldsymbol{U}$ und $\overrightarrow{ab} \in \boldsymbol{W}$ ist.*

Beweis. Es seien die beiden Orbits gleich. Wählt man $\mathfrak{u} = \mathfrak{o} \in \boldsymbol{U}$, so gibt es ein $\mathfrak{w} \in \boldsymbol{W}$ mit $b = a + \mathfrak{w}$, also $\overrightarrow{ab} = \mathfrak{w} \in \boldsymbol{W}$. Analog zeigt man $\overrightarrow{ab} \in \boldsymbol{U}$. Ist nun $\mathfrak{x} \in \boldsymbol{W}$ beliebig, so gibt es ein $\mathfrak{v} \in \boldsymbol{U}$ mit $x = a + \mathfrak{x} = b + \mathfrak{v}$, also $\mathfrak{x} = \overrightarrow{ab} + \mathfrak{v} \in \boldsymbol{U}$, und daher gilt $\boldsymbol{W} \subseteq \boldsymbol{U}$. Analog folgt $\boldsymbol{U} \subseteq \boldsymbol{W}$ und somit $\boldsymbol{W} = \boldsymbol{U}$. Es sei umgekehrt $\boldsymbol{U} = \boldsymbol{W}$ und $\overrightarrow{ab} \in \boldsymbol{W}$. Dann folgt $b = a + \overrightarrow{ab} \in a + \boldsymbol{W}$, und nach einer Eigenschaft des Orbits ist $a + \boldsymbol{W} = b + \boldsymbol{W}$, vgl. Satz 1.4.4. □

Nach Lemma 1 gehört also zu jeder Ebene ein *eindeutig bestimmter* Unterraum, dessen Orbit sie ist. Daher ist die folgende Definition sinnvoll:

Definition 2. Unter der *Dimension einer Ebene* $\boldsymbol{H} = a + \boldsymbol{W}$ versteht man die Dimension des zugehörigen Vektorraumes $\boldsymbol{W}$. Statt k-dimensionaler Ebene sagt man auch *k-Ebene* und schreibt $\boldsymbol{H} = \boldsymbol{H}^k$ oder $\dim \boldsymbol{H} = k$.

Bemerkung. 0-Ebenen sind Punkte, 1-Ebenen sind Geraden und 2-Ebenen die „gewöhnlichen" Ebenen des $\boldsymbol{A}^3$. Im Fall des dreidimensionalen Raumes sprechen wir von Punkten, Geraden und Ebenen immer im Sinne der Dimensionen 0, 1, 2. Die $(n-1)$-Ebenen eines n-dimensionalen affinen Raumes nennt man auch *Hyperebenen*.

Lemma 2. *Es sei $\boldsymbol{W} \subseteq \boldsymbol{V}^n$ ein Unterraum eines n-dimensionalen Vektorraumes. Dann gilt*

$$0 \leqq \dim \boldsymbol{W} \leqq n; \tag{3}$$

dabei gilt $\dim \boldsymbol{W} = 0$ genau dann, wenn $\boldsymbol{W} = \{\mathfrak{o}\}$ der triviale Unterraum ist, und $\dim \boldsymbol{W} = n$ genau dann, wenn $\boldsymbol{W} = \boldsymbol{V}^n$ ist.

Der Beweis folgt unmittelbar aus der Bemerkung, daß eine linear unabhängige Teilmenge $\{\mathfrak{b}_1, ..., \mathfrak{b}_k\} \subset \boldsymbol{W}$ auch linear unabhängige Teilmenge von $\boldsymbol{V}$ ist, vgl. Lemma 4.2. □

Satz 1. *Es sei* $[\boldsymbol{A}^n, \boldsymbol{V}^n, K]$ *eine n-dimensionale affine Geometrie. Dann gilt:*

a) *Zu jeder k-Ebene* $\boldsymbol{H}^k \subseteq \boldsymbol{A}^n$ *gibt es einen eindeutig bestimmten Unterraum* $\boldsymbol{W}^k \subseteq \boldsymbol{V}^n$, $0 \leqq k \leqq n$, *so daß* $\boldsymbol{H}^k = a + \boldsymbol{W}^k$ *für beliebiges* $a \in \boldsymbol{H}^k$ *gilt, und zwar ist* $\boldsymbol{W}^k$ *gleich*

$$V(\boldsymbol{H}) := \{\vec{xy} \mid x, y \in \boldsymbol{H}\}, \tag{4}$$

der zu der Punktmenge $\boldsymbol{H} = \boldsymbol{H}^k$ *gehörenden Vektormenge.*

b) *Es gilt* $\boldsymbol{H}^k = \boldsymbol{A}^n$ *genau dann, wenn* $k = n$ *ist.*

c) *Eine Punktmenge* $H \subseteq \boldsymbol{A}^n$ *ist eine k-Ebene dann und nur dann, wenn* $[\boldsymbol{H}, V(\boldsymbol{H}), K]$ *mit den aus* $[\boldsymbol{A}^n, \boldsymbol{V}^n, K]$ *sich durch Einschränkung ergebenden Operationen eine k-dimensionale affine Geometrie ist.*

d) *Im* $\boldsymbol{A}^n$ *gibt es k-Ebenen für* $k = 0, 1, ..., n$.

Beweis. Wegen der Lemmata 1, 2 ist für a) nur noch zu zeigen: Ist $\boldsymbol{H} = a + \boldsymbol{W}$ eine k-Ebene, so gilt $\boldsymbol{W} = V(\boldsymbol{H})$. In der Tat, sind $x, y \in \boldsymbol{H}$, so gilt nach der Orbiteigenschaft $x + \boldsymbol{W} = y + \boldsymbol{W} = \boldsymbol{H}$, und nach Lemma 1 ist $\vec{xy} \in \boldsymbol{W}$, also $V(\boldsymbol{H}) \subseteq \boldsymbol{W}$. Umgekehrt, aus $\mathfrak{x} \in \boldsymbol{W}$ folgt $x = a + \mathfrak{x} \in \boldsymbol{H}$ und somit $\mathfrak{x} = \vec{ax} \in V(\boldsymbol{H})$, also $\boldsymbol{W} = V(\boldsymbol{H})$.

b) folgt unmittelbar aus Lemma 2.

Für den Beweis von c) sei $\boldsymbol{H}$ eine k-Ebene. Dann sind nach a) die Axiome (I), (II) und das Dimensionsaxiom dim $V(\boldsymbol{H}) = k$ erfüllt. Weil $\boldsymbol{H}$ der $V(\boldsymbol{H})$-Orbit eines Punktes $a \in \boldsymbol{H}$ ist, wirkt $V(\boldsymbol{H})$ transitiv über $\boldsymbol{H}$, und weil die Wirkung von $\boldsymbol{V}$ über $\boldsymbol{A}$ einfach transitiv ist, gilt das auch für die Wirkung von $V(\boldsymbol{H})$ über $\boldsymbol{H}$. Ist umgekehrt $[\boldsymbol{H}, V(\boldsymbol{H}), K]$ eine k-dimensionale affine Geometrie, so ist $V(\boldsymbol{H})$ ein k-dimensionaler Vektorraum und $\boldsymbol{H} = a + V(\boldsymbol{H})$ für beliebiges $a \in \boldsymbol{H}$ eine k-Ebene.

Der Beweis von d) resultiert aus dem folgenden

Beispiel 2. Es sei $(o; \mathfrak{a}_1, ..., \mathfrak{a}_n)$ ein n-Bein des $\boldsymbol{A}^n$ und $a \in \boldsymbol{A}^n$ ein beliebiger Punkt. Für je k Vektoren des n-Beins definieren wir

$$\boldsymbol{W}_{i_1 ... i_k} := \mathfrak{L}(\{\mathfrak{a}_{i_1}, ..., \mathfrak{a}_{i_k}\}), \qquad 1 \leqq i_1 < ... < i_k \leqq n.$$

Dann ist $a + \boldsymbol{W}_{i_1 ... i_k}$ eine durch den Punkt a gehende k-Ebene, die man eine *Koordinatenebene* durch a nennt. (Abb. 4 zeigt die Koordinatenebenen durch einen Punkt $x \in \boldsymbol{A}^3$; sie schneiden sich in den Koordinatengeraden durch diesen Punkt.) □

Aus Satz 1 und Lemma 2 erhält man unmittelbar

Folgerung 1. a) *Für Unterräume* $\boldsymbol{W} \subseteq \boldsymbol{U}$ *gilt* dim $\boldsymbol{W} \leqq$ dim $\boldsymbol{U}$.

b) *Für Ebenen* $\boldsymbol{H} \subseteq \boldsymbol{M}$ *gilt* dim $\boldsymbol{H} \leqq$ dim $\boldsymbol{M}$.

c) *Das Gleichheitszeichen gilt genau dann, wenn* $\boldsymbol{U} = \boldsymbol{W}$ *(bzw.* $\boldsymbol{H} = \boldsymbol{M}$*) ist.* □

Definition 3. Es seien $\boldsymbol{M}, \boldsymbol{H} \subseteq \boldsymbol{A}$ Ebenen. $\boldsymbol{M}$ heißt *parallel zu* $\boldsymbol{H}$, in Zeichen $\boldsymbol{M} \parallel \boldsymbol{H}$, wenn $V(\boldsymbol{M}) \subseteq V(\boldsymbol{H})$ gilt.

Zum Beispiel sind die Koordinatenachsen $o+\boldsymbol{W}_{i_\varkappa}$, $\varkappa=1, \ldots, k$, zu den Koordinatenebenen $a+\boldsymbol{W}_{i_1 \ldots i_k}$ parallel. Eine Koordinatenebene $b+\boldsymbol{W}_{j_1 \ldots j_m}$ ist genau dann zu der Koordinatenebene $a+\boldsymbol{W}_{i_1 \ldots i_k}$ parallel, wenn $\{j_1, \ldots, j_m\} \subseteq \{i_1, \ldots, i_k\}$ gilt (vgl. Beispiel 2). Man beachte, daß die Definition 3 nicht eine Spezialisierung der Definition 3.3 paralleler Punktmengen ist: Sind zwei Ebenen im Sinne der Definition 3.3 parallel, so sind sie es auch im Sinne der Definition 3, aber nicht umgekehrt, vgl. Übung 8. Einige einfache Eigenschaften der Parallelität enthält.

Folgerung 2. a) *Die Relation* $\parallel$ *ist reflexiv und transitiv, d. h., es gilt* $\boldsymbol{H} \parallel \boldsymbol{H}$, *und aus* $\boldsymbol{N} \parallel \boldsymbol{M}$ *und* $\boldsymbol{M} \parallel \boldsymbol{H}$ *folgt* $\boldsymbol{N} \parallel \boldsymbol{H}$.

b) *Aus* $\boldsymbol{M} \parallel \boldsymbol{H}$ *folgt* $\dim \boldsymbol{M} \leqq \dim \boldsymbol{H}$.

c) *Bezeichnet* $H(k, n)$ *die Menge der* k*-Ebenen des* n*-dimensionalen Punktraumes* $\boldsymbol{A}^n$, *so ist* $\parallel$ *über* $H(k, n)$ *eine Äquivalenzrelation; denn es gilt für* $\boldsymbol{M}, \boldsymbol{N} \in H(k, n)$:

$$\boldsymbol{M}^k \parallel \boldsymbol{N}^k \Leftrightarrow V(\boldsymbol{M}^k) = V(\boldsymbol{N}^k) .$$

d) *Ist* $\boldsymbol{M} = b + \boldsymbol{U}$ *und* $\boldsymbol{H} = a + \boldsymbol{W}$, $\boldsymbol{U}, \boldsymbol{W} \subseteq \boldsymbol{V}$ *Unterräume, und* $\boldsymbol{M} \parallel \boldsymbol{H}$, *so gilt entweder* $\boldsymbol{M} \subseteq \boldsymbol{H}$ *oder* $\boldsymbol{M} \cap \boldsymbol{H} = \emptyset$; *dabei tritt die erste Möglichkeit genau dann ein, wenn* $\vec{ab} \in \boldsymbol{W}$ *ist.*

e) *Ist* $\boldsymbol{W}^k \subseteq \boldsymbol{V}^n$ *ein fester Unterraum, so ist die Menge aller* $\boldsymbol{W}^k$*-Orbits* $\{a + \boldsymbol{W}^k\}_{a \in \boldsymbol{A}}$ *gerade eine Äquivalenzklasse der in* c) *angegebenen Äquivalenzrelation.* □

Nach Satz 1, c), ist jede k-Ebene $\boldsymbol{H}^k = a + \boldsymbol{W}^k$ ein k-dimensionaler affiner Raum. Ist also $(\mathfrak{b}_1, \ldots, \mathfrak{b}_k)$ ein k-Bein von $\boldsymbol{W}^k$, so ist $(a; \mathfrak{b}_1, \ldots, \mathfrak{b}_k)$ ein k-Bein von $\boldsymbol{H}^k$. Die Punktkoordinaten des Punktes $x \in \boldsymbol{H}$ bezüglich des k-Beins $(a; \mathfrak{b}_1, \ldots, \mathfrak{b}_k)$ nennt man seine *Parameter*, um Verwechslungen mit den Punktkoordinaten von x bezüglich eines n-Beins $(o; \mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ des umgebenden affinen Raumes $\boldsymbol{A}^n$ zu vermeiden, vgl. (4.10). Analog zu (3.18) ist also

$$(\tau_1, \ldots, \tau_k) \in K^k \mapsto x = a + \sum_{\varkappa=1}^{k} \mathfrak{b}_\varkappa \tau_\varkappa \in \boldsymbol{H}^k \tag{5}$$

eine bijektive Abbildung, die man die *Parameterdarstellung von* $\boldsymbol{H}^k$ *bezüglich des* k*-Beins* $(a; \mathfrak{b}_1, \ldots, \mathfrak{b}_k)$ nennt; $(\tau_\varkappa) \in K^k$ heißen die *Parameter von* x. Im Fall $n = k$ können wir $(o; \mathfrak{a}_1, \ldots, \mathfrak{a}_n) = (a; \mathfrak{b}_1, \ldots, \mathfrak{b}_n)$ setzen; dann stimmen die Parameter (τ_i) mit den Punktkoordinaten (ξ_i) überein, und (5) ist die zu (4.10) inverse Abbildung.

Wir betrachten nun wieder den allgemeinen Fall $\boldsymbol{H}^k \subseteq \boldsymbol{A}^n$ und wollen die Parameterdarstellung (5) durch die Punktkoordinaten bezüglich des n-Beins $(o; \mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ des $\boldsymbol{A}^n$ ausdrücken. Durch die Zerlegungen

$$\vec{oa} = \sum_{i=1}^{n} \mathfrak{a}_i \alpha_i , \qquad \mathfrak{b}_\varkappa = \sum_{i=1}^{n} \mathfrak{a}_i \beta_{i\varkappa} \tag{6}$$

werden die Punktkoordinaten $(\alpha_i) \in K^n$ von a und die Vektorkoordinaten $(\beta_{i\varkappa}) \in K^n$ von $\mathfrak{b}_\varkappa$, $\varkappa = 1, \ldots, k$, bestimmt. Sind $(\xi_i) \in K^n$ die Punktkoordinaten des variablen Punktes $x \in \boldsymbol{H}^k$, so gilt

$$\vec{ox} = \sum_{i=1}^{n} \mathfrak{a}_i \xi_i = \sum_{i=1}^{n} \mathfrak{a}_i \left(\alpha_i + \sum_{\varkappa=1}^{k} \beta_{i\varkappa} \tau_\varkappa \right) . \tag{7}$$

Da die Vektorkoordinaten von $\vec{ox}$ eindeutig bestimmt sind, erhält man durch Koeffizientenvergleich die *Parameterdarstellung einer k-Ebene des A^n in Koordinatenform:*

$$\xi_i = \alpha_i + \sum_{\varkappa=1}^{k} \beta_{i\varkappa}\tau_\varkappa \qquad (i=1, \ldots, n)\,. \tag{8}$$

Aus (5) entsteht also (8), wenn man in jedem Glied zu den Koordinaten übergeht. Man beachte, daß nicht jede Abbildung der Gestalt (5) (bzw. (8)) als Bildmenge eine k-Ebene hat; dazu ist die lineare Unabhängigkeit von $\{\mathfrak{b}_1, \ldots, \mathfrak{b}_k\}$ notwendig und hinreichend.

Satz 2. *Es sei $[\boldsymbol{A}, \boldsymbol{V}, K]$ eine affine Geometrie und $\{\boldsymbol{H}_\iota\}_{\iota\in I}$ eine Familie von Ebenen $\boldsymbol{H}_\iota \subset \boldsymbol{A}$ beliebiger Dimension. Dann ist der Durchschnitt $\bigcap_{\iota\in I}\boldsymbol{H}_\iota$ leer oder eine Ebene mit dem zugehörigen Vektorraum*

$$\boldsymbol{V}\Big(\bigcap_{\iota\in I}\boldsymbol{H}_\iota\Big) = \bigcap_{\iota\in I}\boldsymbol{V}(\boldsymbol{H}_\iota) \qquad (\text{für} \bigcap \boldsymbol{H}_\iota \neq \emptyset)\,. \tag{9}$$

Beweis. Es sei $\boldsymbol{W}_\iota := \boldsymbol{V}(\boldsymbol{H}_\iota)$ und $a \in \bigcap \boldsymbol{H}_\iota$. Nach Satz 1, a), gilt dann $\boldsymbol{H}_\iota = a + \boldsymbol{W}_\iota$. Wir setzen $\boldsymbol{U} := \bigcap_{\iota\in I}\boldsymbol{W}_\iota$ und beweisen

$$\bigcap_{\iota\in I}\boldsymbol{H}_\iota = a + \boldsymbol{U}\,. \tag{10}$$

Ist nämlich $x \in \bigcap \boldsymbol{H}_\iota$, so gilt $\vec{ax} \in \boldsymbol{W}_\iota$ für alle $\iota \in I$ und somit $\vec{ax} \in \boldsymbol{U}$, also $x = a + \vec{ax} \in a + \boldsymbol{U}$. Ist andererseits $x \in a + \boldsymbol{U}$, so gilt $\vec{ax} \in \boldsymbol{U} = \bigcap \boldsymbol{W}_\iota \subseteq \boldsymbol{W}_\iota$ und daher $x = a + \vec{ax} \in a + \boldsymbol{W}_\iota = \boldsymbol{H}_\iota$ für alle $\iota \in I$, also $x \in \bigcap \boldsymbol{H}_\iota$. □

Definition 4. Es sei $\boldsymbol{B} \subset \boldsymbol{A}$ eine beliebige, nichtleere Punktmenge eines affinen Raumes. Die von $\boldsymbol{B}$ *aufgespannte Ebene* $\boldsymbol{H}(\boldsymbol{B})$ wird definiert durch

$$\boldsymbol{H}(\boldsymbol{B}) := \bigcap_{\substack{\boldsymbol{B}\subseteq\boldsymbol{H}\subseteq\boldsymbol{A} \\ \boldsymbol{H}\text{ Ebene}}} \boldsymbol{H}\,. \tag{11}$$

Für $\boldsymbol{B} = \emptyset$ setzen wir $\boldsymbol{H}(\emptyset) := \emptyset$. Dann können wir $\boldsymbol{H}$ als eine Abbildung $\boldsymbol{H}\colon \mathfrak{P}(\boldsymbol{A}) \to \mathfrak{P}(\boldsymbol{A})$ betrachten. Es gilt

Folgerung 3. *Die von $\boldsymbol{B} \neq \emptyset$ aufgespannte Ebene ist die kleinste Ebene, die $\boldsymbol{B}$ enthält. Die Zuordnung $\boldsymbol{B} \in \mathfrak{P}(\boldsymbol{A}) \mapsto \boldsymbol{H}(\boldsymbol{B}) \in \mathfrak{P}(\boldsymbol{A})$ ist ein Hüllenoperator, d. h., es gelten die Beziehungen*

$$\boldsymbol{B} \subseteq \boldsymbol{H}(\boldsymbol{B})\,, \tag{12}$$

$$\textit{aus}\quad \boldsymbol{C} \subseteq \boldsymbol{B}\quad \textit{folgt}\quad \boldsymbol{H}(\boldsymbol{C}) \subseteq \boldsymbol{H}(\boldsymbol{B})\,, \tag{13}$$

$$\boldsymbol{H}(\boldsymbol{H}(\boldsymbol{B})) = \boldsymbol{H}(\boldsymbol{B})\,. \tag{14}$$

Eine nichtleere Punktmenge $\boldsymbol{B}$ ist eine Ebene dann und nur dann, wenn $\boldsymbol{B} = \boldsymbol{H}(\boldsymbol{B})$ gilt.

Der Beweis ist eine fast wörtliche Übertragung des Beweises von Satz 2.3 mit Ersetzung des Wortes „Unterraum" durch „Ebene". □

Satz 3. *Es sei $B \neq \emptyset$ eine Teilmenge des affinen Raumes $\boldsymbol{A}$, $b \in B$ und $V(B)$ die zu B gehörende Vektormenge* (vgl. (4)). *Dann gilt*

$$\boldsymbol{H}(B) = b + \mathfrak{L}(V(B)) \,. \tag{15}$$

Beweis. Wir definieren die Ebene $\boldsymbol{M} := b + \mathfrak{L}(V(B))$ und beweisen $\boldsymbol{H}(B) = \boldsymbol{M}$. Ist $c \in B$, so ist $\vec{bc} \in V(B)$ und $c = b + \vec{bc} \in \boldsymbol{M}$, also $B \subseteq \boldsymbol{M}$. Aus Folgerung 3 resultiert $\boldsymbol{H}(B) \subseteq \boldsymbol{H}(\boldsymbol{M}) = \boldsymbol{M}$. Für den Beweis der umgekehrten Relation $\boldsymbol{M} \subseteq \boldsymbol{H}(B)$ genügt es zu zeigen: Ist $\boldsymbol{H}$ irgendeine Ebene mit $B \subseteq \boldsymbol{H}$, so gilt auch $\boldsymbol{M} \subseteq \boldsymbol{H}$. Aus der Definition der Vektormengen (4) folgt unmittelbar $V(B) \subseteq V(\boldsymbol{H})$. Wegen der Monotonie des Hüllenoperators $\mathfrak{L}$ und weil $V(\boldsymbol{H})$ schon ein Unterraum ist (Satz 1), gilt

$$\mathfrak{L}(V(B)) \subseteq \mathfrak{L}(V(\boldsymbol{H})) = V(\boldsymbol{H}) \tag{16}$$

(vgl. Folgerung 2.1). Aus der Definition von $\boldsymbol{M}$ schließt man nun $\boldsymbol{M} \subseteq b + V(\boldsymbol{H}) = \boldsymbol{H}$; denn es ist $b \in B \subseteq \boldsymbol{H}$. □

Man erhält also die von einer Punktmenge $B \subseteq \boldsymbol{A}$ aufgespannte Ebene, indem man erst alle Vektoren $\vec{bc}$, $b, c \in B$, bildet, von dieser Menge $V(B)$ die lineare Hülle nimmt und diese an einen beliebigen Punkt $b \in B$ anträgt. Daher ist $V(B)$ eine erzeugende Menge des Vektorraumes von $\boldsymbol{H}(B)$. Enthält B mindestens zwei Punkte, so ist jedoch $V(B)$ keinesfalls minimal. Sind nämlich $b, c, d \in B$, so ist $\vec{cd} = \vec{bd} - \vec{bc}$; wir erhalten also schon eine erzeugende Menge, wenn wir alle Vektoren der Form $\vec{b_0 c}$, $b_0, c \in B$, b_0 fest, zusammenfassen:

$$\mathfrak{L}(V(B)) = \mathfrak{L}(\{\vec{b_0 c}\}_{c \in B}) \qquad (b_0 \in B \text{ fest}) \,. \tag{17}$$

Aus diesen Überlegungen und Folgerung 4.3 ergibt sich sofort

Folgerung 4. *Es sei $B = \{b_0, b_1, \ldots, b_k\} \subset \boldsymbol{A}$ eine Menge aus $k+1$ Punkten. Dann gilt $\dim \boldsymbol{H}(B) \leqq k$, wobei das Gleichheitszeichen genau dann zutrifft, wenn die Folge $(\vec{b_0 b_i})_{i=1,\ldots,k}$ linear unabhängig ist.* □

Definition 5. Man sagt, die $k+1$ Punkte $b_0, b_1, \ldots, b_k$ hätten *allgemeine Lage*, wenn die Vektorfolge $(\vec{b_0 b_i})_{i=1,\ldots,k}$ linear unabhängig ist. Offenbar gilt

Folgerung 5. *Auf jeder k-Ebene gibt es $k+1$ Punkte in allgemeiner Lage, während je l ihrer Punkte, $l > k+1$, nicht in allgemeiner Lage sind. Durch je $k+1$ Punkte in allgemeiner Lage geht eine und nur eine k-Ebene.* □

Beispiel 3. Die Grundpunkte $p_0, p_i = p_0 + \mathfrak{b}_i$ eines k-Beins sind stets in allgemeiner Lage. Jede Teilmenge $B' \subseteq B$ einer Menge B von Punkten in allgemeiner Lage, $B' \neq \emptyset$, ist selbst in allgemeiner Lage. Die Grundpunkte einer affinen Skala einer Geraden, die Ecken eines Dreiecks oder die Ecken eines Tetraeders befinden sich in allgemeiner Lage.

Übung 1. Im affinen Punktraum $\boldsymbol{A}^n$ über $\mathbf{R}$ gebe man eine Menge $M \neq \emptyset$ an, die keine Ebene ist und für die $V(M)$ (nach (4)) ein k-dimensionaler Unterraum von $\boldsymbol{V}^n$ ist.

Übung 2. Es sei $(o; a_i)$ ein n-Bein des $\boldsymbol{A}^n$, (ξ_i) seien die zugehörigen Punktkoordinaten, $\gamma, \beta_i \in K$, wenigstens ein $\beta_i \neq 0$. Man beweise, daß die Menge der Punkte

$$x = o + \sum_{i=1}^{n} a_i \xi_i \in \boldsymbol{A}^n,$$

deren Koordinaten der linearen Gleichung

$$\sum_{i=1}^{n} \beta_i \xi_i = \gamma \tag{18}$$

genügen, eine Hyperebene ist. (Hinweis. Ist etwa $\beta_n \neq 0$, so ergeben sich schon $n-1$ der Gleichungen (8) durch die Festsetzung $\xi_\varkappa = \tau_\varkappa$ $(\varkappa = 1, \ldots, n-1)$; die n-te erhält man aus diesen und durch Umstellung von (18). Man bilde nach (6) die Vektoren $\mathfrak{b}_\varkappa$ und beweise deren lineare Unabhängigkeit.) Nach Satz 2 läßt sich also die Lösungsmenge eines lösbaren linearen Gleichungssystems (vgl. § 2.9) als eine Ebene des affinen Raumes $\boldsymbol{K}^n$ (vgl. Beispiel 3.1) geometrisch deuten.

Übung 3. Es sei eine Abbildung

$$f\colon (\tau_\varkappa) \in K^k \mapsto x = a + \sum_{\varkappa=1}^{k} \mathfrak{b}_\varkappa \tau_\varkappa \in \boldsymbol{A}^n$$

der Gestalt (5), aber *ohne* Voraussetzung der linearen Unabhängigkeit der $\mathfrak{b}_\varkappa$ gegeben. Man beweise, daß $f(K^k)$ eine l-Ebene für ein gewisses $l \leqq k$ ist.

Übung 4. Es sei $[\boldsymbol{A}^n, \boldsymbol{V}^n, K]$ eine affine Geometrie, $n \geqq 2$, char $K \neq 2$. Man beweise: Eine Punktmenge $H \subset \boldsymbol{A}^n$, $H \neq \emptyset$, ist eine Ebene dann und nur dann, wenn mit je zwei Punkten $p, q \in H$ auch die Verbindungsgerade $\boldsymbol{H}(p, q)$ in H enthalten ist. (Hinweis. Man beweise zuerst, daß die Vektormenge $V(H)$ von H ein Unterraum von $\boldsymbol{V}^n$ ist.) Ferner zeige man an einem Gegenbeispiel, daß im Fall char $K = 2$ diese Behauptung falsch ist.

Übung 5. Es sei $[\boldsymbol{A}, \boldsymbol{V}, K]$ eine affine Geometrie. Ein Paar $(p, \lambda) \in \boldsymbol{A} \times K$ nennen wir einen *Massepunkt mit der Masse* λ. Es sei $(M, \mu) := ((p_i, \mu_i))_{i=0,1,\ldots,k}$ eine endliche Familie von Massepunkten mit der Gesamtmasse $\mu = \sum_{i=0}^{k} \mu_i \neq 0$. a) Man beweise: Der durch

$$\overrightarrow{os} := \mu^{-1} \sum_{i=0}^{k} \overrightarrow{op_i} \mu_i \tag{19}$$

definierte Punkt s hängt nicht von der Wahl des Punktes $o \in \boldsymbol{A}$ ab; s heißt der *Schwerpunkt der Massepunkte* (M, μ). Setzen wir $\nu_i = \mu_i/\mu$, so gilt $\sum_{i=0}^{k} \nu_i = 1$, und auf Grund unseres Ergebnisses ist die Definition

$$s := \sum_{i=0}^{k} p_i \nu_i \quad \text{mit} \quad \sum_{i=0}^{k} \nu_i = 1 \tag{20}$$

einer *Linearkombination von $k+1$ Punkten mit der Koeffizientensumme* 1 sinnvoll. Im Fall $K = \mathbf{R}$ und $\mu_i \geqq 0$ erhalten wir den physikalischen Begriff des Schwerpunktes von $k+1$ Massepunkten. Ist char $K = 0$, so heißt

$$s = (k+1)^{-1} \sum_{i=0}^{k} p_i \tag{21}$$

der *affine Schwerpunkt* der Punkte p_i, $i = 0, 1, \ldots, k$, die man sich als Massepunkte mit der Masse $\mu_i = 1$ vorstellt. — b) Es sei

$$S(p_0, p_1, \ldots, p_k) := \left\{ s \mid s = \sum_{i=0}^{k} p_i \nu_i,\ \nu_i \in K,\ \sum_{i=0}^{k} \nu_i = 1 \right\} \tag{22}$$

die Menge aller möglichen Schwerpunkte, die durch Belegung der Punkte p_i mit den Massen ν_i der Gesamtmasse 1 entstehen. Man beweise $S(p_0, p_1, ..., p_k) = \boldsymbol{H}(\{p_0, p_1, ..., p_k\})$. — c) Man beweise: In der Darstellung (20) sind die Koeffizienten ν_i für jedes $s \in \boldsymbol{H}(\{p_0, p_1, ..., p_k\})$ eindeutig bestimmt genau dann, wenn die Punkte $\{p_0, p_1, ..., p_k\}$ allgemeine Lage haben. In diesem Fall nennt man die Menge $\{p_0, p_1, ..., p_k\}$ auch ein *k-Simplex*, die Folge $(p_0, p_1, ..., p_k)$ ein *geordnetes k-Simplex* und die Tupel $(\nu_0, \nu_1, ..., \nu_k) \in K^{k+1}$ die *baryzentrischen Koordinaten des Punktes* $s \in \boldsymbol{H}(\{p_0, p_1, ..., p_k\})$ bezüglich des k-Simplex $(p_0, p_1, ..., p_k)$. — d) Man betrachte den Fall $K = \mathbf{R}$, $k = n = 2$ und mache sich die in Abb. 5 angedeuteten Vorzeichen der Koeffizienten ν_i klar.

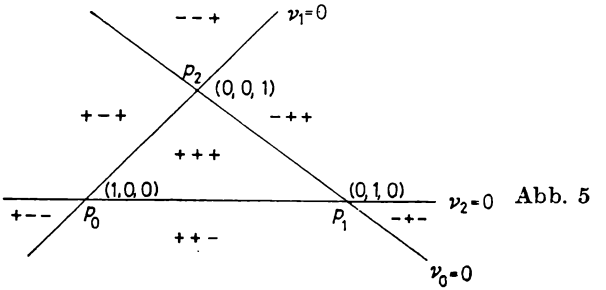


Abb. 5

Übung 6. Es seien $M = ((p_i, \mu_i))_{i=0,1,...,k}$, $N = ((q_j, \nu_j))_{j=0,1,...,l}$ zwei Familien von Massepunkten und $M \circ N$ die durch Aneinanderreihung von M und N entstehende Familie; dabei seien die Gesamtmassen μ, ν und $\mu + \nu$ alle von 0 verschieden. Dann kann man den Schwerpunkt der Familie $M \circ N$ bilden, indem man die Schwerpunkte der Familien M und N mit den Massen μ bzw. ν belegt und von diesen beiden Massepunkten den Schwerpunkt bildet:

$$s(M \circ N) = (\mu + \nu)^{-1} (s(M)\, \mu + s(N)\, \nu) . \tag{23}$$

b) Es sei $B = \{p_0, p_1, ..., p_k\}$ ein k-Simplex. Unter der *i-ten Seite* B_i des *k-Simplex* B versteht man das $(k-1)$-Simplex $B_i = B \setminus \{p_i\}$. Es sei $s_i := s(B_i)$ der affine Schwerpunkt der Seite B_i (char $K = 0$); er hängt offenbar nicht von der Wahl der Reihenfolge der Punkte von B_i ab. Man beweise: Die Verbindungsgeraden $\boldsymbol{H}(p_i, s_i)$ gehen alle durch den Schwerpunkt $s = s(B)$ des k-Simplex B, der die Strecken (p_i, s_i) im Verhältnis $1/k$ teilt: $\overrightarrow{p_i s} = \overrightarrow{s s_i} \cdot k$. (Das ist eine Verallgemeinerung des Satzes über die Seitenhalbierenden eines Dreiecks; mit Hilfe von a) finde man andere Verallgemeinerungen.) — c) Man zeige unter der Voraussetzung char $K = 0$: Das k-Simplex $(s_0, s_1, ..., s_k)$ ist zu $(p_0, p_1, ..., p_k)$ homothetisch, d. h., es gibt eine Homothetie $f \in \mathfrak{H}(\boldsymbol{A})$ mit $f(p_i) = s_i$, $i = 0, 1, ..., k$. — d) Man verallgemeinere die Aussagen b) und c) auf beliebige endliche Punktfolgen $(p_0, p_1, ..., p_k)$, $k \in \mathbf{N}$, eines affinen Raumes $\boldsymbol{A}^n$. (Bemerkung. Im Fall $\dim \boldsymbol{A} = 1$ ist die Definition 3.4 der Homothetien nicht anwendbar. Daher definiert man in diesem Fall die Gruppe $\mathfrak{H}(\boldsymbol{A})$ durch $\mathfrak{H}(\boldsymbol{A}) := \mathfrak{T}(\boldsymbol{A}) \cdot \mathfrak{D}_0$; man zeigt leicht, daß $\mathfrak{H}(\boldsymbol{A}^1)$ eine Gruppe ist, für die die Aussagen von Übung 3.5 gültig sind.)

Übung 7. Es sei char $K \neq 2$. Man beweise: Die Mittelpunkte der Seiten eines eigentlichen Vierecks des affinen Raumes bilden ein Parallelogramm (vgl. Übung 3.2). (Bemerkung. Unter dem *Mittelpunkt* einer Strecke (a, b) versteht man in der affinen Geometrie ihren affinen Schwerpunkt $s = a + \overrightarrow{ab}/2$.)

Übung 8. Man beweise: a) Sind $\boldsymbol{M}, \boldsymbol{H} \subseteq \boldsymbol{A}$ Ebenen und gilt $\boldsymbol{M} \parallel \boldsymbol{H}$ (nach Definition 3), so gibt es ein $a \in \boldsymbol{V}$ mit $t_a(\boldsymbol{M}) \subseteq \boldsymbol{H}$. — b) Sind $\boldsymbol{M}^k, \boldsymbol{H}^k \subseteq \boldsymbol{A}$ Ebenen derselben Dimension k, so gilt $\boldsymbol{M}^k \parallel \boldsymbol{H}^k$ (nach Definition 3) genau dann, wenn ein $a \in \boldsymbol{V}$ existiert mit $t_a(\boldsymbol{M}^k) = \boldsymbol{H}^k$

§ 6. Dimensionssätze und Steinitzscher Austauschsatz

Es seien $\boldsymbol{H}^k, \boldsymbol{M}^l \subseteq \boldsymbol{A}$ zwei Ebenen eines affinen Raumes $\boldsymbol{A}$ über einem beliebigen Körper K. Die kleinste Ebene, die $\boldsymbol{H}^k \cup \boldsymbol{M}^l$ enthält, heißt die *Verbindungsebene von* $\boldsymbol{H}^k$ *und* $\boldsymbol{M}^l$. Bezeichnen wir sie mit $\boldsymbol{H}^k \vee \boldsymbol{M}^l$, so ist nach Definition 5.4

$$\boldsymbol{H}^k \vee \boldsymbol{M}^l := \boldsymbol{H}(\boldsymbol{H}^k \cup \boldsymbol{M}^l) . \tag{1}$$

Wir stellen uns für diesen Paragraphen die Aufgabe, die Dimension der Verbindungsebene zu untersuchen. Es ist anschaulich klar, daß sie von der Dimension des Durchschnitts $\boldsymbol{H}^k \cap \boldsymbol{M}^l$ abhängen wird; je größer der Durchschnitt ist, um so kleiner wird die Verbindungsebene sein. Diese Erwartung bestätigt sich in der Tat, wenn $\boldsymbol{H}^k$ *und* $\boldsymbol{M}^l$ *sich schneiden*, d. h. $\boldsymbol{H}^k \cap \boldsymbol{M}^l \neq \emptyset$ gilt. Falls die Ebenen sich nicht schneiden, muß man eine etwas feinere Untersuchung anstellen. Wir orientieren uns an einigen Beispielen im $\boldsymbol{A}^3$. Sind $\boldsymbol{H}^k, \boldsymbol{M}^l$ Punkte, so ist ihre Verbindungsgerade auch die Verbindungsebene. Es seien nun $\boldsymbol{H}^1, \boldsymbol{M}^1$ Geraden, z. B. die Kanten eines Würfels (Abb. 6); $\boldsymbol{H}_1$ und $\boldsymbol{H}_2$ schneiden sich, ihre Verbindungsebene $\boldsymbol{C}^2$ ist zweidimensional; $\boldsymbol{M}_1$ und $\boldsymbol{H}_1$ sind parallel, ihre Verbindungsebene $\boldsymbol{B}^2$ ist

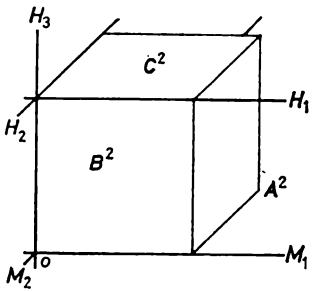


Abb. 6

ebenfalls zweidimensional; $\boldsymbol{M}_1$ und $\boldsymbol{H}_2$ sind *windschief*, d. h., sie schneiden sich nicht und sind nicht parallel, ihre Verbindungsebene ist der ganze Raum $\boldsymbol{A}^3$. Für eine Ebene und eine Gerade gibt es im $\boldsymbol{A}^3$ folgende Lagemöglichkeiten: $\boldsymbol{H}_1 \subset \boldsymbol{B}^2$, $\boldsymbol{H}_3 \cap \boldsymbol{A}^2 = \{o\}$ oder $\boldsymbol{H}_1 \cap \boldsymbol{A}^2 = \emptyset$, in dem letzten Fall gilt notwendig $\boldsymbol{H}_1 \parallel \boldsymbol{A}^2$. Für Ebenen des $\boldsymbol{A}^3$ gibt es nur zwei Möglichkeiten: Entweder sie schneiden sich in einer Geraden, oder sie sind parallel. Alle diese Aussagen werden sich als Spezialfälle der in diesem Paragraphen herzuleitenden Sätze ergeben. Wir betrachten nun zuerst den Fall sich schneidender Ebenen und beweisen

Satz 1. *Es sei* $\boldsymbol{H}^k \cap \boldsymbol{M}^l \neq \emptyset$. *Bezeichnet wie in* (5.4) $V(\boldsymbol{L})$ *den zu der Ebene* $\boldsymbol{L}$ *gehörigen Vektorraum* (Satz 5.1, c)), *so gilt*

$$V(\boldsymbol{H} \cap \boldsymbol{M}) = V(\boldsymbol{H}) \cap V(\boldsymbol{M}) , \tag{2}$$

$$V(\boldsymbol{H} \vee \boldsymbol{M}) = V(\boldsymbol{H}) + V(\boldsymbol{M}) . \tag{3}$$

Beweis. Man beachte, daß die Dimension der Ebenen bei diesem Beweis keine Rolle spielt, sie kann sogar unendlich sein. Die Formel (2) ist ein Spezialfall von

(5.9). Zum Beweis von (3) setzen wir zur Abkürzung $\boldsymbol{U} := V(\boldsymbol{H})$, $\boldsymbol{W} := V(\boldsymbol{M})$ und definieren den Unterraum $\boldsymbol{P} := \boldsymbol{U} + \boldsymbol{W} = \{\mathfrak{x} = \mathfrak{u} + \mathfrak{w} \mid \mathfrak{u} \in \boldsymbol{U}, \mathfrak{w} \in \boldsymbol{W}\}$, vgl. Übung 2.4. Nach Voraussetzung existiert ein Punkt $a \in \boldsymbol{H} \cap \boldsymbol{M}$. Definieren wir $\boldsymbol{L} := a + \boldsymbol{P}$, so ergibt sich (3) unmittelbar aus $\boldsymbol{H} \vee \boldsymbol{M} = \boldsymbol{L}$. Zum Beweis dieser Identität beachten wir $\boldsymbol{U} \subseteq \boldsymbol{P}$, woraus $\boldsymbol{H} = a + \boldsymbol{U} \subseteq a + \boldsymbol{P} = \boldsymbol{L}$ folgt. Analog gilt $\boldsymbol{M} \subseteq \boldsymbol{L}$, also $\boldsymbol{H} \cup \boldsymbol{M} \subseteq \boldsymbol{L}$ und nach Folgerung 5.3 auch $\boldsymbol{H} \vee \boldsymbol{M} \subseteq \boldsymbol{L}$. Zum Beweis der umgekehrten Relation $\boldsymbol{L} \subseteq \boldsymbol{H} \vee \boldsymbol{M}$ betrachten wir eine beliebige Ebene $\boldsymbol{N}$ mit $\boldsymbol{H} \cup \boldsymbol{M} \subseteq \boldsymbol{N}$. Wegen der Monotonie der Bildung der Vektormenge gilt $\boldsymbol{U} = V(\boldsymbol{H}) \subseteq V(\boldsymbol{H} \cup \boldsymbol{M}) \subseteq V(\boldsymbol{N})$ und analog $\boldsymbol{W} \subseteq V(\boldsymbol{N})$. Da $V(\boldsymbol{N})$ als Vektormenge einer Ebene ein Unterraum ist, folgt $\boldsymbol{P} = \boldsymbol{U} + \boldsymbol{W} \subseteq V(\boldsymbol{N})$, also $\boldsymbol{L} = a + \boldsymbol{P} \subseteq a + V(\boldsymbol{N}) = \boldsymbol{N}$; denn es gilt $a \in \boldsymbol{H} \cap \boldsymbol{M} \subset \boldsymbol{N}$. Also ist $\boldsymbol{L}$ in der Tat die kleinste Ebene, die $\boldsymbol{H} \cup \boldsymbol{M}$ enthält. □

Satz 1 reduziert unsere Aufgabe für den Fall $\boldsymbol{H} \cap \boldsymbol{M} \neq \emptyset$ auf ein Problem für die Unterräume $\boldsymbol{U}, \boldsymbol{W} \subseteq \boldsymbol{V}$. Zur Bestimmung der Dimension eines Unterraumes müssen wir eine Basis des Unterraumes finden. Wir wollen nun eine Basis von $\boldsymbol{U} + \boldsymbol{W}$ so wählen, daß gleichzeitig geeignete ihrer Teilmengen Basen von $\boldsymbol{U}, \boldsymbol{W}$ bzw. $\boldsymbol{U} \cap \boldsymbol{W}$ sind. Die Möglichkeit dieser *Basisanpassung* liegt in dem folgenden wichtigen Satz, der sehr viele Anwendungen besitzt:

Satz 2 (Steinitzscher Austauschsatz. *Es sei $\boldsymbol{V}$ ein Vektorraum über dem Körper K, B eine Basis von $\boldsymbol{V}$ und $C_k = \{\mathfrak{c}_1, \ldots, \mathfrak{c}_k\} \subset \boldsymbol{V}$ eine linear unabhängige Menge. Dann gibt es eine Teilmenge aus k Elementen $B_k = \{\mathfrak{b}_1, \ldots, \mathfrak{b}_k\} \subseteq B$, so daß*

$$B_k' := (B \setminus B_k) \cup C_k \tag{4}$$

wieder eine Basis von $\boldsymbol{V}$ ist.

Beweis. Wir führen den Beweis durch Induktion nach k. Für $k = 0$ ist die Behauptung trivial. Angenommen, der Satz sei schon für $k-1$ bewiesen. Wir zerlegen $C_k = C_{k-1} \cup \{\mathfrak{c}_k\}$. Nach Induktionsannahme gibt es eine Basis $B_{k-1}' = (B \setminus B_{k-1}) \cup C_{k-1}$; denn C_{k-1} ist als Teilmenge einer linear unabhängigen Menge selbst linear unabhängig. Unsere Aufgabe besteht nun darin, den Vektor $\mathfrak{c}_k$ gegen einen Vektor aus $B \setminus B_{k-1}$ auszutauschen. Dazu betrachten wir die Basisdarstellung von $\mathfrak{c}_k$ bezüglich der Basis B_{k-1}'

$$\mathfrak{c}_k = \sum_{\mathfrak{b} \in B \setminus B_{k-1}} \mathfrak{b}\zeta_{\mathfrak{b}} + \sum_{\lambda=1}^{k-1} \mathfrak{c}_\lambda \xi_\lambda \,. \tag{5}$$

Da C_k linear unabhängig ist, muß wenigstens einer der Koeffizienten $\zeta_{\mathfrak{b}}$ dieser Darstellung von 0 verschieden sein. Wir wählen ein solches $\mathfrak{b}_k = \mathfrak{b} \in B \setminus B_{k-1}$, setzen $B_k := B_{k-1} \cup \{\mathfrak{b}_k\}$ und definieren die Vektormenge B_k' nach (4). Zuerst zeigen wir, daß B_k' linear unabhängig ist. Es sei also

$$\mathfrak{o} = \sum_{\mathfrak{b} \in B \setminus B_k} \mathfrak{b}\sigma_{\mathfrak{b}} + \sum_{\lambda=1}^{k} \mathfrak{c}_\lambda \eta_\lambda \tag{6}$$

eine Linearkombination des Nullvektors durch Vektoren aus B_k'. Setzen wir in (6) für $\mathfrak{c}_k$ den Ausdruck (5) ein und ordnen nach den Elementen der Basis B_{k-1}', so er-

gibt sich die Darstellung

$$\mathfrak{o}=\sum_{\mathfrak{b}\in B\setminus B_k}\mathfrak{b}\,(\sigma_{\mathfrak{b}}+\eta_k\zeta_{\mathfrak{b}})+\mathfrak{b}_k\eta_k\zeta_{\mathfrak{b}_k}+\sum_{k-1}^{k-1}\mathfrak{c}_\lambda\,(\eta_\lambda+\eta_k\xi_\lambda) \tag{7}$$

des Nullvektors, die trivial sein muß. Wegen $\zeta_{\mathfrak{b}_k}\neq 0$ muß $\eta_k=0$ gelten, und (6) reduziert sich auf eine Linearkombination aus der Menge $(B\setminus B_k)\cup C_{k-1}\subseteq B'_{k-1}$, die als Teilmenge einer Basis linear unabhängig ist, so daß also überhaupt alle Koeffizienten in (6) gleich 0 sind. Als letztes ist noch zu zeigen, daß B'_k eine erzeugende Menge ist. Bringen wir in (5) alle Glieder der rechten Seite außer $\mathfrak{b}_k\zeta_{\mathfrak{b}_k}$ auf die linke und dividieren durch $\zeta_{\mathfrak{b}_k}$, so erhalten wir $\mathfrak{b}_k$ als Linearkombination aus B'_k, d. h. $\mathfrak{b}_k\in\mathfrak{L}(B'_k)$. Andererseits gilt $(B\setminus B_k)\cup C_{k-1}\subseteq B'_k\subseteq\mathfrak{L}(B'_k)$ und daher

$$B'_{k-1}=(B\setminus B_k)\cup\{\mathfrak{b}_k\}\cup C_{k-1}\subseteq\mathfrak{L}(B'_k).$$

Weil B'_{k-1} eine Basis ist, folgt $V=\mathfrak{L}(B'_{k-1})\subseteq\mathfrak{L}(B'_k)=V$. □

Folgerung 1 (Basisergänzungssatz). *Ist $U^k\subset V^n$ ein k-dimensionaler Unterraum des n-dimensionalen Vektorraumes V^n und $C_k\subset U^k$ eine Basis von U^k, so gibt es eine Basis B von V^n mit $C_k\subset B$.*

Zum Beweis nehme man irgendeine Basis von V^n und tausche eine geeignete Teilmenge gegen C_k aus. □

Bemerkung. Beachtet man das Resultat von Übung 4.7, so erkennt man, daß Folgerung 1 auch für unendlichdimensionale Vektorräume V (und endlichdimensionale U^k) gilt.

Satz 3. *Es seien $U^k, W^l\subseteq V$ endlichdimensionale Unterräume. Dann gilt*

$$\dim(U^k+W^l)+\dim(U^k\cap W^l)=\dim U^k+\dim W^l. \tag{8}$$

Beweis. Es sei etwa $s=\dim U\cap W$ und $t=\dim U+W$. Wir wählen eine Basis $\{\mathfrak{a}_1,\ldots,\mathfrak{a}_s\}$ von $U\cap W$, ergänzen sie einerseits durch $\{\mathfrak{b}_{s+1},\ldots,\mathfrak{b}_k\}$ zu einer Basis von U und andererseits durch $\{\mathfrak{c}_{s+1},\ldots,\mathfrak{c}_l\}$ zu einer Basis von W. Mit diesen Vektoren bilden wir die Folge

$$(\mathfrak{a}_1,\ldots,\mathfrak{a}_s,\mathfrak{b}_{s+1},\ldots,\mathfrak{b}_k,\mathfrak{c}_{s+1},\ldots,c_l) \tag{9}$$

und beweisen, daß sie linear unabhängig ist (Übung 4.3). In der Tat, es sei

$$\mathfrak{o}=\sum_{\sigma=1}^{s}\mathfrak{a}_\sigma\alpha_\sigma+\sum_{\varkappa=s+1}^{k}\mathfrak{b}_\varkappa\beta_\varkappa+\sum_{\lambda=s+1}^{l}\mathfrak{c}_\lambda\gamma_\lambda \tag{10}$$

eine Linearkombination des Nullvektors aus der Folge (9). Dann liegt der Vektor

$$\mathfrak{x}=\sum_{\sigma=1}^{s}\mathfrak{a}_\sigma\alpha_\sigma+\sum_{\varkappa=s+1}^{k}\mathfrak{b}_\varkappa\beta_\varkappa=-\sum_{\lambda=s+1}^{l}\mathfrak{c}_\lambda\gamma_\lambda \tag{11}$$

im Durchschnitt $U\cap W\subseteq W$. Weil nun $\{\mathfrak{a}_1,\ldots,\mathfrak{a}_s,\mathfrak{c}_{s+1},\ldots,\mathfrak{c}_l\}$ eine Basis von W und die Teilmenge $\{\mathfrak{a}_1,\ldots,\mathfrak{a}_s\}$ eine Basis von $U\cap W$ ist, muß $\mathfrak{x}$ schon aus dieser Teil-

menge linear kombinierbar sein, woraus wegen (11) $\gamma_\lambda = 0$, also $\mathfrak{x} = \mathfrak{o}$, folgt. Weil nun die Vektoren $\{\mathfrak{a}_1, \ldots, \mathfrak{a}_s, \mathfrak{b}_{s+1}, \ldots, \mathfrak{b}_k\}$ eine Basis von $\boldsymbol{U}$ bilden, müssen auch die Koeffizienten α_σ, $\beta_\varkappa$ alle gleich 0 sein. Andererseits erzeugt die Folge (9) den Unterraum $\boldsymbol{U}+\boldsymbol{W}$; denn sie entsteht durch Vereinigung der Basen der Summanden $\boldsymbol{U}$, $\boldsymbol{W}$. Somit ist (9) eine Basis für $\boldsymbol{U}+\boldsymbol{W}$, und es folgt die Behauptung $t = k+l-s$. □

Wir wenden uns nun wieder den Ebenen zu und beweisen zuerst folgendes Kriterium:

Lemma 1. *Es sei $\boldsymbol{A}$ ein affiner Punktraum und $\boldsymbol{H} = a + \boldsymbol{U}$, $\boldsymbol{M} = b + \boldsymbol{W}$ seien Ebenen in $\boldsymbol{A}$. Dann gilt*

$$\boldsymbol{H} \cap \boldsymbol{M} \neq \emptyset \Leftrightarrow \vec{ab} \in \boldsymbol{U} + \boldsymbol{W} . \tag{12}$$

Beweis. Es sei $c \in \boldsymbol{H} \cap \boldsymbol{M}$. Dann gibt es Vektoren $\mathfrak{u} \in \boldsymbol{U}$, $\mathfrak{w} \in \boldsymbol{W}$ mit $c = a + \mathfrak{u} = b + \mathfrak{w}$, also $\vec{ab} = \mathfrak{u} - \mathfrak{w} \in \boldsymbol{U} + \boldsymbol{W}$. Ist andererseits $\vec{ab} = \mathfrak{u} - \mathfrak{w} \in \boldsymbol{U} + \boldsymbol{W}$, so folgt $\vec{ab} + \mathfrak{w} = \mathfrak{u}$, also $a + \mathfrak{u} = b + \mathfrak{w} \in \boldsymbol{H} \cap \boldsymbol{M}$. □

Satz 4. *Es seien $\boldsymbol{H}^k$, $\boldsymbol{M}^l$ endlichdimensionale Ebenen des affinen Punktraumes $\boldsymbol{A}$. Dann gilt:*

a) *Ist $\boldsymbol{H}^k \cap \boldsymbol{M}^l \neq \emptyset$, so ist*

$$\dim \boldsymbol{H}^k \vee \boldsymbol{M}^l = \dim \boldsymbol{H}^k + \dim \boldsymbol{M}^l - \dim \boldsymbol{H}^k \cap \boldsymbol{M}^l . \tag{13}$$

b) *Wenn $\boldsymbol{H}^k \cap \boldsymbol{M}^l = \emptyset$ gilt, ist*

$$\dim \boldsymbol{H}^k \vee \boldsymbol{M}^l = \dim \boldsymbol{H}^k + \dim \boldsymbol{M}^l - \dim \boldsymbol{U}^k \cap \boldsymbol{W}^l + 1 ; \tag{14}$$

hierbei bezeichnen $\boldsymbol{U}^k$ und $\boldsymbol{W}^l$ die Vektorräume von $\boldsymbol{H}^k$ bzw. $\boldsymbol{M}^l$.

Beweis. Teil a) des Satzes folgt unmittelbar aus Satz 1 und der Dimensionsformel (8) für Vektorräume. Für den Beweis von b) zeigen wir zuerst folgendes: *Ist $\boldsymbol{H} = a + \boldsymbol{U}$ und $\boldsymbol{M} = b + \boldsymbol{W}$, so gilt*

$$\boldsymbol{H} \vee \boldsymbol{M} = a + (\mathfrak{L}(\{\vec{ab}\}) + \boldsymbol{U} + \boldsymbol{W}) . \tag{15}$$

Es sei nämlich $\boldsymbol{P} := \mathfrak{L}(\{\vec{ab}\}) + \boldsymbol{U} + \boldsymbol{W}$. Wegen $\{a\} \cup \{b\} \cup \boldsymbol{H} \cup \boldsymbol{M} \subseteq \boldsymbol{H} \vee \boldsymbol{M}$ gilt $\boldsymbol{P} \subseteq V(\boldsymbol{H} \vee \boldsymbol{M})$, also $a + \boldsymbol{P} \subseteq \boldsymbol{H} \vee \boldsymbol{M}$. Andererseits ist $\boldsymbol{H} = a + \boldsymbol{U} \subseteq a + \boldsymbol{P}$ wegen $\boldsymbol{U} \subseteq \boldsymbol{P}$, $\boldsymbol{M} = b + \boldsymbol{W} = (a + \vec{ab}) + \boldsymbol{W} \subseteq a + \boldsymbol{P}$ wegen $\vec{ab} \in \boldsymbol{P}$, $\boldsymbol{W} \subseteq \boldsymbol{P}$. Somit gilt $\boldsymbol{H} \cup \boldsymbol{M} \subseteq a + \boldsymbol{P}$, und damit ist $\boldsymbol{H} \vee \boldsymbol{M} = a + \boldsymbol{P}$. Zum Beweis von (14) ist $\dim \boldsymbol{P}$ zu berechnen. Wegen $\boldsymbol{H} \cap \boldsymbol{M} = \emptyset$ gilt nach Lemma 1 $\vec{ab} \notin \boldsymbol{U}^k + \boldsymbol{W}^l$, also $\mathfrak{o} \neq \vec{ab}$ und $\mathfrak{L}(\{\vec{ab}\}) \cap (\boldsymbol{U} + \boldsymbol{W}) = \{\mathfrak{o}\}$. Aus (8) folgt $\dim \boldsymbol{P} = \dim (\boldsymbol{U} + \boldsymbol{W}) + 1$. Wendet man nun die Dimensionsformel (8) noch einmal auf $\boldsymbol{U} + \boldsymbol{W}$ an, so erhält man (14). □

Durch (13) bzw. (14) hängen die Dimensionen $\dim \boldsymbol{H}^k \vee \boldsymbol{M}^l$ und $\dim \boldsymbol{U}^k \cap \boldsymbol{W}^l$ zusammen. Ist der umgebende affine Raum n-dimensional, $\boldsymbol{H}^k$, $\boldsymbol{M}^l \subseteq \boldsymbol{A}^n$, so gilt außerdem

$$0 \leqq \dim \boldsymbol{H}^k \vee \boldsymbol{M}^l \leqq n . \tag{16}$$

Anhand von geeignet gewählten Koordinatenebenen zeigt man leicht, daß *alle* den Beziehungen (13), (14) und (16) genügenden Fälle wirklich vorkommen. Für die folgenden Beispiele knüpfen wir an Beispiel 5.2 an und definieren mit $b = o + \mathfrak{a}_n$

$$\boldsymbol{M}_{i_1 \dots i_l} := o + \boldsymbol{W}_{i_1 \dots i_l}, \qquad \boldsymbol{H}_{j_1 \dots j_k} := b + \boldsymbol{W}_{j_1 \dots j_k} . \tag{17}$$

Wir verabreden noch die folgende Redeweise: Zwei Ebenen $\boldsymbol{M}, \boldsymbol{H}$ heißen *windschief zueinander*, wenn $\boldsymbol{M} \cap \boldsymbol{H} = \emptyset$ gilt und weder $\boldsymbol{H}$ zu $\boldsymbol{M}$ noch $\boldsymbol{M}$ zu $\boldsymbol{H}$ parallel ist.

Beispiel 1. Ist $\boldsymbol{H}^0 = \{a\}$ ein Punkt und $\boldsymbol{M}^l$ eine l-Ebene, so gilt $\{a\} \vee \boldsymbol{M}^l = \boldsymbol{M}^l$ genau dann, wenn $a \in \boldsymbol{M}^l$ ist, und dim $\{a\} \vee \boldsymbol{M}^l = l + 1$ sonst.

Beispiel 2. Für $n \geqq 2$ betrachten wir zwei Geraden. Es gibt folgende Möglichkeiten (Abb. 6): $\boldsymbol{M}_1 \cap \boldsymbol{M}_2 = \{o\}$, sich schneidende Geraden; $\boldsymbol{M}_1 \parallel \boldsymbol{H}_1$ disjunkte parallele Geraden; falls $n \geqq 3$ ist, noch windschiefe Geraden $\boldsymbol{M}_1$, $\boldsymbol{H}_2$. Wegen dim $(\boldsymbol{H}^1 \vee \boldsymbol{M}^1) \leqq 3$ ergeben sich auch für große n keine weiteren Lagemöglichkeiten. Für die Dimensionen der Verbindungsebenen erhalten wir entsprechend: dim $\boldsymbol{M}_1 \vee \boldsymbol{M}_2 =$ dim $\boldsymbol{M}_1 \vee \boldsymbol{H}_1 = 2$, dim $\boldsymbol{M}_1 \vee \boldsymbol{H}_2 = 3$.

Beispiel 3. Für eine 2-Ebene und eine Gerade gibt es die Lagemöglichkeiten:

1. $\boldsymbol{M}_1 \subseteqq \boldsymbol{M}_{12}$, dim $\boldsymbol{M}_1 \vee \boldsymbol{M}_{12} = 2 \qquad (n \geqq 2)$;
2. $\boldsymbol{M}_3 \cap \boldsymbol{M}_{12} = \{o\}$, dim $\boldsymbol{M}_3 \vee \boldsymbol{M}_{12} = 3 \qquad (n \geqq 3)$;
3. $\boldsymbol{H}_1 \cap \boldsymbol{M}_{12} = \emptyset$, $\boldsymbol{H}_1 \parallel \boldsymbol{M}_{12}$, dim $\boldsymbol{H}_1 \vee \boldsymbol{M}_{12} = 3 \qquad (n \geqq 3)$;
4. $\boldsymbol{H}_3$ windschief zu $\boldsymbol{M}_{12}$, dim $\boldsymbol{H}_3 \vee \boldsymbol{M}_{12} = 4 \qquad (n \geqq 4)$.

Beispiel 4. Im $\boldsymbol{A}^n$, $n \geqq 5$, sind $(\boldsymbol{M}_{12}, \boldsymbol{H}_{23})$ und $(\boldsymbol{M}_{12}, \boldsymbol{H}_{34})$ je ein zueinander windschiefes 2-Ebenenpaar; dabei gilt

$$\dim \boldsymbol{M}_{12} \vee \boldsymbol{H}_{23} = 4, \qquad \dim \boldsymbol{M}_{12} \vee \boldsymbol{H}_{34} = 5 . \tag{18}$$

Übung 1. In Verallgemeinerung der Beispiele 1 bis 4 zeige man, daß jeder der (13), (14), (16) genügenden Fälle mit Hilfe geeigneter Ebenen der Form (17) realisiert werden kann.

Übung 2. Anknüpfend an Beispiel 5.2 betrachten wir die beliebigen Koordinatenebenen $\boldsymbol{M}(a)_{i_1 \dots i_k} := a + \boldsymbol{W}_{i_1 \dots i_k}$ für $a \in \boldsymbol{A}^n$. a) Man beweise für $\boldsymbol{N} = \boldsymbol{M}(a)_{i_1 \dots i_k}$ und $\boldsymbol{L} = \boldsymbol{M}(b)_{j_1 \dots j_l}$: Ist $c \in \boldsymbol{N} \cap \boldsymbol{L}$, so gilt

$$\boldsymbol{L} \cap \boldsymbol{N} = \boldsymbol{M}(c)_{\{i_1, \dots, i_k\} \cap \{j_1, \dots, j_l\}} \quad \text{und} \quad \boldsymbol{L} \vee \boldsymbol{N} = \boldsymbol{M}(c)_{\{i_1, \dots, i_k\} \cup \{j_1, \dots, j_l\}}.$$

(Man beachte, daß $\boldsymbol{M}(a)_{i_1 \dots i_k}$ nur von der Menge $\{i_1, \dots, i_k\}$ und nicht von der Folge abhängt, so daß die angegebenen Ausdrücke sinnvoll sind.) — b) Ist $\boldsymbol{L} \cap \boldsymbol{N} = \emptyset$, so gilt: $\boldsymbol{L} \vee \boldsymbol{N}$ ist eine Koordinatenebene dann und nur dann, wenn eine Koordinatenlinie $\boldsymbol{M}(c)_i$ existiert mit $\boldsymbol{L} \cap \boldsymbol{M}(c)_i \neq \emptyset$ und $\boldsymbol{N} \cap \boldsymbol{M}(c)_i \neq \emptyset$.

Übung 3. Es sei K ein Körper und $P_n \subset K[x]$ der Vektorraum der Polynome über K vom Grade $\leqq n$. Für Elemente $\alpha_\varrho \in K$ definieren wir durch $W(\alpha_1, \dots, \alpha_r)$ die Menge aller derjenigen Polynome $f \in P_n$, für die $f(\alpha_\varrho) = 0$ gilt für $\varrho = 1, 2, \dots, r$. a) Man beweise: $W(\alpha_1, \dots, \alpha_r)$ ist ein Unterraum von P_n. — b) Man finde eine Basis B' von $W(\alpha_1, \dots, \alpha_r)$ und ergänze sie zu einer Basis $B \supseteqq B'$ von P_n. — c) Für zwei derartige Unterräume bestimme man die Dimension dim $(W(\alpha_1, \dots, \alpha_r) + W(\beta_1, \dots, \beta_s))$. (Hinweis. Für diese Aufgabe beachte man Beispiel 2.5.)

Übung 4. Es sei V^n ein n-dimensionaler Vektorraum über K. Man beweise: Ist $W \subset V^n$ ein echter Unterraum, so gibt es eine Basis $\{\mathfrak{b}_i\}$, $i=1, ..., n$, von V^n mit $\{\mathfrak{b}_i\} \cap W = \emptyset$.

Übung 5. Es seien $U, W \subseteq V$ Unterräume des Vektorraumes V, und es gelte dim U + + dim W = dim $V < \infty$. Man beweise, daß die folgenden Aussagen äquivalent sind: 1. $U \cap W = \{0\}$; – 2. $U + W = V$; – 3. U und W sind *zueinander komplementäre Unterräume*, d. h., es gilt

$$V = U \oplus W, \tag{19}$$

vgl. Definition 4.4.5.

Übung 6. Es sei $U \subseteq V$ ein Unterraum und dim $V < \infty$. Man zeige, daß in V ein zu U komplementärer Unterraum W von V existiert.

Übung 7. Man beweise Folgerung 1 und Satz 3 ohne Benutzung des Steinitzschen Austauschsatzes aus den Ergebnissen von § 4.

§ 7. Volumen und Determinanten

In diesem Paragraphen wird der Begriff des Volumens eines Parallelepipeds, auf den sich letztlich alle allgemeineren Volumenbegriffe stützen, in die affine Geometrie eingeführt. Einfache geometrische Eigenschaften des Volumens, die wir uns am Beispiel des Flächeninhalts von Parallelogrammen veranschaulichen können, führen uns auf den Begriff der Determinante, die ein algebraischer Ausdruck für die Berechnung des Volumens ist. Die Determinanten finden nicht nur in der Geometrie, sondern in fast allen Gebieten der Mathematik wichtige Anwendungen.

Wir betrachten eine n-dimensionale affine Geometrie $[A^n, V^n, K]$. Zur anschaulichen Motivierung wollen wir besonders an den Fall $n=2$ und $K=\mathbf{R}$ denken. Es sei $p_0 \in A^n$, und $\mathfrak{b}_1, ..., \mathfrak{b}_n$ seien n Vektoren aus V^n. Das Tupel

$$\Pi = \Pi(p_0; \mathfrak{b}_i) \in A^n \times (V^n)^n \tag{1}$$

heißt ein *Parallelepiped des* A^n. Die 2^n Punkte

$$p = p_0 + \sum_{i=1}^{n} \mathfrak{b}_i \varepsilon_i, \qquad \varepsilon_i = 0, 1, \qquad i = 1, ..., n,$$

heißen die *Eckpunkte* des Parallelepipeds. Im Fall $K=\mathbf{R}$ versteht man unter dem von $(p_0; \mathfrak{b}_i)$ aufgespannten Parallelepiped häufig auch die Punktmenge

$$Q(\Pi) := \left\{ x \mid \overrightarrow{p_0 x} = \sum_{i=1}^{n} \mathfrak{b}_i \xi_i,\ 0 \leq \xi_i \leq 1 \right\} \subseteq A^n,$$

die offenbar durch Π eindeutig bestimmt ist. Man beachte jedoch, daß es bei der Definition (1) von Π auf die Reihenfolge der Vektoren $\mathfrak{b}_i$ ankommt; will man den Unterschied betonen, so nennt man (1) ein *orientiertes Parallelepiped*. Wir wollen im folgenden stets die Definition (1) zugrunde legen. Offenbar ist jedes n-Bein des A^n ein Parallelepiped, aber nicht umgekehrt. Ein Parallelepiped Π heißt *ausgeartet*,

wenn die Vektoren $(\mathfrak{b}_i)$ linear abhängig sind. Für $n=1$ erhalten wir die *Strecken* und für $n=2$ die *Parallelogramme* als Spezialfälle unserer Definition. Bei einer Translation $t_\mathfrak{a}: x \in \boldsymbol{A}^n \mapsto x+\mathfrak{a} \in \boldsymbol{A}^n$ ist das Bild eines Parallelepipeds wieder ein Parallelepiped, und zwar gilt

$$t_\mathfrak{a} \Pi(p_0; \mathfrak{b}_i) = \Pi(p_0+\mathfrak{a}; \mathfrak{b}_i) . \tag{2}$$

Das *Volumen eines Parallelepipeds* Π ist ein Element $v(\Pi) \in K$. Aus der Elementargeometrie entnehmen wir die folgende sehr natürliche Forderung: *Das Volumen* $v(\Pi)$ *ändert sich bei Translationen nicht:*

$$v(t_\mathfrak{a}(\Pi)) = v(\Pi) . \tag{3}$$

Da wir durch $\mathfrak{a} = \overrightarrow{p_0 q}$ den Eckpunkt p_0 in jeden beliebigen anderen Punkt $q \in \boldsymbol{A}^n$ parallel verschieben können, folgt aus (3), daß das Volumen nicht von dem Punkt p_0, sondern nur von den Π aufspannenden Vektoren $(\mathfrak{b}_i)$ abhängen kann. Für die Volumenfunktion ist die folgende Schreibweise üblich:

$$v(\Pi(p_0; \mathfrak{b}_i)) = [\mathfrak{b}_1, \ldots, \mathfrak{b}_n] . \tag{4}$$

Definition 1. Unter einer *Volumenfunktion* über einem Vektorraum $\boldsymbol{V}^n$ versteht man eine Abbildung $(\mathfrak{x}_1, \ldots, \mathfrak{x}_n) \in (\boldsymbol{V}^n)^n \to [\mathfrak{x}_1, \ldots, \mathfrak{x}_n] \in K$, die jedem n-Tupel von Vektoren aus $\boldsymbol{V}^n$ ein Element aus K, das von ihnen aufgespannte *Volumen*, zuordnet und die folgenden Eigenschaften besitzt:

(I) Es gibt n Vektoren $(\mathfrak{e}_i)$, deren Volumen 1 ist:

$$[\mathfrak{e}_1, \ldots, \mathfrak{e}_n] = 1 . \tag{5}$$

(II) Die Volumenfunktion ist *linear* in jedem Argument, d. h., es gelten für $i=1, \ldots, n$, alle $\lambda \in K$ und alle $\mathfrak{x}_i, \mathfrak{y}_i \in \boldsymbol{V}^n$ die folgenden Rechenregeln:

$$[\mathfrak{x}_1, \ldots, \mathfrak{x}_i \lambda, \ldots, \mathfrak{x}_n] = [\mathfrak{x}_1, \ldots, \mathfrak{x}_i, \ldots, \mathfrak{x}_n] \cdot \lambda , \tag{6}$$

$$[\mathfrak{x}_1, \ldots, \mathfrak{x}_i + \mathfrak{y}_i, \ldots, \mathfrak{x}_n] = [\mathfrak{x}_1, \ldots, \mathfrak{x}_i, \ldots, \mathfrak{x}_n] + [\mathfrak{x}_1, \ldots, \mathfrak{y}_i, \ldots, \mathfrak{x}_n] . \tag{7}$$

(III) Wenn irgend zwei der Argumente gleich sind, ist das Volumen 0: Aus $\mathfrak{x}_i = \mathfrak{x}_j = \mathfrak{c}$ für $i \neq j$ folgt $[\mathfrak{x}_1, \ldots, \mathfrak{x}_n] = 0$, d. h.

$$[\mathfrak{x}_1, \ldots, \underset{i}{\mathfrak{c}}, \ldots, \underset{j}{\mathfrak{c}}, \ldots, \mathfrak{x}_n] = 0 . \tag{8}$$

Zur Motivierung dieser Definition bemerken wir folgendes: (I) bedeutet die Existenz eines Einheitsvolumens; hierdurch wird gesichert, daß das Volumen nicht identisch gleich 0 sein kann. Wegen (6) könnte man (5) auch durch diese letzte Eigen-

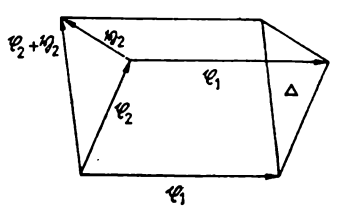


Abb. 7

schaft ersetzen. Die Forderung (II) bedeutet eine Dehnungseigenschaft (6) des Volumens und seine Additivität (7); für $n=2$ zeigt Abb. 7, wie das große Parallelogramm durch Translation des Dreiecks Δ aus den beiden kleinen entsteht. Wenn zwei der Vektoren gleich sind, ist das Parallelepiped ausgeartet, und sein Volumen soll daher 0 sein.

Während in der Elementargeometrie das Volumen in der Regel als eine nichtnegative Zahl definiert wird, folgt aus (II), daß eine Volumenfunktion stets auch negative Werte annimmt ($K=\mathbf{R}$). Um diesen Unterschied hervorzuheben, spricht man vom *orientierten* Volumen $v(\Pi)$; es wird z. B. bei der Begründung des Integrals angewandt. Das elementare Volumen erhält man durch Übergang zum absoluten Betrag $|v(\Pi)|$; dabei geht jedoch die Eigenschaft (II) verloren. Im folgenden gehen wir stets von dem Volumenbegriff der Definition 1 aus.

Als erste Aufgabe haben wir die Frage nach Existenz und Eindeutigkeit von Volumenfunktionen zu klären. Zunächst nehmen wir an, daß eine Volumenfunktion gegeben sei, und leiten aus den Forderungen (I) bis (III) die Determinante her. Indem wir die Determinante (17) zur Definition der Volumenfunktion verwenden und für sie die Eigenschaften (I) bis (III) verifizieren, beweisen wir die Existenz.

Satz 1. *Eine Volumenfunktion ändert ihren Wert nicht, wenn man zu einem Argument $\mathfrak{x}_i$ das Vielfache $\mathfrak{x}_j\lambda$, $\lambda\in K$, eines anderen Argumentes addiert:*

$$[\mathfrak{x}_1, \dots, \mathfrak{x}_i+\mathfrak{x}_j\lambda, \dots, \mathfrak{x}_j, \dots, \mathfrak{x}_n]=[\mathfrak{x}_1, \dots, \mathfrak{x}_i, \dots, \mathfrak{x}_j, \dots, \mathfrak{x}_n], \qquad i\neq j\,. \tag{9}$$

Der Beweis folgt unmittelbar aus (II) und (III). □

Satz 2. *Es sei* $P=\begin{pmatrix}1 & \dots & n\\ j_1 & \dots & j_n\end{pmatrix}\in S_n$ *eine Permutation. Dann gilt*

$$[\mathfrak{x}_{j_1}, \dots, \mathfrak{x}_{j_n}]=\operatorname{sgn}(P)\cdot[\mathfrak{x}_1, \dots, \mathfrak{x}_n]\,, \tag{10}$$

wobei sgn (P) *das Signum der Permutation P bedeutet.*

Beweis. Da sich jede Permutation als Produkt von Transpositionen darstellen läßt (vgl. § 1.2), genügt es zu zeigen: *Bei einer Vertauschung zweier Argumente ändert das Volumen sein Vorzeichen.* Weil alle Argumente der Volumenfunktion die gleiche Rolle spielen, genügt es, irgend zwei, z. B. die beiden ersten, zu betrachten. Nach (7) und (8) gilt

$$\begin{aligned}0&=[\mathfrak{a}+\mathfrak{b}, \mathfrak{a}+\mathfrak{b}, \dots]\\ &=[\mathfrak{a}, \mathfrak{a}, \dots]+[\mathfrak{a}, \mathfrak{b}, \dots]+[\mathfrak{b}, \mathfrak{a}, \dots]+[\mathfrak{b}, \mathfrak{b}, \dots]\,.\end{aligned}$$

Wieder nach (8) sind die beiden äußeren Glieder auf der rechten Seite dieser Gleichung 0, und es folgt

$$[\mathfrak{a}, \mathfrak{b}, \dots]=-[\mathfrak{b}, \mathfrak{a}, \dots] \tag{11}$$

woraus sich die Behauptung ergibt. □

Aus Formel (10) erkennt man, daß bei gegebener Volumenfunktion das Volumen

des Parallelepipeds nur unwesentlich, nämlich um einen Faktor ± 1, von der Reihenfolge der Vektoren $\mathfrak{b}_i$ abhängt.

Es sei nun $(\mathfrak{a}_1, ..., \mathfrak{a}_n)$ ein festes n-Bein von V^n. Wir stellen die variablen Vektoren $\mathfrak{x}_i \in V^n$, $i = 1, ..., n$, bezüglich dieses n-Beins dar:

$$\mathfrak{x}_i = \sum_{k=1}^{n} \mathfrak{a}_k \xi_{ki} . \tag{12}$$

Diese Ausdrücke setzen wir in die Volumenfunktion ein und vertauschen unter Benutzung der Linearität (II) die Bildung des Volumens mit der Addition (Regel (7)) und der Multiplikation mit Elementen aus K (Regel (6)). Es folgt

$$[\mathfrak{x}_1, ..., \mathfrak{x}_n] = \sum_{k_1,...,k_n=1}^{n} [\mathfrak{a}_{k_1}, ..., \mathfrak{a}_{k_n}] \, \xi_{k_1 1} \cdots \xi_{k_n n} . \tag{13}$$

Die Indizes k_i durchlaufen bei dieser Summation unabhängig voneinander die Werte $1, 2, ..., n$. Wir brauchen also nur noch die Werte der Volumenfunktion $[\mathfrak{a}_{k_1}, ..., \mathfrak{a}_{k_n}]$ für die Basisvektoren zu betrachten. Sind in diesem Ausdruck zwei Argumente gleich, so ist er nach (III) gleich 0 und braucht bei der Summation nicht berücksichtigt zu werden. Es bleiben also in (13) höchstens die Glieder übrig, für die $(k_1, ..., k_n)$ eine Permutation von $(1, ..., n)$ ist, und auf diese können wir (10) anwenden. Dann ergibt sich

$$[\mathfrak{x}_1, ..., \mathfrak{x}_n] = [\mathfrak{a}_1, ..., \mathfrak{a}_n] \sum_{P \in S_n} \operatorname{sgn} \begin{pmatrix} 1 & \cdots & n \\ k_1 & \cdots & k_n \end{pmatrix} \xi_{k_1 1} \cdots \xi_{k_n n} . \tag{14}$$

Die Summe auf der rechten Seite dieser Formel ist gerade die Determinante. Dazu erinnern wir an den Begriff einer Matrix, vgl. Beispiel 0.2.11, 3., und führen folgende Bezeichnungen ein:

Definition 2. Es sei D ein assoziativer Ring. Die Abbildungen

$$(\alpha, j) \in N_m \times N_n \mapsto d_{\alpha j} \in D \tag{15}$$

stellen wir in Form einer *Matrix* dar:

$$(d_{\alpha j}) = \begin{pmatrix} d_{11} & d_{12} & \cdots & d_{1n} \\ d_{21} & d_{22} & \cdots & d_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ d_{m1} & d_{m2} & \cdots & d_{mn} \end{pmatrix} . \tag{16}$$

Mit $\mathbf{M}_{m,n}(D)$ bezeichnen wir die Menge aller Matrizen mit m Zeilen und n Spalten und Elementen aus D. Ist $m = n$, so heißt die Matrix *quadratisch*; wir setzen $\mathbf{M}_n(D) := \mathbf{M}_{n,n}(D)$.

Definition 3. Es sei D ein assoziativer und kommutativer Ring. Dann wird durch

$$(d_{ij}) \in \mathbf{M}_n(D) \mapsto \det (d_{ij}) := \sum_{P \in S_n} \operatorname{sgn} (P) \, d_{j_1 1} \cdots d_{j_n n} , \tag{17}$$

wobei $P=\begin{pmatrix}1 & \dots & n\\ j_1 & \dots & j_n\end{pmatrix}\in S_n$ alle Permutationen der Ordnung n durchläuft, jeder quadratischen Matrix aus $\mathbf{M}_n(D)$ ein Element aus D zugeordnet, das man ihre *Determinante* nennt.

Der für uns wichtigste Fall ist der, daß $D=K$ ein Körper ist. Bilden wir aus (12) die Matrix $(\xi_{ki})\in\mathbf{M}_n(K)$, indem wir das n-Tupel der Vektorkoordinaten von $\mathfrak{x}_i$ als i-te Spalte dieser Matrix wählen, so erhalten wir aus der schon bewiesenen Formel (14)

Satz 3. *Es sei* $[\mathfrak{x}_1, \dots, \mathfrak{x}_n]$ *eine Volumenfunktion über dem Vektorraum* V^n *und* $(\mathfrak{a}_i)$ *ein n-Bein von* V^n. *Bezeichnet* $(\xi_{ki})\in\mathbf{M}_n(K)$ *die durch* (12) *eindeutig bestimmte Matrix der Vektorkoordinaten der* $(\mathfrak{x}_i)$, *so gilt*

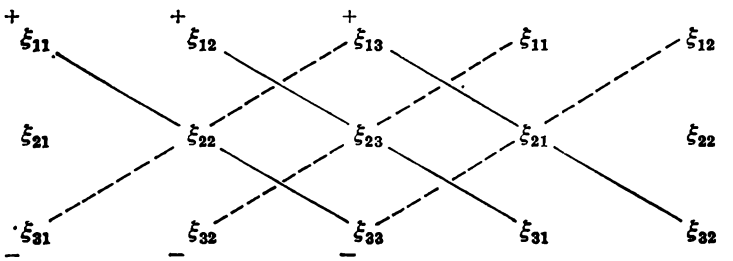
$$[\mathfrak{x}_1, \dots, \mathfrak{x}_n]=[\mathfrak{a}_1, \dots, \mathfrak{a}_n]\det(\xi_{ki}). \quad \square \tag{18}$$

Bemerkung. Statt der runden Klammern in (16) verwendet man auch häufig zwei senkrechte Striche auf jeder Seite der Tabelle. Schreibt man im Fall einer quadratischen Matrix statt der runden Klammern je einen senkrechten Strich, so meint man die Determinante dieser Matrix.

Beispiel 1. Für $n=1$ ist $\det(\xi_{ij})=\xi_{11}$ einfach das einzige Element dieser Matrix. Für $n=2$ gilt

$$\det(\xi_{ij})=\begin{vmatrix}\xi_{11} & \xi_{12}\\ \xi_{21} & \xi_{22}\end{vmatrix}=\xi_{11}\xi_{22}-\xi_{21}\xi_{12}\,. \tag{19}$$

Für $n=3$ läßt sich die Determinante nach der *Sarrusschen Regel* ebenfalls leicht direkt berechnen. Man schreibe die ersten beiden Spalten rechts neben die Matrix und ziehe alle sechs durch die drei Zeilen gehenden schrägen Linien:



Bildet man nun die Produkte der je drei durch die Striche verbundenen Elemente, versieht sie mit den angegebenen Vorzeichen und summiert, so erhält man die Determinante im Fall $n=3$:

$$\det(\xi_{ki})=\xi_{11}\xi_{22}\xi_{33}+\xi_{31}\xi_{12}\xi_{23}+\xi_{21}\xi_{32}\xi_{13}-\xi_{31}\xi_{22}\xi_{13}-\xi_{11}\xi_{32}\xi_{23}-\xi_{21}\xi_{12}\xi_{33}\,. \tag{20}$$

Für größere n werden wir im nächsten Paragraphen rationelle Verfahren zur Berechnung der Determinante angeben; man beachte, daß die Anzahl der Summanden in (17) gleich $n!$ ist. Zunächst beweisen wir eine wichtige Eigenschaft der Volumen-

funktionen, die ein Kriterium für die lineare Unabhängigkeit von n Vektoren des V^n darstellt:

Satz 4. *Es sei* $[\mathfrak{x}_1, ..., \mathfrak{x}_n]$ *eine Volumenfunktion über* V^n. *Dann sind die folgenden drei Aussagen äquivalent*:

1. *Die Vektorfolge* $(\mathfrak{b}_1, ..., \mathfrak{b}_n)$ *ist linear abhängig.*

2. $[\mathfrak{b}_1, ..., \mathfrak{b}_n] = 0$.

3. *Ist* (β_{ki}) *die Matrix der Vektorkoordinaten von* $(\mathfrak{b}_i)$ *bezüglich irgendeines n-Beins* $(\mathfrak{a}_k)$, *so gilt*

$$\det(\beta_{ki}) = 0 .$$

Beweis. Sind die $(\mathfrak{b}_i)$ linear abhängig, so können wir eines von ihnen, etwa $\mathfrak{b}_1$, durch die übrigen linear kombinieren:

$$\mathfrak{b}_1 = \sum_{\alpha=2}^{n} \mathfrak{b}_\alpha \lambda_\alpha . \tag{21}$$

Setzen wir das in die Volumenfunktion ein und benutzen ihre Eigenschaften (II) und (III), so folgt

$$[\mathfrak{b}_1, ..., \mathfrak{b}_n] = \sum_{\alpha=2}^{n} [\mathfrak{b}_\alpha, \mathfrak{b}_2, ..., \mathfrak{b}_n] \lambda_\alpha = 0 . \tag{22}$$

Damit gilt 2. Sind umgekehrt die $(\mathfrak{b}_i)$ linear unabhängig, so bilden sie selbst eine Basis, und wir können in (18) $\mathfrak{a}_i = \mathfrak{b}_i$ setzen. Wäre nun $[\mathfrak{b}_1, ..., \mathfrak{b}_n] = 0$, so würde die Volumenfunktion identisch gleich 0 sein, was der Eigenschaft (I) von Definition 1 widerspräche. Daher sind die Aussagen 1 und 2 äquivalent. Die Äquivalenz der Aussagen 2 und 3 ergibt sich sofort aus (18), wenn man beachtet, daß für das n-Bein $(\mathfrak{a}_i)$ nach dem schon Bewiesenen $[\mathfrak{a}_1, ..., \mathfrak{a}_n]$ von 0 verschieden ist. □

Nun ist es leicht, den Satz über die Existenz und Eindeutigkeit einer Volumenfunktion zu beweisen:

Satz 5. *Es sei* $(\mathfrak{a}_k)$ *ein n-Bein des Vektorraumes* V^n. *Dann gibt es eine und nur eine Volumenfunktion, nämlich*

$$[\mathfrak{x}_1, ..., \mathfrak{x}_n] := \det(\xi_{ki}) , \tag{23}$$

für die $[\mathfrak{a}_1, ..., \mathfrak{a}_n] = 1$ *gilt. Hierbei bezeichnet* $(\xi_{ki}) \in \mathbf{M}_n(K)$ *die Matrix der Vektorkoordinaten der* $\mathfrak{x}_i$ *bezüglich ihrer Basisdarstellungen* (12) *im n-Bein* $(\mathfrak{a}_k)$.

Beweis. Wenn eine Volumenfunktion mit den geforderten Eigenschaften existiert, muß sie nach Satz 3, (18), notwendig die Gestalt (23) besitzen; sie ist daher eindeutig bestimmt. Wir betrachten nun (23) als Definition der Volumenfunktion und weisen nach, daß sie die Eigenschaften (I) bis (III) besitzt. Zum Beweis von (I) stellen wir die Vektoren $\mathfrak{a}_i$ im n-Bein $(\mathfrak{a}_k)$ dar:

$$\mathfrak{a}_i = \sum_{k=1}^{n} \mathfrak{a}_k \delta_{ki} . \tag{24}$$

Hierbei bezeichnet δ_{ki} das *Kronecker-Symbol*, das durch

$$\delta_{ki} := 1 \quad \text{für} \quad k = i, \qquad \delta_{ki} := 0 \quad \text{für} \quad k \neq i \tag{25}$$

definiert wird; die zugehörige Matrix heißt die *Einheitsmatrix*. Sie hat die Gestalt

$$(\delta_{ki}) = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix}. \tag{26}$$

Setzt man ihre Elemente in die Definitionsgleichung (17) der Determinante ein, so erkennt man, daß nur ein einziger von 0 verschiedener Summand übrig bleibt, nämlich der, der zur identischen Permutation $\begin{pmatrix} 1 & \dots & n \\ 1 & \dots & n \end{pmatrix}$ gehört, und dieser ist 1. Also gilt

$$[\mathfrak{a}_1, \dots, \mathfrak{a}_n] = \det(\delta_{ki}) = 1 \,. \tag{27}$$

Zum Beweis von (II) bemerken wir zuerst, daß man die Eigenschaften der *Homogenität* (6) und der *Additivität* (7) in einer einzigen Formel, der *Linearität*

$$[\mathfrak{x}_1, \dots, \underset{i}{\mathfrak{y}\lambda + \mathfrak{z}\mu}, \dots, \mathfrak{x}_n] = [\mathfrak{x}_1, \dots, \underset{i}{\mathfrak{y}}, \dots, \mathfrak{x}_n]\,\lambda + [\mathfrak{x}_1, \dots, \underset{i}{\mathfrak{z}}, \dots, \mathfrak{x}_n]\,\mu \tag{28}$$

ausdrücken kann, die für alle Argumente $i = 1, \dots, n$, alle $\lambda, \mu \in K$ und beliebige Vektoren $\mathfrak{x}_i, \mathfrak{y}, \mathfrak{z} \in \boldsymbol{V}^n$ gelten muß. Da alle Argumente die gleiche Rolle spielen, genügt es, (28) etwa für das erste Argument zu beweisen. Setzen wir $\mathfrak{x}_1 = \mathfrak{y}\lambda + \mathfrak{z}\mu$ und sind

$$\mathfrak{y} = \sum_{k=1}^{n} \mathfrak{a}_k \eta_k, \qquad \mathfrak{z} = \sum_{k=1}^{n} \mathfrak{a}_k \zeta_k \tag{29}$$

die Basisdarstellungen von $\mathfrak{y}$ bzw. $\mathfrak{z}$ in dem n-Bein $(\mathfrak{a}_k)$, so gilt für die Vektorkoordinaten des ersten Arguments

$$\xi_{k_1 1} = \eta_{k_1}\lambda + \zeta_{k_1}\mu \,. \tag{30}$$

Setzen wir nun die Vektorkoordinaten in die Definition (17) der Determinante ein, so folgt unmittelbar (II):

$$\begin{aligned} [\mathfrak{y}\lambda + \mathfrak{z}\mu, \mathfrak{x}_2, \dots, \mathfrak{x}_n] &= \sum \operatorname{sgn}(P)\,(\eta_{k_1}\lambda + \zeta_{k_1}\mu)\,\xi_{k_2 2} \dots \xi_{k_n n} \\ &= (\sum \operatorname{sgn}(P)\,\eta_{k_1}\xi_{k_2 2} \dots \xi_{k_n n})\,\lambda \\ &\quad + (\sum \operatorname{sgn}(P)\,\zeta_{k_1}\xi_{k_2 2} \dots \xi_{k_n n})\,\mu \\ &= [\mathfrak{y}, \mathfrak{x}_2, \dots, \mathfrak{x}_n]\,\lambda + [\mathfrak{z}, \mathfrak{x}_2, \dots, \mathfrak{x}_n]\,\mu. \end{aligned}$$

Zum Beweis von (III) genügt es wieder, etwa die ersten beiden Argumente zu betrachten. Es sei also $\mathfrak{x}_1 = \mathfrak{x}_2 = \mathfrak{y}$ mit der Basisdarstellung (30). Multiplizieren wir jede Permutation $P \in S_n$ von rechts mit der Transposition $T = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 2 & 1 & 3 & \dots & n \end{pmatrix}$,

so erhalten wir die bijektive Abbildung

$$P=\begin{pmatrix}1 & 2 & \dots & n\\ k_1 & k_2 & \dots & k_n\end{pmatrix}\in S_n \mapsto P'=PT=\begin{pmatrix}1 & 2 & \dots & n\\ k_2 & k_1 & \dots & k_n\end{pmatrix}\in S_n\,. \tag{31}$$

Durchläuft also P die Untergruppe A_n der geraden Permutationen, so durchläuft die Menge $\{P, P'\}$ ganz S_n; denn die Abbildung (31) ordnet jeder geraden Permutation eine ungerade zu und umgekehrt. Beachten wir nun $\operatorname{sgn}(P)+\operatorname{sgn}(P')=0$, so folgt

$$\begin{aligned}[\mathfrak{y}, \mathfrak{y}, \mathfrak{x}_3, \dots, \mathfrak{x}_n] &= \sum_{P\in S_n} \operatorname{sgn}(P)\, \eta_{k_1}\eta_{k_2}\xi_{k_3 3}\dots\xi_{k_n n}\\ &= \sum_{P\in A_n} (\operatorname{sgn}(P)+\operatorname{sgn}(P'))\, \eta_{k_1}\eta_{k_2}\xi_{k_3 3}\dots\xi_{k_n n}=0\,. \quad \square\end{aligned}$$

Damit ist Satz 5 bewiesen. Den Kern des Existenzbeweises können wir auch folgendermaßen zusammenfassen:

Folgerung 1. *Betrachten wir die Determinante als Funktion ihrer n Spaltenvektoren* $\mathfrak{x}_i=(\xi_{ki})_{k=1,\dots,n}\in K^n$, *so ist sie die Volumenfunktion über den Vektorraum* K^n, *die dem Standard-n-Bein* $(\mathfrak{e}_i)$ (vgl. Folgerung 4.4) *das Volumen* 1 *zuordnet.* $\square$

Folgerung 2. *Zwei Volumenfunktionen über demselben Vektorraum* $\boldsymbol{V}^n$ *unterscheiden sich nur durch einen konstanten Faktor* $\varkappa\in K$, $\varkappa\neq 0$.

Beweis. Es bezeichne $[\mathfrak{x}_1, \dots, \mathfrak{x}_n]$ bzw. $((\mathfrak{x}_1, \dots, \mathfrak{x}_n))$ je eine Volumenfunktion über $\boldsymbol{V}^n$, und $(\mathfrak{a}_i)$ sei ein beliebiges n-Bein. Nach Satz 3, (18), und Satz 4 haben wir für beliebige $\mathfrak{x}_i\in\boldsymbol{V}^n$

$$((\mathfrak{x}_1, \dots, \mathfrak{x}_n))=((\mathfrak{a}_1, \dots, \mathfrak{a}_n))\det(\xi_{ki})=\varkappa[\mathfrak{x}_1, \dots, \mathfrak{x}_n] \tag{32}$$

mit

$$\varkappa=((\mathfrak{a}_1, \dots, \mathfrak{a}_n))/[\mathfrak{a}_1, \dots, \mathfrak{a}_n]\,. \quad \square \tag{33}$$

Das Volumen ist also in der affinen Geometrie nicht eindeutig definiert, sondern nur bis auf einen konstanten Faktor. Wegen Folgerung 2 gilt jedoch

Folgerung 3. *Das Volumenverhältnis* $v(\Pi(p, \mathfrak{b}_i))/v(\Pi(q, \mathfrak{c}_i))$ *zweier orientierter Parallelepipede hängt nicht von der Auswahl der Volumenfunktion ab.* $\square$

Bemerkung. Für den Vektorraum $\boldsymbol{W}^k$ einer k-Ebene $\boldsymbol{H}^k\subseteq\boldsymbol{A}^n$ können wir natürlich ebenfalls eine Volumenfunktion definieren. Gehört das orientierte Parallelepiped Π_k der Dimension k zu $\boldsymbol{H}^k$ und analog Π'_k zu der parallelen k-Ebene $\boldsymbol{H}'^k$ mit demselben Vektorraum $\boldsymbol{W}^k$, so ist das Volumenverhältnis $v(\Pi)/v(\Pi')$ bezüglich einer Volumenfunktion von $\boldsymbol{W}^k$ wohldefiniert und unabhängig von der Auswahl dieser Volumenfunktion (bei $v(\Pi')\neq 0$). Im Fall $k=1$ erhalten wir das schon in § 3 betrachtete *Streckenverhältnis* homothetischer Strecken. *Liegen die k-dimensionalen Parallelepipede nicht in zueinander parallelen k-Ebenen, so ist ein Vergleich der Volumina in der affinen Geometrie nicht möglich.*

Übung 1. Es seien $\boldsymbol{H}^k = \boldsymbol{H}(a; \mathfrak{b}_1, ..., \mathfrak{b}_k)$, $\boldsymbol{M}^l = \boldsymbol{H}(b; \mathfrak{c}_1, ..., \mathfrak{c}_l)$ zwei Ebenen des $\boldsymbol{A}^n$ mit $k+l=n-1$. Man beweise: Gilt

$$[\vec{ab}, \mathfrak{b}_1, ..., \mathfrak{b}_k, \mathfrak{c}_1, ..., \mathfrak{c}_l] \neq 0\,, \tag{34}$$

so sind $\boldsymbol{H}^k$, $\boldsymbol{M}^l$ windschief zueinander, und es ist $V(\boldsymbol{H}^k) \cap V(\boldsymbol{M}^l) = \{o\}$. Hiervon gilt auch die Umkehrung.

Als Anwendung wollen wir noch den Begriff der Orientierung für reelle Punkt- und Vektorräume erklären. Zwei n-Beine $(\mathfrak{a}_i)$, $(\mathfrak{b}_i)$ des n-dimensionalen Vektorraumes $\boldsymbol{V}_n$ heißen *gleichorientiert*, in Zeichen $(\mathfrak{a}_i) \sim (\mathfrak{b}_i)$, wenn bezüglich irgendeiner Volumenfunktion

$$[\mathfrak{a}_1, ..., \mathfrak{a}_n]/[\mathfrak{b}_1, ..., \mathfrak{b}_n] > 0 \tag{35}$$

gilt, und *entgegengesetzt orientiert* sonst.

Übung 2. Man beweise: Die Relation (35) ist unabhängig von der Wahl der Volumenfunktion. Sie ist eine Äquivalenzrelation. Die Menge aller n-Beine zerfällt in genau zwei Äquivalenzklassen.

Definition 4. Ein reeller Vektorraum $\boldsymbol{V}^n$ heißt *orientiert*, wenn in ihm eine der beiden Äquivalenzklassen als Menge der *positiv orientierten* n-Beine ausgezeichnet ist. Jede derartige Klasse heißt eine *Orientierung* von $\boldsymbol{V}^n$. Ein reeller affiner Punktraum heißt orientiert, wenn der zugehörige Vektorraum orientiert ist.

Beispiel 2. Im Fall $n=1$ entsprechen die beiden Orientierungen den möglichen Durchlaufungsrichtungen der Gerade $\boldsymbol{A}^1$. Für die Ebene $n=2$ sind die beiden 2-Beine der Abb. 8 entgegengesetzt orientiert; man nimmt gewöhnlich die durch a) ge-

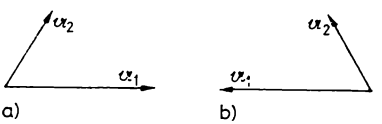


Abb. 8

gebene Orientierung der Zeichenebene als positiv an. Im $\boldsymbol{A}^3$ nennt man positiv zumeist die Orientierung, die der Reihenfolge Daumen, Zeigefinger, Mittelfinger der rechten Hand entspricht (Abb. 9a); die Orientierung verallgemeinert also die Unterscheidung von rechts und links auf beliebige Dimensionen.

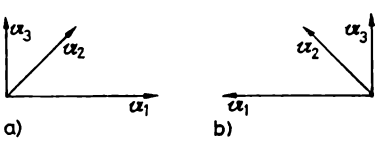


Abb. 9

Übung 3. Es sei $(\mathfrak{a}_i)$ ein n-Bein des reellen Vektorraumes $\boldsymbol{V}^n$. Man beweise: a) Ist $s: i \mapsto s_i$ eine Permutation $s \in S_n$ und gilt $\mathfrak{b}_i = \mathfrak{a}_{s_i}$, so ist $(\mathfrak{b}_i) \sim (\mathfrak{a}_i)$ genau dann, wenn $\operatorname{sgn} s = 1$ gilt. — b) Ist $\mathfrak{b}_i = \mathfrak{a}_i \varepsilon_i$, so ist $(\mathfrak{b}_i) \sim (\mathfrak{a}_i)$ genau dann, wenn $\prod_{i=1}^{n} \varepsilon_i > 0$ gilt $(\varepsilon_i \neq 0)$. — c) Allgemeiner, ist

$$\mathfrak{b}_j = \sum_{k=1}^{n} \alpha_k \beta_{kj}$$

die Darstellung von $\mathfrak{b}_j$ in der Basis $(\mathfrak{a}_k)$, so ist $(\mathfrak{b}_i) \sim (\mathfrak{a}_i)$ genau dann, wenn $\det(\beta_{kj}) > 0$ gilt.

Übung 4. Es sei D ein assoziativer, kommutativer Ring und D^n die Menge der n-Tupel aus Elementen von D. Man beweise: a) Die durch Definition 3 definierte Determinante, betrachtet als Funktion der Spalten-n-Tupel, hat die Eigenschaften (II), (III) einer Volumenfunktion über D^n; dabei sind die Operationen über D^n wie in Beispiel 1 erklärt. Besitzt D ein Einselement, so gilt auch Eigenschaft (I). — b) Es gelten die Analoga von Satz 1 und Satz 2. — c) Man zeige an einem Beispiel, daß das Analogon von Satz 4 nicht mehr gilt. — d) Für einen Integritätsbereich D formuliere und beweise man das Analogon von Satz 4. (Hinweis. Man gehe zum Quotientenkörper über (vgl. § 2.6). Falls die Lösung noch nicht gelingt, lese man erst den nächsten Paragraphen.)

§ 8. Eigenschaften von Determinanten und Methoden zu ihrer Berechnung

In diesem Paragraphen betrachten wir Determinanten von Matrizen mit Elementen aus einem Körper K oder einem assoziativen, kommutativen Ring D. Eine Matrix $(\beta_{ij}) \in \mathbf{M}_n(D)$ heißt eine *obere* (bzw. *untere*) *Dreiecksmatrix*, wenn $\beta_{ij} = 0$ gilt für $i > j$ (bzw. für $i < j$). Eine Matrix, die sowohl obere als auch untere Dreiecksmatrix ist, heißt eine *Diagonalmatrix*. Die Menge der Stellen (i, j) der Matrix, für die $i = j$ ist, nennt man die *Hauptdiagonale*. Für Dreiecksmatrizen ist die Berechnung der Determinante besonders einfach:

Satz 1. *Es sei* $(\beta_{ij}) \in \mathbf{M}_n(K)$ *eine Dreiecksmatrix. Dann ist* $\det(\beta_{ij})$ *das Produkt der in der Hauptdiagonale stehenden Elemente:*

$$\det(\beta_{ij}) = \beta_{11} \cdot \beta_{22} \dots \beta_{nn} . \tag{1}$$

Beweis. Wir betrachten etwa eine obere Dreiecksmatrix

$$\begin{pmatrix} \beta_{11} & \beta_{12} & \dots & \beta_{1n} \\ 0 & \beta_{22} & \dots & \beta_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & \beta_{nn} \end{pmatrix}. \tag{2}$$

Sind alle Summanden auf der rechten Seite der Definition (7.17) der Determinante 0, so ist die Determinante selbst und auch die rechte Seite von (1) gleich 0, und die Behauptung ist richtig. Es sei nun $\beta_{k_1 1} \dots \beta_{k_n n}$ ein von 0 verschiedener Summand. Wir zeigen, daß dann notwendig $k_1 = 1, \dots, k_n = n$ gelten muß. Dazu bemerken wir, daß in jedem beliebigen Summanden von (7.17) aus jeder Zeile und aus jeder Spalte der Matrix genau ein Element als Faktor vorkommt; die Determinante wird durch Summation über alle derartigen, noch mit dem entsprechenden Vorzeichen versehenen Produkte gebildet. Da nun $\beta_{kj} = 0$ ist für $k > j$, muß der erste Faktor unseres Produktes β_{11} sein. Es sei schon $k_1 = 1, \dots, k_s = s$ bewiesen. Ist $s < n$, so muß auch $k_{s+1} = s+1$ gelten; denn die Zahlen $1, \dots, s$ kommen nach In-

duktionsvoraussetzung in der Permutation

$$\begin{pmatrix} 1 & \dots & n \\ k_1 & \dots & k_n \end{pmatrix} = \begin{pmatrix} 1 & \dots & s & \dots & n \\ 1 & \dots & s & \dots & k_n \end{pmatrix}$$

bereits vor, und im Fall $k_{s+1} > s+1$ wäre der Summand 0. Weil die identische Permutation das Signum 1 hat, gilt (1). Den Fall einer unteren Dreiecksmatrix kann man analog erledigen; er ergibt sich aber auch als eine einfache Folgerung aus dem schon Bewiesenen und dem nächsten Satz. □

Definition 1. Es sei $(\beta_{\alpha j}) \in \mathbf{M}_{m,n}(D)$ eine Matrix vom Typ (m, n) mit Elementen aus der beliebigen Menge D. Unter *der zu* $(\beta_{\alpha j})$ *transponierten Matrix* $(\beta_{\alpha j})' \in \mathbf{M}_{n,m}(D)$ versteht man die durch Umklappen an der Hauptdiagonale entstehende Matrix, deren j-te Zeile gleich der j-ten Spalte der ursprünglichen Matrix ist:

$$(\beta_{\alpha j})' := (\gamma_{j\alpha}) \quad \text{mit} \quad \gamma_{j\alpha} := \beta_{\alpha j}, \qquad (\alpha, j) \in N_m \times N_n . \tag{3}$$

Der Übergang zur transponierten Matrix ist also eine bijektive Abbildung $' : \mathbf{M}_{m,n}(D) \to \mathbf{M}_{n,m}(D)$ mit der Eigenschaft

$$(\beta_{\alpha j})'' = (\beta_{\alpha j}) . \tag{4}$$

Satz 2. *Es sei D ein kommutativer, assoziativer Ring. Dann gilt für alle* $(\beta_{ij}) \in \mathbf{M}_n(D)$

$$\det (\beta_{ij})' = \det (\beta_{ij}) . \tag{5}$$

Beweis. Aus (3) und (7.17) erhalten wir für die Determinante der transponierten Matrix

$$\det (\beta_{ij})' = \sum_{P \in S_n} \operatorname{sgn} (P)\, \beta_{1 j_1} \dots \beta_{n j_n} . \tag{6}$$

Vertauschen wir nun in jedem Summanden die Reihenfolge der Faktoren so, daß $(j_1, \dots, j_n) \mapsto (1, \dots, n)$ in die natürliche Anordnung übergeht, d. h., wenden wir auf sie die zu $P = \begin{pmatrix} 1 & \dots & n \\ j_1 & \dots & j_n \end{pmatrix}$ inverse Permutation $P^{-1} = \begin{pmatrix} 1 & \dots & n \\ k_1 & \dots & k_n \end{pmatrix}$ an, so erhalten wir wegen $\operatorname{sgn} (P) = \operatorname{sgn} (P^{-1})$ und $\beta_{1 j_1} \dots \beta_{n j_n} = \beta_{k_1 1} \dots \beta_{k_n n}$ gerade den Ausdruck (7.17) für $\det (\beta_{ij})$. □

Aus Folgerung 7.1 und Satz 2 erhalten wir unmittelbar die entsprechende Aussage für die Determinante als Funktion der Zeilenvektoren:

Folgerung 1. *Betrachten wir die Determinante als Funktion ihrer n Zeilenvektoren $\mathfrak{z}_k = (\xi_{ki})_{i=1,\dots,n} \in K^n$, so ist sie die Volumenfunktion über dem Vektorraum K^n, die dem Standard-n-Bein $(\mathfrak{e}_k)$ das Volumen 1 zuordnet.* □

Nun können wir leicht eine *Methode zur Berechnung der Determinanten* angeben. Aus Satz 7.1, Folgerung 7.1 und der eben bewiesenen Folgerung 1 ergibt sich

Folgerung 2. *Eine Determinante* $\det (\beta_{ij})$, $(\beta_{ij}) \in \mathbf{M}_n(K)$, *ändert ihren Wert nicht, wenn man eine mit einem Element $\lambda \in K$ multiplizierte Zeile (bzw. Spalte) zu einer anderen Zeile (bzw. Spalte) von (β_{ij}) addiert.* □

Mit Hilfe dieser Operationen kann man analog wie beim Gaußschen Algorithmus (vgl. Satz 2.9.2) die Matrix auf Dreiecksgestalt bringen und dann nach Satz 1 den Wert der Determinante leicht bestimmen. Die elementaren Umformungen (I) und (II) aus Definition 2.9.3, die wir zur Umwandlung in eine Stufenmatrix (2.9.4) benötigten, entsprechen der Vertauschung von Zeilen, wobei natürlich die auftretenden Vorzeichenänderungen der Determinante berücksichtigt werden müssen, und den nach Folgerung 2 den Wert einer Determinante nicht ändernden Umformungen. Die Operation (III) wurde nur zur Herstellung der speziellen Stufenmatrix gebraucht; auf sie können wir daher verzichten. Man beachte, daß in (2.9.4) stets $k_\varrho \geqq \varrho$, $\varrho = 1, \ldots, r$, gilt, so daß (2.9.4) im Fall $m = n$ eine obere Dreiecksmatrix ist. Gegenüber dem Gaußschen Algorithmus kann man hier die Operationen nach Belieben auf die Zeilen oder Spalten anwenden; dasselbe gilt für die Rechenregeln (7.6) und (7.7). Schließlich erhält man aus Satz 7.4, daß eine Determinante 0 ist, wenn in einer Zeile (bzw. Spalte) nur Nullen stehen, oder allgemeiner, wenn zwischen ihren Zeilen (bzw. Spalten) eine lineare Abhängigkeit besteht. Kombinieren wir Satz 2 mit Satz 7.4, so ergibt sich

Folgerung 3. *Sind in einer Matrix* $(\beta_{ij}) \in \mathbf{M}_n(K)$ *die Zeilenvektoren linear abhängig, so sind es auch die Spaltenvektoren, und umgekehrt.* □

Ein weiteres Hilfsmittel zur Berechnung von Determinanten liefert uns der *Laplacesche Entwicklungssatz,* dessen Formulierung wir folgende Definition vorausschicken:

Definition 2. Es sei $(\beta_{\varkappa j}) \in \mathbf{M}_{m,n}(D)$ eine Matrix mit Elementen aus einem assoziativen Ring D, k eine natürliche Zahl mit $1 \leqq k \leqq \min(m, n)$, und $p_\varkappa$, $q_\varkappa$ seien natürliche Zahlen mit

$$1 \leqq p_1 < \ldots < p_k \leqq m, \qquad 1 \leqq q_1 < \ldots < q_k \leqq n\,. \tag{7}$$

Dann heißt

$$M\begin{pmatrix} p_1 & \cdots & p_k \\ q_1 & \cdots & q_k \end{pmatrix} := \begin{vmatrix} \beta_{p_1 q_1} & \beta_{p_1 q_2} & \cdots & \beta_{p_1 q_k} \\ \beta_{p_2 q_1} & \beta_{p_2 q_2} & \cdots & \beta_{p_2 q_k} \\ \cdots & \cdots & \cdots & \cdots \\ \beta_{p_k q_1} & \beta_{p_k q_2} & \cdots & \beta_{p_k q_k} \end{vmatrix} \tag{8}$$

ein *Minor k-ter Ordnung* der Matrix $(\beta_{\varkappa j})$. Der Minor (8) wird also gebildet, indem man in der Matrix $(\beta_{\varkappa j})$ alle Zeilen und Spalten streicht, deren Nummern von den $p_\varkappa$ bzw. $q_\varkappa$ verschieden sind; die restlichen Elemente bilden dann eine quadratische Matrix der Ordnung k, deren Determinante der Minor ist. Ist $(\beta_{ij}) \in \mathbf{M}_n(D)$ eine quadratische Matrix und sind $r_1 < \ldots < r_{n-k}$ bzw. $s_1 < \ldots < s_{n-k}$ gerade die natürlichen Zahlen mit $1 \leqq r_\lambda, s_\lambda \leqq n$, die in den Folgen (7) nicht vorkommen, so heißt

$$M'\begin{pmatrix} p_1 & \cdots & p_k \\ q_1 & \cdots & q_k \end{pmatrix} := M\begin{pmatrix} r_1 & \cdots & r_{n-k} \\ s_1 & \cdots & s_{n-k} \end{pmatrix} \tag{9}$$

der zu $M\begin{pmatrix} p_1 & \cdots & p_k \\ q_1 & \cdots & q_k \end{pmatrix}$ *komplementäre Minor.* Ist schließlich D ein kommutativer

assoziativer Ring, so heißt

$$A\begin{pmatrix} p_1 & \cdots & p_k \\ q_1 & \cdots & q_k \end{pmatrix} := M'\begin{pmatrix} p_1 & \cdots & p_k \\ q_1 & \cdots & q_k \end{pmatrix}(-1)^{\sum_{\varkappa=1}^{k}(p_\varkappa+q_\varkappa)} \tag{10}$$

die *Adjunkte* (auch das *algebraische Komplement*) des Minors $M\begin{pmatrix} p_1 & \cdots & p_k \\ q_1 & \cdots & q_k \end{pmatrix}$.

Diese auf den ersten Blick etwas künstliche Definition wird folgendermaßen gerechtfertigt: Hält man für $(\beta_{ij}) \in \mathbf{M}_n(D)$ ein Produkt, beispielsweise $\beta_{p_1q_1} \cdots \beta_{p_kq_k}$, das als Summand in den Minor (8) eingeht, fest, und betrachtet alle diejenigen Summanden der Determinante (7.17) $\det(\beta_{ij})$, die es als Faktor enthalten, so ist die Summe aller dieser Terme gleich

$$\pm\beta_{p_1q_1} \cdots \beta_{p_kq_k} \cdot M'\begin{pmatrix} p_1 & \cdots & p_k \\ q_1 & \cdots & q_k \end{pmatrix}.$$

Summiert man nun über alle derartigen Ausdrücke, die zu dem Minor (8) gehören, so entsteht ein Produkt der Form

$$\pm M\begin{pmatrix} p_1 & \cdots & p_k \\ q_1 & \cdots & q_k \end{pmatrix} \cdot M'\begin{pmatrix} p_1 & \cdots & p_k \\ q_1 & \cdots & q_k \end{pmatrix},$$

wobei allerdings zum Beweis der Richtigkeit dieser Aussage noch die Betrachtung der Vorzeichen der einzelnen Summanden gehört. Jedenfalls machen diese Überlegungen schon die Behauptung des *allgemeinen Laplaceschen Entwicklungssatzes* plausibel, der es gestattet, die Berechnung einer Determinante auf die Berechnung von Determinanten niedrigerer Ordnung zurückzuführen:

Satz 3. *Es sei D ein kommutativer assoziativer Ring und $(\beta_{ij}) \in \mathbf{M}_n(D)$ eine quadratische Matrix der Ordnung n. Ferner seien $p_\varkappa$ natürliche Zahlen mit $1 \leqq p_1 < \ldots < p_k \leqq n$. Dann gilt die folgende Formel für die Entwicklung einer Determinante nach den Zeilen $p_1, \ldots, p_k$:*

$$\det(\beta_{ij}) = \sum_{1 \leqq q_1 < \ldots < q_k \leqq n} M\begin{pmatrix} p_1 & \cdots & p_k \\ q_1 & \cdots & q_k \end{pmatrix} \cdot A\begin{pmatrix} p_1 & \cdots & p_k \\ q_1 & \cdots & q_k \end{pmatrix}. \tag{11}$$

Beweis. Wir betrachten zuerst den Spezialfall einer Matrix der Gestalt

$$(\beta_{ij}) = k\begin{pmatrix} \overset{k}{\beta_{\alpha\gamma}} & \overset{}{0} \\ \beta_{\varkappa\gamma} & \beta_{\varkappa\lambda} \end{pmatrix}, \tag{12}$$

für die also $\beta_{\alpha\lambda} = 0$ gilt für $\alpha = 1, \ldots, k$ und $\lambda = k+1, \ldots, n$. Für sie beweisen wir die Formel

$$\det\begin{pmatrix} \beta_{\alpha\gamma} & 0 \\ \beta_{\varkappa\gamma} & \beta_{\varkappa\gamma} \end{pmatrix} = \det(\beta_{\alpha\gamma}) \cdot \det(\beta_{\varkappa\lambda}). \tag{13}$$

Da für eine Matrix der Form (12) alle Minoren der Gestalt $M\begin{pmatrix} 1 & \cdots & k \\ q_1 & \cdots & q_k \end{pmatrix}$ außer dem

einen $M\begin{pmatrix}1 & \dots & k\\ 1 & \dots & k\end{pmatrix}$ gleich 0 sind – sie enthalten ja wenigstens eine Spalte aus lauter Nullen – ist (13) gerade ein Spezialfall von (11) bei Entwicklung der Determinante der Matrix (12) nach den ersten k Zeilen. Zum Beweis von (13) brauchen wir nur alle die Permutationen $P\in S_n$ zu betrachten, bei denen die Zahlen 1, ..., k und demzufolge auch die Zahlen $k+1$, ..., n untereinander permutiert werden; denn alle anderen Summanden von (7.17) sind wegen der speziellen Form (12) gleich 0. Diese Permutationen P lassen sich aber als Produkt zweier Permutationen $Q=\begin{pmatrix}1 & \dots & k\\ \alpha_1 & \dots & \alpha_k\end{pmatrix}\in S_k$ und $Q'=\begin{pmatrix}k+1 & \dots & n\\ \varkappa_{k+1} & \dots & \varkappa_n\end{pmatrix}\in S_{n-k}$ schreiben, wobei wir uns diese Gruppen als diejenigen Untergruppen von S_n realisiert denken, die die letzten $n-k$ bzw. die ersten k Zahlen der Folge 1, ..., n fest lassen. *Aus* $P=Q\cdot Q'$ ergibt sich

$$\operatorname{sgn}(P)=\operatorname{sgn}(Q)\cdot\operatorname{sgn}(Q'); \tag{14}$$

setzen wir das in (7.17) ein und berücksichtigen, daß wir nur noch über die $P=Q\cdot Q'$ zu summieren haben, für die $Q\in S_k$ und $Q'\in S_{n-k}$ beliebig sind, so folgt aus der Kommutativität der Multiplikation in D

$$\begin{aligned}\det(\beta_{ij}) &= \sum_{Q\in S_k, Q'\in S_{n-k}} \operatorname{sgn}(Q)\,\beta_{\alpha_1 1}\cdots\beta_{\alpha_k k}\operatorname{sgn}(Q')\,\beta_{\varkappa_{k+1}k+1}\cdots\beta_{\varkappa_n n}\\ &= \Big(\sum_{Q\in S_k}\operatorname{sgn}(Q)\,\beta_{\alpha_1 1}\cdots\beta_{\alpha_k k}\Big)\cdot\Big(\sum_{Q'\in S_{n-k}}\operatorname{sgn}(Q')\,\beta_{\varkappa_{k+1}k+1}\cdots\beta_{\varkappa_n n}\Big),\end{aligned}$$

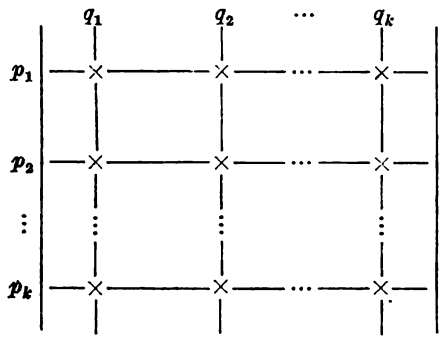
womit (13) bewiesen ist. Wir bemerken noch, daß bei einer Matrix der Gestalt (12) die Elemente $\beta_{\varkappa\nu}$ des linken unteren Blockes keinen Einfluß auf den Wert der Determinante haben, wir können sie also z. B. gleich 0 setzen.

Wir wenden uns nun dem allgemeinen Fall zu. Für eine beliebige Permutation $P=\begin{pmatrix}1 & \dots & n\\ j_1 & \dots & j_n\end{pmatrix}$ betrachten wir die Zahlen j_{p_1}, ..., j_{p_k}, die, in ihre natürliche Reihenfolge gebracht, uns die Kombination $q_1<\dots<q_k$ der Zahlen 1, ..., n ergeben; offenbar gehört zu jeder Permutation $P\in S_n$ eine und nur eine derartige Kombination. Gehen wir unter Berücksichtigung von (5) von der Formel (6) für die Determinante aus, so bedeuten die Zahlen $q_\varkappa$ gerade die Nummern der Spalten, in denen die Elemente $\beta_{p_1 j_{p_1}}$, ..., $\beta_{p_k j_{p_k}}$ stehen, die in den zur Permutation P gehörenden Summanden von (6) eingehen. Wir betrachten jetzt nur die Terme von (6), die dieselbe Kombination q_1, ..., q_k ergeben, und behaupten, daß ihre Summe gerade der Summand

$$M\begin{pmatrix}p_1 & \dots & p_k\\ q_1 & \dots & q_k\end{pmatrix}\cdot A\begin{pmatrix}p_1 & \dots & p_k\\ q_1 & \dots & q_k\end{pmatrix}$$

von (11) ist. Aus der Summation über alle diese zu den Kombinationen q_1, ..., q_k gehörenden Teilsummen folgt dann die Behauptung des Satzes.

In der Tat, markieren wir in der Matrix die Stellen (p_α, q_γ), an denen die Elemente stehen, die sich an unserer Teilsumme beteiligen, so erhalten wir das Schema



Da in jedem Summanden unserer Determinante aus jeder Zeile und jeder Spalte genau ein Element vorkommt, ändert sich der Wert der Teilsumme nicht, wenn wir in den gekennzeichneten Zeilen und Spalten die durch Striche angedeuteten Elemente durch Nullen ersetzen. Wir denken uns das ausgeführt und können nun durch geeignete Vertauschung der Zeilen und Spalten die spezielle Gestalt (12) erreichen. Die p_1-te Zeile wird durch p_1-1 Vertauschungen mit der jeweils davor stehenden in die erste Zeile überführt, die p_2-te durch p_2-2 Vertauschungen in die zweite usw., bis schließlich die p_k-te Zeile durch p_k-k Vertauschungen in die k-te Zeile übergangen ist. Analog verfahren wir mit den Spalten. Dann haben wir insgesamt

$$\sum_{\alpha=1}^{k}(p_\alpha+q_\alpha)-2\sum_{\alpha=1}^{k}\alpha \tag{15}$$

Vertauschungen ausgeführt und eine Matrix der Form (12) hergestellt. Links oben steht die Matrix des Minors $M\begin{pmatrix}p_1 & \cdots & p_k\\ q_1 & \cdots & q_k\end{pmatrix}$ und rechts unten die Matrix des komplementären Minors. Die Anwendung von (13) und Berücksichtigung der Anzahl der Vertauschungen (15) ergibt nach Definition 2 gerade die Behauptung über die Teilsumme. □

Folgerung 4. *Unter den Voraussetzungen von Satz* 3 *gilt die folgende Formel für die Entwicklung einer Determinante nach den Spalten* $p_1, \ldots, p_k$:

$$\det(\beta_{ij})=\sum_{1\leqq q_1<\ldots<q_k\leqq n} M\begin{pmatrix}q_1 & \cdots & q_k\\ p_1 & \cdots & p_k\end{pmatrix}\cdot A\begin{pmatrix}q_1 & \cdots & q_k\\ p_1 & \cdots & p_k\end{pmatrix}. \tag{16}$$

Der Beweis ergibt sich sofort durch Anwendung von Satz 3 auf die transponierte Matrix und Satz 2. □

Von besonderer Wichtigkeit ist der Fall $k=1$. Hier gilt

$$M\begin{pmatrix}p\\ q\end{pmatrix}=\beta_{pq}. \tag{17}$$

Entsprechend schreiben wir für die Adjunkte des Elementes β_{pq}

$$A_{pq}:=A\begin{pmatrix}p\\ q\end{pmatrix}=(-1)^{p+q}M'\begin{pmatrix}p\\ q\end{pmatrix}. \tag{18}$$

Folgerung 5. *Unter den Voraussetzungen von Satz 3 gelten die folgenden Formeln* (19) *bzw.* (20) *für die Entwicklung einer Determinante nach der p-ten Zeile bzw. p-ten Spalte:*

$$\sum_{q=1}^{n} \beta_{rq} A_{pq} = \delta_{rp} \det(\beta_{ij}) , \tag{19}$$

$$\sum_{q=1}^{n} \beta_{qr} A_{qp} = \delta_{rp} \det(\beta_{ij}) . \tag{20}$$

Beweis. Für $r=p$ ist $\delta_{rp}=1$, und es steht nach (17), (18) ein Spezialfall der Formel (11) bzw. (16) da. Ist aber z. B. in (19) $r \neq p$, so entspricht die linke Seite nach dem eben Bewiesenen der Entwicklung nach der p-ten Zeile derjenigen Determinante, die aus der ursprünglichen entsteht, indem man die p-te Zeile durch die r-te ersetzt. Diese Determinante ist aber 0, da sie zwei gleiche Zeilen besitzt. Für $r \neq p$ ist aber auch die rechte Seite 0 (vgl. (7.25)). □

Die Formeln (19), (20) nennt man ebenfalls den *Laplaceschen Entwicklungssatz.* Wir wollen sie zum Beweis der *Cramerschen Regel* anwenden:

Satz 4. *Es sei K ein Körper, $\beta_{ij}, \gamma_i \in K$ und*

$$\sum_{j=1}^{n} \beta_{ij} x_j = \gamma_i, \qquad i=1, \ldots, n, \tag{21}$$

ein lineares Gleichungssystem aus n Gleichungen für n Unbekannte. Ist seine Determinante

$$d := \det(\beta_{ij}) \neq 0 , \tag{22}$$

so hat das System (21) *eine und nur eine Lösung $x_j = d_j/d$, wobei d_j die Determinante derjenigen Matrix ist, die aus (β_{ij}) durch Ersetzen der j-ten Spalte durch die rechte Seite (γ_i) von* (21) *entsteht:*

$$d_j := \begin{vmatrix} \beta_{11} & \cdots & \beta_{1,j-1} & \gamma_1 & \beta_{1,j+1} & \cdots & \beta_{1n} \\ \beta_{21} & \cdots & \beta_{2,j-1} & \gamma_2 & \beta_{2,j+1} & \cdots & \beta_{2n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ \beta_{n1} & \cdots & \beta_{n,j-1} & \gamma_n & \beta_{n,j+1} & \cdots & \beta_{nn} \end{vmatrix} . \tag{23}$$

Beweis. Nach Satz 7.4, angewandt auf die Spaltenvektoren der Matrix (β_{ij}) aus $V^n = K^n$, ergibt sich deren lineare Unabhängigkeit. Sie bilden daher eine Basis. Die Koeffizienten der Basisdarstellung des Spaltenvektors (γ_i) sind die eindeutig bestimmte Lösung von (21). Es bleibt $x_j = d_j/d$ zu verifizieren. Durch Entwicklung von (23) nach der j-ten Spalte folgt nach (20)

$$d_j = \sum_{q=1}^{n} \gamma_q A_{qj} . \tag{24}$$

Multiplizieren wir diese Gleichung mit β_{ij} und summieren über j, so folgt nach (19)

$$\sum_{j=1}^{n} \beta_{ij} d_j = \sum_{q=1}^{n} \gamma_q \sum_{j=1}^{n} \beta_{ij} A_{qj} = \sum_{q=1}^{n} \gamma_q \delta_{iq} \cdot d = \gamma_i \cdot d .$$

Division durch d ergibt die Lösung. □

Bemerkung. Zur rationellen Berechnung von Determinanten empfiehlt sich eine Kombination der nach Folgerung 2 geschilderten Methode mit dem Laplaceschen Entwicklungssatz. Zur Übung möge man viele Zahlenbeispiele auf verschiedene Weise berechnen.

Übung 1. Man beweise die Umkehrung von Satz 4: Hat das Gleichungssystem (21) genau eine Lösung, so gilt $\det(\beta_{ij}) \neq 0$.

Übung 2. Es sei

$$\sum_{j=1}^{n} \beta_{\alpha j} x_j = \gamma_\alpha, \qquad \alpha = 1, \ldots, m \leqq n, \tag{25}$$

ein System aus m Gleichungen mit n Unbekannten über einem Körper K. Man beweise: Besitzt die Matrix $(\beta_{\alpha j})$ einen von 0 verschiedenen Minor m-ter Ordnung, so ist (25) lösbar, und die Lösungsmenge hängt von $n-m$ willkürlich wählbaren Parametern $t_k \in K$, $k = m+1, \ldots, n$, ab.

Übung 3. Im $\boldsymbol{A}^n$ seien $n+1$ Punkte a_ν, $\nu = 0, 1, \ldots, n$, gegeben, und es seien $(\alpha_{j\nu})_{j=1,\ldots,n}$ die Koordinaten von a_ν in dem n-Bein $(o; \mathfrak{a}_i)$. Man beweise: Die Menge $\{a_\nu | \, \nu = 0, 1, \ldots, n\}$ ist *in allgemeiner Lage* genau dann, wenn die Determinante

$$\begin{vmatrix} 1 & 1 & \ldots & 1 \\ \alpha_{10} & \alpha_{11} & \ldots & \alpha_{1n} \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_{n0} & \alpha_{n1} & \ldots & \alpha_{nn} \end{vmatrix} \neq 0 \tag{26}$$

ist (vgl. Definition 5.5).

Übung 4. Es sei $\boldsymbol{H}^{n-1} = \boldsymbol{H}(a; \mathfrak{b}_1, \ldots, \mathfrak{b}_{n-1}) \subset \boldsymbol{A}^n$ eine Hyperebene, (α_j) bzw. (β_{jc}), $j = 1, \ldots, n$, $c = 1, \ldots, n-1$, seien die Koordinaten von a bzw. $\mathfrak{b}_c$ bezüglich $(o; \mathfrak{a}_i)$. Man beweise: Durch

$$\begin{vmatrix} 1 & 0 & \ldots & 0 & 1 \\ \alpha_1 & \beta_{11} & \ldots & \beta_{1,n-1} & \xi_1 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \alpha_n & \beta_{n1} & \ldots & \beta_{n,n-1} & \xi_n \end{vmatrix} = 0 \tag{27}$$

ist eine lineare Gleichung gegeben, die $\boldsymbol{H}^{n-1}$ als Lösungsmenge hat (vgl. Übung 5.2). Man finde analog eine Gleichung einer Hyperebene $\boldsymbol{H}^{n-1} = \boldsymbol{H}(a_1, \ldots, a_n) \subset \boldsymbol{A}^n$, die von n Punkten *in allgemeiner Lage* aufgespannt wird. Speziell gebe man Gleichungen für die Koordinatenhyperebenen durch einen Punkt $a \in \boldsymbol{A}^n$ an (vgl. Übung 6.2). Man stelle jede k-dimensionale Koordinatenebene als Durchschnitt von $n-k$ Koordinatenhyperebenen dar und finde ein diese k-Ebene charakterisierendes Gleichungssystem.

Übung 5. Man beweise

$$\begin{vmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_n \\ x_1^2 & x_2^2 & \ldots & x_n^2 \\ \ldots & \ldots & \ldots & \ldots \\ x_1^{n-1} & x_2^{n-1} & \ldots & x_n^{n-1} \end{vmatrix} = \prod_{1 \leqq i < j \leqq n} (x_j - x_i) \tag{28}$$

(*Vandermondesche Determinante*). Hieraus folgere man: Ist $\boldsymbol{V}^n$ ein Vektorraum über einem unendlichen Körper K, so gibt es eine Folge $(\mathfrak{c}_\mu)_{\mu \in \mathbb{N}}$, $\mathfrak{c}_\mu \in \boldsymbol{V}^n$, so daß alle n-Tupel $(\mathfrak{c}_{\mu_1}, \ldots, \mathfrak{c}_{\mu_n})$, $\mu_1 < \ldots < \mu_n$, aus n Vektoren dieser Folge linear unabhängig sind.

Übung 6. Es seien K ein Körper, $v_0, \ldots, v_n$ und $w_0, \ldots, w_m$ Unbestimmte über K. Wir betrachten die Polynome in der weiteren Unbestimmten x:

$$f_v(x) = v_0x^n + v_1x^{n-1} + \ldots + v_n, \qquad v = (v_0, \ldots, v_n),$$

$$f_w(x) = w_0x^m + w_1x^{m-1} + \ldots + w_m, \qquad w = (w_0, \ldots, w_m).$$

Unter der *Resultante* der Polynome f_v, f_w versteht man die Determinante mit $n+m$ Zeilen

$$R(f_v, f_w) := \begin{vmatrix} v_0 & v_1 & \ldots & v_n & & \\ & v_0 & v_1 & \ldots & v_n & \\ & & \ldots\ldots\ldots & & & \\ & & & v_0 & v_1 & \ldots & v_n \\ w_0 & w_1 & \ldots & w_m & & \\ & w_0 & w_1 & \ldots & w_m & \\ & & \ldots\ldots\ldots & & & \\ & & & w_0 & w_1 & \ldots & w_m \end{vmatrix} \begin{matrix} \\ \\ \\ \Big\} m \\ \\ \\ \\ \Big\} n \end{matrix} \tag{29}$$

(Die leeren Stellen sind durch Nullen zu füllen.) Setzt man $v = (c_0, \ldots, c_n)$, $w = (d_0, \ldots, d_m)$, $c_i, d_\alpha \in K$ die Koeffizienten von Polynomen f_c bzw. f_d aus $K[x]$ ein, so heißt $R(c, d) := R(f_c, f_d)$ ebenfalls die *Resultante* der Polynome f_c, f_d. Man beweise: a) Das Polynom $R(v, w)$ hat ganzzahlige Koeffizienten und ist homogen vom Grad n in w und vom Grad m in v, d. h., es gilt $R(zv, w) = z^m R(v, w)$ und $R(v, zw) = z^n R(v, w)$; seine Darstellung als Summe von Monomen enthält das Monom $v_0^m w_m^n$. — b) Es gilt $R(c, d) = 0$ dann und nur dann, wenn $c_0 = d_0 = 0$ ist oder wenn die Polynome f_c, f_d einen gemeinsamen Teiler $g \in K[x]$ mit $\operatorname{gr} g \geqq 1$ haben. (Hinweis. Man zeige zuerst: Wenn c_0 oder d_0 ungleich 0 ist, haben f_c und f_d genau dann einen gemeinsamen Teiler g, $\operatorname{gr} g \geqq 1$, wenn es Polynome $h, \hat{h} \in K[x]$ gibt mit $\operatorname{gr} h \leqq m-1$, $\operatorname{gr} \hat{h} \leqq n-1$ und $f_c h = f_d \hat{h}$. Diese Gleichung liefert (durch Koeffizientenvergleich) ein homogenes Gleichungssystem aus $n+m$ Gleichungen für die unbekannten Koeffizienten von h und $\hat{h}$, dessen Determinante leicht auf die Form (29) gebracht werden kann.) — c) Es seien K ein Zerfällungskörper von f_c und f_d, $\xi_1, \ldots, \xi_n$ die Wurzeln von f_c und $\eta_1, \ldots, \eta_m$ die Wurzeln von f_d. Man beweise

$$R(c, d) = c_0^m d_0^n \prod_{i=1}^{n} \prod_{\alpha=1}^{m} (\xi_i - \eta_\alpha). \tag{30}$$

(Hinweis. Man betrachte die ξ_i, η_α als Unbestimmte und zeige, daß $R(c, d)$ durch $\xi_i - \eta_\alpha$ teilbar ist. Ferner beachte man, daß R in den ξ_i und in den η_α symmetrisch ist, vgl. § 2.7.) — d) Ist $\Delta(c_1, \ldots, c_n)$ die *Diskriminante* des Polynoms f_c (mit $c_0 = 1$), vgl. Beispiel 2.7.1, so gilt

$$R(f_c, f_c') = (-1)^{\binom{n}{2}} \Delta(c_1, \ldots, c_n); \tag{31}$$

hierbei bezeichnet f' die Ableitung des Polynoms f.

Übung 7. Es sei $(\beta_{ij}) \in \mathbf{M}_n(K)$. Man beweise: Es gilt $\det(\beta_{ij}) \neq 0$ dann und nur dann, wenn (β_{ij}) durch Anwendung der elementaren Operationen (I) bis (III) auf die Zeilen in die Einheitsmatrix $(\delta_{ij}) \in \mathbf{M}_n(K)$ übergeführt werden kann. Wendet man diese Operationen auf die Gleichungen eines Systems (21) an, so erscheint die Lösung (im Fall $\det(\beta_{ij}) \neq 0$) als rechte Seite des umgeformten Systems.

5. Affine Geometrie

Dieses Kapitel beginnen wir mit der Untersuchung der affinen Abbildungen, das sind Abbildungen zwischen Punkträumen, die Parallelität und Streckenverhältnisse ungeändert lassen. Jeder affinen Abbildung entspricht eine eindeutig bestimmte lineare Abbildung der zugehörigen Vektorräume. Umgekehrt kann man jede lineare Abbildung als eine spezielle affine Abbildung geometrisch interpretieren. Damit ist die Untersuchung der affinen Abbildungen auf die der linearen Abbildungen reduziert, die den wichtigsten Gegenstand dieses Kapitels bilden. Vom algebraischen Standpunkt aus sind die linearen Abbildungen spezielle Homomorphismen der additiven Gruppen der Vektorräume. Hierdurch gibt es viele Analogien und Beziehungen zur Gruppentheorie. Aus den begrifflich leicht zu beherrschenden Operationen mit linearen Abbildungen gewinnen wir durch Übergang zu den Koordinatendarstellungen alle Operationen der Matrixalgebra. Das Rechnen mit Matrizen ist das wichtigste Hilfsmittel für den weiteren Aufbau der Geometrie; dieser Kalkül wird darüber hinaus in allen Gebieten der Mathematik und in den Anwendungen viel benutzt. Wir behandeln damit die Theorie der linearen Gleichungssysteme und ihre geometrischen Deutungen, die dualen Vektoren, die Koordinatentransformationen, die Jordansche Normalform eines aufspaltenden linearen Endomorphismus und die affine Klassifikation der Quadriken. Dabei werden gleichzeitig die allgemeinen Grundzüge des Problems der Klassifikation der Elemente $x \in X$ des Raumes X einer Transformationsgruppe $[G, X]$ gegenüber der Wirkung von G sowie die Beziehungen zwischen Invarianten und Koordinatentransformationen herausgearbeitet.

§ 1. Affine Abbildungen

Definition 1. Es seien $[\boldsymbol{A}, \boldsymbol{V}, K]$ und $[\boldsymbol{B}, \boldsymbol{W}, K]$ zwei affine Geometrien über demselben Körper K. Eine Abbildung $f: \boldsymbol{A} \to \boldsymbol{B}$ heißt *affin*, wenn sie die folgende Eigenschaft besitzt: Sind $p, q, r, s \in \boldsymbol{A}$ und gilt für ein $\lambda \in K$ die Beziehung

$$\overrightarrow{rs} = \overrightarrow{pq}\lambda\,, \tag{1}$$

so gilt für die Bildpunkte ebenfalls

$$\overrightarrow{f(r)\,f(s)} = \overrightarrow{f(p)\,f(q)}\,\lambda\,. \tag{2}$$

Beispiel 1. Die identische Abbildung $\mathrm{id}_{\mathbf{A}}$, die Translationen t_a (4.3.5), die Dehnungen (4.3.23) und damit überhaupt alle Homothetien (4.3.27) sind affine Abbildungen. Man überprüfe durch eine leichte Rechnung, daß sie die Bedingungen der Definition 1 erfüllen.

Beispiel 2. Die *konstanten* Abbildungen $f: x \in \boldsymbol{A} \mapsto f(x) = b_0 \in \boldsymbol{B}$ sind ebenfalls affin; die Gleichung (2) reduziert sich für sie auf die triviale $\mathfrak{o} = \mathfrak{o}\lambda$.

Die geometrische Deutung der affinen Abbildungen resultiert aus dem folgenden Satz:

Satz 1. *Jede affine Abbildung $f: \boldsymbol{A} \to \boldsymbol{B}$ besitzt die folgenden Eigenschaften:*

1. *Sind $p, q \in \boldsymbol{A}$, $p \neq q$, zwei Punkte, die dasselbe Bild $p' = f(q) \in \boldsymbol{B}$ besitzen, so ist das Bild $f(\boldsymbol{H}(p, q)) = \{p'\}$, und das Bild $f(\boldsymbol{H}_0)$ jeder zu $\boldsymbol{H}(p, q)$ parallelen Geraden $\boldsymbol{H}_0 \parallel \boldsymbol{H}(p, q)$ besteht ebenfalls aus einem einzigen Punkt.*

2. *Gilt dagegen $f(p) = p' \neq q' = f(q)$, so ist das Bild*

$$f(\boldsymbol{H}(p, q)) = \boldsymbol{H}(f(p), f(q)) \tag{3}$$

der von den Punkten p, q aufgespannten Geraden $\boldsymbol{H}(p, q)$ die von den Bildpunkten aufgespannte Gerade $\boldsymbol{H}' = \boldsymbol{H}(p', q')$, und die Bilder von zu $\boldsymbol{H}(p, q)$ parallelen Geraden $\boldsymbol{H}_0 \parallel \boldsymbol{H}(p, q)$ sind zum Bild $\boldsymbol{H}'$ parallele Geraden:

$$\text{Wenn} \quad \boldsymbol{H}_0 \parallel \boldsymbol{H}(p, q), \quad \text{so} \quad f(\boldsymbol{H}_0) \parallel f(\boldsymbol{H}(p, q))\,. \tag{4}$$

3. *Gilt wieder $f(p) \neq f(q)$ und ist (r, s) eine zu (p, q) homothetische Strecke, so sind auch die Bildstrecken zueinander homothetisch, und das Streckenverhältnis ist gleich:*

$$(f(r), f(s))/(f(p), f(q)) = (r, s)/(p, q)\,. \tag{5}$$

Erfüllt umgekehrt eine Abbildung $f: \boldsymbol{A} \to \boldsymbol{B}$ des affinen Raumes $\boldsymbol{A}$ in den affinen Raum $\boldsymbol{B}$ die Eigenschaften 1 und 3, so ist sie affin.

Beweis. Zu 1. Sind $r, s \in \boldsymbol{H}_0$, so ergibt sich aus Lemma 4.3.2 $\overrightarrow{rs} = \overrightarrow{pq}\lambda$ für ein gewisses $\lambda \in K$. Nach Definition 1 gilt dann wegen $f(p) = f(q)$ die Beziehung $\overrightarrow{f(r)\,f(s)} = \overrightarrow{f(p)\,f(q)}\,\lambda = \mathfrak{o}$, also $\{f(r)\} = \{f(s)\} = f(\boldsymbol{H}_0)$. – Zu 2. Es sei $\sigma \in K$ beliebig und $x = p + \overrightarrow{pq}\sigma$ ein beliebiger Punkt aus $\boldsymbol{H}(p, q)$. Dann gilt $\overrightarrow{px} = \overrightarrow{pq}\sigma$, also nach Definition 1 $\overrightarrow{p'f(x)} = \overrightarrow{p'q'}\sigma$ oder $f(x) = p' + \overrightarrow{p'q'}\sigma$, also $f(\boldsymbol{H}(p, q)) \subseteq \boldsymbol{H}(p', q')$. Da $\sigma \in K$ beliebig war, kommt jeder Punkt von $\boldsymbol{H}(p', q')$ wirklich als Bildpunkt eines Punktes $x \in \boldsymbol{H}(p, q)$ vor, und es gilt (3). Ist schließlich $\boldsymbol{H}_0 = \boldsymbol{H}(r, s)$, $r \neq s$, eine zu $\boldsymbol{H}(p, q)$ parallele Gerade, so gilt nach Lemma 4.3.2 $\overrightarrow{rs} = \overrightarrow{pq}\lambda$ mit $\lambda \neq 0$, also nach Definition 1 $\overrightarrow{f(r)f(s)} = \overrightarrow{p'q'}\lambda \neq \mathfrak{o}$ und somit $f(r) \neq f(s)$. Nach dem schon Bewiesenen und Lemma 4.3.2 ist $f(\boldsymbol{H}_0) = \boldsymbol{H}(f(r), f(s)) \parallel \boldsymbol{H}(p', q') = f(\boldsymbol{H}(p, q))$. Die Eigenschaft 3 ergibt sich unmittelbar aus Definition 1, Lemma 4.3.5 und der Definition (4.3.30) des Streckenverhält-

nisses. – Zum Beweis der Umkehrung seien $p, q, r, s \in \boldsymbol{A}$ mit $\overrightarrow{rs} = \overrightarrow{pq}\lambda$. Ist $p = q$, so ist $r = s$, also $f(r) = f(s)$, und (2) ist wegen $\mathfrak{o} = \mathfrak{o}\lambda$ erfüllt. Ist $p \neq q$ und $r = s$, so ist $\lambda = 0$, und (2) ist wieder trivial wegen $\mathfrak{o} = \overrightarrow{p'q'}0$. Es sei also $p \neq q$ und $r \neq s$. Wenn dann $f(p) = f(q)$ gilt, folgt aus der Eigenschaft 1 $\{f(r)\} = \{f(s)\} = f(\boldsymbol{H}(r, s))$, also (2) in der Gestalt $\mathfrak{o} = \mathfrak{o}\lambda$. Ist schließlich $f(p) \neq f(q)$, so ergibt sich die Beziehung (2) unmittelbar aus der Eigenschaft 3, (5), Lemma 4.3.5 und (4.3.30). □

Folgerung 1. *Eine injektive Abbildung $f: \boldsymbol{A} \to \boldsymbol{B}$ ist genau dann affin, wenn sie homothetische Strecken wieder in homothetische Strecken überführt und das Streckenverhältnis dabei invariant bleibt* (d. h., (5) gilt). □

Bemerkung. Die Übung 8 enthält eine schwächere Bedingung für die Charakterisierung der affinen Abbildungen. Da die Bewegungen der Elementargeometrie injektive Abbildungen sind, die Längen invariant lassen, lassen sie erst recht Streckenverhältnisse invariant und sind daher spezielle affine Abbildungen (vgl. Übung 6.2.13). Sie werden im nächsten Kapitel systematisch untersucht. Schon Beispiel 1 zeigt, daß es noch andere affine Abbildungen gibt.

Satz 2. *Sind $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}$ affine Räume über K, $f: \boldsymbol{A} \to \boldsymbol{B}$ und $g: \boldsymbol{B} \to \boldsymbol{C}$ affine Abbildungen, so ist auch $g \circ f: \boldsymbol{A} \to \boldsymbol{C}$ eine affine Abbildung. Ist f bijektive affine Abbildung, so ist auch $f^{-1}: \boldsymbol{B} \to \boldsymbol{A}$ affin.*

Beweis. Die erste Behauptung ergibt sich unmittelbar durch zweimalige Anwendung der Definition 1. Es sei nun f affin und bijektiv. Das Bild des Punktes $x \in \boldsymbol{A}$ bezeichnen wir mit $x' = f(x) \in \boldsymbol{B}$; es gilt also $x = f^{-1}(x')$. Es seien $p', q', r', s' \in \boldsymbol{B}$ beliebig mit $\overrightarrow{r's'} = \overrightarrow{p'q'}\lambda$. Wir definieren den Punkt $c := r + \overrightarrow{pq}\lambda \in \boldsymbol{A}$. Da f affin ist, gilt $c' = r' + \overrightarrow{p'q'}\lambda = s'$, was wegen Definition 1 unmittelbar aus $\overrightarrow{rc} = \overrightarrow{pq}\lambda$, $\overrightarrow{r'c'} = \overrightarrow{r's'} = \overrightarrow{p'q'}\lambda$ folgt. Somit ist $\overrightarrow{f^{-1}(r')\,f^{-1}(s')} = \overrightarrow{f^{-1}(p')\,f^{-1}(q')}\lambda$, d. h., f^{-1} ist affin. □

Folgerung 2. *Die Klasse der affinen Räume über demselben Grundkörper K mit den affinen Abbildungen als Morphismen ist eine Kategorie, die wir die affine Kategorie über K nennen.* □

Definition 2. Unter einer *affinen Transformation* von $\boldsymbol{A}$ versteht man eine bijektive affine Abbildung $f: \boldsymbol{A} \to \boldsymbol{A}$. Die Menge $\mathfrak{A}(\boldsymbol{A})$ der affinen Transformationen von $\boldsymbol{A}$ bildet bezüglich der Operation der Verknüpfung $\circ$ von Abbildungen eine Gruppe, die *affine Gruppe* von $\boldsymbol{A}$, vgl. Satz 1.5.1.

Folgerung 3. *Das Paar $[\mathfrak{A}(\boldsymbol{A}), \boldsymbol{A}]$ ist bezüglich der durch die Anwendung der Abbildungen definierten Wirkung*

$$(f, x) \in \mathfrak{A}(\boldsymbol{A}) \times \boldsymbol{A} \mapsto f(x) \in \boldsymbol{A} \tag{6}$$

eine effektive und transitive Transformationsgruppe (vgl. die Definitionen 1.4.2 und 1.4.5).

Da nämlich $\mathfrak{A}(\boldsymbol{A})$ nach Beispiel 1 alle Translationen enthält, die ja nach § 4.3 einfach transitiv über $\boldsymbol{A}$ wirken, muß erst recht $\mathfrak{A}(\boldsymbol{A})$ transitiv sein. □

Die Menge der affinen Abbildungen von $\boldsymbol{A}$ in $\boldsymbol{B}$ wollen wir mit

$$\mathfrak{A}(\boldsymbol{A}, \boldsymbol{B}) := \{f \mid f: \boldsymbol{A} \to \boldsymbol{B} \text{ affine Abbildung}\} \tag{7}$$

bezeichnen. Wenn nicht ausdrücklich etwas anderes gesagt wird, wollen wir im folgenden stets annehmen, daß die betrachteten Punkt- und Vektorräume *denselben Grundkörper* K haben.

Es seien nun $\boldsymbol{V}, \boldsymbol{W}$ die Vektorräume von $\boldsymbol{A}$ bzw. $\boldsymbol{B}$ und $f \in \mathfrak{A}(\boldsymbol{A}, \boldsymbol{B})$. Gilt $\vec{rs} = \vec{pq}$, so folgt aus (2) mit $\lambda = 1$ unmittelbar $\overrightarrow{f(r)\, f(s)} = \overrightarrow{f(p)\, f(q)}$, und daher können wir durch die folgende Definition jeder affinen Abbildung $f \in \mathfrak{A}(\boldsymbol{A}, \boldsymbol{B})$ eine eindeutig bestimmte Abbildung der zugehörigen Vektorräume zuordnen:

$$\mathfrak{x} = \vec{pq} \in \boldsymbol{V} \mapsto a(\mathfrak{x}) := \overrightarrow{f(p)\, f(q)} \in \boldsymbol{W}. \tag{8}$$

Satz 3. *Es sei* $f \in \mathfrak{A}(\boldsymbol{A}, \boldsymbol{B})$. *Dann wird durch* (8) *eine Abbildung* $a: \boldsymbol{V} \to \boldsymbol{W}$ *definiert, die folgende Eigenschaften besitzt:*

$$a(\mathfrak{x}\lambda) = a(\mathfrak{x})\,\lambda \quad \textit{für alle} \quad \mathfrak{x} \in \boldsymbol{V}, \qquad \lambda \in K, \tag{9}$$

$$a(\mathfrak{x} + \mathfrak{y}) = a(\mathfrak{x}) + a(\mathfrak{y}) \quad \textit{für alle} \quad \mathfrak{x}, \mathfrak{y} \in \boldsymbol{V}. \tag{10}$$

Beweis. Nach der obigen Bemerkung hängt $a(\mathfrak{x})$ nicht von der Wahl der Punkte p, q mit $\vec{pq} = \mathfrak{x}$ *ab*; wir können z. B. einen beliebigen Punkt $o \in \boldsymbol{A}$ fixieren und erhalten

$$a(\mathfrak{x}) = \overrightarrow{f(o)\, f(o + \mathfrak{x})}. \tag{11}$$

Zum Beweis von (9) sei etwa $\mathfrak{x} = \vec{pq}$ und $r = p + \vec{pq}\lambda$. Dann gilt $\vec{pr} = \vec{pq}\lambda$, und aus (2) und (8) folgt $a(\mathfrak{x}\lambda) = \overrightarrow{f(p)\, f(r)} = \overrightarrow{f(p)\, f(q)}\ \lambda = a(\mathfrak{x})\,\lambda$. Zum Beweis von (10) sei $\mathfrak{x} = \vec{pq}$, $\mathfrak{y} = \vec{qr}$. Dann gilt $\mathfrak{x} + \mathfrak{y} = \vec{pq} + \vec{qr} = \vec{pr}$, und aus (8) ergibt sich

$$a(\mathfrak{x} + \mathfrak{y}) = \overrightarrow{f(p)\, f(r)} = \overrightarrow{f(p)\, f(q)} + \overrightarrow{f(q)\, f(r)} = a(\mathfrak{x}) + a(\mathfrak{y}). \quad \square$$

Definition 3. Eine Abbildung $a: \boldsymbol{V} \to \boldsymbol{W}$ des Vektorraumes $\boldsymbol{V}$ in den Vektorraum $\boldsymbol{W}$ mit den Eigenschaften (9) und (10) heißt *linear* oder ein *Operator*.

Diese Eigenschaften lassen sich auch äquivalent durch die eine Formel

$$a(\mathfrak{x}\lambda + \mathfrak{y}\mu) = a(\mathfrak{x})\,\lambda + a(\mathfrak{y})\,\mu \quad \text{für alle} \quad \mathfrak{x}, \mathfrak{y} \in \boldsymbol{V}, \qquad \lambda, \mu \in K \tag{12}$$

ausdrücken. Die Linearitätseigenschaft ist uns schon bei der Definition 4.7.1, Eigenschaft (II), der Volumenfunktion begegnet. Die folgenden beiden Sätze zeigen zusammen mit Satz 3, daß die Untersuchung der affinen Abbildungen im wesentlichen auf die Untersuchung der linearen Abbildungen zurückgeführt werden kann.

Satz 4. *Es seien* $\boldsymbol{A}, \boldsymbol{B}$ *affine Räume mit den Vektorräumen* $\boldsymbol{V}$ *bzw.* $\boldsymbol{W}$, $p \in \boldsymbol{A}$, $p' \in \boldsymbol{B}$ *und* $a: \boldsymbol{V} \to \boldsymbol{W}$ *eine lineare Abbildung. Dann gibt es genau eine affine Abbildung* $f: \boldsymbol{A} \to \boldsymbol{B}$ *mit* $f(p) = p'$, *für die*

$$a(\vec{xy}) = \overrightarrow{f(x)\, f(y)} \tag{13}$$

für alle $x, y \in \boldsymbol{A}$ gilt (d. h. für die die vorgegebene Abbildung a gerade die zu f gehörige lineare Abbildung ist), nämlich

$$f\colon x \in \boldsymbol{A} \mapsto f(x) := p' + a(\vec{px}) \in \boldsymbol{B}\,. \tag{14}$$

Beweis. Aus $f(x) = f(p) + \overrightarrow{f(p)\,f(x)}$, (13) und $f(p) = p'$ erhalten wir sofort die Gestalt (14) der affinen Abbildung; sie ist also durch die Vorgaben eindeutig bestimmt. Zum Beweis der Existenz ist zu zeigen, daß (14) eine die Bedingungen erfüllende affine Abbildung ist. Ist $x = p$, also $\vec{px} = \mathfrak{o}$, so folgt aus der Linearität von a sofort $a(\mathfrak{o}) = \mathfrak{o}$, also aus (14) $f(p) = p'$. Sind weiter $x, y \in \boldsymbol{A}$ beliebig, so gilt

$$\begin{aligned}\overrightarrow{f(x)\,f(y)} &= \overrightarrow{(p' + a(\vec{px}))\,(p' + a(\vec{py}))} = a(\vec{py}) - a(\vec{px}) \\ &= a\,(\vec{py} - \vec{px}) = a(\vec{xy})\,,\end{aligned}$$

vgl. (4.3.13); denn wegen der Linearität von a gilt

$$a\,(\mathfrak{y} - \mathfrak{x}) = a(\mathfrak{y}) - a(\mathfrak{x})\,. \tag{15}$$

Also erfüllt die durch (14) definierte Abbildung auch die Bedingung (13). Um zu zeigen, daß f affin ist, betrachten wir die Punkte $x, y, r, s \in \boldsymbol{A}$ mit $\vec{xy} = \vec{rs}\lambda$. Da f die Bedingung (13) erfüllt, folgt

$$\overrightarrow{f(x)\,f(y)} = a(\vec{xy}) = a\,(\vec{rs}\lambda) = a(\vec{rs})\lambda = \overrightarrow{f(r)\,f(s)}\,\lambda. \quad \square$$

Beispiel 3. Nach Beispiel 4.3.1 können wir die Vektorräume $\boldsymbol{V}, \boldsymbol{W}$ auch als affine Räume betrachten. Ist $a\colon \boldsymbol{V} \to \boldsymbol{W}$ linear, so gilt $a(\mathfrak{o}) = \mathfrak{o} \in \boldsymbol{W} = \boldsymbol{B}$, und die Gleichung (14) reduziert sich auf $f(\mathfrak{x}) = a(\mathfrak{x})$; im Sinne dieses Beispiels sind also die linearen Abbildungen spezielle affine Abbildungen.

Beispiel 4. Es sei $\boldsymbol{A} = \boldsymbol{B}$ und $f \in \mathfrak{A}(\boldsymbol{A}, \boldsymbol{A})$. Gilt für ein $p \in \boldsymbol{A}$ die Gleichung $f(p) = p$, so heißt p ein *Fixpunkt* von f. (14) spezialisiert sich auf

$$f(x) = p + a(\vec{px})\,, \tag{16}$$

und aus den Sätzen 3 und 4 folgt, daß die affinen Abbildungen $f\colon \boldsymbol{A} \to \boldsymbol{A}$ mit dem Fixpunkt p und die linearen Abbildungen $a\colon \boldsymbol{V} \to \boldsymbol{V}$ einander umkehrbar eindeutig entsprechen. Allgemeiner gilt

Satz 5. *Es sei $f \in \mathfrak{A}(\boldsymbol{A}, \boldsymbol{A})$ eine beliebige affine Abbildung von $\boldsymbol{A}$ in sich, $p \in \boldsymbol{A}$ ein beliebig ausgewählter Punkt und $q = f(p)$. Dann gibt es einen eindeutig bestimmten Vektor $\mathfrak{a} \in \boldsymbol{V}$ und eine eindeutig bestimmte affine Abbildung f_0 mit dem Fixpunkt p, so daß $f = t_{\mathfrak{a}} \circ f_0$ gilt.*

Beweis. Wenn $f = t_{\mathfrak{a}} \circ f_0$ eine solche Zerlegung ist, folgt

$$q = f(p) = t_{\mathfrak{a}} \circ f_0(p) = t_{\mathfrak{a}}(p) = p + \mathfrak{a}\,;$$

also ist $\mathfrak{a} = \vec{pq}$ eindeutig bestimmt. Aus $f = t_{\mathfrak{a}} \circ f_0 = t_{\mathfrak{a}} \circ g_0$ ergibt sich durch Multiplikation mit $t_{\mathfrak{a}}^{-1} = t_{-\mathfrak{a}}$ von links sofort $f_0 = g_0$. Die Existenz der Zerlegung ergibt

sich aus (14) und (16) nach

$$f(x) = q + a(\vec{px}) = p + a(\vec{px}) + \vec{pq} = t_a \circ f_0(x) ,$$

wobei $f_0(x) = p + a(\vec{px})$ dieselbe lineare Abbildung a wie f besitzt. □

Übung 1. Es sei $f: \boldsymbol{A} \to \boldsymbol{B}$ affin und $\boldsymbol{M} \subseteq \boldsymbol{A}$ eine Ebene mit dem Vektorraum $\boldsymbol{U} = V(\boldsymbol{M})$. Dann ist auch die Einschränkung $f \mid \boldsymbol{M}: \boldsymbol{M} \to \boldsymbol{B}$ affin, und für die zu f bzw. $f \mid \boldsymbol{M}$ gehörenden linearen Abbildungen a_f bzw. $a_{f|\boldsymbol{M}}$ gilt

$$a_{f|\boldsymbol{M}} = a_f \mid V(\boldsymbol{M}) . \tag{17}$$

Übung 2. a) Es seien eine Hyperebene $\boldsymbol{B}^n \subset \boldsymbol{A}^{n+1}$ und ein Vektor $\mathfrak{p}$, $\mathfrak{p} \notin V(\boldsymbol{B}^n)$, gegeben. Man beweise, daß jede Gerade in Richtung $\mathfrak{p}$ die Hyperebene $\boldsymbol{B}^n$ in genau einem Punkt schneidet und daß die Abbildung

$$f: x \in \boldsymbol{A}^{n+1} \mapsto x' := \boldsymbol{B}^n \cap \boldsymbol{H}(x, \mathfrak{p}) \in \boldsymbol{B}^n \tag{18}$$

affin ist; sie heißt die *Parallelprojektion in Richtung* $\mathfrak{p}$ *von* $\boldsymbol{A}^{n+1}$ *auf* $\boldsymbol{B}^n$. – b) Es sei f wie in (18) definiert und $\boldsymbol{N} \subset \boldsymbol{A}^{n+1}$ eine Ebene. Man beweise: $f \mid \boldsymbol{N}$ ist injektiv genau dann, wenn $\mathfrak{p} \notin V(\boldsymbol{N})$ gilt.

Übung 3. Man beweise: Ist $f: \boldsymbol{A}^{n+1} \to \boldsymbol{A}^{n+1}$ eine affine Abbildung mit den folgenden Eigenschaften: 1°. Es gibt eine Hyperebene $\boldsymbol{B}^n \subset \boldsymbol{A}^{n+1}$ mit $f(x) = x$ für alle $x \in \boldsymbol{B}^n$; 2°. f ist nicht injektiv; dann ist f eine Parallelprojektion von $\boldsymbol{A}^{n+1}$ auf $\boldsymbol{B}^n$.

Übung 4. Es sei $K = \mathbf{R}$, $\boldsymbol{H} = \boldsymbol{H}(o; \mathfrak{a}_1, \mathfrak{a}_2)$ und $\boldsymbol{H}'$ seien zwei zweidimensionale Ebenen des $\boldsymbol{A}^3$ und $z \in \boldsymbol{A}^3 \setminus (\boldsymbol{H} \cup \boldsymbol{H}')$ ein nicht in diesen Ebenen liegender Punkt. Ferner sei $\Pi \subset \boldsymbol{H}$ ein Parallelogramm mit der folgenden Eigenschaft: Für jedes $x \in \Pi$ schneidet die Gerade $\boldsymbol{H}(z, x)$ die Ebene $\boldsymbol{H}'$ in genau einem Punkt $x' = \varphi(x)$. (φ nennt man auch eine *Zentralprojektion* mit dem Zentrum z.) Man beweise: Es gibt genau dann eine affine Abbildung $f: \boldsymbol{H} \to \boldsymbol{H}'$ mit $f \mid \Pi = \varphi$, wenn $\boldsymbol{H}$ und $\boldsymbol{H}'$ parallel sind.

Beispiel 5. Für eine beliebige Menge $A \neq \emptyset$ heißt eine Abbildung $f: A \to A$ *involutiv* (oder eine *Involution*), wenn $f^2 = \mathrm{id}_A$ gilt; hierbei ist $f^2 := f \circ f$. Aus Übung 0.2.4 folgt sofort, daß jede Involution bijektiv ist und $f^{-1} = f$ gilt. Wir bemerken noch folgende leicht zu beweisende Eigenschaft der Involutionen: Sind $f, g: A \to A$ Involutionen, so ist $f \circ g$ genau dann eine Involution, wenn $f \circ g = g \circ f$ gilt. Es sei nun $[\boldsymbol{A}^2, \boldsymbol{V}^2, K]$ eine affine Ebene, char $K \neq 2$. Wir wählen ein 2-Bein $(o; \mathfrak{a}_1, \mathfrak{a}_2)$ von $\boldsymbol{A}^2$ und definieren die Abbildung $f: \boldsymbol{A}^2 \to \boldsymbol{A}^2$ folgendermaßen: Ist $\vec{ox} = \mathfrak{a}_1\xi_1 + \mathfrak{a}_2\xi_2$, so sei

$$f(x) := o + \mathfrak{a}_1\xi_1 - \mathfrak{a}_2\xi_2 . \tag{19}$$

Man beweist leicht, daß f eine affine Involution ist; ihre Fixpunktmenge

$$C_f := \{x \mid x \in \boldsymbol{A} \text{ und } f(x) = x\} \tag{20}$$

ist die Gerade $C_f = \boldsymbol{H}(o, \mathfrak{a}_1)$. Man nennt f die *Schrägspiegelung an der Geraden* $\boldsymbol{H}(o, \mathfrak{a}_1)$ *in Richtung* $\mathfrak{a}_2$. Eine andere affine Involution ist

$$s_o: x \in \boldsymbol{A} \mapsto s_o(x) := o - \vec{ox} \in \boldsymbol{A}; \tag{21}$$

sie heißt die *Spiegelung am Punkt* o und stimmt offenbar mit der Dehnung $d_{o,-1}$ überein, vgl. (4.3.23).

Übung 5. Man beweise, daß durch (19) eine affine Involution f mit $C_f = \boldsymbol{H}(o, a_1)$ definiert wird. In Analogie zu (19) definiere man in $\boldsymbol{A}^3$ a) Schrägspiegelungen an einer Ebene $\boldsymbol{H}^2 = \boldsymbol{H}(o; a_1, a_2)$ in Richtung a_3 und b) Schrägspiegelungen an einer Geraden $\boldsymbol{H}^1 = \boldsymbol{H}(o, a_1)$ in Richtung des Unterraums $\boldsymbol{W}^2 = \mathfrak{L}(\{a_2, a_3\})$, wobei $(o; a_1, a_2, a_3)$ ein Repère des $\boldsymbol{A}^3$ sei. Man definiere diese Abbildungen so, daß sie affine Involutionen mit der Fixpunktmenge $\boldsymbol{H}^2$ bzw. $\boldsymbol{H}^1$ sind.

Übung 6. Es sei $f: \boldsymbol{A} \to \boldsymbol{A}$ eine affine Abbildung. Man beweise: Die Fixpunktmenge C ist leer oder eine Ebene $C_f \subseteq \boldsymbol{A}$, $0 \leqq \dim C_f \leqq \dim \boldsymbol{A}$. Man charakterisiere im Fall $C_f \neq \emptyset$ den Vektorraum $V(C_f)$ von C_f mit Hilfe der zu f gehörenden linearen Abbildung $a = a_f$.

Übung 7. a) Es sei $\operatorname{char} K \neq 2$ und $f: \boldsymbol{A} \to \boldsymbol{A}$ eine affine Involution. Man beweise $C_f \neq \emptyset$, d. h., f hat wenigstens einen Fixpunkt. — b) Ist $\operatorname{char} K = 2$ und $0 < \dim \boldsymbol{A} < \infty$, so gibt es stets eine affine Involution $f: \boldsymbol{A} \to \boldsymbol{A}$ ohne Fixpunkte.

Übung 8. Es seien $\boldsymbol{A}$, $\boldsymbol{B}$ affine Punkträume über einem Körper K, der wenigstens drei Elemente enthält. Man zeige: Eine Abbildung $f: \boldsymbol{A} \to \boldsymbol{B}$ ist genau dann affin, wenn für $p, q, s \in \boldsymbol{A}$ mit $p \neq q$ und $\vec{ps} = \vec{pq}\lambda$ stets auch $\overrightarrow{f(p)\,f(s)} = \overrightarrow{f(p)\,f(q)}\,\lambda$ gilt. (Hinweis. Zum Beweis der Bedingung von Definition 1 betrachte man zuerst den Fall $\lambda \neq 1$ und denke an die Figur des Strahlensatzes 4.3.6.)

§ 2. Lineare Abbildungen

Im vorigen Paragraphen haben wir die affinen Abbildungen auf die linearen (Definition 1.3) zurückgeführt. Deswegen und vor allem wegen der fundamentalen Bedeutung der linearen Abbildungen für die Anwendungen der Algebra in Analysis und Geometrie sollen diese jetzt von einem überwiegend algebraischen Standpunkt aus betrachtet werden. Die Eigenschaft (1.10) der Definition der linearen Abbildungen besagt, daß sie Homomorphismen der Vektorgruppe $[\boldsymbol{V}, +]$ sind (vgl. § 1.2); daher ergeben sich viele Parallelen der Theorie der Vektorräume zur Theorie der abelschen Gruppen. Zuerst werden einige sehr allgemeine Begriffe und Eigenschaften der linearen Abbildungen behandelt, die auch für unendlichdimensionale Vektorräume wichtig sind. Danach betrachten wir besonders die linearen Abbildungen zwischen endlichdimensionalen Vektorräumen, die im folgenden im Vordergrund stehen werden. Im nächsten Paragraphen wenden wir die erhaltenen Ergebnisse dann auf die affinen Abbildungen an.

Beispiel 1. Die *identische Abbildung* $\mathrm{id}_{\boldsymbol{V}}$ eines Vektorraums $\boldsymbol{V}$ ist linear. Ist $\boldsymbol{W} \subseteq \boldsymbol{V}$ ein Unterraum, so ist die *Einbettung* $\iota: \boldsymbol{W} \to \boldsymbol{V}$ linear. Die *Dehnungen* eines Vektorraumes $\boldsymbol{V}$ um einen Faktor $\lambda \in K$

$$d_\lambda: \mathfrak{x} \in \boldsymbol{V} \mapsto d_\lambda(\mathfrak{x}) := \mathfrak{x}\lambda \in \boldsymbol{V} \tag{1}$$

sind linear. Die *triviale lineare Abbildung* (*Nullabbildung*), die jedem $\mathfrak{x} \in \boldsymbol{V}$ den Nullvektor $o(\mathfrak{x}) = \mathfrak{o} \in \boldsymbol{W}$ zuordnet, ist ebenfalls linear.

Unmittelbar aus der Definition 1.3 verifiziert man

Satz 1. 1°. *Sind* $a: \boldsymbol{V} \to \boldsymbol{W}$ *und* $b: \boldsymbol{W} \to \boldsymbol{U}$ *linear, so ist auch* $b \circ a: \boldsymbol{V} \to \boldsymbol{U}$ *linear.*

2°. *Ist* $a: V \to W$ *linear und bijektiv, so ist auch* $a^{-1}: W \to V$ *linear.*

3°. *Ist* $a: V \to W$ *linear und* $U \subseteq V$ *ein Unterraum, so ist auch die Einschränkung* $a \mid U: U \to W$ *linear.* □

Definition 1. Mit $L(V, W)$ bezeichnen wir die *Menge der linearen Abbildungen* von V in W. Die Elemente von $L(V) := L(V, V)$ heißen *lineare Endomorphismen*, die bijektiven linearen Abbildungen *lineare Isomorphismen*. Nach Satz 1 bilden die *linearen Automorphismen*, d. h. die bijektiven Endomorphismen, eine Gruppe $GL(V) \subset L(V)$, die man die *lineare Gruppe des Vektorraumes* V nennt.

Folgerung 1. *Die Klasse der Vektorräume über demselben Grundkörper* K *mit den linearen Abbildungen als Morphismen ist eine Kategorie, die „Kategorie der Vektorräume über* K*“.* □

Satz 2. *Es sei* $a \in L(V, W)$. *Ist* $V' \subseteq V$ *ein Unterraum, so ist auch das Bild* $a(V') \subseteq W$ *ein Unterraum. Ist* $W' \subseteq W$ *ein Unterraum, so ist auch das Urbild* $a^{-1}(W') \subseteq V$ *ein Unterraum.*

Zum Beweis verifiziere man unmittelbar aus Definition 1.3 die Bedingungen von Lemma 4.2.1. □

Definition 2. Unter dem *Bild von* $a \in L(V, W)$ versteht man $\operatorname{Im} a := a(V)$ und unter dem *Kern von* a

$$\operatorname{Ker} a := a^{-1}(0) . \tag{2}$$

Folgerung 2. *Für* $a \in L(V, W)$ *sind* $\operatorname{Im} a \subseteq W$ *und* $\operatorname{Ker} a \subseteq V$ *Unterräume. Die Abbildung* a *ist surjektiv genau dann, wenn* $\operatorname{Im} a = W$, *und injektiv genau dann, wenn* $\operatorname{Ker} a = 0$ *ist.* □

Ganz analog zum Begriff der Faktorgruppe (vgl. Definition 3.1.2), des Faktorringes (vgl. Definition 3.3.2) und der im Zusammenhang mit diesen behandelten Homomorphiesätze sind die entsprechenden Begriffe und Sätze über Vektorräume, deren Beweise wir dem Leser überlassen wollen.

Satz 3. *Es sei* $W \subset V$ *ein Unterraum. Dann wird durch die Definition*

$$\mathfrak{a} \equiv \mathfrak{b}(W) :\Leftrightarrow \mathfrak{a} - \mathfrak{b} \in W \tag{3}$$

eine Äquivalenzrelation in V *erklärt; die Äquivalenzklassen sind die Nebenklassen* $[\mathfrak{a}] = \mathfrak{a} + W \subseteq V$. *In der Menge* V/W *der Äquivalenzklassen wird durch vertreterweise Erklärung der Operationen*

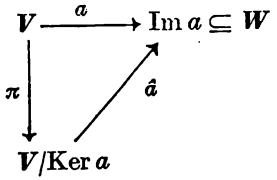
$$[\mathfrak{a}] + [\mathfrak{b}] := [\mathfrak{a} + \mathfrak{b}] , \tag{4}$$

$$[\mathfrak{a}]\, \lambda := [\mathfrak{a}\lambda] \qquad (\lambda \in K) \tag{5}$$

die Struktur eines Vektorraumes $[V/W, +, K]$ *über* K *definiert, der der Faktorraum von* V *nach dem Unterraum* W *heißt. Die kanonische Abbildung* $\pi: \mathfrak{x} \in V \mapsto [\mathfrak{x}] \in V/W$, *die jedem* $\mathfrak{x} \in V$ *seine Äquivalenzklasse* $[\mathfrak{x}] \in V/W$ *zuordnet, ist linear, und es gilt* $\operatorname{Ker} \pi = W$. □

Bemerkung. Nach Beispiel 4.3.1 können wir den Vektorraum $\boldsymbol{V}$ auch als Punktraum der affinen Geometrie $[\boldsymbol{V}, \boldsymbol{V}, K]$ betrachten. Dann stimmt die Einteilung von $\boldsymbol{V}$ in die Äquivalenzklassen $\mathfrak{a}+\boldsymbol{W}$ mit der in Folgerung 4.5.2, e) angegebenen Zerlegung in die $\boldsymbol{W}$-Orbits überein.

Satz 4 (Homomorphiesatz für Vektorräume). *Ist $a \in \boldsymbol{L}(\boldsymbol{V}, \boldsymbol{W})$, so gibt es einen kanonischen linearen Isomorphismus $\hat{a}\colon \boldsymbol{V}/\mathrm{Ker}\, a \to \mathrm{Im}\, a$ derart, daß das Diagramm*



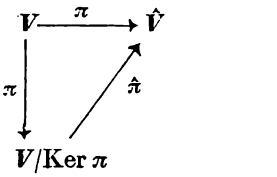
(6)

kommutativ ist, nämlich

$$\hat{a}([\mathfrak{x}]) = a(\mathfrak{x}) \,. \quad \square \tag{7}$$

Folgerung 3. *In der Menge $\boldsymbol{V}/\boldsymbol{W}$ der Äquivalenzklassen von $\boldsymbol{V}$ nach $\boldsymbol{W}$ gibt es genau eine Vektorraumstruktur derart, daß die kanonische Abbildung π linear ist und* $\mathrm{Ker}\, \pi = \boldsymbol{W}$ *gilt, nämlich die in Satz 3 definierte.*

Zum Beweis von Folgerung 3 bezeichne $\hat{\boldsymbol{V}}$ die Menge $\boldsymbol{V}/\boldsymbol{W}$, versehen mit irgendeiner den Forderungen genügenden Vektorraumstruktur über K. Das (6) entsprechende Diagramm ist dann



(8)

und wegen $\mathrm{Ker}\, \pi = \boldsymbol{W}$ ist $\hat{\pi} = \mathrm{id}_{\boldsymbol{V}/\boldsymbol{W}}$ der kanonische Isomorphismus nach Satz 4, der zeigt, daß die Vektorraumstruktur von $\hat{\boldsymbol{V}}$ mit der von $\boldsymbol{V}/\boldsymbol{W}$ übereinstimmt. $\square$

Es sei nun $\boldsymbol{V}^n$ ein endlichdimensionaler Vektorraum und $(\mathfrak{a}_i)$ eine Basis von $\boldsymbol{V}^n$, $i = 1, \ldots, n$. Für einen beliebigen Vektorraum $\boldsymbol{W}$ und $a \in \boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{W})$ erhalten wir aus der Linearität durch Anwendung der Abbildung a auf die Basisdarstellung eines variablen Vektors

$$\mathfrak{x} = \sum_{i=1}^{n} \mathfrak{a}_i \xi_i \in \boldsymbol{V}^n \mapsto a(\mathfrak{x}) = \sum_{i=1}^{n} a(\mathfrak{a}_i)\, \xi_i \in \boldsymbol{W} \,. \tag{9}$$

Satz 5. *Es sei $(\mathfrak{a}_i)$ eine Basis des Vektorraumes $\boldsymbol{V}^n$ und $(\mathfrak{c}_i)$, $i = 1, \ldots, n$, eine Folge von Vektoren des Vektorraumes $\boldsymbol{W}$. Dann gibt es eine und nur eine lineare Abbildung $a \in \boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{W})$, für die $\mathfrak{c}_i$ das Bild des Basisvektors $\mathfrak{a}_i$ ist:*

$$a(\mathfrak{a}_i) = \mathfrak{c}_i \,. \tag{10}$$

Beweis. Setzen wir (10) in (9) ein, so folgt $a(\mathfrak{x}) = \sum_{i=1}^{n} \mathfrak{c}_i \xi_i$; die Abbildung a ist also durch die Bilder einer Basis eindeutig bestimmt. Betrachten wir nun diese letzte Gleichung als Definition der Abbildung a, so folgt durch eine leichte Rechnung deren Linearität:

$$a(\mathfrak{x}\lambda + \mathfrak{y}\mu) = \sum_{i=1}^{n} \mathfrak{c}_i (\xi_i \lambda + \eta_i \mu) = \left(\sum_{i=1}^{n} \mathfrak{c}_i \xi_i \right) \lambda + \left(\sum_{i=1}^{n} \mathfrak{c}_i \eta_i \right) \mu$$
$$= a(\mathfrak{x})\, \lambda + a(\mathfrak{y})\, \mu;$$

dabei bezeichnen η_i die Vektorkoordinaten von $\mathfrak{y}$ bezüglich $(\mathfrak{a}_i)$. □

Die in diesem Satz enthaltene Methode der Definition linearer Abbildungen nennt man auch *„Prinzip der linearen Fortsetzung"*. Wir wollen aus ihm nun eine Reihe einfacher, aber wichtiger Folgerungen ziehen.

Folgerung 4. *Die in Satz* 5 *definierte lineare Abbildung ist ein linearer Isomorphismus dann und nur dann, wenn* $(\mathfrak{c}_i)$, $i = 1, \ldots, n$, *eine Basis von* $\boldsymbol{W}$ *ist.*

Beweis. Ist a ein Isomorphismus, so ist a surjektiv, und wegen

$$\mathfrak{x} = \sum_{i=1}^{n} \mathfrak{a}_i \xi_i \in \boldsymbol{V} \mapsto a(\mathfrak{x}) = \sum_{i=1}^{n} \mathfrak{c}_i \xi_i \in \boldsymbol{W} \tag{11}$$

ist $\{\mathfrak{c}_i\}$ erzeugende Menge von $\boldsymbol{W}$. Aus $\sum_{i=1}^{n} \mathfrak{c}_i \lambda_i = \mathfrak{o}$ folgt $\mathfrak{o} = \sum a(\mathfrak{a}_i)\, \lambda_i = a(\sum \mathfrak{a}_i \lambda_i)$, und da a injektiv ist, muß $\sum \mathfrak{a}_i \lambda_i = \mathfrak{o}$ sein. Weil nun $(\mathfrak{a}_i)$ eine Basis ist, müssen alle $\lambda_i = 0$ sein. Ist umgekehrt $(\mathfrak{c}_i)$ eine Basis von $\boldsymbol{W}$, so ist a injektiv und surjektiv und daher ein linearer Isomorphismus. □

Folgerung 5. *Es seien* $\boldsymbol{V}, \boldsymbol{W}$ *Vektorräume über* K, $\dim \boldsymbol{V} < \infty$, $a \in \boldsymbol{L}(\boldsymbol{V}, \boldsymbol{W})$. *Dann gilt*

$$\dim \operatorname{Im} a \leqq \min (\dim \boldsymbol{V}, \dim \boldsymbol{W}), \tag{12}$$

und a *ist ein linearer Isomorphismus dann und nur dann, wenn*

$$\dim \boldsymbol{V} = \dim \operatorname{Im} a = \dim \boldsymbol{W} \tag{13}$$

gilt. □

Folgerung 6. *Zwei endlichdimensionale Vektorräume* $\boldsymbol{V}, \boldsymbol{W}$ *über demselben Körper* K *sind genau dann isomorph, wenn* $\dim \boldsymbol{V} = \dim \boldsymbol{W}$ *gilt.* □

Beispiel 2. Die durch (4.4.9) definierte Koordinatenabbildung ist ein Isomorphismus zwischen $\boldsymbol{V}^n$ und dem n-Tupel-Raum K^n; vgl. Übung 4.4.1. Die Vektorräume K^n, $n \in \boldsymbol{N}_0$, sind also ein vollständiges Repräsentantensystem für die Isomorphieklassen endlichdimensionaler Vektorräume über K.

Bemerkungen. 1°. Es gibt im allgemeinen keinen kanonischen Isomorphismus zwischen gleichdimensionalen Vektorräumen; der nach Satz 5 definierte Isomor-

phismus hängt ja von der willkürlichen Auswahl der n-Beine $(\mathfrak{a}_i)$, $(\mathfrak{c}_i)$ von V bzw. W ab. – 2^0. Wie bei allen algebraischen Strukturen überträgt ein Isomorphismus zwischen Vektorräumen alle nur auf die Grundbegriffe und Axiome zurückzuführenden Eigenschaften (vgl. den Beweis von Folgerung 4); von dieser Tatsache werden wir im folgenden häufig stillschweigend Gebrauch machen. – 3^0. Aus Übung 4.4.7 erhält man durch eine leichte Verallgemeinerung des Prinzips der linearen Fortsetzung auf den unendlichdimensionalen Fall folgendes Resultat: *Zwei Vektorräume V, W über demselben Körper K sind genau dann isomorph, wenn ihre Basen dieselbe Mächtigkeit haben.*

Beispiel 3. Wir betrachten einen Vektorraum V^n über K. Es sei $(\mathfrak{a}_i)$ ein festes Repère, und $(\mathfrak{c}_i)$ durchlaufe alle Repères von V^n. Es sei g diejenige lineare Abbildung, für die $g(\mathfrak{a}_i)=\mathfrak{c}_i$ gilt. Dann durchläuft g die lineare Gruppe von V^n, und die Zuordnung $(\mathfrak{c}_i)\mapsto g$ ist eine bijektive Abbildung der Menge aller Repères von V^n auf die lineare Gruppe $GL(V^n)$. Hierdurch ist eine Veranschaulichung der linearen Gruppe gegeben.

Definition 3. Es sei $a\in L(V^n, W)$. Unter dem *Rang von a* versteht man

$$\operatorname{rg} a := \dim \operatorname{Im} a\,. \tag{14}$$

Lemma 1. *Es sei $a\in L(V^n, W^m)$. Dann gilt $\operatorname{rg} a=r$ dann und nur dann, wenn Basen $\{\mathfrak{a}_i\}$ von V^n und $\{\mathfrak{b}_\alpha\}$ von W^m mit den folgenden Eigenschaften existieren:*

1^0. $\operatorname{Im} a=\mathfrak{L}(\{\mathfrak{b}_1, \ldots, \mathfrak{b}_r\})$, (15)

2^0. $\operatorname{Ker} a=\mathfrak{L}(\{\mathfrak{a}_{r+1}, \ldots, \mathfrak{a}_n\})$, (16)

3^0. $a(\mathfrak{a}_\varrho)=\mathfrak{b}_\varrho$ *für* $\varrho=1, \ldots, r$. (17)

Beweis. Es sei $n-s=\dim \operatorname{Ker} a$. Wir wählen zuerst eine Basis von $\operatorname{Ker} a$, die wir mit $\{\mathfrak{a}_{s+1}, \ldots, \mathfrak{a}_n\}$ bezeichnen. Nach dem Basisergänzungssatz Folgerung 4.6.1 können wir sie zu einer Basis $\{\mathfrak{a}_i\}$, $i=1, \ldots, n$, von V^n ergänzen. Es sei $\mathfrak{b}_\varrho := a(\mathfrak{a}_\varrho)$ für $\varrho=1, \ldots, s$. Wegen $a(\mathfrak{a}_\varkappa)=\mathfrak{o}$ für $\varkappa>s$ erhalten wir aus (9) sofort $a(\mathfrak{x})=\sum_{\varrho=1}^{s}\mathfrak{b}_\varrho\xi_\varrho$, so daß $\{\mathfrak{b}_1, \ldots, \mathfrak{b}_s\}$ eine erzeugende Menge für $\operatorname{Im} a$ ist und $r\leqq s$ gilt. Wir zeigen, daß $\{\mathfrak{b}_1, \ldots, \mathfrak{b}_s\}$ auch linear unabhängig ist. Aus

$$\mathfrak{o}=\sum_{\varrho=1}^{s}\mathfrak{b}_\varrho\lambda_\varrho=\sum_{\varrho=1}^{s}a(\mathfrak{a}_\varrho)\,\lambda_\varrho=a\left(\sum_{\varrho=1}^{s}\mathfrak{a}_\varrho\lambda_\varrho\right)$$

folgt nämlich $\sum_{\varrho=1}^{s}\mathfrak{a}_\varrho\lambda_\varrho\in\operatorname{Ker} a=\mathfrak{L}(\{\mathfrak{a}_{s+1}, \ldots, \mathfrak{a}_n\})$, und weil $\{\mathfrak{a}_i\}$ eine Basis von V^n ist, muß $\sum_{\varrho=1}^{s}\mathfrak{a}_\varrho\lambda_\varrho=\mathfrak{o}$ und somit auch $\lambda_\varrho=0$ für $\varrho=1, \ldots, s$ gelten. Daher ist $\{\mathfrak{b}_1, \ldots, \mathfrak{b}_s\}$ eine Basis von $\operatorname{Im} a$, und es folgt $s=r$. Ergänzen wir $\{\mathfrak{b}_1, \ldots, \mathfrak{b}_s\}$ noch zu einer Basis $\{\mathfrak{b}_\alpha\}$, $\alpha=1, \ldots, m$, von W^m, so sind die Eigenschaften 1^0 bis 3^0 erfüllt. Die Umkehrung der Behauptung ist trivial. □

Beispiel 4. Eine lineare Abbildung $p \in \boldsymbol{L}(\boldsymbol{V})$ heißt eine *Projektion*, wenn $p^2 = p \circ p = p$ gilt. *Für jede Projektion ist* $\boldsymbol{V}$ *die direkte Summe* (Definition 4.4.5) *von* $\operatorname{Im} p$ *und* $\operatorname{Ker} p$:

$$\boldsymbol{V} = \operatorname{Im} p \oplus \operatorname{Ker} p \,. \tag{18}$$

In der Tat, es sei $\mathfrak{x} \in \boldsymbol{V}$ beliebig. Wir setzen $\mathfrak{z} = \mathfrak{x} - p(\mathfrak{x})$. Dann ist $\mathfrak{z} \in \operatorname{Ker} p$; denn es ist

$$p(\mathfrak{z}) = p(\mathfrak{x}) - p^2(\mathfrak{x}) = p(\mathfrak{x}) - p(\mathfrak{x}) = \mathfrak{o} \,.$$

Die Gleichung $\mathfrak{x} = p(\mathfrak{x}) + \mathfrak{z}$ zeigt, daß $\boldsymbol{V}$ die Summe von $\operatorname{Im} p$ und $\operatorname{Ker} p$ ist. Andererseits ist diese Summe auch direkt; denn für $\mathfrak{y} \in \operatorname{Im} p \cap \operatorname{Ker} p$ gibt es ein $\mathfrak{x} \in \boldsymbol{V}$ mit $\mathfrak{y} = p(\mathfrak{x})$, und es gilt

$$\mathfrak{o} = p(\mathfrak{y}) = p^2(\mathfrak{x}) = p(\mathfrak{x}) = \mathfrak{y} \,.$$

Umgekehrt beweist man leicht: *Ist* $\boldsymbol{V} = \bigoplus_{\iota \in I} \boldsymbol{W}_\iota$ *direkte Summe der Familie* $(\boldsymbol{W}_\iota)_{\iota \in I}$ *von Unterräumen und ist* $p_\iota : \mathfrak{x} \in \boldsymbol{V} \mapsto \mathfrak{x}_\iota \in \boldsymbol{W}_\iota$ *die Abbildung, die jedem* $\mathfrak{x} \in \boldsymbol{V}$ *seine Komponente in* $\boldsymbol{W}_\iota$ *zuordnet* (vgl. (4.4.12)), *so ist* p_ι *eine Projektion.* Als Spezialfall erhält man die *Projektionen eines Vektors* $\mathfrak{x} = \sum_{i=1}^{n} \mathfrak{a}_i \xi_i$ *auf die Koordinatenachsen*

$$\mathfrak{x} \in \boldsymbol{V} \mapsto p_i(\mathfrak{x}) := \mathfrak{a}_i \xi_i \in \mathfrak{L}(\{\mathfrak{a}_i\}) \,. \tag{19}$$

Im allgemeinen gilt für $a \in \boldsymbol{L}(\boldsymbol{V})$ natürlich nicht (18). Aus Lemma 1 ergibt sich jedoch sofort

Folgerung 7. *Ist* $n = \dim \boldsymbol{V} < \infty$ *und* $a \in \boldsymbol{L}(\boldsymbol{V}, \boldsymbol{W})$, *so gilt*

$$n = \dim \boldsymbol{V} = \dim \operatorname{Im} a + \dim \operatorname{Ker} a \,. \tag{20}$$

Folgerung 8. *Es sei* $n = \dim \boldsymbol{V} = \dim \boldsymbol{W} < \infty$ *und* $a \in \boldsymbol{L}(\boldsymbol{V}, \boldsymbol{W})$. *Dann gilt*

a injektiv $\Leftrightarrow$ *a surjektiv* $\Leftrightarrow$ *a bijektiv.*

Zum Beweis von Folgerung 7 beachte man, daß man $\boldsymbol{W}$ durch $\operatorname{Im} a$ ersetzen kann und (12) gilt; für Folgerung 8 beachte man Folgerung 2. □

Übung 1. Es sei $a : \boldsymbol{V} \to \boldsymbol{W}$ eine lineare Abbildung und $M \subseteq \boldsymbol{V}$ eine Teilmenge. Man beweise: a) $a(\mathfrak{L}(M)) = \mathfrak{L}(a(M))$. – b) Für alle $N \in \mathfrak{P}(\boldsymbol{W})$ gilt $\mathfrak{L}(a^{-1}(N)) \subseteq a^{-1}(\mathfrak{L}(N))$. – c) Für alle $N \in \mathfrak{P}(\boldsymbol{W})$ mit $\emptyset \neq N \subseteq \operatorname{Im} a$ gilt $\mathfrak{L}(a^{-1}(N)) = a^{-1}(\mathfrak{L}(N))$. – d) Es gilt $\mathfrak{L}(a^{-1}(N)) = a^{-1}(\mathfrak{L}(N))$ für alle $N \in \mathfrak{P}(\boldsymbol{W})$ dann und nur dann, wenn a ein Isomorphismus ist oder wenn $\boldsymbol{V} = \{\mathfrak{o}\}$ gilt.

Übung 2. Es sei $\boldsymbol{V}$ ein Vektorraum, $a \in \boldsymbol{L}(\boldsymbol{V})$ und $\lambda \in K$. Wir definieren

$$\boldsymbol{U}_\lambda := \{\mathfrak{x} \in \boldsymbol{V} \mid a\mathfrak{x} = \mathfrak{x}\lambda\} \,. \tag{21}$$

Man beweise: $\boldsymbol{U}_\lambda$ ist ein Unterraum von $\boldsymbol{V}$, und $a \mid \boldsymbol{U}_\lambda$ ist die Dehnung der Vektoren aus $\boldsymbol{U}_\lambda$ um den Faktor λ.

Definition 4. Es sei $a \in \boldsymbol{L}(\boldsymbol{V})$. Gilt für ein $\lambda \in K$, daß der Unterraum $\boldsymbol{U}_\lambda$ (nach (21)) nicht trivial ist: $\boldsymbol{U}_\lambda \neq \{\mathfrak{o}\}$, so heißt λ ein *Eigenwert von* a, $\boldsymbol{U}_\lambda$ der zum Eigenwert

λ gehörende *Eigenunterraum*, und die $\mathfrak{x} \in \boldsymbol{U}_\lambda$ mit $\mathfrak{x} \neq \mathfrak{o}$ heißen *Eigenvektoren* von a zum Eigenwert λ.

Zum Beispiel folgt für $\lambda = 0$ sofort

$$\boldsymbol{U}_0 = \operatorname{Ker} a \qquad (a \in \boldsymbol{L}(\boldsymbol{V})) \,. \tag{22}$$

Die in Definition 4 eingeführten Begriffe werden im folgenden eine wichtige Rolle spielen. Dasselbe gilt für die in Übung 3 formulierten, einfachen Eigenschaften dieser Begriffe:

Übung 3. Mit den Bezeichnungen und Voraussetzungen von Übung 2 und Definition 4 beweise man: a) Für $\lambda \neq \mu$, $\lambda, \mu \in K$, gilt $\boldsymbol{U}_\lambda \cap \boldsymbol{U}_\mu = \{\mathfrak{o}\}$. — b) Es seien $\lambda_1, \ldots, \lambda_r$ paarweise verschiedene Eigenwerte von a und $\mathfrak{x}_\varrho$ Eigenvektoren zu λ_ϱ, $\varrho = 1, \ldots, r$. Dann ist die Menge $\{\mathfrak{x}_1, \ldots, \mathfrak{x}_r\}$ linear unabhängig, und die Summe $\sum_{\varrho=1}^{r} \boldsymbol{U}_{\lambda_\varrho}$ ist direkt. — c) Gilt $\dim \boldsymbol{V} = n$ und besitzt $a \in \boldsymbol{L}(\boldsymbol{V})$ genau n verschiedene Eigenwerte λ_i, so ist $\dim \boldsymbol{U}_{\lambda_i} = 1$, und es gilt $\boldsymbol{V}^n = \bigoplus_{i=1}^{n} \boldsymbol{U}_{\lambda_i}$. (Hinweis. Zum Beweis von b) wende man vollständige Induktion nach r an und führe den Induktionsschluß indirekt.)

Übung 4. Es sei $\boldsymbol{V}^2$ ein zweidimensionaler Vektorraum über $\mathbf{R}$. Wir betrachten die nach Satz 5 durch die Bilder einer Basis $\{\mathfrak{a}_1, \mathfrak{a}_2\}$ von $\boldsymbol{V}^2$ eindeutig bestimmte lineare Abbildung a, für die $a(\mathfrak{a}_1) = \mathfrak{a}_2$ und $a(\mathfrak{a}_2) = -\mathfrak{a}_1$ gilt. Man beweise, daß diese Abbildung keinen Eigenwert $\lambda \in \mathbf{R}$ besitzt.

Übung 5. Es sei $a \in \boldsymbol{L}(\boldsymbol{V})$ eine Involution. Man beweise: a) Ist $\lambda \in K$ Eigenwert von a, so gilt $\lambda = e$ oder $\lambda = -e$, e die Eins des Körpers. — b) Unter der zusätzlichen Voraussetzung $\operatorname{char} K \neq 2$ gilt $\boldsymbol{V} = \boldsymbol{U}_e \oplus \boldsymbol{U}_{-e}$, d. h., $\boldsymbol{V}$ ist direkte Summe der Eigenunterräume zu den Eigenwerten $\pm e$. Für $\boldsymbol{U}_{-e} = \{\mathfrak{o}\}$ folgt $a = \mathrm{id}_{\boldsymbol{V}}$, und für $\boldsymbol{U}_e = \{\mathfrak{o}\}$ ergibt sich die Abbildung $s\colon \mathfrak{x} \in \boldsymbol{V} \mapsto -\mathfrak{x} \in \boldsymbol{V}$ (Spiegelung an $\mathfrak{o}$). — c) Man zeige anhand eines Beispiels, daß die Behauptung b) im Fall $\operatorname{char} K = 2$ nicht zu gelten braucht.

Übung 6. Unter den Voraussetzungen von Übung 5 und $\operatorname{char} K \neq 2$ beweise man: Sind $\boldsymbol{U}_e$, $\boldsymbol{U}_{-e}$ die Eigenunterräume von a und ist $b \in \boldsymbol{L}(\boldsymbol{V})$ ebenfalls eine Involution, so ist $a \circ b$ eine Involution genau dann, wenn $b(\boldsymbol{U}_e) = \boldsymbol{U}_e$ und $b(\boldsymbol{U}_{-e}) = \boldsymbol{U}_{-e}$ gilt. (Hinweis. Man beachte die Bemerkungen in Beispiel 1.5.)

Übung 7. Es sei $[\boldsymbol{A}^n, \boldsymbol{V}^n, K]$ eine n-dimensionale affine Geometrie mit $\operatorname{char} K \neq 2$. Man beweise: Ist $f\colon \boldsymbol{A}^n \to \boldsymbol{A}^n$ eine affine Involution, so ist f entweder die Identität oder die Spiegelung an einem Punkt $p \in \boldsymbol{A}^n$ oder eine Schrägspiegelung an einer k-Ebene $C_f = p + \boldsymbol{W}^k$ in Richtung eines Unterraumes $\boldsymbol{U}^{n-k} \subseteq \boldsymbol{V}$ mit $\boldsymbol{W}^k \oplus \boldsymbol{U}^{n-k} = \boldsymbol{V}^n$. (Vgl. Beispiel 1.5, Übung 1.7.)

Übung 8. Es sei $\boldsymbol{W} \subseteq \boldsymbol{V}$ ein Unterraum des Vektorraumes $\boldsymbol{V}$, $\dim \boldsymbol{V} < \infty$. Man beweise

$$\dim \boldsymbol{V}/\boldsymbol{W} = \dim \boldsymbol{V} - \dim \boldsymbol{W} \,. \tag{23}$$

Man nennt $\dim \boldsymbol{V}/\boldsymbol{W}$ die *Kodimension von $\boldsymbol{W}$ in $\boldsymbol{V}$*; falls $\dim \boldsymbol{V}$ unendlich, aber $\dim \boldsymbol{V}/\boldsymbol{W}$ endlich ist, heißt $\boldsymbol{W}$ ein Unterraum *endlicher Kodimension* $m = \dim \boldsymbol{V}/\boldsymbol{W}$.

Übung 9. Die Darstellung eines Vektorraumes $\boldsymbol{V}$ als direkte Summe seiner Unterräume (Definition 4.4.5) entspricht der Definition 3.2.1 für Gruppen. Wir wollen in dieser Übung die direkte Summe von r beliebigen Vektorräumen $\boldsymbol{V}_i$, $i = 1, \ldots, r$, über dem Körper K definieren, die nicht als Unterräume eines Vektorraumes gegeben sein müssen. Dazu gehen wir vom Produkt der die Vektorraumstruktur tragenden Mengen

$V := \bigtimes_{i=1}^{r} V_i$ aus. Man beweise: a) Über V gibt es eine eindeutig bestimmte Vektorraumstruktur $[V, +, K]$, bezüglich der alle Projektionen $p_k: \mathfrak{v} = (\mathfrak{v}_i) \in V \mapsto p_k(\mathfrak{v}) = \mathfrak{v}_k \in V_k$, $k = 1, ..., r$, lineare Abbildungen sind. Man nennt daher $[V, +, K]$ die *direkte Summe der Vektorräume* V_i und schreibt

$$V = \bigoplus_{i=1}^{r} V_i . \tag{24}$$

(Hinweis. Man erinnere sich an Satz 3.2.4.) — b) Es ist leicht zu sehen, daß die in a) gegebene Definition der direkten Summe mit Definition 4.4.5 verträglich ist. Dazu betrachte man die Injektionen

$$\iota_i: \mathfrak{x}_i \in V_i \mapsto \iota_i(\mathfrak{x}_i) := (\mathfrak{o}, ..., \mathfrak{o}, \mathfrak{x}_i, \mathfrak{o}, ..., \mathfrak{o}) \in V , \tag{25}$$

verifiziere, daß sie injektive lineare Abbildungen sind, formuliere und beweise das Analogon von Satz 3.2.5.

Übung 10. Es sei V ein Vektorraum über $\mathbf{R}$ und $\mathrm{i} = \sqrt{-1} \in \mathbf{C}$ die imaginäre Einheit. Wir bilden den zu V über $\mathbf{R}$ isomorphen Vektorraum $V\mathrm{i} := \{\mathfrak{v}\mathrm{i} \mid \mathfrak{v} \in V\}$; hierbei sei $\mathfrak{v}\mathrm{i} + \mathfrak{w}\mathrm{i} := (\mathfrak{v} + \mathfrak{w})\,\mathrm{i}$ und $(\mathfrak{v}\mathrm{i})\,\alpha := \mathfrak{v}\alpha\mathrm{i}$ $(\alpha \in \mathbf{R})$. Schließlich betrachten wir die direkte Summe $cV := V \oplus V\mathrm{i}$; cV ist zunächst ein Vektorraum über $\mathbf{R}$; jedes $\mathfrak{w} \in cV$ ist eindeutig in der Form $\mathfrak{w} = \mathfrak{x} + \mathfrak{y}\mathrm{i}$, $\mathfrak{x}, \mathfrak{y} \in V$, darstellbar. Man beweise: a) Mit der in cV schon definierten Addition und der durch

$$\left.\begin{array}{l} \mathfrak{w} = \mathfrak{x} + \mathfrak{y}\mathrm{i} \in cV, \\ z \;\; = \xi + \eta\mathrm{i} \in \mathbf{C} \end{array}\right\} \mapsto \mathfrak{w}z := (\mathfrak{x}\xi - \mathfrak{y}\eta) + (\mathfrak{x}\eta + \mathfrak{y}\xi)\,\mathrm{i} \in cV$$

definierten Multiplikation mit Skalaren $z \in \mathbf{C}$ wird $[cV, +, \mathbf{C}]$ ein Vektorraum über $\mathbf{C}$, der die *Komplexifizierung* cV des reellen Vektorraumes V heißt. Da andererseits jeder Vektorraum W über $\mathbf{C}$ auch ein Vektorraum über $\mathbf{R}$ ist (Übung 4.2.7), müssen wir bei vielen Begriffen angeben, welchen Skalarbereich wir gerade betrachten; wir sprechen von $\mathbf{R}$-linearen oder $\mathbf{C}$-linearen Abbildungen, von reeller Dimension $\dim_{\mathbf{R}} W$ oder komplexer Dimension $\dim_{\mathbf{C}} W$ usw. — b) Es gilt $\dim_{\mathbf{C}} cV = \dim_{\mathbf{R}} V$. — c) Ferner gilt $r(cV) = V \oplus_{\mathbf{R}} V\mathrm{i}$, also $\dim_{\mathbf{R}} r(cV) = 2 \dim_{\mathbf{R}} V$. Komplexifizierung und Reellifizierung sind nicht zueinander inverse Operationen!

§ 3. Anwendungen auf die affinen Abbildungen

Wir knüpfen an die durch Satz 1.3 gegebene Zuordnung

$$\Phi: f \in \mathfrak{A}(A^n, B^m) \mapsto \Phi(f) = a_f \in L(V^n, W^m) \tag{1}$$

mit

$$a_f(\vec{xy}) = \overrightarrow{f(x)\,f(y)} \tag{2}$$

an, die jeder affinen Abbildung die entsprechende lineare Abbildung der zu den affinen Räumen gehörenden Vektorräume zuordnet, und beginnen mit einigen Beispielen.

Beispiel 1. Ist $f = t_a$ eine Translation, so ist $a_f = \mathrm{id}_V$. In der Tat, nach (2) ist

$a_f(\vec{xy}) = \overrightarrow{(x+\mathfrak{a})\,(y+\mathfrak{a})} = \vec{xy}$ für alle $x, y \in \boldsymbol{A}$. Für $\mathfrak{a} = \mathfrak{o}$ ist $t_\mathfrak{a} = \mathrm{id}_{\boldsymbol{A}}$, und es folgt

$$a_{\mathrm{id}_{\boldsymbol{A}}} = \mathrm{id}_{\boldsymbol{V}} \qquad (\boldsymbol{V} \text{ der Vektorraum von } \boldsymbol{A}) . \tag{3}$$

Beispiel 2. Den Dehnungen (4.3.23) $d_{p,\lambda}$ des Punktraumes $\boldsymbol{A}$ entsprechen die Dehnungen (2.1) d_λ des zugehörigen Vektorraumes $\boldsymbol{V}$:

$$f = d_{p,\lambda} \mapsto a_f = d_\lambda ; \tag{4}$$

denn es gilt $\overrightarrow{f(x)\,f(y)} = \overrightarrow{(p+\vec{px}\,\lambda)\,(p+\vec{py}\,\lambda)} = \vec{xy}\,\lambda$.

Beispiel 3. Den konstanten affinen Abbildungen (Beispiel 1.2) entspricht die Nullabbildung (Beispiel 2.1) der zugehörigen Vektorräume.

Aus der Formel (1.14) ergibt sich leicht, daß zu den Beispielen 1 bis 3 auch die folgenden Umkehrungen gelten: Ist a_f die Identität $\mathrm{id}_{\boldsymbol{V}}$, die Dehnung d_λ mit $\lambda \neq 0, 1$ bzw. die Nullabbildung, so ist f eine Translation bzw. eine Dehnung von $\boldsymbol{A}$ bzw. eine konstante Abbildung. Zum Beweis beachte man auch den Beweis von Satz 4.3.5.

Satz 1. *Die Zuordnung, die jedem affinen Punktraum $\boldsymbol{A}^n$ den zugehörigen Vektorraum $\boldsymbol{V}^n$ und jeder affinen Abbildung f die zugehörige lineare Abbildung a_f nach* (1) *zuordnet, ist ein kovarianter Funktor der affinen Kategorie über dem Körper K in die Kategorie der Vektorräume über K, d. h., es gelten* (3) *und*

$$a_{g \circ f} = a_g \circ a_f . \tag{5}$$

Beweis. Es ist nur noch (5) zu zeigen. Diese Gleichung ergibt sich unmittelbar aus Satz 1.2 und (2):

$$a_{g \circ f}(\vec{xy}) = \overrightarrow{g(f(x))\,g(f(y))} = a_g(\overrightarrow{f(x)\,f(y)}) = a_g(a_f(\vec{xy})) . \quad \square$$

Folgerung 1. a) *Die affine Abbildung $f \in \mathfrak{A}(\boldsymbol{A}, \boldsymbol{B})$ ist injektiv bzw. surjektiv bzw. bijektiv dann und nur dann, wenn die zugeordnete lineare Abbildung a_f die entsprechende Eigenschaft besitzt.* — b) *Ist f bijektiv, so gilt*

$$a_{f^{-1}} = (a_f)^{-1} . \tag{6}$$

c) *Ist* $\dim \boldsymbol{A} = \dim \boldsymbol{B} = n < \infty$, *so gilt*

$$f \text{ injektiv} \Leftrightarrow f \text{ surjektiv} \Leftrightarrow f \text{ bijektiv} .$$

Beweis. a) ergibt sich sofort aus (2) wegen

$$f(x) = f(p) + a_f(\vec{px}) . \tag{7}$$

b) folgt wie bei jedem Funktor aus (3) und (5). — c) ergibt sich aus a) und Folgerung 2.8. $\square$

Satz 2. *Es seien $f, g \in \mathfrak{A}(\boldsymbol{A}, \boldsymbol{B})$. Dann gilt $a_f = a_g$ dann und nur dann, wenn ein Vektor $\mathfrak{a}$ aus dem Vektorraum $\boldsymbol{W}$ von $\boldsymbol{B}$ existiert mit $f = t_\mathfrak{a} \circ g$.*

Beweis. Es sei $p \in \boldsymbol{A}$, $p' = f(p)$ und $q' = g(p)$. Mit $a := a_f = a_g$ erhalten wir $f(x) = p' + a(\vec{px})$ und $g(x) = q' + a(\vec{px})$ aus (7). Hieraus folgt für alle $x \in \boldsymbol{A}$

$$f(x) = (q' + a(\vec{px})) + \vec{q'p'} = t_{\mathfrak{a}} \circ g(x)$$

mit $\mathfrak{a} = \vec{q'p'}$. Die Umkehrung ergibt sich sofort aus (5) und Beispiel 1. □

Folgerung 2. *Es sei* $\mathfrak{A}(\boldsymbol{A})$ *die Gruppe der affinen Transformationen von* $\boldsymbol{A}$ *und* $\mathfrak{T}(\boldsymbol{A}) \subset \mathfrak{A}(\boldsymbol{A})$ *die Untergruppe der Translationen* (Satz 4.3.1). *Dann ist* $\Phi: f \in \mathfrak{A}(\boldsymbol{A}) \mapsto \Phi(f) = a_f \in \boldsymbol{GL}(\boldsymbol{V})$, $\boldsymbol{V}$ *der Vektorraum von* $\boldsymbol{A}$, *ein Homomorphismus von* $\mathfrak{A}(\boldsymbol{A})$ *auf die lineare Gruppe* $\boldsymbol{GL}(\boldsymbol{V})$ *mit dem Kern* $\mathfrak{T}(\boldsymbol{A})$. *Daher ist* $\mathfrak{T}(\boldsymbol{A})$ *ein Normalteiler von* $\mathfrak{A}(\boldsymbol{A})$, *und es besteht ein kanonischer Isomorphismus der Gruppen*

$$\boldsymbol{GL}(\boldsymbol{V}) \cong \mathfrak{A}(\boldsymbol{A})/\mathfrak{T}(\boldsymbol{A}) \,. \tag{8}$$

Beweis. Wegen (5) ist Φ eine Homomorphie. Nach Satz 1.4 können wir die Abbildung $a \in \boldsymbol{GL}(\boldsymbol{V})$ beliebig vorgeben; somit ist Φ surjektiv. Ist $\Phi(f) = \mathrm{id}_{\boldsymbol{V}}$, so ist nach (3) und Satz 2 $f = t_{\mathfrak{a}} \circ \mathrm{id}_{\boldsymbol{A}} = t_{\mathfrak{a}}$ eine Translation, also Ker $\Phi = \mathfrak{T}(\boldsymbol{A})$. Der Rest der Behauptung folgt aus dem Homomorphiesatz für Gruppen, Satz 3.1.6. □

Satz 3. *Es sei* $\boldsymbol{A}$ *ein affiner Punktraum mit dem Vektorraum* $\boldsymbol{V}$ *und* $o \in \boldsymbol{A}$, *ferner sei* $\mathfrak{H}_0 \subset \mathfrak{A}(\boldsymbol{A})$ *die Isotropiegruppe des Punktes* o. *Dann wird durch*

$$a \in \boldsymbol{GL}(\boldsymbol{V}) \mapsto f_a \in \mathfrak{H}_0 \quad \textit{mit} \quad f_a(x) := o + a(\vec{ox}) \tag{9}$$

ein Isomorphismus von $\boldsymbol{GL}(\boldsymbol{V})$ *auf* $\mathfrak{H}_0$ *definiert, und es gilt*

$$\mathfrak{H}_0 \cap \mathfrak{T}(\boldsymbol{A}) = \{\mathrm{id}_{\boldsymbol{A}}\}. \qquad \mathfrak{T}(\boldsymbol{A}) \circ \mathfrak{H}_0 = \mathfrak{A}(\boldsymbol{A}) \,. \tag{10}$$

Beweis. Nach (7) ist f_a eine affine Abbildung mit $f_a(o) = o$, also $f_a \in \mathfrak{H}_0$. Nach Satz 1.4 kann man jedes $f \in \mathfrak{H}_0$ in der Form (9) darstellen, also ist die Abbildung (9) surjektiv. Wegen $\Phi(f_a) = a$ ist $\Phi \mid \mathfrak{H}_0$ die Inverse der Abbildung (9); also ist sie bijektiv und, weil Φ ein Homomorphismus ist, ein Isomorphismus. Die erste der Beziehungen (10) ist trivial, und die zweite ist durch Satz 1.5 bereits bewiesen. □

Bemerkung. Wegen Folgerung 2 und (10) ist $\mathfrak{A}(\boldsymbol{A})$ halbdirektes Produkt von $\mathfrak{H}_0 \cong \boldsymbol{GL}(\boldsymbol{V})$ und $\mathfrak{T}(\boldsymbol{A})$, vgl. Übung 3.2.3. Identifizieren wir $\mathfrak{H}_0 \equiv \boldsymbol{GL}(\boldsymbol{V})$ mittels (9), so erhalten wir einen Isomorphismus der Transformationsgruppen $[\mathfrak{A}(\boldsymbol{A}), \boldsymbol{A}]$ und $[\mathfrak{A}(\boldsymbol{A}), \mathfrak{A}(\boldsymbol{A})/\boldsymbol{GL}(\boldsymbol{V})]$, vgl. Satz 3.1.7.

Ähnlich, wie wir in § 2 die linearen Abbildungen durch die Bilder einer Basis charakterisieren konnten, wollen wir jetzt die affinen Abbildungen durch die Bilder von $n+1$ Punkten in allgemeiner Lage beschreiben.

Satz 4. *Es sei* (p_i), $i = 0, 1, \ldots, n$, *eine Folge aus* $n+1$ *Punkten* $p_i \in \boldsymbol{A}^n$ *in allgemeiner Lage und* (q_i) *eine beliebige Punktfolge aus* $n+1$ *Punkten des affinen Raumes* $\boldsymbol{B}$ *über demselben Körper* K. *Dann gilt:* a) *Es existiert genau eine affine Abbildung* $f: \boldsymbol{A}^n \to \boldsymbol{B}$ *mit* $f(p_i) = q_i$ *für* $i = 0, \ldots, n$. — b) f *ist injektiv dann und nur dann, wenn die Punktfolge* (q_i) *ebenfalls in allgemeiner Lage ist.* — c) f *ist surjektiv dann und nur dann, wenn die von* $\{q_i\}$ *erzeugte Ebene* $\boldsymbol{H}(\{q_i\}) = \boldsymbol{B}$ *ist.*

Beweis. a) Nach Definition 4.5.5 sind die Vektoren $\mathfrak{a}_i = \overrightarrow{p_0 p_i}$, $i = 1, \ldots, n$, linear unabhängig und bilden daher eine Basis des zu $\boldsymbol{A}^n$ gehörenden Vektorraumes $\boldsymbol{V}^n$. Wenn f die gesuchte affine Abbildung ist, muß notwendig für die zugehörige lineare Abbildung

$$a_f(\mathfrak{a}_i) = \overrightarrow{q_0 q_i}, \qquad i = 1, \ldots, n\,, \tag{11}$$

sein. Umgekehrt wird durch (11) nach Satz 2.5 eindeutig eine lineare Abbildung a_f von $\boldsymbol{V}^n$ in den Vektorraum $\boldsymbol{W}$ von $\boldsymbol{B}$ definiert, und diese bestimmt zusammen mit $f(p_0) = q_0$ nach Satz 1.4 eindeutig die gesuchte affine Abbildung. – b) Nach Folgerung 1 ist f injektiv genau dann, wenn a_f injektiv, also Ker $a_f = 0$ und wegen Folgerung 2.7 dim Im $a_f = n$ gilt. Da die Menge $\{\overrightarrow{q_0 q_i}\}_{i=1,\ldots,n}$ Im a_f erzeugt, muß sie linear unabhängig sein und aus n Vektoren bestehen. – c) f ist surjektiv genau dann, wenn a_f surjektiv ist, und das ist äquivalent zu $\mathfrak{L}(\{\overrightarrow{q_0 q_i}\}_i) = \boldsymbol{W}$. Setzt man in Satz 4.5.3 $b = q_0$ und $B = \{q_i\}_{i=0,\ldots,n}$, so folgt nach (4.5.17) die Behauptung. □

Folgerung 3. *Die affine Abbildung $f\colon \boldsymbol{A}^n \to \boldsymbol{B}^m$ ist ein Isomorphismus dann und nur dann, wenn $n = m$ ist und $n+1$ Punkte $p_i \in \boldsymbol{A}^n$ in allgemeiner Lage wieder in $n+1$ Punkte $q_i = f(p_i)$, $i = 0, \ldots, n$, in allgemeiner Lage übergehen.* □

Folgerung 4. *Zwei affine Punkträume $\boldsymbol{A}^n$, $\boldsymbol{B}^m$ über demselben Körper K sind genau dann isomorph, wenn $n = m$ gilt.* □

Beispiel 4. Fassen wir nach Beispiel 4.3.1 den n-Tupelraum K^n als n-dimensionalen affinen Raum über K auf, so ist die Koordinatenabbildung (4.4.10) ein Isomorphismus von $\boldsymbol{A}^n$ auf K^n; die affinen Räume K^n sind also ein vollständiges Repräsentantensystem für die Isomorphieklassen der endlichdimensionalen affinen Räume über K.

Beispiel 5. Im $\boldsymbol{A}^n$ können wir für $n = 1$ jede Strecke in jede Strecke, für $n = 2$ jedes Dreieck in jedes Dreieck, für $n = 3$ jedes Tetraeder in jedes Tetraeder durch eine affine Transformation überführen, wobei die Reihenfolge, in der die Eckpunkte p_i von Δ in die Eckpunkte q_i von $f(\Delta)$ übergehen sollen, noch beliebig vorgegeben werden kann. So gibt es $(n+1)!$ verschiedene affine Transformationen, die eine Punktmenge $B \subset \boldsymbol{A}^n$ aus $n+1$ Punkten in allgemeiner Lage in sich transformieren: $f(B) = B$; sie entsprechen den Permutationen dieser Menge. Analog zu Beispiel 2.3 macht man sich leicht klar, daß die Menge aller Folgen (q_i) aus $n+1$ Punkten in allgemeiner Lage des affinen Raumes $\boldsymbol{A}^n$ zur Veranschaulichung der affinen Gruppe $\mathfrak{A}(\boldsymbol{A}^n)$ dienen kann.

Die affinen Isomorphismen übertragen alle affinen, d. h. aus den Axiomen der affinen Geometrie folgenden Eigenschaften, „sie lassen diese invariant". Es ergibt sich die Frage, welche affinen Eigenschaften bei allgemeinen, nicht notwendig injektiven affinen Abbildungen erhalten bleiben. Hierüber geben die folgenden Sätze Auskunft.

Satz 5. *Es sei $f \in \mathfrak{A}(\boldsymbol{A}, \boldsymbol{B})$ und $\boldsymbol{H}(p, \boldsymbol{U}) \subseteq \boldsymbol{A}$ die von $p \in \boldsymbol{A}$ und dem Unterraum $\boldsymbol{U}$ aufgespannte Ebene. Dann gilt*

$$f(\boldsymbol{H}(p, \boldsymbol{U})) = \boldsymbol{H}(f(p), a_f(\boldsymbol{U}))\,. \tag{12}$$

Beweis. Ist $y=f(x)$, $x=p+\mathfrak{u}\in\boldsymbol{H}(p, \boldsymbol{U})$, so ist $\mathfrak{u}\in\boldsymbol{U}$ und

$$y=f(p)+\overrightarrow{f(p)\,f(x)}=f(p)+a_f(\mathfrak{u})\in\boldsymbol{H}(f(p), a_f(\boldsymbol{U}))\,.$$

Umgekehrt, ist $y=f(p)+\mathfrak{z}$, $\mathfrak{z}=a_f(\mathfrak{u})\in a_f(\boldsymbol{U})$, $\mathfrak{u}\in\boldsymbol{U}$, so ist $x=p+\mathfrak{u}$ ein Punkt aus $\boldsymbol{H}(p, \boldsymbol{U})$ mit $f(x)=y$, und es gilt (12). □

Aus Satz 2.2 und Folgerung 2.5 erhält man unmittelbar

Folgerung 5. *Unter den Voraussetzungen von Satz* 5 *gilt:* a) *Das Bild einer Ebene ist wieder eine Ebene, und es ist*

$$\dim f(\boldsymbol{H}(p, \boldsymbol{U}))\leqq\dim\boldsymbol{H}(p, \boldsymbol{U})\,. \tag{13}$$

b) *Ist f injektiv, so gilt in* (13) *das Gleichheitszeichen.*

c) $\dim f(\boldsymbol{A})\leqq\min(\dim\boldsymbol{A}, \dim\boldsymbol{B})$. □ (14)

Aus der Definition der Parallelität und Satz 5 folgt

Folgerung 6. *Ist $f\in\mathfrak{A}(\boldsymbol{A}, \boldsymbol{B})$ und sind $\boldsymbol{H}_1, \boldsymbol{H}_2\subset\boldsymbol{A}$ parallele Ebenen, so sind auch die Bilder parallel: $f(\boldsymbol{H}_1)\parallel f(\boldsymbol{H}_2)$.* □

Satz 6. *Es sei $f\in\mathfrak{A}(\boldsymbol{A}, \boldsymbol{B})$ und $M\subseteq\boldsymbol{A}$ eine Punktmenge. Für das Bild der von M aufgespannten Ebene gilt*

$$f(\boldsymbol{H}(M))=\boldsymbol{H}(f(M))\,. \tag{15}$$

Beweis. Für $M=\emptyset$ ist die Behauptung des Satzes trivial. Nach Satz 4.5.3 gilt für ein $b\in M$ die Darstellung $\boldsymbol{H}(M)=b+\mathfrak{L}(V(M))$, $V(M)$ die Vektormenge von M. Aus (12) folgt $f(\boldsymbol{H}(M))=\boldsymbol{H}(f(b), a_f(\mathfrak{L}(V(M))))$. Nach Übung 2.1 ist $a_f(\mathfrak{L}(V(M)))=$ $=\mathfrak{L}(a_f(V(M)))$. Aus (2) und der Definition (4.5.4) der Vektormenge erhält man

$$a_f(V(M))=V(f(M))\,. \tag{16}$$

Setzt man die erhaltenen Identitäten ein, so ergibt sich wieder aus Satz 4.5.3

$$f(\boldsymbol{H}(M))=\boldsymbol{H}(f(b), V(f(M)))=\boldsymbol{H}(f(M))\,.$$ □

Folgerung 7. *Es sei $f\in\mathfrak{A}(\boldsymbol{A}, \boldsymbol{B})$ und $\boldsymbol{H}_1, \boldsymbol{H}_2\subseteq\boldsymbol{A}$ seien Ebenen. Dann gilt für die Verbindungsebene*

$$f(\boldsymbol{H}_1\vee\boldsymbol{H}_2)=f(\boldsymbol{H}_1)\vee f(\boldsymbol{H}_2)\,.$$ □ (17)

Wir überlassen dem Leser die Beweise der folgenden Sätze über die Urbilder von Ebenen:

Satz 7. *Es sei $f\in\mathfrak{A}(A, \boldsymbol{B})$ und $\boldsymbol{H}=\boldsymbol{H}(q, \boldsymbol{U})\subseteq\boldsymbol{B}$ eine Ebene. Dann ist $f^{-1}(\boldsymbol{H})=\emptyset$, oder für ein beliebiges $p\in f^{-1}(\boldsymbol{H})$ gilt*

$$f^{-1}(\boldsymbol{H})=\boldsymbol{H}(p, a_f^{-1}(\boldsymbol{U}))\,.$$ □ (18)

Folgerung 8. *Sind bei den Voraussetzungen von Satz 7 $\boldsymbol{H}_1, \boldsymbol{H}_2\subset\boldsymbol{B}$ Ebenen mit $\boldsymbol{H}_1\parallel\boldsymbol{H}_2$ und gilt $f^{-1}(\boldsymbol{H}_i)\neq\emptyset$ für $i=1, 2$, so ist*

$$f^{-1}(\boldsymbol{H}_1)\parallel f^{-1}(\boldsymbol{H}_2)\,.$$ □ (19)

Übung 1. Man zeige: Für $n \geqq 2$ gibt es eine affine Transformation $f \in \mathfrak{A}(\boldsymbol{A}^n)$, die keinen Fixpunkt hat und keine Translation ist.

Übung 2. Es sei $\boldsymbol{A}^n$ ein n-dimensionaler affiner Raum über einem Körper K mit $\operatorname{char} K = 0$, $B := \{p_0, p_1, \ldots, p_n\} \subset \boldsymbol{A}^n$ eine Menge aus $n+1$ Punkten in allgemeiner Lage und $\mathfrak{J} \subseteq \mathfrak{A}(\boldsymbol{A}^n)$ die stationäre Untergruppe der Menge B, d. h. $\mathfrak{J} := \{f \in \mathfrak{A}(\boldsymbol{A}^n) \mid f(B) = B\}$. Offenbar ist $\mathfrak{J}$ isomorph zur symmetrischen Gruppe S_{n+1}. Man bestimme den einzigen Punkt $x_0 \in \boldsymbol{A}^n$, der bei allen Transformationen $f \in \mathfrak{J}$ fest bleibt: $f(x_0) = x_0$ für alle $f \in \mathfrak{J}$. (Hinweis. Man beachte Übung 4.5.5.)

Übung 3. Es sei $\boldsymbol{B}^k \subseteq \boldsymbol{A}^n$ eine k-Ebene des affinen Punktraumes $\boldsymbol{A}^n$. Nach Satz 4.5.1 ist dann $\boldsymbol{B}^k$ ebenfalls ein affiner Punktraum. Man beweise: a) Ist $f: \boldsymbol{A}^n \to \boldsymbol{A}^n$ eine affine Abbildung und gilt $f(\boldsymbol{B}^k) \subseteq \boldsymbol{B}^k$, so ist $f \mid \boldsymbol{B}^k$ eine affine Abbildung von $\boldsymbol{B}^k$ in sich. — b) Ist $g: \boldsymbol{B}^k \to \boldsymbol{B}^k$ eine beliebige affine Abbildung, so gibt es eine affine Abbildung $f: \boldsymbol{A}^n \to \boldsymbol{A}^n$ mit $f \mid \boldsymbol{B}^k = g$; hierbei kann man sogar zusätzlich $f(\boldsymbol{A}^n) \subseteq \boldsymbol{B}^k$ fordern. — c) Ist $g \in \mathfrak{A}(\boldsymbol{B}^k)$, so gibt es eine bijektive Abbildung $f \in \mathfrak{A}(\boldsymbol{A}^n)$ mit $f \mid \boldsymbol{B}^k = g$.

Übung 4. Es seien $\boldsymbol{A}^n$, $\boldsymbol{B}^m$ affine Punkträume, $\boldsymbol{H}^1 \subseteq \boldsymbol{A}^n$, $\boldsymbol{M}^1 \subseteq \boldsymbol{B}^m$ zwei Geraden und $\{a_1, \ldots, a_r\} \subseteq \boldsymbol{H}^1$, $\{b_1, \ldots, b_r\} \subseteq \boldsymbol{M}^1$ zwei Mengen aus lauter verschiedenen Punkten, $r \in \mathbf{N}$, $r \geqq 3$. Es gibt eine affine Abbildung $f: \boldsymbol{A}^n \to \boldsymbol{B}^m$ mit $f(a_i) = b_i$ für $i = 1, \ldots, r$ dann und nur dann, wenn für $\varrho = 3, \ldots, r$ stets

$$\frac{\overrightarrow{b_1 b_\varrho}}{\overrightarrow{b_1 b_2}} = \frac{\overrightarrow{a_1 a_\varrho}}{\overrightarrow{a_1 a_2}}$$

gilt.

Übung 5. Man zeige: Die affine Gruppe $\mathfrak{A}(\boldsymbol{A}^n)$ ist im Fall $n > 0$, $|K| \neq 2$, nicht abelsch.

Übung 6. a) Es seien $\boldsymbol{V}$ ein Vektorraum, $a, b \in \boldsymbol{L}(\boldsymbol{V})$ und $a \circ b = \mathrm{id}_{\boldsymbol{V}}$. Man beweise, daß a bijektiv ist und $b = a^{-1}$ gilt. — b) Es seien $\boldsymbol{A}$ ein affiner Raum, $f, g: \boldsymbol{A} \to \boldsymbol{A}$ affine Abbildungen und $f \circ g = \mathrm{id}_{\boldsymbol{A}}$. Man zeige wieder $g = f^{-1}$, f bijektiv. — c) Man gebe ein Beispiel für eine Menge M und zwei Abbildungen $g, f: M \to M$ an, für die $f \circ g = \mathrm{id}_M$, aber nicht $g = f^{-1}$ gilt.

§ 4. Endomorphismenalgebra und Matrizenalgebra

Gegenstand dieses Paragraphen ist die Begründung der Matrizenrechnung. Die Theorie der Matrizen ist ein wichtiges Hilfsmittel für die Lösung geometrischer Probleme. Die Bedeutung dieser Theorie geht jedoch weit über die Geometrie hinaus; es gibt wohl kaum eine mathematische Disziplin, in der die Matrizen keine Anwendung finden.

In diesem Paragraphen wollen wir durchweg voraussetzen, daß ein Körper K gegeben sei; $\boldsymbol{V}, \boldsymbol{W}, \ldots$, seien *endlichdimensionale* Vektorräume über K. Jeder linearen Abbildung wollen wir umkehrbar eindeutig eine von den Basen in $\boldsymbol{V}, \boldsymbol{W}$ abhängende Matrix aus Elementen von K zuordnen. Neben der Verknüpfung $\circ$ werden wir noch eine Addition $+$ für die linearen Abbildungen einführen; bezüglich dieser Operationen wird $\boldsymbol{L}(\boldsymbol{V})$ ein Ring, besser gesagt, eine Algebra, vgl. Definition 7. Die oben erwähnte bijektive Zuordnung übersetzt diese Algebren-Struktur isomorph in die betrachteten Matrizenmengen, und die so entstehenden Operationen für die Matrizen bilden die Grundlage der Matrizenrechnung.

Definition 1. Mit $\mathbf{M}_{m,n}(K)$, oder kurz $\mathbf{M}_{m,n}$, bezeichnen wir die Menge der Matrizen

$$(a_{\alpha i}) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}, \qquad a_{\alpha i} \in K . \tag{1}$$

Wir werden, wenn nichts anderes gesagt ist, immer voraussetzen, daß die Indizes i, j, k, l die Werte 1, ..., n und die Indizes α, β, γ, ... die Werte 1, ..., m durchlaufen. (Zur allgemeinen Definition einer Matrix vgl. Beispiel 0.2.11, Definition 4.7.2.)

Definition 2. Es seien $\boldsymbol{V}^n$, $\boldsymbol{W}^m$ Vektorräume über K, $(\mathfrak{a}_i)$ Basis von $\boldsymbol{V}^n$, $(\mathfrak{b}_\alpha)$ Basis von $\boldsymbol{W}^m$ und $a \in \boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{W}^m)$. Setzen wir

$$a(\mathfrak{a}_i) = \sum_{\alpha=1}^{m} \mathfrak{b}_\alpha a_{\alpha i}, \qquad i = 1, \dots, n , \tag{2}$$

so entsteht eine Matrix $(a_{\alpha i}) \in \mathbf{M}_{m,n}(K)$, die man die *Matrix von a bezüglich der Basen* $(\mathfrak{a}_i)$, $(\mathfrak{b}_\alpha)$ nennt.

Satz 1. *Es seien die Voraussetzungen der Definition 2 erfüllt. Dann ist die Abbildung*

$$a \in \boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{W}^m) \mapsto (a_{\alpha i}) \in \mathbf{M}_{m,n}(K) \tag{3}$$

bijektiv.

Beweis. Nach Satz 2.5 ist jede lineare Abbildung durch die Bilder $\mathfrak{c}_i = a(\mathfrak{a}_i)$ einer Basis eindeutig bestimmt. Da die Spalten der Matrix $(a_{\alpha i})$ aus den Koordinaten der Bildvektoren $\mathfrak{c}_i$ bestehen, gibt es zu jeder Matrix eine und nur eine lineare Abbildung, nämlich die durch

$$\mathfrak{c}_i = \sum_{\alpha} \mathfrak{b}_\alpha a_{\alpha i} \tag{4}$$

und (2) gegebene. □

Beispiel 1. Der Nullabbildung $a(\mathfrak{x}) = \mathfrak{o}$ für alle $\mathfrak{x} \in \boldsymbol{V}^n$ entspricht die *Nullmatrix* $(a_{\alpha i}) = (0)$, d. h. $a_{\alpha i} = 0$ für alle α, i.

Beispiel 2. Es sei $a \in \boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{W}^m)$ mit $\operatorname{rg} a = r$. Wir wählen die Basen $(\mathfrak{a}_i)$, $(\mathfrak{b}_\alpha)$ wie in Lemma 2.1. Dann hat a die Matrix

$$(a_{\alpha i}) = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & \dots & \dots & 1 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & \dots & \dots & 0 & 0 & \dots & 0 \end{pmatrix} \begin{matrix} \\ \\ \\ r \\ \\ \\ \end{matrix}, \tag{5}$$
$$\qquad\qquad r$$

d. h. $a_{\alpha i} = 1$ für $\alpha = i = 1, \dots, r$ und $a_{\alpha i} = 0$ sonst.

Lemma 2.1 besagt, daß man zu jeder Abbildung a vom Rang r die beiden Basen $(\mathfrak{a}_i)$, $(\mathfrak{b}_\alpha)$ so wählen kann, daß die Matrix $(a_{\alpha i})$ von a die nur von $\operatorname{rg} a$ abhängige Gestalt (5) hat.

Beispiel 3. Es sei $e = \mathrm{id}_{V^n}$ die identische Abbildung von V^n. Dann gilt für jede Basis $(\mathfrak{a}_i)$ von V^n die Beziehung $e(\mathfrak{a}_i) = \mathfrak{a}_i$; die Matrix von e ist also die Einheitsmatrix (4.7.26)

$$e = \mathrm{id}_{V^n} \mapsto (\delta_{ij}) , \tag{6}$$

δ_{ij} das Kronecker-Symbol (4.7.25). Offenbar ist (6) ein Spezialfall von (5).

Beispiel 4. Es sei $m = n$. In diesem Fall schreibt man zur Abkürzung

$$\mathbf{M}_n(K) := \mathbf{M}_{n,n}(K) . \tag{7}$$

Die Matrizen $(a_{ij}) \in \mathbf{M}_n(K)$ heißen *quadratisch* (mit n Zeilen). Als Spezialfall von (3) erhalten wir die Abbildung

$$a \in \boldsymbol{L}(V^n) \mapsto (a_{ij}) \in \mathbf{M}_n(K) \tag{8}$$

bei Wahl einer einzigen Basis $(\mathfrak{a}_i) = (\mathfrak{b}_\alpha)$ von $V^n = W^m$. Man beachte, daß es durch Wahl einer einzigen Basis im allgemeinen nicht möglich ist, die Matrix eines linearen Endomorphismus auf die Gestalt (5) zu bringen. Zum Beispiel hat jede Dehnung $d_\lambda(\mathfrak{x}) = \mathfrak{x}\lambda$ bei jeder Basis $(\mathfrak{a}_i)$ von V^n die Matrix

$$(a_{ij}) = \begin{pmatrix} \lambda & 0 & \dots & 0 \\ 0 & \lambda & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda \end{pmatrix} = (\lambda \delta_{ij}) . \tag{9}$$

Beispiel 5. Es sei $a \in \boldsymbol{L}(V^n)$ ein Endomorphismus, der eine Basis $(\mathfrak{a}_i)$ aus lauter Eigenvektoren (Definition 2.4) besitzt: $a(\mathfrak{a}_i) = \mathfrak{a}_i \lambda_i$. In dieser Basis hat die Matrix von a Diagonalform (§ 4.8):

$$(a_{ij}) = (\lambda_i \delta_{ij}) \tag{10}$$

mit den Eigenwerten in der Hauptdiagonalen. Endomorphismen, für die eine Basis aus Eigenvektoren existiert, heißen *diagonalisierbar*. Das Ergebnis von Übung 2.3, c), kann man auch so formulieren: Hat ein Endomorphismus $a \in \boldsymbol{L}(V^n)$ n verschiedene Eigenwerte, so ist er diagonalisierbar.

Übung 1. Man zeige: a) Der Operator $a \in \boldsymbol{L}(V^n)$ ist diagonalisierbar genau dann, wenn $V^n = \overset{r}{\underset{i=1}{\oplus}} \boldsymbol{U}_{\lambda_i}$ gilt, wobei $\boldsymbol{U}_{\lambda_i}$ die Eigenunterräume der verschiedenen Eigenwerte λ_i von a sind. — b) Der Rang des diagonalisierbaren Operators a ist gleich der Anzahl der von 0 verschiedenen Elemente auf der Hauptdiagonalen der Matrix von a in einer Basis aus Eigenvektoren von a.

Übung 2. Es sei $a \in \boldsymbol{L}(V^n)$ und $\operatorname{char} K \neq 2$. Man beweise: a ist eine Involution genau dann, wenn es eine Basis $(\mathfrak{a}_i)$ von V^n gibt, bezüglich der die Matrix von a folgende Ge-

stalt hat:

$$(a_{ij}) = (\varepsilon_i \delta_{ij}), \qquad \varepsilon_i = 1 \quad \text{für} \quad i = 1, \ldots, s,$$
$$\varepsilon_i = -1 \quad \text{für} \quad i = s+1, \ldots, n. \tag{11}$$

Definition 3. Es sei $a \in \boldsymbol{L}(\boldsymbol{V})$. Ein Unterraum $\boldsymbol{U} \subseteq \boldsymbol{V}$ heißt *invariant bei* a, wenn $a(\boldsymbol{U}) \subseteq \boldsymbol{U}$ gilt.

Beispiel 6. Die Eigenunterräume $\boldsymbol{U}_\lambda$ (Definition 2.4) eines Endomorphismus a sind invariante Unterräume.

Übung 3. Es sei $a \in \boldsymbol{L}(\boldsymbol{V})$. Man beweise: Ker a und Im a sind bei a invariante Unterräume.

Übung 4. Es sei $a \in \boldsymbol{L}(\boldsymbol{V}^n)$. Man beweise: a) Ist a diagonalisierbar, so ist ein Unterraum $\boldsymbol{W} \subseteq \boldsymbol{V}$ dann und nur dann bei a invariant, wenn $\boldsymbol{W} = \overset{r}{\underset{i=1}{\oplus}} \boldsymbol{W} \cap \boldsymbol{U}_{\lambda_i}$ gilt, vgl. Übung 1a). — b) Sind $a, b \in \boldsymbol{L}(\boldsymbol{V}^n)$ diagonalisierbar und gilt $a \circ b = b \circ a$, dann gibt es eine Basis von $\boldsymbol{V}^n$, deren Vektoren Eigenvektoren von a *und* von b sind. Man verallgemeinere dieses Ergebnis auf eine beliebige Menge $\boldsymbol{M} \subseteq \boldsymbol{L}(\boldsymbol{V})$ von paarweise kommutierenden Operatoren.

Definition 4. Eine Folge von Unterräumen

$$\boldsymbol{U}_1 \subset \ldots \subset \boldsymbol{U}_n = \boldsymbol{V}^n, \qquad \dim \boldsymbol{U}_i = i, \tag{12}$$

heißt eine *Flagge* von $\boldsymbol{V}^n$. Eine Basis $(\mathfrak{a}_i)$ von $\boldsymbol{V}^n$ heißt *der Flagge angepaßt*, wenn

$$\mathfrak{L}(\{\mathfrak{a}_1, \ldots, \mathfrak{a}_i\}) = \boldsymbol{U}_i, \qquad i = 1, \ldots, n, \tag{13}$$

gilt.

Übung 5. Man beweise: Zu jeder Flagge $(\boldsymbol{U}_i)$ von $\boldsymbol{V}^n$ gibt es eine angepaßte Basis.

Übung 6. Es sei $a \in \boldsymbol{L}(\boldsymbol{V}^n)$. Wir sagen, *$a$ läßt die Flagge $(\boldsymbol{U}_i)$ invariant*, wenn $a(\boldsymbol{U}_i) \subseteq \boldsymbol{U}_i$ für $i = 1, \ldots, n$ gilt. Man beweise: Es gibt zu $a \in \boldsymbol{L}(\boldsymbol{V}^n)$ eine invariante Flagge dann und nur dann, wenn eine Basis $(\mathfrak{a}_i)$ von $\boldsymbol{V}^n$ existiert, bezüglich der die Matrix (a_{ij}) von a Dreiecksgestalt hat:

$$(a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \ldots & a_{1n} \\ & a_{22} & a_{23} & \ldots & a_{2n} \\ & & a_{33} & \ldots & a_{3n} \\ & & & \ddots & \vdots \\ & 0 & & & a_{nn} \end{pmatrix} \tag{14}$$

Wir kehren nun wieder zum allgemeinen Fall zurück und wollen die bereits in den einleitenden Bemerkungen angekündigte Addition sowie eine Multiplikation mit einem Skalar $\alpha \in K$ punktweise definieren (vgl. Beispiel 1.1.8):

Definition 5. Es seien $a, b \in \boldsymbol{L}(\boldsymbol{V}, \boldsymbol{W})$, $\alpha \in K$. Wir definieren für alle $\mathfrak{x} \in \boldsymbol{V}$

$$(a+b)(\mathfrak{x}) := a(\mathfrak{x}) + b(\mathfrak{x}), \tag{15}$$

$$(a\alpha)(\mathfrak{x}) := a(\mathfrak{x}) \cdot \alpha. \tag{16}$$

Satz 2. *Mit den Operationen* (15) *und* (16) *wird* $[\boldsymbol{L}(\boldsymbol{V}, \boldsymbol{W}), +, K]$ *ein Vektorraum über* K.

Beweis. Man beweist leicht, daß $[\boldsymbol{L}(\boldsymbol{V}, \boldsymbol{W}), +]$ eine abelsche Gruppe ist mit der Nullabbildung als 0 und dem inversen $(-a)(\mathfrak{x}) = -a(\mathfrak{x})$; denn mit a und b ist auch $a+b$ wieder linear, und mit $\alpha \in K$, $a \in \boldsymbol{L}(\boldsymbol{V}, \boldsymbol{W})$ gilt auch $a\alpha \in \boldsymbol{L}(\boldsymbol{V}, \boldsymbol{W})$. Es bleiben die Bedingungen (4.2.2) bis (4.2.5) der Definition 4.2.1 eines Vektorraumes zu überprüfen. Diese folgen leicht aus den entsprechenden Eigenschaften von $\boldsymbol{W}$. Wir zeigen z. B. die Distributivität:

$$\begin{aligned}((a+b)\,\alpha)(\mathfrak{x}) &= (a+b)(\mathfrak{x})\,\alpha = (a(\mathfrak{x})+b(\mathfrak{x}))\,\alpha \\ &= a(\mathfrak{x})\alpha + b(\mathfrak{x})\,\alpha = (a\alpha)(\mathfrak{x}) + (b\alpha)(\mathfrak{x}) = (a\alpha + b\alpha)(\mathfrak{x})\,.\end{aligned}$$

Da diese Beziehung für alle $\mathfrak{x}$ gilt, erhalten wir $(a+b)\,\alpha = a\alpha + b\alpha$. Analog beweist man die restlichen Bedingungen. □

Wir bemerken, daß Satz 2 ein Analogon zu Übung 1.2.12 darstellt, man beachte hierzu Beispiel 4.2.4. Weiter erkennt man, daß für die Richtigkeit von Satz 2 keine Voraussetzungen über die Dimensionen von $\boldsymbol{V}$ und $\boldsymbol{W}$ gemacht werden müssen. Wir wollen Satz 2 nun auf den Fall endlichdimensionaler Vektorräume spezialisieren.

Satz 3. *Gilt* dim $\boldsymbol{V}^n = n$, dim $\boldsymbol{W}^m = m$, so ist

$$\dim \boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{W}^m) = n \cdot m; \tag{17}$$

die Abbildung (3) *ist ein Isomorphismus von* $\boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{W}^m)$ *auf den Vektorraum* $\mathbf{M}_{m,n}(K) = K^{m \cdot n}$, *der sich bei Auffassung der Matrizen als* $(m \cdot n)$*-Tupel ergibt.*

Beweis. Offenbar genügt es, die zweite Behauptung zu beweisen (vgl. Folgerung 4.4.4). Wir wählen Basen $(\mathfrak{a}_i)$ von $\boldsymbol{V}^n$ und $(\mathfrak{b}_\alpha)$ von $\boldsymbol{W}^m$. Nach Satz 1 ist (3) bijektiv. Wir berechnen die Matrix von $(a+b)$ aus den Matrizen $(a_{\alpha i})$ von a und $(b_{\alpha i})$ von b. Nach (15) gilt

$$(a+b)(\mathfrak{a}_i) = a(\mathfrak{a}_i) + b(\mathfrak{a}_i) = \sum_\alpha \mathfrak{b}_\alpha a_{\alpha i} + \sum_\alpha \mathfrak{b}_\alpha b_{\alpha i} = \sum_\alpha \mathfrak{b}_\alpha (a_{\alpha i} + b_{\alpha i})\,. \tag{18}$$

Somit ist

$$(a_{\alpha i}) + (b_{\alpha i}) := (a_{\alpha i} + b_{\alpha i}) \tag{19}$$

die zu $a+b$ gehörende Matrix; (19) entspricht aber der komponentenweisen Addition in $K^{m \cdot n}$. Analog zeigt man, daß zur Abbildung $a\lambda$, $a \in \boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{W}^m)$, $\lambda \in K$, die Matrix

$$(a_{\alpha i})\,\lambda := (a_{\alpha i}\lambda) \tag{20}$$

gehört, die der komponentenweisen Multiplikation eines $(m \cdot n)$-Tupels mit einem Skalar $\lambda \in K$ entspricht. □

Folgerung 1. $\mathbf{M}_{m,n}(K)$ *ist mit den Operationen* (19), (20) *ein zu* $K^{m \cdot n}$ *isomorpher Vektorraum über* K; *ein natürlicher Isomorphismus wird durch*

$$(a_{\alpha i}) \in \mathbf{M}_{m,n}(K) \mapsto (\xi_I) \in K^{m \cdot n}, \qquad 1 \leqq I \leqq m \cdot n\,,$$

mit

$$\xi_{sn+i} := a_{s+1,i}, \qquad i=1, \ldots, n, \qquad s=0, 1, \ldots, m-1, \tag{21}$$

gegeben. □

Folgerung 2. *Die nach Satz* 1 *durch*

$$e_{\alpha i}(\mathfrak{a}_j) := \mathfrak{b}_\alpha \delta_{ij} \tag{22}$$

definierten $m \cdot n$ *Elemente* $e_{\alpha i} \in \boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{W}^m)$ *bilden eine Basis von* $\boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{W}^m)$; *sie heißt die zu den Basen* $(\mathfrak{a}_i)$ *von* $\boldsymbol{V}^n$ *und* $(\mathfrak{b}_\alpha)$ *von* $\boldsymbol{W}^m$ *gehörende Basis von* $\boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{W}^m)$. □

Zum Beweis von Folgerung 2 ist nur zu bemerken, daß die Matrizen von $e_{\alpha i}$ in bezug auf $(\mathfrak{a}_i)$, $(\mathfrak{b}_\alpha)$ gerade der kanonischen Basis von $K^{m \cdot n}$ entsprechen; die zu $e_{\alpha i}$ gehörende Matrix enthält nur ein einziges von 0 verschiedenes Element, nämlich die Eins in der α-ten Zeile und i-ten Spalte. Es ergibt sich unmittelbar:

Folgerung 3. *Die Elemente* $a_{\alpha i}$ *der zur Abbildung* $a \in \boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{W}^m)$ *nach Satz* 1 *gehörenden Matrix sind die Koordinaten von* a *bezüglich der in Folgerung* 2 *beschriebenen Basis* $(e_{\alpha i})$ *von* $\boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{W}^m)$. □

Übung 7. Man betrachte den Vektorraum $\boldsymbol{V}^3$ des dreidimensionalen affinen Raumes $\boldsymbol{A}^3$ über $\mathbf{R}$, wähle eine Basis $(\mathfrak{a}_i) = (\mathfrak{b}_\alpha)$ und mache sich die geometrische Bedeutung der linearen Endomorphismen e_{ij}, $i, j = 1, 2, 3$, anhand des zugehörigen Koordinatensystems klar.

Nach der Addition wollen wir nun die durch die Verknüpfung der linearen Abbildungen (vgl. Satz 2.1) gegebene Operation in den Matrizen ausdrücken. Es seien $\boldsymbol{V}^n$, $\boldsymbol{W}^m$, $\boldsymbol{X}^p$ Vektorräume mit den Basen $\{\mathfrak{a}_i\} \subset \boldsymbol{V}^n$, $\{\mathfrak{b}_\alpha\} \subset \boldsymbol{W}^m$ und $\{\mathfrak{c}_\varkappa\} \subset \boldsymbol{X}^p$; die Indizes $\varkappa, \lambda, \mu$ mögen die Werte 1, ..., p annehmen. Ferner sei $a \in \boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{W}^m)$ eine Abbildung mit der Matrix $(a_{\alpha i}) \in \mathbf{M}_{m,n}$, $b \in \boldsymbol{L}(\boldsymbol{W}^m, \boldsymbol{X}^p)$ eine Abbildung mit der Matrix $(b_{\varkappa\alpha}) \in \mathbf{M}_{p,m}$. Wir setzen $c := b \circ a$. Dann gilt $c \in \boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{X}^p)$; wir wollen die nach Satz 1 eindeutig bestimmte Matrix $(c_{\varkappa i}) \in \mathbf{M}_{p,n}$ von c bezüglich der Basen $(\mathfrak{a}_i)$, $(\mathfrak{c}_\varkappa)$ finden. Nach unseren Voraussetzungen gilt neben (2) auch

$$b(\mathfrak{b}_\alpha) = \sum_\varkappa \mathfrak{c}_\varkappa b_{\varkappa\alpha}. \tag{23}$$

Wenden wir b auf (2) an und beachten die Linearität, so folgt aus (23)

$$b \circ a(\mathfrak{a}_i) = \sum_\alpha b(\mathfrak{b}_\alpha)\, a_{\alpha i} = \sum_\varkappa \mathfrak{c}_\varkappa \sum_\alpha b_{\varkappa\alpha} a_{\alpha i} = c(\mathfrak{a}_i) = \sum_\varkappa \mathfrak{c}_\varkappa c_{\varkappa i}. \tag{24}$$

Da die Basisdarstellungen die Vektorkoordinaten eindeutig bestimmen, ergibt sich durch Vergleich der Koeffizienten bei $\mathfrak{c}_\varkappa$:

$$c_{\varkappa i} = \sum_{\alpha=1}^{m} b_{\varkappa\alpha} a_{\alpha i}, \qquad \varkappa = 1, \ldots, p, \qquad i = 1, \ldots, n. \tag{25}$$

Die Gleichung (25) legt nun folgende Definition nahe.

Definition 6. Für $(b_{\varkappa\alpha}) \in \mathbf{M}_{p,m}$ und $(a_{\alpha i}) \in \mathbf{M}_{m,n}$ definieren wir als *Produkt* die

Matrix

$$(c_{\varkappa i}) = (b_{\varkappa\alpha}) \cdot (a_{\alpha i}) \in \mathbf{M}_{p,n}\,, \tag{26}$$

deren Elemente $c_{\varkappa i}$ durch (25) definiert sind.

Damit gilt

Satz 4. *Ist $c = b \circ a \in \boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{X}^p)$, $a \in \boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{W}^m)$, $b \in \boldsymbol{L}(\boldsymbol{W}^m, \boldsymbol{X}^p)$, so ist die Matrix von c bezüglich der Basen $(\mathfrak{a}_i)$, $(\mathfrak{c}_\varkappa)$ von $\boldsymbol{V}^n$ bzw. $\boldsymbol{X}^p$ gleich dem Produkt der Matrizen von b bezüglich $(\mathfrak{b}_\alpha)$, $(\mathfrak{c}_\varkappa)$ und von a bezüglich $(\mathfrak{a}_i)$, $(\mathfrak{b}_\alpha)$. Für die Multiplikation der linearen Abbildungen gelten die distributiven Gesetze*

$$b \circ (a + \hat{a}) = b \circ a + b \circ \hat{a}\,, \tag{27}$$

$$(b + \hat{b}) \circ a = b \circ a + \hat{b} \circ a \tag{28}$$

und die Regel

$$(b\lambda) \circ a = b \circ (a\lambda) = (b \circ a)\,\lambda, \qquad \lambda \in K\,, \tag{29}$$

die bei Übergang zu den zugehörigen Matrizen die entsprechenden Rechenregeln der Matrizenalgebra ergeben:

$$(b_{\varkappa\alpha})\,((a_{\alpha i}) + (\hat{a}_{\alpha i})) = (b_{\varkappa\alpha})\,(a_{\alpha i}) + (b_{\varkappa\alpha})\,(\hat{a}_{\alpha i})\,, \tag{27'}$$

$$((b_{\varkappa\alpha}) + (\hat{b}_{\varkappa\alpha}))\,(a_{\alpha i}) = (b_{\varkappa\alpha})\,(a_{\alpha i}) + (\hat{b}_{\varkappa\alpha})\,(a_{\alpha i})\,, \tag{28'}$$

$$((b_{\varkappa\alpha})\,\lambda)\,(a_{\alpha i}) = (b_{\varkappa\alpha})\,((a_{\alpha i})\,\lambda) = ((b_{\varkappa\alpha})\,(a_{\alpha i}))\,\lambda\,. \tag{29'}$$

Aus der Assoziativität der Verknüpfung von Abbildungen folgt weiter das assoziative Gesetz der Matrizenmultiplikation:

$$((c_{\varrho\varkappa}) \cdot (b_{\varkappa\alpha})) \cdot (a_{\alpha i}) = (c_{\varrho\varkappa}) \cdot ((b_{\varkappa\alpha}) \cdot (a_{\alpha i}))\,. \tag{30}$$

Beweis. Die erste Behauptung erhält man sofort aus Definition 6. Die Beziehungen (27) bis (29) ergeben sich durch unmittelbares Nachrechnen; wir zeigen etwa (27): Für alle $\mathfrak{x} \in \boldsymbol{V}$ gilt

$$\begin{aligned} b \circ (a + \hat{a})\,(\mathfrak{x}) &= b\,((a + \hat{a})\,(\mathfrak{x})) = b\,(a(\mathfrak{x}) + \hat{a}(\mathfrak{x})) \cdot \\ &= b(a(\mathfrak{x})) + b(\hat{a}(\mathfrak{x})) = b \circ a(\mathfrak{x}) + b \circ \hat{a}(\mathfrak{x}) \\ &= (b \circ a + b \circ \hat{a})\,(\mathfrak{x})\,. \end{aligned}$$

Weil die Beziehungen zwischen Matrizen und linearen Abbildungen bijektiv sind und die Operationen wie bei einem Isomorphismus ineinander übergehen, folgen die Rechenregeln für die Matrizen unmittelbar aus den entsprechenden für lineare Abbildungen. □

Übung 8. Man beweise die Rechenregeln (27′) bis (29′) und (30) direkt aus (19), (20) und Definition 6, ohne die Beziehungen zu den linearen Abbildungen anzuwenden.

Die Beziehungen (27) bis (29) kann man auch durch die Redeweise kennzeichnen, daß die Multiplikation der linearen Abbildungen eine *bilineare* Operation ist, d. h., daß

$$b \circ (a\lambda + \hat{a}\mu) = (b \circ a)\,\lambda + (b \circ \hat{a})\,\mu\,, \tag{31}$$

$$(b\lambda + \hat{b}\mu) \circ a = (b \circ a)\,\lambda + (\hat{b} \circ a)\,\mu \tag{32}$$

gelten. Eine entsprechende Bemerkung gilt für die Matrizenmultiplikation.

Bekanntlich wirken die identischen Abbildungen stets als Einselemente der Verknüpfung. Aus

$$\mathrm{id}_W \circ a = a \circ \mathrm{id}_V = a \tag{33}$$

ergibt sich wegen der Isomorphie zur Matrizenmultiplikation nach Beispiel 3:

$$(\delta_{\alpha\beta})\,(a_{\beta j}) = (a_{\alpha i})\,(\delta_{ij})\,, \tag{34}$$

wobei $(\delta_{\alpha\beta}) \in \mathbf{M}_m$ und $(\delta_{ij}) \in \mathbf{M}_n$ die entsprechenden Einheitsmatrizen sind; hierdurch ist ihr Name gerechtfertigt.

Man beachte, daß die Multiplikation und die Addition der Matrizen über im allgemeinen verschiedenen Mengen operieren. *Die Addition ist nur für Matrizen gleichen Typs definiert*

$$+ : \mathbf{M}_{m,n} \times \mathbf{M}_{m,n} \to \mathbf{M}_{m,n}\,, \tag{35}$$

während für die Multiplikation die Anzahl der Spalten des linken Faktors gleich der Anzahl der Zeilen des rechten sein muß:

$$\cdot : \mathbf{M}_{p,m} \times \mathbf{M}_{m,n} \to \mathbf{M}_{p,n}\,; \tag{36}$$

nach (25) wird ja das Element $c_{\varkappa i}$ durch elementweise Multiplikation des $\varkappa$-ten Zeilen-m-Tupels von $(b_{\varkappa\alpha})$ mit dem i-ten Spalten-m-Tupel von $(a_{\alpha i})$ und nachfolgenden Addition der so entstehenden Produkte $b_{\varkappa\alpha}a_{\alpha i}$, $\alpha = 1, \ldots, m$, gebildet. Man spricht daher auch von *Zeilen-Spalten-Multiplikation* der Matrizen. Analog ist ja auch die Verknüpfung der Abbildungen nur definiert, wenn der Bildraum der rechten im Definitionsraum der linken enthalten ist. Beide Operationen (35) und (36) sind jedoch gleichzeitig im Fall $p = m = n$ erklärt, d. h. in der Menge $\mathbf{M}_n$ der quadratischen Matrizen mit n Zeilen. Diesem Fall, der dem Raum $\boldsymbol{L}(\boldsymbol{V}^n)$ der Endomorphismen entspricht, wollen wir uns nun zuwenden.

Die Beziehungen (27), (28) und die Assoziativität der Verknüpfung gestatten uns sofort zu sagen, daß $[\boldsymbol{L}(\boldsymbol{V}), +, \circ]$ ein assoziativer Ring mit Einselement $e = \mathrm{id}_V$ ist. Jedoch wird dabei weder die Vektorraumstruktur noch die Beziehung (29) berücksichtigt. Um auch diese Strukturen mit zu erfassen, formulieren wir den auch für die Anwendungen sehr wichtigen, in vielen Varianten vorkommenden Begriff einer Algebra:

Definition 7. Eine Struktur $[\boldsymbol{A}, +, K, \circ]$ heißt eine *Algebra*, wenn folgende Bedingungen erfüllt sind: 1. $[\boldsymbol{A}, +, K]$ ist ein Vektorraum über dem Körper K.

2. $\circ : \boldsymbol{A} \times \boldsymbol{A} \to \boldsymbol{A}$ ist eine multiplikativ geschriebene, bilineare Operation über $\boldsymbol{A}$, für die also (31) und (32) mit $a, \hat{a}, b, \hat{b} \in \boldsymbol{A}$, $\mu, \lambda \in K$ gelten.

Folgerung 4. *Vergißt man in einer Algebra den Körper K und die Multiplikation mit Elementen $\mu \in K$, so entsteht ein Ring* $[\boldsymbol{A}, +, \circ]$. □

Nach Folgerung 4 sind also die Begriffe und Resultate der Ringtheorie auf die Algebren anwendbar. Wir sprechen in diesem Sinne von kommutativen und assoziativen Algebren, Algebren mit Einselement, der Gruppe $\boldsymbol{A}^*$ der invertierbaren Elemente usw. In diesem Sinne erhält man sofort aus den bisher bewiesenen Sätzen:

Satz 5. *Die Menge $\boldsymbol{L}(\boldsymbol{V})$ der Endomorphismen eines Vektorraumes $\boldsymbol{V}$ bildet mit den in Satz 2 betrachteten Operationen und der Verknüpfung $\circ$ eine assoziative Algebra* $[\boldsymbol{L}(\boldsymbol{V}), +, K, \circ]$ *mit Einselement $e = \mathrm{id}_{\boldsymbol{V}}$.* □

Folgerung 5. *Die Menge $\mathbf{M}_n(K)$ der quadratischen Matrizen mit n Zeilen und Werten in einem Körper K ist eine assoziative Algebra mit Einselement; sie ist isomorph zur Algebra $\boldsymbol{L}(\boldsymbol{V}^n)$, $\boldsymbol{V}^n$ ein n-dimensionaler Vektorraum über K.* □

Definition 8. $[\boldsymbol{L}(\boldsymbol{V}), +, K, \circ]$ heißt die *Endomorphismenalgebra* des Vektorraumes $\boldsymbol{V}$, und $[\mathbf{M}_n(K), +, K, \cdot]$ heißt *Matrizenalgebra* der n-zeiligen quadratischen Matrizen.

Die vielen Anwendungsmöglichkeiten des Algebrenbegriffs mögen durch eine Reihe von Beispielen illustriert werden.

Beispiel 7. Es sei $M \neq \emptyset$ eine Menge und K ein Körper. Dann ist die Menge K^M der Abbildungen von M in K eine assoziative, kommutative Algebra mit Einselement, wenn die Operationen wie üblich punktweise definiert werden. Nach Beispiel 4.2.4 ist nämlich K^M ein Vektorraum, und die Multiplikation wird durch

$$f \cdot g(x) := f(x) \cdot g(x) \qquad (x \in M)$$

erklärt. Ist beispielsweise M ein offenes Intervall $M = (a, b) \subseteq \mathbf{R}$ und setzen wir $K = \mathbf{R}$, so sind auch die Mengen der stetigen oder differenzierbaren Funktionen Algebren, und zwar „Unteralgebren" von $\mathbf{R}^M$.

Beispiel 8. Die Polynomringe in einer oder mehreren Unbestimmten mit Koeffizienten aus einem Körper K sind nullteilerfreie, assoziative und kommutative Algebren mit Einselement (vgl. Beispiel 4.2.5). Das gleiche gilt auch vom Ring der formalen Potenzreihen $K[[x]]$ über einem Körper K (vgl. Übung 4.4.6).

Beispiel 9. Eine Algebra $\boldsymbol{A}$, in der jedes von 0 verschiedene Element ein Inverses besitzt, d. h. $\boldsymbol{A}^* = \boldsymbol{A} \setminus \{o\}$ gilt, heißt eine *Divisionsalgebra*, vgl. § 8.9. Jeder Körper kann als Divisionsalgebra über sich selbst aufgefaßt werden. Die komplexen Zahlen bilden eine zweidimensionale, die Quaternionen eine vierdimensionale Divisionsalgebra über $\mathbf{R}$. Die Bemerkung zum Schluß von § 2.3 besagt, daß Divisionsalgebren über $\mathbf{R}$ nur für die Dimensionen 1, 2, 4 und 8 existieren.

Wir wollen uns nun wieder den Endomorphismenalgebren zuwenden und emp-

fehlen dem Leser, die folgende Übungsaufgabe (durch Übergang zu den isomorphen Matrizenalgebren) zu lösen:

Übung 9. Man beweise: a) Die Algebra $\boldsymbol{L}(\boldsymbol{V}^n)$ ist im allgemeinen weder kommutativ noch nullteilerfrei. — b) Sind $a, b \in \boldsymbol{L}(\boldsymbol{V}^n)$ diagonalisierbar und gilt $a \circ b = b \circ a$, so sind auch $a+b$ und $a \circ b$ diagonalisierbar (vgl. Übung 4).

Als nächstes wollen wir ein Kriterium für die Invertierbarkeit einer linearen Abbildung $a \in \boldsymbol{L}(\boldsymbol{V}^n)$ herleiten und eine Methode zur Berechnung des inversen Elementes angeben. Wir gehen dabei etwas allgemeiner vor, indem wir $a \in \boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{W}^n)$ betrachten; im Fall $n \neq m$ existieren ja keine linearen Isomorphismen (vgl. Folgerung 2.6).

Satz 6. *Es sei* $(a_{ij}) \in \mathbf{M}_n(K)$ *die Matrix der linearen Abbildung* $a \in \boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{W}^n)$ *bezüglich der Basen* $(\mathfrak{a}_j)$, $(\mathfrak{b}_i)$. *Die Abbildung* a *ist ein Isomorphismus genau dann, wenn* $\det(a_{ij}) \neq 0$ *gilt.*

Beweis. Nach Folgerung 2.4 ist a ein Isomorphismus genau dann, wenn die Bilder $(a(\mathfrak{a}_i))$ der Basis $(\mathfrak{a}_i)$ eine Basis von $\boldsymbol{W}^n$ sind. Nach Satz 4.7.4 ist das genau dann der Fall, wenn $\det(a_{ij}) \neq 0$ gilt. □

Eine Formel zur Berechnung einer inversen Matrix ergibt sich sofort aus dem Laplaceschen Entwicklungssatz in der Form (4.8.19). Da (δ_{ij}) das Einselement von $\mathbf{M}_n(K)$ ist, erhalten wir für die unbekannten Koeffizienten ξ_{ij} der Matrix $(\xi_{ij}) = (a_{ij})^{-1}$ aus $(a_{rq})(\xi_{qp}) = (\delta_{rp})$ das Gleichungssystem

$$\sum_{q=1}^{n} a_{rq}\xi_{qp} = \delta_{rp}, \qquad r, p = 1, \ldots, n\,. \tag{37}$$

Bezeichnet nun $(A_{pq}) \in \mathbf{M}_n(K)$ die Matrix der Adjunkten unserer Matrix (a_{ij}), so folgt aus Formel (4.8.19)

$$(a_{rq})(A_{pq})' = (\delta_{rp}) \det(a_{ij});$$

dabei beachte man die Definition 4.8.1 der transponierten Matrix. Der Übergang zur transponierten Matrix ist notwendig, weil in (4.8.19) die Summation sich bei beiden Faktoren über den zweiten, d. h. den Spaltenindex, erstreckt; um Übereinstimmung mit (25) zu erzielen, müssen wir den rechten Faktor transponieren. Ist die Matrix (a_{ij}) invertierbar, so muß nach Satz 6 ihre Determinante ungleich 0 sein (Isomorphie von $\boldsymbol{L}(\boldsymbol{V}^n)$ und $\mathbf{M}_n(K)$), und es ergibt sich (vgl. auch Übung 13d))

Folgerung 6. *Eine Matrix* $(a_{ij}) \in \mathbf{M}_n(K)$ *ist invertierbar genau dann, wenn* $\det(a_{ij}) \neq 0$ *gilt. In diesem Fall berechnet man die inverse Matrix* $(a_{ij})^{-1}$ *nach der Formel*

$$(a_{ij})^{-1} = \left(\frac{A_{ij}}{\det(a_{ij})}\right)', \tag{38}$$

wobei A_{ij} *die durch* (4.8.18) *definierte Adjunkte des Elementes* a_{ij} *ist.* □

Folgerung 7. *Die Menge*

$$\mathbf{GL}(n, K) := \{(a_{ij}) \mid (a_{ij}) \in \mathbf{M}_n(K) \text{ mit } \det(a_{ij}) \neq 0\}$$

ist eine Gruppe bezüglich der Matrizenmultiplikation; ist V^n ein beliebiger n-dimensionaler Vektorraum über K, so gilt

$$\boldsymbol{GL}(V^n) \cong \mathbf{GL}(n, K) . \tag{39}$$

Beweis. Bei Einführung einer Basis ist (8) nach Folgerung 5 ein Isomorphismus der Algebren $\boldsymbol{L}(V^n) \cong \mathbf{M}_n(K)$; hierbei muß

$$\boldsymbol{L}(V^n)^* = \boldsymbol{GL}(V^n) \cong \mathbf{GL}(n, K) = \mathbf{M}_n(K)^*$$

sein. □

Beispiel 10. *Koordinatendarstellung einer linearen Abbildung.* Es sei $a \in \boldsymbol{L}(V^n, W^m)$, $(\mathfrak{a}_i)$ Basis von V^n, $(\mathfrak{b}_\alpha)$ Basis von W^m und $(a_{\alpha i})$ die Matrix von a. Es sei $\mathfrak{x} = \sum_i \mathfrak{a}_i \xi_i \in V^n$ und $\mathfrak{y} = a(\mathfrak{x}) = \sum_\alpha \mathfrak{b}_\alpha \eta_\alpha$. Aus (2) folgt

$$\sum_\alpha \mathfrak{b}_\alpha \eta_\alpha = a(\mathfrak{x}) = a\left(\sum_i \mathfrak{a}_i \xi_i\right) = \sum_i a(\mathfrak{a}_i)\, \xi_i = \sum_\alpha \mathfrak{b}_\alpha \sum_i a_{\alpha i} \xi_i .$$

Koeffizientenvergleich ergibt die *Koordinatendarstellung von a*

$$\eta_\alpha = \sum_i a_{\alpha i} \xi_i, \qquad \alpha = 1, \ldots, m . \tag{40}$$

Betrachten wir nun (η_α) als Spaltenvektor, d. h. $(\eta_\alpha) \in \mathbf{M}_{m,1}$ und analog $(\xi_i) \in \mathbf{M}_{n,1}$, so können wir (40) sofort als Matrizenprodukt schreiben:

$$(\eta_\alpha) = (a_{\alpha i})\,(\xi_i) . \tag{41}$$

Nach Folgerung 3 ist die Matrix $(a_{\alpha i})$ gerade Koordinatenmatrix von a; die Formel (41) geht also aus der (koordinatenfreien) Gleichung $\mathfrak{y} = a(\mathfrak{x})$ durch Übergang zu den entsprechenden Koordinatenmatrizen fast automatisch hervor. Dieser Übergang wird beim praktischen Rechnen mit linearen Abbildungen ständig benutzt. Gilt beispielsweise $m = n$ und definieren wir im Fall einer invertierbaren Matrix $(a_{ij}) \in \mathbf{M}_n$

$$(\overset{-1}{a}_{ij}) := (a_{ij})^{-1} \tag{42}$$

(man beachte: $\overset{-1}{a}_{ij}$ sind die Elemente der inversen Matrix, nicht die Inversen der Elemente der Matrix!), so erhält man im Fall eines Isomorphismus $a: V^n \to W^n$ die Umkehrung $a^{-1}: W^n \to V^n$ in den Koordinaten durch Multiplikation mit $(a_{ij})^{-1}$ von links:

$$(a_{ij})^{-1}\,(\eta_k) = (\xi_i) , \tag{43}$$

d. h.

$$\xi_i = \sum_j \overset{-1}{a}_{ij} \eta_j . \tag{44}$$

Beispiel 11. Man beachte, daß die Matrizenoperationen unabhängig von den linearen Abbildungen definierte Rechenvorschriften darstellen. Diese Definitionen lassen sich auch auf viel allgemeinere Bereiche als nur auf Körper anwenden; für die Elemente der Matrix müssen nur die in den Definitionen auftretenden Operationen definiert sein (vgl. Übung 10). Das ist z. B. auch der Fall, wenn die linke Matrix eines Produktes aus Vektoren und die rechte aus Skalaren besteht; beispielsweise können wir die Spaltenmatrizen aus Vektoren $(\mathfrak{a}_i)$, $(a(\mathfrak{a}_i))$, $(\mathfrak{b}_\alpha)$ bilden. Dann wird (2) zu

$$(a\mathfrak{a}_i)' = (\mathfrak{b}_\alpha)'\,(a_{\alpha i})\,. \tag{45}$$

Übung 10. Es sei D ein beliebiger Ring und $\mathbf{M}_n(D)$ die Menge der n-zeiligen quadratischen Matrizen aus D. Dann bleiben die Definitionen (19), (20) und (25), also auch Definition 6, sinnvoll. Man beweise: a) $\mathbf{M}_n(D)$ ist wiederum ein Ring. — b) Besitzt D ein Einselement, so gilt das auch für $\mathbf{M}_n(D)$. — c) Ist D assoziativ, so ist auch $\mathbf{M}_n(D)$ assoziativ. (Aus Übung 9 ist klar, daß $\mathbf{M}_n(D)$ weder kommutativ noch nullteilerfrei sein muß, auch wenn D diese Eigenschaften besitzt.)

Übung 11. Es sei K ein Körper. Wir betrachten die Abbildung

$$f\colon \lambda \in K \mapsto \begin{pmatrix} \lambda & 0 \\ 0 & 0 \end{pmatrix} \in \mathbf{M}_2(K)\,.$$

Man beweise: a) f ist ein Ringhomomorphismus, Im f ist ein Unterring von $\mathbf{M}_2(K)$, aber es gilt $e = (\delta_{ij}) \notin \operatorname{Im} f$, und kein Element $a \in \operatorname{Im} f$ besitzt in $\mathbf{M}_2(K)$ ein Inverses. — b) Das Element $\hat{e} = f(1) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ ist Einselement in Im f, und bezüglich dieses Einselementes ist Im f ein Körper, vgl. Satz 2.2.2. — c) Man beweise: Für einen beliebigen Ring D existiert in $\mathbf{M}_n(D)$ ein zu D isomorpher Unterring $\hat{D}$; wenn D ein Einselement $1 \in D$ besitzt, kann man den Isomorphismus $f\colon D \to \mathbf{M}_n(D)$ so wählen, daß $f(D^*) \subseteq \mathbf{M}_n(D)^*$ gilt.

Um diesen langen Paragraphen endlich abschließen zu können, müssen wir noch den Produktsatz der Matrizenrechnung beweisen. Hierzu gehen wir von einer einfachen geometrischen Fragestellung aus: Es sei $\boldsymbol{V}^n$ ein n-dimensionaler Vektorraum über K, in dem eine Volumenfunktion gegeben sei; nach § 4.7 gibt es also ein n-Bein $(\mathfrak{a}_i)$ von $\boldsymbol{V}^n$ mit dem Volumen $[\mathfrak{a}_1, \ldots, \mathfrak{a}_n] = 1$, so daß für beliebige Vektoren $\mathfrak{b}_i$ mit den Basisdarstellungen

$$\mathfrak{b}_j = \sum_i \mathfrak{a}_i \beta_{ij}, \qquad j = 1, \ldots, n\,, \tag{46}$$

die Beziehung

$$[\mathfrak{b}_1, \ldots, \mathfrak{b}_n] = \det(\beta_{ij}) \tag{47}$$

gilt. Wir betrachten nun den linearen Endomorphismus $a \in \boldsymbol{L}(\boldsymbol{V}^n)$ und fragen nach dem Volumen des Bildparallelepipeds $[a(\mathfrak{b}_1), \ldots, a(\mathfrak{b}_n)]$. Für die Koordinatendarstellung von $a(\mathfrak{b}_i)$ erhalten wir nach (2)

$$a(\mathfrak{b}_j) = \sum_i a(\mathfrak{a}_i)\,\beta_{ij} = \sum_l \mathfrak{a}_l \sum_i a_{li}\beta_{ij}\,.$$

Offenbar ist die Koordinatenmatrix der Bildvektoren die Produktmatrix

$$(c_{lj}) := (a_{li})\,(\beta_{ij})\,, \tag{48}$$

und aus (47) folgt

$$[a(\mathfrak{b}_1), \ldots, a(\mathfrak{b}_n)] = \det((a_{li})(\beta_{ij})) . \tag{49}$$

Andererseits erhalten wir aus den Eigenschaften der Volumenfunktion und (46)

$$\begin{aligned}[a(\mathfrak{b}_1), \ldots, a(\mathfrak{b}_n)] &= \sum_{i_1,\ldots,i_n} [a(\mathfrak{a}_{i_1}), \ldots, a(\mathfrak{a}_{i_n})]\, \beta_{i_n 1} \cdots \beta_{i_1 n} \\ &= [a(\mathfrak{a}_1), \ldots, a(\mathfrak{a}_n)] \sum_{P \in S_n} \operatorname{sgn}(P)\, \beta_{i_1 1} \cdots \beta_{i_n n}; \end{aligned} \tag{50}$$

hier haben wir (4.7.10) angewandt. Nach der Definition der Matrix (a_{ij}) als Koordinatenmatrix der Bildvektoren folgt wegen $[\mathfrak{a}_1, \ldots, \mathfrak{a}_n] = 1$

$$[a(\mathfrak{a}_1), \ldots, a(\mathfrak{a}_n)] = \det(a_{ij}) , \tag{51}$$

und die Summe auf der rechten Seite von (50) ist $\det(\beta_{ij})$. Der Vergleich von (49) und (50) gibt also

Satz 7 (Produktsatz). *Für* $(a_{ij}), (\beta_{ij}) \in \mathbf{M}_n(K)$ *gilt*

$$\det((a_{ij})(\beta_{jl})) = \det(a_{ij}) \det(\beta_{jl}) . \ \square \tag{52}$$

Weiter ergibt sich aus (47) und (50)

Satz 8. *Ist* $a \in \boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{W}^n)$ *und sind über* $\boldsymbol{V}^n$, $\boldsymbol{W}^n$ *Volumenfunktionen gegeben, so gilt für alle Parallelepipede* $(\mathfrak{b}_i)$ *aus* $\boldsymbol{V}^n$ *und n-Beine* $(\mathfrak{a}_i)$ *von* $\boldsymbol{V}^n$

$$[a(\mathfrak{b}_1), \ldots, a(\mathfrak{b}_n)] = [a(\mathfrak{a}_1), \ldots, a(\mathfrak{a}_n)] \frac{[\mathfrak{b}_1, \ldots, \mathfrak{b}_n]}{[\mathfrak{a}_1, \ldots, \mathfrak{a}_n]}; \tag{53}$$

ist speziell a ein linearer Isomorphismus, so bleiben die Volumenverhältnisse von Parallelepipeden invariant.

Beweis. Im Fall $[\mathfrak{a}_1, \ldots, \mathfrak{a}_n] = 1$ sind (53) und (50) identisch. Falls $[\mathfrak{a}_1, \ldots, \mathfrak{a}_n] \neq 1$ ist, gilt statt (47) $\det(\beta_{ij}) = [\mathfrak{b}_1, \ldots, \mathfrak{b}_n]/[\mathfrak{a}_1, \ldots, \mathfrak{a}_n]$, und hieraus folgt die Behauptung. $\square$

Wir bemerken, daß die zu Satz 8 analoge Behauptung auch für affine Abbildungen gilt; man braucht nur zu den zugehörigen linearen Abbildungen überzugehen (man beachte die Bemerkungen zu Beginn von § 4.7). Damit resultiert aus Satz 8 folgende wichtige Verallgemeinerung des Satzes über die Invarianz der Streckenverhältnisse:

Satz 9. *Es seien* $\boldsymbol{A}^n$, $\boldsymbol{B}^m$ *affine Räume,* $f: \boldsymbol{A}^n \to \boldsymbol{B}^m$ *eine affine Abbildung und* Π^k, Π_1^k *zwei k-dimensionale Parallelepipede von* $\boldsymbol{A}^n$, *die nicht ausgeartet sind und in parallelen k-Ebenen liegen:*

$$\boldsymbol{H}(\Pi_1^k) \parallel \boldsymbol{H}(\Pi^k) . \tag{54}$$

Dann sind $f(\Pi^k)$ *und* $f(\Pi_1^k)$ *entweder beide ausgeartet, oder sie sind beide nicht ausgeartet, und es gilt für ihr Volumenverhältnis*

$$v(f(\Pi^k))/v(f(\Pi_1^k)) = v(\Pi^k)/v(\Pi_1^k) . \tag{55}$$

Beweis. Wir betrachten den gemeinsamen Vektorraum $\boldsymbol{W}^k \subseteq \boldsymbol{V}^n$ von $\boldsymbol{H}(\Pi^k) \parallel \boldsymbol{H}(\Pi_1^k)$. Es sei a_f die zu f gehörende lineare Abbildung. Ist $a_f \mid \boldsymbol{W}^k$ nicht injektiv, so gilt $\operatorname{rg}(a_f \mid \boldsymbol{W}^k) = \dim a_f(\boldsymbol{W}^k) < k$, und beide Bildparallelepipede sind ausgeartet. Gilt andererseits $\operatorname{rg}(a_f \mid \boldsymbol{W}^k) = k$, so folgt die Behauptung sofort aus Satz 8 bei Anwendung auf die Π^k und Π_1^k definierenden Vektorfolgen. □

Bemerkung. Wegen Folgerung 4.7.2 kommt es bei der Betrachtung der Volumenverhältnisse nicht auf die Wahl der Volumenfunktion über $\boldsymbol{W}^k$ an.

Übung 12. Man beweise für die Transponierte (vgl. Definition 4.8.1) des Produkts zweier Matrizen:

$$((b_{\varkappa\alpha})\,(a_{\alpha i}))' = (a_{\alpha i})'\,(b_{\varkappa\alpha})'. \tag{56}$$

Übung 13. Es seien K ein Körper, $\boldsymbol{V}$ ein Vektorraum über K, $(a_{\alpha i}) \in \mathbf{M}_{m,n}(K)$, $(\mathfrak{b}_{\varkappa j}) \in \mathbf{M}_{p,n}(\boldsymbol{V})$ eine Matrix mit Vektoren als Elementen, und $(x_{\varkappa\alpha})$ eine Matrix vom Typ p, m mit Unbestimmten $x_{\varkappa\alpha}$ als Elementen. Aus (25), (26) ist ersichtlich, daß die Produkte $(x_{\varkappa\alpha})\,(a_{\alpha j})$, $(\mathfrak{c}_{\varkappa\alpha})\,(a_{\alpha j})$ für $(\mathfrak{c}_{\varkappa\alpha}) \in \mathbf{M}_{p,m}(\boldsymbol{V})$ analog zu Definition 6 sinnvoll definiert sind. a) Man beweise: Ist $m = n$ und $\det(a_{ij}) \neq 0$, so existiert genau eine Lösung $(x_{\varkappa i}) = (\mathfrak{c}_{\varkappa i}) \in \mathbf{M}_{p,n}(\boldsymbol{V})$ der Gleichung $(x_{\varkappa i})\,(a_{ij}) = (\mathfrak{b}_{\varkappa j})$. — b) Bildet man die zusammengesetzte Matrix

$$\begin{pmatrix} a_{ij} \\ \mathfrak{b}_{\varkappa j} \end{pmatrix}$$

mit $n+p$ Zeilen und n Spalten, die durch Untereinanderschreiben von (a_{ij}) und $(\mathfrak{b}_{\varkappa j})$ entsteht, so kann man unter den Voraussetzungen von a) die Lösung gewinnen, indem man die zusammengesetzte Matrix durch Anwendung der elementaren Umformungen (I) bis (III) auf die Spalten so abändert, daß die ersten n Zeilen zur Einheitsmatrix $(\delta_{ij}) \in \mathbf{M}_n(K)$ werden; die letzten p Zeilen der umgeformten Matrix enthalten dann die Lösung. — c) Im Fall $\boldsymbol{V} = K$ gelten zu a), b) analoge Aussagen für die Matrizengleichung $(a_{ij})\,(x_{j\varkappa}) = (b_{i\varkappa})$, $(b_{i\varkappa}) \in \mathbf{M}_{n,p}(K)$; man präzisiere dies und wende es zur Auflösung eines linearen Gleichungssystems der Form (4.8.21) mit von 0 verschiedener Determinante an. — d) Mittels b) oder c) erhält man im Fall $p = n$ und $(b_{i\alpha}) = (\delta_{i\alpha})$ ein Verfahren zur Bestimmung der Inversen einer Matrix, welches rechnerisch einfacher ist als die Anwendung von (38).

Übung 14. Durch eine direkte Rechnung beweise man, daß der Produktsatz (Satz 7) auch für Matrizen (a_{ij}), $(\beta_{ij}) \in \mathbf{M}_n(D)$ mit Elementen aus einem assoziativen, kommutativen Ring D gilt. (Hinweis. Man wende Übung 4.7.4a) an). — Man zeige: Ist D ein assoziativer, kommutativer Ring mit Einselement, so gilt $(a_{ij}) \in \mathbf{M}_n(D)^*$ dann und nur dann, wenn $\det(a_{ij}) \in D^*$ ist, und dann gilt (38), vgl. Übung 10.

Übung 15. Man betrachte den Körper $K = \mathbf{Z}_2$ und beweise: a) Die affine Gruppe $\mathfrak{A}(\boldsymbol{A}^1)$ (für $K = \mathbf{Z}_2$) ist abelsch. — b) Man stelle die Gruppentafel für $\boldsymbol{GL}(2, \mathbf{Z}_2)$ auf und zeige, daß $\mathfrak{A}(\boldsymbol{A}^2)$ nicht abelsch ist (vgl. Übung 3.5).

Übung 16. Es seien $\boldsymbol{V}^n = \overset{r}{\underset{\varrho=1}{\oplus}} \boldsymbol{V}_\varrho^{n_\varrho}$, $\boldsymbol{W}^m = \overset{s}{\underset{\sigma=1}{\oplus}} \boldsymbol{W}_\sigma^{m_\sigma}$ Darstellungen von $\boldsymbol{V}^n$ und $\boldsymbol{W}^m$ als direkte Summe von Unterräumen, $p_\varrho\colon \boldsymbol{V}^n \to \boldsymbol{V}_\varrho$ (bzw. $p_\sigma\colon \boldsymbol{W}^m \to \boldsymbol{W}_\sigma$) und $\iota_\varrho\colon \boldsymbol{V}_\varrho \to \boldsymbol{V}^n$ (bzw. $\iota_\sigma\colon \boldsymbol{W}_\sigma \to \boldsymbol{W}^m$) die zugehörigen Projektionen und Injektionen (Übung 2.9). Man zeige: a) Jede lineare Abbildung $a \in \boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{W}^m)$ läßt sich eindeutig in der Gestalt

$$a = \sum_{\sigma,\varrho} \iota_\sigma \circ A_{\sigma\varrho} \circ p_\varrho \quad \text{mit} \quad A_{\sigma\varrho} \in \boldsymbol{L}(\boldsymbol{V}_\varrho, \boldsymbol{W}_\sigma)$$

darstellen. (Hinweis. Man beachte die leicht zu beweisende Beziehung $p_\varrho \circ \iota_\mu = \delta_{\varrho\mu}\,\mathrm{id}_{\boldsymbol{V}_\varrho}$.) — b) Eine Basis $(\mathfrak{a}_i)$ von $\boldsymbol{V}^n$ heißt der direkten Summenzerlegung von $\boldsymbol{V}^n$ *angepaßt*,

wenn sie Vereinigung von Basen der Summanden V_ϱ ist. Es seien in V^n, W^m und in $U^k = \overset{t}{\underset{\tau=1}{\oplus}} U_\tau^{k_\tau}$ den direkten Summenzerlegungen angepaßte Basen gegeben. Wir können dann die Matrix $(a_{\alpha i})$ von $a \in L(V^n, W^m)$ (und analog $(b_{\varkappa\beta})$ von $b \in L(W^m, U^k)$) in Gestalt einer *Blockmatrix* schreiben:

$$(a_{\alpha i}) = \begin{array}{c} \begin{matrix} n_1 & n_2 & & n_r \end{matrix} \\ \left(\begin{array}{c|c|c|c} A_{11} & A_{12} & \dots & A_{1r} \\ \hline A_{21} & A_{22} & \dots & A_{2r} \\ \hline \vdots & \vdots & & \vdots \\ \hline A_{s1} & A_{s2} & \dots & A_{sr} \end{array}\right) \end{array} \begin{matrix} m_1 \\ m_2 \\ \\ m_s \end{matrix};$$

dabei denken wir uns die Basen fest gegeben und identifizieren zur Vereinfachung der Schreibweise die linearen Abbildungen $A_{\sigma\varrho}$ und die ihnen entsprechenden Matrizen $A_{\sigma\varrho} \in \mathbf{M}_{m_\sigma, n_\varrho}$. Man zeige, daß für die Blockmatrix $(C_{\tau\varrho})$ von $c = b \circ a \in L(V^n, U^k)$ die Formel

$$C_{\tau\varrho} = \sum_{\sigma=1}^{s} B_{\tau\sigma} \circ A_{\sigma\varrho}$$

gilt, $(B_{\tau\sigma})$ die Blockmatrix von b; diese Formel verallgemeinert (25). Man verallgemeinere analog (19) und (20) zu Operationen für Blockmatrizen und mache sich klar, daß für das Rechnen mit Blockmatrizen die zu (27′) bis (29′) sowie (30) analogen Formeln gelten. — c) Wir betrachten $L(V^n)$. Man beweise: Die Menge $P := \{a \mid a \in L(V^n), a(V_\varrho) \subseteq \subseteq V_\varrho, \varrho = 1, \dots, r\}$ der Endomorphismen, welche die gegebene direkte Summendarstellung von V^n invariant lassen, ist eine *Unteralgebra* (d. h. Unterraum und Unterring) der Endomorphismenalgebra $L(V^n)$; die Gruppe P^* der invertierbaren Elemente von P ist isomorph zu dem direkten Produkt linearer Gruppen $P^* \cong \overset{r}{\underset{\varrho=1}{\prod}} GL(n_\varrho, K)$. Ein Endomorphismus $a \in L(V^n)$ gehört zu P dann und nur dann, wenn die zu einer angepaßten Basis gehörende Blockmatrix von a *quasidiagonal* ist, d. h. $A_{\varrho\sigma} = 0$ ist für $\varrho \neq \sigma$ (0 ist die Nullmatrix).

Übung 17. Eine Blockmatrix $(A_{\varrho\sigma})$ heißt *quadratisch zerlegt*, wenn $r = s$ und $m_\varrho = n_\varrho$, $\varrho = 1, \dots, r$, gelten. Eine quadratisch zerlegte Blockmatrix heißt *obere* (bzw. *untere*) *quasi-Dreiecksmatrix*, wenn $A_{\varrho\sigma} = 0$ für $\varrho > \sigma$ (bzw. für $\varrho < \sigma$) gilt. Man beweise: a) Für eine quasi-Dreiecksmatrix $(A_{\varrho\sigma})$ ist $\det(A_{\varrho\sigma}) = \overset{r}{\underset{\varrho=1}{\prod}} \det A_{\varrho\varrho}$. — b) Die oberen (bzw. unteren) quasi-Dreiecksmatrizen eines festen quadratischen Zerlegungstyps $(n_1, \dots, n_r)$ bilden eine Unteralgebra von $\mathbf{M}_n(K)$. Welche Eigenschaft charakterisiert eine isomorphe Unteralgebra der Endomorphismenalgebra $L(V^n)$?

Übung 18. Man beweise: Die Reellifizierung der Matrizenalgebra $\mathbf{M}_n(\mathbf{C})$ (vgl. Übung 4.2.7) ist isomorph zur Unteralgebra $\mathfrak{C}_{2n} \subset \mathbf{M}_{2n}(\mathbf{R})$ der Blockmatrizen der Gestalt

$$\begin{pmatrix} A & -B \\ B & A \end{pmatrix} \quad \text{mit} \quad A, B \in \mathbf{M}_n(\mathbf{R}).$$

(Hinweis. Für $(z_{jk}) \in \mathbf{M}_n(\mathbf{C})$ setze man $(z_{jk}) = A + Bi$ mit $A = (R(z_{jk}))$, $B = (I(z_{jk}))$, vgl. Definition 2.3.1.) Analog ist $GL(n, \mathbf{C})$ zur Untergruppe der invertierbaren Blockmatrizen $\mathfrak{C}_{2n}^* \subset GL(2n, \mathbf{R})$ isomorph.

Übung 19. Es seien $a \in L(V^n)$ und $W^k \subset V^n$ ein bei a invarianter Unterraum. Dann gilt $b := a \mid W^k \in L(W^k)$. Man zeige, daß durch $c(\mathfrak{x} + W) = a(\mathfrak{x}) + W$ ein Operator die Formel

$c \in \boldsymbol{L}(\boldsymbol{V}/\boldsymbol{W})$ korrekt definiert wird. Ist $(\mathfrak{a}_i)$, $i=1, \ldots, n$, eine Basis von $\boldsymbol{V}^n$ derart, daß $\mathfrak{a}_\alpha \in \boldsymbol{W}^k$ für $\alpha=1, \ldots, k$ gilt, so können wir die Matrix von a bezüglich dieser Basis als quadratische Blockmatrix $(a_{ij})=(A_{\varrho\sigma})$, $\varrho, \sigma=1, 2$, $n_1=m_1=k$, $n_2=m_2=n-k$ schreiben; man zeige, daß dabei A_{11} die Matrix von b bezüglich $(\mathfrak{a}_\alpha)$, $\alpha=1, \ldots, k$, ist; A_{22} ist die Matrix von c bezüglich der Basis $(\mathfrak{a}_\varkappa + \boldsymbol{W})$, $\varkappa=k+1, \ldots, n$, von $\boldsymbol{V}/\boldsymbol{W}$, und es gilt $A_{21}=0$.

§ 5. Rangbestimmung. Lineare Gleichungssysteme

In Definition 2.3 haben wir bereits den Rang einer linearen Abbildung $\operatorname{rg} a := \dim \operatorname{Im} a$ eingeführt. Etwas allgemeiner definieren wir:

Definition 1. Es sei $\boldsymbol{V}$ ein Vektorraum über K und $M \subseteq \boldsymbol{V}$ eine Teilmenge. Unter dem *Rang von* M versteht man

$$\operatorname{rg}(M) := \dim \mathfrak{L}(M) . \tag{1}$$

Beispiel 1. Für eine lineare Abbildung $a \in \boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{W}^m)$ gilt nach Definition 2.3

$$\operatorname{rg} a := \operatorname{rg}(a(\boldsymbol{V}^n)) = \dim \operatorname{Im} a . \tag{2}$$

Beispiel 2. Wir betrachten eine Matrix $(a_{\alpha i}) \in \mathbf{M}_{m,n}(K)$ und ordnen ihr die Menge $\{(a_{\alpha 1}), \ldots, (a_{\alpha n})\} \subseteq K^m$ ihrer Spaltenvektoren zu. Unter dem *Rang von* $(a_{\alpha i})$ versteht man

$$\operatorname{rg}(a_{\alpha i}) := \operatorname{rg}\{(a_{\alpha 1}), \ldots, (a_{\alpha n})\} . \tag{3}$$

Man könnte analog statt der Menge der Spaltenvektoren auch die Zeilenvektoren betrachten. Wir werden weiter unten zeigen (vgl. Satz 3), daß wir dabei denselben Rang bekommen, so daß eine Unterscheidung der Begriffe nicht nötig ist.

Übung 1. a) Man zeige, daß alle oben betrachteten Rangbegriffe sich dem folgenden unterordnen lassen: Es sei X eine Menge, $f: X \to \boldsymbol{V}$ eine Abbildung. Unter dem *Rang von* f versteht man $\operatorname{rg} f := \dim \mathfrak{L}(f(X))$. — b) Man beweise: Ist $M \subseteq \boldsymbol{V}$ eine endliche Menge oder ist $\dim \boldsymbol{V} < \infty$, so gilt $\operatorname{rg}(M) = r$ dann und nur dann, wenn r die Anzahl der Vektoren einer maximalen linear unabhängigen Teilmenge $B \subseteq M$ ist.

Aus der Definition (3) und Übung 1 b) erhalten wir sofort eine Aussage über den Rang einer Matrix, die oft zur Definition des Ranges benutzt wird:

Folgerung 1. *Der Rang einer Matrix ist gleich r genau dann, wenn es eine linear unabhängige Folge aus r Spaltenvektoren der Matrix gibt und jede Folge aus $r+1$ ihrer Spaltenvektoren linear abhängig ist.* □

Beispiel 3. Der Rang einer Stufenmatrix der Form (2.9.4) ist gleich r. Zum Beweis betrachten wir die Spalten dieser Matrix als m-Tupelvektoren $\mathfrak{c}_i := (c_{\alpha i}) \in K^m$, $i=1, \ldots, n$. Da die letzten $m-r$ Komponenten alle 0 sind, folgt $\{\mathfrak{c}_1, \ldots, \mathfrak{c}_n\} \subseteq \mathfrak{L}(\{\mathfrak{e}_1, \ldots, \mathfrak{e}_r\})$, wobei $\mathfrak{e}_\varrho$, $\varrho=1, \ldots, r$, die ersten r Vektoren der Standardbasis des K^m sind, vgl. Folgerung 4.4.4. Also gilt $\operatorname{rg}(c_{\alpha i}) \leqq r$. Andererseits sind die Vektoren

$\mathfrak{c}_{k_1}, \ldots, \mathfrak{c}_{k_r}$ linear unabhängig; ihre Determinante bezüglich der Basis $(\mathfrak{e}_\varrho)$, $\varrho = 1, \ldots, r$, von $\mathfrak{L}(\mathfrak{e}_1, \ldots, \mathfrak{e}_r)$ ist nämlich $c_{1k_1} \cdot c_{2k_2} \ldots c_{rk_r} \neq 0$, vgl. Satz 4.7.4 und Satz 4.8.1. Weil aus $P \subseteq M$ nach (4.2.14) $\mathfrak{L}(P) \subseteq \mathfrak{L}(M)$ und damit auch $\operatorname{rg}(P) \leqq \operatorname{rg}(M)$ folgt, ergibt sich $r = \operatorname{rg}\{\mathfrak{c}_{k_1}, \ldots, \mathfrak{c}_{k_r}\} \leqq \operatorname{rg}(c_{\alpha i}) = r$.

Wir wollen nun folgende nicht allzu schwierige, aber sehr wichtige Aufgabe behandeln: Wie bestimmt man den Rang einer linearen Abbildung $a \in \boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{W}^m)$? Ein Spezialfall wird bereits durch Satz 4.6 beantwortet: Der Rang von $a \in \boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{W}^n)$ ist gleich n genau dann, wenn $\det(a_{ij}) \neq 0$ für die Matrix (a_{ij}) von a gilt. Als ersten Schritt wollen wir auch die allgemeine Aufgabe auf die Matrix von a zurückführen.

Satz 1. *Es sei* $a \in \boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{W}^m)$, $(\mathfrak{a}_i)$ *eine Basis von* $\boldsymbol{V}^n$, $(\mathfrak{b}_\alpha)$ *eine Basis von* $\boldsymbol{W}^m$ *und* $(a_{\alpha i})$ *die Matrix von* a *bezüglich dieser Basen. Dann gilt*

$$\operatorname{rg} a = \operatorname{rg}(a_{\alpha i}) . \tag{4}$$

Beweis. Nach (2) ist $\operatorname{rg} a$ gleich $\dim \operatorname{Im} a$. Nun wird $\operatorname{Im} a$ von den Vektoren $a(\mathfrak{a}_i)$, $i = 1, \ldots, n$, erzeugt (vgl. (2.9)). Der Übergang zur Basisdarstellung von $a(\mathfrak{a}_i)$ bezüglich $(\mathfrak{b}_\alpha)$ ergibt die Spaltenvektoren der Matrix $(a_{\alpha i})$ nach (4.2). Bekanntlich ist der Übergang von den Vektoren zu den Vektorkoordinaten $\boldsymbol{W}^m \to K^m$ ein linearer Isomorphismus (vgl. Beispiel 2.2). Dabei geht $\operatorname{Im} a$ als lineare Hülle der Folge $(a(\mathfrak{a}_1), \ldots, a(\mathfrak{a}_n))$ in die lineare Hülle der Folge der Spaltenvektoren über, deren Dimensionen somit übereinstimmen. □

Satz 1 führt unsere Aufgabe auf die Bestimmung des Ranges einer Matrix zurück. Das gelingt analog zum Gaußschen Algorithmus:

Satz 2 A. *Es sei* $(a_{\alpha i}) \in \mathbf{M}_{m,n}(K)$. *Wendet man die elementaren Umformungen* (I), (II), (III) *nach Definition* 2.9.3 *auf die Zeilenvektoren der Matrix* $(a_{\alpha i})$ *an, so ändert sich der Rang der Matrix nicht.*

Beweis. Wir betrachten den K^m als Vektorraum, der die Spaltenvektoren enthält, und zeigen, daß die elementaren Umformungen auf Isomorphismen des K^m hinauslaufen. Da sich bei Isomorphismen die Dimensionen von Unterräumen nicht ändern, folgt hieraus die Behauptung. Wir betrachten zuerst die Operation (I). Dabei erfährt jeder Spaltenvektor die Transformation

$$\mathfrak{y} = \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_\alpha \\ \vdots \\ \eta_\beta \\ \vdots \\ \eta_m \end{pmatrix} \mapsto \hat{\mathfrak{y}} = \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_\beta \\ \vdots \\ \eta_\alpha \\ \vdots \\ \eta_m \end{pmatrix} ;$$

das entspricht dem durch

$$\varphi(\mathfrak{e}_\gamma) = \begin{cases} \mathfrak{e}_\alpha & \text{für } \gamma = \beta , \\ \mathfrak{e}_\beta & \text{für } \gamma = \alpha , \\ \mathfrak{e}_\gamma & \text{für } \gamma \neq \alpha, \beta \end{cases} \tag{5}$$

gegebenen Isomorphismus von K^m. Die Operation (II) läuft analog auf den folgenden Isomorphismus hinaus:

$$\psi(\mathfrak{e}_\gamma)=\begin{cases}\mathfrak{e}_\alpha+\mathfrak{e}_\beta c & \text{für } \gamma=\alpha\,,\\ \mathfrak{e}_\gamma & \text{für } \gamma\neq\alpha;\end{cases} \tag{6}$$

dabei ist $c\in K$ und β eine feste Zahl, $\beta\neq\alpha$. In der Tat, betrachten wir einen beliebigen Spaltenvektor (η_γ), so erfährt er durch φ gerade eine Transformation vom Typ (II):

$$\begin{aligned}\psi\Big(\sum_\gamma \mathfrak{e}_\gamma\eta_\gamma\Big)&=\sum_\gamma \psi(\mathfrak{e}_\gamma)\,\eta_\gamma=\sum_{\gamma\neq\alpha}\mathfrak{e}_\gamma\eta_\gamma+(\mathfrak{e}_\alpha+\mathfrak{e}_\beta c)\,\eta_\alpha\\ &=\sum_{\gamma\neq\beta}\mathfrak{e}_\gamma\eta_\gamma+\mathfrak{e}_\beta\,(\eta_\beta+c\eta_\alpha)\,.\end{aligned} \tag{7}$$

Die Abbildung (6) führt also auf die Multiplikation der α-ten Zeile mit c und ihre Addition zur β-ten Zeile. Offenbar ist auch ψ ein Isomorphismus; denn die Determinante der durch (6) bestimmten Matrix von ψ ist 1. Analog wird die Operation (III) durch den Isomorphismus (mit $c\in K^*$)

$$\theta(\mathfrak{e}_\gamma)=\begin{cases}\mathfrak{e}_\alpha c & \text{für } \gamma=\alpha\,,\\ \mathfrak{e}_\gamma & \text{für } \gamma\neq\alpha\end{cases} \tag{8}$$

bewirkt. □

Um den Rang einer Matrix zu bestimmen, führt man sie durch Anwendung der elementaren Umformungen (I), (II) in Stufenform über; (III) wurde nur zur Normierung $c_{\varrho k_\varrho}=1$, $\varrho=1,\ldots,r$, bei der Herstellung einer speziellen Stufenmatrix benötigt. Aus dieser Form (2.9.4) liest man dann nach Beispiel 3 den Rang unmittelbar ab. Häufig ist es günstig, die elementaren Umformungen nicht nur auf die Zeilen, sondern auch auf die Spalten der Matrix anzuwenden. Diese Methode wird durch den folgenden Satz gerechtfertigt:

Satz 2 B. *Wendet man die elementaren Umformungen* (I), (II), (III) *auf die Spalten einer Matrix* $(a_{\alpha i})\in\mathbf{M}_{m,n}(K)$ *an, so ändert sich ihr Rang nicht.*

Beweis. Der Beweis läuft auf sehr einfache geometrische Überlegungen über die lineare Hülle $\boldsymbol{U}$ der endlichen Vektorfolge $(\mathfrak{c}_1,\ldots,\mathfrak{c}_n)$ der Spaltenvektoren hinaus. Offenbar ändert sich diese lineare Hülle nicht, wenn man die Reihenfolge zweier Vektoren vertauscht (Operation (I)) oder einen Vektor mit einem Skalar $c\neq 0$ multipliziert (Operation (III)). Die Operation (II) bedeutet Ersetzung z. B. von $\mathfrak{c}_1$ durch $\hat{\mathfrak{c}}_1=\mathfrak{c}_1+\mathfrak{c}_2 c$, $c\in K$. Offenbar ist $\hat{\mathfrak{c}}_1\in\boldsymbol{U}$, also $\hat{\boldsymbol{U}}:=\mathfrak{L}(\hat{\mathfrak{c}}_1,\mathfrak{c}_2,\ldots,\mathfrak{c}_n)\subseteq\boldsymbol{U}$. Andererseits ist $\mathfrak{c}_1=\hat{\mathfrak{c}}_1-\mathfrak{c}_2 c\in\hat{\boldsymbol{U}}$, also analog $\boldsymbol{U}\subseteq\hat{\boldsymbol{U}}$, und somit $\boldsymbol{U}=\hat{\boldsymbol{U}}$. Da sich sogar die lineare Hülle nicht ändert, gilt das erst recht für ihre Dimension. □

Nun ist es leicht, den schon in Beispiel 2 angekündigten Sachverhalt zu beweisen, daß man den Rang einer Matrix analog auch über die Zeilen definieren kann. Da bei Übergang zur transponierten Matrix die Zeilen in die Spalten übergehen und umgekehrt die Spalten in die Zeilen, folgt unsere Behauptung unmittelbar aus

Satz 3. *Für jede Matrix* $(a_{\alpha i}) \in \mathbf{M}_{m,n}(K)$ *gilt*

$$\operatorname{rg}(a_{\alpha i}) = \operatorname{rg}(a_{\alpha i})'.$$

Beweis. Wir können für unsere Behauptung o. B. d. A. voraussetzen, daß die Matrix spezielle Stufenform hat, denn bei Ausführung der Operationen (I) bis (III) etwa auf die Zeilen ändert sich nach Satz 2A nicht der Rang von $(a_{\alpha i})$ und nach Satz 2B nicht der Rang von $(a_{\alpha i})'$, deren Spalten ja gerade die Zeilen von $(a_{\alpha i})$ sind. Nach Beispiel 2 ist der Rang der Spaltenfolge der Stufenmatrix (2.9.4) gleich r. Wir zeigen, daß auch der Rang der Zeilenfolge von (2.9.4) gleich r ist. Dazu wenden wir die Operation (II) auf die Spalten folgendermaßen an: Wir multiplizieren zuerst die k_1-te Spalte mit $-c_{1l}$ und addieren zur l-ten, $l > k_1$. Da $c_{1k_1} = 1$ gilt, erhält die erste Zeile die Form

$$e_{k_1} = (0, \ldots, 0, \underset{k}{1}, 0, \ldots, 0).$$

Die übrigen Zeilen der Matrix ändern sich dabei nicht; wir arbeiten analog die zweite, . . ., r-te Zeile ab und erhalten die Matrix

$$\begin{pmatrix} 0 \ldots 0\ 1\ 0 \ldots\ldots\ldots\ldots\ldots\ldots\ldots 0 \\ 0 \ldots\ldots\ldots 0\ 1\ 0 \ldots\ldots\ldots\ldots\ldots 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ 0 \ldots\ldots\ldots\ldots\ldots\ldots 0\ 1\ 0 \ldots\ldots 0 \\ 0 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 0 \end{pmatrix}. \qquad (9)$$

$k_1 \quad k_2 \ldots\ldots\ldots k_r$

Die Zeilenfolge dieser Matrix besteht aus den Vektoren $(e_{k_1}, \ldots, e_{k_r}, 0, \ldots, 0)$ mit $k_1 < \ldots < k_r$ des K^n, welche offenbar den Rang r hat. □

Folgerung 2. *Der Rang einer Matrix* $(a_{\alpha i}) \in \mathbf{M}_{m,n}(K)$ *ist gleich der maximalen Anzahl linear unabhängiger Zeilen.* □

Aus dem Beweis von Satz 3 wird auch die Richtigkeit der folgenden Behauptung klar:

Folgerung 3. *Der Rang einer Matrix* $(a_{\alpha i}) \in \mathbf{M}_{m,n}(K)$ *ist gleich* r *genau dann, wenn man sie durch Anwendung der elementaren Umformungen* (I) *bis* (III) *auf die Spalten und auf die Zeilen in die Form* (9) *oder, noch spezieller, in die Form* (4.5), *überführen kann, also in eine Matrix, die nur* r *Einsen und sonst nur Nullen enthält, wobei in jeder Spalte und in jeder Zeile höchstens eine* 1 *steht.* □

Durch die vorangehenden Sätze ist die gestellte Aufgabe völlig erledigt. Wir wollen jedoch abschließend zum Thema Rangbestimmung noch ein vor allem für theoretische Untersuchungen nützliches Kriterium für den Rang einer Matrix herleiten. Dazu erinnere man sich zunächst an die Definition 4.8.2 der Minoren einer Matrix. Es gilt:

Satz 4. *Es sei* $(a_{\alpha i}) \in \mathbf{M}_{m,n}(K)$. *Dann gilt* $\operatorname{rg}(a_{\alpha i}) = r$ *dann und nur dann, wenn* $(a_{\alpha i})$ *einen von* 0 *verschiedenen Minor* r*-ter Ordnung besitzt, während alle Minoren der Ordnung* $r+1$ *gleich* 0 *sind.*

Beweis. Wir zerlegen den Beweis in mehrere Schritte. – 1. Schritt. Gibt es in $(a_{\alpha i})$ einen Minor r-ter Ordnung $M_r \neq 0$, so gilt $\operatorname{rg}(a_{\alpha i}) \geqq r$. In der Tat, seien o. B. d. A. die ersten r Spalten am Minor beteiligt, d. h. $M_r = M\begin{pmatrix} p_1 \cdots p_r \\ 1 \ldots r \end{pmatrix}$. Dann müssen diese linear unabhängig sein; denn eine lineare Abhängigkeit der vollen Spalten in K^m würde die lineare Abhängigkeit der Spalten des Minors nach sich ziehen, woraus nach Satz 4.7.4 $M_r = 0$ folgen würde. – 2. Schritt. Gilt $\operatorname{rg}(a_{\alpha i}) \geqq r$, so gibt es einen Minor r-ter Ordnung $M_r \neq 0$. Zum Beweis können wir o. B. d. A. annehmen, daß die ersten r Spalten der Matrix linear unabhängig sind. Dann hat die Teilmatrix $(a_{\alpha\varrho}) \in \mathbf{M}_{m,n}(K)$, $\varrho = 1, \ldots, r$, den Rang r. Nach Folgerung 2 hat diese Matrix auch r linear unabhängige Zeilen; der Minor M_r aus diesen Zeilen ist dann wieder nach Satz 4.7.4 von 0 verschieden; er ist auch der gesuchte Minor $M_r \neq 0$ der Ausgangsmatrix. – 3. Schritt. Nun ist es leicht, den Satz zu beweisen: Gilt $\operatorname{rg}(a_{\alpha i}) = r$, so gibt es nach dem zweiten Schritt einen Minor $M_r \neq 0$, und nach dem ersten Schritt müssen alle Minoren M_k, $k > r$, verschwinden. Umgekehrt, gilt die Bedingung des Satzes, so ist nach dem ersten Schritt $\operatorname{rg}(a_{\alpha i}) \geqq r$. Nach dem zweiten Schritt muß aber $\operatorname{rg}(a_{\alpha i}) < r+1$ sein; denn alle Minoren $(r+1)$-ter Ordnung verschwinden. □

Während wir im ersten Teil des Paragraphen eine algebraische Methode, nämlich den Gaußschen Algorithmus, heranzogen, um das geometrische Problem der Bestimmung von $rg\, a = \dim \operatorname{Im} a$ zu lösen, wollen wir nun mit Hilfe geometrischer Überlegungen die Hauptsätze der Theorie der linearen Gleichungssysteme beweisen. Zunächst wollen wir das allgemeine lineare Gleichungssystem (2.9.1) in Matrixform schreiben. Dazu führen wir den Spaltenvektor $(x_i)_{i=1,\ldots,n}$ der Unbekannten x_i und den Spaltenvektor $(b_\alpha)_{\alpha=1,\ldots,m} \in K^m$ ein; nach Definition der Matrizenmultiplikation ist dann (2.9.1) äquivalent zu

$$(a_{\alpha i})\,(x_i) = (b_\alpha)\,. \tag{10}$$

Der Vergleich mit (4.41) legt nun folgende geometrische Interpretation von (10) nahe: Wir betrachten (x_i) als variablen Vektor aus K^n, $(a_{\alpha i})$ als Matrix der linearen Abbildung

$$a\colon (x_i) \in K^n \mapsto (y_\alpha) := (a_{\alpha i})\,(x_i) \in K^m\,, \tag{11}$$

wobei die Vektorräume K^n, K^m als Räume von Spaltenvektoren $K^n = \mathbf{M}_{n,1}$, $K^m = \mathbf{M}_{m,1}$ aufgefaßt und auf ihre Standardbasen bezogen werden. (Wir könnten analog $(a_{\alpha i})$ als Matrix einer linearen Abbildung $a\colon V^n \to V^m$ bezüglich geeigneter Basen deuten.) Die Auflösung des linearen Gleichungssystems (10) erhält dann folgende geometrische Interpretation: Gegeben seien die lineare Abbildung (11) und ein fester Vektor $(b_\alpha) \in K^m$. Man bestimme das volle Urbild

$$a^{-1}(b_\alpha) = \{(\xi_i) \mid (\xi_i) \in K^n,\ a(\xi_i) = (b_\alpha)\}\,. \tag{12}$$

Aus dieser Interpretation erhält man sofort den „1. Hauptsatz“:

Satz 5 (Kriterium von Kronecker-Capelli). *Ein lineares Gleichungssystem* (2.9.1) *ist lösbar dann und nur dann, wenn der Rang der Matrix des Systems und*

der Rang der erweiterten Matrix übereinstimmen:

$$\operatorname{rg}(a_{\alpha i}) = \operatorname{rg}(a_{\alpha i} b_\alpha) . \tag{13}$$

Beweis. Das System ist lösbar genau dann, wenn (b_α) überhaupt ein Urbild besitzt, d. h., $(b_\alpha) \in \operatorname{Im} a$ gilt. Nach (2.9) wird $\operatorname{Im} a$ von den Bildern der Basis $(\mathfrak{e}_i)$ von K^n erzeugt; diese Bilder sind aber gerade die n Spaltenvektoren der Matrix $(a_{\alpha i})$:

$$a(\mathfrak{e}_i) = \begin{pmatrix} a_{1i} \\ \vdots \\ a_{mi} \end{pmatrix}, \qquad i = 1, \ldots, n . \tag{14}$$

Nun ist (b_α) eine Linearkombination dieser Vektoren genau dann, wenn der Rang der Vektormenge $\{a(\mathfrak{e}_i)\}_{i=1,\ldots,n}$ durch Hinzufügen von (b_α) nicht erhöht wird, d. h., wenn (13) gilt. (Vgl. Übung 4.2.6.) □

Um nun die Urbildmenge $a^{-1}(b_\alpha)$, das ist die Lösungsmenge des Gleichungssystems (2.9.1), zu erhalten, erinnern wir an den Homomorphiesatz 2.4 für Vektorräume. Ist nämlich $\mathfrak{b} \in \operatorname{Im} a$ und $\mathfrak{a} \in \boldsymbol{V}$ ein Vektor mit $a(\mathfrak{a}) = \mathfrak{b}$, so folgt aus dem Diagramm (2.6) sofort

$$a^{-1}(\mathfrak{b}) = \mathfrak{a} + \operatorname{Ker} a \subseteq \boldsymbol{V} . \tag{15}$$

Man erhält also das ganze Urbild $a^{-1}(\mathfrak{b})$, indem man zu irgendeinem seiner Elemente $\mathfrak{a}$ alle Vektoren aus dem Urbild $a^{-1}(\mathfrak{o}) = \operatorname{Ker} a$ addiert. Nun ist $\operatorname{Ker} a$ die Lösungsmenge des homogenen Systems

$$(a_{\alpha i})\,(x_i) = 0 , \tag{16}$$

das aus (2.9.1) entsteht, wenn man die b_α der rechten Seite durch Nullen ersetzt. Man nennt es das *zugehörige homogene System*. Aus dieser Interpretation und Folgerung 2.7 ergibt sich für die Lösung eines homogenen Systems (2. Hauptsatz):

Satz 6. *Ist in dem homogenen System* (16) *von m Gleichungen in den n Unbekannten* x_i, $i = 1, \ldots, n$, *der Rang* $\operatorname{rg}(a_{\alpha i}) = r$, *so ist die Lösungsmenge des Systems ein* $(n-r)$*-dimensionaler Unterraum des Vektorraumes* K^n.

Beweis. Ein homogenes System ist stets trivial lösbar. Die Behauptung folgt aus Folgerung 2.7 und Satz 1. □

Die Formel (15) ergibt, in die Sprache der linearen Gleichungssysteme übersetzt, den folgenden 3. Hauptsatz:

Satz 7. *Es sei* (2.9.1) (*oder* (10)) *ein lösbares lineares Gleichungssystem aus m Gleichungen mit n Unbekannten; dabei gelte* $\operatorname{rg}(a_{\alpha i}) = r$. *Dann hängt die Lösungsmenge* (12) *des Systems von* $n-r$ *Parametern* $t_\varkappa$, $\varkappa = 1, \ldots, n-r$, *ab. Genauer gilt: Ist* $(\alpha_i) \in K^n$ *irgendeine Lösung des Systems* (2.9.1) *und bezeichnen die n-Tupel* $(\beta_{i\varkappa}) \in K^n$, $\varkappa = 1, \ldots, n-r$, *eine Basis der Lösungsmenge des zugehörigen homogenen Systems,*

so ist

$$\xi_i = \alpha_i + \sum_{\varkappa=1}^{n-r} \beta_{i\varkappa} t_\varkappa, \qquad i = 1, \ldots, n, \qquad t_\varkappa \in K, \tag{17}$$

die Lösungsmenge des Systems (2.9.1). □

Man erhält also alle Lösungen eines (lösbaren) inhomogenen Systems, indem man zu irgendeiner seiner Lösungen alle Lösungen des zugehörigen homogenen Systems addiert. Vergleicht man (17) mit (4.5.8), so liegt eine Interpretation der Lösungsmenge eines inhomogenen Systems als k-Ebene, $k = n - r$, des n-dimensionalen affinen Raumes K^n (Beispiel 4.3.1) nahe; hierauf werden wir im nächsten Paragraphen zurückkommen.

Es sei bemerkt, daß die praktische Lösung eines linearen Gleichungssystems in der Regel mit Hilfe des Gaußschen Algorithmus erfolgt. Die Bedeutung der Sätze 5 bis 7 liegt also eher in der Klärung des theoretischen Hintergrundes dieses Algorithmus. Wir vergleichen sie daher noch mit dem Satz 2.9.3. Der Fall a) dieses Satzes entspricht einem unlösbaren, Fall b) einem lösbaren System. Der Gaußsche Algorithmus liefert also von selbst die Entscheidung, ob das System lösbar ist oder nicht. Nach Beispiel 3 ist r der Rang der Matrix $(a_{\alpha i})$, und (2.9.6) entspricht der Parameterdarstellung (17) der Lösungsmenge. Nach einer Umnumerierung der Unbekannten können wir o. B. d. A. $k_1 = 1, \ldots, k_r = r$ annehmen. Die Gleichungen (2.9.6) können wir dann in der Gestalt

$$\left.\begin{aligned} \xi_\varrho &= \alpha_\varrho + \sum_{\varkappa=1}^{n-r} \beta_{\varrho\varkappa} t_\varkappa, \qquad \varrho = 1, \ldots, r, \\ \xi_\sigma &= t_{\sigma-r}, \qquad\qquad\quad \sigma = r+1, \ldots, n, \end{aligned}\right\} \tag{18}$$

lösen, wobei einige Umbezeichnungen vorgenommen werden. (18) ist offenbar ein Spezialfall von (17). Der Gaußsche Algorithmus erledigt natürlich auch die Rangbestimmung „von selbst".

Beispiel 4. Besteht das Gleichungssystem aus einer einzigen Gleichung

$$a_1 x_1 + \ldots + a_n x_n = b \tag{19}$$

und sind nicht alle a_i gleich 0, so ist das System stets lösbar. Gilt etwa $a_n \neq 0$, so können wir die Lösungsmenge sofort hinschreiben:

$$\left.\begin{aligned} \xi_n &= a_n^{-1} \left(b - \sum_{\alpha=1}^{n-1} a_\alpha t_\alpha \right), \\ \xi_\alpha &= t_\alpha, \qquad \alpha = 1, \ldots, n-1. \end{aligned}\right\} \tag{20}$$

Beispiel 5. Eine einfache Verallgemeinerung von Beispiel 4 erhält man folgendermaßen: Es sei (2.9.1) ein Gleichungssystem vom Rang $r = \operatorname{rg}(a_{\alpha i}) = m \leqq n$; dabei sei o. B. d. A. der Minor

$$\det(a_{\mu,n-m+\nu}) = \begin{vmatrix} a_{1,n-m+1} & a_{1,n-m+2} & \cdots & a_{1n} \\ a_{2,n-m+1} & a_{2,n-m+2} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m,n-m+1} & a_{m,n-m+2} & \cdots & a_{mn} \end{vmatrix} \neq 0 . \tag{21}$$

Dann ist das System stets lösbar, und wir können die Lösungsmenge in der Form

$$\left.\begin{aligned} \begin{pmatrix} \xi_{n-m+1} \\ \vdots \\ \xi_\mu \\ \vdots \\ \xi_n \end{pmatrix} &= (a_{\mu,n-m+\nu})^{-1} \left(\begin{pmatrix} b_1 \\ \vdots \\ b_\nu \\ \vdots \\ b_m \end{pmatrix} - (a_{\mu\tau}) \begin{pmatrix} t_1 \\ \vdots \\ t_\tau \\ \vdots \\ t_{n-m} \end{pmatrix} \right), \\ \xi_\tau &= t_\tau, \qquad \tau = 1, \ldots, n-m, \qquad \mu, \nu = 1, \ldots, m , \end{aligned}\right\} \tag{22}$$

schreiben; dabei ist $(a_{\mu,n-m+\nu})^{-1}$ die Inverse der den Minor (21) definierenden Matrix, und $(a_{\mu\tau}) \in \mathbf{M}_{m,n-m}$ ist die aus den ersten $n-m$ Spalten von $(a_{\alpha i})$ bestehende Teilmatrix.

Übung 2. a) Man beweise die Behauptung von Beispiel 5 mit Hilfe der Cramerschen Regel, Satz 4.8.4. — b) Man beweise die Cramersche Regel als Spezialfall der Behauptung von Beispiel 5.

Übung 3. Man beweise für den Rang des Produkts zweier Matrizen

$$\operatorname{rg}((b_{\alpha\varkappa})(a_{\varkappa i})) \leqq \min(\operatorname{rg}(b_{\alpha\varkappa}), \operatorname{rg}(a_{\varkappa i})) . \tag{23}$$

Übung 4. Es sei $(b_{\alpha i}) \in \mathbf{M}_{m,n}(K)$, $(a_{ij}) \in \mathbf{GL}(n, K)$, $(c_{\beta\alpha}) \in \mathbf{GL}(m, K)$. Man beweise $\operatorname{rg}(b_{\alpha i}) = \operatorname{rg}((c_{\beta\alpha})(b_{\alpha i})(a_{ij}))$.

Übung 5. Man beweise, daß aus einer maximalen linear unabhängigen Menge von Spalten der Matrix $(a_{\alpha i}) \in \mathbf{M}_{m,n}(K)$ bei den Unformungen aus Satz 2A wieder eine maximale linear unabhängige Menge von Spalten der umgeformten Matrix entsteht.

Übung 6. Es sei $(a_{\alpha i}) \in \mathbf{M}_{m,n}(K)$, $\operatorname{rg}(a_{\alpha i}) = r$. Dann bilden die zu einem von 0 verschiedenen Minor r-ter Ordnung der Matrix gehörenden Spalten (bzw. Zeilen) der Matrix $(a_{\alpha i})$ eine maximale linear unabhängige Spaltenfolge (bzw. Zeilenfolge).

§ 6. Duale Vektorräume

In diesem Paragraphen wollen wir einen besonders für die Anwendungen der linearen Algebra in der Analysis wichtigen Spezialfall der linearen Abbildungen, nämlich die Linearformen oder dualen Vektoren, betrachten. Unter dem zu einem Vektorraum $\boldsymbol{V}$ über K *dualen Raum* $\boldsymbol{V}'$ versteht man den Vektorraum

$$\boldsymbol{V}' := \boldsymbol{L}(\boldsymbol{V}, K) \tag{1}$$

der linearen Abbildungen von $\boldsymbol{V}$ in K (vgl. Satz 4.2), dessen Elemente man auch *Linearformen* oder *duale Vektoren* nennt. Aus den Ergebnissen von § 4 folgt leicht

Satz 1. *Ist $\boldsymbol{V}^n$ ein Vektorraum über K,* dim $\boldsymbol{V}^n = n$, *so gilt auch* dim $\boldsymbol{V}' = n$. *Zu jeder Basis $(\mathfrak{a}_i)$ von $\boldsymbol{V}^n$ gehört eine eindeutig bestimmte Basis $(\mathfrak{u}_j)$ von $\boldsymbol{V}'^n$ derart, daß*

$$\mathfrak{u}_j(\mathfrak{a}_i) = \delta_{ij} \tag{2}$$

gilt.

Beweis. Die Dimensionsbehauptung ist ein Spezialfall von Satz 4.3; denn $K = \boldsymbol{W}$ ist eindimensional. In diesem Vektorraum besteht die Standardbasis aus dem einzigen Element $e_1 = 1$. Deshalb ist Formel (2) ein Spezialfall von (4.22); die zweite Behauptung ergibt sich aus der Folgerung 4.2. □

Die durch (2) bestimmte Basis $(\mathfrak{u}_j)$ heißt die zu $(\mathfrak{a}_i)$ *duale Basis*. Wir wollen noch einen Beweis ihrer Basiseigenschaften angeben. Zunächst bemerken wir, daß für alle $\mathfrak{x} \in \boldsymbol{V}^n$

$$\mathfrak{x} = \sum_i \mathfrak{a}_i \xi_i \leftrightarrow \mathfrak{u}_i(\mathfrak{x}) = \xi_i \qquad (i = 1, \ldots, n) \tag{3}$$

gilt, d. h., die Linearform $\mathfrak{u}_i$ ordnet dem Vektor $\mathfrak{x}$ seine i-te Komponente bezüglich der Basis $(\mathfrak{a}_j)$ zu (anschaulich: Koordinate der Parallelprojektion von $\mathfrak{x}$ auf die i-te Achse). Da die $\mathfrak{u}_i$ als lineare Abbildungen durch die Werte auf einer Basis eindeutig bestimmt sind, erhalten wir nach Satz 2.5 n wohlbestimmte duale Vektoren. Diese erzeugen den $\boldsymbol{V}'$. Ist nämlich $\mathfrak{v} \in \boldsymbol{V}'$ irgendeine Linearform, so gilt für alle $\mathfrak{x} \in \boldsymbol{V}^n$ nach (3)

$$\mathfrak{v}(\mathfrak{x}) = \sum_{i=1}^{n} \mathfrak{v}(\mathfrak{a}_i)\, \xi_i = \sum_{i=1}^{n} v_i \mathfrak{u}_i(\mathfrak{x}); \tag{4}$$

dabei wurde

$$v_i := \mathfrak{v}(\mathfrak{a}_i), \qquad i = 1, \ldots, n \tag{5}$$

gesetzt. Die v_i sind nach (4) gerade die Koordinaten von $\mathfrak{v}$ bezüglich $\mathfrak{u}_i$; denn (4) gilt ja für alle $\mathfrak{x}$, und wir haben $\mathfrak{v} = \sum_i \mathfrak{u}_i v_i$. Daher ist $\{\mathfrak{u}_i\}$ eine erzeugende Menge. Andererseits ist $\{\mathfrak{u}_i\}$ linear unabhängig; denn aus $\sum_i \mathfrak{u}_i \lambda_i = \mathfrak{o}$ folgt

$$\sum_i \mathfrak{u}_i \lambda_i(\mathfrak{a}_j) = \sum_i \mathfrak{u}_i(\mathfrak{a}_j)\, \lambda_i = \sum_i \delta_{ij} \lambda_i = \lambda_j = 0$$

für $j = 1, \ldots, n$. Damit ist noch einmal ein Beweis von Satz 1 erbracht. Die Beziehungen (4) und (5) können wir zu der Beziehung

$$\mathfrak{v} = \sum_{i=1}^{n} \mathfrak{u}_i v_i \leftrightarrow \mathfrak{v}(\mathfrak{a}_i) = v_i \qquad (i = 1, \ldots, n) \tag{6}$$

zusammenfassen, die zu (3) analog ist. Bevor wir die allgemeinen Betrachtungen fortsetzen, geben wir zunächst einige Beispiele:

Beispiel 1. Es sei $[\boldsymbol{A}^n, \boldsymbol{V}^n, K]$ eine n-dimensionale affine Geometrie. Wir wählen einen Punkt $o \in \boldsymbol{A}^n$ und ein $\mathfrak{v} \in \boldsymbol{V}'$, $\mathfrak{v} \neq \mathfrak{o}$. Dann beschreibt

$$\mathfrak{v}(\overrightarrow{ox}) = c, \qquad c \in K,$$

eine Schar paralleler Hyperebenen; in der Tat erhalten wir bezüglich eines n-Beins $(o; \mathfrak{a}_i)$ für $\overrightarrow{ox} = \sum_i \mathfrak{a}_i x_i$ sofort die lineare Gleichung

$$\sum_i v_i x_i = c$$

(vgl. Beispiel 5.4, (5.20) ist eine Parameterdarstellung der Hyperebene). Durchläuft c den Körper K, so sind die entstehenden Hyperebenen parallel und disjunkt. Der Vektorraum der Hyperebenen ist nämlich für alle diese Ebenen derselbe: Ist $\mathfrak{v}(\overrightarrow{ox}) = c$ und $\mathfrak{v}(\overrightarrow{oy}) = c$, so gilt für den beliebigen Vektor $\overrightarrow{xy}$ der Hyperebene

$$\mathfrak{v}(\overrightarrow{xy}) = \mathfrak{v}\,(\overrightarrow{oy} - \overrightarrow{ox}) = \mathfrak{v}(\overrightarrow{oy}) - \mathfrak{v}(\overrightarrow{ox}) = 0\,.$$

Die Vektorkoordinaten ξ_i von $\overrightarrow{xy} = \sum_i a_i \xi_i$ genügen also für alle Hyperebenen der zugehörigen homogenen Gleichung

$$\mathfrak{v}(\overrightarrow{xy}) = \sum_{i=1}^{n} v_i \xi_i = 0\,.$$

Jedem dualen Vektor $\mathfrak{v} \neq \mathfrak{o}$ entspricht also – als Schar seiner Niveauflächen – eine Schar paralleler Hyperebenen. Offenbar bestimmen $\mathfrak{v}$ und $\mathfrak{v}\lambda$, $\lambda \neq 0$, dieselbe Schar. Wir erinnern daran, daß wir speziell die affine Geometrie $[\boldsymbol{V}^n, \boldsymbol{V}^n, K]$ betrachten können, vgl. Beispiel 4.3.1. Im Raum $\boldsymbol{V}^n = \boldsymbol{A}^n$ ist ein Punkt, nämlich der Vektor $\mathfrak{o}$, ausgezeichnet. Man beweist leicht

Übung 1. In der affinen Geometrie $[\boldsymbol{V}^n, \boldsymbol{V}^n, K]$ wird durch die Gleichung

$$\mathfrak{v}(\mathfrak{x}) = 1 \tag{7}$$

jedem dualen Vektor $\mathfrak{v} \in \boldsymbol{V}'$, $\mathfrak{v} \neq \mathfrak{o}$, eine eindeutig bestimmte, nicht durch das „Zentrum" $\mathfrak{o}$ gehende Hyperebene zugeordnet (*nichtzentrale Hyperebene*). Diese Beziehung zwischen $\boldsymbol{V}' \setminus \{\mathfrak{o}\}$ und der Menge aller nichtzentralen Hyperebenen ist bijektiv.

Beispiel 2. Es sei $[a, b] \subset \mathbf{R}$ ein Intervall und $\boldsymbol{V}$ die Menge aller auf $[a, b]$ beliebig oft stetig differenzierbaren Funktionen. In der Analysis wird bewiesen, daß $\boldsymbol{V}$ ein Vektorraum über $\mathbf{R}$ (nicht endlicher Dimension) ist. Wir geben einige Beispiele dualer Vektoren an, die man in diesem Fall auch „*Funktionale*" nennt.

1. Für $x \in [a, b]$, x fest, setzen wir

$$\mu_x : f \in \boldsymbol{V} \mapsto f(x) \in \mathbf{R}\,. \tag{8}$$

2. Für $n \in \mathbf{N}$ bezeichne $f^{(n)}$ die n-te Ableitung von f. Es sei $x \in [a, b]$. Wir setzen

$$\mu_{x,n} : f \in \boldsymbol{V} \mapsto f^{(n)}(x) \in \mathbf{R}\,. \tag{9}$$

3. Es sei $p(x)$ eine über $[a, b]$ integrierbare Funktion. Wir setzen

$$I_p : f \in \boldsymbol{V} \mapsto \int_a^b f(x)\, p(x)\, dx \in \mathbf{R}\,. \tag{10}$$

Übung 2. Es sei K ein Körper. Wir betrachten den Polynomring $\boldsymbol{V} := K[x]$ als Vektorraum über K. Man beweise die Vektorraumisomorphie $\boldsymbol{V}' \cong K[[x]]$ (Ring der formalen Potenzreihen, vgl. Übung 2.4.1, Übung 4.4.6).

Beispiel 2 und Übung 2 lehren, daß die Untersuchung von $\boldsymbol{V}'$ im unendlichdimensionalen Fall bedeutend komplizierter ist als für endlichdimensionale Vektorräume. Daher wollen wir uns im folgenden auf diese beschränken; die unendlichdimensio-

nalen Vektorräume und ihre dualen Räume werden unter Hinzuziehung topologischer Hilfsmittel in der Funktionalanalysis untersucht.

Satz 1 zeigt, daß für dim $V<\infty$ die Räume V und V' zueinander isomorph sind. Es ist jedoch kein Isomorphismus zwischen ihnen in natürlicher Weise gegeben, so daß wir die Räume nicht miteinander identifizieren können. Bilden wir nun das Dual $(V')'$ des dualen Raumes, so zeigt der folgende Satz 2, daß $(V')'=V$ gesetzt werden kann. Vorerst bemerken wir jedoch

Übung 3. Für den Vektorraum V von Übung 2 zeige man im Fall eines endlichen Körpers K, daß V' nicht isomorph zu V ist.

Satz 2. *Es sei V ein Vektorraum über K,* dim $V<\infty$, *und V' sein Dual. Dann wird jedem $\mathfrak{x}\in V$ durch die Definition*

$$\mathfrak{v}\in V'\mapsto(\mathfrak{v}\mid\mathfrak{x}):=\mathfrak{v}(\mathfrak{x})\in K \tag{11}$$

eine Linearform über V' zugeordnet. Diese Zuordnung ist ein kanonischer linearer Isomorphismus φ, mit dessen Hilfe wir V und $(V')'$ identifizieren:

$$V=(V')'. \tag{12}$$

Beweis. Zunächst bemerken wir, daß in (11) $\mathfrak{x}$ als fest, $\mathfrak{v}\in V'$ als variabel anzusehen ist. Die Schreibweise ist wegen der völligen Symmetrie von V und V' zweckmäßig. Nach dem Beweis unseres Satzes 2 haben wir dann das Recht, (11) als sogenanntes *Skalarprodukt eines Vektors und eines dualen Vektors* anzusehen und ganz nach Belieben

$$(\mathfrak{v}\mid\mathfrak{x})=(\mathfrak{x}\mid\mathfrak{v})=\mathfrak{v}(\mathfrak{x})=\mathfrak{x}(\mathfrak{v}) \tag{13}$$

zu schreiben. Zum Beweis ist zunächst einmal auf Grund der Definition 4.5 klar, daß $\varphi(\mathfrak{x})\,(\mathfrak{v})$ linear in $\mathfrak{v}$ ist, d. h. $\varphi(\mathfrak{x})\in(V')'$ gilt. Ebenso leicht folgt, daß $\varphi: V\to(V')'$ eine lineare Abbildung ist. Wir haben nämlich für $\mathfrak{x},\mathfrak{y}\in V$, $\mathfrak{v}\in V'$, $\lambda,\mu\in K$

$$\begin{aligned}\varphi(\mathfrak{x}\lambda+\mathfrak{y}\mu)\,(\mathfrak{v})&=\mathfrak{v}\,(\mathfrak{x}\lambda+\mathfrak{y}\mu)=\mathfrak{v}(\mathfrak{x})\,\lambda+\mathfrak{v}(\mathfrak{y})\,\mu\\&=\varphi(\mathfrak{x})\,(\mathfrak{v})\,\lambda+\varphi(\mathfrak{y})\,(\mathfrak{v})\,\mu=(\varphi(\mathfrak{x})\,\lambda+\varphi(\mathfrak{y})\,\mu)\,(\mathfrak{v})\,.\end{aligned}$$

Da dim $V=$dim $V'=$dim $(V')'<\infty$ nach Satz 1 gilt, ist nach Folgerung 2.8 der Beweis erbracht, wenn wir Ker $\varphi=\{\mathfrak{o}\}$ zeigen. Das ist aber leicht einzusehen: Aus $\varphi(\mathfrak{x})=\mathfrak{o}$ folgt $\mathfrak{v}(\mathfrak{x})=0$ für alle $\mathfrak{v}\in V'$. Ist $\mathfrak{x}=\sum_i \mathfrak{a}_i\xi_i$ eine Basisdarstellung von $\mathfrak{x}$ und $(\mathfrak{u}_i)$ die zu $(\mathfrak{a}_i)$ duale Basis, so können wir speziell $\mathfrak{v}=\mathfrak{u}_i$ einsetzen und erhalten nach (3) $\mathfrak{u}_i(\mathfrak{x})=\xi_i=0$, also $\mathfrak{x}=\mathfrak{o}$. □

Die Beziehung zwischen V^n und V'^n ist also völlig symmetrisch. Wir wollen als nächstes eine Relation zwischen den Unterräumen von V und V' herstellen.

Definition 1. Es sei V ein Vektorraum über K, $W\subseteq V$ ein Unterraum. Unter dem *Annullator* $W^\perp$ von W versteht man den Unterraum

$$W^\perp:=\{\mathfrak{v}\mid\mathfrak{v}\in V' \text{ und } (\mathfrak{v}\mid\mathfrak{x})=0 \text{ für alle } \mathfrak{x}\in W\}\,. \tag{14}$$

Satz 3. *Unter den Voraussetzungen von Definition* 1 *ist* $\boldsymbol{W}^\perp$ *ein Unterraum von* $\boldsymbol{V}'$. *Gilt* dim $\boldsymbol{V}=n<\infty$ *und* dim $\boldsymbol{W}=k$, *so ist* dim $\boldsymbol{W}^\perp=n-k$.

Beweis. Die erste Behauptung ist trivial. Für die zweite wählen wir die Basis $\{\mathfrak{a}_i\}\subset\boldsymbol{V}^n$ so, daß $\mathfrak{L}(\{\mathfrak{a}_1, ..., \mathfrak{a}_k\})=\boldsymbol{W}^k$ gilt. Dann ist $\boldsymbol{W}^\perp=\mathfrak{L}(\{\mathfrak{u}_{k+1}, ..., \mathfrak{u}_n\})$, $\{\mathfrak{u}_i\}$ die zu $\{\mathfrak{a}_i\}$ duale Basis. □

Übung 4. Unter den Voraussetzungen von Satz 3 zeige man: a) Gilt $\boldsymbol{W}_0\subseteq\boldsymbol{W}_1$, so ist $\boldsymbol{W}_0^\perp\supseteq\boldsymbol{W}_1^\perp$. — b) Ist dim $\boldsymbol{V}<\infty$, so gilt

$$(\boldsymbol{W}^\perp)^\perp=\boldsymbol{W}\,, \tag{15}$$

$$(\boldsymbol{W}_0+\boldsymbol{W}_1)^\perp=\boldsymbol{W}_0^\perp\cap\boldsymbol{W}_1^\perp, \tag{16}$$

$$(\boldsymbol{W}_0\cap\boldsymbol{W}_1)^\perp=\boldsymbol{W}_0^\perp+\boldsymbol{W}_1^\perp. \tag{17}$$

Beispiel 3. Ein lineares Gleichungssystem (2.9.1) können wir auch noch anders als in § 5 geometrisch interpretieren. Beziehen wir nämlich einen Vektor $\mathfrak{x}\in\boldsymbol{V}$ und einen dualen Vektor $\mathfrak{v}\in\boldsymbol{V}'$ auf zueinander duale Basen:

$$\mathfrak{x}=\sum_i\mathfrak{a}_i\xi_i, \qquad \mathfrak{v}=\sum_i\mathfrak{u}_iv_i,$$

so folgt in diesen Koordinaten nach (2)

$$(\mathfrak{v}\mid\mathfrak{x})=\sum_{i,j}(\mathfrak{u}_j\mid\mathfrak{a}_i)\,\xi_iv_j=\sum_i\xi_iv_i\,. \tag{18}$$

Deuten wir nun die x_i in (2.9.1) als Koordinaten eines Punktes x bezüglich eines affinen n-Beins $(o;\mathfrak{a}_i)$ und die $(a_{\alpha i})_{i=1,...,n}$, α fest, als Koordinaten eines dualen Vektors $\mathfrak{v}_\alpha$,

$$\mathfrak{v}_\alpha:=\sum_{i=1}^n\mathfrak{u}_ia_{\alpha i}\,, \tag{19}$$

so ist (2.9.1) äquivalent zu dem System

$$(\mathfrak{v}_\alpha\mid\overrightarrow{ox})=b_\alpha, \qquad \alpha=1, ..., m\,. \tag{20}$$

Setzen wir nun $\mathfrak{v}_\alpha\neq\mathfrak{o}$, $\alpha=1, ..., m$, voraus — die Gleichungen, für die $\mathfrak{v}_\alpha=\mathfrak{o}$ und $b_\alpha=0$ ist, können wir ja fortlassen, und wenn $\mathfrak{v}_\alpha=\mathfrak{o}$, aber $b_\alpha\neq0$ gilt, ist das System unlösbar —, so erscheint die Lösungsmenge von (2.9.1) als Durchschnitt der m durch die Gleichungen (20) beschriebenen Hyperebenen. Das System ist genau dann lösbar, wenn der Durchschnitt nicht leer ist; in diesem Fall ist (5.17) oder in koordinatenfreier Schreibweise

$$x=a+\sum_{\varkappa=1}^{n-r}\mathfrak{b}_\varkappa t_\varkappa, \qquad t_\varkappa\in K\,, \tag{21}$$

die Parameterdarstellung des Durchschnittes; dabei sind $\mathfrak{b}_1, ..., \mathfrak{b}_{n-r}$ als Basis des Annullators von $\mathfrak{L}(\{\mathfrak{v}_1, ..., \mathfrak{v}_m\})$ linear unabhängig.

Beispiel 4. Es sei umgekehrt die Parameterdarstellung (21) einer k-Ebene $(k=n-r)$ gegeben. Wir zeigen, daß man diese k-Ebene als Lösung eines Systems

(20) von $r=n-k$ linearen Gleichungen darstellen kann. Dazu genügt es, den Annullator $W^{\perp}\subseteq V'$ des Vektorraumes W^k der Ebene durch Lösung des homogenen Systems vom Rang k

$$(\mathfrak{v} \mid \mathfrak{b}_\varkappa)=0, \qquad \varkappa=1, \ldots, k, \tag{22}$$

zu bestimmen, d. h. r linear unabhängige Lösungen $\mathfrak{w}_1, \ldots, \mathfrak{w}_r$ von (22) zu finden. Dann folgt aus (21) durch Bilden der Ortsvektoren bezüglich o und skalare Multiplikation mit $\mathfrak{w}_\varrho$

$$(\mathfrak{w}_\varrho \mid \overrightarrow{ox})=c_\varrho := (\mathfrak{w}_\varrho \mid \overrightarrow{oa}), \qquad \varrho=1, \ldots, r=n-k. \tag{23}$$

Geht man zu den Koordinaten über, so erhält man ein lineares Gleichungssystem aus r Gleichungen mit n Unbekannten vom Rang r. Man nennt dieses oder auch (23) eine *implizite Darstellung der k-Ebene*. Den Übergang zur impliziten Darstellung, den man auch durch Auflösen von (5.17) nach den $t_\varkappa$ bewerkstelligen kann, nennt man *„Elimination der Parameter"*.

Übung 5. Es sei $(o; \mathfrak{a}_i)$ ein festes n-Bein des affinen Raumes A^n und $H^k\subseteq A^n$ eine k-Ebene, $k=n-r$, mit der Parameterdarstellung (5.17). Für die Matrix $(\beta_{i\varkappa})\in \mathbf{M}_{\overline{n,k}}$ sei der Minor

$$\det(\beta_{\lambda\varkappa})_{\lambda,\varkappa=1,\ldots,k}\neq 0.$$

Man beweise: Die k-Ebene H^k besitzt dann eine und nur eine Darstellung der Form

$$x_\sigma = a_\sigma + \sum_{\varkappa=1}^{k} b_{\sigma\varkappa}x_\varkappa, \qquad \sigma=k+1, \ldots, n. \tag{24}$$

Die Darstellung (24) können wir gleichzeitig als implizite oder als Parameterdarstellung von H^k auffassen; für die zweite Möglichkeit ist nur $x_\varkappa=t_\varkappa$, $\varkappa=1, \ldots, k$, einzusetzen. Die Zahlen $a_\sigma, b_{\sigma\varkappa}\in K$, $\sigma=k+1, \ldots, n$, $\varkappa=1, \ldots, k$, sind als *Koordinaten der k-Ebene* in dem betrachteten Bezugssystem $(o; \mathfrak{a}_i)$ anzusehen. Die Voraussetzung über die Determinante bedeutet: Stellt man den Vektorraum V^n von A^n in der Form

$$V^n = W_1 \oplus W_2, \qquad W_1 = \mathfrak{L}(\{\mathfrak{a}_1, \ldots, \mathfrak{a}_k\}), \qquad W_2 = \mathfrak{L}(\{\mathfrak{a}_{k+1}, \ldots, \mathfrak{a}_n\})$$

dar, so bestimmt diese Zerlegung eine Projektion

$$\begin{aligned} p_1 : x\in A^n &\mapsto \overrightarrow{ox}\in V^n \mapsto p_{W_1}(\overrightarrow{ox})\in W_1 \\ &\mapsto p_1(x) := o + p_{W_1}(\overrightarrow{ox})\in H_0^k ; \end{aligned} \tag{25}$$

dabei ist $H_0^k = H(o; \mathfrak{a}_1, \ldots, \mathfrak{a}_k)$ (vgl. Beispiel 2.4); dann gilt: $p_1 \mid H^k : H^k \to H_0^k$ ist ein affiner Isomorphismus. Man sagt in diesem Fall: H^k projiziert sich eineindeutig auf H_0^k oder „liegt *schlicht* über H_0^k".

Wir wollen nun jeder linearen Abbildung $a\in L(V, W)$ ihre transponierte Abbildung $a'\in L(W', V')$ zuordnen. Dazu beginnen wir mit einem einfachen geometrischen Beispiel.

Beispiel 5. Es sei $a\in L(V, W)$. In W sei ein Unterraum P als Annullator eines endlichdimensionalen Unterraumes $U^k\subseteq W'$ definiert: $P := U^{k\perp}\subseteq W$. Ist also

$\{\mathfrak{v}_1, ..., \mathfrak{v}_k\}$ eine Basis von U^k, so gilt

$$\mathfrak{y} \in P \Leftrightarrow (\mathfrak{v}_\varkappa \mid \mathfrak{y}) = 0, \qquad \varkappa = 1, ..., k. \tag{26}$$

Wir fragen nach dem Urbild $a^{-1}(P)$, das wir ebenfalls implizit charakterisieren wollen. Offenbar gilt:

$$\mathfrak{x} \in a^{-1}(P) \Leftrightarrow a(\mathfrak{x}) \in P \Leftrightarrow (\mathfrak{v}_\varkappa \mid a(\mathfrak{x})) = 0, \qquad \varkappa = 1, ..., k. \tag{27}$$

Der Ausdruck $(\mathfrak{v}_\varkappa \mid a(\mathfrak{x}))$ aus Gleichung (27) ist linear in $\mathfrak{x}$ als Verkettung der linearen Abbildungen $a: V \to W$ und $\mathfrak{v}_\varkappa: W \to K$; er stellt daher eine lineare Abbildung von V in K, also ein Element aus V' dar. (27) ist ein lineares Gleichungssystem, dessen Lösungsmenge $a^{-1}(P)$ ist. Diese Betrachtungen führen uns auf die folgende Definition:

Definition 2. Es sei $a \in L(V, W)$. Dann ist jedem $\mathfrak{v} \in W'$ durch

$$(a'\mathfrak{v} \mid \mathfrak{x}) := (\mathfrak{v} \mid a\mathfrak{x}) \qquad (\mathfrak{x} \in V) \tag{28}$$

ein eindeutig bestimmtes Element $a'\mathfrak{v} \in V'$ zugeordnet. Die Abbildung $a': W' \to V'$ heißt die *zu a transponierte Abbildung.*

Bevor wir die Eigenschaften der transponierten Abbildungen näher untersuchen, wollen wir zuerst Beispiel 5 zu Ende führen. Unter Berücksichtigung von Definition 2 folgt aus (27):

$$\mathfrak{x} \in a^{-1}(P) \Leftrightarrow (a'\mathfrak{v}_\varkappa \mid \mathfrak{x}) = 0, \qquad \varkappa = 1, ..., k; \tag{26a}$$

ist also $P \subseteq W$ Lösungsmenge des mit $\mathfrak{v}_\varkappa \in W'$ gebildeten Gleichungssystems (26), so wird das Urbild $a^{-1}(P)$ durch das analoge, mit $a'\mathfrak{v}_\varkappa$ gebildete homogene Gleichungssystem (26a) beschrieben.

Übung 6. Es seien $a \in L(V, W)$ und $U \subseteq W'$. Man beweise

$$a^{-1}(U^\perp) = a'(U)^\perp. \tag{29}$$

Satz 4. *Die in Definition 2 definierte Abbildung a' ist linear. Ist a surjektiv, so ist a' injektiv. Für $a, b \in L(V, W)$ und $\alpha \in K$ gilt*

$$(a+b)' = a' + b', \tag{30}$$

$$(a\alpha)' = a'\alpha. \tag{31}$$

Ist schließlich $a \in L(V, W)$ und $b \in L(W, X)$, so gilt

$$(b \circ a)' = a' \circ b'. \tag{32}$$

Beweis. Für $\mathfrak{v}, \mathfrak{w} \in W'$ und $\lambda, \mu \in K$ gilt

$$\begin{aligned}(a'(\mathfrak{v}\lambda + \mathfrak{w}\mu) \mid \mathfrak{x}) &= (\mathfrak{v}\lambda + \mathfrak{w}\mu \mid a\mathfrak{x}) = (\mathfrak{v} \mid a\mathfrak{x})\,\lambda + (\mathfrak{w} \mid a\mathfrak{x})\,\mu \\ &= (a'(\mathfrak{v})\,\lambda \mid \mathfrak{x}) + (a'(\mathfrak{w})\,\mu \mid \mathfrak{x}) = (a'(\mathfrak{v})\,\lambda + a'(\mathfrak{w})\,\mu \mid \mathfrak{x})\end{aligned}$$

für alle $\mathfrak{x} \in V$. Daher müssen diese Linearformen übereinstimmen:

$$a'(\mathfrak{v}\lambda + \mathfrak{w}\mu) = a'(\mathfrak{v})\,\lambda + a'(\mathfrak{w})\,\mu,$$

und die erste Behauptung ist bewiesen. Zum Beweis der zweiten genügt es, Ker $a' = \{\mathfrak{o}\}$ zu zeigen. Es gilt sogar allgemeiner

$$\operatorname{Ker} a' = (\operatorname{Im} a)^{\perp}. \tag{33}$$

In der Tat, es gilt $\mathfrak{v} \in \operatorname{Ker} a'$, d. h. $a'(\mathfrak{v}) = \mathfrak{o}$ dann und nur dann, wenn für alle $\mathfrak{x} \in \boldsymbol{V}$ die Gleichung $(a'(\mathfrak{v}) \mid \mathfrak{x}) = (\mathfrak{v} \mid a\mathfrak{x}) = 0$ gilt, also $\mathfrak{v} \in \operatorname{Im} a^{\perp}$ ist. Aus $\operatorname{Im} a = \boldsymbol{W}$ folgt aber $\operatorname{Ker} a' = \boldsymbol{W}^{\perp} = \{\mathfrak{o}\}$. Die Beziehungen (30), (31) ergeben sich durch einfaches Zurückgehen auf die Definitionen. Wir beweisen noch (32). In der Tat gilt für alle $\mathfrak{x} \in \boldsymbol{V}$ und $\mathfrak{z} \in \boldsymbol{X}'$

$$\begin{aligned}((b \circ a)'\,\mathfrak{z} \mid \mathfrak{x}) &= (\mathfrak{z} \mid b \circ a(\mathfrak{x})) = (\mathfrak{z} \mid b(a(\mathfrak{x}))) = (b'(\mathfrak{z}) \mid a(\mathfrak{x})) \\ &= (a'(b'(\mathfrak{z})) \mid \mathfrak{x}) = (a' \circ b'(\mathfrak{z}) \mid \mathfrak{x}),\end{aligned}$$

also $(b \circ a)'(\mathfrak{z}) = a' \circ b'(\mathfrak{z})$. □

Beachtet man noch die triviale Beziehung $(\mathrm{id}_{\boldsymbol{V}})' = \mathrm{id}_{\boldsymbol{V}'}$, so ergibt sich aus (32) sofort (vgl. Definition 1.5.3)

Folgerung 1. *Die Zuordnung $\boldsymbol{V} \mapsto \boldsymbol{V}'$, $a \mapsto a'$ ist ein kontravarianter Funktor der Kategorie der Vektorräume über dem Körper K in sich.* □

Wir wollen nun wieder voraussetzen, daß die betrachteten Vektorräume $\boldsymbol{V} = \boldsymbol{V}^n$, $\boldsymbol{W} = \boldsymbol{W}^m$ endlichdimensional sind. Dann können wir Satz 4 durch die folgende Aussage vervollständigen:

Satz 5. *Es seien $\boldsymbol{V}^n$, $\boldsymbol{W}^m$ endlichdimensionale Vektorräume über K. Dann ist die Zuordnung*

$$\theta\colon a \in \boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{W}^m) \mapsto a' \in \boldsymbol{L}(\boldsymbol{W}', \boldsymbol{V}') \tag{34}$$

ein kanonischer Isomorphismus der Vektorräume.

Beweis. Wegen (30), (31) ist θ eine lineare Abbildung. Nach $\dim \boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{W}^m) = \dim \boldsymbol{L}(\boldsymbol{W}', \boldsymbol{V}') = nm$ genügt es, $\operatorname{Ker} \theta = \{\mathfrak{o}\}$ zu zeigen (vgl. Folgerung 2.8). Aus $\theta(a) = a' = o$ folgt $(a'\mathfrak{v} \mid \mathfrak{x}) = (\mathfrak{v} \mid a\mathfrak{x}) = 0$ für alle $\mathfrak{v} \in \boldsymbol{W}'$ und alle $\mathfrak{x} \in \boldsymbol{V}$. Wenn $(\mathfrak{v} \mid \mathfrak{z}) = 0$ gilt für alle $\mathfrak{v} \in \boldsymbol{W}'$, muß $\mathfrak{z} = \mathfrak{o}$ sein; das folgt z. B. aus (3), wenn man für $\mathfrak{v}$ die Vektoren einer dualen Basis einsetzt. Somit gilt $a(\mathfrak{x}) = \mathfrak{o}$ für alle $\mathfrak{x} \in \boldsymbol{V}$, d. h., a ist die Nullabbildung. □

Satz 6. *Unter den Voraussetzungen von Satz 5 gilt:*

a) *Ist a injektiv, so ist a' surjektiv.*

b) $(a')' = a$. (35)

Beweis. Zum Beweis von a) setzen wir $\boldsymbol{W}_0 := \operatorname{Im} a$ und wählen einen komplementären Unterraum $\boldsymbol{W}_1$ so, daß $\boldsymbol{W} = \boldsymbol{W}_0 \oplus \boldsymbol{W}_1$ gilt; das ist nach dem Basisergänzungssatz Folgerung 4.6.1 jedenfalls möglich. Dann ist $a\colon \boldsymbol{V} \to \boldsymbol{W}_0$ ein Isomorphismus. Für $\mathfrak{u} \in \boldsymbol{V}'$ definieren wir $\mathfrak{w} \in \boldsymbol{W}'$ folgendermaßen:

$$(\mathfrak{w} \mid \mathfrak{z}) := (\mathfrak{u} \mid a^{-1} \operatorname{pr}_0 \mathfrak{z}) \qquad (\mathfrak{z} \in \boldsymbol{W});$$

dabei ist pr_0 die Projektion $\mathrm{pr}_0\colon \boldsymbol{W} \to \boldsymbol{W}_0$. Offenbar gilt

$$(a'\mathfrak{w} \mid \mathfrak{x}) = (\mathfrak{w} \mid a\mathfrak{x}) = (\mathfrak{u} \mid a^{-1}a(\mathfrak{x})) = (\mathfrak{u} \mid \mathfrak{x})$$

für alle $\mathfrak{x} \in \boldsymbol{V}$; denn wegen $a\mathfrak{x} \in \boldsymbol{W}_0$ folgt $\mathrm{pr}_0(a\mathfrak{x}) = a\mathfrak{x}$. Daher muß $a'\mathfrak{w} = \mathfrak{u}$ sein, und weil $\mathfrak{u}$ beliebig war, ist a' surjektiv.

Nun beweisen wir b). Nach Satz 2 haben wir $(\boldsymbol{V}')' = \boldsymbol{V}$, $(\boldsymbol{W}')' = \boldsymbol{W}$, also $(a')'\colon \boldsymbol{V} \to \boldsymbol{W}$ für $a \in \boldsymbol{L}(\boldsymbol{V}, \boldsymbol{W})$. Weiter gilt für alle $\mathfrak{x} \in \boldsymbol{V}, \mathfrak{w} \in \boldsymbol{W}'$

$$((a')'\,\mathfrak{x} \mid \mathfrak{w}) = (\mathfrak{x} \mid a'\mathfrak{w}) = (a\mathfrak{x} \mid \mathfrak{w})\,.$$

Da dies für alle $\mathfrak{w}$ gilt, folgt wie beim Beweis von Satz 5 $(a')'(\mathfrak{x}) = a(\mathfrak{x})$ für alle $\mathfrak{x} \in \boldsymbol{V}$, also $(a')' = a$. □

Satz 7. *Für $a \in \boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{W}^m)$ sei $(a_{\alpha i}) \in \mathbf{M}_{m,n}(K)$ die Matrix bezüglich der Basen $(\mathfrak{a}_i)$ von $\boldsymbol{V}^n$, $(\mathfrak{b}_\alpha)$ von $\boldsymbol{W}^m$. Dann hat a' bezüglich der entsprechenden dualen Basen $(\mathfrak{u}_i)$ von $\boldsymbol{V}'$ bzw. $(\mathfrak{w}_\alpha)$ von $\boldsymbol{W}'$ die zu $(a_{\alpha i})$ transponierte Matrix $(b_{i\alpha}) = (a_{\alpha i})' \in \mathbf{M}_{m,n}(K)$.*

Beweis. Nach (4.2) machen wir für die Matrix von a' den Ansatz

$$a'(\mathfrak{w}_\alpha) = \sum_i \mathfrak{u}_i b_{i\alpha}, \qquad \alpha = 1, \ldots, m\,. \tag{36}$$

Wenden wir diese Linearform auf $\mathfrak{a}_k$ an, so folgt aus (2)

$$(a'(\mathfrak{w}_\alpha) \mid \mathfrak{a}_k) = \sum_i (\mathfrak{u}_i \mid \mathfrak{a}_k)\, b_{i\alpha} = b_{k\alpha}\,.$$

Andererseits erhalten wir aus der Definition von a' und aus (4.2)

$$(a'(\mathfrak{w}_\alpha) \mid \mathfrak{a}_k) = (\mathfrak{w}_\alpha \mid a(\mathfrak{a}_k)) = \sum_\beta (\mathfrak{w}_\alpha \mid \mathfrak{b}_\beta)\, a_{\beta k} = a_{\alpha k}\,.$$

Somit gilt $b_{k\alpha} = a_{\alpha k}$. □

Folgerung 2. *Für die Transponierte des Produkts zweier Matrizen gilt*

$$((b_{\varkappa\alpha})\,(a_{\alpha i}))' = (a_{\alpha i})'\,(b_{\varkappa\alpha})'. \tag{37}$$

Zum Beweis genügt es, die Matrizen als lineare Abbildungen zu deuten (vgl. (5.11)) und Satz 7 auf (32) anzuwenden. □

Übung 7. Es sei $\boldsymbol{V}^n$ ein endlichdimensionaler Vektorraum, $\boldsymbol{V}'$ sein Dual, $(\mathfrak{a}_i)$ eine Basis von $\boldsymbol{V}^n$, $(\mathfrak{v}_i)$ eine Basis von $\boldsymbol{V}'$. Man beweise die Äquivalenz der folgenden Aussagen: 1. $(\mathfrak{a}_i)$ und $(\mathfrak{v}_i)$ sind zueinander duale Basen. — 2. Sind $\mathfrak{x} = \sum_i \mathfrak{a}_i \xi_i$ und $\mathfrak{u} = \sum_j \mathfrak{v}_j u_j$ die Basisdarstellungen beliebiger Elemente $\mathfrak{x} \in \boldsymbol{V}$ und $\mathfrak{u} \in \boldsymbol{V}'$, so gilt $(\mathfrak{u} \mid \mathfrak{x}) = \sum_i u_i \xi_i$. — 3. Für alle $\mathfrak{x} = \sum_i \mathfrak{a}_i \xi_i \in \boldsymbol{V}$ gilt $\mathfrak{v}_i(\mathfrak{x}) = \xi_i$, $i = 1, \ldots, n$. — 4. Für alle $\mathfrak{u} = \sum_j \mathfrak{v}_j u_j \in \boldsymbol{V}'$ gilt $\mathfrak{u}(\mathfrak{a}_j) = u_j$, $j = 1, \ldots, n$.

Übung 8. Für $a \in \boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{W}^m)$ beweise man

$$\mathrm{Im}\, a' = (\mathrm{Ker}\, a)^\perp. \tag{38}$$

§ 7. Koordinatentransformationen. Invarianten

Häufig ist es bei theoretischen Überlegungen und vor allem bei technischen oder physikalischen Anwendungen notwendig, ein Koordinatensystem der geometrischen Situation so anzupassen, daß die Gleichungen und damit auch die auszuführenden Rechnungen möglichst einfach werden. Man vergleiche hierzu etwa die Beispiele 4.2, 4.5 und die Übungen 4.2, 4.6. In diesem Paragraphen sollen nun die dabei oft nützlichen Koordinatentransformationen, d. h. die Änderungen der Koordinaten beim Übergang zu einem neuen Koordinatensystem, systematisch untersucht werden.

Wir beginnen mit den Vektorkoordinaten. Es sei V^n ein n-dimensionaler Vektorraum über K. Mit $(\mathfrak{a}_i)$ und $(\hat{\mathfrak{a}}_i)$ bezeichnen wir zwei Basen des V^n. Jeder Vektor $\mathfrak{x} \in V^n$ besitzt dann die Basisdarstellungen

$$\mathfrak{x} = \sum_i \mathfrak{a}_i \xi_i = \sum_i \hat{\mathfrak{a}}_i \hat{\xi}_i \,, \tag{1}$$

wobei (ξ_i) bzw. $(\hat{\xi}_i)$ die Vektorkoordinaten von $\mathfrak{x}$ bezüglich $(\mathfrak{a}_i)$ bzw. $(\hat{\mathfrak{a}}_i)$ sind. Wir fragen, wie sich die „neuen" Koordinaten $\hat{\xi}_i$ durch die alten ξ_i ausdrücken. Dazu stellen wir die alten Basisvektoren $\mathfrak{a}_i$ in der neuen Basis dar:

$$\mathfrak{a}_i = \sum_j \hat{\mathfrak{a}}_j \alpha_{ji} \,, \tag{2}$$

Dadurch ist die Matrix $(\alpha_{ji}) \in \mathbf{M}_n(K)$ eindeutig bestimmt; sie heißt die *Matrix der Koordinatentransformation*. Da die $(\mathfrak{a}_i)$ linear unabhängig sind, folgt (vgl. Satz 4.7.4)

$$\det(\alpha_{ji}) \neq 0, \quad \text{d. h.} \quad (\alpha_{ji}) \in \mathbf{GL}(n, K) \,. \tag{3}$$

Setzt man nun (2) in (1) ein, so folgt aus

$$\mathfrak{x} = \sum_j \hat{\mathfrak{a}}_j \sum_i \alpha_{ji} \xi_i = \sum_j \hat{\mathfrak{a}}_j \hat{\xi}_j \tag{4}$$

durch Koeffizientenvergleich wegen der Eindeutigkeit der Basisdarstellung

$$\hat{\xi}_j = \sum_{i=1}^{n} \alpha_{ji} \xi_i, \qquad j = 1, \ldots, n \,. \tag{5}$$

Wir wollen wieder zur Matrixschreibweise übergehen und betrachten die Spaltenvektoren $(\hat{\xi}_i)$, (ξ_i) sowie die Basisspalten $(\hat{\mathfrak{a}}_i)$, $(\mathfrak{a}_i)$, vgl. Beispiel 4.11. Dann ist (5) äquivalent zu

$$(\hat{\xi}_j) = (\alpha_{ji})\,(\xi_i) \,, \tag{6}$$

und (2) ist mit den Basiszeilen $(\mathfrak{a}_i)'$ zu schreiben:

$$(\mathfrak{a}_i)' = (\hat{\mathfrak{a}}_j)'\,(\alpha_{ji}) \,. \tag{7}$$

Gehen wir auch hier zu den Basisspalten über, so folgt

$$(\mathfrak{a}_i) = (\alpha_{ji})'\,(\hat{\mathfrak{a}}_j) \,. \tag{8}$$

Wollen wir nun noch die neue Basis auf die linke Seite bringen und durch die alte ausdrücken, so müssen wir mit $(\alpha_{ji})'^{-1}$ von links multiplizieren. Zuerst definieren wir

Definition 1. Für $(\alpha_{ij}) \in \mathbf{GL}(n, K)$ sei

$$(\alpha_{ij})^* := (\alpha_{ij})'^{-1}; \tag{9}$$

$(\alpha_{ij})^*$ heißt die zu (α_{ij}) *kontragrediente* Matrix.

Diese Definition ist wegen $\det(\alpha_{ij})' = \det(\alpha_{ij}) \neq 0$ offenbar sinnvoll. Damit gilt

$$(\hat{\mathfrak{a}}_j) = (\alpha_{ji})^* (\mathfrak{a}_i) , \tag{10}$$

und der Vergleich von (6) und (10) gibt uns die folgende Merkregel:

Die Basisvektoren transformieren sich kontragredient zu den Vektorkoordinaten.

Wir gehen nun zum dualen Raum V' über und betrachten die zu $(\mathfrak{a}_i)$ bzw. $(\hat{\mathfrak{a}}_i)$ dualen Basen $(\mathfrak{u}_j)$ bzw. $(\hat{\mathfrak{u}}_j)$. Aus (6.3) und (5) folgt

$$\hat{\mathfrak{u}}_j(\mathfrak{x}) = \xi_j = \sum_{i=1}^{n} \alpha_{ji} \xi_i = \sum_{i=1}^{n} \alpha_{ji} \mathfrak{u}_i(\mathfrak{x}) . \tag{11}$$

Da (11) für alle $\mathfrak{x} \in V$ gilt, erhalten wir

$$\hat{\mathfrak{u}}_j = \sum_{i=1}^{n} \alpha_{ji} \mathfrak{u}_i, \qquad j = 1, \ldots, n , \tag{12}$$

oder in Matrixschreibweise mit $(\hat{\mathfrak{u}}_j)$, $(\mathfrak{u}_i)$ als Spalten:

$$(\hat{\mathfrak{u}}_j) = (\alpha_{ji}) (\mathfrak{u}_i) . \tag{13}$$

Beachten wir nun die leicht zu beweisende Formel (Übung 1)

$$((\alpha_{ji})^*)^* = (\alpha_{ji}) , \tag{14}$$

so erhalten wir nach der oben angegebenen Merkregel, angewandt auf V', für die Transformation der Koordinaten eines beliebigen dualen Vektors $\mathfrak{u} \in V'$,

$$\mathfrak{u} = \sum_i \mathfrak{u}_i u_i = \sum_i \hat{\mathfrak{u}}_i \hat{u}_i , \tag{15}$$

die Beziehung

$$(\hat{u}_j) = (\alpha_{ji})^* (u_i) . \tag{16}$$

Somit gilt

Satz 1. *Bei einer Transformation der Vektorkoordinaten mit der Matrix* $(\alpha_{ji}) \in \mathbf{GL}(n, K)$ *gelten die Formeln* (6), (10), (12), (16); *dabei zieht jede dieser Formeln die anderen nach sich.* □

Übung 1. Man beweise: Die Abbildung

$$(\alpha_{ij}) \in \mathbf{GL}(n, K) \mapsto (\alpha_{ij})^* \in \mathbf{GL}(n, K) \tag{17}$$

ist ein involutiver Automorphismus der Gruppe $\mathbf{GL}(n, K)$, d. h., es gilt (14) und

$$((\alpha_{ij})\,(\beta_{jk}))^* = (\alpha_{ij})^*\,(\beta_{jk})^*. \tag{18}$$

Übung 2. Man beweise für $(\alpha_{ij}) \in \mathbf{GL}(n, K)$

$$((\alpha_{ij})')^{-1} = ((\alpha_{ij})^{-1})'. \tag{19}$$

Beispiel 1. Wir betrachten eine lineare Abbildung $a \in \boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{W}^m)$. Bezüglich der Basen $(\mathfrak{a}_i)$ von $\boldsymbol{V}^n$ und $(\mathfrak{b}_\alpha)$ von $\boldsymbol{W}^m$ habe sie die Koordinatendarstellung (4.41). Analog erhalten wir bezüglich der „neuen" Basen $(\hat{\mathfrak{b}}_\alpha)$ von $\boldsymbol{W}^m$ und $(\hat{\mathfrak{a}}_i)$ von $\boldsymbol{V}^n$ die Koordinatendarstellung derselben Abbildung a in der Gestalt

$$(\hat{\eta}_\alpha) = (\hat{a}_{\alpha i})\,(\hat{\xi}_i)\,. \tag{20}$$

Setzen wir für die Koordinatentransformation in $\boldsymbol{W}^m$

$$(\hat{\eta}_\alpha) = (\beta_{\alpha\gamma})\,(\eta_\gamma) \tag{21}$$

oder invers dazu

$$(\eta_\gamma) = (\beta_{\alpha\gamma})^{-1}\,(\hat{\eta}_\alpha) \tag{22}$$

und setzen das mit der zu (6) inversen Transformation in (4.41) ein, so folgt

$$(\beta_{\alpha\gamma})^{-1}\,(\hat{\eta}_\alpha) = (a_{\gamma j})\,(\alpha_{ji})^{-1}\,(\hat{\xi}_i)\,,$$

und nach Multiplikation mit $(\beta_{\alpha\gamma})$ von links ergibt sich

$$(\hat{\eta}_\alpha) = (\beta_{\alpha\gamma})\,(a_{\gamma j})\,(\alpha_{ji})^{-1}\,(\hat{\xi}_i)\,. \tag{23}$$

Da $(\hat{\xi}_i)$ das Koordinaten-n-Tupel von $\mathfrak{x}$ und $(\hat{\eta}_\alpha)$ das von $a(\mathfrak{x})$ in den jeweils neuen Koordinaten ist, ist auch (23) die Koordinatendarstellung von a in den neuen Koordinaten. Weil nun die Matrix einer linearen Abbildung durch die gewählten Basen eindeutig bestimmt ist (Satz 4.1), folgt durch Vergleich mit (20) das Transformationsgesetz der Matrix einer linearen Abbildung:

$$(\hat{a}_{\alpha i}) = (\beta_{\alpha\gamma})\,(a_{\gamma j})\,(\alpha_{ji})^{-1}. \tag{24}$$

Satz 2. *Die lineare Abbildung $a \in \boldsymbol{L}(\boldsymbol{V}^n)$ habe bezüglich der Basis $(\mathfrak{a}_i)$ die Matrix (a_{ij}) und bezüglich der Basis $(\hat{\mathfrak{a}}_i)$ die Matrix $(\hat{a}_{ij})$. Ist (α_{ij}) die durch (2) bestimmte Matrix der Koordinatentransformation, so gilt*

$$(\hat{a}_{ij}) = (\alpha_{ik})\,(a_{kl})\,(\alpha_{lj})^{-1}. \tag{25}$$

Dabei ist

$$\det(\hat{a}_{ij}) = \det(a_{ij})\,. \tag{26}$$

Definiert man die Spur von $(a_{kl}) \in \mathbf{M}_n(K)$ durch

$$\operatorname{Tr}(a_{kl}) := \sum_{k=1}^{n} a_{kk}\,, \tag{27}$$

so gilt auch

$$\operatorname{Tr}(\hat{a}_{kl}) = \operatorname{Tr}(a_{kl})\,. \tag{28}$$

Beweis. Die Beziehung (25) ist ein Spezialfall der bereits bewiesenen Formel (24). Die Formel (26) ergibt sich sofort aus dem Produktsatz 4.7 und (25). Wir beweisen (28). Nach (25) gilt

$$\sum_{i=1}^{n} \hat{a}_{ii} = \sum_{i,k,l=1}^{n} \alpha_{ik} a_{kl} \bar{\alpha}^{1}_{li} = \sum_{k,l} a_{kl} \sum_{i} \bar{\alpha}^{1}_{li} \alpha_{ik} = \sum_{k,l} a_{kl} \delta_{lk} = \sum_{k} a_{kk} .$$

Dabei haben wir mit $\bar{\alpha}^{1}_{li}$ die Elemente der Matrix $(\alpha_{li})^{-1}$ bezeichnet und die (4.37) entsprechende Beziehung

$$\sum_{i} \bar{\alpha}^{1}_{li} \alpha_{ik} = \sum_{i} \alpha_{li} \bar{\alpha}^{1}_{ik} = \delta_{lk} \tag{29}$$

angewandt. □

Satz 2 berechtigt uns zu der folgenden Definition:

Definition 2. Ist $(a_{ij}) \in \mathbf{M}_n(K)$ die Matrix des linearen Endomorphismus $a \in \boldsymbol{L}(\boldsymbol{V}^n)$, so sei durch

$$N(a) := \det (a_{ij}) , \tag{30}$$

$$\mathrm{Tr}\,(a) := \mathrm{Tr}\,(a_{ij}) \tag{31}$$

die *Norm* $N(a)$ und die *Spur* (englisch „trace") $\mathrm{Tr}(a)$ definiert.

Die Definition 2 ist ein erstes Beispiel für das allgemeine Verfahren, durch Untersuchung der Koordinatentransformationen von den Koordinaten unabhängige, dem geometrischen Objekt selbst zukommende Größen oder Eigenschaften zu gewinnen. Die Koordinaten geben ja nur die relative Beziehung zu dem gerade zufällig betrachteten Koordinatensystem an; geometrisch bedeutungsvolle Größen dagegen dürfen nicht von dieser zufälligen Wahl der Koordinaten abhängen. Die Norm $N(a)$ findet ihre geometrische Deutung als Dehnungsverhältnis. Aus (4.53) folgt nämlich für ein beliebiges n-Bein $(\mathfrak{b}_i)$:

$$[a(\mathfrak{b}_1), \ldots, a(\mathfrak{b}_n)] = N(a)\,[\mathfrak{b}_1, \ldots, \mathfrak{b}_n] \tag{32}$$

wegen

$$[a(\mathfrak{a}_1), \ldots, a(\mathfrak{a}_n)] = \det (a_{ij})\,[\mathfrak{a}_1, \ldots, \mathfrak{a}_n] .$$

Im Fall $N(a) \neq 0$ ist das Volumen des Bildparallelepipeds um den festen Faktor $N(a)$ gegenüber dem Urbild gedehnt; gilt $N(a) = 0$, so ist der lineare Endomorphismus ausgeartet, d. h. $\mathrm{rg}\,(a) < n$, und die Bilder aller n-dimensionalen Parallelepipede sind ausgeartet, haben also das Volumen 0. Soll also das Volumen jedes Parallelepipeds bei der linearen Abbildung $a \in \boldsymbol{L}(\boldsymbol{V}^n)$ invariant bleiben, so muß $N(a) = 1$ sein, und umgekehrt. Die Menge

$$\boldsymbol{SL}(\boldsymbol{V}^n) := \{a \in \boldsymbol{L}(\boldsymbol{V}^n) \mid N(a) = 1\}$$

ist ein Normalteiler in $\boldsymbol{GL}(\boldsymbol{V}^n)$ (vgl. Übung 3); sie ist isomorph zur Untergruppe $\boldsymbol{SL}(n, K) \subset \boldsymbol{GL}(n, K)$ der invertierbaren Matrizen mit der Determinante 1. Die

Gruppen $\boldsymbol{SL}(\boldsymbol{V}^n)$ und $\boldsymbol{SL}(n, K)$ werden *spezielle lineare Gruppen* genannt. Für die Spur gibt es keine so einfache geometrische Deutung.

Übung 3. Für $a, b \in \boldsymbol{L}(\boldsymbol{V}^n)$, $\alpha \in K$, beweise man

$$N(a \circ b) = N(a) \cdot N(b) , \tag{33}$$

$$N(a\alpha) = N(a)\, \alpha^n . \tag{34}$$

$N \mid \boldsymbol{GL}(\boldsymbol{V}^n)$ ist also ein Homomorphismus von $\boldsymbol{GL}(\boldsymbol{V}^n)$ in K^* mit dem Kern $\boldsymbol{SL}(\boldsymbol{V}^n)$.

Übung 4. Man beweise, daß $\mathrm{Tr} \in \boldsymbol{L}(\boldsymbol{V}^n)'$ gilt. Ferner zeige man für $a, b \in \boldsymbol{L}(\boldsymbol{V}^n)$

$$\mathrm{Tr}(a \circ b) = \mathrm{Tr}(b \circ a) . \tag{35}$$

Wir wollen nun die Transformation der Punktkoordinaten in einem affinen Raum behandeln. Dazu betrachten wir wieder zwei n-Beine $(o; \mathfrak{a}_i)$ und $(\hat{o}; \hat{\mathfrak{a}}_i)$ des $\boldsymbol{A}^n$; (x_i) bzw. $(\hat{x}_i)$ seien die entsprechenden Punktkoordinaten des Punktes $x \in \boldsymbol{A}^n$. Dann gilt

$$\overrightarrow{\hat{o}x} = \sum_i \hat{\mathfrak{a}}_i \hat{x}_i = \overrightarrow{\hat{o}o} + \overrightarrow{ox} = \sum_i \hat{\mathfrak{a}}_i \alpha_i + \sum_i \mathfrak{a}_i x_i .$$

Hierbei sind die (α_i) die Koordinaten des alten Ursprungs o im neuen n-Bein $(\hat{o}; \hat{\mathfrak{a}}_i)$. Wenden wir (2) auf die letzte Summe an, so folgt

$$\sum_j \hat{\mathfrak{a}}_j \hat{x}_j = \sum_j \hat{\mathfrak{a}}_j \left(\alpha_j + \sum_i \alpha_{ji} x_i\right) ,$$

und der Koeffizientenvergleich gibt das Transformationsgesetz der affinen Punktkoordinaten:

$$\hat{x}_j = \alpha_j + \sum_{i=1}^{n} \alpha_{ji} x_i , \qquad \det(\alpha_{ji}) \neq 0 . \tag{36}$$

Gehen wir wieder zur Matrixschreibweise über, so folgt

$$(\hat{x}_j) = (\alpha_j) + (\alpha_{ji})\,(x_i) . \tag{37}$$

Hieraus erhält man leicht die inverse Koordinatentransformation

$$(x_i) = (\alpha_{ij})^{-1}\,((\hat{x}_j) - (\alpha_j)) . \tag{38}$$

Beispiel 2. Wir betrachten eine Hyperebene $\boldsymbol{H}^{n-1} \subset \boldsymbol{A}^n$ in ihrer impliziten Darstellung

$$(\mathfrak{u} \mid \overrightarrow{ox}) = c ,$$

$\mathfrak{u} \in \boldsymbol{V}'$, $\mathfrak{u} \neq \mathfrak{o}$, $c \in K$. Bezüglich des n-Beins $(o; \mathfrak{a}_i)$ habe sie die Gleichung

$$\sum_i u_i x_i = c$$

oder in Matrixform

$$(u_i)'\,(x_i) = c . \tag{39}$$

Dabei gilt (u_i), $(x_i) \in \mathbf{M}_{n,1}(K)$. Setzen wir (38) in (39) ein, so folgt nach einer einfachen Rechnung

$$(u_i)' (\alpha_{ij})^{-1} (\hat{x}_j) = c + (u_i)' (\alpha_{ij})^{-1} (\alpha_j) .$$

Vergleichen wir diese Gleichung mit dem (39) entsprechenden Ausdruck in den neuen Koordinaten $(\hat{u}_i)' (\hat{x}_i) = \hat{c}$, so erhalten wir für die Koeffizienten $\hat{u}_i, \hat{c}$ der Hyperebenengleichung das folgende Transformationsgesetz:

$$(\hat{u}_i) = (\alpha_{ij})^* (u_j), \qquad \hat{c} = c + ((\alpha_{ji})^* (u_i))' (\alpha_j) . \tag{40}$$

Die erste Gleichung reproduziert natürlich das Transformationsgesetz (16) der Koordinaten eines dualen Vektors; die zweite resultiert aus der Translation $\vec{\hat{o}o}$ des Ursprungs. Ist speziell $o = \hat{o}$, so gilt $(\alpha_j) = (0)$ und $\hat{c} = c$.

Beispiel 3. *Koordinatendarstellung einer affinen Abbildung.* Wir betrachten eine affine Abbildung $f \in \mathfrak{A}(\boldsymbol{A}^n, \boldsymbol{B}^m)$. Es sei a die zugehörige lineare Abbildung. In $\boldsymbol{A}^n$ und $\boldsymbol{B}^m$ wählen wir ein n-Bein $(o; \mathfrak{a}_i)$ bzw. ein m-Bein $(p; \mathfrak{b}_\alpha)$ und betrachten die zugehörigen Punktkoordinaten. Nach Satz 1.4 können wir f in der Form

$$y = f(x) = f(o) + a(\vec{ox}) \tag{41}$$

darstellen. Bezeichnen wir mit (y_α) die Koordinaten von y und mit (a_α) die Koordinaten von $f(o)$ bezüglich $(p; \mathfrak{b}_\alpha)$, so folgt aus der Koordinatendarstellung (4.40) bzw. (4.41) der linearen Abbildung a (mit (x_i) statt (ξ_i)) sofort die Koordinatendarstellung der affinen Abbildung:

$$y_\alpha = a_\alpha + \sum_{i=1}^{n} a_{\alpha i} x_i, \qquad \alpha = 1, \ldots, m , \tag{42}$$

oder in Matrixform

$$(y_\alpha) = (a_\alpha) + (a_{\alpha i}) (x_i) . \tag{43}$$

Man erkennt wie in Beispiel 4.10 den engen Zusammenhang von (41) und (43): Die Beziehung (43) entsteht aus (41), indem man einfach gliedweise zu den Koordinaten übergeht. Die Matrizen (a_α), $(a_{\alpha i})$ können wir als *Koordinaten der affinen Abbildung* f betrachten.

Ist speziell $\boldsymbol{A}^n = \boldsymbol{B}^m$, so werden wir in (42), (43) j statt α schreiben und in der Regel $(o; \mathfrak{a}_i) = (p; \mathfrak{b}_j)$ annehmen. Wenn f invertierbar ist — dafür ist nach Folgerung 3.1 und Satz 4.6 die Bedingung $\det(a_{ij}) \neq 0$ notwendig und hinreichend —, können wir aus (43) sofort die Koordinatendarstellung der Umkehrung $x = f^{-1}(y)$ berechnen; es folgt

$$(x_i) = (a_{ij})^{-1} ((y_i) - (a_i)) . \tag{44}$$

Wir überlassen dem Leser die Herleitung des Transformationsgesetzes für die Koordinaten (a_α), $(a_{\alpha i})$ einer affinen Abbildung:

Übung 5. Ist (37) eine Koordinatentransformation im $\boldsymbol{A}^n$ und $(\hat{y}_\alpha) = (\beta_\alpha) + (\beta_{\alpha\gamma}) (y_\gamma)$ eine Koordinatentransformation im $\boldsymbol{B}^m$, so gilt für die Koordinaten $(\hat{a}_\alpha)$, $(\hat{a}_{\alpha i})$ der

affinen Abbildung (41) das Transformationsgesetz (24) und

$$(\hat{a}_\alpha) = (\beta_\alpha) + (\beta_{\alpha\gamma})\,(a_\gamma) - (\beta_{\alpha\gamma})\,(a_{\gamma j})\,(\alpha_{ji})^{-1}\,(\alpha_i)\,. \tag{45}$$

Wir wollen nun eine wichtige Beziehung zwischen Automorphismen und Koordinatentransformationen diskutieren. Vergleicht man die Koordinatendarstellung einer affinen Transformation $f \in \mathfrak{A}(\boldsymbol{A}^n)$,

$$(y_i) = (a_i) + (a_{ij})\,(x_j), \qquad \det(a_{ij}) \neq 0\,, \tag{46}$$

und die affine Koordinatentransformation (37), so erkennt man sofort, daß beide Formeln bis auf einige Bezeichnungen übereinstimmen. Diese formale Übereinstimmung hat folgenden inhaltlichen Hintergrund: Transformieren wir das n-Bein $(o; \mathfrak{a}_i)$ ebenfalls durch f, d. h., setzen wir $(\hat{o}; \hat{\mathfrak{a}}_i) = (f(o); a_f(\mathfrak{a}_i))$, so gilt $(\hat{y}_i) = (x_i)$, d. h., die neuen Koordinaten des Bildpunktes sind gleich den alten des Urbildpunktes: Aus $x = o + \sum_{i=1}^{n} \mathfrak{a}_i x_i$ folgt ja sofort

$$y = f(x) = f(o) + \sum_{i=1}^{n} a_f(\mathfrak{a}_i)\; x_i = \hat{o} + \sum_{i=1}^{n} \hat{\mathfrak{a}}_i x_i\,, \quad .$$

also $x_i = \hat{y}_i$: In dem mitbewegten Koordinatensystem bleiben die Koordinaten des bewegten Punktes konstant. Man spricht in diesem Sinne vom *Mitschleppen des Koordinatensystems*. Zum Beispiel kann man sich vorstellen, daß ein Flugzeug ein starr mit ihm verbundenes Koordinatensystem mitschleppt; alle fest mit dem Flugzeug gekoppelten, sich mitbewegenden Gegenstände haben in ihm konstante Koordinaten. Jedem Automorphismus haben wir auf diese Weise eine Koordinatentransformation zugeordnet; man weist leicht nach, daß diese Zuordnung bijektiv ist. Sind umgekehrt zwei Koordinatensysteme mit den n-Beinen $(o; \mathfrak{a}_i)$ bzw. $(\hat{o}; \hat{\mathfrak{a}}_i)$ gegeben, so wissen wir nach Satz 2.5 und Satz 3.4, daß genau ein affiner Automorphismus f mit $f(o) = \hat{o}$, $a_f(\mathfrak{a}_i) = \hat{\mathfrak{a}}_i$ existiert; er wird wieder durch $(\hat{y}_i) = (x_i)$ beschrieben. Man nennt diese mit Hilfe zweier n-Beine definierte Abbildung auch *Zuordnung durch gleiche Koordinaten*; sie ist in unserem Fall stets ein affiner Automorphismus. Analog sind die Verhältnisse bei den linearen Automorphismen.

Zum Abschluß dieses Paragraphen wollen wir noch den für alle geometrischen Untersuchungen grundlegenden und sehr allgemeinen Begriff einer Invarianten definieren.

Definition 3. Es sei $[G, X]$ eine Transformationsgruppe und $M \neq \emptyset$ eine Menge. Eine Funktion $I: X \to M$ heißt eine *Invariante*, wenn für alle $g \in G$ und $x \in X$

$$I(gx) = I(x) \tag{47}$$

gilt.

Beispiel 4. Wir beginnen ganz unsystematisch mit einem Beispiel aus der Elementargeometrie. Es sei G die Gruppe der euklidischen Bewegungen (einschließlich der Spiegelungen) der Ebene $\boldsymbol{E}$, und $X := \bigtimes_k \boldsymbol{E}$ der Raum der k-Tupel von

Punkten $(p_1, ..., p_k)$, $p_\varkappa \in \boldsymbol{E}$. Die Wirkung von G sei über X durch

$$g(p_1, ..., p_k) := (gp_1, ..., gp_k) \tag{48}$$

definiert. Bezeichnet $\varrho(x, y)$ den Abstand zweier Punkte der Ebene, so sind

$$I_{\alpha\beta}(p_1, ..., p_k) := \varrho(p_\alpha, p_\beta), \qquad 1 \leqq \alpha < \beta \leqq k, \tag{49}$$

offenbar Invarianten. Man kann elementargeometrisch beweisen, daß folgender Satz gilt: Zwei Punktfolgen $(p_1, ..., p_k)$, $(q_1, ..., q_k)$ sind kongruent, d. h., es gibt ein $g \in G$ mit $g(p_1, ..., p_k) = (q_1, ..., q_k)$ genau dann, wenn

$$I_{\alpha\beta}(p_1, ..., p_k) = I_{\alpha\beta}(q_1, ..., q_k) \quad \text{für} \quad 1 \leqq \alpha < \beta \leqq k$$

gilt. Die Invarianten $I_{\alpha\beta}$, also alle Abstände $\varrho(p_\alpha, p_\beta)$, charakterisieren die Punktfolge bis auf die Lage in der Ebene eindeutig.

Definition 4. Es sei $N \neq \emptyset$ eine Indexmenge und $\{I_\varkappa\}_{\varkappa \in N}$ eine Menge von Invarianten von $[G, X]$. Die Menge $\{I_\varkappa\}_{\varkappa \in N}$ heißt ein *vollständiges Invariantensystem von* $[G, X]$, wenn folgendes gilt:

Für $x, y \in X$ ist x G-äquivalent zu y (vgl. Definition (1.4.9)) dann und nur dann, wenn $I_\varkappa(x) = I_\varkappa(y)$ für alle $\varkappa \in N$ gilt.

Beispiel 4 besagt also, daß $\{I_{\alpha\beta}\}_{1 \leqq \alpha < \beta \leqq k}$ ein vollständiges Invariantensystem ist. Zum Beispiel ist ein Dreieck durch seine Seitenlängen bis auf Kongruenz eindeutig bestimmt. Es ist eine Grundaufgabe der Geometrie, geometrische Figuren oder Objekte durch vollständige Invariantensysteme zu charakterisieren.

Beispiel 5. Es sei G transitiv über X. Dann gibt es nur die trivialen Invarianten $I(x) = \text{konstant}$.

Beispiel 6. Es sei $X = \boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{W}^m)$, $G = \boldsymbol{GL}(\boldsymbol{V}^n) \times \boldsymbol{GL}(\boldsymbol{W}^m)$, und die Wirkung von G über X sei definiert durch

$$(g_1, g_2) \cdot a := g_2 \circ a \circ g_1^{-1}. \tag{50}$$

Dann ist bereits die Invariante $r = \operatorname{rg} a$ allein ein vollständiges Invariantensystem. Das folgt aus Lemma 2.1. Es sei $\operatorname{rg} a = \operatorname{rg} b = r$. Nach dem Lemma finden wir Basen $(\mathfrak{a}_i)$, $(\mathfrak{b}_\alpha)$ bzw. $(\hat{\mathfrak{a}}_i)$, $(\hat{\mathfrak{b}}_\alpha)$ so, daß a bzw. b bezüglich dieser Basen die Normalform (4.5) hat. Es sei g_1 der lineare Automorphismus von $\boldsymbol{V}^n$, der $(\mathfrak{a}_i)$ in $(\hat{\mathfrak{a}}_i)$ überführt, und g_2 der lineare Automorphismus von $\boldsymbol{W}^m$, der $(\mathfrak{b}_\alpha)$ in $(\hat{\mathfrak{b}}_\alpha)$ überführt. Dann gilt für $g = (g_1, g_2)$

$$g \cdot a = g_2 \circ a \circ g_1^{-1} = b,$$

wie man unmittelbar durch Anwenden dieser linearen Abbildungen auf die Basis $(\hat{\mathfrak{a}}_i)$ erkennt.

Beispiel 7. Aus Satz 4.9 folgt speziell, daß das Volumenverhältnis zweier parallel liegender, nicht ausgearteter, k-dimensionaler Parallelepipede eine Invariante bei affinen Transformationen des $\boldsymbol{A}^n$ $(1 \leqq k \leqq n)$ ist, kurz eine affine Invariante. Man

bemerkt, daß wir den Raum X der Transformationsgruppe nicht angegeben und die Invariante daher auch nicht streng definiert haben, auch die Wirkung von $\mathfrak{A}(\boldsymbol{A}^n)$ über X wurde nicht beschrieben. Es ist aber klar, wie das zu erledigen ist: X ist die Menge aller Paare (Π_1^k, Π_2^k) nicht ausgearteter, k-dimensionaler Parallelepipede des $\boldsymbol{A}^n$. Die Wirkung der affinen Gruppe $\mathfrak{A}(\boldsymbol{A}^n)$ wird durch die über $\boldsymbol{A}^n$ auf X definiert:

$$g(\Pi_1^k, \Pi_2^k) := (g\Pi_1^k, g\Pi_2^k) .$$

Die Invariante I wird folgendermaßen definiert: $I(\Pi_1^k, \Pi_2^k) := v(\Pi_1^k)/v(\Pi_2^k)$, wenn Π_1^k, Π_2^k in parallelen k-Ebenen liegen, und $I(\Pi_1^k, \Pi_2^k) = 0$ sonst. Man beweist leicht, daß I eine Invariante ist.

Häufig haben wir in der Geometrie die in der folgenden Definition beschriebene Situation.

Definition 5. Es sei $[G, X]$ eine Transformationsgruppe und M eine Menge. Eine Menge Φ von Abbildungen $\varphi: X \to M$ heißt ein $[G, X]$ *angepaßter Atlas* mit Werten in M, und die Elemente $\varphi \in \Phi$ heißen die *Karten* oder die *Koordinatensysteme* des Atlasses, wenn folgende Eigenschaften erfüllt sind:

1. Jedes $\varphi \in \Phi$ ist eine bijektive Abbildung $\varphi: X \to M$.
2. Sind $\varphi_1, \varphi_2 \in \Phi$, so gibt es genau ein $g \in G$ mit
$$\varphi_2 = \varphi_1 \circ g . \tag{51}$$
3. Für $\varphi \in \Phi$ und $g \in G$ gilt auch $\varphi \circ g \in \Phi$.

Offenbar bilden die Vektorkoordinatensysteme eines Vektorraumes $\boldsymbol{V}^n$ einen $[\boldsymbol{GL}(\boldsymbol{V}^n), \boldsymbol{V}^n]$ angepaßten Atlas mit Werten in $M = K^n$, die Punktkoordinatensysteme eines affinen Raumes $\boldsymbol{A}^n$ einen $[\mathfrak{A}(\boldsymbol{A}^n), \boldsymbol{A}^n]$ angepaßten Atlas mit Werten in K^n; Beispiel 4.4 beschreibt einen $\boldsymbol{L}(\boldsymbol{V}^n)$ angepaßten Atlas mit Werten in $\mathbf{M}_n(K)$ usw.

Übung 6. Es sei Φ ein $[G, X]$ angepaßter Atlas mit Werten in M. Man beweise: a) Zu jedem $\varphi_0 \in \Phi$, φ_0 fest, definiert $g \in G \mapsto \varphi := \varphi_0 \circ g \in \Phi$ eine bijektive Abbildung von G auf Φ. — b) Durch
$$(g, m) \in G \times M \mapsto g \cdot m := \varphi_0(g\varphi_0^{-1}(m)) \tag{52}$$
wird eine Wirkung von G über M definiert, für die $[G, M]$ eine zu $[G, X]$ isomorphe Transformationsgruppe wird. — c) Ist $f: M \to H$ eine Funktion auf M mit Werten in einer Menge H, die folgende Eigenschaft besitzt: Für alle $x \in X$ gilt $f(\varphi_1(x)) = f(\varphi_2(x))$ für alle $\varphi_1, \varphi_2 \in \Phi$, so wird durch $I(x) := f(\varphi(x))$ für $x \in X$ und beliebiges $\varphi \in \Phi$ eine Invariante von $[G, X]$ definiert. (Nach diesem Schema ist zum Beispiel Definition 2 gebildet.)

Unter der *Klassifikation* der Elemente des Raumes X einer Transformationsgruppe $[G, X]$ versteht man die Aufzählung aller Orbits durch die Angabe eines vollständigen Invariantensystems. Häufig geht man dabei so vor, daß man aus jedem Orbit einen eindeutig bestimmten Repräsentanten als sogenannte *Normalform* auszeichnet. Dazu wird oft ein angepaßter Atlas benutzt. Es sei $\varphi_0 \in \Phi$ eine beliebige, fest gewählte Karte. Dann bilden die Mengen $\{\varphi_0(Gx)\}_{x \in X}$ eine Klassen-

einteilung von M; durch φ_0 wird ja die Einteilung von X in Orbits nach Satz 1.4.4 übertragen; die Klasseneinteilung von M ist übrigens durch die in Übung 6 definierte Wirkung von G über M erzeugt. In jeder Klasse $\varphi_0(Gx)$ wählen wir einen Repräsentanten, den wir eine *Normalform* nennen. Es sei $M_0 \subseteq M$ die Normalformenmenge; offenbar bestimmt die kanonische Abbildung $\pi\colon M \to M/\sim$ durch $\pi \mid M_0\colon M_0 \to M/\sim$ eine Bijektion. Es gilt nun der folgende Satz:

Satz 3. *Es sei $[G, X]$ eine Transformationsgruppe, Φ ein angepaßter Atlas mit Werten in M, $M_0 \subseteq M$ eine Normalformenmenge. Dann gilt für $x, y \in X$:*

$$x \sim_G y \Leftrightarrow \text{es existieren Koordinatensysteme } \varphi_1, \varphi_2 \in \Phi \text{ derart,}$$

$$\text{daß } \varphi_1(x) = \varphi_2(y) \in M_0 \text{ gilt.}$$

Beweis. Es sei $x \sim_G y$. Dann existiert ein $\varphi_1 \in \Phi$ mit $\varphi_1(x) \in M_0$. Weiter sei $g \in G$ so gewählt, daß $g(x) = y$ gilt. Dann ist $\varphi_2 = \varphi_1 \circ g^{-1} \in \Phi$, und wir haben $\varphi_2(y) = \varphi_1(g^{-1}y) = \varphi_1(x) \in M_0$. Umgekehrt, ist $\varphi_1(x) = \varphi_2(y) \in M_0$, so wählen wir ein g mit $\varphi_2 = \varphi_1 \circ g$. Es folgt $\varphi_1(x) = \varphi_1(gy)$. Da φ_1 bijektiv ist, erhalten wir $x = gy$, also $x \sim_G y$. □

Folgerung 1. *Unter den Voraussetzungen von Satz 3 gilt: Die Abbildung*

$$x \in X \mapsto \mathbf{N}(x) := \text{Normalform von } \varphi(x) = (\pi \mid M_0)^{-1} \circ \pi \circ \varphi(x) \in M_0$$

ist unabhängig von der Wahl der Karte $\varphi \in \Phi$; sie ist eine Invariante von $[G, X]$, die bereits allein ein vollständiges Invariantensystem bildet.

Beweis. Nach Satz 3 haben G-äquivalente Punkte $x, y \in X$ dieselbe Normalform, d. h., $\mathbf{N}(x)$ ist eine Invariante. Weil in jedem G-Orbit von M genau eine Normalform $m \in M_0$ liegt, ist x durch Angabe der Normalform bis auf G-Äquivalenz eindeutig bestimmt. □

Bisher haben wir nur für Beispiel 6 die Klassifizierung über die Normalform durchgeführt. Die Menge M ist hier die Menge der Matrizen $\mathbf{M}_{m,n}(K)$, und M_0 ist die Menge der Matrizen der Form (4.5) für $0 \leqq r \leqq \min(m, n)$. Es gibt also nur endlich viele Äquivalenzklassen linearer Abbildungen von $\boldsymbol{V}^n$ in $\boldsymbol{W}^m$, die durch ihren Rang klassifiziert werden. Die Verfahren zur Rangbestimmung aus § 5 gestatten es, zu jeder gegebenen linearen Abbildung die Normalform zu bestimmen. Im allgemeinen Fall läuft das Klassifikationsproblem also auf zwei Teilaufgaben hinaus:

1. Aufgabe: *Auffinden eines vollständigen Invariantensystems oder einer Normalformenmenge.*

2. Aufgabe: *Angabe von Algorithmen zur Berechnung der Invarianten des gewählten Systems bzw. zur Bestimmung der Normalform.*

Für viele Transformationsgruppen sind diese Probleme sehr kompliziert. Wir werden in den folgenden Paragraphen einige derartige Klassifikationen durchführen.

§ 8. Die Jordansche Normalform linearer Endomorphismen

Wir betrachten in diesem Paragraphen die Endomorphismenalgebra $\boldsymbol{L} := \boldsymbol{L}(\boldsymbol{V}^n)$ eines n-dimensionalen Vektorraumes $\boldsymbol{V}$. Über ihr wirkt die Gruppe $\boldsymbol{G} := \boldsymbol{GL}(\boldsymbol{V}^n)$ folgendermaßen:

$$(g, a) \in \boldsymbol{G} \times \boldsymbol{L} \mapsto \alpha_g(a) := g \circ a \circ g^{-1} \in \boldsymbol{L} . \tag{1}$$

Zwei Endomorphismen a und b, die $\boldsymbol{G}$-äquivalent im Sinne dieser Wirkung sind, heißen *ähnlich*. Es gilt also, die Endomorphismen im Sinne von § 7 zu klassifizieren. Für den Fall $K = \mathbf{C}$ gelingt das durch die Bestimmung der Jordanschen Normalform.

Nach Satz 4.1 und Beispiel 4.4 läuft unsere Aufgabe etwas vage ausgedrückt darauf hinaus, zu jedem $a \in \boldsymbol{L}$ eine Basis $(\mathfrak{a}_i)$ von $\boldsymbol{V}^n$ so zu finden, daß die Matrix von a in dieser Basis „möglichst einfach" wird. Gehen wir nämlich von (1) zu den Matrizen (a_{ij}) von a und (α_{ik}) von g über, so resultiert das Transformationsgesetz (7.25). Aus den „möglichst einfachen" Matrizen ist dann die Normalformenmenge zu bilden. Will man das Schema aus § 7 anwenden, so ist $M := \mathbf{M}_n(K)$, und der angepaßte Atlas Φ ist die Menge der durch die Basen von $\boldsymbol{V}^n$ bestimmten Abbildungen $\boldsymbol{L} \to M$ nach Satz 4.1. Die Transformationsgruppe $[\boldsymbol{G}, \boldsymbol{L}]$ ist isomorph zu $[\mathbf{GL}(n, K), \mathbf{M}_n(K)]$ mit der Wirkung (7.25) (vgl. Übung 7.6, b)), und wir haben eine Normalformenmenge $M_0 \subseteq \mathbf{M}_n(K)$ geeignet zu finden. Im ersten Teil des Paragraphen werden wir die wichtigsten Invarianten der linearen Endomorphismen bestimmen und anschließend die Jordansche Normalform herleiten. Zuerst erinnern wir an die Definition 2.4 der Eigenwerte und Eigenvektoren: Ein Element $\lambda \in K$ ist *Eigenwert* des Endomorphismus $a \in \boldsymbol{L}$, wenn ein $\mathfrak{e} \in \boldsymbol{V}$, $\mathfrak{e} \neq \mathfrak{o}$, existiert mit $a\mathfrak{e} = \mathfrak{e}\lambda$; der Vektor $\mathfrak{e}$ ist dann ein *Eigenvektor* von a zum Eigenwert λ. Nach Übung 2.2 und Beispiel 4.6 sind die Eigenunterräume

$$\boldsymbol{U}_\lambda := \{\mathfrak{x} \in \boldsymbol{V} \mid a\mathfrak{x} = \mathfrak{x}\lambda\} \tag{2}$$

bei a invariante Unterräume von $\boldsymbol{V}$. Man beweist leicht:

Lemma 1. *Ist λ Eigenwert von $a \in \boldsymbol{L}$, so ist λ auch Eigenwert von $\alpha_g(a) = g \circ a \circ g^{-1}$ für beliebige $g \in G$.*

Beweis. Der Vektor $g\mathfrak{e}$ ist ungleich $\mathfrak{o}$, da g ein Automorphismus ist, und es gilt $\alpha_g(a)\, g\mathfrak{e} = gag^{-1}g\mathfrak{e} = ga\mathfrak{e} = g\mathfrak{e}\lambda$. □

Die Eigenwerte sind also mit den Endomorphismen invariant verknüpft. Wie wir wissen, brauchen jedoch Eigenwerte nicht zu existieren (vgl. Übung 2.4). Um das Problem der Existenz der Eigenwerte zu untersuchen, setzen wir $e := \mathrm{id}_{\boldsymbol{V}}$ und bemerken, daß $a\mathfrak{e} = \mathfrak{e}\lambda$ zu

$$(a - e\lambda)\,\mathfrak{e} = \mathfrak{o} \tag{3}$$

äquivalent ist. Somit ist λ Eigenwert von a genau dann, wenn

$$\mathrm{Ker}\,(a - e\lambda) \neq \{\mathfrak{o}\} \tag{4}$$

gilt; und das ist genau dann der Fall, wenn $a-e\lambda$ kein Automorphismus ist (vgl. Folgerung 2.8), also wenn

$$\det(a-e\lambda)=0 \tag{5}$$

gilt. Wir nennen

$$\chi_a(x):=\det(a-ex) \tag{6}$$

das *charakteristische Polynom von* a und zeigen

Satz 1. *Für jedes* $a\in\boldsymbol{L}=\boldsymbol{L}(V^n)$ *ist* $\chi_a(x)\in K[x]$ *ein Polynom n-ten Grades; es hat die Gestalt*

$$\chi_a(x)=(-1)^n\,(x^n-d_1x^{n-1}+d_2x^{n-2}-\ldots+(-1)^n\,d_n) \tag{7}$$

mit

$$d_1=\operatorname{Tr}a \quad \textit{und} \quad d_n=N(a)\,. \tag{8}$$

$\chi_a(x)$ *ist eine Invariante des Endomorphismus.* λ *ist Eigenwert genau dann, wenn* $\chi_a(\lambda)=0$ *gilt.*

Beweis. Aus der Definition der Determinante folgt

$$d_k=\sum_{1\leqq i_1<\ldots<i_k\leqq n} M\binom{i_1\ldots i_k}{i_1\ldots i_k}, \qquad k=1,\ldots,n; \tag{9}$$

denn wir müssen alle Faktoren von $(-1)^{n-k}x^{n-k}$ in der Determinante sammeln. Die in (9) vorkommenden Minoren heißen die *Hauptminoren der Ordnung* k; sie liegen symmetrisch zur Hauptdiagonalen (vgl. (4.8.8)). Für das höchste Glied erhalten wir $(-1)^nx^n$ aus dem Produkt der Elemente der Hauptdiagonale; $d_1\equiv\sum_{i=1}^{n}a_{ii}$ ist die Summe der Hauptminoren erster Ordnung, und das letzte Glied d_n ergibt sich aus $d_n=\chi_a(0)=\det a$. Die Behauptung über die Invarianz folgt durch eine einfache Rechnung aus dem Produktsatz 4.7: $gag^{-1}-ex=g\,(a-ex)\,g^{-1}$, also durch Übergang zur Determinante:

$$\chi_a(x)=\chi_{a(g)a}(x)\,. \tag{10}$$

Der Produktsatz wurde für Matrizen mit Elementen aus einem Körper bewiesen; er ist daher auch hier anwendbar, weil die Elemente der Matrix von $a-ex$ im Polynomring $K[x]$ liegen, der in seinem Quotientenkörper $K(x)$ enthalten ist. Andererseits gilt der Produktsatz auch unter allgemeineren Voraussetzungen, vgl. Übung 4.14. Die letzte Behauptung folgt unmittelbar aus (5). □

Die Existenz der Eigenwerte ist gesichert, wenn K ein Zerfällungskörper von $\chi_a(x)$ ist. Die Jordansche Normalform bezieht sich gerade auf diesen Fall.

Definition 1. Ein Endomorphismus $a\in\boldsymbol{L}$ heißt *aufspaltend*, wenn K ein Zerfällungskörper von $\chi_a(x)$ ist, d. h., wenn

$$\chi_a(x)=\prod_{i=1}^{n}(\lambda_i-x) \tag{11}$$

gilt, $\lambda_i\in K$ die (nicht notwendig verschiedenen) Eigenwerte von a.

Wir betrachten nun zuerst einen Spezialfall, nämlich einen nilpotenten Endomorphismus:

Definition 2. Ein $b \in \boldsymbol{L}(\boldsymbol{V}^n)$ heißt *nilpotent*, wenn ein $k \in \mathbf{N}$ existiert mit $b^k = 0$.

Übung 1. Man beweise, daß jeder Endomorphismus b, der bei geeigneter Basis eine Matrix der Form

$$(b_{ij}) = \begin{pmatrix} 0 & & & \\ \varepsilon_1 & 0 & & \mathbf{0} \\ & \varepsilon_2 & \ddots & \\ & & \ddots & 0 \\ \mathbf{0} & & & \varepsilon_{n-1}\ 0 \end{pmatrix} \quad \text{mit} \quad \varepsilon_i = 0 \quad \text{oder} \quad \varepsilon_i = 1 \tag{12}$$

besitzt, nilpotent ist. Allgemeiner: Jede untere (oder obere) Dreiecksmatrix mit lauter Nullen auf der Hauptdiagonale ist nilpotent.

Wir werden beweisen, daß umgekehrt jeder nilpotente Endomorphismus bei geeigneter Basis eine Matrix der Form (12) besitzt; (12) ist im wesentlichen die Jordansche Normalform eines nilpotenten Endomorphismus. Die Jordansche Normalform eines beliebigen aufspaltenden $a \in \boldsymbol{L}$ läßt sich auf die nilpotenten Endomorphismen zurückführen. Zunächst wollen wir zeigen, daß jeder Endomorphismus in einen nilpotenten und einen bijektiven Bestandteil zerlegt werden kann.

Definition 3. Es sei $a \in \boldsymbol{L}(\boldsymbol{V}^n)$. Wir sagen, *$a$ spaltet in die Endomorphismen $a_1, \ldots, a_m$ auf*, wenn es eine direkte Zerlegung

$$\boldsymbol{V}^n = \boldsymbol{M}_1 \oplus \ldots \oplus \boldsymbol{M}_m \tag{13}$$

in bei a invariante Unterräume $\boldsymbol{M}_\mu$, $a\boldsymbol{M}_\mu \subseteq \boldsymbol{M}_\mu$, gibt (vgl. Definition 4.3), wobei

$$a_\mu \mid \boldsymbol{M}_\nu = \begin{cases} a \mid \boldsymbol{M}_\mu & \text{für} \quad \mu = \nu\,, \\ 0 & \text{für} \quad \mu \neq \nu;\ \mu, \nu = 1, \ldots, m\,, \end{cases} \tag{14}$$

gilt. In diesem Fall schreiben wir

$$a = a_1 \oplus \ldots \oplus a_m\,. \tag{15}$$

Offenbar spaltet jeder Endomorphismus a, der eine Darstellung (13) von $\boldsymbol{V}^n$ als direkte Summe invariant läßt, in die durch (14) definierten Summanden auf; ein a_μ heißt *bijektiv*, wenn $a_\mu \mid \boldsymbol{M}_\mu$ bijektiv ist.

Satz 2. *Jeder Endomorphismus $a \in \boldsymbol{L}(\boldsymbol{V}^n)$ spaltet in einen nilpotenten Bestandteil a_0 und einen bijektiven Bestandteil a_1 auf: $a = a_0 \oplus a_1$. Diese Bestandteile sind eindeutig bestimmt.*

Beweis. Wir zeigen zuerst die Existenz der Aufspaltung. Dazu definieren wir

$$\boldsymbol{U}_i := \operatorname{Ker} a^i, \tag{16}$$

$$\boldsymbol{W}_i := \operatorname{Im} a^i, \qquad i = 0, 1, \ldots \tag{17}$$

Dann gilt

Lemma 2. *Es gibt eine Zahl* $k \in \mathbf{N}_0$, *so daß*

$$\boldsymbol{U}_0 = \{\mathfrak{o}\} \subset \boldsymbol{U}_1 \subset \ldots \subset \boldsymbol{U}_k = \boldsymbol{U}_l \quad \textit{für} \quad l > k \tag{18}$$

gilt. Ferner sind die $\boldsymbol{U}_i$ *bei a invariant; es gilt sogar*

$$a\boldsymbol{U}_i \subset \boldsymbol{U}_{i-1}\,. \tag{19}$$

Beweis. Für $\mathfrak{x} \in \boldsymbol{U}_i$ gilt $a^i\mathfrak{x} = \mathfrak{o}$, also auch $a^{i+1}\mathfrak{x} = \mathfrak{o}$, und somit $\boldsymbol{U}_i \subset \boldsymbol{U}_{i+1}$. Es sei k die kleinste natürliche Zahl mit $\boldsymbol{U}_k = \boldsymbol{U}_{k+1}$, dieser Fall muß ja wegen $\dim \boldsymbol{V}^n = n < \infty$ einmal eintreten. Wir zeigen durch Induktion nach s, daß dann $\boldsymbol{U}_{k+s} = \boldsymbol{U}_k$ für alle $s \geqq 1$ gilt. Angenommen, es sei schon $\boldsymbol{U}_l = \boldsymbol{U}_k$ für ein $l > k$ gezeigt, und es sei $\mathfrak{x} \in \boldsymbol{U}_{l+1}$. Dann gilt $a^{l+1}\mathfrak{x} = \mathfrak{o}$, also $a\mathfrak{x} \in \boldsymbol{U}_l = \boldsymbol{U}_k$, und daher $a^{k+1}\mathfrak{x} = \mathfrak{o}$. Somit ist $\mathfrak{x} \in \boldsymbol{U}_{k+1} = \boldsymbol{U}_k$. Zum Beweis von (19) sei $\mathfrak{x} \in \boldsymbol{U}_i$. Dann ist $a^i\mathfrak{x} = a^{i-1}(a\mathfrak{x}) = \mathfrak{o}$, also $a\mathfrak{x} \in \boldsymbol{U}_{i-1}$. Aus (18) und (19) folgt die Behauptung über die Invarianz. □

Lemma 3. *Es gilt für die Zahl* k *von Lemma* 2

$$\boldsymbol{W}_0 = \boldsymbol{V}^n \supset \boldsymbol{W}_1 \supset \ldots \supset \boldsymbol{W}_k = \boldsymbol{W}_l \quad \textit{für} \quad l > k\,. \tag{20}$$

Ferner sind die $\boldsymbol{W}_i$ *bei a invariant, es gilt sogar*

$$a\boldsymbol{W}_i = \boldsymbol{W}_{i+1}\,. \tag{21}$$

Beweis. Gilt $\mathfrak{x} \in \boldsymbol{W}_i$, so existiert ein $\mathfrak{y} \in \boldsymbol{V}$ mit $\mathfrak{x} = a^i\mathfrak{y} = a^{i-1}(a\mathfrak{y})$, also ist auch $\mathfrak{x} \in \boldsymbol{W}_{i-1}$. Offenbar muß die Folge einmal abbrechen. Nach Folgerung 2.7 haben wir für alle i

$$\dim \boldsymbol{U}_i + \dim \boldsymbol{W}_i = n\,. \tag{22}$$

Somit muß sie genau an der Stelle k abbrechen. Ist $\mathfrak{x} \in \boldsymbol{W}_i$, so gilt $\mathfrak{x} = a^i\mathfrak{y}$, also $a\mathfrak{x} = a^{i+1}\mathfrak{y}$, und daher $a\boldsymbol{W}_i \subseteq \boldsymbol{W}_{i+1}$. Ist umgekehrt $\mathfrak{x} \in \boldsymbol{W}_{i+1}$, so folgt $\mathfrak{x} = a^{i+1}(\mathfrak{y}) = a(a^i\mathfrak{y})$ und $a^i\mathfrak{y} \in \boldsymbol{W}_i$. □

Wir beweisen nun Satz 2. Zunächst folgt aus (21) und (20)

$$a\boldsymbol{W}_k = \boldsymbol{W}_{k+1} = \boldsymbol{W}_k\,.$$

Daher ist $a \mid \boldsymbol{W}_k$ surjektiv und somit bijektiv (vgl. Folgerung 2.8). Weiter ist $a \mid \boldsymbol{U}_k$ nilpotent; denn offenbar gilt $a^k \mid \boldsymbol{U}_k = (a \mid \boldsymbol{U}_k)^k = o$. Es bleibt

$$\boldsymbol{V}^n = \boldsymbol{U}_k \oplus \boldsymbol{W}_k \tag{23}$$

zu zeigen. Wegen (22) und der Dimensionsformel (4.6.8) genügt es, $\boldsymbol{U}_k \cap \boldsymbol{W}_k = \{\mathfrak{o}\}$ zu beweisen. Es sei $\mathfrak{x} \in \boldsymbol{U}_k \cap \boldsymbol{W}_k$. Wegen $\mathfrak{x} \in \boldsymbol{U}_k = \operatorname{Ker} a^k$ gilt $a^k\mathfrak{x} = \mathfrak{o}$, und weil $a^k \mid \boldsymbol{W}_k = (a \mid \boldsymbol{W}_k)^k$ bijektiv ist, muß wegen $\mathfrak{x} \in \boldsymbol{W}_k$ auch $\mathfrak{x} = \mathfrak{o}$ sein. Die Einschränkungen von a auf $\boldsymbol{U}_k$ und $\boldsymbol{W}_k$ bestimmen die Aufspaltung $a = a_0 \oplus a_1$ mit den geforderten Eigenschaften.

Es bleibt die Eindeutigkeit zu beweisen. Dazu sei $a = \tilde{a}_0 \oplus \tilde{a}_1$ ebenfalls eine Aufspaltung von a mit $\boldsymbol{V}^n = \tilde{\boldsymbol{U}} \oplus \tilde{\boldsymbol{W}}$, welche die geforderten Eigenschaften besitzt. Wir behaupten: Es gilt

$$\tilde{\boldsymbol{U}} \subseteq \boldsymbol{U}_k \quad \text{und} \quad \tilde{\boldsymbol{W}} \subseteq \boldsymbol{W}_k \tag{24}$$

für das k nach Lemma 2. Aus Dimensionsgründen muß dann wegen $\boldsymbol{V}^n = \tilde{\boldsymbol{U}} \oplus \tilde{\boldsymbol{W}} = \boldsymbol{U}_k \oplus \boldsymbol{W}_k$ sogar $\tilde{\boldsymbol{U}} = \boldsymbol{U}_k$ und $\tilde{\boldsymbol{W}} = \boldsymbol{W}_k$ gelten, und die Zerlegungen $a = a_0 \oplus a_1 = \tilde{a}_0 \oplus \tilde{a}_1$ stimmen überein. Wegen $a \mid \tilde{\boldsymbol{W}}$ bijektiv gilt $a^i \tilde{\boldsymbol{W}} = \tilde{\boldsymbol{W}} \subseteq \boldsymbol{W}_i$ für alle $i \in \mathbf{N}_0$, also auch $\tilde{\boldsymbol{W}} \subseteq \boldsymbol{W}_k$. Zum Beweis der ersten Relation (24) stellen wir $\mathfrak{x} \in \tilde{\boldsymbol{U}}$ in der Form $\mathfrak{x} = \mathfrak{x}_0 + \mathfrak{x}_1$ entsprechend der Zerlegung $\boldsymbol{V} = \boldsymbol{U}_k \oplus \boldsymbol{W}_k$ dar. Dann gilt $a^l(\mathfrak{x}) = a_0^l(\mathfrak{x}_0) + a_1^l(\mathfrak{x}_1) = \mathfrak{o}$ für genügend großes l; denn $a \mid \tilde{\boldsymbol{U}}$ ist nilpotent. Aus der Aufspaltung (15) folgt nämlich wegen

$$a_\mu \circ a_\nu = o \quad \text{für} \quad \mu \neq \nu \tag{25}$$

und (14) sofort die Aufspaltung (bezüglich (13))

$$a^i = a_1^i \oplus \ldots \oplus a_m^i , \qquad i \in \mathbf{N}_0 . \tag{26}$$

Da wir jetzt die direkte Summe $\boldsymbol{V}^n = \boldsymbol{U}_k \oplus \boldsymbol{W}_k$ betrachten, muß speziell $a^l(\mathfrak{x}_1) = \mathfrak{o}$ sein, und weil $a \mid \boldsymbol{W}_k$ bijektiv ist, folgt $\mathfrak{x}_1 = \mathfrak{o}$, d. h. $\mathfrak{x} = \mathfrak{x}_0 \in \boldsymbol{U}_k$. □

Bevor wir zur Definition einer Jordanschen Normalform kommen, ist es zweckmäßig, sich die Bedeutung der Aufspaltung eines Endomorphismus in eine direkte Summe anhand der folgenden einfachen Übung klarzumachen:

Übung 2. Es sei $\boldsymbol{V}^n = \boldsymbol{B}^b \oplus \boldsymbol{C}^c \oplus \ldots \oplus \boldsymbol{W}^w$ eine Aufspaltung von $\boldsymbol{V}^n$ in eine direkte Summe bei $a \in \boldsymbol{L}(\boldsymbol{V}^n)$ invarianter Unterräume. Passen wir dann die Basis von $\boldsymbol{V}^n$ dieser Zerlegung an, d. h., setzen wir sie aus den Basen $(\mathfrak{b}_\alpha)_{\alpha=1,\ldots,b}$, $(\mathfrak{c}_\gamma)_{\gamma=1,\ldots,c}$, ..., $(\mathfrak{w}_\varrho)_{\varrho=1,\ldots,w}$ zusammen, so hat die Matrix von a bezüglich dieser Basis die Form

$$(a_{ij}) = \begin{pmatrix} (b_{\alpha\beta}) & 0 & \ldots & 0 \\ 0 & (c_{\gamma\delta}) & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & (w_{\varrho\sigma}) \end{pmatrix}, \tag{27}$$

wobei die Matrizen $(b_{\alpha\beta}) \in \mathbf{M}_b$, $(c_{\gamma\delta}) \in \mathbf{M}_c$, ..., $(w_{\varrho\sigma}) \in \mathbf{M}_w$ hintereinander längs der Hauptdiagonale gruppiert sind, $b + c + \ldots + w = n$ gilt und alle übrigen Elemente in der Matrix (27) gleich 0 sind. Gelingt es umgekehrt, zu einem Endomorphismus eine Basis $(\mathfrak{a}_i)$ von $\boldsymbol{V}^n$ zu finden, bezüglich der die Matrix die Form (27) hat, so spaltet a bezüglich der Unterräume $\boldsymbol{B}^b := \mathfrak{L}(\mathfrak{a}_1, \ldots, \mathfrak{a}_b)$, $\boldsymbol{C}^c := \mathfrak{L}(\mathfrak{a}_{b+1}, \ldots, \mathfrak{a}_{b+c})$, ..., $\boldsymbol{W}^w = \mathfrak{L}(\mathfrak{a}_{n-w+1}, \ldots, \mathfrak{a}_n)$ auf.

Nun wollen wir definieren, was wir unter der Jordanschen Normalform eines beliebigen aufspaltenden Endomorphismus verstehen.

Definition 4. Unter einem *Jordanschen Kästchen der Ordnung k* verstehen wir eine Matrix der Form

$$D_k(\lambda) := \begin{pmatrix} \lambda & & & 0 \\ 1 & \lambda & & \\ & 1 & \ddots & \\ & & \ddots & \lambda \\ 0 & & & 1 \;\; \lambda \end{pmatrix} \in \mathbf{M}_k(K) . \tag{28}$$

Unter einer *Jordanschen Matrix* verstehen wir eine Matrix, die aus längs der Hauptdiagonale aneinandergereihten Jordanschen Kästchen besteht, während alle anderen Elemente 0 sind:

$$\begin{pmatrix} \lambda_1 & & 0 & & & \mathbf{0} \\ 1 & \ddots & & & & \\ & \ddots & \ddots & & & \\ 0 & 1 & \lambda_1 & & & \\ & & & \lambda_2 & & 0 \\ & & & 1 & \ddots & \\ & & & & \ddots & \ddots \\ & & & 0 & 1 & \lambda_2 \\ & & & & & & \ddots \\ & & & & & & \lambda_m & & 0 \\ & & & & & & 1 & \ddots & \\ & & & & & & & \ddots & \ddots \\ & \mathbf{0} & & & & & 0 & 1 & \lambda_m \end{pmatrix}. \tag{29}$$

Wir schreiben zur Abkürzung dafür auch

$$\begin{pmatrix} D_{k_1}(\lambda_1) & & \mathbf{0} \\ & D_{k_2}(\lambda_2) & \\ & & \ddots \\ \mathbf{0} & & D_{k_m}(\lambda_m) \end{pmatrix}. \tag{30}$$

Beispiel 1. Ein Endomorphismus $a \in \boldsymbol{L}(\boldsymbol{V}^n)$ ist diagonalisierbar (Beispiel 4.5) genau dann, wenn eine Basis existiert, für die seine Matrix Jordansche Normalform aus n Kästchen der Ordnung $k_1 = \ldots = k_n = 1$ besitzt.

Folgerung 1. *Gibt es zu $a \in \boldsymbol{L}(\boldsymbol{V}^n)$ eine Basis, bezüglich der seine Matrix Jordansche Normalform* (29) *hat, so ist a aufspaltend, und das charakteristische Polynom von a hat die Form*

$$\chi_a(x) = \prod_{\mu=1}^{m} (\lambda_\mu - x)^{k_\mu}. \quad \square \tag{31}$$

Der Beweis von Folgerung 1 ergibt sich sofort aus der Dreiecksgestalt der Jordanschen Normalform, vgl. Satz 4.8.1. Wir kehren nun wieder zu den nilpotenten Endomorphismen zurück und beweisen

Satz 3. *Ein Endomorphismus $b \in \boldsymbol{L}(\boldsymbol{V}^n)$ ist nilpotent dann und nur dann, wenn es eine Basis $(\mathfrak{a}_i)$ von $\boldsymbol{V}^n$ so gibt, daß die Matrix (b_{ij}) von b Jordansche Normalform* (30) *mit $\lambda_1 = \ldots = \lambda_m = 0$ und*

$$k_1 \geqq \ldots \geqq k_m \geqq 1 \tag{32}$$

besitzt.

Beweis. Die eine Richtung des Satzes ist trivial (vgl. Übung 1). Für den Beweis der Existenz der Jordanschen Normalform von b betrachten wir die im Lemma 3 angegebene Folge (20). Da b nilpotent ist, muß in der Zerlegung von Satz 2 $b=b_0$, $b_1=o$, d. h. $W_k=\{o\}$ gelten. Wir führen den Beweis durch vollständige Induktion nach $n=\dim V$. Für $n=0$ und $n=1$ ist die Behauptung trivial. Angenommen, sie sei schon für alle $m<n$ bewiesen. Wir betrachten den Endomorphismus $\hat{b}:=b\mid W_1$. Offenbar ist $\hat{b}$ ebenfalls nilpotent. Wir können eine Basis $\mathfrak{a}_1, \ldots, \mathfrak{a}_{n_1}$ von W_1 finden, $n_1:=\dim W_1$, bezüglich der $\hat{b}$ Jordansche Normalform mit $\lambda_\nu=0$ hat. Es seien $\hat{D}_{\hat{k}_1}, \ldots, \hat{D}_{\hat{k}_{\hat{m}}}$ die Jordanschen Kästchen von $\hat{b}$. Zu jedem Kästchen gehört derjenige Basisvektor $\mathfrak{a}_{e_\mu}$, dessen Bild $b(\mathfrak{a}_{e_\mu})$ die Koordinaten der ersten Spalte des μ-ten Kästchens besitzt. Wegen $\mathfrak{a}_{e_\mu}\in W_1=bV$ gibt es Vektoren $\mathfrak{b}_1, \ldots, \mathfrak{b}_{\hat{m}}$ mit $b(\mathfrak{b}_\mu)=\mathfrak{a}_{e_\mu}$, $\mu=1, \ldots, \hat{m}$. Wir behaupten

1. *Die Vektoren* $\mathfrak{b}_1, \ldots, \mathfrak{b}_{\hat{m}}, \mathfrak{a}_1, \ldots, \mathfrak{a}_{n_1}$ *sind linear unabhängig.*

In der Tat, wäre

$$\sum_{\mu=1}^{\hat{m}} \mathfrak{b}_\mu \xi_\mu + \sum_{\nu=1}^{n_1} \mathfrak{a}_\nu \eta_\nu = \mathfrak{o}\,, \tag{33}$$

so folgte durch Anwendung von b

$$\sum_{\mu=1}^{\hat{m}} \mathfrak{a}_{e_\mu} \xi_\mu + \sum_{\nu=1}^{n_1} b(\mathfrak{a}_\nu)\, \eta_\nu = \mathfrak{o}\,. \tag{34}$$

Da $b(\mathfrak{a}_\nu)=\mathfrak{a}_{\nu+1}$ oder $b(\mathfrak{a}_\nu)=\mathfrak{o}$ gilt — weil ja die Basis $(\mathfrak{a}_\nu)$ zur Jordanschen Normalform von $\hat{b}$ gehört —, müssen in (34) alle Koeffizienten an den von $\mathfrak{o}$ verschiedenen Vektoren verschwinden; denn diese sind Teil der Basis $(\mathfrak{a}_\nu)$, $\nu=1, \ldots, n_1$, von W_1. Speziell sind alle $\xi_\mu=0$. Dann folgt aber wegen (33), daß auch alle η_ν gleich 0 sind.

2. *Aus jedem Kästchen* $\hat{D}_{\hat{k}_\mu}$ *von* $\hat{b}$ *entsteht ein Kästchen* $\hat{D}_{\hat{k}_\mu+1}$ *von* b.

Das folgt sofort aus der Wahl der Vektoren $\mathfrak{b}_\mu$; denn es gilt

$$b(\mathfrak{b}_\mu)=\mathfrak{a}_{e_\mu}, \qquad b(\mathfrak{a}_{e_\mu})=\mathfrak{a}_{e_\mu+1}, \ldots, b(\mathfrak{a}_{l_\mu})=\mathfrak{o}\,,$$

$\mathfrak{a}_{l_\mu}$ der letzte Vektor zum Kästchen $\hat{D}_{\hat{k}_\mu}$, $\mu=1, \ldots, \hat{m}$.

Wir bezeichnen nun die in 1. angegebenen Vektoren mit $(\mathfrak{c}_1, \ldots, \mathfrak{c}_{n_1+\hat{m}})$ in der Reihenfolge der Kästchen. Dann gilt $k_\mu=k_\mu+1$, also $k_1\geqq\ldots\geqq k_{\hat{m}}\geqq 2$; denn die Anzahl der Kästchen blieb ja bisher dieselbe. Es werden in der Folge $(\mathfrak{c}_i)$ alle letzten Vektoren $\mathfrak{a}_{l_\mu}$, $\mu=1, \ldots, \hat{m}$, der Kästchen entfernt; es sei $(\mathfrak{c}_{\nu_i})$ die übrigbleibende Teilfolge. Nach Konstruktion dieser Teilfolge gilt für ihre lineare Hülle $\tilde{W}_1:=\mathfrak{L}(\{\mathfrak{c}_{\nu_i}\})$:

3. $b\mid\tilde{W}_1\colon \tilde{W}_1\to W_1$ *ist ein Isomorphismus.*

Die Dimensionen dieser Räume sind nämlich gleich, $b\mid\tilde{W}_1$ ist offenbar sur-

jektiv. Folglich ist

$$V = \tilde{W}_1 \oplus \operatorname{Ker} b; \tag{35}$$

denn wegen $b \mid \tilde{W}_1$ injektiv folgt $\tilde{W}_1 \cap \operatorname{Ker} b = \{0\}$, und es gilt dim Ker $b = n - \dim \tilde{W}_1$ nach Folgerung 2.7. In Ker b liegen speziell die vorhin weggelassenen letzten Vektoren der Kästchen; diese sind als Teilmenge einer Basis linear unabhängig. Wir ergänzen sie zu einer Basis von Ker b; es seien $c_{n_1+\hat{m}+1}, \ldots, c_n$ diese ergänzenden Vektoren. Da sie in Ker b liegen, bestimmen sie jeder ein Jordansches Kästchen $D_1(0)$, d. h. eine 0 in der Hauptdiagonale. Damit ist die Existenz der Jordanschen Normalform für nilpotente b bewiesen; man macht sich leicht klar, daß der Beweis ein effektives Verfahren zur Bestimmung der Jordanschen Normalform durch Abarbeiten der Räume $W_i = \operatorname{Im} b^i$, beginnend mit W_{k-1}, enthält. □

Nun können wir leicht den allgemeinen Fall erledigen.

Satz 4. *Es sei $a \in L(V^n)$ ein aufspaltender Endomorphismus. Dann gilt:* 1. *Es gibt eine Basis (a_i) von V^n, bezüglich der die Matrix (a_{ij}) von a Jordansche Normalform* (29) *besitzt.* — 2. *Die Jordansche Normalform ist durch a bis auf die Reihenfolge der Kästchen $D_{k_\mu}(\lambda_\mu)$ eindeutig bestimmt.* — 3. *Ein Endomorphismus $\tilde{a}$ ist genau dann ähnlich zu a, wenn $\tilde{a}$ ebenfalls aufspaltend ist und dieselbe Jordansche Normalform (bis auf die Reihenfolge der Kästchen) wie a besitzt.*

Beweis. Wir führen den Existenzbeweis durch Induktion nach $n = \dim V^n$. Für $n = 0, 1$ ist die Behauptung trivial. Angenommen, sie sei schon für alle Dimensionen $< n$ bewiesen. Da a aufspaltend ist, gibt es einen Eigenwert $\lambda \in K$ von a. Wir definieren $b := a - e\lambda$ und betrachten die Zerlegung $V^n = U_k \oplus W_k$ nach Satz 2 von b. Diese Zerlegung ist auch bei a invariant; denn es gilt $a = b + e\lambda$, und $e\lambda$ läßt jeden Unterraum invariant. Da λ ein Eigenwert von a ist, gilt Ker $b \neq \{0\}$, also $U_k \neq \{0\}$ und dim $W_k < n$. Nach Induktionsvoraussetzung können wir $a \mid W_k$ in Jordanscher Normalform darstellen. Aus Satz 3 erhalten wir eine Jordansche Normalform von $b \mid U_k$, und bezüglich derselben Basis von U_k folgt, daß $a \mid U_k = b \mid U_k + e \mid U_k \lambda$ ebenfalls Jordansche Normalform mit λ statt 0 auf allen Stellen der Hauptdiagonale hat. Wir bemerken, daß $a \mid W_k$ nicht den Eigenwert λ besitzen kann, da $b \mid W_k$ bijektiv, also Ker $(b \mid W_k) = \{0\}$ gilt.

Zum Beweis der Eindeutigkeit bemerken wir, daß V^n in die durch (36) definierten *Nilunterräume* U_σ zu den verschiedenen Eigenwerten λ_σ, $\sigma = 1, \ldots, s$, $\lambda_\sigma \neq \lambda_\varrho$ für $\sigma \neq \varrho$, aufspaltet; diese Unterräume sind gerade die U_σ von $b_\sigma = a - e\lambda_\sigma$:

$$U_\sigma := \{\mathfrak{x} \in V^n \mid \textit{es existiert ein } l \in \mathbf{N} \textit{ mit } (a - e\lambda_\sigma)^l \mathfrak{x} = 0\}. \tag{36}$$

Das folgt durch fortgesetzte Abspaltung der U_σ wie beim Beweis der ersten Behauptung. Die U_σ sind nach (36) und Satz 1 durch a eindeutig bestimmt, und es gilt die bei a invariante Aufspaltung

$$V^n = \bigoplus_{\sigma=1}^{s} U_\sigma. \tag{37}$$

Folglich ist auch $a_\sigma = a \mid \boldsymbol{U}_\sigma$ und somit der auf $\boldsymbol{U}_\sigma$ nilpotente Endomorphismus $b_\sigma = a_\sigma - e_\sigma \lambda_\sigma$, $e_\sigma = \mathrm{id}_{\boldsymbol{U}_\sigma}$, eindeutig bestimmt. Wegen Folgerung 1 genügt es also zu zeigen, daß die Folge (32) durch den nilpotenten Endomorphismus b eindeutig bestimmt ist. Wir betrachten also nur noch einen derartigen Endomorphismus. Es bezeichne ν_l die Anzahl der Kästchen in einer Jordanschen Normalform von b, deren Länge $\geqq l$ ist; wir zeigen, daß die ν_l durch b eindeutig bestimmt sind; damit ist auch die Folge (32) eindeutig bestimmt; denn $\nu_l - \nu_{l+1}$ ist die Anzahl der k_μ mit $k_\mu = l$ der Folge. Nun sind offenbar die $\boldsymbol{W}_i = \mathrm{Im}\ b^i$ durch b eindeutig bestimmt, somit auch $n_i := \dim \boldsymbol{W}_i$. Eine leichte Überlegung anhand der speziellen Normalform eines nilpotenten Endomorphismus zeigt uns

$$n_1 = n - \nu_1 = n - m, \qquad n_2 = n - \nu_1 - \nu_2, \ \ldots$$

und allgemein

$$n_i = n - \sum_{l=1}^{i} \nu_l . \tag{38}$$

Hieraus folgt aber

$$\nu_i = n_{i-1} - n_i . \tag{39}$$

Es bleibt die dritte Behauptung zu zeigen. Die ist aber nach den Erörterungen am Schluß von § 7 klar: Sind zwei Endomorphismen $a, \tilde{a}$ ähnlich, so sind sie beide aufspaltend nach Satz 1. Hat a in der Basis $(\mathfrak{a}_i)$ Jordansche Normalform und gilt $\tilde{a} = \alpha_g(a)$, so hat $\tilde{a}$ in $(g\mathfrak{a}_i)$ dieselbe Jordansche Normalform; denn $\tilde{a}$ hat in dieser Basis dieselbe Matrix wie a bezüglich $(\mathfrak{a}_i)$. Haben umgekehrt a und $\tilde{a}$ bezüglich $(\mathfrak{a}_i)$ bzw. $(\tilde{\mathfrak{a}}_i)$ dieselbe Matrix (z. B. dieselbe Jordansche Normalform) und ist $(g\mathfrak{a}_i) = (\tilde{\mathfrak{a}}_i)$, so gilt $\alpha_g(a) = \tilde{a}$. □

Folgerung 2. *Es sei $K = \mathbf{C}$. Dann ist jeder Endomorphismus $a \in \boldsymbol{L}(\boldsymbol{V}^n)$ aufspaltend. Zwei Endomorphismen $a, \tilde{a} \in \boldsymbol{L}(\boldsymbol{V}^n)$ sind genau dann ähnlich, wenn sie dieselbe Jordansche Normalform (bis auf die Reihenfolge der Jordanschen Kästchen) besitzen.*

Zum Beweis genügt es, den Fundamentalsatz der Algebra (Folgerung 2.8.1 und § 3.5) anzuwenden. Offenbar genügt es vorauszusetzen, daß K *algebraisch abgeschlossen* ist, d. h., daß jedes Polynom $f \in K[x]$ über K zerfällt. Durch Folgerung 2 ist das Klassifikationsproblem für die Transformationsgruppe $[\boldsymbol{GL}(\boldsymbol{V}^n), \boldsymbol{L}(\boldsymbol{V}^n)]$ und $K = \mathbf{C}$ vollkommen gelöst; die Jordanschen Kästchen bzw. die sie bestimmenden Paare (λ_μ, k_μ) sind ein vollständiges Invariantensystem. □

Übung 3. Es sei $a \in \boldsymbol{L}(\boldsymbol{V}^n)$ und $(\mathfrak{a}_i)$ eine Basis von $\boldsymbol{V}^n$, bezüglich der (a_{ij}) Jordansche Normalform hat. Man bestimme $\mathrm{Ker}\ a$, $\mathrm{Im}\ a$, $\boldsymbol{U}_k$, $\boldsymbol{W}_k$ und die Aufspaltung $a = a_0 \oplus a_1$ nach Satz 2 durch Angabe geeigneter Basen dieser Räume.

Übung 4. Man betrachte den Endomorphismus von Übung 2.4, aber über $K = \mathbf{C}$, und bestimme seine Jordansche Normalform.

Übung 5. Unter den Bedingungen der Übung 4.19 zeige man, daß $\chi_a = \chi_b \cdot \chi_c$ gilt.

Hieraus schließe man: Ist W der Eigenunterraum U_λ von a, so ist dim U_λ kleiner oder gleich der Vielfachheit der Nullstelle λ des Polynoms χ_a.

Übung 6. Es sei K ein beliebiger Körper und $a \in L(V^n)$. Man beweise: a ist nilpotent dann und nur dann, wenn $\chi_a(x) = (-x)^n$ gilt.

Übung 7. Es sei $K = \mathbf{C}$ und $\mathfrak{F}$ die Menge aller affinen Abbildungen von A^n in sich, $\mathfrak{A}(A^n)$ die Gruppe der affinen Automorphismen. Man klassifiziere die affinen Abbildungen gegenüber der Wirkung $(f, g) \in \mathfrak{A}(A^n) \times \mathfrak{F} \mapsto fgf^{-1} \in \mathfrak{F}$.

Übung 8. Es sei V^n ein Vektorraum über $\mathbf{C}$ und $a \in L(V^n)$. Man beweise: Gilt $a^m = e$, so ist a diagonalisierbar, und die Eigenwerte von a sind m-te Einheitswurzeln $\sqrt[m]{1}$.

Übung 9. Man beweise, daß Summe und Produkt zweier kommutierender, nilpotenter Operatoren $a, b \in L(V)$ wieder nilpotente Operatoren sind.

Übung 10. Es sei $a \in L(V^n)$ ein aufspaltender Endomorphismus. Man beweise: Es existieren ein nilpotenter Operator b und ein diagonalisierbarer Operator s derart, daß $b \circ s = s \circ b$ und $a = s + b$ gelten; durch diese Bedingungen sind s und b eindeutig bestimmt. (Hinweis. Für den Beweis der Eindeutigkeit beachte man die Übungen 9 und 4.9, b).)

§ 9. Symmetrische Bilinearformen. Hermitesche Formen. Affine Klassifikation der Quadriken

In diesem Paragraphen betrachten wir einen n-dimensionalen affinen Raum A^n über einem Körper K. Für die Geometrie der Ebene und des Raumes sind dabei besonders die Fälle $K = \mathbf{R}$ und $n = 2, 3$ interessant. Bei vielen Anwendungen der Geometrie in der Analysis und in der Physik benötigt man auch höherdimensionale Räume und Betrachtungen über dem komplexen Zahlkörper $\mathbf{C}$. Die klassische Definition der Quadrik lautet folgendermaßen: Es sei $(o; \mathfrak{a}_i)$ ein n-Bein des A^n, und (x_i) seien die zugehörigen Punktkoordinaten. Unter einer *Quadrik* Q versteht man die Menge aller Punkte $x \in A^n$, deren Koordinaten x_i einer quadratischen Gleichung

$$\sum_{i,j=1}^{n} q_{ij} x_i x_j + \sum_{i=1}^{n} q_i x_i + q = 0 \tag{1}$$

mit $q_{ij}, q_i, q \in K$ genügen, wobei die erste Summe, das quadratische Glied, nicht für alle $x \in A^n$ gleich 0 sein soll. Wir werden weiter unten eine von den Koordinaten freie Definition der Quadriken geben. Es ist eine interessante Aufgabe, die verschiedenen Arten von Quadriken geometrisch zu beschreiben. Die affine Gruppe $\mathfrak{A}(A^n)$ transformiert Quadriken wieder in Quadriken; daher läuft unsere Aufgabe auf die affine Klassifikation der Quadriken hinaus. Zunächst erinnern wir an einige Beispiele aus der Elementargeometrie.

Beispiel 1. $K = \mathbf{R}$, $n = 2$, $a_1, a_2, a, p > 0$.

a) *Ellipse mit Zentrum in o:*

$$(x_1/a_1)^2 + (x_2/a_2)^2 - 1 = 0\,. \tag{2}$$

b) *Hyperbel mit Zentrum in o:*

$$(x_1/a_1)^2-(x_2/a_2)^2-1=0\,. \tag{3}$$

c) *Parabel mit Scheitelpunkt o:*

$$(x_1)^2+2px_2=0\,. \tag{4}$$

d) *Paar sich schneidender Geraden:*

$$(a_1x_1)^2-(a_2x_2)^2=0\,. \tag{5}$$

e) *Paar paralleler Geraden:*

$$x_1^2-a^2=0\,. \tag{6}$$

f) *Doppelt zählende Gerade:*

$$x_1^2=0\,. \tag{7}$$

g) *Der Punkt o:*

$$x_1^2+x_2^2=0\,. \tag{8}$$

h) *Imaginäre Quadriken.* Die Gleichungen

$$x_1^2+x_2^2+a=0, \qquad a>0\,, \tag{9}$$

oder

$$x_1^2+a=0, \qquad a>0\,, \tag{10}$$

haben keine reellen Lösungen. Wegen $\mathbf{R}\subset\mathbf{C}$ können wir (9) und (10) jedoch auch als Gleichungen im zweidimensionalen affinen Raum A^2 über $\mathbf{C}$ deuten. Hier existieren Lösungen. Man nennt diese Quadriken daher im Fall $K=\mathbf{R}$ *imaginär.*

Zwei Mengen M_1, $M_2\subseteq A^n$ heißen *affin-kongruent,* wenn es eine affine Transformation $f\in\mathfrak{A}(A^n)$ gibt mit $f(M_1)=M_2$. Da wir aus jeder Transformationsgruppe $[G, X]$ sofort eine induzierte Transformationsgruppe $[G, \mathfrak{P}(X)]$ erhalten (vermöge der durch (0.2.24) zu definierenden Wirkung), ist die affine Kongruenz eine Äquivalenzrelation, die zum Begriff der Kongruenz von Figuren in der Elementargeometrie analog ist. Als Spezialfall der allgemeinen Theorie der Quadriken wird sich ergeben, daß jede Quadrik $Q\subseteq A^2$ zu einer der angegebenen Quadriken (2) bis (10) affin-kongruent ist. Dabei können wir sogar noch $a_1=a_2=p=a=1$ annehmen. Hierdurch wird das Klassifikationsproblem gelöst. Außerdem werden wir ein Verfahren angeben, um die Klassifikation tatsächlich auszuführen. In unserem Spezialfall bedeutet das, die folgende Aufgabe zu lösen: Gegeben sei eine quadratische Gleichung in x_1, x_2:

$$q_{11}x_1^2+2q_{12}x_1x_2+q_{22}x_2^2+q_1x_1+q_2x_2+q=0\,, \tag{11}$$

wobei q_{ij}, q_i, $q\in\mathbf{R}$ gilt und wenigstens einer der Koeffizienten q_{11}, q_{12}, $q_{22}\neq 0$ ist. Man bestimme diejenige der Quadriken (2) bis (10), zu der (11) affin-kongruent ist.

Übung 1. Man betrachte die Gleichungen (9) und (10) im Fall $K=\mathbf{C}$, $a\in\mathbf{R}$, bestimme die Menge ihrer Lösungen $Q\subset\mathbf{C}^2$ und zeige, daß diese Mengen verschieden sind.

Übung 2. Man beweise unter den Voraussetzungen von Beispiel 1, daß man in den Gleichungen (2) bis (10) $a_1=a_2=a=2p=1$ setzen kann. Das bedeutet: Alle Quadriken Q, die zu einer festen dieser Gleichungen bei verschiedenen positiven Parametern a_1, a_2, a bzw. p gehören, sind affin-kongruent. Zum Beispiel sind alle Ellipsen affin-kongruent zum „Einheitskreis".

Übung 3. In der Elementargeometrie nennt man die ebenen Quadriken auch *Kegelschnitte*. Unter einem *Kegel* versteht man eine Quadrik des dreidimensionalen reellen affinen Raumes, deren Gleichung durch geeignete Wahl der Koordinaten auf die Form

$$x_1^2+x_2^2-x_3^2=0 \tag{12}$$

gebracht werden kann. Es sei nun $\boldsymbol{H}^2\subset\boldsymbol{A}^3$ eine beliebige Ebene und Q der durch (12) beschriebene Kegel. Man beweise: Der Durchschnitt $\boldsymbol{H}^2\cap Q$ ist eine Quadrik in $\boldsymbol{H}^2$. Ferner untersuche man, welche der in Beispiel 1 angegebenen Quadriken man wirklich als Kegelschnitte $\boldsymbol{H}^2\cap Q$ erhält. (Hinweis. Man unterscheide die Koordinaten in $\boldsymbol{H}^2$ und $\boldsymbol{A}^3$! Wenn die Lösung des zweiten Teiles der Aufgabe jetzt noch nicht gelingt, versuche man es nach dem Studium dieses Paragraphen noch einmal.)

Für die koordinatenfreie Definition der Quadriken benötigen wir den Begriff einer symmetrischen Bilinearform.

Definition 1. Es sei $\boldsymbol{V}$ ein Vektorraum über K. Unter einer *Bilinearform* versteht man eine Abbildung

$$b\colon(\mathfrak{x},\mathfrak{y})\in\boldsymbol{V}\times\boldsymbol{V}\mapsto b(\mathfrak{x},\mathfrak{y})\in K\,, \tag{13}$$

die linear in jedem Argument ist. Für $\alpha,\beta\in K$ und $\mathfrak{x}_i,\mathfrak{y}_i\in\boldsymbol{V}$ gilt also

$$b\,(\mathfrak{x}_1\alpha+\mathfrak{x}_2\beta,\mathfrak{y})=b(\mathfrak{x}_1,\mathfrak{y})\,\alpha+b(\mathfrak{x}_2,\mathfrak{y})\,\beta\,, \tag{14}$$

$$b\,(\mathfrak{x},\mathfrak{y}_1\alpha+\mathfrak{y}_2\beta)=b(\mathfrak{x},\mathfrak{y}_1)\,\alpha+b(\mathfrak{x},\mathfrak{y}_2)\,\beta\,. \tag{15}$$

Eine Bilinearform heißt *symmetrisch*, wenn für alle $\mathfrak{x},\mathfrak{y}\in\boldsymbol{V}$

$$b(\mathfrak{x},\mathfrak{y})=b(\mathfrak{y},\mathfrak{x}) \tag{16}$$

gilt.

Definition 2. Es sei $[\boldsymbol{A}^n,\boldsymbol{V}^n,K]$ eine affine Geometrie über dem Körper K. Unter einer *Quadrik* $Q\subseteq\boldsymbol{A}^n$ versteht man die Menge derjenigen Punkte $x\in\boldsymbol{A}^n$, deren Ortsvektoren bezüglich eines festen Punktes $o\in\boldsymbol{A}^n$ einer Gleichung der Form

$$b(\overrightarrow{ox},\overrightarrow{ox})+\mathfrak{v}(\overrightarrow{ox})+q=0 \tag{17}$$

genügen; hierbei ist $b\neq0$ eine symmetrische Bilinearform über $\boldsymbol{V}$, $\mathfrak{v}\in\boldsymbol{V}'$ ein dualer Vektor und $q\in K$.

Wir werden bald zeigen, daß die im zweiten Absatz dieses Paragraphen gegebene Definition einer Quadrik als Lösungsmenge von (1) zu Definition 2 äquivalent ist, jedenfalls für Körper mit $\operatorname{char}K\neq2$. Zunächst bemerken wir jedoch, daß die Wahl des Ursprungs $o\in\boldsymbol{A}^n$ nicht wesentlich ist. Es sei etwa $\bar{o}\neq o$ ein anderer Ur-

sprung. Dann gilt

$$\overrightarrow{ox} = \overrightarrow{o\hat{o}} + \overrightarrow{\hat{o}x} = \mathfrak{a} + \overrightarrow{\hat{o}x} \tag{18}$$

mit $\mathfrak{a} := \overrightarrow{o\hat{o}}$. Setzen wir das in (17) ein, so folgt

$$b(\overrightarrow{\hat{o}x}, \overrightarrow{\hat{o}x}) + 2b(\mathfrak{a}, \overrightarrow{\hat{o}x}) + \mathfrak{v}(\overrightarrow{\hat{o}x}) + b(\mathfrak{a}, \mathfrak{a}) + \mathfrak{v}(\mathfrak{a}) + q = 0 ,$$

also

$$b(\overrightarrow{\hat{o}x}, \overrightarrow{\hat{o}x}) + \hat{\mathfrak{v}}(\overrightarrow{\hat{o}x}) + \hat{q} = 0 \tag{19}$$

mit

$$\hat{\mathfrak{v}}(\mathfrak{x}) = \mathfrak{v}(\mathfrak{x}) + 2b(\mathfrak{a}, \mathfrak{x}) , \tag{20}$$

$$\hat{q} = b(\mathfrak{a}, \mathfrak{a}) + \mathfrak{v}(\mathfrak{a}) + q . \tag{21}$$

Die Eigenschaft, Quadrik zu sein, hängt also nicht von der Wahl des Ursprungs ab; bei einer Translation $\hat{o} = o + \mathfrak{a}$ des Ursprungs bleibt die Bilinearform b ungeändert, während $\mathfrak{v}$ und q sich nach (20) bzw. (21) transformieren.

Satz 1. *Eine Bilinearform b ist durch ihre Werte auf einer Basis $(\mathfrak{a}_i)$ von V^n*

$$b_{ij} := b(\mathfrak{a}_i, \mathfrak{a}_j), \qquad i, j = 1, \ldots, n , \tag{22}$$

eindeutig bestimmt. Ist eine Matrix $(b_{ij}) \in \mathbf{M}_n(K)$ gegeben, so gibt es eine und nur eine Bilinearform $b: V^n \times V^n \to K$, deren Matrix bezüglich $(\mathfrak{a}_i)$ gerade (b_{ij}) ist, d. h., für die (22) *gilt* (Prinzip der linearen Fortsetzung).

Beweis. Der Beweis folgt wie bei den linearen Abbildungen aus der Linearität, nach der für $\mathfrak{x} = \sum_i \mathfrak{a}_i \xi_i$, $\mathfrak{y} = \sum_j \mathfrak{a}_j \eta_j$

$$b(\mathfrak{x}, \mathfrak{y}) = \sum_{i,j=1}^{n} b_{ij} \xi_i \eta_j \tag{23}$$

gilt. □

Folgerung 1. *Eine Bilinearform ist symmetrisch dann und nur dann, wenn*

$$b_{ij} = b_{ji} \quad \textit{für alle} \quad i < j, \qquad 1 \leqq i, j \leqq n , \tag{24}$$

erfüllt ist. □

Definition 3. Es bezeichne $\boldsymbol{L}_2(\boldsymbol{V})$ die Menge aller Bilinearformen, $\boldsymbol{L}_2(\boldsymbol{V})_s$ die Teilmenge der symmetrischen Bilinearformen und $\boldsymbol{L}_2(\boldsymbol{V})_a$ die Teilmenge der alternierenden Bilinearformen; eine Bilinearform b heißt *alternierend*, wenn für alle $\mathfrak{x} \in \boldsymbol{V}$

$$b(\mathfrak{x}, \mathfrak{x}) = 0 \tag{25}$$

gilt.

Wie beim Beweis von (4.7.11) erkennt man, daß jede alternierende Bilinearform b auch *schiefsymmetrisch* ist, d. h.

$$b(\mathfrak{x}, \mathfrak{y}) + b(\mathfrak{y}, \mathfrak{x}) = 0 \quad \text{für alle} \quad \mathfrak{x}, \mathfrak{y} \in \boldsymbol{V} \tag{26}$$

gilt. Offenbar ergibt sich aus (26) für $\mathfrak{x} = \mathfrak{y}$ die Beziehung $2b(\mathfrak{x}, \mathfrak{x}) = 0$, so daß im Fall char $K \neq 2$ jede schiefsymmetrische Form auch alternierend ist. Nach (22) ist eine Bilinearform b alternierend genau dann, wenn ihre *Koordinatenmatrix* (b_{ij}) die Gleichungen

$$b_{ij} + b_{ji} = 0 \quad \text{und} \quad b_{ii} = 0, \qquad 1 \leqq i, j \leqq n \tag{27}$$

erfüllt; falls char $K \neq 2$ ist, folgt $b_{ii} = 0$ für $i = j$ aus den ersten Gleichungen von (27). Als Beispiel einer alternierenden Bilinearform erwähnen wir eine Volumenfunktion $(\mathfrak{x}, \mathfrak{y}) \in \boldsymbol{V}^2 \times \boldsymbol{V}^2 \mapsto [\mathfrak{x}, \mathfrak{y}] \in K$. Der Beweis des folgenden Satzes ist so einfach, daß wir ihn dem Leser überlassen.

Satz 2. *$\boldsymbol{L}_2(\boldsymbol{V})$ ist ein Vektorraum bezüglich der argumentweise erklärten Operationen: Für $b_1, b_2, b \in \boldsymbol{L}_2(\boldsymbol{V})$ sei*

$$\begin{aligned} &(b_1 + b_2)(\mathfrak{x}, \mathfrak{y}) := b_1(\mathfrak{x}, \mathfrak{y}) + b_2(\mathfrak{x}, \mathfrak{y}), \\ &(b\alpha)(\mathfrak{x}, \mathfrak{y}) := b(\mathfrak{x}, \mathfrak{y})\,\alpha, \qquad \alpha \in K, \quad \mathfrak{x}, \mathfrak{y} \in \boldsymbol{V}. \end{aligned} \tag{28}$$

Die Räume $\boldsymbol{L}_2(\boldsymbol{V})_s$, $\boldsymbol{L}_2(\boldsymbol{V})_a$ sind Unterräume von $\boldsymbol{L}_2(\boldsymbol{V})$, und wenn char $K \neq 2$ *ist, gilt*

$$\boldsymbol{L}_2(\boldsymbol{V}) = \boldsymbol{L}_2(\boldsymbol{V})_a \oplus \boldsymbol{L}_2(\boldsymbol{V})_s. \tag{29}$$

Ist dim $\boldsymbol{V} = n < \infty$, *so gilt*

$$\dim \boldsymbol{L}_2(\boldsymbol{V}) = n^2, \qquad \dim \boldsymbol{L}_2(\boldsymbol{V})_s = \frac{n(n+1)}{2}, \qquad \dim \boldsymbol{L}_2(\boldsymbol{V})_a = \frac{n(n-1)}{2}.$$

Zu jeder Basis $(\mathfrak{a}_i)$ von $\boldsymbol{V}^n$ gehört eine eindeutig bestimmte Basis von $\boldsymbol{L}_2(\boldsymbol{V}^n)$, für die $(b_{ij}) \in \mathbf{M}_n(K)$ (nach (22)) die Koordinatenmatrix von b ist. □

Wie wir sehen, macht der Fall char $K = 2$ gewisse Schwierigkeiten. Die direkte Zerlegung (29) wird nämlich durch die Formel

$$b(\mathfrak{x}, \mathfrak{y}) = \frac{1}{2}(b(\mathfrak{x}, \mathfrak{y}) + b(\mathfrak{y}, \mathfrak{x})) + \frac{1}{2}(b(\mathfrak{x}, \mathfrak{y}) - b(\mathfrak{y}, \mathfrak{x})) \tag{30}$$

gegeben, die wir nur im Fall char $K \neq 2$ hinschreiben können. Daher soll von nun an ohne besondere Erwähnung die

Voraussetzung: char $K \neq 2$ (31)

gelten, die auch für den folgenden Satz wesentlich ist.

Definition 4. Für $b \in \boldsymbol{L}_2(\boldsymbol{V})$ definieren wir die zugehörige *quadratische Form* durch

$$b(\mathfrak{x}) := b(\mathfrak{x}, \mathfrak{x}), \qquad \mathfrak{x} \in \boldsymbol{V}. \tag{32}$$

Satz 3. *Die Abbildung, die jeder symmetrischen Bilinearform ihre quadratische Form zuordnet, ist injektiv.*

Beweis. In der Tat, ist $b(\mathfrak{x})$ die durch (32) definierte quadratische Form, so gilt

$$b(\mathfrak{x}, \mathfrak{y}) = \frac{1}{4}\left(b(\mathfrak{x}+\mathfrak{y}) - b(\mathfrak{x}-\mathfrak{y})\right). \quad \square \tag{33}$$

Nun ist es leicht, die Äquivalenz von (1) und (17) zu beweisen. Gehen wir nämlich in (17) zur Koordinatendarstellung über, wobei die Spaltenvektoren (x_i), (q_i) die Koordinaten von $\overrightarrow{ox}$ bzw. $\mathfrak{v}$ sind, so ist (17) äquivalent zu

$$\sum_{i,j} b_{ij} x_i x_j + \sum_i q_i x_i + q = 0;$$

das ist aber eine Gleichung der Form (1). Um von (1) zu (17) zu kommen, bemerken wir, daß wir o. B. d. A. $q_{ij} = q_{ji}$ annehmen können; ersetzen wir nämlich die q_{ij} durch

$$b_{ij} := \frac{1}{2}(q_{ij} + q_{ji}), \tag{34}$$

so ändert sich die Lösungsmenge Q der Gleichung (1) nicht. Damit können wir $(q_{ij}) = (b_{ij})$ als Matrix von b und (q_i) als Koordinatenvektor von $\mathfrak{v}$ auffassen und erhalten (17) aus (1). Für unsere Zwecke nützlich ist auch der Übergang zur Matrixschreibweise:

$$b(\mathfrak{x}, \mathfrak{y}) = (\xi_i)'\,(b_{ij})\,(\eta_j). \tag{35}$$

Gehen wir damit in (17) ein, so erhalten wir die zu (1) äquivalente Gleichung

$$(x_i)'\,(q_{ij})\,(x_j) + (q_i)'\,(x_i) + q = 0, \tag{36}$$

die für viele Rechnungen bequem ist. Die Transformationsgesetze (20) und (21) schreiben sich mit dem Spaltenvektor (α_i) der Koordinaten von $\mathfrak{a}$ bezüglich $(\mathfrak{a}_i)$ dann so:

$$(\hat{q}_j)' = (q_j)' + 2(\alpha_i)'\,(q_{ij}), \tag{37}$$

$$\hat{q} = (\alpha_i)'\,(q_{ij})\,(\alpha_j) + (q_i)'\,(\alpha_i) + q. \tag{38}$$

Damit ist gleichzeitig das *Transformationsgesetz der Gleichung einer Quadrik bei einer Translation des Ursprungs* gegeben. Wir untersuchen noch das Transformationsgesetz der Koordinaten (b_{ij}) einer Bilinearform und der Gleichung einer Quadrik bei einer Koordinatentransformation mit der Matrix (α_{ij}):

$$(\hat{\xi}_i) = (\alpha_{ij})\,(\xi_j). \tag{39}$$

Gehen wir mit der zu (39) inversen Gleichung in (35) ein, so folgt

$$b(\mathfrak{x}, \mathfrak{y}) = (\hat{\xi}_i)'\,(\alpha_{ij})^*\,(b_{jk})\,(\alpha_{kl})^{-1}\,(\hat{\eta}_l) = (\hat{\xi}_i)'\,(\hat{b}_{il})\,(\hat{\eta}_l). \tag{40}$$

Da die (b_{il}) nach Satz 1 durch b und $(\mathfrak{a}_i)$ eindeutig bestimmt sind, folgt

$$(\hat{b}_{il}) = (\alpha_{ij})^*\,(b_{jk})\,(\alpha_{kl})^{-1} \tag{41}$$

als *Transformationsgesetz der Koordinaten einer Bilinearform.* Man beachte den Unterschied zum Transformationsgesetz (7.25) der Koordinaten eines linearen Endomorphismus. Gehen wir mit (41) und dem Transformationsgesetz (7.16) der Koordinaten eines dualen Vektors in (36) ein, so erhalten wir bei der (39) entsprechenden Transformation der Punktkoordinaten:

$$(\hat{x}_i)'\,(\hat{q}_{ij})\,(\hat{x}_j)+(\hat{q}_i)'\,(\hat{x}_i)+\hat{q}=0$$

mit

$$(\hat{q}_{ij})=(\alpha_{ik})^*\,(q_{kl})\,(\alpha_{lj})^{-1}, \tag{42}$$

$$(\hat{q}_i)=(\alpha_{ik})^*\,(q_k), \qquad \hat{q}=q\,. \tag{43}$$

Durch zu dem Fall der linearen Abbildungen ganz analoge Überlegungen und Rechnungen stellt man fest:

Satz 4. $[\boldsymbol{GL}(\boldsymbol{V}^n), \boldsymbol{L}_2(\boldsymbol{V}^n)]$ *ist eine Transformationsgruppe mit der Wirkung*

$$(g, b)\in \boldsymbol{GL}(\boldsymbol{V}^n)\times \boldsymbol{L}_2(\boldsymbol{V}^n)\mapsto gb\in \boldsymbol{L}_2(\boldsymbol{V}^n)\,,$$

$$(gb)\,(\mathfrak{x}, \mathfrak{y}):=b(g^{-1}\mathfrak{x}, g^{-1}\mathfrak{y}), \qquad \mathfrak{x}, \mathfrak{y}\in \boldsymbol{V}\,. \tag{44}$$

Die Transformationen $l_g: b\mapsto gb$ *sind lineare Automorphismen der in Satz 2 angegebenen Vektorraumstruktur von* $\boldsymbol{L}_2(\boldsymbol{V}^n)$, *welche die Unterräume* $\boldsymbol{L}_2(\boldsymbol{V}^n)_a$ *und* $\boldsymbol{L}_2(\boldsymbol{V}^n)_s$ *invariant lassen. Bei festem Koordinatensystem ist die Matrix* (c_{ij}) *von* $c:=gb$ *durch*

$$(c_{ij})=(g_{ik})^*\,(b_{kl})\,(g_{lj})^{-1} \tag{45}$$

gegeben; (g_{ij}) *und* (b_{ij}) *die Matrix von g bzw. von b. Die durch Satz 1 definierten, von den Basen* $(\mathfrak{a}_i)$ *von* $\boldsymbol{V}^n$ *abhängigen Abbildungen* $b\in \boldsymbol{L}_2(\boldsymbol{V}^n)\mapsto (b_{ij})\in \mathbf{M}_n(K)$ *bilden einen der Transformationsgruppe* $[\boldsymbol{GL}(\boldsymbol{V}^n), \boldsymbol{L}_2(\boldsymbol{V}^n)]$ *angepaßten Atlas (analog für* $\boldsymbol{L}_2(\boldsymbol{V}^n)_a$, $\boldsymbol{L}_2(\boldsymbol{V}^n)_s$*).* □

Folgerung 2. *Der Rang von b,*

$$\operatorname{rg} b:=\operatorname{rg}(b_{ij})\,, \tag{46}$$

ist unabhängig von der Wahl der Koordinaten; er ist eine Invariante der Transformationsgruppe $[\boldsymbol{GL}(\boldsymbol{V}^n), \boldsymbol{L}_2(\boldsymbol{V}^n)]$.

Zum Beweis genügt es, an Übung 5.4 zu erinnern; ein anderer Beweis folgt unmittelbar aus Lemma 1 (siehe unten). □

Übung 4. Es sei $f: x\mapsto y=o+g(\vec{ox})+\mathfrak{a}$ eine affine Transformation von $\boldsymbol{A}^n$, $g\in \boldsymbol{GL}(\boldsymbol{V}^n)$, $\mathfrak{a}\in \boldsymbol{V}^n$. Man beweise: Das Bild $f(Q)$ der durch (17) definierten Quadrik Q ist wieder eine Quadrik $\bar{Q}$. Man finde eine Gleichung für $\bar{Q}=f(Q)$.

Wir wollen nun das Klassifikationsproblem für die Quadriken in Angriff nehmen und beweisen zuerst einen wichtigen Satz für Bilinearformen.

Satz 5. *Es sei* $b\in \boldsymbol{L}_2(\boldsymbol{V}^n)_s$ *eine symmetrische Bilinearform über* $\boldsymbol{V}^n$. *Dann gibt es eine Basis* $(\mathfrak{a}_i)$ *von* $\boldsymbol{V}^n$, *bezüglich der die Koordinatenmatrix* (b_{ij}) *von b Diagonalgestalt hat.*

Beweis. Ist $b=0$, so ist $b_{ij}=0$ für alle Basen $(\mathfrak{a}_i)$ und $i, j=1, \ldots, n$. Da hier die Behauptung trivial ist, können wir $b\neq 0$ voraussetzen. Aus (33) folgt, daß es dann auch einen Vektor geben muß — wir nennen ihn $\mathfrak{a}_n$ —, für den $b(\mathfrak{a}_n, \mathfrak{a}_n)\neq 0$ gilt. Wir betrachten den Unterraum

$$\boldsymbol{W}=\{\mathfrak{x} \mid \mathfrak{x}\in \boldsymbol{V},\ b(\mathfrak{a}_n, \mathfrak{x})=0\}\,. \tag{47}$$

Da b linear ist in $\mathfrak{x}$, ist die Abbildung $\mathfrak{x}\mapsto \mathfrak{w}(\mathfrak{x}):=b(\mathfrak{a}_n, \mathfrak{x})$ ein Element $\mathfrak{w}\in \boldsymbol{V}'$. Aus $\mathfrak{w}(\mathfrak{a}_n)=b(\mathfrak{a}_n, \mathfrak{a}_n)\neq 0$ folgt $\mathfrak{w}\neq \mathfrak{o}$, und (47) definiert den Annullator von $\mathfrak{L}(\mathfrak{w})$; $\boldsymbol{W}=\mathfrak{L}(\mathfrak{w})^{\perp}$ (vgl. Satz 6.3). Somit gilt $\dim \boldsymbol{W}=n-1$. Nun ist $b_1:=b \mid \boldsymbol{W}\times \boldsymbol{W}$ ebenfalls eine symmetrische Bilinearform $b_1\in \boldsymbol{L}_2(\boldsymbol{W})_s$, und wir können unseren Satz leicht durch Induktion beweisen. Für $n=0, 1$ ist der Satz trivial. Wegen $\dim \boldsymbol{W}=n-1$ finden wir nach Induktionsvoraussetzung eine Basis $(\mathfrak{a}_1, \ldots, \mathfrak{a}_{n-1})$ von $\boldsymbol{W}$ mit $b(\mathfrak{a}_\alpha, \mathfrak{a}_\beta)=0$ für $\alpha\neq\beta$, $\alpha, \beta=1, \ldots, n-1$. Aus der Definition von $\mathfrak{a}_n$ folgt $b(\mathfrak{a}_\alpha, \mathfrak{a}_n)=0$ für $\alpha=1, \ldots, n-1$. Wegen $b(\mathfrak{a}_n, \mathfrak{a}_n)\neq 0$ gilt $\mathfrak{a}_n\notin \boldsymbol{W}$, und daher ist $(\mathfrak{a}_i)$, $i=1, \ldots, n$, eine Basis von $\boldsymbol{V}$ mit der gewünschten Eigenschaft. Man beachte, daß genau $\operatorname{rg} b$ Elemente der Hauptdiagonale von 0 verschieden sind. Der Beweis zeigt, daß man durch schrittweisen Abbau der Dimension eine geeignete Basis $(\mathfrak{a}_i)$ durch Lösen homogener linearer Gleichungssysteme effektiv bestimmen kann. □

Folgerung 3. *Für $K=\mathbf{C}$ sind zwei symmetrische Bilinearformen $b, \hat{b}\in \boldsymbol{L}_2(\boldsymbol{V}^n)_s$ dann und nur dann $\boldsymbol{GL}(\boldsymbol{V}^n)$-äquivalent, wenn $\operatorname{rg} b=\operatorname{rg} \hat{b}$ gilt.*

Beweis. Die Notwendigkeit der Bedingung ist trivial (Folgerung 2). Es sei nun $\operatorname{rg}(b)=r$. Wir betrachten eine Basis $(\mathfrak{a}_i)$, für die (b_{ij}) die Gestalt

$$(b_{ij})=\begin{pmatrix} \lambda_1 & & & & & \mathbf{0} \\ & \lambda_2 & & & & \\ & & \ddots & & & \\ & & & \lambda_r & & \\ & & & & 0 & \\ \mathbf{0} & & & & & \ddots \\ & & & & & & 0 \end{pmatrix} \quad \text{mit} \quad \lambda_\varrho\neq 0,\ \varrho=1, \ldots, r\,,$$

besitzt; nach Satz 5 können wir nämlich die $\mathfrak{a}_i$ so wählen, daß (b_{ij}) Diagonalform hat, und durch eine geeignete Numerierung der Basisvektoren erhalten wir die angegebene Gestalt. Wir definieren nun die Basis $(\mathfrak{b}_i)$ durch eine einfache Normierung:

$$\mathfrak{b}_\varrho:=\mathfrak{a}_\varrho/\sqrt{\lambda_\varrho}, \qquad \varrho=1, \ldots, r, \qquad \mathfrak{b}_\sigma:=\mathfrak{a}_\sigma, \qquad \sigma=r+1, \ldots, n;$$

hierbei ist $\sqrt{\lambda_\varrho}$ eine der beiden in $\mathbf{C}$ existierenden Wurzeln (vgl. Folgerung 2.3.2) Dann gilt

$$\tilde{b}_{\varrho\varrho}:=b(\mathfrak{b}_\varrho, \mathfrak{b}_\varrho)=1, \qquad \varrho=1, \ldots, r\,,$$

und $\tilde{b}_{\alpha\beta}=0$ sonst. Daher hat bezüglich $(\mathfrak{b}_i)$ die Matrix $(\tilde{b}_{ij})$ der Bilinearform b die Normalform

$$(b_{ij}) = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & 0 & \\ & & & & \ddots \\ & & & & & 0 \end{pmatrix} \begin{matrix} \\ \\ \\ r \\ \\ \\ \end{matrix} \cdot \qquad (48)$$

$$\begin{matrix} & & & & & & \\ & & & & & & \\ & & & & & & \\ & & & r & & & \end{matrix}$$

Ebenso finden wir für $\hat{b}$ eine entsprechende Basis $(\hat{\mathfrak{b}}_i)$, bezüglich der b dieselbe Normalform (48) hat, und dann gilt $\hat{b} = gb$, wobei g die Transformation mit $g(\mathfrak{b}_i) = \hat{\mathfrak{b}}_i$ ist („Mitschleppen der Koordinaten"). □

Die symmetrischen Bilinearformen über $\mathbf{C}$ werden also einfach durch ihren Rang klassifiziert; es gibt $n+1$ verschiedene Klassen entsprechend den Werten $\operatorname{rg} b = r$, $0 \leqq r \leqq n$. Im Reellen ist die Situation etwas komplizierter:

Satz 6 (Trägheitssatz von SYLVESTER). *Im Fall $K = \mathbf{R}$ existiert zu jeder symmetrischen Bilinearform $b \in \boldsymbol{L}_2(\boldsymbol{V}^n)_s$ eine Basis $(\mathfrak{b}_i)$ derart, daß die Matrix (b_{ij}) die folgende Normalform besitzt:*

$$(b_{ij}) = \begin{pmatrix} -1 & & & & & & \\ & \ddots & & & & & \\ & & -1 & & & & \\ & & & 1 & & & \\ & & & & \ddots & & \\ & & & & & 1 & \\ & & & & & & 0 \\ & & & & & & & \ddots \\ & & & & & & & & 0 \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ l \\ \\ \\ \\ r \\ \\ \\ \end{matrix} \cdot \qquad (49)$$

$$\begin{matrix} & & & & & & & & \\ & & & & & & & & \\ & & l & & & r & & & \end{matrix}$$

Zwei Bilinearformen $b, \hat{b} \in \boldsymbol{L}_2(\boldsymbol{V}^n)_s$ sind genau dann $\boldsymbol{GL}(\boldsymbol{V}^n)$-äquivalent, wenn sie dieselbe Normalform besitzen.

Beweis. Die Existenz einer Basis mit (49) ergibt sich genauso wie für $K = \mathbf{C}$ in Folgerung 3; der einzige Unterschied ist, daß wir $\mathfrak{b}_\varrho := \mathfrak{a}_\varrho / \sqrt{|\lambda_\varrho|}$ setzen müssen, da in $\mathbf{R}$ die Wurzel nur für nicht negative Zahlen existiert. Man erhält dann $b(\mathfrak{b}_\varrho, \mathfrak{b}_\varrho) = \pm 1$. Durch eine Umnumerierung der Basiselemente können wir die Gestalt (49) erreichen. Als nächstes wollen wir beweisen, daß die Anzahl l der Elemente -1 in der Hauptdiagonale von (49) durch b eindeutig bestimmt ist und nicht von der Wahl der Basis $(\mathfrak{b}_i)$ abhängt. Damit ist der Beweis von Satz 6 im wesentlichen abgeschlossen: Zwei Bilinearformen mit derselben Normalform sind offenbar äquivalent („Zuordnung durch gleiche Koordinaten"), und zwei äquivalente Bilinearformen haben dieselbe Normalform („Mitschleppen der Koordinaten"). Wir erinnern daran, daß der Rang $r = \operatorname{rg} b$ nach Folgerung 2 eine Invariante und daher mit l auch die Anzahl $r - l$ der Elemente $b_{ii} = 1$ eindeutig bestimmt ist. Zum Nachweis der Eindeutigkeit von l formulieren wir zuerst ein allgemeines Lemma:

Lemma 1. *Es sei* $b \in L_2(V^n)$ (*K beliebig*). *Dann wird durch*

$$W_0 := \{\mathfrak{x} \in V^n \mid b(\mathfrak{x}, \mathfrak{y}) = 0 \text{ für alle } \mathfrak{y} \in V^n\} \tag{50}$$

ein Unterraum der Dimension

$$\dim W_0 = n - \operatorname{rg} b \tag{51}$$

definiert.

Beweis. Es sei (b_{ij}) die Matrix von b bezüglich einer beliebigen Basis $(\mathfrak{a}_i)$. Ein Vektor $\mathfrak{x} = \sum_{i=1}^{n} \mathfrak{a}_i \xi_i$ liegt in W_0 genau dann, wenn $\sum_{i,j} b_{ij} \xi_i \eta_j = 0$ für alle $\mathfrak{y} = \sum_i \mathfrak{a}_j \eta_j \in V^n$, d. h. alle $(\eta_j) \in K^n$ gilt. Setzt man für (η_j) die Elemente der Standardbasis $\mathfrak{e}_k = (\delta_{jk}) \in K^n$, $k = 1, \ldots, n$, ein, so folgt:

$$\mathfrak{x} \in W_0 \Leftrightarrow \sum_{i=1}^{n} b_{ij} \xi_i = 0 \quad \text{für} \quad j = 1, \ldots, n .$$

Aus Satz 5.6 ergibt sich die Behauptung. □

Definition 5. Die Zahl $n - \operatorname{rg} b$ heißt der *Defekt von b*, und der durch (50) definierte Unterraum heißt der *Defektunterraum*. Eine Bilinearform heißt *nicht ausgeartet*, wenn $n = \operatorname{rg} b$, d. h. $W_0 = \{\mathfrak{o}\}$ gilt.

Offenbar ist b genau dann nicht ausgeartet, wenn für die Matrix (b_{ij}) von b bezüglich einer beliebigen Basis

$$\det (b_{ij}) \neq 0 \tag{52}$$

ist.

Definition 6. Es sei $K = \mathbf{R}$. Eine Bilinearform $b \in L_2(V^n)$, heißt *positiv* (bzw. *negativ*) *semidefinit*, wenn $b(\mathfrak{x}, \mathfrak{x}) \geqq 0$ (bzw. $\leqq 0$) für alle $\mathfrak{x} \in V^n$ gilt. Eine positiv (negativ) semidefinite Bilinearform b heißt *positiv* (bzw. *negativ*) *definit*, wenn gilt:

$$b(\mathfrak{x}, \mathfrak{x}) = 0 \Leftrightarrow \mathfrak{x} = \mathfrak{o} . \tag{53}$$

Nun können wir die eindeutige Bestimmtheit von l beweisen. Es sei $W_+ \subseteq V^n$ ein Unterraum maximaler Dimension mit der Eigenschaft, daß $b \mid W_+ \times W_+$ positiv definit ist. Analog bezeichne W_- einen Unterraum maximaler Dimension, für den $b \mid W_- \times W_-$ negativ definit ist. Wenn b in irgendeiner Basis die Normalform (49) besitzt, gilt offenbar

$$\dim W_- \geqq l, \qquad \dim W_+ \geqq r - l; \tag{54}$$

denn b ist auf $\mathfrak{L}(\{\mathfrak{b}_1, \ldots, \mathfrak{b}_l\})$ negativ definit. Wir behaupten, daß

$$V^n = W_- \oplus W_+ \oplus W_0 \tag{55}$$

gilt. Es sei $\mathfrak{x} \in (W_0 + W_+) \cap W_-$. Wegen $\mathfrak{x} \in W_-$ ist $b(\mathfrak{x}, \mathfrak{x}) \leqq 0$, und wegen $\mathfrak{x} \in W_0 + W_+$ folgt $\mathfrak{x} = \mathfrak{x}_0 + \mathfrak{x}_+$ mit $\mathfrak{x}_0 \in W_0$, $\mathfrak{x}_+ \in W_+$ und $b(\mathfrak{x}, \mathfrak{x}) = b(\mathfrak{x}_+, \mathfrak{x}_+) \geqq 0$, also $b(\mathfrak{x}, \mathfrak{x}) = 0$. Da $\mathfrak{x} \in W_-$ ist, muß nach (53) $\mathfrak{x} = \mathfrak{o}$ sein. Ferner gilt $W_0 \cap W_+ = \{\mathfrak{o}\}$, denn wegen

$\mathfrak{x} \in \boldsymbol{W}_0$ ist $b(\mathfrak{x}, \mathfrak{x}) = 0$, und wegen $\mathfrak{x} \in \boldsymbol{W}_+$ folgt hieraus $\mathfrak{x} = \mathfrak{o}$. Nach der auf Satz 3.2.3 folgenden Bemerkung (vgl. auch Beispiel 3.2.3) ist die Summe $\boldsymbol{W}_- + \boldsymbol{W}_+ + \boldsymbol{W}_0$ tatsächlich direkt. Aus (54) erhalten wir für die Dimension (vgl. (4.4.16))

$$n \geqq \dim(\boldsymbol{W}_- + \boldsymbol{W}_+ + \boldsymbol{W}_0) \geqq l + (r - l) + (n - r) = n .$$

Damit ist (55) bewiesen; ferner ist klar, daß diese Ungleichung und (54)

$$\dim \boldsymbol{W}_- = l \tag{56}$$

nach sich ziehen. Wir haben l somit eindeutig und unabhängig von der Wahl der Basis als Dimension von $\boldsymbol{W}_-$ charakterisiert. □

Definition 7. Die im Fall $K = \mathbf{R}$ nach Satz 6 der symmetrischen Bilinearform b eindeutig zugeordnete Zahl l heißt ihr *Index*. Ist $0 < l < \operatorname{rg} b$, so heißt b *indefinit*.

Folgerung 4. *Für $K = \mathbf{R}$ sind zwei Formen $b, \hat{b} \in \boldsymbol{L}_2(\boldsymbol{V}^n)_s$ genau dann $\boldsymbol{GL}(\boldsymbol{V}^n)$-äquivalent, wenn sie denselben Rang und denselben Index haben. Eine Form b ist positiv (bzw. negativ) definit dann und nur dann, wenn $\operatorname{rg} b = n$ und $l(b) = 0$ (bzw. $l(b) = n$) gilt.* □

Übung 5. Es sei $K = \mathbf{R}$, $b \in \boldsymbol{L}_2(\boldsymbol{V}^n)_s$, $\operatorname{rg} b = n$ und b indefinit. Man beweise: Es gibt Vektoren $\mathfrak{x} \in \boldsymbol{V}^n$, $\mathfrak{x} \neq \mathfrak{o}$, mit $b(\mathfrak{x}, \mathfrak{x}) = 0$.

Bevor wir uns der affinen Klassifikation der Quadriken zuwenden, beweisen wir noch einen einfachen Satz, der auch selbständiges Interesse verdient:

Satz 7. *Es sei $b \in \boldsymbol{L}_2(\boldsymbol{V}^n)_s$. Dann wird durch*

$$\varphi_b : \mathfrak{x} \in \boldsymbol{V} \mapsto \varphi_b(\mathfrak{x}) \in \boldsymbol{V}'$$

mit

$$(\varphi_b(\mathfrak{x}) \mid \mathfrak{y}) := b(\mathfrak{x}, \mathfrak{y}) \tag{57}$$

eine lineare Abbildung $\varphi_b \in \boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{V}')$ definiert, für die

$$\varphi_b' = \varphi_b \tag{58}$$

gilt. Umgekehrt bestimmt jede Abbildung $\varphi \in \boldsymbol{L}(\boldsymbol{V}, \boldsymbol{V}')$ mit der Eigenschaft (58) durch

$$b_\varphi(\mathfrak{x}, \mathfrak{y}) := (\varphi(\mathfrak{x}) \mid \mathfrak{y}) \tag{59}$$

eine symmetrische Bilinearform $b_\varphi \in \boldsymbol{L}_2(\boldsymbol{V}^n)_s$, wobei $b_{\varphi_b} = b$ und $\varphi_{b_\varphi} = \varphi$ gilt. Die durch (57) definierte Abbildung φ_b hat als Kern den Defektunterraum von b

$$\boldsymbol{W}_0 = \operatorname{Ker} \varphi_b , \tag{60}$$

und für das Bild von φ_b gilt

$$\operatorname{Im} \varphi_b = \boldsymbol{W}_0^\perp . \tag{61}$$

Beweis. Offenbar ist $\varphi_b(\mathfrak{x})$ linear in $\mathfrak{y}$, d. h. $\varphi_b(\mathfrak{x}) \in \boldsymbol{V}'$, und außerdem linear in $\mathfrak{x}$, d. h. $\varphi_b \in \boldsymbol{L}(\boldsymbol{V}^n, \boldsymbol{V}')$. Wir zeigen, daß (58) gilt: $\varphi_b' : (\boldsymbol{V}')' = \boldsymbol{V} \to \boldsymbol{V}'$ ist definiert

durch (vgl. (6.28))

$$(\mathfrak{x} \mid \varphi_b'(\mathfrak{z})) = (\varphi_b(\mathfrak{x}) \mid \mathfrak{z}) = b(\mathfrak{x}, \mathfrak{z}) = b(\mathfrak{z}, \mathfrak{x}) = (\varphi_b(\mathfrak{z}) \mid \mathfrak{x})$$

für alle $\mathfrak{x}, \mathfrak{z} \in \boldsymbol{V}$, und hieraus folgt (58). Umgekehrt ist die Symmetrie der durch (59) definierten Bilinearform eine Folge von (58). Wir bemerken, daß φ_b und b in jeder Basis $(\mathfrak{a}_i)$ dieselbe Matrix (b_{ij}) besitzen, ebenso φ und b_φ. Hieraus folgen $b_{\varphi_b} = b$ und $\varphi_{b_\varphi} = \varphi$. Zum Beweis von (60) sei $\mathfrak{x} \in \operatorname{Ker} \varphi_b$, d. h. $\varphi_b(\mathfrak{x}) = \mathfrak{o}$. Dann folgt $(\varphi_b(\mathfrak{x}) \mid \mathfrak{y}) = b(\mathfrak{x}, \mathfrak{y}) = 0$ für alle $\mathfrak{y} \in \boldsymbol{V}$, d. h. $\mathfrak{x} \in \boldsymbol{W}_0$ und umgekehrt. Ist schließlich $\mathfrak{v} = \varphi_b(\mathfrak{x})$, so gilt $(\mathfrak{v} \mid \mathfrak{y}) = (\varphi_b(\mathfrak{x}) \mid \mathfrak{y}) = b(\mathfrak{x}, \mathfrak{y}) = 0$ für alle $\mathfrak{y} \in \boldsymbol{W}_0$, also ist $\operatorname{Im} \varphi_b \subseteq \boldsymbol{W}_0^\perp$. Andererseits gilt

$$\dim \operatorname{Im} \varphi_b = n - \dim \operatorname{Ker} \varphi_b = n - (n - r) = r = \dim \boldsymbol{W}_0^\perp,$$

wobei wir (60) und Satz 6.3 anwenden. Hieraus folgt (61). □

Wir kehren nun wieder zu den Quadriken zurück und definieren:

Definition 8. Eine Quadrik $Q \subseteq \boldsymbol{A}^n$ heißt *zentral*, wenn ein Punkt $o \in \boldsymbol{A}^n$ existiert, so daß mit $x \in Q$ auch $x' = o - \overrightarrow{ox} \in Q$ gilt; in diesem Fall heißt o ein *Zentrum von* Q.

Beispiel 3. Es seien x_1, x_2, x_3 affine Punktkoordinaten des $\boldsymbol{A}^3$. Dann definiert die Gleichung $x_1^2 + x_2^2 = a^2$, $a \in K$, $a \neq 0$, eine Quadrik, für die alle Punkte mit den Koordinaten $(0, 0, t)$, $t \in K$, Zentren sind. (Diese Quadrik nennt man einen *elliptischen Zylinder*.)

Satz 8. *Für die durch* (17) *definierte Quadrik sind folgende Aussagen äquivalent:*

1. *Q ist zentral.*
2. *$\mathfrak{v} \in \boldsymbol{W}_0^\perp$, $\boldsymbol{W}_0$ der Defektunterraum von b.*
3. *Es gibt einen Punkt $\hat{o} \in \boldsymbol{A}^n$, bezogen auf den Q durch eine Gleichung der Form*

$$b(\overrightarrow{\hat{o}x}, \overrightarrow{\hat{o}x}) + q = 0 \tag{62}$$

definiert wird.

Beweis. Wir beweisen die Äquivalenz durch die Schlüsse 2.⇒3.⇒1.⇒2. Wegen $\mathfrak{v} \in \boldsymbol{W}_0^\perp = \operatorname{Im} \varphi_b$ nach (61) ist auch $-\mathfrak{v}/2 \in \operatorname{Im} \varphi_b$; also gibt es ein $\mathfrak{a} \in \boldsymbol{V}$ mit $\varphi_b(\mathfrak{a}) = -\mathfrak{v}/2$. Nach (20) erhalten wir bei der Translation des Ursprungs $\hat{o} = o + \mathfrak{a}$ die Beziehung $\hat{\mathfrak{v}} = \mathfrak{v} + 2\varphi_b(\mathfrak{a}) = \mathfrak{o}$, und hieraus folgt die Bedingung 3. Der Schluß 3.⇒1. ist trivial: $\hat{o}$ ist ein Zentrum. Um 1.⇒2. zu zeigen, nehmen wir $\mathfrak{v} \notin \boldsymbol{W}_0^\perp$ an und beweisen, daß Q dann nicht zentral sein kann. Wegen $\mathfrak{v} \notin \boldsymbol{W}_0^\perp$ finden wir ein $\mathfrak{x} \in \boldsymbol{W}_0$ mit $\mathfrak{v}(\mathfrak{x}) \neq 0$. Dann gibt es zu jedem $\mathfrak{y} \in \boldsymbol{V}^n$ ein eindeutig bestimmtes $\lambda \in K$ so, daß der Punkt z mit $\overrightarrow{oz} = \mathfrak{y} + \mathfrak{x}\lambda$ in Q liegt. (Geometrische Deutung: Jede Gerade parallel zu $\mathfrak{x}$ schneidet Q in genau einem Punkt.) Wegen $\mathfrak{x} \in \boldsymbol{W}_0$ gilt nämlich

$$b(\mathfrak{y} + \mathfrak{x}\lambda, \mathfrak{y} + \mathfrak{x}\lambda) + \mathfrak{v}(\mathfrak{y}) + \lambda\mathfrak{v}(\mathfrak{x}) + q = b(\mathfrak{y}, \mathfrak{y}) + \mathfrak{v}(\mathfrak{y}) + q + \lambda\mathfrak{v}(\mathfrak{x}),$$

und der letzte Ausdruck gleich 0 gesetzt, bestimmt $\lambda \in K$ eindeutig. Da $b \neq 0$ gilt, können wir gewiß ein $\mathfrak{y} \in \boldsymbol{V}$ mit $b(\mathfrak{y}, \mathfrak{y}) + q \neq 0$ finden. Bestimmen wir den zugehörigen Punkt $z \in Q$ mit $\mathfrak{z} := \overrightarrow{oz} = \mathfrak{y} + \mathfrak{x}\lambda$, so gilt $z' = o - \overrightarrow{oz} \notin Q$; denn wegen $\overrightarrow{oz'} = -\mathfrak{z}$ folgte aus $b(-\mathfrak{z}, -\mathfrak{z}) = b(\mathfrak{z}, \mathfrak{z})$ und $z' \in Q$ sofort $\mathfrak{v}(\mathfrak{z}) = 0$, was wegen $b(\mathfrak{z}, \mathfrak{z}) + q = b(\mathfrak{y}, \mathfrak{y}) + q \neq 0$ nicht möglich ist. Daher kann der Punkt $o \in \boldsymbol{A}^n$ kein Zentrum von Q sein. Weil o ganz beliebig war, kann folglich überhaupt kein Punkt des $\boldsymbol{A}^n$ Zentrum von Q sein, d. h., Q ist nicht zentral; man beachte, daß die Bedingung 2 wegen (19) und (61) unabhängig von der Wahl des Ursprungs o ist. □

Folgerung 5. *Hat eine Quadrik Q eine Darstellung* (17) *mit* $\operatorname{rg} b = \dim \boldsymbol{A}^n = n$, *so ist Q zentral.*

Zum Beweis genügt es zu bemerken, daß in diesem Fall $\boldsymbol{W}_0^{\perp} = \boldsymbol{V}'$ gilt. Man beachte jedoch, daß auch hier $Q = \emptyset$ gelten kann (vgl. (9)). □

Übung 6. Es sei $Q \neq \emptyset$ definiert durch (17). Man beweise: a) Der Punkt o ist Zentrum von Q dann und nur dann, wenn $\mathfrak{v} = \mathfrak{o}$ gilt. (Hinweis. Falls $\mathfrak{v} \neq \mathfrak{o}$ ist, wähle man eine Basis von $\boldsymbol{V}^n$ so, daß $\mathfrak{v}(\mathfrak{x}) = \xi_n$ die n-te Komponente von $\mathfrak{x}$ wird, und zeige indirekt, daß o dann kein Zentrum sein kann.) — b) Ist $\boldsymbol{W}_0$ der Defektunterraum von b und o ein Zentrum von Q, so ist die Ebene $o + \boldsymbol{W}_0$ die Menge aller Zentren von Q; im Fall $\operatorname{rg} b = n$ ist also das Zentrum eindeutig bestimmt. — c) Ist $\sum_{i,j=1}^{n} b_{ij} x_i x_j + q = 0$ die Gleichung einer Quadrik Q bezogen auf ein Zentrum o, so ändert sich diese Gleichung bei der Wahl eines anderen Zentrums o von Q als Ursprung nicht.

Satz 9. *Es sei $\boldsymbol{A}^n$ ein affiner Raum über einem Körper K mit* $\operatorname{char} K \neq 2$. *Dann läßt sich zu jeder Quadrik* (17) *ein n-Bein* $(o; \mathfrak{a}_i)$ *so angeben, daß die Koordinatendarstellung von* (17) *eine der folgenden ist:*

$$\text{(I)} \qquad \sum_{\alpha=1}^{r} \lambda_\alpha x_\alpha^2 - 1 = 0; \tag{63}$$

$$\text{(II)} \qquad \sum_{\alpha=1}^{r} \lambda_\alpha x_\alpha^2 = 0; \tag{64}$$

$$\text{(III)} \qquad \sum_{\alpha=1}^{r} \lambda_\alpha x_\alpha^2 + x_{r+1} = 0\,. \tag{65}$$

Dabei gilt $\lambda_\alpha \neq 0$ und $r = \operatorname{rg} b$.

Beweis. Nach Satz 5 können wir zunächst einmal die angegebene Diagonalgestalt von b durch eine geeignete Wahl der $\mathfrak{a}_i$ erreichen. Ist Q zentral, so ergibt sich bezüglich eines Zentrums o die Gestalt (63) oder (64) aus (62), je nachdem, ob $q \neq 0$ oder $q = 0$ gilt. Im ersten Fall multiplizieren wir die Gleichung mit $-q^{-1}$, um auf (63) zu kommen. Im nichtzentralen Fall ist $\mathfrak{v} \notin \boldsymbol{W}_0^{\perp}$. Bei der gewählten Basis gilt also für Q eine Gleichung der Form

$$\sum_{\alpha=1}^{r} \lambda_\alpha x_\alpha^2 + \sum_{\alpha=1}^{r} q_\alpha x_\alpha + \sum_{\varrho=r+1}^{n} q_\varrho x_\varrho + q = 0\,, \tag{66}$$

wobei wenigstens ein $q_\varrho \neq 0$ ist. Wegen $\lambda_\alpha \neq 0$ können wir die Translation des Ur-

sprungs

$$\hat{x}_\alpha = x_\alpha + \frac{q_\alpha}{2\lambda_\alpha}, \qquad \hat{x}_\varrho = x_\varrho, \qquad \alpha = 1, \ldots, r, \qquad \varrho = r+1, \ldots, n,$$

ausführen. Dann nimmt (66) die Form

$$\sum_{\alpha=1}^{r} \lambda_\alpha \hat{x}_\alpha^2 + \sum_{\varrho=r+1}^{n} q_\varrho \hat{x}_\varrho + \hat{q} = 0 \tag{67}$$

an, wobei wir durch geeignete Numerierung der Koordinaten $q_{r+1} \neq 0$ voraussetzen können. Wir erhalten dann durch die affine Koordinatentransformation

$$x_i' = \hat{x}_i \quad \text{für} \quad i \neq r+1, \qquad x_{r+1}' = \sum_{\varrho=r+1}^{n} q_\varrho \hat{x}_\varrho + \hat{q}, \tag{68}$$

die Gestalt (65); die Determinante der Koordinatentransformation (68) ist nämlich gleich $q_{r+1} \neq 0$. □

Es ist klar, daß innerhalb einer der Typen (I), (II) oder (III) dieselbe Quadrik je nach Wahl der n-Beine durch verschiedene Gleichungen beschrieben werden kann, oder, anders ausgedrückt: Es kann der Fall eintreten, daß zwei Quadriken von demselben Typ, aber mit verschiedenen λ_α, affin-kongruent sind. Wir beweisen jedoch, daß Quadriken verschiedener Typen nicht affin-kongruent sein können:

Satz 10. *Zwei affin-kongruente Quadriken $Q, \hat{Q} \subseteq \boldsymbol{A}^n$ haben denselben Typ* (I), (II) *oder* (III) (*aus Satz* 9). *Dabei hat Q den Typ* (III) *genau dann, wenn Q nicht zentral ist, den Typ* (I) *genau dann, wenn Q zentral ist und kein Zentrum z von Q auf Q liegt, und den Typ* (II) *genau dann, wenn Q zentral ist und ein Zentrum $z \in Q$ existiert; in diesem Fall liegt jedes Zentrum auf Q.*

Beweis. Offenbar folgt die erste Behauptung aus der zweiten; denn der Begriff Zentrum ist affin invariant, und die Fälle schließen sich gegenseitig aus. Ist Q vom Typ (III), so ist $\mathfrak{v} = \mathfrak{u}_{r+1} \notin \boldsymbol{W}_0^\perp$; denn es gilt $\boldsymbol{W}_0 = \mathfrak{L}(\{\mathfrak{a}_{r+1}, \ldots, \mathfrak{a}_n\})$ und $\langle \mathfrak{u}_{r+1}, \mathfrak{a}_{r+1} \rangle = 1$, wobei $(\mathfrak{u}_i)$ die zu $(\mathfrak{a}_i)$ duale Basis ist. Eine Quadrik vom Typ (II) hat $o \in Q$ als Zentrum, und nach Übung 6c) liegt jedes Zentrum z von Q auf Q. Eine Quadrik vom Typ (I) hat o als Zentrum, wobei $o \notin Q$ gilt; nach dem eben Bewiesenen kann dann aber kein Zentrum von Q auf Q liegen. Weil unsere Fallunterscheidung eine vollständige Disjunktion ist, ergibt sich die Behauptung. □

Schon im Fall $K = \mathbf{R}$ braucht eine Gleichung der Form (17) keine Lösung $x \in \boldsymbol{A}^n$ zu haben; im Fall $K = \mathbf{Q}$ ist es noch schwieriger, sich einen Überblick über alle *rationalen Punkte* einer Quadrik zu verschaffen, dieses Problem und seine Verallgemeinerungen werden in der Zahlentheorie und der algebraischen Geometrie behandelt. Für die Körper $K = \mathbf{R}, \mathbf{C}$ können wir jedoch leicht die affine Klassifikation der Quadriken durchführen.

Satz 11. *Im Fall $K = \mathbf{R}$ können wir jede Quadrik $Q \subseteq \boldsymbol{A}^n$ bei geeigneter Wahl der affinen Punktkoordinaten durch eine Gleichung in einer der folgenden Normalformen*

charakterisieren:

$$\text{(I)} \quad -\sum_{\alpha=1}^{l} x_\alpha^2 + \sum_{\beta=l+1}^{r} x_\beta^2 - 1 = 0, \qquad 0 \leqq l \leqq r, \qquad 1 \leqq r \leqq n; \tag{69}$$

$$\text{(II)} \quad -\sum_{\alpha=1}^{l} x_\alpha^2 + \sum_{\beta=l+1}^{r} x_\beta^2 = 0, \qquad 0 \leqq l \leqq r/2, \qquad 1 \leqq r \leqq n; \tag{70}$$

$$\text{(III)} \quad -\sum_{\alpha=1}^{l} x_\alpha^2 + \sum_{\beta=l+1}^{r} x_\beta^2 + x_{r+1} = 0, \qquad 0 \leqq l \leqq r/2, \qquad 1 \leqq r \leqq n-1. \tag{71}$$

Die Quadriken vom Typ (I) *mit $r=l$ und nur diese sind imaginär. Zwei nicht imaginäre Quadriken sind genau dann affin-kongruent, wenn sie dieselbe Normalform haben, d. h., Typennummer $N=$(I), (II), (III), Rang r und Index l sind unter den angegebenen Einschränkungen ein vollständiges Invariantensystem der nicht imaginären Quadriken. Im Fall $K=\mathbf{C}$ sind zwei Quadriken genau dann affin-kongruent, wenn sie in Typennummer und Rang übereinstimmen.*

Beweis. Die Existenz der Normalform folgt für $K=\mathbf{R}$ unmittelbar aus Satz 6 und Satz 9 und für $K=\mathbf{C}$ aus Folgerung 3 und Satz 9; die Normalformen für $K=\mathbf{C}$ sind (69), (70), (71) mit $l=0$. Im Fall $K=\mathbf{R}$ ist noch zu bemerken, daß wir aus (64) durch Multiplikation der Gleichung mit -1 o. B. d. A. zu $l \leqq r/2$ kommen können; für (65) erreichen wir das durch Multiplikation mit -1 und die affine Koordinatentransformation $x_i' = x_i$ für $i \neq r+1$ und $x_{r+1}' = -x_{r+1}$. Die zweite Behauptung folgt unmittelbar aus der Gestalt der Normalformen. Wenn zwei Quadriken dieselbe Normalform besitzen, sind sie offenbar affin-kongruent (Zuordnung durch gleiche Koordinaten). Für die Umkehrung dieses Sachverhaltes genügt es wegen Satz 10 zu zeigen, daß nie zwei Quadriken desselben Typs, aber mit verschiedenen r oder l affin-kongruent sein können. Dazu ist es nötig, die Zahlen r, l geometrisch, d. h. unabhängig von den Koordinaten und der Wahl der Q bestimmenden Gleichung, zu charakterisieren. Für den Rang r gelingt das durch das folgende allgemeine Lemma, welches die in Satz 10 gegebene grobe Klassifikation im Fall eines beliebigen Körpers K, char $K \neq 2$, weiter verfeinert:

Lemma 2. *Es sei K ein Körper,* char $K \neq 2$, *$Q \subseteq \boldsymbol{A}^n$, $Q \neq \emptyset$, eine Quadrik vom Typ $N=$*(I), (II), (III) *(vgl. Satz* 9*),*

$$s := n-r, \quad \textit{falls} \quad N=\text{(I), (II)}, \quad \textit{und} \quad s := n-r-1, \quad \textit{falls} \quad N=\text{(III)}$$

gilt, $\boldsymbol{A}^n$ ein affiner Raum über K mit dem Vektorraum $\boldsymbol{V}^n$. Dann ist s die maximale Dimension eines Unterraumes $\boldsymbol{W} \subseteq \boldsymbol{V}$ derart, daß für alle $\mathfrak{a} \in \boldsymbol{W}$

$$t_{\mathfrak{a}}(Q) = Q + \mathfrak{a} = Q$$

gilt.

Beweis. Es sei $(o; \mathfrak{a}_i)$ ein n-Bein des $\boldsymbol{A}^n$, für das die Gleichung von Q eine der in Satz 9 angegebenen Normalformen hat. Dann ist $\boldsymbol{W}^s := \mathfrak{L}(\{\mathfrak{a}_{r+1}, \ldots, \mathfrak{a}_n\}) = \boldsymbol{W}_0$ für $N=$(I), (II) und $\boldsymbol{W}^s := \mathfrak{L}(\{\mathfrak{a}_{r+2}, \ldots, \mathfrak{a}_n\})$ für $N=$(III) ein Unterraum mit der geforderten Eigenschaft. (Man nennt die Quadriken mit $s>0$ *zylindrisch* und die

s-Ebenen $x+\boldsymbol{W}^s$ für $x\in Q$ ihre *Erzeugenden.*) Es bleibt zu zeigen, daß es keinen größeren derartigen Unterraum gibt. Wir beweisen sogar: Gilt $\mathfrak{a}\notin \boldsymbol{W}^s$, so ist $t_\mathfrak{a}(Q)\neq Q$. Für die zentralen Quadriken ist das einfach: Aus $t_\mathfrak{a}(Q)=Q$ folgt, daß auch die Menge der Zentren von Q in sich übergehen muß; nach Übung 6b) muß also $t_\mathfrak{a}(o+\boldsymbol{W}_0)=o+\boldsymbol{W}_0$, also $\mathfrak{a}\in \boldsymbol{W}_0=\boldsymbol{W}^s$ sein. Den Fall $N=(\mathrm{III})$ erledigen wir durch eine kleine Rechnung. Es seien (α_i) die Koordinaten eines Vektors $\mathfrak{a}$ mit $t_\mathfrak{a}(Q)=Q$. Ist also $x\in Q$, so muß auch $x+\mathfrak{a}\in Q$ sein, d. h., die Koordinaten müssen (65) erfüllen. Hieraus folgt,

$$c:=-\alpha_{r+1}-\sum_{\beta=1}^{r}\lambda_\beta\alpha_\beta^2=2\sum_{\beta=1}^{r}\lambda_\beta x_\beta\alpha_\beta$$

muß für alle $x\in Q$ gelten. Der Punkt $o\in Q$ ergibt $c=0$, und die Punkte mit den Koordinaten $x_{r+1}=-\lambda_\beta$, $x_\beta=1$ und $x_i=0$ für $i\neq r+1$, β führen auf $\lambda_\beta\alpha_\beta=0$, also $\alpha_\beta=0$, $\beta=1,\ldots,r$. Wegen $c=0$ folgt schließlich $\alpha_{r+1}=0$, und wir erhalten $\mathfrak{a}\in \boldsymbol{W}^s$. □

Weil klar ist, daß affin-kongruente Quadriken denselben Wert s, also auch denselben Rang r besitzen, ist r eine affine Invariante der Quadrik, und damit ist Satz 11 für $K=\mathbf{C}$ bewiesen.

Um den Fall $K=\mathbf{R}$ abzuschließen, müssen wir noch für l eine invariante geometrische Deutung finden. Da r schon als affin invariant nachgewiesen wurde, genügt es, für jeden Typ und jedes r eine l eindeutig bestimmende geometrische Eigenschaft anzugeben. Das geschieht in der folgenden Übung, deren Ausführung wir dem Leser empfehlen. □

Übung 7. Es sei $K=\mathbf{R}$. Man beweise: a) Ist Q eine Quadrik vom Typ (I) und Rang r, so ist $m:=n-r+l$ die maximale Dimension einer Ebene $\boldsymbol{H}$, die durch ein Zentrum $o\in Q$ geht und zu Q disjunkt ist; offenbar bestimmt $x_{l+1}=\ldots=x_r=0$ eine derartige Ebene. — b) Für eine Quadrik vom Typ (II) ist $m:=r-l$ die maximale Dimension einer Ebene $\boldsymbol{H}$ durch ein Zentrum o, für die $\boldsymbol{H}\cap Q=\{o\}$ gilt; $x_1=\ldots=x_l=x_{r+1}=\ldots=x_n=0$ bestimmt eine derartige Ebene. — c) Für eine Quadrik vom Typ (III) gibt es eine Hyperebene $\boldsymbol{H}^{n-1}\subset \boldsymbol{A}^n$ so, daß $Q_1:=Q\cap\boldsymbol{H}^{n-1}\subseteqq\boldsymbol{H}^{n-1}$ eine Quadrik vom Rang r, Typ (I) und Index $r-l$ in $\boldsymbol{H}^{n-1}$ ist; $x_{r+1}=1$ bestimmt eine derartige Hyperebene; jede durch eine beliebige Ebene $\boldsymbol{P}\subset\boldsymbol{A}^n$ ausgeschnittene Quadrik $\boldsymbol{P}\cap Q$ hat einen Index $l'\leqq r-l$. (Hinweis. Man benutze Satz 6 und den Dimensionssatz 4.6.3; ferner beachte man Übung 6c).)

Übung 8. Man beweise, daß die in Beispiel 1 mit $a_1=a_2=a=2p=1$ (vgl. Übung 2) beschriebenen Quadriken eine vollständige Serie der affinen Normalformen der ebenen reellen Quadriken darstellen.

Übung 9. Es sei Q eine Quadrik mit der Gleichung (1), wobei $q_{ij}=q_{ji}$ gelte. Man beweise: Q ist zentral genau dann, wenn

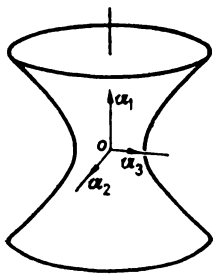
$$\mathrm{rg}\,(q_{ij},\,q_i)=\mathrm{rg}\,(q_{ij}),\qquad i,j=1,\ldots,n,$$

gilt.

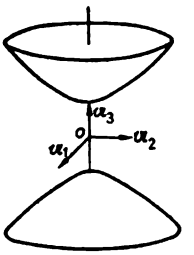
Beispiel 2. Wir wollen die Klassifikation nach Satz 11 für $K=\mathbf{R}$ und $n=3$ ausführen (vgl. Abb. 10).

I. Zentrale Quadriken vom Typ (I).

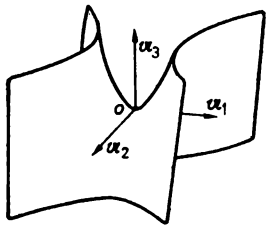
I.3. $r=3$ – nicht ausgeartete zentrale Quadriken



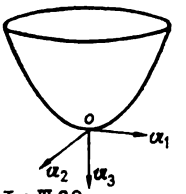
Typ I.3.1



Typ I.3.2



Typ III.2.1



Typ III.2.0

Abb.10

I.3.0: $x_1^2+x_2^2+x_3^2=1$, *Ellipsoid*;

I.3.1: $-x_1^2+x_2^2+x_3^2=1$, *einschaliges Hyperboloid*;

I.3.2: $-x_1^2-x_2^2+x_3^2=1$, *zweischaliges Hyperboloid*;

I.3.3. $-x_1^2-x_2^2-x_3^2=1$, imaginär

I.r. $r<3$ – ausgeartete (zylindrische) zentrale Quadriken;

I.2.0: $x_1^2+x_2^2=1$, *elliptischer Zylinder;*

I.2.1: $-x_1^2+x_2^2=1$, *hyperbolischer Zylinder*;

I.2.2.: $-x_1^2-x_2^2=1$, imaginär;

I.1.0: $x_1^2=1$, Paar paralleler Ebenen;

I.1.1: $-x_1^2=1$, imaginär.

II. Zentrale konische Quadriken

II.3.0: $x_1^2+x_2^2+x_3^2=0$, Punkt;

II.3.1: $-x_1^2+x_2^2+x_3^2=0$, *Kegel;*

II.2.0: $x_1^2+x_2^2=0$, Gerade (x_3-Achse);

II.2.1: $-x_1^2+x_2^2=0$, Paar sich schneidender Ebenen;

II.1.0: $x_1^2=0$, doppelt zählende Ebene.

III. Parabolische Quadriken

III.2.0: $x_1^2+x_2^2+x_3=0$, *elliptisches Paraboloid;*

III.2.1: $-x_1^2+x_2^2+x_3=0$, *hyperbolisches Paraboloid;*

III.1.0: $x_1^2+x_2=0$, *parabolischer Zylinder.*

Abschließend wollen wir noch einen für die Anwendungen in der Analysis besonders wichtigen Begriff einführen:

Definition 9. Es sei V ein Vektorraum über $\mathbf{C}$. Eine Abbildung

$$h: (\mathfrak{x}, \mathfrak{y}) \in V \times V \mapsto h(\mathfrak{x}, \mathfrak{y}) \in \mathbf{C}$$

heißt eine *hermitesche Form*, wenn sie folgende Eigenschaften besitzt:

1. $h(\mathfrak{x}, \mathfrak{y})$ ist linear in $\mathfrak{x}$.

2. Es gilt für alle $x, \mathfrak{y} \in V$

$$h(\mathfrak{y}, \mathfrak{x}) = \overline{h(\mathfrak{x}, \mathfrak{y})} \,. \tag{72}$$

Folgerung 6. *Für jede hermitesche Form gelten*

$$h(\mathfrak{x}, \mathfrak{y}_1+\mathfrak{y}_2) = h(\mathfrak{x}, \mathfrak{y}_1)+h(\mathfrak{x}, \mathfrak{y}_2) \,, \tag{73}$$

$$h(\mathfrak{x}, \mathfrak{y}z) = h(\mathfrak{x}, \mathfrak{y})\, \bar{z} \,, \tag{74}$$

$$h(\mathfrak{x}, \mathfrak{x}) \in \mathbf{R} \quad \textit{für alle} \quad \mathfrak{x}, \mathfrak{y}, \mathfrak{y}_1, \mathfrak{y}_2 \in V \quad \textit{und} \quad z \in \mathbf{C} \,. \ \square \tag{75}$$

Satz 12. *Es sei V^n ein n-dimensionaler Vektorraum über $\mathbf{C}$ und h eine hermitesche Form über V^n. Dann gehört zu jeder Basis $(\mathfrak{a}_i)$ von V^n die durch h eindeutig bestimmte Matrix*

$$(h_{ij}) := (h(\mathfrak{a}_i, \mathfrak{a}_j)) \in \mathbf{M}_n(\mathbf{C}); \tag{76}$$

diese Matrix ist hermitesch, d. h., sie erfüllt

$$(h_{ij})' = (\bar{h}_{ij}) \,. \tag{77}$$

Umgekehrt gehört zu jeder hermiteschen Matrix (h_{ij}) bei gegebener Basis $(\mathfrak{a}_i)$ genau eine hermitesche Form h, nämlich

$$h(\mathfrak{x}, \mathfrak{y}) := \sum_{i,j=1}^{n} h_{ij} \xi_i \bar{\eta}_j \tag{78}$$

für $\mathfrak{x} = \sum_i \mathfrak{a}_i \xi_i$, $\mathfrak{y} = \sum_i \mathfrak{a}_i \eta_i \in V^n$. $\square$

Der Beweis ist analog zu dem von Satz 1. Das Analogon zu Satz 2 formulieren wir in der folgenden Übungsaufgabe:

Übung 10. Man beweise: Durch die analog (28) mit $\alpha \in \mathbf{R}$ definierten Operationen wird die Menge $\mathfrak{H}(V^n)$ der hermiteschen Formen ein Vektorraum über $\mathbf{R}$. Es gilt $\dim \mathfrak{H}(V^n) = n^2$.

Wie in (32) können wir die zu der hermiteschen Form gehörende *quadratische hermitesche Funktion*

$$\mathfrak{x} \in V \mapsto h(\mathfrak{x}) := h(\mathfrak{x}, \mathfrak{x}) \in \mathbf{R} \tag{79}$$

bilden. Analog zu (33) ist dann die für jede hermitesche Form gültige Formel:

$$h(\mathfrak{x}, \mathfrak{y}) = \frac{1}{4}\left[h(\mathfrak{x}+\mathfrak{y}) - h(\mathfrak{x}-\mathfrak{y}) + \mathrm{i}\,(h(\mathfrak{x}+\mathrm{i}\mathfrak{y}) - h(\mathfrak{x}-\mathrm{i}\mathfrak{y}))\right]. \tag{80}$$

Wir können eine Wirkung von $\boldsymbol{GL}(\boldsymbol{V}^n)$ über $\mathfrak{H}(\boldsymbol{V}^n)$ durch

$$(a, h) \in \boldsymbol{GL}(\boldsymbol{V}^n) \times \mathfrak{H}(\boldsymbol{V}^n) \mapsto ah \in \mathfrak{H}(\boldsymbol{V}^n) \quad \text{mit}$$

$$ah(\mathfrak{x}, \mathfrak{y}) := h(a^{-1}\mathfrak{x}, a^{-1}\mathfrak{y}) \tag{81}$$

definieren und mit Hilfe von (80) die Analoga von Satz 5 und Satz 6 beweisen, was wir dem Leser überlassen wollen. Zusammenfassend formulieren wir

Satz 13. *Es sei h eine hermitesche Form über dem n-dimensionalen komplexen Vektorraum $\boldsymbol{V}^n$. Dann gibt es eine Basis $(\mathfrak{a}_i)$ von $\boldsymbol{V}^n$, bezüglich der die hermitesche Form h eine Matrix (h_{ij}) der Form* (49) *hat; Rang $r = \mathrm{rg}\,(h_{ij})$ und der Index l von h, d. h. die Anzahl der -1 in der Matrix* (49), *bilden ein vollständiges Invariantensystem der Transformationsgruppe $[\boldsymbol{GL}(\boldsymbol{V}^n), \mathfrak{H}(\boldsymbol{V}^n)]$ mit der Wirkung* (81). □

Bemerkung. Aus der Gestalt der Normalform ergibt sich unmittelbar, daß die Definitionen 5, 6, 7 auch für hermitesche Formen sinnvoll sind. Die Theorie der bilinearen Formen über $\mathbf{R}$ und der hermiteschen Formen über $\mathbf{C}$ ist weitgehend analog. Zum Beispiel gilt für beide folgendes *Kriterium für die Definitheit* (vgl. F. R. Gantmacher [1]): *Eine hermitesche Form (bzw. symmetrische Bilinearform über $\mathbf{R}$) ist genau dann positiv definit, wenn alle sogenannten Hauptminoren $M\begin{pmatrix}1 & \dots & p\\ 1 & \dots & p\end{pmatrix}$, $1 \leqq p \leqq n = \dim \boldsymbol{V}$ ihrer Matrix bezüglich einer beliebigen Basis von $\boldsymbol{V}^n$* (vgl. (4.8.8)) *positiv sind.*

Übung 11. Man beweise: a) Ein zu Lemma 1 analoges Lemma gilt für den durch $\hat{\boldsymbol{W}}_0 := \{\mathfrak{x} \in \boldsymbol{V}^n \mid b(\mathfrak{y}, \mathfrak{x}) = 0 \text{ für alle } \mathfrak{y} \in \boldsymbol{V}^n\}$ definierten Unterraum. — b) Im allgemeinen ist $\hat{\boldsymbol{W}}_0 \neq \boldsymbol{W}_0$. — c) Man formuliere und beweise Analoga zu Satz 7 in den Fällen, daß die Abbildung φ_b für alternierende oder für beliebige Bilinearformen definiert wird.

Übung 12. Es sei $b \in \boldsymbol{L}_2(\boldsymbol{V}^n)$ und $\boldsymbol{U} \subseteq \boldsymbol{V}^n$ ein Unterraum. Wir definieren $\boldsymbol{W}(\boldsymbol{U}) := \{\mathfrak{x} \in \boldsymbol{V}^n \mid b(\mathfrak{u}, \mathfrak{x}) = 0 \text{ für alle } \mathfrak{u} \in \boldsymbol{U}\}$. Man beweise: a) $\boldsymbol{W}(\boldsymbol{U})$ ist ein Unterraum von $\boldsymbol{V}^n$, für dessen Dimension $\dim \boldsymbol{W}(\boldsymbol{U}) \geqq n - \dim \boldsymbol{U}$ gilt; das Gleichheitszeichen steht hier genau dann für alle $\boldsymbol{U}$, wenn b nicht ausgeartet ist. — b) $b \mid \boldsymbol{U} \times \boldsymbol{U}$ ist genau dann nicht ausgeartet, wenn $\boldsymbol{V}^n = \boldsymbol{U} \oplus \boldsymbol{W}(\boldsymbol{U})$ gilt.

Übung 13. Es sei K ein Körper und $b \in \boldsymbol{L}_2(\boldsymbol{V}^n)_a$ eine alternierende Bilinearform über dem n-dimensionalen Vektorraum $\boldsymbol{V}^n$ mit dem Körper K. Man beweise: Der Rang $\mathrm{rg}\, b$ ist stets gerade, und zwei alternierende Bilinearformen sind genau dann $\boldsymbol{GL}(\boldsymbol{V}^n)$-äquivalent, wenn sie denselben Rang haben (vgl. Satz 4). Hinweis. Man zeige, daß es eine Basis $(\mathfrak{a}_i)$ von $\boldsymbol{V}^n$ gibt, bezüglich der die Matrix von $b \in \boldsymbol{L}_2(\boldsymbol{V}^n)_a$ die folgende Normal-

form hat:

$$(b_{ij}) = \begin{pmatrix} \begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix} & & & 0 \\ & \ddots & & \\ & & \begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix} & \\ 0 & & & \begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix} \\ 0 & \cdots & & 0 \end{pmatrix} \begin{matrix} \\ \\ \\ \\ 2r \end{matrix} \tag{82}$$

$2r$

6. Euklidische Geometrie

In diesem Kapitel wollen wir die elementare Geometrie durch Einführung eines Skalarproduktes abschließen, das es ermöglicht, die noch fehlenden Grundbegriffe wie Länge und Winkel, Metrik, Orthogonalität, Bewegungen und anderes zu definieren und im Fall $K = \mathbf{R}$, $n = 3$ die euklidische Geometrie des Anschauungsraumes durch Spezialisierung der affinen Geometrie herzuleiten. Für die wichtige Klasse der selbstadjungierten Operatoren werden wir ihre orthogonale Normalform bestimmen; diese Operatoren sind sämtlich diagonalisierbar. Als Anwendung erhalten wir hieraus die euklidische Klassifikation der Quadriken. Für die Funktionalanalysis ist die Ausdehnung eines Teils der Ergebnisse auf den Grundkörper $K = \mathbf{C}$ der komplexen Zahlen von Bedeutung. Das geschieht durch die Einführung der unitären Räume, die wir soweit wie möglich und notwendig parallel zu den euklidischen Vektorräumen behandeln.

§ 1. Euklidische und unitäre Räume

Wir beginnen mit einigen heuristischen Vorbemerkungen, für die wir die Elementargeometrie als bekannt voraussetzen. Dazu gehen wir wie in § 4.1 von dem natürlichen Koordinatensystem im Raum $\mathbf{R}^3$ der reellen Tripel aus. Deuten wir dieses Koordinatensystem euklidisch, so werden wir voraussetzen, daß auf den Achsen dieselbe Maßeinheit gewählt wurde und daß sie paarweise aufeinander senkrecht stehen (vgl. Abb. 4). Durch zweimalige Anwendung des Satzes von PYTHAGORAS erhalten wir für den Abstand $\varrho(o, x)$ des Punktes $x = (\xi_1, \xi_2, \xi_3) \in \mathbf{R}^3$ vom Ursprung o:

$$\varrho(o, x)^2 = \xi_1^2 + \xi_2^2 + \xi_3^2. \tag{1}$$

Betrachten wir nun in der Ebene $\mathbf{R}^2$ zwei Einheitsvektoren

$$\mathfrak{x} = (\xi_1, \xi_2), \qquad \mathfrak{y} = (\eta_1, \eta_2), \qquad \xi_1^2 + \xi_2^2 = \eta_1^2 + \eta_2^2 = 1\ ,$$

dann gibt es eindeutig bestimmte Winkel φ, ψ, $0 \leqq \varphi$, $\psi < 2\pi$, mit

$$\xi_1 = \cos\varphi, \qquad \xi_2 = \sin\varphi; \qquad \eta_1 = \cos\psi, \qquad \eta_2 = \sin\psi\ .$$

Für den Winkel $\alpha = \psi - \varphi$ zwischen $\mathfrak{x}$ und $\mathfrak{y}$ erhalten wir nach dem Additionstheorem für den Kosinus

$$\cos \alpha = \xi_1\eta_1 + \xi_2\eta_2 . \tag{2}$$

Die beiden Ausdrücke (1), (2) und viele andere geometrische Überlegungen führten darauf, daß die Funktion

$$(\mathfrak{x}, \mathfrak{y}) \in \mathbf{R}^n \times \mathbf{R}^n \mapsto \langle \mathfrak{x}, \mathfrak{y} \rangle := \sum_{i=1}^{n} \xi_i\eta_i \in \mathbf{R} \tag{3}$$

für die Begründung der euklidischen Geometrie von grundlegender Bedeutung ist. Zum Beispiel können wir statt (1) nun $\varrho(o, x)^2 = \langle \overrightarrow{ox}, \overrightarrow{ox} \rangle$ und statt (2) $\cos \alpha = \langle \mathfrak{x}, \mathfrak{y} \rangle$ schreiben. Es ist ganz offensichtlich, daß die Funktion (3) die folgenden Eigenschaften besitzt:

1. *Die Abbildung* $\langle\ ,\ \rangle$ *ist bilinear* (Definition 5.9.1);

2. *die Bilinearform* $\langle\ ,\ \rangle$ *ist symmetrisch:*

$$\langle \mathfrak{x}, \mathfrak{y} \rangle = \langle \mathfrak{y}, \mathfrak{x} \rangle, \qquad \mathfrak{x}, \mathfrak{y} \in V;$$

3. *die Bilinearform* $\langle\ ,\ \rangle$ *ist positiv definit* (Definition 5.9.6), *d. h., es gilt* $\langle \mathfrak{x}, \mathfrak{x} \rangle \geqq 0$ *und* $\langle \mathfrak{x}, \mathfrak{x} \rangle = 0$ *dann und nur dann, wenn* $\mathfrak{x} = \mathfrak{o}$ *ist.*

Aus den Sätzen 5.9.5 und 5.9.6 folgt leicht, daß es umgekehrt zu jeder Bilinearform $\langle\ ,\ \rangle$ eines n-dimensionalen Vektorraumes $\boldsymbol{V}^n$ über $\mathbf{R}$, welche die Eigenschaften 1 bis 3 besitzt, ein Vektorkoordinatensystem im $\boldsymbol{V}^n$ gibt, in dem $\langle\ ,\ \rangle$ die Normalform (3) besitzt. Da man aus einem derartigen Koordinatensystem, wie wir oben andeuteten, die Grundbegriffe der euklidischen Geometrie ablesen kann, wird man vermuten, daß die Einschränkung auf den Körper $K = \mathbf{R}$ und die Hinzunahme eines Skalarproduktes $\langle\ ,\ \rangle$ mit den Eigenschaften 1 bis 3 zu den Axiomen einer affinen Geometrie (Definition 4.3.1) es bereits gestatten, die euklidische Geometrie zu begründen. Es ist dabei wegen der zahlreichen Anwendungen wieder zweckmäßig, die Dimension nicht auf den Fall $n = 3$ einzuschränken. Auch der unendlichdimensionale Fall ist von großer Wichtigkeit für die Analysis.

Wir beginnen nun mit der exakten Durchführung dieses Programms und definieren:

Definition 1. Es sei $\boldsymbol{V}$ ein Vektorraum über $\mathbf{R}$. Ein Tripel $[\boldsymbol{V}, \mathbf{R}, \langle\ ,\ \rangle]$ heißt ein *euklidischer Vektorraum* und $\langle\ ,\ \rangle$ ein *Skalarprodukt* über $\boldsymbol{V}$, wenn $\langle\ ,\ \rangle$ eine symmetrische, positiv definite Bilinearform über $\boldsymbol{V}$ ist; sie erfüllt also die oben angegebenen Eigenschaften 1 bis 3. Ein Quadrupel $[\boldsymbol{E}, \boldsymbol{V}, \mathbf{R}, \langle\ ,\ \rangle]$ heißt eine *euklidische Geometrie,* wenn $[\boldsymbol{E}, \boldsymbol{V}, \mathbf{R}]$ eine affine Geometrie und $[\boldsymbol{V}, \mathbf{R}, \langle\ ,\ \rangle]$ ein euklidischer Vektorraum ist; $\boldsymbol{E}$ wird *euklidischer Raum* genannt.

Aus der Definition ist klar, daß alle Ergebnisse der affinen Geometrie auch in der euklidischen Geometrie gültig bleiben. Speziell können wir von der Dimension des euklidischen Raumes sprechen; wir nennen $\boldsymbol{E}$ n-dimensional, $n \in \mathbf{N}_0$ oder $n = \infty$,

und schreiben $\boldsymbol{E}=\boldsymbol{E}^n$ oder $\dim \boldsymbol{E}=n$, wenn $\dim \boldsymbol{V}=n$ gilt. Für die einfachen Betrachtungen in diesem Paragraphen benötigen wir jedoch keine Dimensionsvoraussetzungen; sie gelten auch im Fall $\dim \boldsymbol{E}=\infty$. Da viele Begriffsbildungen und Beweise im euklidischen und unitären Fall analog sind, ist es zweckmäßig, auch die unitären Räume schon jetzt zu definieren:

Definition 2. Ein Tripel $[\boldsymbol{V}, \mathbf{C}, \langle\ ,\ \rangle]$ heißt ein *unitärer Raum*, wenn $[\boldsymbol{V}, \mathbf{C}]$ ein Vektorraum über $\mathbf{C}$ und $\langle\ ,\ \rangle: \boldsymbol{V}\times\boldsymbol{V}\to\mathbf{C}$ eine positiv definite, hermitesche Form über $\boldsymbol{V}$ ist; $\langle\ ,\ \rangle$ heißt ein *Skalarprodukt* über $\boldsymbol{V}$.

Im folgenden wollen wir jedoch unter einem *unitären Raum* schlechthin entweder, wenn $K=\mathbf{C}$ ist, einen unitären Raum nach Definition 2, oder, wenn $K=\mathbf{R}$ ist, einen euklidischen Vektorraum verstehen. Häufig werden wir die Sätze nur für den Fall $K=\mathbf{C}$ beweisen; im Fall $K=\mathbf{R}$ gilt dann fast derselbe Beweis mit einigen Vereinfachungen.

Aus der Definition 5.9.9 einer hermiteschen Form folgt, daß das Skalarprodukt eines unitären Raumes über $\mathbf{C}$ durch die folgenden Eigenschaften charakterisiert wird:

1. a) $\langle \mathfrak{x}, \mathfrak{y}\rangle$ ist *linear* in $\mathfrak{x}$.

1. b) $\langle \mathfrak{x}, \mathfrak{y}\rangle$ ist *konjugiert-linear* in $\mathfrak{y}$, d. h., es gilt für $\mathfrak{x}, \mathfrak{y}_1, \mathfrak{y}_2\in\boldsymbol{V}$, $z_1, z_2\in\mathbf{C}$

$$\langle \mathfrak{x}, \mathfrak{y}_1 z_1+\mathfrak{y}_2 z_2\rangle=\langle \mathfrak{x}, \mathfrak{y}_1\rangle\,\bar{z}_1+\langle \mathfrak{x}, \mathfrak{y}_2\rangle\,\bar{z}_2\,. \tag{4}$$

2. Es gilt für alle $\mathfrak{x}, \mathfrak{y}\in\boldsymbol{V}$

$$\langle \mathfrak{y}, \mathfrak{x}\rangle=\overline{\langle \mathfrak{x}, \mathfrak{y}\rangle}\,. \tag{5}$$

3. Es gilt die Eigenschaft 3 von Definition 1.

Die letzte Forderung ist sinnvoll, weil aus (5) sofort $\langle \mathfrak{x}, \mathfrak{x}\rangle\in\mathbf{R}$ folgt.

Beispiel 1. Es sei $\boldsymbol{V}=\mathbf{R}$ der eindimensionale reelle Vektorraum. Dann ist das gewöhnliche Produkt $(\alpha, \beta)\mapsto\langle\alpha, \beta\rangle:=\alpha\cdot\beta$ gleichzeitig ein Skalarprodukt. Für $\boldsymbol{V}=\mathbf{C}$ ist $(z, w)\in\mathbf{C}\times\mathbf{C}\mapsto z\cdot\bar{w}\in\mathbf{C}$ ein Skalarprodukt.

Beispiel 2. Es sei $\boldsymbol{V}$ der Raum der stetigen, auf einem abgeschlossenen, beschränkten Intervall $[\alpha, \beta]\subset\mathbf{R}$ definierten Funktionen mit Werten in $\mathbf{R}$ (bzw. $\mathbf{C}$). Dann wird $\boldsymbol{V}$ durch die Definition

$$(f, g)\in\boldsymbol{V}\times\boldsymbol{V}\quad \langle f, g\rangle:=\int_\alpha^\beta f\cdot g\,dx\in\mathbf{R}$$

$$\left(\text{bzw. } \langle f, g\rangle:=\int_\alpha^\beta f\cdot\bar{g}\,dx\in\mathbf{C}\right)$$

ein unitärer Vektorraum. Dieses Beispiel besitzt viele Varianten und Verallgemeinerungen, die in der Funktionalanalysis untersucht werden.

Übung 1. Man beweise, daß es in einem n-dimensionalen unitären Raum $\boldsymbol{V}^n$ stets eine Basis (a_i) gibt, bezüglich der das Skalarprodukt der Vektoren $\mathfrak{x}=\sum_i a_i\xi_i$ und $\mathfrak{y}=\sum_i a_i\eta_i$ die Koordinatendarstellung

$$\langle \mathfrak{x}, \mathfrak{y}\rangle = \sum_i \xi_i\bar{\eta}_i \tag{6}$$

besitzt. Umgekehrt, ist (a_i) eine Basis in $\boldsymbol{V}^n$ und definiert man eine Funktion $\langle\ ,\ \rangle$: $\boldsymbol{V}^n\times\boldsymbol{V}^n\to\mathbf{C}$ durch (6), so wird $[\boldsymbol{V}^n, \mathbf{C}, \langle\ ,\ \rangle]$ ein unitärer Raum. (Hinweis. Man beachte die Sätze 5.9.12, 5.9.13.)

Satz 1. *Es sei $\boldsymbol{V}$ ein unitärer Vektorraum und $\boldsymbol{W}\subseteq\boldsymbol{V}$ ein Unterraum. Dann ist $\langle\ ,\ \rangle \mid \boldsymbol{W}\times\boldsymbol{W}$ ein Skalarprodukt über $\boldsymbol{W}$.* □

Der Beweis von Satz 1 ist trivial. Im folgenden werden wir für Unterräume immer die durch $\langle\ ,\ \rangle \mid \boldsymbol{W}\times\boldsymbol{W}$ definierte unitäre Struktur betrachten. Für den Aufbau der euklidischen Geometrie ist die *Ungleichung von Cauchy-Schwarz-Bunjakovskij*, die wir beweisen wollen, von grundlegender Bedeutung:

Satz 2. *Es sei $\boldsymbol{V}$ ein unitärer Vektorraum. Dann gilt für alle $\mathfrak{x}, \mathfrak{y}\in\boldsymbol{V}$*

$$|\langle \mathfrak{x}, \mathfrak{y}\rangle|^2 \leqq \langle \mathfrak{x}, \mathfrak{x}\rangle \langle \mathfrak{y}, \mathfrak{y}\rangle; \tag{7}$$

das Gleichheitszeichen gilt in (7) genau dann, wenn $\mathfrak{x}, \mathfrak{y}$ linear abhängig sind.

Beweis. Wir betrachten nur den Fall $K=\mathbf{C}$. Wegen der positiven Definitheit ist für alle $z\in\mathbf{C}$

$$0\leqq\langle \mathfrak{x}-\mathfrak{y}z, \mathfrak{x}-\mathfrak{y}z\rangle = \langle \mathfrak{x}, \mathfrak{x}\rangle - \langle \mathfrak{x}, \mathfrak{y}\rangle \bar{z} - \langle \mathfrak{y}, \mathfrak{x}\rangle z + \langle \mathfrak{y}, \mathfrak{y}\rangle z\bar{z}\,. \tag{8}$$

Gilt $\mathfrak{y}=\mathfrak{o}$, so sind in (7) beide Seiten 0, und $\mathfrak{x}, \mathfrak{y}$ sind linear abhängig. Es sei also $\mathfrak{y}\neq\mathfrak{o}$. Wir setzen $z=\langle \mathfrak{x}, \mathfrak{y}\rangle/\langle \mathfrak{y}, \mathfrak{y}\rangle$ und erhalten die Ungleichung (7) durch eine einfache Rechnung unter Berücksichtigung von (5) und $z\cdot\bar{z}=|z|^2$ für alle $z\in\mathbf{C}$. Sind $\mathfrak{x}, \mathfrak{y}$ linear unabhängig, so gilt wegen der Eigenschaft 3 für alle $z\in\mathbf{C}$ in (8) und folglich auch in (7) das Zeichen $<$. Sind $\mathfrak{x}, \mathfrak{y}$ linear abhängig, so gibt es wegen $\mathfrak{y}\neq\mathfrak{o}$ ein $c\in\mathbf{C}$ mit $\mathfrak{x}=\mathfrak{y}c$; es folgt

$$|\langle \mathfrak{x}, \mathfrak{y}\rangle|^2 = \langle \mathfrak{x}, \mathfrak{x}\rangle^2 |c|^2 = \langle \mathfrak{x}, \mathfrak{x}\rangle^2 c\bar{c} = \langle \mathfrak{x}, \mathfrak{x}\rangle \langle \mathfrak{y}, \mathfrak{y}\rangle\,. \quad \square$$

Wir definieren nun die *Norm* $|\mathfrak{x}|$ eines Vektors $\mathfrak{x}$ eines unitären Raumes $\boldsymbol{V}$ durch

$$\mathfrak{x}\in\boldsymbol{V}\mapsto |\mathfrak{x}| := \sqrt{\langle \mathfrak{x}, \mathfrak{x}\rangle}\in\mathbf{R}; \tag{9}$$

statt Norm sagt man auch „*Betrag*" oder „*Länge*". Man spricht allgemein von einem *normierten Vektorraum* $\boldsymbol{V}$ (mit $K=\mathbf{R}$ oder $K=\mathbf{C}$), wenn über $\boldsymbol{V}$ eine Funktion $\mathfrak{x}\in\boldsymbol{V}\mapsto|\mathfrak{x}|\in\mathbf{R}$ gegeben ist, welche die folgenden Eigenschaften besitzt:

1. *Für alle $\mathfrak{x}\in\boldsymbol{V}$ gilt $|\mathfrak{x}|\geqq 0$; dabei ist $|\mathfrak{x}|=0$ dann und nur dann, wenn $\mathfrak{x}=\mathfrak{o}$ ist.*
2. *Für alle $\mathfrak{x}\in\boldsymbol{V}$ und $z\in K$ $(=\mathbf{R}, \mathbf{C})$ gilt*

   $$|\mathfrak{x}z| = |\mathfrak{x}|\,|z|.$$

3. *Für alle $\mathfrak{x}, \mathfrak{y}\in\boldsymbol{V}$ gilt die Dreiecksungleichung*

   $$|\mathfrak{x}+\mathfrak{y}| \leqq |\mathfrak{x}|+|\mathfrak{y}|\,. \tag{10}$$

Diese drei Eigenschaften haben eine unmittelbar einleuchtende geometrische Bedeutung. Wir beweisen

Satz 3. *In einem unitären Vektorraum erfüllt die durch* (9) *definierte Funktion die Eigenschaften* 1 *bis* 3 *einer Norm; gilt in* (10) *das Gleichheitszeichen, so sind* $\mathfrak{x}$, $\mathfrak{y}$ *linear abhängig.*

Beweis. Die Eigenschaft 1 der Norm ergibt sich unmittelbar aus der positiven Definitheit, Eigenschaft 3, des Skalarproduktes. Aus $\langle \mathfrak{x}z, \mathfrak{x}z\rangle = \langle \mathfrak{x}, \mathfrak{x}\rangle z\bar{z} = |\mathfrak{x}|^2 |z|^2$ erhält man Eigenschaft 2. Zum Beweis von Eigenschaft 3 benutzen wir die Ungleichung (7):

$$|\mathfrak{x}+\mathfrak{y}|^2 = \langle \mathfrak{x}+\mathfrak{y}, \mathfrak{x}+\mathfrak{y}\rangle = |\mathfrak{x}|^2 + |\mathfrak{y}|^2 + \langle \mathfrak{x}, \mathfrak{y}\rangle + \langle \mathfrak{y}, \mathfrak{x}\rangle$$
$$= |\mathfrak{x}|^2 + |\mathfrak{y}|^2 + 2R(\langle \mathfrak{x}, \mathfrak{y}\rangle) .$$

Nun ist für jede komplexe Zahl z offenbar

$$R(z) \leqq |z| = \sqrt{R^2(z) + I^2(z)}; \tag{11}$$

also gilt

$$R(\langle \mathfrak{x}, \mathfrak{y}\rangle) \leqq |\langle \mathfrak{x}, \mathfrak{y}\rangle| . \tag{12}$$

Schreiben wir die Cauchy-Schwarz-Bunjakovskijsche Ungleichung in der Form

$$|\langle \mathfrak{x}, \mathfrak{y}\rangle| \leqq |\mathfrak{x}|\, |\mathfrak{y}| , \tag{13}$$

so folgt aus dem oben Bewiesenen, daß $|\mathfrak{x}+\mathfrak{y}|^2 \leqq (|\mathfrak{x}| + |\mathfrak{y}|)^2$ gilt, wobei das Gleichheitszeichen genau dann eintritt, wenn in (12) und in (13) das Gleichheitszeichen steht, also wenn $R(\langle \mathfrak{x}, \mathfrak{y}\rangle) = \langle \mathfrak{x}, \mathfrak{y}\rangle \geqq 0$ ist und $\mathfrak{x}$, $\mathfrak{y}$ linear abhängig sind. □

Die Norm erlaubt es uns, in naheliegender Weise eine *Metrik* oder *Abstandsfunktion* ϱ über V einzuführen. Der Begriff eines metrischen Raumes ist einer der Grundbegriffe der allgemeinen Topologie; unter einem *metrischen Raum* versteht man ein Paar $[M, \varrho]$, in dem $M \neq \emptyset$ eine nichtleere Menge und $\varrho: M \times M \to \mathbf{R}$ eine Funktion ist, welche die folgenden Eigenschaften besitzt:

1. $\varrho(x, y) \geqq 0$; $\varrho(x, y) = 0$ *dann und nur dann, wenn* $x = y$ *ist* (*positive Definitheit*);
2. $\varrho(x, y) = \varrho(y, x)$ (*Symmetrie*);
3. $\varrho(x, z) \leqq \varrho(x, y) + \varrho(y, z)$; $x, y, z \in M$ (*Dreiecksungleichung*).

Satz 4. *Es sei* V *ein normierter Vektorraum. Dann wird durch*

$$\varrho(\mathfrak{x}, \mathfrak{y}) := |\mathfrak{y} - \mathfrak{x}| \tag{14}$$

eine Metrik über V *definiert.*

Beweis. Die Eigenschaft 1 folgt aus der positiven Definitheit der Norm. Die Eigenschaft 2 ergibt sich nach $\varrho(\mathfrak{y}, \mathfrak{x}) = |\mathfrak{x} - \mathfrak{y}| = |(\mathfrak{y} - \mathfrak{x})\,(-1)| = |\mathfrak{y} - \mathfrak{x}| = \varrho(\mathfrak{x}, \mathfrak{y})$ aus der Eigenschaft 2 der Norm, und die Dreiecksungleichung folgt aus $\mathfrak{z} - \mathfrak{x} = (\mathfrak{z} - \mathfrak{y}) + (\mathfrak{y} - \mathfrak{x})$ und (10). □

Folgerung 1. *In einem euklidischen Punktraum* $\boldsymbol{E}$ *wird durch*

$$\varrho(x, y) := |\overrightarrow{xy}|, \qquad x, y \in \boldsymbol{E}, \tag{15}$$

eine Metrik definiert. □

Zum Beweis genügt es, einen Ursprung $o \in \boldsymbol{E}$ zu fixieren und auf $\varrho(x, y) = \varrho(\overrightarrow{ox}, \overrightarrow{oy})$ Satz 4 anzuwenden. (15) entspricht dem Begriff des Abstandes zweier Punkte aus der Elementargeometrie.

Übung 2. Es seien x, y, z drei verschiedene Punkte des euklidischen Raumes. Man beweise: Gilt $\varrho(x, z) = \varrho(x, y) + \varrho(y, z)$, so sind x, y, z kollinear. An einem Beispiel zeige man, daß die Umkehrung dieses Satzes falsch ist. (Man überzeuge sich davon, daß die Beziehung $\varrho(x, z) = \varrho(x, y) + \varrho(y, z)$ damit gleichbedeutend ist, daß z *zwischen* x *und* y liegt, im Sinne einer beliebigen, auf der Geraden $\boldsymbol{H}(x, y)$ durch eine reelle Skala definierten linearen Ordnung.)

Es seien nun $\mathfrak{x}, \mathfrak{y} \in \boldsymbol{V}$ zwei von $\mathfrak{o}$ verschiedene Vektoren eines euklidischen Vektorraumes. Dann erhalten wir aus (13) wegen $|\mathfrak{x}|\,|\mathfrak{y}| \neq 0$

$$-1 \leqq \frac{\langle \mathfrak{x}, \mathfrak{y} \rangle}{|\mathfrak{x}|\,|\mathfrak{y}|} \leqq 1; \tag{16}$$

es gibt also genau einen Wert φ, für den

$$\cos \varphi = \frac{\langle \mathfrak{x}, \mathfrak{y} \rangle}{|\mathfrak{x}|\,|\mathfrak{y}|} \quad \text{mit} \quad 0 \leqq \varphi \leqq \pi \tag{17}$$

gilt; φ heißt der *Winkel* zwischen $\mathfrak{x}$ und $\mathfrak{y}$.

Es ist klar, daß man die Winkel zwischen zwei sich schneidenden Geraden, einer Geraden und einer sie schneidenden Ebene und andere in der Elementargeometrie auftretende Winkel auf den soeben definierten Winkelbegriff zurückführen kann. In § 3 werden wir noch den orientierten Winkel zwischen zwei Vektoren kennenlernen.

Übung 3. Es seien $\mathfrak{x}, \mathfrak{y}, \mathfrak{z}$ drei Vektoren des euklidischen Vektorraumes $\boldsymbol{V}$, für die $|\mathfrak{x}| = |\mathfrak{y}| = |\mathfrak{z}|$ und $|\mathfrak{y} - \mathfrak{x}| = 2|\mathfrak{x}|$ gelten. Man beweise $\langle \mathfrak{z} - \mathfrak{x}, \mathfrak{z} - \mathfrak{y} \rangle = 0$. (Hinweis. Sind die drei Vektoren verschieden, so ist die Behauptung der „Satz des THALES" der Elementargeometrie.)

Übung 4. Man beweise, daß die Definition (17) von $\cos \varphi$ mit der bekannten Definition des Kosinus $\cos \varphi$ = Ankathete/Hypotenuse verträglich ist.

Übung 5. Man beweise den Kosinussatz $c^2 = a^2 + b^2 - 2ab \cos \gamma$ für ein Dreieck mit den Seitenlängen a, b, c und dem der Seite c gegenüberliegenden Winkel γ.

§ 2. Orthogonalität

Bereits in der Elementargeometrie wird deutlich, daß neben dem gestreckten Winkel $\alpha = \pi$ auch der rechte Winkel $\alpha = \pi/2$ eine besondere Bedeutung besitzt. Etwas allgemeiner als Rechtwinkligkeit ist der Begriff der Orthogonalität, der auch im Fall $K = \mathbf{C}$ gültig ist:

Definition 1. Es sei V ein unitärer Raum. Die Vektoren $\mathfrak{x}, \mathfrak{y} \in V$ heißen zueinander *orthogonal*, wenn $\langle \mathfrak{x}, \mathfrak{y} \rangle = 0$ gilt. Zwei Unterräume $U, W \subseteq V$ heißen zueinander *orthogonal*, wenn für alle $\mathfrak{x} \in U$ und $\mathfrak{y} \in W$ die Beziehung $\langle \mathfrak{x}, \mathfrak{y} \rangle = 0$ gilt; in diesem Fall schreiben wir auch $\langle U, W \rangle = 0$.

In einem euklidischen Vektorraum sind also $\mathfrak{x}, \mathfrak{y}$ genau dann zueinander orthogonal, wenn $\mathfrak{x}$ oder $\mathfrak{y}$ gleich $\mathfrak{o}$ sind oder, im Fall $\mathfrak{x} \neq \mathfrak{o}$, $\mathfrak{y} \neq \mathfrak{o}$, wenn sie aufeinander senkrecht stehen.

Beispiel 1. Es sei V^n ein n-dimensionaler unitärer Raum und $(\mathfrak{a}_i)$ eine *beliebige* Basis von V^n. Nach (5.9.76), (5.9.78) hat das Skalarprodukt die Basisdarstellung

$$\text{im Fall } K = \mathbf{C}: \qquad \langle \mathfrak{x}, \mathfrak{y} \rangle = \sum_{i,j=1}^{n} g_{ij} \xi_i \bar{\eta}_j \tag{1}$$

$$\text{und im Fall } K = \mathbf{R}: \qquad \langle \mathfrak{x}, \mathfrak{y} \rangle = \sum_{i,j=1}^{n} g_{ij} \xi_i \eta_j \,, \tag{2}$$

wobei (ξ_i) bzw. (η_i) die Koordinaten von $\mathfrak{x}$ bzw. $\mathfrak{y}$ sind und

$$g_{ij} := \langle \mathfrak{a}_i, \mathfrak{a}_j \rangle \tag{3}$$

gilt. Im Fall $K = \mathbf{R}$ erhalten wir für g_{ij} nach (1.17)

$$g_{ij} = |\mathfrak{a}_i| \, |\mathfrak{a}_j| \cos \alpha_{ij} \,, \tag{4}$$

wobei α_{ij} der Winkel zwischen $\mathfrak{a}_i$ und $\mathfrak{a}_j$ ist. Es folgt: Eine Basis des unitären Raumes V^n besteht genau dann aus paarweise orthogonalen Vektoren, wenn die Matrix (g_{ij}) der Koordinatendarstellung des Skalarproduktes Diagonalform hat, wenn also $g_{ij} = 0$ für $i \neq j$ gilt.

Definition 2. Eine Vektorfamilie $(\mathfrak{a}_i)_{i \in I}$ heißt *orthonormiert*, wenn für alle $i, j \in I$

$$\langle \mathfrak{a}_i, \mathfrak{a}_j \rangle = \delta_{ij} \tag{5}$$

gilt. Speziell heißt ein Vektor $\mathfrak{a}$ *normiert* (oder ein *Einheitsvektor*), wenn $|\mathfrak{a}| = 1$ gilt.

Satz 1. *Es sei $(\mathfrak{a}_i)_{i \in I}$ eine Familie paarweise orthogonaler, von $\mathfrak{o}$ verschiedener Vektoren des unitären Raumes V. Dann ist $(\mathfrak{a}_i)$ linear unabhängig.*

Beweis. Es sei $\mathfrak{o} = \sum \mathfrak{a}_i \lambda_i$ eine formal unendliche Linearkombination. Skalare Multiplikation mit $\mathfrak{a}_j$ von rechts ergibt $0 = \langle \mathfrak{o}, \mathfrak{a}_j \rangle = \langle \mathfrak{a}_j, \mathfrak{a}_j \rangle \lambda_j$. Wegen $\mathfrak{a}_j \neq \mathfrak{o}$ gilt $\langle \mathfrak{a}_j, \mathfrak{a}_j \rangle \neq 0$, und es folgt $\lambda_j = 0$ für alle $j \in I$. □

Beispiel 2. Aus Beispiel 1 erkennt man sofort: Eine Basis $(\mathfrak{a}_i)$ des unitären Raumes $\boldsymbol{V}^n$ ist orthonormiert genau dann, wenn die Koordinatendarstellung des Skalarproduktes die Normalform (1.3) bzw. (1.6) hat.

Übung 1. Es sei $\boldsymbol{V}^n$ ein n-dimensionaler unitärer Raum. Man beweise: Eine Basis $(\mathfrak{a}_i)$ von $\boldsymbol{V}^n$ ist orthonormiert genau dann, wenn man die Vektorkoordinaten (ξ_i) jedes beliebigen Vektors $\mathfrak{x}=\sum_{i=1}^{n}\mathfrak{a}_i\xi_i\in\boldsymbol{V}^n$ durch

$$\xi_i=\langle\mathfrak{x},\,\mathfrak{a}_i\rangle \tag{6}$$

bestimmen kann. ($\langle\mathfrak{x},\,\mathfrak{a}_i\rangle=|\mathfrak{x}|\cos\sphericalangle(\mathfrak{x},\,\mathfrak{a}_i)$ ist im Fall $K=\mathbf{R}$ und $|\mathfrak{a}_i|=1$ die Länge der orthogonalen Projektion von $\mathfrak{x}$ auf die $\mathfrak{a}_i$-Achse.)

Aus § 5.9 folgt die Existenz orthonormierter Basen in endlichdimensionalen unitären Räumen. Das für die Konstruktion angegebene Verfahren ist jedoch nur im endlichdimensionalen Fall zweckmäßig. Wir wollen nun ein von Erhard Schmidt stammendes *Orthogonalisierungsverfahren* herleiten, bei dem aus einer linear unabhängigen, endlichen oder abzählbaren Vektorfamilie $(\mathfrak{a}_i)$ iterativ eine orthonormierte Vektorfamilie $(\mathfrak{e}_i)$ konstruiert wird, $i\in\mathbf{N}$. Dazu beweisen wir zuerst einen Hilfssatz, der auch selbständiges Interesse verdient:

Lemma 1. *Es sei $\boldsymbol{W}^k\subseteqq\boldsymbol{V}$ ein k-dimensionaler Unterraum des unitären Raumes $\boldsymbol{V}$. Dann gibt es zu jedem $\mathfrak{x}\in\boldsymbol{V}$ eine und nur eine Darstellung*

$$\mathfrak{x}=\mathfrak{x}_0+\mathfrak{x}_1\quad\textit{mit}\quad\mathfrak{x}_0\in\boldsymbol{W}^k\quad\textit{und}\quad\langle\mathfrak{x}_1,\,\boldsymbol{W}^k\rangle=0; \tag{7}$$

ist $(\mathfrak{e}_\alpha)$ eine orthonormierte Basis von $\boldsymbol{W}^k$, so gilt

$$\mathfrak{x}_0=\sum_{\alpha=1}^{k}\mathfrak{e}_\alpha\langle\mathfrak{x},\,\mathfrak{e}_\alpha\rangle\,. \tag{8}$$

Beweis. Wir bemerken zuerst, daß man $\mathfrak{x}_0$ die *Projektion von $\mathfrak{x}$ auf $\boldsymbol{W}^k$* und $\mathfrak{x}_1$ das *Lot von $\mathfrak{x}$ auf $\boldsymbol{W}^k$* nennt. Zum Beweis setzen wir $\mathfrak{x}_0=\sum_{\alpha=1}^{k}\mathfrak{e}_\alpha\xi_\alpha$. Dann folgt wegen $\langle\mathfrak{x}_1,\,\boldsymbol{W}^k\rangle=0$

$$\langle\mathfrak{x}_1,\,\mathfrak{e}_\alpha\rangle=\langle\mathfrak{x}-\mathfrak{x}_0,\,\mathfrak{e}_\alpha\rangle=\langle\mathfrak{x},\,\mathfrak{e}_\alpha\rangle-\langle\mathfrak{x}_0,\,\mathfrak{e}_\alpha\rangle=0$$

für $\alpha=1,\,\ldots,\,k$. Nach (6) muß also $\xi_\alpha=\langle\mathfrak{x},\,\mathfrak{e}_\alpha\rangle$ gelten, d. h., $\mathfrak{x}_0$ und $\mathfrak{x}_1$ sind eindeutig bestimmt. Definiert man $\mathfrak{x}_0$ durch (8), so gilt $\mathfrak{x}_0\in\boldsymbol{W}^k$, und man verifiziert sofort $\langle\mathfrak{x}-\mathfrak{x}_0,\,\mathfrak{e}_\alpha\rangle=0$ für alle $\alpha=1,\,\ldots,\,k$, also auch $\langle\mathfrak{x}_1,\,\boldsymbol{W}^k\rangle=0$. □

Übung 2. Unter den Voraussetzungen von Lemma 1 beweise man: Ist $\mathfrak{x}=\mathfrak{y}_0+\mathfrak{y}_1$ eine beliebige Darstellung von $\mathfrak{x}$ mit $\mathfrak{y}_0\in\boldsymbol{W}^k$, so gilt $|\mathfrak{y}_1|\geqq|\mathfrak{x}_1|$; das Gleichheitszeichen trifft hier genau dann zu, wenn $\mathfrak{y}_1=\mathfrak{x}_1$ gleich dem Lot von $\mathfrak{x}$ auf $\boldsymbol{W}^k$ ist.

Übung 3. Es sei $\boldsymbol{E}$ ein euklidischer Punktraum, $\boldsymbol{H}^k\subset\boldsymbol{E}$ eine k-dimensionale Ebene und $x\in\boldsymbol{E}$. Man beweise: Es gibt genau ein absolutes Minimum y_0 der Funktion $y\in\boldsymbol{H}^k\mapsto f(y):=\varrho(y,\,x)$; der Punkt y_0 ist derjenige Punkt von $\boldsymbol{H}^k$, für den $\overrightarrow{y_0x}$ zu dem Vektorraum $\boldsymbol{W}^k$ von $\boldsymbol{H}^k$ orthogonal ist. (Man nennt y_0 den *Fußpunkt des Lotes* $\overrightarrow{y_0x}$ von x auf $\boldsymbol{H}^k$ und $\varrho(x,\,\boldsymbol{H}^k):=|\overrightarrow{y_0x}|$ den *Abstand von x und $\boldsymbol{H}^k$*).

Satz 2. *Es sei V ein unitärer Raum und $(\mathfrak{a}_i)$ eine endliche oder abzählbare linear unabhängige Familie, $\mathfrak{a}_i \in V$. Dann gibt es eine und nur eine orthonormierte Familie $(\mathfrak{e}_i)$, $\mathfrak{e}_i \in V$, mit den folgenden Eigenschaften:*

$$\mathfrak{e}_j = \sum_{i=1}^{j} \mathfrak{a}_i \mu_{ij}, \qquad j = 1, 2, \ldots, n, \ldots, \tag{9}$$

$$\mu_{jj} \in \mathbf{R}, \qquad \mu_{jj} > 0 . \tag{10}$$

Beweis. Für $j=1$ lautet die Gleichung (9): $\mathfrak{e}_1 = \mathfrak{a}_1 \mu_{11}$. Aus (10) folgt $|\mathfrak{e}_1| = 1 = |\mathfrak{a}_1| \mu_{11}$, also $\mu_{11} = |\mathfrak{a}_1|^{-1}$; denn es ist $\mathfrak{a}_1 \neq \mathfrak{o}$, da $(\mathfrak{a}_i)$ linear unabhängig ist. Offenbar ist $\mathfrak{e}_1 := \mathfrak{a}_1/|\mathfrak{a}_1|$ ein eindeutig bestimmter, (9) und (10) erfüllender Vektor. Angenommen, $\mathfrak{e}_1, \ldots, \mathfrak{e}_k$ seien schon eindeutig bestimmte, den Forderungen des Satzes genügende Vektoren. Für den Beweis der Existenz des Vektors $\mathfrak{e}_{k+1}$ setzen wir $\boldsymbol{W}^k := \mathfrak{L}(\{\mathfrak{a}_1, \ldots, \mathfrak{a}_k\})$; dann gilt $\dim \boldsymbol{W}^k = k$ wegen der linearen Unabhängigkeit der $(\mathfrak{a}_i)$, und aus (9) und Satz 1 ergibt sich $\boldsymbol{W}^k = \mathfrak{L}(\{\mathfrak{e}_1, \ldots, \mathfrak{e}_k\})$. Der Vektor $\hat{\mathfrak{e}}_{k+1}$ sei das nach Lemma 1 eindeutig bestimmte Lot von $\mathfrak{a}_{k+1}$ auf $\boldsymbol{W}^k$; aus (8) folgt

$$\hat{\mathfrak{e}}_{k+1} = \mathfrak{a}_{k+1} - \sum_{\alpha=1}^{k} \mathfrak{e}_\alpha \langle \mathfrak{a}_{k+1}, \mathfrak{e}_\alpha \rangle . \tag{11}$$

Weil das Lot $\mathfrak{x}_1$ eines Vektors $\mathfrak{x}$ auf $\boldsymbol{W}^k$ genau dann gleich $\mathfrak{o}$ ist, wenn $\mathfrak{x} \in \boldsymbol{W}^k$ gilt, muß $\hat{\mathfrak{e}}_{k+1} \neq \mathfrak{o}$ sein; sonst wären ja $(\mathfrak{a}_1, \ldots, \mathfrak{a}_{k+1})$ linear abhängig. Für den Betrag von $\hat{\mathfrak{e}}_{k+1}$ erhalten wir nach einer leichten Rechnung:

$$\langle \hat{\mathfrak{e}}_{k+1}, \hat{\mathfrak{e}}_{k-1} \rangle = \langle \mathfrak{a}_{k+1}, \mathfrak{a}_{k+1} \rangle - 2 \sum_{\alpha=1}^{k} |\langle \mathfrak{a}_{k+1}, \mathfrak{e}_\alpha \rangle|^2 + \sum_{\alpha=1}^{k} |\langle \mathfrak{a}_{k+1}, \mathfrak{e}_\alpha \rangle|^2,$$

also

$$|\hat{\mathfrak{e}}_{k+1}| = \Big(|\mathfrak{a}_{k+1}|^2 - \sum_{\alpha=1}^{k} |\langle \mathfrak{a}_{k+1}, \mathfrak{e}_\alpha \rangle|^2 \Big)^{1/2}. \tag{12}$$

Offenbar ist

$$\mathfrak{e}_{k+1} := \frac{\mathfrak{a}_{k+1} - \sum_{\alpha=1}^{k} \mathfrak{e}_\alpha \langle \mathfrak{a}_{k+1}, \mathfrak{e}_\alpha \rangle}{\Big(|\mathfrak{a}_{k+1}|^2 - \sum_{\alpha=1}^{k} |\langle \mathfrak{a}_{k+1}, \mathfrak{e}_\alpha \rangle|^2 \Big)^{1/2}} \tag{13}$$

der gesuchte Vektor; er ist normiert, nach Definition $\mathfrak{e}_{k+1} = \hat{\mathfrak{e}}_{k+1}/|\hat{\mathfrak{e}}_{k+1}|$ als Produkt des Lotes von $\mathfrak{a}_{k+1}$ auf $\boldsymbol{W}^k$ mit einer reellen Zahl orthogonal zu $\boldsymbol{W}^k$, also auch zu allen $\mathfrak{e}_\alpha$, $\alpha = 1, \ldots, k$, und er erfüllt (9) und (10) für $j = k+1$. Betrachten wir nämlich (9) für $j = 1, \ldots, k$, so erhalten wir die Matrix $(\mu_{ij}) \in \mathbf{M}_k(\mathbf{C})$ der Darstellung der Basis $(\mathfrak{e}_1, \ldots, \mathfrak{e}_k)$ von $\boldsymbol{W}^k$ in der Basis $(\mathfrak{a}_1, \ldots, \mathfrak{a}_k)$. Nach (9), (10) ist (μ_{ij}) eine Dreiecksmatrix mit

$$\det (\mu_{ij}) = \prod_{j=1}^{k} \mu_{jj} > 0 . \tag{14}$$

Daher können wir umgekehrt die $\mathfrak{e}_\alpha$ durch die $\mathfrak{a}_\beta$ mit Hilfe der inversen Matrix

$(\mu_{ij})^{-1}$ ausdrücken und damit in (13) eingehen. Weil sich hierbei der Koeffizient von $\mathfrak{a}_{k+1}$ nicht ändert, erhalten wir

$$\mathfrak{e}_{k+1} = \sum_{i=1}^{k+1} \mathfrak{a}_i \mu_{i,k+1}, \qquad \mu_{k+1,k+1} = |\hat{\mathfrak{e}}_{k+1}|^{-1} > 0 . \tag{15}$$

Zum Beweis der Eindeutigkeit nehmen wir an, daß $\mathfrak{b}_{k+1}$ ebenfalls ein Vektor sei, für den $(\mathfrak{e}_1, ..., \mathfrak{e}_k, \mathfrak{b}_{k+1})$ eine orthonormierte Familie ist und (9), (10) erfüllt sind. Nach (9) ist dann $\mathfrak{b}_{k+1} \in \boldsymbol{W}^{k+1} := \mathfrak{L}(\{\mathfrak{a}_1, ..., \mathfrak{a}_{k+1}\})$; da $(\mathfrak{e}_1, ..., \mathfrak{e}_{k+1})$ wegen Satz 1 und (9) eine orthonormierte Basis von $\boldsymbol{W}^{k+1}$ ist, ergibt sich eine eindeutig bestimmte Basisdarstellung

$$\mathfrak{b}_{k+1} = \sum_{\lambda=1}^{k+1} \mathfrak{e}_\lambda \beta_\lambda .$$

Aus $\langle \mathfrak{b}_{k+1}, \mathfrak{e}_\alpha \rangle = 0$, $\alpha = 1, ..., k$, folgt $\beta_\alpha = \langle \mathfrak{b}_{k+1}, \mathfrak{e}_\alpha \rangle = 0$ für $\alpha = 1, ..., k$. Somit gilt $\mathfrak{b}_{k+1} = \mathfrak{e}_{k+1}\beta$, $\beta := \beta_{k+1}$. Setzen wir (15) in diese Gleichung ein, so ergibt sich für den Koeffizienten ν_{k+1} der Darstellung von $\mathfrak{b}_{k+1}$ in der Basis $(\mathfrak{a}_1, ..., \mathfrak{a}_{k+1})$

$$\nu_{k+1} = \mu_{k+1,k+1}\beta ,$$

und hieraus folgt $\beta = \nu_{k+1}/\mu_{k+1,k+1} \in \mathbf{R}$, $\beta > 0$. Andererseits ist $\mathfrak{b}_{k+1}$ normiert, es gilt also $1 = |\mathfrak{b}_{k+1}| = |\mathfrak{e}_{k+1}|\,|\beta| = |\beta|$. Damit muß aber $\beta = 1$, also $\mathfrak{b}_{k+1} = \mathfrak{e}_{k+1}$ gelten. □

Folgerung 1. *Es sei $\boldsymbol{W}^k \subseteq \boldsymbol{V}^n$, $0 \leq k \leq n$, ein Unterraum des n-dimensionalen unitären Raumes $\boldsymbol{V}^n$. Dann gibt es eine orthonormierte Basis $(\mathfrak{e}_i)$, $i = 1, ..., n$, von $\boldsymbol{V}^n$, so daß $(\mathfrak{e}_1, ..., \mathfrak{e}_k)$ eine orthonormierte Basis von $\boldsymbol{W}^k$ ist. Jede orthonormierte Folge $(\mathfrak{e}_1, ..., \mathfrak{e}_k)$, $k \geqq 0$, von Vektoren des $\boldsymbol{V}^n$ läßt sich zu einer orthonormierten Basis des $\boldsymbol{V}^n$ ergänzen.*

Zum Beweis genügt es, eine Basis $(\mathfrak{a}_i)$ von $\boldsymbol{V}^n$ mit $\boldsymbol{W}^k = \mathfrak{L}(\{\mathfrak{a}_1, ..., \mathfrak{a}_k\})$ zu wählen (Basisergänzungssatz, Folgerung 4.6.1) und diese nach E. Schmidt zu orthogonalisieren. Aus (9) erhält man $\mathfrak{L}(\{\mathfrak{a}_1, ..., \mathfrak{a}_k\}) = \mathfrak{L}(\{\mathfrak{e}_1, ..., \mathfrak{e}_k\})$. Speziell gibt der Fall $k = n$ uns einen neuen, von § 5.9 unabhängigen Beweis der Existenz einer orthonormierten Basis von $\boldsymbol{V}^n$. Zum Beweis der zweiten Behauptung orthogonalisiere man eine Basis der Form $(\mathfrak{e}_1, ..., \mathfrak{e}_k, \mathfrak{a}_{k+1}, ..., \mathfrak{a}_n)$; die ersten k Vektoren bleiben dabei ungeändert. □

Definition 3. Es sei $\boldsymbol{W} \subseteq \boldsymbol{V}$ ein Unterraum des unitären Raumes $\boldsymbol{V}$. Dann heißt

$$\boldsymbol{W}^\perp := \{\mathfrak{x} \mid \mathfrak{x} \in \boldsymbol{V} \text{ und } \langle \mathfrak{x}, \boldsymbol{W} \rangle = 0\} \tag{16}$$

das *orthogonale Komplement* des Unterraumes $\boldsymbol{W}$.

Folgerung 2. *Es sei $\boldsymbol{W} \subseteq \boldsymbol{V}$, $\boldsymbol{V}$ unitär und* dim $\boldsymbol{W} = k < \infty$. *Dann gilt*

$$\boldsymbol{V} = \boldsymbol{W} \oplus \boldsymbol{W}^\perp . \tag{17}$$

Der Beweis folgt unmittelbar aus Lemma 1 und Definition 3. □

Beispiel 3. Es sei $\boldsymbol{V}^n$ ein n-dimensionaler euklidischer Vektorraum. Nach Satz

5.9.7 entspricht jedem $\mathfrak{x} \in \boldsymbol{V}^n$ die Linearform $\varphi(\mathfrak{x})$ mit

$$(\varphi(\mathfrak{x}) \mid \mathfrak{y}) := \langle \mathfrak{x}, \mathfrak{y} \rangle . \tag{18}$$

Man erkennt sofort: Die Abbildung $\mathfrak{x} \in \boldsymbol{V}^n \mapsto \varphi(\mathfrak{x}) \in \boldsymbol{V}^{n'}$ ist ein durch das Skalarprodukt eindeutig bestimmter linearer Isomorphismus auf den dualen Raum $\boldsymbol{V}^{n'}$. Wir können also im euklidischen Fall $\boldsymbol{V}^n$ und $\boldsymbol{V}^{n'}$ identifizieren, indem wir $\varphi(\mathfrak{x}) = \mathfrak{x}$ setzen. Dann gilt nach (18)

$$(\mathfrak{x} \mid \mathfrak{y}) = \langle \mathfrak{x}, \mathfrak{y} \rangle; \tag{19}$$

das Skalarprodukt stimmt mit dem Wert der Linearform $\mathfrak{x}$ an der Stelle $\mathfrak{y}$ überein. Hieraus folgt: Der Annullator wird mit dem orthogonalen Komplement identifiziert (vgl. Definition 5.6.1). Damit ist die Bezeichnung aus Definition 3 gerechtfertigt, und man erkennt die Gültigkeit der Beziehungen (5.6.15) bis (5.6.17) für das orthogonale Komplement.

Beispiel 4. Es sei nun $K = \mathbf{C}$ und $\boldsymbol{V}^n$ ein unitärer Raum. In diesem Fall liefert uns (18) nicht ein Element von $\boldsymbol{V}^{n'}$; denn die rechte Seite ist *konjugiert-linear* in $\mathfrak{y}$, vgl. (1.4). Man erkennt nun leicht: Ist $\boldsymbol{V}^n$ ein Vektorraum über $\mathbf{C}$, so wird die Menge $\bar{\boldsymbol{V}}'$ aller *konjugiert-linearen Abbildungen* $f: \boldsymbol{V} \to \mathbf{C}$ bei argumentweiser Definition der Operationen ein Vektorraum über $\mathbf{C}$. Es ist nicht schwer, die Resultate aus § 5.6 mit kleinen Modifikationen auf das konjugierte Dual $\bar{\boldsymbol{V}}'$ zu übertragen. In Analogie zu Beispiel 3 ergibt sich: Für einen unitären Vektorraum $\boldsymbol{V}^n$ über $\mathbf{C}$ definiert (18) einen linearen Isomorphismus $\varphi: \boldsymbol{V}^n \to \bar{\boldsymbol{V}}^{n'}$, mit dessen Hilfe man diese Räume identifizieren kann. Daher läßt sich die Betrachtung von $\bar{\boldsymbol{V}}'$ übergehen. Andererseits kann man jedem Vektor $\mathfrak{v}$ des unitären Raumes $\boldsymbol{V}$ eine lineare Funktion $\psi(\mathfrak{v}) \in \boldsymbol{V}'$ durch $\psi(\mathfrak{v})(\mathfrak{x}) := \langle \mathfrak{x}, \mathfrak{v} \rangle$ zuordnen. Gilt $\dim \boldsymbol{V} < \infty$, so ist ψ bijektiv und konjugiert-linear, d. h., es gilt $\psi(\mathfrak{v}\alpha) = \psi(\mathfrak{v})\,\bar{\alpha}$, so daß eine Identifizierung von $\boldsymbol{V}$ und $\boldsymbol{V}'$ nicht möglich ist; jedoch kann man wegen der Bijektivität von ψ die Betrachtung der dualen Vektoren auch hier vermeiden.

Definition 4. Es seien $\boldsymbol{V}$, $\boldsymbol{W}$ unitäre Vektorräume über demselben Körper K ($= \mathbf{R}$ oder $\mathbf{C}$). Eine Abbildung $a: \boldsymbol{V} \to \boldsymbol{W}$ heißt *unitär* im Fall $K = \mathbf{C}$ oder *orthogonal* im Fall $K = \mathbf{R}$, wenn a linear ist und für alle $\mathfrak{x}, \mathfrak{y} \in \boldsymbol{V}$

$$\langle a\mathfrak{x}, a\mathfrak{y} \rangle = \langle \mathfrak{x}, \mathfrak{y} \rangle \tag{20}$$

gilt. Die Abbildung a heißt ein *Isomorphismus der unitären Räume*, wenn sie bijektiv und unitär (bzw. orthogonal) ist.

Folgerung 3. *Jede unitäre (orthogonale) Abbildung ist injektiv. Jede derartige Abbildung zwischen Räumen gleicher, endlicher Dimension ist ein Isomorphismus der unitären Räume.* □

Definition 5. Unter *orthogonalen kartesischen Punkt-* bzw. *Vektorkoordinaten* versteht man kartesische Punkt- bzw. Vektorkoordinaten eines euklidischen Punktraumes bzw. eines unitären Raumes, deren n-Bein-Vektoren eine orthonormierte Basis bilden.

Satz 3. *Zwei endlichdimensionale, unitäre Räume V, W über demselben Körper sind isomorph genau dann, wenn* dim V = dim W *gilt.*

Beweis. Die Notwendigkeit der Bedingung ist trivial. Ist umgekehrt dim V = dim $W = n$, so können wir nach Folgerung 1 (für $k = n$) in V und W orthonormierte n-Beine finden, die entsprechende orthogonale kartesische Koordinaten (ξ_i) bzw. $(\hat{\xi}_i)$ bestimmen. Da dann das Skalarprodukt in beiden Räumen die Normalform (1.3) bzw. (1.6) hat, ist die Zuordnung durch gleiche Koordinaten $(\hat{\xi}_i) = (\xi_i)$ ein Isomorphismus (vgl. § 5.7):

$$\langle \varphi(\mathfrak{x}), \varphi(\mathfrak{y}) \rangle = \sum_i \hat{\xi}_i \bar{\hat{\eta}}_i = \sum_i \xi_i \bar{\eta}_i = \langle \mathfrak{x}, \mathfrak{y} \rangle . \quad \square$$

Folgerung 4. *Die Menge der unitären bzw. orthogonalen Abbildungen des n-dimensionalen unitären bzw. euklidischen Vektorraumes V^n in sich bildet eine Untergruppe der linearen Gruppe $GL(V^n)$; sie heißt die unitäre Gruppe $U(n)$ im Fall $K = \mathbf{C}$ bzw. die orthogonale Gruppe $O(n)$ im Fall $K = \mathbf{R}$.* $\square$

Der Beweis von Folgerung 4 ergibt sich einfach aus Definition 4 und Folgerung 3. Eine Beschreibung der Gruppen $O(n)$ und $U(n)$ durch Matrizengruppen liefert der folgende

Satz 4. *Es sei V^n ein unitärer Vektorraum und $(\mathfrak{e}_i)$ eine orthonormierte Basis von V^n. Eine lineare Abbildung $a \in L(V^n)$ ist genau dann unitär (bzw. orthogonal), wenn für die Matrix (a_{ij}) von a bezüglich $(\mathfrak{e}_i)$*

$$(a_{ij})^{-1} = (\bar{a}_{ij})' \qquad (K = \mathbf{C}) \tag{21}$$

bzw.

$$(a_{ij})^{-1} = (a_{ij})' \qquad (K = \mathbf{R}) \tag{22}$$

gilt.

Beweis. Wir betrachten etwa den Fall $K = \mathbf{C}$. Aus

$$a(\mathfrak{e}_j) = \sum_i \mathfrak{e}_i a_{ij}$$

folgt durch Bildung des Skalarproduktes

$$\langle a(\mathfrak{e}_j), a(\mathfrak{e}_k) \rangle = \sum_i a_{ij} \bar{a}_{ik} = \langle \mathfrak{e}_j, \mathfrak{e}_k \rangle = \delta_{jk} . \tag{23}$$

In Matrixschreibweise lautet diese Beziehung $(a_{ij})'\,(\bar{a}_{jk}) = (\delta_{jk})$. Geht man in dieser Gleichung zu den konjugiert-komplexen Matrizen über, so folgt (21). Gilt umgekehrt (21), so erhalten wir daraus (23), d. h., das Bild $(a(\mathfrak{e}_i))$ der orthonormierten Basis $(\mathfrak{e}_i)$ ist wieder orthonormiert. Der Beweis des Satzes ergibt sich aus dem folgenden

Lemma 2. *Eine lineare Abbildung $a \in L(V^n)$ des unitären Raumes V^n ist genau dann unitär (orthogonal), wenn das Bild $(a(\mathfrak{e}_i))$ einer orthonormierten Basis $(\mathfrak{e}_i)$ wieder orthonormiert ist. Zu zwei orthonormierten Basen $(\mathfrak{e}_i)$, $(\hat{\mathfrak{e}}_i)$ gibt es genau einen unitären (orthogonalen) Isomorphismus a mit $a(\mathfrak{e}_i) = \hat{\mathfrak{e}}_i$, $i = 1, \ldots, n$.*

Beweis. Nach (20) ist die Bedingung offenbar notwendig. Ist sie erfüllt, so gilt für $\mathfrak{x} = \sum_i \mathfrak{e}_i \xi_i$, $\mathfrak{y} = \sum_i \mathfrak{e}_i \eta_i$

$$\langle a(\mathfrak{x}), a(\mathfrak{y})\rangle = \sum_{i,j} \langle a(\mathfrak{e}_i), a(\mathfrak{e}_j)\rangle \xi_i \bar{\eta}_j = \sum_{i,j} \delta_{ij} \xi_i \bar{\eta}_j = \sum_i \xi_i \bar{\eta}_i = \langle \mathfrak{x}, \mathfrak{y}\rangle ,$$

d. h., a ist unitär. Die zweite Behauptung folgt unmittelbar aus der ersten und Satz 5.2.5. □

In jeder festen, orthonormierten Basis erhalten wir also einen Isomorphismus von $\boldsymbol{U}(n)$ bzw. $\boldsymbol{O}(n)$ auf eine gewisse Matrizengruppe, die man, wenn keine Verwechselungen zu befürchten sind, durch dasselbe Symbol bezeichnet und ebenfalls die unitäre bzw. orthogonale Gruppe nennt. Eine Matrix $(a_{ij}) \in \boldsymbol{GL}(n, \mathbf{C})$ heißt *unitär*, wenn $(a_{ij}) \in \boldsymbol{U}(n)$ gilt; jede der folgenden Bedingungen ist dafür notwendig und hinreichend:

$$\sum_i a_{ij} \bar{a}_{ik} = \delta_{jk}, \qquad j, k = 1, \ldots, n; \tag{24}$$

$$(a_{ij})^{-1} = (\bar{a}_{ij})'; \tag{25}$$

$$(a_{ij})^* = (\bar{a}_{ij}) . \tag{26}$$

Analog heißt eine Matrix $(a_{ij}) \in \boldsymbol{GL}(n, \mathbf{R})$ *orthogonal*, wenn $(a_{ij}) \in \boldsymbol{O}(n)$ gilt; hierzu ist jede der folgenden Bedingungen äquivalent:

$$\sum_i a_{ij} a_{ik} = \delta_{jk}, \quad j, k = 1, \ldots, n; \tag{27}$$

$$(a_{ij})^{-1} = (a_{ij})'; \tag{28}$$

$$(a_{ij})^* = (a_{ij}) . \tag{29}$$

Übung 4. Die Bedingungen (24) bzw. (27) drücken aus, daß die Spaltenvektoren der Matrix orthonormiert sind in dem unitären n-Tupel-Raum $\mathbf{C}^n$ bzw. $\mathbf{R}^n$ (vgl. (1.6) bzw. (1.3)). Man beweise, daß die Bedingung (24) bzw. (27) auch zu der Bedingung

$$\sum_i a_{ji} \bar{a}_{ki} = \delta_{jk}, \qquad j, k = 1, \ldots, n , \tag{30}$$

bzw.

$$\sum_i a_{ji} a_{ki} = \delta_{jk}, \qquad j, k = 1, \ldots, n , \tag{31}$$

äquivalent ist, welche die Orthonormiertheit der Zeilenvektoren der Matrix ausdrückt.

Aus (25) und (28) erhält man sofort

Folgerung 5. *Für jede unitäre bzw. orthogonale Matrix gilt* $|\det(a_{ij})| = 1$; *für* $(a_{ij}) \in \boldsymbol{O}(n)$ *gibt es also nur die beiden Möglichkeiten* $\det(a_{ij}) = \pm 1$.

Die Mengen (vgl. Definition 5.7.2)

$$\boldsymbol{SO}(n) := \{a \mid a \in \boldsymbol{O}(n) \text{ und } N(a) = 1\}, \tag{32}$$

$$\boldsymbol{SU}(n) := \{a \mid a \in \boldsymbol{U}(n) \text{ und } N(a) = 1\} \tag{33}$$

heißen die *spezielle orthogonale* bzw. die *spezielle unitäre Gruppe*.

Übung 5. Man beweise, daß $SO(n)$ und $SU(n)$ Untergruppen von $O(n)$ bzw. von $U(n)$ sind. Ferner beweise man folgende Beziehungen für die Matrizengruppen:

$$O(n) \subseteq U(n) \subseteq GL(n, \mathbf{C}), \tag{34}$$

$$SO(n) = O(n) \cap SU(n), \tag{35}$$

$$O(n) = U(n) \cap GL(n, \mathbf{R}). \tag{36}$$

(Hinweis. Man benutze die durch $\mathbf{R} \subset \mathbf{C}$ induzierten Einbettungen $\mathbf{R}^n \subset \mathbf{C}^n$, $GL(n, \mathbf{R}) \subset GL(n, \mathbf{C})$.)

Übung 6. Es sei $K = \mathbf{R}$ oder $\mathbf{C}$. Man beweise: Die Menge $\Delta(n, K)$ der oberen Dreiecksmatrizen mit von 0 verschiedenen Elementen in der Hauptdiagonale ist eine Untergruppe von $GL(n, K)$; ebenso die Menge $\Delta_+(n, K) \subset \Delta(n, K)$ der oberen Dreiecksmatrizen, für die alle Elemente der Hauptdiagonale reell und positiv sind. Ferner zeige man, daß

$$GL(n, \mathbf{C}) = U(n) \cdot \Delta_+(n, \mathbf{C}), \qquad U(n) \cap \Delta_+(n, \mathbf{C}) = \{e\}, \tag{37}$$

$$GL(n, \mathbf{R}) = O(n) \cdot \Delta_+(n, \mathbf{R}), \qquad O(n) \cap \Delta_+(n, \mathbf{R}) = \{e\}, \tag{38}$$

gelten; mit anderen Worten, jede komplexe (reelle), quadratische Matrix vom Rang n besitzt eine und nur eine Darstellung als Produkt einer unitären (bzw. orthogonalen) Matrix und einer oberen Dreiecksmatrix aus $\Delta_+(n, \mathbf{C})$ (bzw. $\Delta_+(n, \mathbf{R})$). (Hinweis. Man wende Satz 2 an; ferner beachte man Übung 5.4.6.)

Es ist nun leicht, die euklidische Gruppe zu definieren. Eine affine Transformation f des euklidischen Punktraumes E^n heißt *euklidisch* oder eine *Bewegung*, wenn sie den Abstand invariant läßt:

$$\varrho(f(x), f(y)) = \varrho(x, y), \qquad x, y \in E^n. \tag{39}$$

Die Menge der euklidischen Transformationen wird mit $\mathfrak{E}(n)$ bezeichnet. Wir bemerken, daß bei der Definition einer Bewegung auf die Bedingung, f sei affin, verzichtet werden kann (vgl. Übung 13).

Satz 5. *Es sei E^n ein n-dimensionaler euklidischer Punktraum. Dann ist $\mathfrak{E}(n)$ eine Untergruppe der Gruppe $\mathfrak{A}(n)$ der affinen Transformationen von E^n. Eine affine Transformation $f \in \mathfrak{A}(n)$ ist genau dann euklidisch, wenn die zugeordnete lineare Abbildung $a_f: V^n \to V^n$ orthogonal ist.*

Beweis. Die erste Behauptung ergibt sich sofort aus der Definition. Zum Beweis der zweiten beachten wir, daß nach (39) und (1.15) für alle $x, y \in E^n$ die Beziehung

$$|a_f(\overrightarrow{xy})| = |\overrightarrow{f(x)\, f(y)}| = |\overrightarrow{xy}|$$

gelten muß; da wir jeden Vektor in der Form $\mathfrak{x} = \overrightarrow{xy}$ darstellen können, ist (39) äquivalent zu der Bedingung, daß a_f die Norm erhält:

$$|a_f(\mathfrak{x})| = |\mathfrak{x}| \quad \text{für alle} \quad \mathfrak{x} \in V^n. \tag{40}$$

Wenn also a_f orthogonal ist, ist f euklidisch. Gilt umgekehrt (40), so ist auch a_f orthogonal; denn nach (5.9.33) mit $\langle\ ,\ \rangle$ statt b folgt aus (40) unmittelbar (20). □

Folgerung 6. *Die Gruppe* $\mathfrak{T}(\boldsymbol{E}^n) \cong [\boldsymbol{V}^n, +]$ *der Translationen ist ein Normalteiler von* $\mathfrak{E}(n)$, *und es gilt*

$$\mathfrak{E}(n) = \boldsymbol{O}(n) \cdot \mathfrak{T}(\boldsymbol{E}^n), \qquad \boldsymbol{O}(n) \cap \mathfrak{T}(\boldsymbol{E}^n) = \{e\}, \tag{41}$$

d. h., $\mathfrak{E}(n)$ *ist halbdirektes Produkt von* $\boldsymbol{O}(n)$ *mit* $\mathfrak{T}(\boldsymbol{E}^n)$; *dabei ist* $\boldsymbol{O}(n)$ *die Isotropiegruppe eines Punktes* $o \in \boldsymbol{E}^n$ (vgl. Folgerung 5.3.2 und Satz 5.3.3). □

Nach Folgerung 6 und den allgemeinen Eigenschaften der affinen Transformationen können wir also bezüglich eines Ursprungs $o \in \boldsymbol{E}^n$ jede euklidische Transformation in der Form

$$f(x) = o + a_f(\overrightarrow{ox}) + \mathfrak{a}, \qquad x \in \boldsymbol{E}^n, \tag{42}$$

mit $a_f \in \boldsymbol{O}(n)$, $\mathfrak{a} \in \boldsymbol{V}^n$ darstellen. Ist $(o; \mathfrak{e}_i)$ ein orthonormiertes n-Bein, so erhalten wir die Koordinatendarstellung von f in der Form

$$y_i = \sum_j a_{ij} x_j + a_i, \qquad i = 1, \ldots, n, \tag{43}$$

mit (a_{ij}) orthogonal. Für die Beschreibung der euklidischen Transformationen kommt es also vor allem auf die Untersuchung der orthogonalen Abbildungen an. Es gilt

Satz 6. *Ist* λ *ein Eigenwert eines unitären oder orthogonalen Automorphismus, so gilt* $|\lambda| = 1$; *die einzig möglichen reellen Eigenwerte sind also* ± 1.

Beweis. In der Tat folgt aus $a(\mathfrak{x}) = \mathfrak{x}\lambda$ und $|a(\mathfrak{x})| = |\mathfrak{x}|\ |\lambda| = |\mathfrak{x}|$ sowie $\mathfrak{x} \neq \mathfrak{o}$ sofort $|\lambda| = 1$. □

Beispiel 5. Die *Spiegelungen* an einer k-Ebene sind euklidische (bzw. orthogonale) Transformationen. Für sie gilt $\boldsymbol{V}^n = \boldsymbol{W}^k \oplus \boldsymbol{W}^{k\perp}$ mit den Eigenunterräumen $\boldsymbol{W}^k = \boldsymbol{W}_1$, $\boldsymbol{W}^{k\perp} = \boldsymbol{W}_{-1}$, also $a(\mathfrak{x}) = \mathfrak{x}$ für $\mathfrak{x} \in \boldsymbol{W}^k$, $a(\mathfrak{x}) = -\mathfrak{x}$ für $\mathfrak{x} \in \boldsymbol{W}_{-1}$ und der Koordinatendarstellung

$$y_\alpha = x_\alpha, \qquad \alpha = 1, \ldots, k,$$

$$y_\varkappa = -x_\varkappa, \qquad \varkappa = k+1, \ldots, n.$$

Beispiel 6. Im Fall $n = 1$ ist jede unitäre Abbildung eine Multiplikation $x \in \mathbf{C} \mapsto$ $\mapsto xe^{i\alpha} \in \mathbf{C}$; die unitäre Gruppe $\boldsymbol{U}(1)$ ist also gleich der multiplikativen Gruppe S^1 der komplexen Zahlen vom Betrag 1. Aus (36) folgt $\boldsymbol{O}(1) = \{1, -1\}$ für $n = 1$. Die Gruppen $\boldsymbol{SO}(1) = \boldsymbol{SU}(1) = \{1\}$ sind trivial.

In den folgenden wichtigen Beispielen wollen wir die euklidischen Transformationen der Ebene $\boldsymbol{E}^2$ und des Raumes $\boldsymbol{E}^3$ beschreiben. Dazu beginnen wir mit den orthogonalen Transformationen.

Beispiel 7. Ist $(a_{ij}) \in \boldsymbol{O}(2)$, so ergibt (27) für $j = k = 1$ die Beziehung $a_{11}^2 + a_{21}^2 = 1$. Es gibt also einen eindeutig bestimmten Winkel φ, $0 \leqq \varphi < 2\pi$, mit

$$a_{11} = \cos\varphi, \qquad a_{21} = \sin\varphi.$$

Aus (27) für $j=1$, $k=2$ folgt dann

$$a_{12}\cos\varphi + a_{22}\sin\varphi = 0\,,$$

und daher muß $a_{12}=-t\sin\varphi$, $a_{22}=t\cos\varphi$ für ein $t\in\mathbf{R}$ gelten. Die Beziehung (27) für $j=k=2$ ergibt sofort $t^2=1$, also $t=\pm 1$. Die Matrizen für den Fall $t=+1$,

$$\begin{pmatrix}\cos\varphi & -\sin\varphi\\ \sin\varphi & \cos\varphi\end{pmatrix}, \tag{44}$$

haben die Determinante $+1$; (44) stellt eine *Drehung* der Ebene um den Winkel φ mit dem Fixpunkt o dar. Da die Matrizen für $t=-1$,

$$\begin{pmatrix}\cos\varphi & \sin\varphi\\ \sin\varphi & -\cos\varphi\end{pmatrix}, \tag{45}$$

die Determinante -1 haben, besteht $\boldsymbol{SO}(2)$ aus allen Matrizen der Form (44). Bezeichnet d_φ die zugehörige Drehung der Ebene, so gilt

$$d_{\varphi_1+\varphi_2}=d_{\varphi_1}\circ d_{\varphi_2}\,, \tag{46}$$

wobei mit den Winkeln mod 2π zu rechnen ist; es folgt die Isomorphie

$$\boldsymbol{SO}(2)\cong\boldsymbol{S}^1; \tag{47}$$

speziell ist $\boldsymbol{SO}(2)$ abelsch. (Vgl. Beispiel 1.3.3 und Übung 2.3.1.)

Übung 7. Man beweise: a) Die Drehung d_φ mit der Matrix (44) hat nur für $\varphi=0$, d. h. $d_0=\mathrm{id}_{V^2}$ und $\varphi=\pi$ (Spiegelung an o) reelle Eigenwerte. — b) Jede orthogonale Abbildung von $\boldsymbol{V}^2$, die bezüglich eines orthonormierten 2-Beines eine Matrix der Form (45) besitzt, hat die reellen Eigenwerte $+1, -1$; man kann daher eine Basis so finden, daß sie in dieser die Darstellung nach Beispiel 5 mit $k=1$, $n=2$ besitzt.

Übung 8. Man beweise: $\boldsymbol{O}(2)$ ist nicht abelsch.

Nach Übung 7 ist also jede euklidische Bewegung der Ebene die Verknüpfung einer Translation mit einer Drehung oder einer Spiegelung an einer Geraden.

Beispiel 8. Wir betrachten nun $\boldsymbol{O}(3)$. Da das charakteristische Polynom $\chi_a(t)$ für jede Matrix aus $\mathbf{M}_3(\mathbf{R})$ ein reelles Polynom dritten Grades ist, hat $\chi_a(t)$ (nach Folgerung 2.8.5) wenigstens eine reelle Nullstelle, die im Fall $a\in\boldsymbol{O}(3)$ nur gleich ± 1 sein kann. Wir bemerken zuerst folgenden wichtigen Hilfssatz:

Lemma 3. *Ist $a\in\boldsymbol{L}(\boldsymbol{V}^n)$ unitär oder orthogonal und $\boldsymbol{W}\subseteqq\boldsymbol{V}^n$ ein gegen a invarianter Unterraum, so ist auch $\boldsymbol{W}^\perp$ bei a invariant. Sind λ, μ verschiedene Eigenwerte von a, so sind die zugehörigen Eigenunterräume $\boldsymbol{W}_\lambda$, $\boldsymbol{W}_\mu$ zueinander orthogonal.*

Beweis. Offenbar ist $a\mid\boldsymbol{W}$ ebenfalls orthogonal und daher ein Automorphismus. Gilt nun $\langle\mathfrak{x},\boldsymbol{W}\rangle=0$, so folgt $\langle a\mathfrak{x},a\boldsymbol{W}\rangle=\langle a\mathfrak{x},\boldsymbol{W}\rangle=0$, also $a\mathfrak{x}\in\boldsymbol{W}^\perp$ für $\mathfrak{x}\in\boldsymbol{W}^\perp$. Zum Beweis der zweiten Behauptung sei $\mathfrak{x}\in\boldsymbol{W}_\lambda$, $\mathfrak{y}\in\boldsymbol{W}_\mu$. Dann gilt

$$\langle\mathfrak{x},\mathfrak{y}\rangle=\langle a\mathfrak{x},a\mathfrak{y}\rangle=\lambda\bar{\mu}\langle\mathfrak{x},\mathfrak{y}\rangle\,.$$

Nach Satz 6 ist $\lambda=e^{i\alpha}$, $\mu=e^{i\beta}$, also $\lambda\cdot\bar{\mu}=e^{i(\alpha-\beta)}\neq 1$, da sonst $\lambda=\mu$ wäre. Somit muß $\langle\mathfrak{x},\mathfrak{y}\rangle=0$ sein, woraus $\langle\boldsymbol{W}_\lambda,\boldsymbol{W}_\mu\rangle=0$ folgt. □

Wir setzen nun die Betrachtungen zum Beispiel 8 fort. Es bezeichne W_λ, $\lambda = +1, -1$, den Eigenunterraum von $\alpha \in O(3)$ zum Eigenwert λ. Folgende Fallunterscheidung bietet sich an:

1. Fall. $W_1 \neq 0$, $W_{-1} \neq 0$. In diesem Fall kann kein nicht reeller Eigenwert existieren, da die nicht reellen Nullstellen eines reellen Polynoms stets in Paaren konjugiert-komplexer auftreten (Satz 2.8.2). Ist e_1 ein Einheitsvektor aus W_1 und e_3 ein Einheitsvektor aus W_{-1}, so sind e_1, e_3 linear unabhängig, $U^2 := \mathfrak{L}(\{e_1, e_3\})$ ist ein zweidimensionaler invarianter Unterraum, und $U^{2\perp}$ ist nach Lemma 3 ein eindimensionaler invarianter Unterraum. Es sei e_2 ein Einheitsvektor aus $U^{2\perp}$; da $\alpha \mid U^{2\perp}$ ebenfalls orthogonal ist, muß nach Beispiel 6 $e_2 \in W_1$ oder $e_2 \in W_{-1}$ gelten. Ebenfalls nach Lemma 3 ist $\langle W_1, W_{-1}\rangle = 0$, so daß $W_{-1} = W_1^\perp$ gelten muß und (e_i) ein orthonormiertes 3-Bein ist. Es gibt also bis auf die Numerierung der Koordinatenachsen nur die folgenden Fälle:

$$\text{a) } (a_{ij}) = \begin{pmatrix} 1 & & 0 \\ & 1 & \\ 0 & & -1 \end{pmatrix}, \qquad \text{b) } (b_{ij}) = \begin{pmatrix} 1 & & 0 \\ & -1 & \\ 0 & & -1 \end{pmatrix}; \tag{48}$$

die erste Matrix definiert eine Spiegelung an der e_1, e_2-Ebene und die zweite eine Spiegelung an der e_3-Achse. (Im Unterschied zu den Schrägspiegelungen (Übung 5.2.7) versteht man in der euklidischen Geometrie unter *Spiegelungen* stets die Involutionen bezüglich der orthogonalen Zerlegungen $V^n = W^k + W^{k\perp}$, das sind also spezielle Schrägspiegelungen, vgl. auch Übung 5.4.2.)

2. Fall. $W_1 \neq 0$, $W_{-1} = 0$. In diesem Fall kann $\dim W_1 = 3$ sein – dann ist $\alpha = \mathrm{id}_{V^3}$ –, oder es muß $\dim W_1 = 1$ sein. Der Fall $\dim W_1 = 2$ ist nicht möglich, wenn -1 kein Eigenwert ist (Satz 2.8.2). Es sei nun e_3 ein Einheitsvektor aus W_1. Dann ist $\mathfrak{L}(\{e_3\})$ ein invarianter Unterraum, und folglich ist auch der dazu orthogonale Unterraum $W^2 := \mathfrak{L}(\{e_3\})^\perp$ invariant. Da $\alpha \mid W^2$ orthogonal ist, können wir Beispiel 7 heranziehen: In einer beliebigen orthogonalen Basis (e_1, e_2) von W^2 muß $\alpha \mid W^2$ die Darstellung (44) oder (45) haben. Nach Übung 7 kann aber nur (44) eintreten; denn aus (45) folgt, daß -1 Eigenwert von $\alpha \mid W^2$, also auch von α ist. Wir erhalten:

Eine orthogonale Transformation des V^3, die nicht den Eigenwert -1 besitzt, ist die Identität oder eine Drehung um eine feste Achse; wählen wir diese als e_3-Achse, so hat α in einem sonst beliebigen orthonormierten 3-Bein (e_i) eine Matrix der Form

$$(a_{ij}) = \begin{pmatrix} \cos\varphi & -\sin\varphi & 0 \\ \sin\varphi & \cos\varphi & 0 \\ 0 & 0 & 1 \end{pmatrix}; \tag{49}$$

φ ist der *Drehwinkel*; wegen $W_{-1} = 0$ muß hier $\varphi \not\equiv \pi \bmod 2\pi$ sein.

3. Fall. $W_1 = 0$, $W_{-1} \neq 0$. Wie im zweiten Fall schließt man, daß nur $\dim W_{-1} = 3$ oder $\dim W_{-1} = 1$ möglich ist. Dann ist

a) $\dim W_{-1} = 3$:

$$(a_{ij}) = \begin{pmatrix} -1 & & 0 \\ & -1 & \\ 0 & & -1 \end{pmatrix} \tag{50}$$

bei beliebiger Wahl des 3-Beins (e_i); a ist die *Spiegelung an* o. Ganz analoge Überlegungen wie im zweiten Fall ergeben

b) dim $W_{-1} = 1$:

$$(b_{ij}) = \begin{pmatrix} \cos\varphi & -\sin\varphi & 0 \\ \sin\varphi & \cos\varphi & 0 \\ 0 & 0 & -1 \end{pmatrix}; \tag{51}$$

eine solche Transformation nennt man eine *Drehspiegelung*, weil gleichzeitig in der e_1, e_2-Ebene gedreht und an ihr gespiegelt wird.

Man beachte, daß der Fall 1 a) und der Fall 3 a) in (51) enthalten sind, wenn man alle Werte von φ zuläßt. Man braucht nur $\varphi = 0, \pi$ zu setzen. Numeriert man im Fall 1 b) die Achsen geeignet um, so kann man ihn als Spezialfall von (49) ansehen, und zwar für $\varphi = \pi$. Daher können wir zusammenfassend feststellen:

Eine orthogonale Transformation $a \in \boldsymbol{SO}(3)$ ist stets eine Drehung, d. h., sie kann bei geeigneter Wahl der Achsen in der Form (49) *dargestellt werden; gilt $a \in \boldsymbol{O}(3) \setminus \boldsymbol{SO}(3)$, so ist a eine Drehspiegelung, die bei geeigneter Wahl der Achsen in der Form* (51) *dargestellt wird.*

Es ist nun leicht, auch die Bewegungen $f \in \mathfrak{E}(n)$, $n = 2, 3$, zu beschreiben. Für beliebiges $n \in \mathbf{N}$ nennt man $f \in \mathfrak{E}(n)$ eine *eigentliche* bzw. *uneigentliche* Bewegung, je nachdem, ob $\det a_f = 1$ oder $\det a_f = -1$ gilt (Folgerung 5). Für eine feinere Einteilung ist es zweckmäßig, die Fixpunktmenge (vgl. Übung 5.1.6)

$$\boldsymbol{M}_f := \{x \mid x \in \boldsymbol{E}^n, f(x) = x\}$$

zu betrachten. Stellt man unter Benutzung der schon angegebenen Matrizendarstellungen von a_f und der Verknüpfung mit einer beliebigen Translation das sich aus (43) mit $y_i = x_i$ ergebende Gleichungssystem auf und diskutiert die Lösungsmöglichkeiten, so erhält man folgende Fälle:

$n = 2$, *eigentliche Bewegungen*, $f \neq \mathrm{id}_{\boldsymbol{E}^2}$:

1. $\boldsymbol{M}_f = \emptyset \leftrightarrow f$ *Translation*,

2. $\boldsymbol{M}_f = \{x_0\}$ einpunktig $\leftrightarrow f$ *Drehung um* x_0.

Mit $x_0 = o$ als Ursprung ist dann die Koordinatendarstellung von f von der Form (vgl. (44))

$$y_1 = x_1 \cos\varphi + x_2 \sin\varphi, \qquad y_2 = -x_1 \sin\varphi + x_2 \cos\varphi\,. \tag{52}$$

$n = 2$, *uneigentliche Bewegungen:*

3. $\boldsymbol{M}_f = \boldsymbol{H}^1$ Gerade $\leftrightarrow f$ *Spiegelung an der Geraden* $\boldsymbol{H}^1$.

Wählt man $\boldsymbol{H}^1$ als $\mathfrak{e}_1$-Achse, so gilt

$$y_1 = x_1, \qquad y_2 = -x_2 . \tag{53}$$

4. $\boldsymbol{M}_f = \emptyset \leftrightarrow f$ *Gleitspiegelung:*

$$y_1 = x_1 + a_1, \qquad y_2 = -x_2 \qquad (a_1 \neq 0); \tag{54}$$

hierbei ist $\mathfrak{e}_1 \in \boldsymbol{W}_1$, $\mathfrak{e}_2 \in \boldsymbol{W}_{-1}$ gewählt; der Ursprung liegt auf der einzigen Geraden $\boldsymbol{H}^1 \subset \boldsymbol{E}^2$, für die $f(\boldsymbol{H}^1) = \boldsymbol{H}^1$ gilt.

$n = 3$, *eigentliche Bewegungen*, $f \neq \mathrm{id}_{\boldsymbol{E}^3}$:

1. $\boldsymbol{M}_f = \emptyset$, $a_f = \mathrm{id}_{\boldsymbol{V}^3} \leftrightarrow f$ *Translation.*

2. $\boldsymbol{M}_f = \emptyset$, $a_f \neq \mathrm{id}_{\boldsymbol{V}^3} \leftrightarrow f$ *Schraubung:*

$$\left.\begin{aligned} y_1 &= x_1 \cos\varphi + x_2 \sin\varphi , \\ y_2 &= -x_1 \sin\varphi + x_2 \cos\varphi , \\ y_3 &= x_3 + a_3, \qquad a_3 \neq 0 ; \end{aligned}\right\} \tag{55}$$

dabei hat a_f die Matrix (49), $\mathfrak{e}_3 \in \boldsymbol{W}_1$, $\boldsymbol{W}_{-1} = \{0\}$ für $\varphi \neq \pi$; der Ursprung o ist auf der *Schraubachse* gewählt; das ist die einzige Gerade $\boldsymbol{H}^1 \subset \boldsymbol{E}^3$, für die $f(\boldsymbol{H}^1) = \boldsymbol{H}^1$ gilt.

3. $\boldsymbol{M}_f = \boldsymbol{H}^1 \leftrightarrow f$ ist *Drehung um die Gerade* $\boldsymbol{H}^1$.

Wählt man $\mathfrak{e}_3 \in \boldsymbol{W}^1$ und $o \in \boldsymbol{H}^1$, so hat f eine Darstellung (55) mit $a_3 = 0$.

$n = 3$, *uneigentliche Bewegungen:*

4. $\boldsymbol{M}_f = \{x_0\} \leftrightarrow f$ ist *Drehspiegelung:*

$$\left.\begin{aligned} y_1 &= x_1 \cos\varphi + x_2 \sin\varphi , \\ y_2 &= -x_1 \sin\varphi + x_2 \cos\varphi , \\ y_3 &= -x_3 . \end{aligned}\right\} \tag{56}$$

Dabei wurde $o = x_0$ in den Fixpunkt gelegt und $\mathfrak{e}_3 \in \boldsymbol{W}_{-1}$ gewählt; es gilt $0 < \varphi < 2\pi$.

5. $\boldsymbol{M}_f = \boldsymbol{H}^2 \leftrightarrow f$ ist *Spiegelung an der Ebene* $\boldsymbol{H}^2$:

$$y_1 = x_1, \qquad y_2 = x_2, \qquad y_3 = -x_3 . \tag{57}$$

Dabei gilt $o \in \boldsymbol{H}^2$, $\mathfrak{e}_3 \in \boldsymbol{W}_{-1}$.

6. $\boldsymbol{M}_f = \emptyset \leftrightarrow f$ ist *Gleitspiegelung:*

$$y_1 = x_1 + a_1, \qquad y_2 = x_2, \qquad y_3 = -x_3 \qquad (a_1 \neq 0) . \tag{58}$$

Hier ist $\mathfrak{e}_3 \in \boldsymbol{W}_{-1}$ gewählt, o liegt in der einzigen Ebene $\boldsymbol{H}^2$ mit $f(\boldsymbol{H}^2) = \boldsymbol{H}^2$ und $\boldsymbol{H}^2$ orthogonal zu $\mathfrak{e}_3$, $\mathfrak{e}_1$ hat die Richtung des Translationsvektors.

Für die Herleitung dieser vollständigen Fallunterscheidung diskutieren wir etwa den Fall $n = 3$, f uneigentliche Bewegung. Wählen wir $\mathfrak{e}_3 \in \boldsymbol{W}_{-1}$, so hat a_f eine Matrix der Gestalt (51); nach Verknüpfung mit einer Translation erhalten wir die Koordi-

natendarstellung von f:

$$y_1 = x_1 \cos\varphi + x_2 \sin\varphi + a_1\,, \tag{59}$$

$$y_2 = -x_1 \sin\varphi + x_2 \cos\varphi + a_2\,, \tag{60}$$

$$y_3 = -x_3 + a_3\,. \tag{61}$$

Schreiben wir statt (61) $y_3 - (a_3/2) = -(x_3 - (a_3/2))$, so erkennt man, daß man durch die Koordinatentransformation $\hat{x}_1 = x_1$, $\hat{x}_2 = x_2$, $\hat{x}_3 = x_3 - (a_3/2)$ statt (61) sogar

$$y_3 = -x_3 \tag{62}$$

schreiben kann. Wir betrachten nun die Gleichungen (59), (60) für sich allein; sie stellen eine eigentliche Bewegung g der $\mathfrak{e}_1, \mathfrak{e}_2$-Ebene $\boldsymbol{E}^2$ dar. Die Bedingungen für einen Fixpunkt von g lauten $y_i = x_i$, $i = 1, 2$, d. h.

$$\left.\begin{aligned} x_1(1-\cos\varphi) - x_2 \sin\varphi &= a_1\,, \\ x_1 \sin\varphi + x_2(1-\cos\varphi) &= a_2\,. \end{aligned}\right\} \tag{63}$$

Die Determinante dieses linearen Gleichungssystems ist $2(1-\cos\varphi)$; für $\varphi \not\equiv 0 \bmod 2\pi$ gibt es also genau einen Fixpunkt x_0. Legen wir den Ursprung in diesen Fixpunkt, so gilt $x_0 = o$ (in bezug auf $\boldsymbol{E}^2$), und (59), (60) gehen in (52) über; (52) und (62) ergeben aber gerade (56). Hieraus erkennt man, daß $o \in \boldsymbol{E}_3$ der einzige Fixpunkt ist und der Fall 4 vorliegt.

Im Fall $\varphi \equiv 0 \bmod 2\pi$ erhalten wir wegen (62) für f die Koordinatendarstellung

$$y_1 = x_1 + a_1, \qquad y_2 = x_2 + a_2, \qquad y_3 = -x_3\,. \tag{64}$$

Es gibt nun zwei einander ausschließende Möglichkeiten: Entweder der Translationsvektor $\mathfrak{a}$ mit den Koordinaten $(a_1, a_2, 0)$ ist gleich $\mathfrak{o}$ oder $\mathfrak{a} \neq \mathfrak{o}$. Der Fall $\mathfrak{a} = \mathfrak{o}$ führt sofort auf (57); im Fall $\mathfrak{a} \neq \mathfrak{o}$ läßt sich $\mathfrak{a} = \mathfrak{e}_1 a_1$ mit $a_1 > 0$ erreichen, da $\mathfrak{e}_1, \mathfrak{e}_2$ beliebig (orthonormiert) in $\boldsymbol{W}_1$ gewählt werden können, und es resultiert Fall 6. Weil die Fälle einander ausschließen, gelten die ausgesprochenen Behauptungen.

Wir wollen abschließend noch die unitäre Gruppe $\boldsymbol{U}(n)$ betrachten und den folgenden Satz beweisen.

Satz 7. *Zu jeder unitären Abbildung $a \in \boldsymbol{U}(n)$ gibt es eine orthonormierte Basis $(\mathfrak{e}_i)$ des unitären Raumes $\boldsymbol{V}^n$, so daß die Matrix (a_{ij}) von a die Form*

$$(a_{ij}) = \begin{pmatrix} e^{i\alpha_1} & & & \mathbf{0} \\ & e^{i\alpha_2} & & \\ & & \ddots & \\ \mathbf{0} & & & e^{i\alpha_n} \end{pmatrix}, \qquad \alpha_j \in \mathbf{R}\,, \tag{65}$$

besitzt.

Beweis. Da hier $K=\mathbf{C}$ ist, existiert ein Eigenwert λ von a, der wegen Satz 6 die Form $\lambda=e^{i\alpha_1}$, $\alpha_1\in\mathbf{R}$, besitzt. Dann ist $W^1:=\mathfrak{L}(\{e_1\})$, e_1 ein Eigenvektor zu $e^{i\alpha_1}$ vom Betrag $|e_1|=1$, ein bei a invarianter Unterraum, und nach Lemma 3 ist auch $W^{1\perp}$ invariant. In $W^{1\perp}$ finden wir einen Eigenvektor e_2 zu einem Eigenwert $e^{i\alpha_2}$ usw. Ein einfacher Induktionsschluß beweist die Behauptung. □

Übung 9. Man beweise: Die Menge aller Matrizen der Gestalt (65) ist eine Untergruppe der Matrixgruppe $\boldsymbol{U}(n)$; sie ist zur *Torusgruppe* T^n isomorph und daher abelsch; T^n ist definiert als das n-fache direkte Produkt der Gruppe $T^1:=S^1$ der komplexen Zahlen vom Betrag 1 mit sich selbst.

Übung 10. Man beweise, daß man jede Matrix $(a_{lj})\in\boldsymbol{U}(2)$ in der Gestalt

$$(a_{lj})=\begin{pmatrix} e^{i\beta}\cos\alpha & -e^{i\gamma}\sin\alpha \\ e^{i\delta}\sin\alpha & e^{i\varepsilon}\cos\alpha \end{pmatrix}$$

mit $0\leqq\alpha\leqq\pi/2$ darstellen kann, wobei $\alpha=0$ oder $\alpha=\pi/2$ oder $\beta-\gamma\equiv\delta-\varepsilon \bmod 2\pi$ erfüllt sein muß.

Übung 11. Man beweise, daß man jeden orthogonalen Operator $a\in\boldsymbol{O}(n)$ in bezug auf eine geeignete Basis des euklidischen Vektorraumes $\boldsymbol{V}^n$ durch eine Matrix der Gestalt

$$\begin{pmatrix} D(\alpha_1) & & & & & & \\ & D(\alpha_2) & & & & \mathbf{0} & \\ & & \ddots & & & & \\ & & & D(\alpha_k) & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \\ & & & & & & & -1 & \\ & & & & & & & & \ddots & \\ \mathbf{0} & & & & & & & & & -1 \end{pmatrix}$$

darstellen kann; hier bezeichnet $D(\alpha_i)$ die Matrix (44) mit $\varphi=\alpha_i$. Man betrachte die bei a invarianten Unterräume und deute das Resultat geometrisch.

Übung 12. Man zeige: Zu jedem $a\in\boldsymbol{SO}(n)$ existiert eine zur Torusgruppe T^k, $(n/2)-1<k\leqq n/2$, isomorphe Untergruppe $\tilde{T}^k\subseteq\boldsymbol{SO}(n)$ mit $a\in\tilde{T}^k$.

Übung 13. Es seien $\boldsymbol{E}^n$, $\boldsymbol{B}^k$ euklidische Punkträume und $f:\boldsymbol{E}^n\to\boldsymbol{B}^k$ eine Abbildung, die (39) erfüllt. Man beweise, daß f dann affin ist und $n\leqq k$ gilt. Eine den Abstand erhaltende Abbildung $f:\boldsymbol{E}^n\to\boldsymbol{E}^n$ ist eine Bewegung. (Hinweis. Man benutze Übung 1.2, um die Bedingung von Übung 5.1.8 nachzuweisen.)

§ 3. Orientierung. Volumen. Vektorprodukt

In diesem Paragraphen betrachten wir euklidische Punkt- und Vektorräume $[\boldsymbol{E}^n, \boldsymbol{V}^n, \mathbf{R}, \langle\ ,\ \rangle]$. Wählen wir in $\boldsymbol{V}^n$ zwei orthonormierte n-Beine (e_i), $(\hat{e}_i)$, so ist die Matrix der Darstellung

$$\hat{e}_j=\sum_{i=1}^{n} e_i\alpha_{ij} \tag{1}$$

orthogonal; denn das ist ja die Matrix der linearen Abbildung $a \in \boldsymbol{L}(\boldsymbol{V}^n)$ mit $a(\mathfrak{e}_i) = \hat{\mathfrak{e}}_i$, $i = 1, \ldots, n$, bezüglich der Basis $(\mathfrak{e}_i)$, und diese muß nach Satz 2.4 orthogonal sein. Nach Lemma 2.2 gilt folgendes: Ist $(\mathfrak{e}_i)$ eine feste orthonormierte Basis des $\boldsymbol{V}^n$, so ist die Zuordnung

$$(\alpha_{ij}) \in \boldsymbol{O}(n) \mapsto (\hat{\mathfrak{e}}_j)' := (\mathfrak{e}_i)' (\alpha_{ij}) \in \mathfrak{O}_n \tag{2}$$

eine bijektive Abbildung von $\boldsymbol{O}(n)$ auf die Menge $\mathfrak{O}_n$ aller orthonormierten n-Beine des Vektorraumes $\boldsymbol{V}^n$, so daß wir uns die orthogonalen Abbildungen durch die zugehörigen orthonormierten n-Beine veranschaulichen können.

In der euklidischen Geometrie werden wir nur orthogonale, kartesische Koordinatensysteme betrachten. Es ist klar, daß die Gesamtheit der orthogonalen Punktkoordinatensysteme einen der euklidischen Geometrie $[\mathfrak{E}(n), \boldsymbol{E}^n]$ angepaßten Atlas bilden; Entsprechendes gilt für die Vektorkoordinaten und die Transformationsgruppe $[\boldsymbol{O}(n), \boldsymbol{V}^n]$ (vgl. Definition 5.7.5). Die Formeln (5.7.6), (5.7.10) für die Transformation der Vektorkoordinaten und der Basisvektoren bleibt erhalten; da nach obigem die Matrix $(\alpha_{ij}) \in \boldsymbol{O}(n)$ ist, *transformieren sich wegen* $(\alpha_{ij}) = (\alpha_{ij})^*$ *(nach* (2.29)) *Basisvektoren und Vektorkoordinaten mit derselben Matrix.*

Nach Beispiel 2.3 können wir $\boldsymbol{V}^n$ und $\boldsymbol{V}^{n\prime}$ vermöge (2.18) identifizieren. Die Orthogonalitätsrelationen $\langle \mathfrak{e}_i, \mathfrak{e}_j \rangle = \delta_{ij}$ besagen, daß jede orthogonale Basis zu sich selbst dual ist. Daher stimmen die Transformationsformeln für die duale Basis und die dualen Vektorkoordinaten (5.7.13), (5.7.16) mit den entsprechenden des Raumes $\boldsymbol{V}^n$ überein, d. h., alle erfolgen mit derselben Matrix. Analog bleibt die Formel (5.7.36) für die Transformation der orthogonalen Punktkoordinaten erhalten, es ist nur $(\alpha_{ij}) \in \boldsymbol{O}(n)$ zu beachten. Für die Orientierung von $\boldsymbol{V}^n$ und $\boldsymbol{E}^n$ (Definition 4.7.4) ergibt sich aus Folgerung 2.5 unmittelbar

Satz 1. *Zwei orthonormierte n-Beine* $(\mathfrak{e}_i)$, $(\hat{\mathfrak{e}}_i)$ *des euklidischen Vektorraumes* $\boldsymbol{V}^n$ *sind gleich orientiert genau dann, wenn für die durch* (1) *bestimmte Matrix* $(\alpha_{ij}) \in \boldsymbol{SO}(n)$, *also* $\det(\alpha_{ij}) = 1$ *gilt;* $(\mathfrak{e}_i)$, $(\hat{\mathfrak{e}}_i) \in \mathfrak{O}_n$ *sind daher genau dann gleich orientiert, wenn sie dieselbe Volumenfunktion*

$$[\mathfrak{x}_1, \ldots, \mathfrak{x}_n] = \det(\xi_{ij}) \quad \text{für} \quad \mathfrak{x}_j = \sum_{i=1}^{n} \mathfrak{e}_i \xi_{ij} \in \boldsymbol{V}^n, \qquad j = 1, \ldots, n, \tag{3}$$

bestimmen. □

Wenn wir von dem (*orientierten*) *Volumen* in einem orientierten euklidischen Raum sprechen, meinen wir stets das durch (3) eindeutig bestimmte, von der Wahl der *positiv orientierten* Basis $(\mathfrak{e}_i)$ unabhängige Volumen; ist der euklidische Raum nicht orientiert, so verstehen wir unter dem (nicht orientierten) *Volumen* die stets nicht negative, von der Wahl der orthonormierten Basis $(\mathfrak{e}_i)$ unabhängige Funktion

$$v(\mathfrak{x}_1, \ldots, \mathfrak{x}_n) := |\det(\xi_{ij})| . \tag{4}$$

Während

$$v(\mathfrak{e}_1, \ldots, \mathfrak{e}_n) = 1 \quad \text{für alle} \quad (\mathfrak{e}_i) \in \mathfrak{O}_n \tag{5}$$

gilt, zerfällt $\mathfrak{D}_n$ in die beiden Klassen der positiv bzw. negativ orientierten n-Beine des orientierten $\boldsymbol{V}^n$:

$$\mathfrak{D}_n = \mathfrak{D}_n^+ \cup \mathfrak{D}_n^-,\ (\mathfrak{e}_i) \in \mathfrak{D}_n^+ \text{ (bzw. } \mathfrak{D}_n^-) :\Leftrightarrow [\mathfrak{e}_1, \ldots, \mathfrak{e}_n] = 1 \text{ (bzw. } -1)\,. \tag{6}$$

Wählen wir $(\mathfrak{e}_i)$ positiv orientiert, so folgt aus (2) die bijektive Abbildung

$$(\alpha_{ij}) \in \boldsymbol{SO}(n) \mapsto (\hat{\mathfrak{e}}_i) \in \mathfrak{D}_n^+\,. \tag{7}$$

Wenn (α_{ij}) die Matrix der orthogonalen Transformation $a \in \boldsymbol{O}(n)$ ist, bedeutet (7), daß die Elemente $a \in \boldsymbol{SO}(n)$ gleich orientierte n-Beine wieder in gleich orientierte überführen; man erkennt allgemeiner, daß ein Element $a \in \boldsymbol{GL}(\boldsymbol{V}^n)$ *die Orientierung erhält*, wenn die Norm $N(a) > 0$ ist, vgl. (5.7.32) für $K = \mathbf{R}$.

Das Skalarprodukt des euklidischen Vektorraumes bestimmt somit eine Volumenfunktion bis auf das Vorzeichen, das durch Vorgabe einer Orientierung festgelegt wird. Bildet man die Determinante des Matrizenproduktes $(\xi_{ij})\,(\xi_{ij})'$, so folgt gus Satz 4.8.2 und (1.3)

$$v(\mathfrak{x}_1, \ldots, \mathfrak{x}_n)^2 = \begin{vmatrix} \langle \mathfrak{x}_1, \mathfrak{x}_1 \rangle & \langle \mathfrak{x}_1, \mathfrak{x}_2 \rangle & \cdots & \langle \mathfrak{x}_1, \mathfrak{x}_n \rangle \\ \langle \mathfrak{x}_2, \mathfrak{x}_1 \rangle & \langle \mathfrak{x}_2, \mathfrak{x}_2 \rangle & \cdots & \langle \mathfrak{x}_2, \mathfrak{x}_n \rangle \\ \cdots & \cdots & \cdots & \cdots \\ \langle \mathfrak{x}_n, \mathfrak{x}_1 \rangle & \langle \mathfrak{x}_n, \mathfrak{x}_2 \rangle & \cdots & \langle \mathfrak{x}_n, \mathfrak{x}_n \rangle \end{vmatrix}; \tag{8}$$

$\det(\langle \mathfrak{x}_i, \mathfrak{x}_j \rangle)$ heißt die *Gramsche Determinante* der Vektoren $\mathfrak{x}_1, \ldots, \mathfrak{x}_n$. Da $m \leqq n$ Vektoren $(\mathfrak{x}_\alpha)_{\alpha=1,\ldots,m}$ des $\boldsymbol{V}^n$ immer in einem m-dimensionalen Unterraum liegen, der selbst ein euklidischer Vektorraum ist (vgl. Satz 1.1), erhalten wir

Folgerung 1. *Es sei $\boldsymbol{V}$ ein euklidischer Vektorraum beliebiger Dimension und $m \in \mathbf{N}$, $m \leqq \dim \boldsymbol{V}$. Dann wird durch*

$$v(\mathfrak{x}_1, \ldots, \mathfrak{x}_m)^2 = \det(\langle \mathfrak{x}_\alpha, \mathfrak{x}_\beta \rangle)_{\alpha,\beta=1,\ldots,m} \tag{9}$$

jedem m-Tupel von Vektoren $\mathfrak{x}_\alpha \in \boldsymbol{V}$ eine nichtnegative Zahl $v(\mathfrak{x}_1, \ldots, \mathfrak{x}_m)^2 \in \mathbf{R}$ zugeordnet, die gleich dem Quadrat des Volumens des von $\mathfrak{x}_1, \ldots, \mathfrak{x}_m$ aufgespannten Parallelepipeds ist. Die Vektoren $\mathfrak{x}_1, \ldots, \mathfrak{x}_m$ sind linear abhängig genau dann, wenn $\det(\langle \mathfrak{x}_\alpha, \mathfrak{x}_\beta \rangle) = 0$ *gilt. Die Gramsche Determinante* (9) *ist invariant gegenüber orthogonalen Transformationen $a \in \boldsymbol{O}(n)$:*

$$\det(\langle a\mathfrak{x}_\alpha, a\mathfrak{x}_\beta \rangle) = \det(\langle \mathfrak{x}_\alpha, \mathfrak{x}_\beta \rangle)\,. \quad \square \tag{10}$$

Man beachte, daß in der euklidischen Geometrie m-dimensionale Volumina für alle m-Parallelepipede Π^m, $0 < m \leqq n$, definiert sind; sie sind bis auf das Vorzeichen eindeutig bestimmt. Im Unterschied zur affinen Geometrie, in der nur Volumenverhältnisse parallel liegender Parallelepipede einen invarianten Sinn haben (vgl. Satz 5.4.9), können wir in der euklidischen Geometrie Volumina beliebig zueinander liegender Parallelepipede miteinander vergleichen.

Beispiel 1. Es sei $\boldsymbol{W}^m \subset \boldsymbol{V}^n$ ein orientierter Unterraum des Vektorraumes $\boldsymbol{V}^n$, $0 < m < n$. Dann sind die Orientierungen von $\boldsymbol{W}^{m\perp}$ und die von $\boldsymbol{V}^n$ einander umkehrbar eindeutig durch folgende *Verträglichkeitsbedingung* zugeordnet: *Ist* $(\mathfrak{e}_\alpha)$,

$\alpha=1, \ldots, m$, *ein positiv orientiertes* m*-Bein von* $\boldsymbol{W}^m$ *und* $(\mathfrak{e}_\varkappa)$, $\varkappa=m+1, \ldots, n$, *ein positiv orientiertes* $(n-m)$*-Bein von* $\boldsymbol{W}^{m\perp}$, *so sei* $(\mathfrak{e}_i)$, $i=1, \ldots, n$, *ein positiv orientiertes* n*-Bein von* $\boldsymbol{V}^n$.

Sind die Orientierungen von $\boldsymbol{W}^m$, $\boldsymbol{W}^{m\perp}$, $\boldsymbol{V}^n$ so gewählt, daß die Verträglichkeitsbedingung erfüllt ist, so nennen wir diese Räume *verträglich orientiert*. Man beweist leicht für die zu den verträglichen Orientierungen gehörenden Volumenfunktionen: Gilt $\mathfrak{x}_\alpha \in \boldsymbol{W}^m$, $\alpha=1, \ldots, m$, und $\mathfrak{x}_\varkappa \in \boldsymbol{W}^{m\perp}$, $\varkappa=m+1, \ldots, n$, so ist

$$[\mathfrak{x}_1, \ldots, \mathfrak{x}_n]=[\mathfrak{x}_1, \ldots, \mathfrak{x}_m]\,[\mathfrak{x}_{m+1}, \ldots, \mathfrak{x}_n]\,. \tag{11}$$

Mit Hilfe der Gramschen Determinante beweist man leicht die analoge Formel für die nicht orientierten Volumina

$$v(\mathfrak{x}_1, \ldots, \mathfrak{x}_n)=v(\mathfrak{x}_1, \ldots, \mathfrak{x}_m)\cdot v(\mathfrak{x}_{m+1}, \ldots, \mathfrak{x}_n)\,. \tag{12}$$

Beispiel 2. Wir gehen von einer k-Ebene $\boldsymbol{H}^k=\boldsymbol{H}(a, \boldsymbol{W}^k)\subset\boldsymbol{E}^n$, $0<k<n$, aus und wollen das Lot $\overrightarrow{y_0x}$ von einem Punkt $x\in\boldsymbol{E}^n$ auf $\boldsymbol{H}^k$ bestimmen, vgl. Übung 2.3. Nach Lemma 2.1 ist $\mathfrak{x}_1=\overrightarrow{y_0x}$ der durch $\langle \boldsymbol{W}^k, \overrightarrow{y_0x}\rangle=0$, $y_0\in\boldsymbol{H}^k$, d. h. der durch die orthogonale Zerlegung $\overrightarrow{ax}=\overrightarrow{ay_0}+\overrightarrow{y_0x}$, $\overrightarrow{ay_0}\in\boldsymbol{W}^k$, $\overrightarrow{y_0x}\in\boldsymbol{W}^{k\perp}$, eindeutig definierte Vektor; er hängt wegen a, $y_0\in\boldsymbol{H}^k$ nicht von der Wahl des Bezugspunktes $a\in\boldsymbol{H}^k$ ab. Es sei $(\mathfrak{w}_\alpha)$ eine beliebige, nicht notwendig orthonormierte Basis von $\boldsymbol{W}^k$. Die Bedingung $\langle \boldsymbol{W}^k, \overrightarrow{y_0x}\rangle=0$ ist äquivalent zu $\langle \mathfrak{w}_\alpha, \overrightarrow{y_0x}\rangle=0$ für $\alpha=1, \ldots, k$. Aus $\overrightarrow{y_0x}=\overrightarrow{ax}-\overrightarrow{ay_0}$ erhalten wir wegen $\overrightarrow{ay_0}=\sum_{\alpha=1}^{k}\mathfrak{w}_\alpha\eta_\alpha\in\boldsymbol{W}^k$ das lineare Gleichungssystem

$$\langle \mathfrak{w}_\alpha, \overrightarrow{ay_0}\rangle=\sum_{\alpha=1}^{k}\langle \mathfrak{w}_\alpha, \mathfrak{w}_\beta\rangle\,\eta_\beta=\langle \mathfrak{w}_\alpha, \overrightarrow{ax}\rangle, \qquad \alpha=1, \ldots, k\,. \tag{13}$$

Nach Folgerung 1 gilt $\det(\langle \mathfrak{w}_\alpha, \mathfrak{w}_\beta\rangle)\neq 0$, und die Anwendung der Cramerschen Regel ergibt uns die Koordinaten η_α der orthogonalen Projektion $\overrightarrow{ay_0}$ von $\overrightarrow{ax}$ auf $\boldsymbol{W}^k$:

$$\eta_\alpha=D_\alpha/v(\mathfrak{w}_1, \ldots, \mathfrak{w}_k)^2$$

mit

$$D_\alpha=\begin{vmatrix} \langle \mathfrak{w}_1, \mathfrak{w}_1\rangle & \ldots & \langle \mathfrak{w}_1, \mathfrak{w}_{\alpha-1}\rangle & \langle \mathfrak{w}_1, \overrightarrow{ax}\rangle & \langle \mathfrak{w}_1, \mathfrak{w}_{\alpha+1}\rangle & \ldots & \langle \mathfrak{w}_1, \mathfrak{w}_k\rangle \\ \langle \mathfrak{w}_2, \mathfrak{w}_1\rangle & \ldots & \langle \mathfrak{w}_2, \mathfrak{w}_{\alpha-1}\rangle & \langle \mathfrak{w}_2, \overrightarrow{ax}\rangle & \langle \mathfrak{w}_2, \mathfrak{w}_{\alpha+1}\rangle & \ldots & \langle \mathfrak{w}_2, \mathfrak{w}_k\rangle \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \langle \mathfrak{w}_k, \mathfrak{w}_1\rangle & \ldots & \langle \mathfrak{w}_k, \mathfrak{w}_{\alpha-1}\rangle & \langle \mathfrak{w}_k, \overrightarrow{ax}\rangle & \langle \mathfrak{w}_k, \mathfrak{w}_{\alpha+1}\rangle & \ldots & \langle \mathfrak{w}_k, \mathfrak{w}_k\rangle \end{vmatrix}. \tag{14}$$

Das Lot erhält man aus $\overrightarrow{y_0x}=\overrightarrow{ax}-\sum_\alpha \mathfrak{w}_\alpha\eta_\alpha$, und den Abstand $\varrho(x, \boldsymbol{H}^k)=|\overrightarrow{y_0x}|$ bestimmt man aus der Formel (15) der folgenden Übung (mit $\mathfrak{x}_1=\overrightarrow{y_0x}$, $\mathfrak{x}=\overrightarrow{ax}$).

Übung 1. Man zeige: Mit den Voraussetzungen und Bezeichnungen von Lemma 2.1 (im Fall $K=\mathbf{R}$) gilt bei einer beliebigen Basis $(\mathfrak{w}_\alpha)$ von $\boldsymbol{W}^k$ für die Länge des Lotes $\mathfrak{x}_1$ von $\mathfrak{x}\in\boldsymbol{V}^n$ auf $\boldsymbol{W}^k$

$$|\mathfrak{x}_1|=v(\mathfrak{w}_1, \ldots, \mathfrak{w}_k, \mathfrak{x})/v(\mathfrak{w}_1, \ldots, \mathfrak{w}_k)\,, \tag{15}$$

d. h., $|\mathfrak{x}_1|^2$ ist Quotient zweier Gramscher Determinanten. (Hinweis. (15) entspricht der bekannten Formel Höhe = Volumen/Grundfläche für das Volumen eines Quaders.)

Übung 2. a) Unter den Voraussetzungen von Folgerung 1 beweise man die Ungleichung

$$v(\mathfrak{x}_1, \ldots, \mathfrak{x}_m)^2 \leqq \prod_{\mu=1}^{m} \langle \mathfrak{x}_\mu, \mathfrak{x}_\mu \rangle \tag{16}$$

und zeige, daß das Gleichheitszeichen dann und nur dann gilt, wenn die Vektoren $\mathfrak{x}_\mu$ paarweise orthogonal sind oder wenigstens ein $\mathfrak{x}_\mu = \mathfrak{o}$ ist. — b) Man gebe eine geometrische Deutung für (16) an. — c) Man beweise für eine beliebige Matrix $(a_{ij}) \in \mathbf{M}_n(\mathbf{R})$ die *Hadamardsche Ungleichung*

$$\det (a_{ij})^2 \leqq \prod_{j=1}^{n} \left(\sum_{i=1}^{n} a_{ij}^2 \right) \tag{17}$$

und gebe ein Kriterium dafür an, daß in (17) das Gleichheitszeichen gilt.

Übung 3. Man beweise die Cauchy-Schwarz-Bunjakovskijsche Ungleichung (Satz 1.2) mit Hilfe von Folgerung 1.

Wir benötigen nun folgenden Hilfssatz:

Lemma 1. *Es seien* $\mathfrak{b}_\alpha \in \boldsymbol{V}^n$, $\alpha = 1, \ldots, m \leqq n$, *Vektoren des euklidischen Vektorraumes* $\boldsymbol{V}^n$ *und* $(b_{\varkappa\alpha}) \in \mathbf{M}_{m-1,m}(\mathbf{R})$ *eine Matrix. Dann gibt es genau einen Vektor* $\mathfrak{n} \in \boldsymbol{V}^n$ *so, daß für alle* $\mathfrak{x} \in \boldsymbol{V}^n$ *die Gleichung*

$$\langle \mathfrak{n}, \mathfrak{x} \rangle = \begin{vmatrix} \langle \mathfrak{b}_1, \mathfrak{x} \rangle & \langle \mathfrak{b}_2, \mathfrak{x} \rangle & \ldots & \langle \mathfrak{b}_m, \mathfrak{x} \rangle \\ b_{11} & b_{12} & \ldots & b_{1m} \\ \ldots & \ldots & \ldots & \ldots \\ b_{m-1,1} & b_{m-1,2} & \ldots & b_{m-1,m} \end{vmatrix} \tag{18}$$

gilt. Dabei ist

$$\mathfrak{n} = \sum_{\alpha=1}^{m} \mathfrak{b}_\alpha A_{1\alpha} \in \mathfrak{L}(\{\mathfrak{b}_1, \ldots, \mathfrak{b}_m\}), \tag{19}$$

wobei $A_{1\alpha}$ *die Adjunkten der ersten Zeile der in* (18) *stehenden Matrix bezeichnen.*

Beweis. Offenbar ist die rechte Seite von (18) eine in $\mathfrak{x}$ lineare Funktion $f: \boldsymbol{V}^n \to \mathbf{R}$, d. h. $f \in \boldsymbol{V}^{n\prime}$. Benutzen wir den kanonischen Isomorphismus φ aus Beispiel 2.3 zur Identifizierung von $\boldsymbol{V}^n$ und $\boldsymbol{V}^{n\prime}$, so erhalten wir den eindeutig bestimmten Vektor $\mathfrak{n} = \varphi^{-1}(f)$. Aus dem Laplaceschen Entwicklungssatz folgt bei Entwicklung von (18) nach der ersten Zeile

$$\langle \mathfrak{n}, \mathfrak{x} \rangle = \sum_{\alpha=1}^{m} \langle \mathfrak{b}_\alpha, \mathfrak{x} \rangle A_{1\alpha} = \left\langle \sum_{\alpha=1}^{m} \mathfrak{b}_\alpha A_{1\alpha}, \mathfrak{x} \right\rangle,$$

und weil diese Gleichung für alle $\mathfrak{x} \in \boldsymbol{V}^n$ gilt, folgt (19). □

Die Beziehung (19) können wir auch als formale Definition von $\mathfrak{n}$ auffassen und in der Gestalt

$$n=\begin{vmatrix} \mathfrak{b}_1 & \mathfrak{b}_2 & \dots & \mathfrak{b}_m \\ b_{11} & b_{12} & \dots & b_{1m} \\ \dots & \dots & \dots & \dots \\ b_{m-1,1} & b_{m-1,2} & \dots & b_{m-1,m} \end{vmatrix} \tag{20}$$

schreiben. Man bemerkt, daß man (20) auch nach der Formel (4.7.17) der Definition der Determinanten berechnen kann.

Übung 4 (*Orthogonalisierung nach* G. Szegö). Es sei $(\mathfrak{a}_k)$, $\mathfrak{a}_k \in \boldsymbol{V}$, eine linear unabhängige Familie des euklidischen Vektorraumes $\boldsymbol{V}$ und $G_k := v(\mathfrak{a}_1, \dots, \mathfrak{a}_k)^2$. Man beweise, daß die nach Satz 2.2 eindeutig bestimmte orthonormierte Familie $(\mathfrak{e}_k)$ durch

$$\mathfrak{e}_1 = \frac{\mathfrak{a}_1}{\sqrt{G_1}}, \qquad \mathfrak{e}_k = \begin{vmatrix} \mathfrak{a}_1 & \mathfrak{a}_2 & \dots & \mathfrak{a}_k \\ \langle \mathfrak{a}_1, \mathfrak{a}_1 \rangle & \langle \mathfrak{a}_1, \mathfrak{a}_2 \rangle & \dots & \langle \mathfrak{a}_1, \mathfrak{a}_k \rangle \\ \dots & \dots & \dots & \dots \\ \langle \mathfrak{a}_{k-1}, \mathfrak{a}_1 \rangle & \langle \mathfrak{a}_{k-1}, \mathfrak{a}_2 \rangle & \dots & \langle \mathfrak{a}_{k-1}, \mathfrak{a}_k \rangle \end{vmatrix} (G_{k-1} \cdot G_k)^{-1/2} \tag{21}$$

gegeben wird.

Es sei $\boldsymbol{V}^n$ ein orientierter euklidischer Vektorraum und $[\ ,\dots,\ ]$ die zu der Orientierung gehörende Volumenfunktion. Wir betrachten $n-1$ Vektoren $\mathfrak{c}_1, \dots, \mathfrak{c}_{n-1} \in \boldsymbol{V}^n$. Offenbar ist die Abbildung

$$\mathfrak{x} \in \boldsymbol{V}^n \mapsto [\mathfrak{c}_1, \dots, \mathfrak{c}_{n-1}, \mathfrak{x}] \in \mathbf{R} \tag{22}$$

linear in $\mathfrak{x}$. Wie beim Beweis von Lemma 1 schließen wir auf die Existenz eines eindeutig bestimmten Vektors $\mathfrak{c}_1 \times \dots \times \mathfrak{c}_{n-1} \in \boldsymbol{V}^n$, der durch die Bedingung

$$\langle \mathfrak{c}_1 \times \dots \times \mathfrak{c}_{n-1}, \mathfrak{x} \rangle = [\mathfrak{c}_1, \dots, \mathfrak{c}_{n-1}, \mathfrak{x}] \quad \text{für alle} \quad \mathfrak{x} \in \boldsymbol{V}^n \tag{23}$$

charakterisiert wird; er heißt das *Vektorprodukt* von $\mathfrak{c}_1, \dots, \mathfrak{c}_{n-1}$. Das Vektorprodukt ist also eine $(n-1)$-stellige Operation auf $\boldsymbol{V}^n$, vgl. (1.1.11).

Satz 2. *Es sei $\boldsymbol{V}^n$ ein orientierter euklidischer Vektorraum und $n>1$. Dann hat das durch* (23) *bestimmte Vektorprodukt die folgenden Eigenschaften:*

1. *Die Abbildung* $(\mathfrak{c}_1, \dots, \mathfrak{c}_{n-1}) \in \underset{n-1}{\boldsymbol{X}} \boldsymbol{V}^n \mapsto \mathfrak{c}_1 \times \dots \times \mathfrak{c}_{n-1} \in \boldsymbol{V}^n$ *ist multilinear.*

2. *Diese Abbildung ist schiefsymmetrisch, d. h., es gilt*

$$\mathfrak{c}_{\alpha_1} \times \dots \times \mathfrak{c}_{\alpha_{n-1}} = \operatorname{sgn}(P)\, \mathfrak{c}_1 \times \dots \times \mathfrak{c}_{n-1}$$

für jede Permutation $P = \begin{pmatrix} 1 & \dots & n-1 \\ \alpha_1 & \dots & \alpha_{n-1} \end{pmatrix} \in S_{n-1}$.

3. *Es gilt* $\mathfrak{c}_1 \times \dots \times \mathfrak{c}_{n-1} = \mathfrak{o}$ *dann und nur dann, wenn* $(\mathfrak{c}_1, \dots, \mathfrak{c}_{n-1})$ *linear abhängig ist.*

4. $\mathfrak{c}_1 \times \dots \times \mathfrak{c}_{n-1}$ *ist orthogonal zu jedem Faktor* $\mathfrak{c}_\alpha$:

$$\langle \mathfrak{c}_1 \times \dots \times \mathfrak{c}_{n-1}, \mathfrak{c}_\alpha \rangle = 0, \qquad \alpha = 1, \dots, n-1\ .$$

5. $|\mathfrak{c}_1 \times \dots \times \mathfrak{c}_{n-1}| = v(\mathfrak{c}_1, \dots, \mathfrak{c}_{n-1})$.

6. *Ist* $(\mathfrak{c}_1, \ldots, \mathfrak{c}_{n-1})$ *linear unabhängig, so ist* $(\mathfrak{c}_1, \ldots, \mathfrak{c}_{n-1}, \mathfrak{c}_1 \times \ldots \times \mathfrak{c}_{n-1})$ *eine positiv orientierte Basis.*

7. *Für jedes* $a \in \boldsymbol{O}(n)$ *gilt* $a\mathfrak{c}_1 \times \ldots \times a\mathfrak{c}_{n-1} = a\,(\mathfrak{c}_1 \times \ldots \times \mathfrak{c}_{n-1})\, N(a)$.

Beweis. Die Behauptungen 1, 2 und 4 ergeben sich unmittelbar aus den definierenden Eigenschaften (I) bis (III) einer Volumenfunktion, vgl. Definition 4.7.1. Zum Beweis der Eigenschaft 3 stützen wir uns auf Satz 4.7.4: Ist $(\mathfrak{c}_1, \ldots, \mathfrak{c}_{n-1})$ linear abhängig, so ist für alle $\mathfrak{x} \in \boldsymbol{V}^n$ auch $(\mathfrak{c}_1, \ldots, \mathfrak{c}_{n-1}, \mathfrak{x})$ linear abhängig, also $[\mathfrak{c}_1, \ldots, \mathfrak{c}_{n-1}, \mathfrak{x}] = 0$, die Abbildung (22) ist die Nullform, und folglich ist $\mathfrak{c}_1 \times \ldots \times \mathfrak{c}_{n-1} = \mathfrak{o}$. Ist umgekehrt $(\mathfrak{c}_1, \ldots, \mathfrak{c}_{n-1})$ linear unabhängig, so können wir diese Folge durch einen Vektor $\mathfrak{x} \in \boldsymbol{V}^n$ zu einem n-Bein ergänzen, dessen Volumen natürlich von 0 verschieden ist; nach (23) muß dann auch $\mathfrak{c}_1 \times \ldots \times \mathfrak{c}_{n-1} \neq \mathfrak{o}$ gelten. Die Behauptung 6 folgt aus der Eigenschaft 3 durch Einsetzen von $\mathfrak{x} = \mathfrak{c}_1 \times \ldots \times \mathfrak{c}_{n-1}$ in (23). Ist $(\mathfrak{c}_1, \ldots, \mathfrak{c}_{n-1})$ linear abhängig, so gilt Eigenschaft 5 wegen der Eigenschaft 3 und Folgerung 1. Andererseits können wir, falls $(\mathfrak{c}_1, \ldots, \mathfrak{c}_{n-1})$ linear unabhängig ist, nach Folgerung 2.1 eine positiv orientierte, orthonormierte Basis $(\mathfrak{e}_i)$ so finden, daß $\boldsymbol{W}^{n-1} := \mathfrak{L}(\{\mathfrak{c}_1, \ldots, \mathfrak{c}_{n-1}\}) = \mathfrak{L}(\{\mathfrak{e}_1, \ldots, \mathfrak{e}_{n-1}\})$ gilt. Nach der Eigenschaft 4 erhalten wir $\mathfrak{v} := \mathfrak{c}_1 \times \ldots \times \mathfrak{c}_{n-1} = \mathfrak{e}_n b$; denn es ist $\dim \boldsymbol{W}^{n-1\perp} = 1$. In dieser Basis gilt mit $\mathfrak{c}_\alpha = \sum_{i=1}^{n} \mathfrak{e}_i \gamma_{i\alpha}$ wegen $\gamma_{n\alpha} = 0$

$$b^2 = \langle \mathfrak{v}, \mathfrak{v} \rangle = [\mathfrak{c}_1, \ldots, \mathfrak{c}_{n-1}, \mathfrak{v}] = \begin{vmatrix} & & 0 \\ & \gamma_{\alpha\beta} & \vdots \\ & & 0 \\ 0 & \ldots\ 0 & b \end{vmatrix} = b \det(\gamma_{\alpha\beta}),$$

$\alpha, \beta = 1, \ldots, n-1$,

also $|\mathfrak{v}| = |b| = |\det(\gamma_{\alpha\beta})| = v(\mathfrak{c}_1, \ldots, \mathfrak{c}_{n-1})$. Zum Beweis der Behauptung 7 erhalten wir aus (23) und (5.7.32)

$$\langle a\mathfrak{c}_1 \times \ldots \times a\mathfrak{c}_{n-1}, \mathfrak{x} \rangle = [a\mathfrak{c}_1, \ldots, a\mathfrak{c}_{n-1}, a(a^{-1}\mathfrak{x})] = [\mathfrak{c}_1, \ldots, \mathfrak{c}_{n-1}, a^{-1}\mathfrak{x}]\, N(a)$$
$$= \langle \mathfrak{c}_1 \times \ldots \times \mathfrak{c}_{n-1}, a^{-1}\mathfrak{x} \rangle\, N(a) = \langle a\,(\mathfrak{c}_1 \times \ldots \times \mathfrak{c}_{n-1}), \mathfrak{x} \rangle\, N(a);$$

zum Beweis der letzten Gleichung haben wir noch die Invarianz des Skalarproduktes bei Anwendung von $a \in \boldsymbol{O}(n)$ benutzt. Da diese Beziehungen für alle $\mathfrak{x} \in \boldsymbol{V}^n$ gelten, erhalten wir durch Vergleich des ersten und letzten Gliedes dieser Gleichungskette die Behauptung. Die Eigenschaft 7 drückt aus, daß das Vektorprodukt eine $\boldsymbol{SO}(n)$-Abbildung ist, vgl. Beispiel 1.5.4. □

Beispiel 3. Für $n = 2$ ist das Vektorprodukt eine einstellige Operation, für die man mitunter $\mathfrak{c} \in \boldsymbol{V}^2 \mapsto \mathfrak{c}^\perp \in \boldsymbol{V}^2$ schreibt. Aus den Eigenschaften 4, 5, 6 aus Satz 2 ergibt sich

$$\langle \mathfrak{c}, \mathfrak{c}^\perp \rangle = 0, \qquad |\mathfrak{c}| = |\mathfrak{c}^\perp|, \qquad [\mathfrak{c}, \mathfrak{c}^\perp] > 0 \quad \text{für} \quad \mathfrak{c} \neq \mathfrak{o}; \tag{24}$$

hierdurch ist $\mathfrak{c}^\perp$ eindeutig bestimmt. Man beweist leicht, daß die Zuordnung $\mathfrak{c} \mapsto \mathfrak{c}^\perp$ mit der Drehung $d_{\pi/2} \in \boldsymbol{SO}(2)$ übereinstimmt, in einer orthogonalen Basis $(\mathfrak{e}_1, \mathfrak{e}_2)$

gilt

$$\mathfrak{c} = e_1\gamma_1 + e_2\gamma_2 \in V^2 \mapsto \mathfrak{c}^\perp = e_2\gamma_1 - e_1\gamma_2 \in V^2 . \tag{25}$$

Übung 5. Man beweise: a) Das Vektorprodukt von V^n ist durch die Eigenschaften 4, 5, 6 aus Satz 2 bereits eindeutig bestimmt. — b) Ist (e_i) eine positiv orientierte, orthonormierte Basis von V^n und sind $\mathfrak{c}_\alpha = \sum_i e_i\gamma_{i\alpha}$ die Basisdarstellungen der Vektoren $\mathfrak{c}_\alpha$, $\alpha = 1, \ldots, n-1$, so gilt analog (20)

$$\mathfrak{c}_1 \times \ldots \times \mathfrak{c}_{n-1} = \begin{vmatrix} \gamma_{11} & \gamma_{12} \cdots \gamma_{1,n-1} & e_1 \\ \gamma_{21} & \gamma_{22} \cdots \gamma_{2,n-1} & e_2 \\ \vdots & \vdots & \vdots \\ \gamma_{n1} & \gamma_{n2} \cdots \gamma_{n,n-1} & e_n \end{vmatrix} . \tag{26}$$

Beispiel 4. Die Ergebnisse der Übung 5 führen auf zwei zu der gegebenen äquivalente Definitionen des Vektorprodukts, die vor allem im Fall $n = 3$ häufig benutzt werden. Hier besagt a), daß $\mathfrak{a} \times \mathfrak{b}$ ein zu $\mathfrak{a}$ und $\mathfrak{b}$ orthogonaler Vektor ist; seine Länge ist gleich dem Flächeninhalt des von $\mathfrak{a}$ und $\mathfrak{b}$ aufgespannten Parallelogramms, und wenn $\mathfrak{a} \times \mathfrak{b} \neq \mathfrak{o}$ gilt, ist $(\mathfrak{a}, \mathfrak{b}, \mathfrak{a} \times \mathfrak{b})$ ein positiv orientiertes 3-Bein; es gilt also die *Rechtehandregel*, vgl. Abb. 9a (S. 182) mit $\mathfrak{a}_1 \times \mathfrak{a}_2 = \mathfrak{a}_3$. Die Formel (26) führt mit $\mathfrak{a} = \sum_{i=1}^{3} e_i\alpha_i$, $\mathfrak{b} = \sum_{i=1}^{3} e_i\beta_i$ auf

$$\mathfrak{a} \times \mathfrak{b} = e_1(\alpha_2\beta_3 - \alpha_3\beta_2) + e_2(\alpha_3\beta_1 - \alpha_1\beta_3) + e_3(\alpha_1\beta_2 - \alpha_2\beta_1) . \tag{27}$$

Übung 6. Im Fall $n = 3$ ist $\times : (\mathfrak{a}, \mathfrak{b}) \mapsto \mathfrak{a} \times \mathfrak{b}$ eine Operation auf V^3. Man beweise: a) $[V^3, +, \mathbf{R}, \times]$ ist eine Algebra (Definition 5.4.7). — b) Die Operation $\times$ ist weder kommutativ noch assoziativ, vielmehr gilt

$$\mathfrak{b} \times \mathfrak{a} = -\mathfrak{a} \times \mathfrak{b} , \tag{28}$$

$$(\mathfrak{a} \times \mathfrak{b}) \times \mathfrak{c} + (\mathfrak{b} \times \mathfrak{c}) \times \mathfrak{a} + (\mathfrak{c} \times \mathfrak{a}) \times \mathfrak{b} = \mathfrak{o} \qquad \mathfrak{a}, \mathfrak{b}, \mathfrak{c} \in V^3 . \tag{29}$$

(Hinweis. Man wähle eine orthonormierte Basis und beweise die *Jacobi-Identität* (29) zuerst für die Basisvektoren.) — c) Es gelten die Relationen

$$\langle \mathfrak{a}_1 \times \mathfrak{a}_2, \mathfrak{b}_1 \times \mathfrak{b}_2 \rangle = \langle \mathfrak{a}_1, \mathfrak{b}_1 \rangle \langle \mathfrak{a}_2, \mathfrak{b}_2 \rangle - \langle \mathfrak{a}_1, \mathfrak{b}_2 \rangle \langle \mathfrak{a}_2, \mathfrak{b}_1 \rangle , \tag{30}$$

$$(\mathfrak{a}_1 \times \mathfrak{a}_2) \times \mathfrak{a}_3 = \langle \mathfrak{a}_1, \mathfrak{a}_3 \rangle \mathfrak{a}_2 - \langle \mathfrak{a}_2, \mathfrak{a}_3 \rangle \mathfrak{a}_1 , \tag{31}$$

$$(\mathfrak{a}_1 \times \mathfrak{a}_2) \times (\mathfrak{b}_1 \times \mathfrak{b}_2) = [\mathfrak{a}_1, \mathfrak{b}_1, \mathfrak{b}_2]\, \mathfrak{a}_2 - [\mathfrak{a}_2, \mathfrak{b}_1, \mathfrak{b}_2]\, \mathfrak{a}_1 . \tag{32}$$

Übung 7. Man beweise: In einem orientierten euklidischen Vektorraum V^n gilt

$$[\mathfrak{a}_1, \ldots, \mathfrak{a}_n]\,[\mathfrak{b}_1, \ldots, \mathfrak{b}_n] = \det(\langle \mathfrak{a}_i, \mathfrak{b}_j \rangle), \qquad i, j = 1, \ldots, n . \tag{33}$$

Beispiel 5. *Orientierte Winkel.* Durch (1.17) ist der Winkel φ nur modulo π bestimmt; denn φ und $2\pi - \varphi$ haben denselben Kosinus. Aus (16) erhalten wir in einer orientierten Ebene für $m = n = 2$

$$-1 \leqq \frac{[\mathfrak{x}, \mathfrak{y}]}{|\mathfrak{x}|\,|\mathfrak{y}|} \leqq 1, \qquad \mathfrak{x}, \mathfrak{y} \neq \mathfrak{o} . \tag{34}$$

Hieraus und aus (1.16) folgt sofort: *Zu jedem Paar* $(\mathfrak{x}, \mathfrak{y})$ *von* $\mathfrak{o}$ *verschiedener Vektoren des orientierten* V^2 *gibt es genau einen Winkel* φ, $0 \leqq \varphi < 2\pi$, *so daß*

$$\cos\varphi = \frac{\langle \mathfrak{x}, \mathfrak{y} \rangle}{|\mathfrak{x}|\,|\mathfrak{y}|} \quad \textit{und} \quad \sin\varphi = \frac{[\mathfrak{x}, \mathfrak{y}]}{|\mathfrak{x}|\,|\mathfrak{y}|} \tag{35}$$

gilt; φ heißt der *orientierte Winkel* von $(\mathfrak{x}, \mathfrak{y})$. Man beachte, daß φ von der Reihenfolge der Vektoren abhängt. Es ist nicht schwer, das aus der Schule bekannte Addieren und Subtrahieren von Winkeln zu begründen; man rechnet mit den Winkeln wie in der additiven Gruppe $\mathbf{R}/2\pi\mathbf{Z}$ (Rechnen modulo 2π).

Übung 8. Es seien $\mathfrak{d}$, $\mathfrak{n}$ Einheitsvektoren des orientierten V^2. Man beweise: Der orientierte Winkel von $(\mathfrak{d}, \mathfrak{n})$ ist gleich φ genau dann, wenn $\mathfrak{n} = \mathfrak{d}\cos\varphi + \mathfrak{d}^{\perp}\sin\varphi$ gilt.

Übung 9. Es seien (p_i), (q_i), $i = 1, 2, 3$, Tripel aus Punkten der euklidischen Ebene. Man gebe eine notwendige und hinreichende Bedingung dafür an, daß eine eigentliche Bewegung f der Ebene existiert, für die $f(p_i) = q_i$, $i = 1, 2, 3$, gilt.

Beispiel 6. Es sei $\boldsymbol{H}^{n-1} = \boldsymbol{H}(a; \mathfrak{w}_1, \ldots, \mathfrak{w}_{n-1}) \subset \boldsymbol{E}^n$ eine durch das $(n-1)$-Bein $(\mathfrak{w}_1, \ldots, \mathfrak{w}_{n-1})$ orientierte Hyperebene des orientierten euklidischen Raumes $\boldsymbol{E}^n$. Dann heißt der Vektor

$$\mathfrak{n} := \mathfrak{w}_1 \times \ldots \times \mathfrak{w}_{n-1} / |\mathfrak{w}_1 \times \ldots \times \mathfrak{w}_{n-1}| \tag{36}$$

der *Normaleneinheitsvektor* der orientierten Hyperebene $\boldsymbol{H}^{n-1}$; nach Beispiel 1 ist die Orientierung von $\boldsymbol{H}^{n-1}$ umgekehrt durch die Vorgabe von $\mathfrak{n}$ eindeutig bestimmt. Im nichtorientierten Fall bezeichnet man jeden der beiden Einheitsvektoren $\pm\mathfrak{n} \in \boldsymbol{W}^{n-1\perp}$, $\boldsymbol{W}^{n-1}$ der Vektorraum von $\boldsymbol{H}^{n-1}$, als Normaleneinheitsvektor. Es sei nun $o \in \boldsymbol{E}^n$ ein Ursprungspunkt. Dann ist $x \in \boldsymbol{H}^{n-1}$ genau dann, wenn

$$\langle \overrightarrow{ox}, \mathfrak{n} \rangle = p \tag{37}$$

mit $p := \langle \overrightarrow{oa}, \mathfrak{n} \rangle$ gilt; (37) heißt die *Hessesche Normalform* der Gleichung der orientierten Hyperebene $\boldsymbol{H}^{n-1}$. Wegen der Identifizierung $\boldsymbol{V}^n = \boldsymbol{V}^{n\prime}$ erhalten wir die Hessesche Normalform (in orthogonalen kartesischen Koordinaten x_i) einfach durch Normierung einer beliebigen Gleichung $\langle a, \overrightarrow{ox} \rangle = \sum_{i=1}^{n} a_i x_i = c$, $\mathfrak{a} \neq \mathfrak{o}$, der Hyperebene durch $|\mathfrak{a}| = \left(\sum_i a_i^2\right)^{1/2}$:

$$\mathfrak{n} = \mathfrak{a}/|\mathfrak{a}|\,\varepsilon, \qquad p = c/|\mathfrak{a}|\,\varepsilon, \qquad \varepsilon = \pm 1; \tag{38}$$

die Wahl des Vorzeichens ε entscheidet bei orientiertem $\boldsymbol{E}^n$ über die Orientierung von $\boldsymbol{H}^{n-1}$. Jede Hyperebene des $\boldsymbol{E}^n$ zerlegt den $\boldsymbol{E}^n$ in zwei abgeschlossene Halbräume

$$H^+ := \{x \mid \langle \overrightarrow{ax}, \mathfrak{n} \rangle \geqq 0\}, \qquad H^- := \{x \mid \langle \overrightarrow{ax}, \mathfrak{n} \rangle \leqq 0\} \qquad (a \in \boldsymbol{H}^{n-1}), \tag{39}$$

die man den *äußeren* (bzw. *inneren*) *Halbraum* nennt. Offenbar gilt $H^+ \cap H^- = \boldsymbol{H}^{n-1}$. Im Fall $n = 2$ können wir $\mathfrak{n}$ in der Form $\mathfrak{n} = \mathfrak{e}_1 \cos\varphi + \mathfrak{e}_2 \sin\varphi$ schreiben; dann ergibt (37) die Hessesche Normalform der Geradengleichung für $\boldsymbol{H}^1 \subset \boldsymbol{E}^2$ in der Gestalt

$$x_1 \cos\varphi + x_2 \sin\varphi = p\,, \tag{40}$$

vgl. Abb. 11. Es sei nun $x \in \boldsymbol{E}^n$ ein beliebiger Punkt und $y_0 \in \boldsymbol{H}^{n-1}$ der Fußpunkt des Lotes von x auf $\boldsymbol{H}^{n-1}$, vgl. Übung 2.3. Dann gilt

$$\overrightarrow{y_0 x} = \mathfrak{n}\delta(\boldsymbol{H}^{n-1}, x); \tag{41}$$

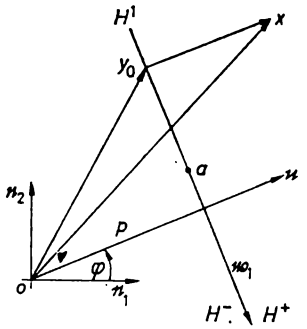


Abb. 11

$\delta(\boldsymbol{H}^{n-1}, x)$ heißt der *orientierte Abstand von* x *und* $\boldsymbol{H}^{n-1}$. Offenbar ist $|\delta(\boldsymbol{H}^{n-1}, x)|$ gleich dem Abstand $\varrho(x, \boldsymbol{H}^{n-1})$, und es gilt: Der orientierte Abstand ist positiv für $x \in H^+ \setminus \boldsymbol{H}^{n-1}$, nicht positiv für $x \in H^-$ und 0 für $x \in \boldsymbol{H}^{n-1}$. Aus $\delta = \langle \mathfrak{n}, \overrightarrow{y_0 x} \rangle = \langle \mathfrak{n}, \overrightarrow{y_0 o} \rangle + \langle \mathfrak{n}, \overrightarrow{ox} \rangle$ folgt wegen $y_0 \in \boldsymbol{H}^{n-1}$ und (37)

$$\delta(\boldsymbol{H}^{n-1}, x) = \langle \mathfrak{n}, \overrightarrow{ox} \rangle - p; \tag{42}$$

das ist eine sehr einfache Formel zur Bestimmung des Abstandes eines Punktes von einer Hyperebene. Speziell gilt $-p = \delta(\boldsymbol{H}^{n-1}, o)$, woraus sich die geometrische Deutung der Zahl p ergibt: $|p|$ ist der Abstand $\varrho(o, \boldsymbol{H}^{n-1})$, und es ist $p \gtreqless 0$ dann und nur dann, wenn o im inneren Halbraum H^- liegt.

Beispiel 7. Die Matrix (2.44) durchläuft die Gruppe $\boldsymbol{SO}(2)$, wenn der Drehwinkel zwischen 0 und 2π variiert; man kann also (2.44) als eine Parameterdarstellung von $\boldsymbol{SO}(2)$ auffassen. Für $n > 2$ lassen sich analoge Parameterdarstellungen gewinnen; man kann zeigen, daß $n(n-1)/2$ Parameter nötig sind, um $\boldsymbol{SO}(n)$ zu beschreiben. Für $n = 3$ verfährt man folgendermaßen: Es sei $a \in \boldsymbol{SO}(3)$ die eigentliche Drehung mit

$$\hat{\mathfrak{e}}_i = a(\mathfrak{e}_i) = \sum_{i=1}^{3} \mathfrak{e}_j \alpha_{ji}, \qquad i = 1, 2, 3; \tag{43}$$

hier seien $(\mathfrak{e}_i)$, $(\hat{\mathfrak{e}}_i)$ zwei rechtsorientierte orthonormierte Dreibeine des Vektorraumes $\boldsymbol{V}^3$. Die Matrix (α_{ji}) von a in der Basis $(\mathfrak{e}_i)$ stimmt mit ihrer Matrix in der Basis $(\hat{\mathfrak{e}}_i)$ überein, wie man unmittelbar durch Anwenden der Abbildung a auf (43) feststellt. Die Abbildung a zerlegen wir nun eindeutig in ein Produkt von drei Abbildungen: 1°. Die Abbildung a_1 lasse den Vektor $\hat{\mathfrak{e}}_1$ fest und drehe $\mathfrak{e}_1$ in die $\hat{\mathfrak{e}}_1, \hat{\mathfrak{e}}_2$-Ebene; ihre Matrix bezüglich $(\hat{\mathfrak{e}}_i)$ ist

$$a_1: \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\vartheta_1 & -\sin\vartheta_1 \\ 0 & \sin\vartheta_1 & \cos\vartheta_1 \end{pmatrix}, \qquad 0 \leqq \vartheta_1 < \pi;$$

ϑ_1 ist durch die Ungleichung eindeutig bestimmt. 2°. Es bezeichne $\mathfrak{e}_i' = a_1(\mathfrak{e}_i)$. Die Drehung a_2 lasse $\hat{\mathfrak{e}}_3$ fest und drehe in der $\hat{\mathfrak{e}}_1, \hat{\mathfrak{e}}_2$-Ebene den Vektor $\mathfrak{e}_1'$ in den Vektor $\hat{\mathfrak{e}}_1$:

$$a_2\colon \quad \begin{pmatrix} \cos\vartheta_2 & -\sin\vartheta_2 & 0 \\ \sin\vartheta_2 & \cos\vartheta_2 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad 0 \leqq \vartheta_2 < 2\pi\,.$$

3°. Es sei $e_i'' = a_2(e_i')$; speziell gilt also $e_1'' = \hat{e}_1$. Die Drehung a_3 lasse $\hat{e}_1$ fest und drehe e_2'' in den Vektor $\hat{e}_2$; dann muß auch $a_3(e_3'') = \hat{e}_3$ gelten, da wir nur rechtsorientierte Dreibeine und eigentliche Bewegungen betrachten: $a_3(e_3'') = a_3(e_1'' \times e_2'') = \hat{e}_1 \times \hat{e}_2 = \hat{e}_3$. Die Matrix von a_3 bezüglich $(\hat{e}_i)$ hat dieselbe Gestalt wie die von a_1 mit einem Winkel ϑ_3, $0 \leqq \vartheta_3 < 2\pi$. Durch Multiplikation der Matrizen der drei Abbildungen a_i erhält man die Matrix (α_{ji}) der Abbildung $a = a_3 \circ a_2 \circ a_1$ bezüglich (e_i) und bezüglich (e_i):

$$(\alpha_{ji}) = \begin{pmatrix} \cos\vartheta_2 & -\sin\vartheta_2\cos\vartheta_1 & \sin\vartheta_2\sin\vartheta_1 \\ \cos\vartheta_3\sin\vartheta_2 & \cos\vartheta_3\cos\vartheta_2\cos\vartheta_1 - \sin\vartheta_3\sin\vartheta_1 & -\cos\vartheta_3\cos\vartheta_2\sin\vartheta_1 - \sin\vartheta_3\cos\vartheta_1 \\ \sin\vartheta_3\sin\vartheta_2 & \sin\vartheta_3\cos\vartheta_2\cos\vartheta_1 + \cos\vartheta_3\sin\vartheta_1 & -\sin\vartheta_3\cos\vartheta_2\sin\vartheta_1 + \cos\vartheta_3\cos\vartheta_1 \end{pmatrix},$$

$$0 \leqq \vartheta_1 < \pi, \qquad 0 \leqq \vartheta_2 < 2\pi, \qquad 0 \leqq \vartheta_3 < 2\pi; \tag{44}$$

die in ihr vorkommenden, eindeutig bestimmten Winkel ϑ_1, ϑ_2, ϑ_3 nennt man die *Eulerschen Winkel* der eigentlichen Drehung a bezüglich des Dreibeins (e_i).

§ 4. Selbstadjungierte Operatoren

Zunächst sei bemerkt, daß man, besonders in der Analysis, statt „*lineare Abbildung*" auch „*Operator*" sagt. Durch Definition 5.6.2 haben wir jedem Operator $a \in \boldsymbol{L}(\boldsymbol{V}, \boldsymbol{W})$ den transponierten Operator $a' \in \boldsymbol{L}(\boldsymbol{W}', \boldsymbol{V}')$ der zugehörigen dualen Räume zugeordnet. Da wir im euklidischen Fall die dualen Räume mit den Vektorräumen identifizieren können (Beispiel 2.3), ist der transponierte Operator auch als Element $a \in \boldsymbol{L}(\boldsymbol{W}^m, \boldsymbol{V}^n)$, $m, n < \infty$, aufzufassen. Nach (2.19) und (5.6.28) gilt dann für alle $\mathfrak{x} \in \boldsymbol{V}$, $\mathfrak{y} \in \boldsymbol{W}$

$$\langle \mathfrak{x}, a'\mathfrak{y} \rangle = \langle a\mathfrak{x}, \mathfrak{y} \rangle\,. \tag{1}$$

Bei dieser Identifizierung nennt man a' auch den zu a *adjungierten* Operator. Wir könnten nun die Eigenschaften der adjungierten Operatoren im euklidischen Fall ($K = \mathbf{R}$) unmittelbar aus § 5.6 übertragen. Da jedoch im unitären Fall ($K = \mathbf{C}$) die Verhältnisse etwas anders liegen (vgl. Beispiel 2.4), ziehen wir es vor, hier eine von der Theorie der dualen Räume unabhängige Darstellung zu geben, die sich direkt auf das Skalarprodukt stützt. Dadurch können wir den unitären und euklidischen Fall einheitlich behandeln. Man erinnere sich an die Verabredung nach Definition 1.2.

Definition 1. Es seien $\boldsymbol{V}$, $\boldsymbol{W}$ unitäre Räume, $K = \mathbf{R}$, $\mathbf{C}$ und $a \in \boldsymbol{L}(\boldsymbol{V}, \boldsymbol{W})$. Ein Operator $a' \in \boldsymbol{L}(\boldsymbol{W}, \boldsymbol{V})$ heißt zu a *adjungiert*, wenn für alle $\mathfrak{x} \in \boldsymbol{V}$, $\mathfrak{y} \in \boldsymbol{W}$ die Gleichung (1) erfüllt ist.

Satz 1. *Es seien V^n, W^m endlichdimensionale unitäre Räume. Dann gibt es zu jedem $a \in L(V^n, W^m)$ genau einen adjungierten Operator $a' \in L(W^m, V^n)$. Hat a bezüglich der orthonormierten Basen $(\mathfrak{e}_i)$ von V^n und $(\mathfrak{b}_\alpha)$ von W^m die Matrix $(a_{\alpha i})$, so hat a' bezüglich dieser Basen im Fall $K = \mathbf{C}$ die konjugiert-transponierte Matrix $(\bar{a}_{\alpha i})'$ und im Fall $K = \mathbf{R}$ die transponierte Matrix $(a_{\alpha i})'$.*

Beweis. Wir führen den Beweis für $K = \mathbf{C}$. Es gilt $a(\mathfrak{e}_k) = \sum_{\alpha=1}^{n} \mathfrak{b}_\alpha a_{\alpha k}$. Für a' machen wir den Ansatz $a'(\mathfrak{b}_\beta) \equiv \sum_{j=1}^{n} \mathfrak{e}_j b_{j\beta}$. Gehen wir damit in (1) ein, so folgt

$$\langle \mathfrak{e}_l, a'(\mathfrak{b}_\beta)\rangle = b_{l\beta} = \langle a(\mathfrak{e}_l), \mathfrak{b}_\beta\rangle = a_{\beta l}\,.$$

Daher gilt für die Matrix von a'

$$b_{j\beta} = \bar{a}_{\beta j}\,, \tag{2}$$

d. h., die adjungierte Abbildung a' ist durch a eindeutig bestimmt und ihre Matrix hat die im Satz angegebene Form. Definiert man a' durch Angabe seiner Matrix mit den Elementen (2), so prüft man durch eine einfache Rechnung nach, daß a' zu a adjungiert ist. □

Folgerung 1. *Die durch*

$$a \in L(V^n, W^m) \mapsto a' \in L(W^m, V^n)\,, \tag{3}$$

a' die zu a adjungierte Abbildung der unitären Räume W^m, V^n, definierte Abbildung ist bijektiv und konjugiert-linear; im einzelnen gelten

$$(a+b)' = a' + b'\,, \tag{4}$$

$$(a\alpha)' = \begin{cases} a'\bar{\alpha} & \text{im Fall } K = \mathbf{C}, \\ a'\alpha & \text{im Fall } K = \mathbf{R}, \end{cases} \qquad \alpha \in K\,, \tag{5}$$

$$(a')' = a\,, \tag{6}$$

$$(b \circ a)' = a' \circ b' \qquad (b \in L(W^m, U^k))\,, \tag{7}$$

$$\operatorname{Ker} a' = (\operatorname{Im} a)^\perp. \tag{8}$$

Den Beweis kann man durch Übergang zu den Matrizen nach Satz 1 oder analog zum Beweis von Satz 5.6.4 führen. □

Definition 2. Ein Operator $a \in L(V)$ des unitären Vektorraumes V in sich heißt *selbstadjungiert*, wenn für alle $\mathfrak{x}, \mathfrak{y} \in V$

$$\langle a\mathfrak{x}, \mathfrak{y}\rangle = \langle \mathfrak{x}, a\mathfrak{y}\rangle \tag{9}$$

gilt. Statt selbstadjungiert sagt man auch *symmetrisch* im Fall $K = \mathbf{R}$ und *hermitesch* im Fall $K = \mathbf{C}$. Entsprechend heißt ein Operator *schiefsymmetrisch* im Fall $K = \mathbf{R}$ und *schiefhermitesch* im Fall $K = \mathbf{C}$, wenn für alle $\mathfrak{x}, \mathfrak{y} \in V$

$$\langle a\mathfrak{x}, \mathfrak{y}\rangle + \langle \mathfrak{x}, a\mathfrak{y}\rangle = 0\,, \tag{10}$$

d. h. $a' = -a$, gilt.

Folgerung 2. *Es sei V^n ein endlichdimensionaler unitärer Vektorraum. Ein Operator $a \in L(V^n)$ ist selbstadjungiert genau dann, wenn seine Matrix (a_{ij}) bezüglich einer beliebigen orthonormierten Basis im Fall $K = \mathbf{C}$ hermitesch und im Fall $K = \mathbf{R}$ symmetrisch ist; a ist schiefhermitesch, wenn (a_{ij}) schiefhermitesch ist, d. h.*

$$(a_{ij})' = -(\bar{a}_{ij}), \quad \text{also} \quad a_{ij} = -\bar{a}_{ji}, \qquad i, j = 1, \ldots, n, \tag{11}$$

gilt, und schiefsymmetrisch genau dann, wenn (a_{ij}) schiefsymmetrisch ist, d. h.

$$(a_{ij})' = -(a_{ij}), \quad \text{also} \quad a_{ji} + a_{ij} = 0, \qquad i, j = 1, \ldots, n, \tag{12}$$

gilt. Jeder Operator $a \in L(V^n)$ besitzt eine eindeutig bestimmte Zerlegung

$$a = \frac{1}{2}(a + a') + \frac{1}{2}(a - a') \tag{13}$$

in einen hermiteschen (bzw. symmetrischen) und einen schiefhermiteschen (bzw. schiefsymmetrischen) Bestandteil. □

Satz 2. *Zu jedem selbstadjungierten Operator $a \in L(V^n)$ eines endlichdimensionalen unitären Raumes gibt es eine orthonormierte Basis $(\mathfrak{d}_j)$ von V^n, bezüglich der die Matrix (a_{jk}) von a Diagonalform hat. Alle Eigenwerte von a sind reell.*

Beweis. Es sei (a_{ij}) die Matrix von a bezüglich einer orthonormierten Basis. Die Eigenwerte von a sind die Nullstellen des charakteristischen Polynoms $\chi_a(t) = \det(a_{jk} - t\delta_{jk})$. Da jede reelle symmetrische Matrix $(a_{jk}) \in \mathbf{M}_n(\mathbf{R}) \subset \mathbf{M}_n(\mathbf{C})$ auch hermitesch ist, genügt es, hermitesche Operatoren zu betrachten; wir interpretieren die reelle Matrix (a_{jk}) als Operator $(a_{jk}) \in L(\mathbf{C}^n)$ des hermiteschen Raumes $\mathbf{C}^n$ mit dem Skalarprodukt (1.6). Es sei nun $\lambda \in \mathbf{C}$ ein Eigenwert des hermiteschen Operators a und $\mathfrak{x}$ ein Eigenvektor von a zum Eigenwert λ. Dann gilt

$$\langle a\mathfrak{x}, \mathfrak{x}\rangle = \lambda\langle \mathfrak{x}, \mathfrak{x}\rangle = \langle \mathfrak{x}, a\mathfrak{x}\rangle = \bar{\lambda}\langle \mathfrak{x}, \mathfrak{x}\rangle,$$

und wegen $\mathfrak{x} \neq \mathfrak{o}$ folgt, daß $\lambda = \bar{\lambda}$ reell ist. Zum Beweis von Satz 2 benötigen wir noch

Lemma 1. *Es sei V^n ein unitärer Raum, $a \in L(V^n)$ und $W \subseteq V^n$ ein bei a invarianter Unterraum. Dann ist $W^\perp$ bei a' invariant. Wenn also a selbstadjungiert oder schiefhermitesch im Fall $K = \mathbf{C}$ oder schiefsymmetrisch im Fall $K = \mathbf{R}$ ist, dann ist mit W auch $W^\perp$ bei a invariant.*

Beweis. Für alle $\mathfrak{x} \in W^\perp$ und alle $\mathfrak{y} \in W$ gilt $\langle a'\mathfrak{x}, \mathfrak{y}\rangle = \langle \mathfrak{x}, a\mathfrak{y}\rangle = 0$, und somit ist mit $\mathfrak{x} \in W^\perp$ auch $a'\mathfrak{x} \in W^\perp$. Die zweite Behauptung folgt wegen $a' = a$ bzw. $a' = -a$ unmittelbar aus der ersten. □

Nun ist es leicht, den Beweis von Satz 2 durch vollständige Induktion nach der Dimension n zu führen. Angenommen, die Behauptung sei schon für alle W^m mit $m < n$ bewiesen. Nach dem Fundamentalsatz der Algebra existiert ein Eigenwert λ von $a \in L(V^n)$, und weil a selbstadjungiert ist, gilt $\lambda \in \mathbf{R}$. Wir finden daher einen Eigenvektor $\mathfrak{d}_n \in V^n$ zum Eigenwert λ, für den wir $|\mathfrak{d}_n| = 1$ annehmen können. Dann ist $W^1 := \mathfrak{L}(\{\mathfrak{d}_n\})$ invariant, und wegen Lemma 1 ist auch $W^{1\perp}$ bei a invariant.

Offenbar ist auch $a \mid \boldsymbol{W}^{1\perp}$ selbstadjungiert, und wegen dim $\boldsymbol{W}^{1\perp} = n-1$ finden wir nach Induktionsannahme in $\boldsymbol{W}^{1\perp}$ eine Basis $(\mathfrak{d}_\alpha)$, $\alpha = 1, \ldots, n-1$, aus orthonormierten Eigenvektoren von $a \mid \boldsymbol{W}^{1\perp}$. Dann ist $(\mathfrak{d}_1, \ldots, \mathfrak{d}_{n-1}, \mathfrak{d}_n)$ eine orthonormierte Basis aus Eigenvektoren von a. □

Folgerung 3. *Die Eigenunterräume $\boldsymbol{U}_\lambda$, $\boldsymbol{U}_\mu$, $\lambda \neq \mu$, eines selbstadjungierten Operators a sind paarweise orthogonal. Die Dimension* dim $\boldsymbol{U}_\lambda$ *ist gleich der Vielfachheit der Nullstelle λ in $\chi_a(t)$.* □

Unter einem *reellen Unterraum* eines komplexen Vektorraumes $\boldsymbol{V}$ versteht man einen Unterraum der Reellifizierung $r\boldsymbol{V}$, vgl. Übung 4.2.7, das ist also eine nichtleere, bezüglich Linearkombinationen mit reellen Koeffizienten abgeschlossene Teilmenge von $\boldsymbol{V}$. Unter Beachtung von (1) ergibt sich

Folgerung 4. *Die Teilmenge $\boldsymbol{L}_s(\boldsymbol{V}^n)$ der selbstadjungierten Operatoren des unitären Raumes $\boldsymbol{V}^n$ ist ein reeller Unterraum von $\boldsymbol{L}(\boldsymbol{V}^n)$, der bei unitären Transformationen invariant bleibt. Zwei Operatoren aus $\boldsymbol{L}_s(\boldsymbol{V}^n)$ sind $\boldsymbol{U}(n)$-äquivalent im Fall $K = \mathbf{C}$ (bzw. $\boldsymbol{O}(n)$-äquivalent im Fall $K = \mathbf{R}$) genau dann, wenn ihre charakteristischen Polynome übereinstimmen.*

Beweis. Die Wirkung von $\boldsymbol{U}(n)$ über $\boldsymbol{L}(\boldsymbol{V}^n)$ ist die Einschränkung der Wirkung von $\boldsymbol{GL}(\boldsymbol{V}^n)$, d. h., es gilt $\alpha_g(a) = g \circ a \circ g^{-1}$, vgl. (5.8.1). Die Behauptung über die Invarianz von $\boldsymbol{L}_s(\boldsymbol{V}^n)$ folgt unmittelbar aus Definition 2. Nach Satz 5.8.1 sind die charakteristischen Polynome invariant; die von ihnen bestimmten Eigenwerte, für die wir noch $\lambda_1 \geqq \ldots \geqq \lambda_n$ voraussetzen können, bilden gerade die Diagonalelemente der Diagonalform von a in einer geeigneten orthonormierten Basis (Satz 2). Sind nun $a, \hat{a} \in \boldsymbol{L}_s(\boldsymbol{V}^n)$ mit $\chi_a(t) = \chi_{\hat{a}}(t)$ und sind $(\mathfrak{d}_j)$ bzw. $(\hat{\mathfrak{d}}_j)$ Basen, die orthonormiert sind und für die a bzw. $\hat{a}$ Diagonalform mit der Größe nach geordneten Eigenwerten in der Hauptdiagonale haben, so müssen diese Diagonalmatrizen übereinstimmen. Die durch $g(\mathfrak{d}_j) = \hat{\mathfrak{d}}_j$ bestimmte unitäre Transformation ergibt die Äquivalenz $\alpha_g(a) = \hat{a}$. □

Die beschriebene Theorie liefert auch die Hilfsmittel zur *Herstellung der Normalform*: Man bestimme die Nullstellen des charakteristischen Polynoms, löse die homogenen Gleichungssysteme für die Eigenunterräume $\boldsymbol{U}_\lambda$ zu den verschiedenen Eigenwerten λ und wähle in jedem von ihnen eine orthonormierte Basis, z. B. durch Orthogonalisierung einer beliebigen Basis von $\boldsymbol{U}_\lambda$. Nach Folgerung 3 entsteht so eine orthonormierte Basis von $\boldsymbol{V}^n$ aus Eigenvektoren von $\boldsymbol{a}$, deren Koordinaten gerade die Spalten der Matrix der unitären Transformation g ergeben, welche die Transformation auf Normalform bewirkt.

Übung 1. Man beweise: Die Menge der Diagonalmatrizen $(\lambda_i \delta_{ij})$ mit lauter reellen Elementen $\lambda_1 \geqq \ldots \geqq \lambda_n$ ist eine Normalformenmenge der Transformationsgruppe $[\boldsymbol{U}(n), \boldsymbol{L}_s(\boldsymbol{V}^n)]$ bzw. $[\boldsymbol{O}(n), \boldsymbol{L}_s(\boldsymbol{V}^n)]$, vgl. Satz 5.7.3.

Übung 2. Es sei $K = \mathbf{C}$ und $\boldsymbol{L}_{sh}(\boldsymbol{V}^n)$ die Menge der schiefhermiteschen Operatoren des unitären Raumes $\boldsymbol{V}^n$. Man beweise: a) $\boldsymbol{L}_{sh}(\boldsymbol{V}^n)$ ist ein bei $\boldsymbol{U}(n)$ invarianter reeller Unterraum von $\boldsymbol{L}(\boldsymbol{V}^n)$. — b) Für jedes $a \in \boldsymbol{L}_{sh}(\boldsymbol{V}^n)$ sind alle von 0 verschiedenen Eigenwerte λ_i rein imaginär, d. h., es gilt $\lambda_j = \mathrm{i}\alpha_j$, $\alpha_j \in \mathbf{R}$, $j = 1, \ldots, n$, $\mathrm{i}^2 = -1$. — c) Zu jedem $a \in \boldsymbol{L}_{sh}(\boldsymbol{V}^n)$ gibt es eine orthonormierte Basis $(\mathfrak{d}_j)$ von $\boldsymbol{V}^n$, bezüglich der die Matrix von a

Diagonalform $(i\alpha_j\delta_{jl})$ mit $\alpha_j \in \mathbf{R}$, $\alpha_1 \geqq \ldots \geqq \alpha_n$ besitzt; die Menge aller dieser Matrizen ist eine Normalformenmenge der Transformationsgruppe $[\boldsymbol{U}(n), \boldsymbol{L}_{sh}(\boldsymbol{V}^n)]$.

Übung 3. Im Fall $K = \mathbf{R}$ beweise man für den Raum $\boldsymbol{L}_a(\boldsymbol{V}^n)$ der schiefsymmetrischen Operatoren des euklidischen Vektorraumes $\boldsymbol{V}^n$ und die Gruppe $\boldsymbol{O}(n)$ anstelle von $\boldsymbol{U}(n)$ die zu a), b) von Übung 2 analogen Aussagen. Ferner zeige man, daß die unten angegebenen Matrizen der Gestalt (14) eine Normalformenmenge der Transformationsgruppe $[\boldsymbol{O}(n), \boldsymbol{L}_a(\boldsymbol{V}^n)]$ bilden. Hinweis. Man betrachte die Komplexifizierung $c\boldsymbol{V}^n = \boldsymbol{V}^n + \boldsymbol{V}^n \cdot \mathrm{i}$ von $\boldsymbol{V}^n$, vgl. Übung 5.2.10. Das Skalarprodukt von $\boldsymbol{V}^n$ dehnen wir zu einem hermiteschen Skalarprodukt auf $c\boldsymbol{V}^n$ aus, indem wir $\langle \mathfrak{x}, \mathfrak{y}\mathrm{i}\rangle = -\langle \mathfrak{x}, \mathfrak{y}\rangle \mathrm{i} = -\langle \mathfrak{x}\mathrm{i}, \mathfrak{y}\rangle$ und $\langle \mathfrak{x}\mathrm{i}, \mathfrak{y}\mathrm{i}\rangle = \langle \mathfrak{x}, \mathfrak{y}\rangle$, $\mathfrak{x}, \mathfrak{y} \in \boldsymbol{V}$, setzen. Für $a \in \boldsymbol{L}(\boldsymbol{V})$ erhalten wir durch lineare Ausdehnung $a(\mathfrak{x}\mathrm{i}) = a(\mathfrak{x})\,\mathrm{i}$ einen auf $c\boldsymbol{V}$ definierten schiefhermiteschen Operator; dazu genügt es zu beachten, daß eine orthonormierte Basis von $\boldsymbol{V}$ auch eine orthonormierte Basis des unitären Raumes $c\boldsymbol{V}$ ist, und Folgerung 2 anzuwenden. Da die Eigenwerte $\lambda \neq 0$ von a alle rein imaginär sind und das charakteristische Polynom von a reelle Koeffizienten hat, müssen diese Eigenwerte in Paaren $\lambda = \mathrm{i}\alpha$, $\bar{\lambda} = -\mathrm{i}\alpha$ auftreten (Satz 2.8.2). Ist $\mathfrak{z} = \mathfrak{x} + \mathfrak{y}\mathrm{i} \in c\boldsymbol{V}$ ein Eigenvektor zu λ, so ist $\bar{\mathfrak{z}} = \mathfrak{x} - \mathfrak{y}\mathrm{i}$ ein Eigenvektor zu $\bar{\lambda}$. Man beweist leicht, daß für $\lambda \neq 0$ die Vektoren $\mathfrak{x}, \mathfrak{y} \in \boldsymbol{V}$ orthogonal sind, bei geeigneter Normierung von $\mathfrak{z}$ beide die Länge 1 haben und $a(\mathfrak{x}) = -\mathfrak{y}\alpha$, $a(\mathfrak{y}) = \mathfrak{x}\alpha$ gelten; wegen $\mathfrak{x}, \mathfrak{y} \in \boldsymbol{V}$ spannen $\mathfrak{x}, \mathfrak{y}$ einen zweidimensionalen, invarianten reellen Unterraum $\boldsymbol{W}_\alpha \subseteqq \boldsymbol{V}$ auf, für den $a \mid \boldsymbol{W}_\alpha$ bezogen auf $\mathfrak{x}, \mathfrak{y}$ die Normalform

$$\begin{pmatrix} 0 & \alpha \\ -\alpha & 0 \end{pmatrix}$$

besitzt. Aus Lemma 1 erhält man durch einen einfachen Induktionsschluß, daß es eine orthonormierte Basis (e_j) von $\boldsymbol{V}$ gibt, für welche die Matrix (a_{ij}) von a folgende Normalform hat; $\alpha, \beta, \ldots, \gamma$ sind dabei die Imaginärteile der Eigenwerte von a unter Berücksichtigung ihrer Vielfachheiten:

$$\begin{pmatrix} \begin{matrix} 0 & \alpha \\ -\alpha & 0 \end{matrix} & & & \mathbf{0} \\ & \begin{matrix} 0 & \beta \\ -\beta & 0 \end{matrix} & & \\ & & \ddots & \\ & & & \begin{matrix} 0 & \gamma \\ -\gamma & 0 \end{matrix} \\ \mathbf{0} & & & \begin{matrix} 0 & & \\ & \ddots & \\ & & 0 \end{matrix} \end{pmatrix}. \tag{14}$$

Übung 4. Es sei $\boldsymbol{V}^n$ unitär und $a \in \boldsymbol{L}(\boldsymbol{V})$. Man beweise: a) $b := a' \circ a$ ist selbstadjungiert, alle Eigenwerte von b sind nichtnegativ, und es gilt $\mathrm{Ker}\, a = \mathrm{Ker}\, b$. — b) Es gibt eine Darstellung $a = u \circ g$, $u \in \boldsymbol{U}(n)$, $g \in \boldsymbol{L}_s(\boldsymbol{V})$, alle Eigenwerte von g nichtnegativ; dabei ist g und im Fall $a \in \boldsymbol{GL}(\boldsymbol{V})$ auch u eindeutig bestimmt. (Hinweis. Man betrachte eine orthonormierte Basis aus Eigenvektoren $(\mathfrak{e}_k)$ von b; $b(\mathfrak{e}_k) = \mathfrak{e}_k\lambda_k$. Die Vektoren $a(\mathfrak{e}_k)$ genügen dann der Beziehung $\langle a(\mathfrak{e}_k), a(\mathfrak{e}_l)\rangle = \lambda_k\delta_{kl}$. Durch Normierung und eventuell Ergänzung dieser orthogonalen Vektoren findet man eine gewisse orthonormierte Basis $(\hat{\mathfrak{e}}_k)$ von $\boldsymbol{V}$. Dann sind u mit $u(\mathfrak{e}_k) = \hat{\mathfrak{e}}_k$ und g mit $g(\mathfrak{e}_k) = \sqrt{\lambda_k}\mathfrak{e}_k$, $\sqrt{\lambda_k} \geqq 0$, Faktoren der gesuchten Zerlegung. Jedes g, das den Forderungen genügt, erfüllt $g^2 = b$. Hieraus folgt die Eindeutigkeitsaussage.) — c) Im Fall $K = \mathbf{R}$ beweise man die Existenz und analoge Eindeutigkeitseigenschaften der Darstellung $a = u \circ g$ mit $g \in \boldsymbol{L}_s(\boldsymbol{V})$, $u \in \boldsymbol{O}(n)$, g mit nichtnegativen Eigen-

werten. Ferner zeige man das analoge Ergebnis für Darstellungen der Form $a = g \circ u$, $g \in \boldsymbol{L}_s(\boldsymbol{V})$, $u \in \boldsymbol{U}(n)$.

Übung 5. Es sei $\boldsymbol{V}^n$ ein unitärer Raum, $\boldsymbol{W}^m$ und $\boldsymbol{U}^k$ Unterräume, $1 \leqq m \leqq k < n$. Die Zerlegung $\boldsymbol{V} = \boldsymbol{U} + \boldsymbol{U}^\perp$ definiert eine Projektion $p_2 \colon \boldsymbol{V} \to \boldsymbol{U}$; wir setzen $p := p_2 \mid \boldsymbol{W}^m$. Man beweise: a) $p' \circ p \colon \boldsymbol{W} \to \boldsymbol{W}$ ist selbstadjungiert, und für die Eigenwerte λ_α, $\alpha = 1, \ldots, m$, von $p' \circ p$ gilt $0 \leqq \lambda_\alpha \leqq 1$. — b) $\operatorname{Ker} p = \operatorname{Ker} p' \circ p = \boldsymbol{W} \cap \boldsymbol{U}$. — Man setzt $\cos \varphi_\alpha = \sqrt{\lambda_\alpha}$, $0 \leqq \varphi_\alpha \leqq \pi/2$, und nennt φ_α die *Winkel zwischen $\boldsymbol{W}$ und $\boldsymbol{U}^\perp$*. — c) Ist $(\boldsymbol{W}_0^m, \boldsymbol{U}_0^k)$ ein weiteres Paar von Unterräumen, so gibt es genau dann ein $g \in \boldsymbol{U}(n)$ mit $g\boldsymbol{W}_0 = \boldsymbol{W}$ und $g\boldsymbol{U}_0 = \boldsymbol{U}$, wenn die Winkel $\varphi_{0\alpha}$ zwischen $\boldsymbol{W}_0$ und $\boldsymbol{U}_0{}^\perp$ mit den Winkeln φ_α zwischen $\boldsymbol{W}$ und $\boldsymbol{U}^\perp$ unter Berücksichtigung der Vielfachheiten übereinstimmen. (Hinweis. Weil $\boldsymbol{U}(n)$ über den k-dimensionalen Unterräumen von $\boldsymbol{V}$ transitiv wirkt, kann man o. B. d. A. $\boldsymbol{U}_0 = \boldsymbol{U}$ annehmen. Man passe die orthogonale Basis von $\boldsymbol{U}$, $\boldsymbol{U}^\perp$ an die orthogonalen Projektionen der Eigenvektoren von $p' \circ p$ (bzw. $p_0' \circ p_0$) an und erhält nach eventueller Ergänzung zwei orthonormierte Basen (a_j) bzw. (a_{0j}) von $\boldsymbol{V}$, welche durch $g(a_{0j}) = a_j$, $j = 1, \ldots, n$, die gesuchte Transformation liefern.) Man macht sich leicht klar, daß ein entsprechendes Resultat auch für den euklidischen Vektorraum $\boldsymbol{V}^n$ gilt.

§ 5. Euklidische Klassifikation der Quadriken

In diesem Paragraphen wollen wir die folgende Frage behandeln: Es seien Q, $\hat{Q}$ zwei Quadriken des euklidischen Raumes $\boldsymbol{E}^n$. Wann sind diese Quadriken kongruent, d. h., wann gibt es eine Bewegung $f \in \mathfrak{E}(n)$ mit $f(Q) = \hat{Q}$? Offenbar ist das der Fall, wenn es orthonormierte n-Beine $(o; \mathfrak{e}_i)$ bzw. $(\hat{o}, \hat{\mathfrak{e}})$ des $\boldsymbol{E}^n$ derart gibt, daß Q und $\hat{Q}$ bezüglich $(o; \mathfrak{e}_i)$ bzw. $(\hat{o}; \hat{\mathfrak{e}}_i)$ durch Gleichungen mit entsprechend gleichen Koeffizienten definiert werden können; die durch $f \colon (o; \mathfrak{e}_i) \mapsto {}'\hat{o}; \hat{\mathfrak{e}}_i)$ bestimmte Bewegung leistet dann $f(Q) = \hat{Q}$ (Zuordnung durch gleiche Koordinaten, vgl. § 5.7). Wir werden also auf folgendes Problem geführt: Wann lassen sich zwei quadratische Gleichungen (5.9.1) oder in Matrixschreibweise (5.9.36) durch eine orthogonale kartesische Transformation der Koordinaten und durch Multiplikation mit einer Zahl $c \in \mathbf{R}$, $c \neq 0$, ineinander überführen? Diese Klassifikationsaufgabe für die quadratischen Gleichungen wird durch Satz 2 gelöst. Wegen $\mathfrak{E}(n) \subset \mathfrak{A}(n)$ gelten für die Koordinatentransformation und die Transformation der Koeffizienten der Gleichungen die Formeln der affinen Geometrie, insbesondere also (37), (38), (42) und (43) aus § 5.9, wobei jedoch nur orthogonale Matrizen (α_{ij}) auftreten, da wir nur orthonormierte n-Beine ineinander transformieren können.

Wie in der affinen Geometrie untersuchen wir zuerst das Transformationsgesetz für die Matrix (q_{ij}) einer symmetrischen Bilinearform. Wegen $(\alpha_{ik}) \in \boldsymbol{O}(n)$ gilt $(\alpha_{ik}) = (\alpha_{ik})^*$, und aus (5.9.42) folgt

$$(\hat{q}_{ij}) = (\alpha_{ik})\,(q_{kl})\,(\alpha_{lj})^{-1}. \tag{1}$$

Ein Vergleich mit dem Transformationsgesetz (5.7.25) der Matrix eines linearen Operators zeigt, daß für $(\alpha_{ij}) \in \boldsymbol{O}(n)$ beide Transformationsgesetze übereinstimmen. Übersetzen wir daher Satz 4.2 in die Matrixsprache, so ergibt sich unmittelbar:

Satz 1. *Es sei V^n ein euklidischer Vektorraum und $b: V^n \times V^n \to \mathbf{R}$ eine symmetrische Bilinearform. Ist $(\mathfrak{e}_i)$ irgendeine orthonormierte Basis und $(b_{ij}) := (b(\mathfrak{e}_i, \mathfrak{e}_j))$ die Matrix von b bezüglich $(\mathfrak{e}_i)$, so ist das charakteristische Polynom*

$$\chi_b(t) := \det(b_{ij} - t\delta_{ij}) \tag{2}$$

unabhängig von der Wahl der orthonormierten Basis $(\mathfrak{e}_i)$, und die Eigenwerte λ_i, $\chi_b(\lambda_i) = 0$, sind alle reell. Es gibt eine orthonormierte Basis $(\mathfrak{d}_i)$ von V^n, so daß

$$b(\mathfrak{d}_i, \mathfrak{d}_j) = \lambda_i \delta_{ij}, \qquad i, j = 1, \ldots, n, \tag{3}$$

gilt; die Matrix der Form b bezüglich $(\mathfrak{d}_i)$ hat also Diagonalform mit den Eigenwerten λ_i auf der Hauptdiagonale. Zwei symmetrische Bilinearformen sind genau dann $\boldsymbol{O}(n)$-äquivalent, wenn ihre charakteristischen Polynome übereinstimmen. □

Man beachte, daß das charakteristische Polynom einer Bilinearform im allgemeinen nur bei orthogonalen Transformationen invariant bleibt, wie man unmittelbar durch Vergleich von Satz 1 mit dem Trägheitssatz 5.9.6 erkennt; einen direkten Invarianzbeweis kann man analog zu Satz 5.8.1 auf Grund von (1) führen. Die enge Beziehung zwischen der euklidischen Theorie der symmetrischen Bilinearformen und den selbstadjungierten Operatoren wird auch durch die am Schluß des Paragraphen angegebene Übung 1 beleuchtet.

Ist $(\mathfrak{d}_i)$ eine orthonormierte Basis, bezüglich der die Matrix von b Diagonalform hat, so nennt man die Richtungen von $\mathfrak{d}_i$, $i = 1, \ldots, n$, *Hauptrichtungen* der Bilinearform; eine Koordinatentransformation, die die Diagonalform herstellt, nennt man auch *Hauptachsentransformation*. Man beachte, daß die Hauptrichtungen durch die Bilinearform genau dann eindeutig bestimmt sind, wenn alle Eigenwerte die Vielfachheit 1 haben. Für die Durchführung der Hauptachsentransformation gilt natürlich wieder das nach dem Beweis von Folgerung 4.4 Bemerkte.

Satz 2. *Es seien x_i orthogonale kartesische Punktkoordinaten des euklidischen Raumes V^n. Die Gleichung*

$$(x_i)'(q_{ij})(x_j) + (q_i)'(x_i) + q = 0, \qquad (q_{ij})' = (q_{ij}), \tag{4}$$

einer Quadrik $Q \subset \boldsymbol{E}^n$ kann durch eine orthogonale Koordinatentransformation

$$(\hat{x}_i) = (\alpha_{ij})(x_j) + (\alpha_i), \qquad (\alpha_{ij}) \in \boldsymbol{O}(n), \tag{5}$$

und Normierung, d. h. Multiplikation mit einer Zahl $c \neq 0$, $c \in \mathbf{R}$, auf eine und nur eine der folgenden Normalformen gebracht werden:

$$\text{(I)} \qquad \sum_{\alpha=1}^{r} \lambda_\alpha x_\alpha^2 - 1 = 0, \tag{6}$$

$$\text{(II)} \qquad \sum_{\alpha=1}^{r} \lambda_\alpha x_\alpha^2 = 0 \quad \textit{mit} \quad \lambda_1 = 1, \tag{7}$$

$$\text{(III)} \qquad \sum_{\alpha=1}^{r} \lambda_\alpha x_\alpha^2 + x_{r+1} = 0; \tag{8}$$

dabei gelten:

a) $\lambda_\alpha \neq 0, \qquad \alpha = 1, \ldots, r = \operatorname{rg}(q_{ij}), \qquad r \geqq 1;$ (9)

b) $\lambda_1 \geqq \ldots \geqq \lambda_r;$ (10)

c) *in den Fällen* (II) *und* (III) *ist die Anzahl* l *der negativen* λ_α *kleiner oder gleich* $r/2$; *wenn* $l = r/2$ *und* ϱ *die kleinste Zahl mit* $|\lambda_\varrho| \neq |\lambda_{r-\varrho+1}|$ *ist, sei* $|\lambda_\varrho| > |\lambda_{r-\varrho+1}|$.

Beweis. Zum Beweis der Existenz der Normalform brauchen wir nur dem Beweis von Satz 5.9.9 zu folgen. Ist Q zentral, so legen wir o in ein Zentrum und erreichen $(q_i) = (0)$. Die Hauptachsentransformation für die Matrix (q_{ij}) liefert bei geeigneter Numerierung der Achsen und Normierung die Typen (I) oder (II), wobei a), b) und c) erfüllt sind. Ist Q nicht zentral, so führen wir zuerst die Hauptachsentransformation aus und erhalten eine Gleichung der Form (5.9.66), woraus wir durch eine Translation auf (5.9.67) kommen. Da die Transformation (5.9.68) nicht orthogonal ist, müssen wir das Verfahren hier etwas abändern, um durch eine euklidische Transformation die Normalform (III) herzustellen. Wir setzen

$$x'_\alpha = \hat{x}_\alpha, \qquad \alpha = 1, \ldots, r, \qquad x'_{r+1} = \mu^{-1} \sum_{\varrho=r+1}^{n} q_\varrho \hat{x}_\varrho \tag{11}$$

mit

$$\mu := \left(\sum_{\varrho=r+1}^{n} q_\varrho^2 \right)^{1/2} \neq 0; \tag{12}$$

denn sonst wäre die Quadrik zentral. Die Matrix aus $r+1$ orthonormierten Spaltenvektoren des $\mathbf{R}^n$

$$\begin{pmatrix} 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & & \vdots & \vdots \\ \vdots & 0 & \ddots & 1 & 0 \\ \vdots & \vdots & & 0 & \alpha_{r+1,r+1} \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & \alpha_{r+1,n} \end{pmatrix} \quad \text{mit} \quad \alpha_{r+1,\varrho} := \mu^{-1} q_\varrho, \qquad \varrho = r+1, \ldots, n,$$

ergänzen wir durch Hinzufügen geeigneter Spaltenvektoren zu einer orthogonalen Matrix $(\alpha_{ij}) \in \boldsymbol{O}(n)$; das ist nach Folgerung 2.1 möglich. Setzen wir

$$x'_\varrho = \sum_{\sigma=r+1}^{n} \alpha_{\varrho\sigma} \hat{x}_\sigma, \qquad \varrho = r+2, \ldots, n, \tag{13}$$

so folgt nach Ausführung der durch (11) und (13) bestimmten Transformation

$$\sum_{\alpha=1}^{r} \lambda_\alpha x'^2_\alpha + \mu x'_{r+1} = 0. \tag{14}$$

Division durch μ führt auf die Form (III). Zum Beweis der Eindeutigkeit bemerken wir zuerst, daß wegen der Bedingungen a), b), c) bzw. wegen der Form der Gleichungen eine Normierung nicht mehr möglich ist. Wie schon durch Satz 5.9.10 be-

wiesen, lassen sich Gleichungen verschiedener Typen (I), (II), (III), nicht einmal durch eine affine Koordinatentransformation, also erst recht nicht durch eine euklidische, ineinander überführen. Da bei einer euklidischen Transformation die charakteristischen Polynome der quadratischen Bestandteile der Gleichungen invariant bleiben, lassen sich auch Gleichungen desselben Typs, aber mit verschiedenen r oder λ_α nicht ineinander transformieren. □

Mit Hilfe von Satz 2 läßt sich die euklidische Klassifikation der Quadriken leicht durchführen. Jede Klasse affin-kongruenter Quadriken spaltet in der Regel in eine unendliche Menge euklidischer Klassen auf, welche durch die Konstanten $\lambda_1, \ldots, \lambda_r$ beschrieben werden. So sind z. B. alle *Ellipsoide*

$$\left(\frac{x_1}{a_1}\right)^2 + \ldots + \left(\frac{x_n}{a_n}\right)^2 = 1 \tag{15}$$

affin-kongruent; euklidisch jedoch unterscheiden sie sich durch ihre *Halbachsen* $a_i := (\lambda_i)^{-1/2}$ (vgl. Abb. 12). Sind alle a_i gleich derselben Zahl a, so erhalten wir als Spezialfall die Gleichung einer *Hypersphäre vom Radius* a. Wir empfehlen dem

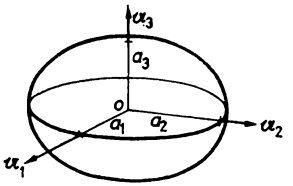


Abb. 12

Leser die Durchführung der Klassifikation vor allem für $n=2, 3$ im einzelnen; hierbei kann man sich an der affinen Klassifikation orientieren und hat dann nur die euklidische Aufspaltung der affinen Klassen zu untersuchen. Das folgende Beispiel weist auf eine gewisse Schwierigkeit hin.

Beispiel 1. Die Gleichungen

$$x_1^2 + \lambda_2 x_2^2 = 0, \qquad 0 < \lambda_2 \leqq 1\,, \tag{16}$$

etwa gedacht über dem E^3, sind für verschiedene Werte von λ_2 nicht $\mathfrak{E}(3)$-äquivalent, obwohl sie alle dieselbe Quadrik, nämlich den in die x_3-Achse ausgearteten Kegel $x_1 = x_2 = 0$ beschreiben.

Um also von der Klassifikation der Gleichungen auf die Klassifikation der Quadriken zu kommen, muß man noch untersuchen, wann zwei verschiedene der Normalformen der Gleichungen kongruente Quadriken bestimmen; denn die Übereinstimmung der Normalformen ihrer Gleichungen ist hinreichend, aber, wie Beispiel 1 zeigt, nicht notwendig für die Kongruenz der Quadriken. Wir nennen eine Quadrik $Q \subset A^n$ *degeneriert*, wenn sie schon in einer k-Ebene H^k, $k < n-1$, des affinen (bzw. euklidischen) Raumes A^n liegt. Man macht sich leicht klar, daß nur die imaginären Quadriken (Typ (I), alle $\lambda_\alpha \leqq 0$) und die doppelt zählenden Ebenen, das sind die Quadriken vom Typ (II) mit $\lambda_\alpha > 0$ für $\alpha = 1, \ldots, r$ im Fall $r \geqq 2$ degeneriert sind. Aus Übung 3 erhält man

Satz 3. *Zwei nicht degenerierte Quadriken des euklidischen Raumes $\boldsymbol{E}^n$ sind genau dann kongruent, wenn ihre Gleichungen dieselbe Normalform aus Satz 2 haben.* □

Übung 1. Es sei $\boldsymbol{V}^n$ ein unitärer Raum, $K = \mathbf{R}, \mathbf{C}$. Für $K = \mathbf{C}$ sei $L_{1,1}(\boldsymbol{V}^n)$ die Menge der Abbildungen $b\colon \boldsymbol{V}^n \times \boldsymbol{V}^n \to \mathbf{C}$, die im ersten Argument linear und im zweiten konjugiert-linear sind. Man beweise: a) Die Menge $L_{1,1}(\boldsymbol{V}^n)$ ist ein Vektorraum über $\mathbf{C}$, und die Abbildung

$$\Phi\colon a \in \boldsymbol{L}(\boldsymbol{V}^n) \mapsto b_a \in L_{1,1}(\boldsymbol{V}^n) \quad \text{mit} \quad b_a(\mathfrak{x}, \mathfrak{y}) := \langle a\mathfrak{x}, \mathfrak{y}\rangle \tag{17}$$

ist ein Isomorphismus der Vektorräume. — b) im Fall $K = \mathbf{R}$ ist die analog definierte Abbildung $\Phi\colon \boldsymbol{L}(\boldsymbol{V}^n) \to \boldsymbol{L}_2(\boldsymbol{V}^n)$ von $\boldsymbol{L}(\boldsymbol{V}^n)$ auf die Menge der Bilinearformen (Definition 5.9.3) ebenfalls ein Isomorphismus der Vektorräume. — c) Die Räume $L_{1,1}(\boldsymbol{V}^n)$ (bzw. $\boldsymbol{L}_2(\boldsymbol{V}^n)$) sind $\boldsymbol{GL}(\boldsymbol{V}^n)$-Transformationsgruppen mit der Wirkung

$$gb(\mathfrak{x}, \mathfrak{y}) = b(g^{-1}\mathfrak{x}, g^{-1}\mathfrak{y}), \qquad \mathfrak{x}, \mathfrak{y} \in \boldsymbol{V}^n, \tag{18}$$

für $g \in \boldsymbol{GL}(\boldsymbol{V}^n)$ und $b \in L_{1,1}(\boldsymbol{V}^n)$ (bzw. $\boldsymbol{L}_2(\boldsymbol{V}^n)$). Schränkt man diese Wirkung und ebenso die Wirkung (5.8.1) von $\boldsymbol{GL}(\boldsymbol{V}^n)$ über $\boldsymbol{L}(\boldsymbol{V}^n)$ auf $\boldsymbol{U}(n)$ (bzw. $\boldsymbol{O}(n)$) ein, so wird Φ ein $\boldsymbol{U}(n)$-Isomorphismus (bzw. $\boldsymbol{O}(n)$-Isomorphismus) der Transformationsgruppen (vgl. Beispiel 1.5.4). — d) $\Phi \mid \boldsymbol{L}_s(\boldsymbol{V}^n)$ ist ein $\boldsymbol{U}(n)$-Isomorphismus (bzw. $\boldsymbol{O}(n)$-Isomorphismus) des Raumes der selbstadjungierten Operatoren auf den Raum $\mathfrak{H}(\boldsymbol{V}^n)$ der hermiteschen Formen (bzw. $\boldsymbol{L}_2(\boldsymbol{V}^n)_s$ der symmetrischen Bilinearformen). Hieraus und aus Satz 4.2 leite man die unitäre Normalform

$$\sum_{j=1}^{r} \lambda_j \xi_j \bar{\eta}_j, \qquad 0 \neq \lambda_j \in \mathbf{R}, \qquad \lambda_1 \geqq \ldots \geqq \lambda_r, \qquad r = \operatorname{rg} b\,, \tag{19}$$

der hermiteschen Formen und Satz 1 her. Zwei hermitesche Formen sind genau dann $\boldsymbol{U}(n)$-äquivalent, wenn die aus ihren Matrizen bezüglich irgendwelcher orthonormierter n-Beine gebildeten charakteristischen Polynome (2) übereinstimmen.

Übung 2. Man beweise, daß $\Phi \mid \boldsymbol{L}_{sh}(\boldsymbol{V}^n)$ ebenfalls ein $\boldsymbol{U}(n)$-Isomorphismus auf den reellen Vektorraum der schiefhermiteschen Formen $L_{1,1}(\boldsymbol{V}^n)_a \subset L_{1,1}(\boldsymbol{V}^n)$ ist; dabei heißt eine Form $b \in L_{1,1}(\boldsymbol{V}^n)$ *schiefhermitesch*, wenn

$$b(\mathfrak{y}, \mathfrak{x}) = -\overline{b(\mathfrak{x}, \mathfrak{y})} \quad \text{für alle} \quad \mathfrak{x}, \mathfrak{y} \in \boldsymbol{V}^n \tag{20}$$

gilt. Aus Übung 4.2 leite man eine unitäre Normalform für die schiefhermiteschen Formen her. Analoges zeige man für $K = \mathbf{R}$ und $\Phi \mid \boldsymbol{L}_a(\boldsymbol{V}^n)$, $\boldsymbol{V}^n$ euklidisch; aus Übung 4.3 erhält man dann eine orthogonale Normalform der schiefsymmetrischen Bilinearformen.

Übung 3. Offenbar ist der Begriff degenerierte Quadrik schon in der affinen Geometrie sinnvoll. Wir betrachten einen reellen, affinen Raum $\boldsymbol{A}^n$ mit den kartesischen Punktkoordinaten (x_i). Man beweise: Zwei Gleichungen der Form (5.9.1) mit den Koeffizienten q_{ij}, q_i, q bzw. $\hat{q}_{ij}, \hat{q}_i, \hat{q}$ und $q_{ij} = q_{ji}$, $\hat{q}_{ij} = \hat{q}_{ji}$, $i, j = 1, \ldots, n$, nicht alle q_{ij} (bzw. $\hat{q}_{ij}$) gleich 0, bestimmen genau dann dieselbe nicht degenerierte Quadrik $\boldsymbol{Q} \subset \boldsymbol{A}^n$, wenn es eine Zahl $\mu \in \mathbf{R}$ mit $\mu \neq 0$ und

$$\hat{q}_{ij} = q_{ij}\mu, \qquad \hat{q}_i = q_i\mu, \qquad \hat{q} = q\mu, \qquad i, j = 1, \ldots, n\,, \tag{21}$$

gibt. (Hinweis. Die Bedingung ist offenbar hinreichend. Für den Beweis der Notwendigkeit überzeugt man sich anhand der in § 5.9 hergeleiteten Transformationsformeln davon, daß die Bedingung (21) bei Transformation der affinen Koordinaten (x_i) (simultan in beiden Gleichungen) und Normierung der Gleichungen erhalten bleibt. Für $n = 1, 2$ beweist man die Behauptung direkt; dabei kann man o. B. d. A. eine der Gleichungen als Normalform annehmen. Für $n \geqq 3$ führt man den Beweis durch

vollständige Induktion: Man lege das n-Bein $(o; \mathfrak{a}_i)$ des $\boldsymbol{A}^n$ so, daß $a_i := o + \mathfrak{a}_i \in Q$, $i = 1, \ldots, n$, und $o \notin Q$ gilt. Es sei $\boldsymbol{H}_i$ die Koordinaten-Hyperebene $x_i = 0$ und $Q_i := Q \cap \boldsymbol{H}_i$. Man zeigt, daß die Q_i in $\boldsymbol{H}_i$ nicht degeneriert sind. Ein Blick auf die Gleichungen von drei der Q_i schließt die Induktion ab.) — Zum Beweis von Satz 3 beachte man, daß die Zuordnung „nichtdegenerierte Quadrik $Q \mapsto$ Gleichung" bei gegebenem Koordinatensystem bis auf einen Faktor eindeutig ist, und wende Satz 2 an.

Übung 4. Es sei $q(\mathfrak{x}) := b(\mathfrak{x}, \mathfrak{x})$, b eine hermitesche Form (bzw. symmetrische Bilinearform) auf dem unitären Vektorraum $\boldsymbol{V}^n$. Man beweise: a)

$$\min \{q(\mathfrak{x}) \mid |\mathfrak{x}| = 1\} = \min \{\lambda \mid \lambda \text{ Eigenwert von } b\},$$

$$\max \{q(\mathfrak{x}) \mid |\mathfrak{x}| = 1\} = \max \{\lambda \mid \lambda \text{ Eigenwert von } b\}.$$

f) Im Fall $K = \mathbf{R}$ leite man die zu (5.8.5) analoge charakteristische Gleichung $\chi_b(\lambda) = 0$ für die Eigenwerte durch Betrachtung eines Extremalproblems mit Nebenbedingungen her (Lagrangesche Multiplikatorenregel, vgl. ein Lehrbuch der Analysis). Weiter sei Q eine zentrale Quadrik des euklidischen Raumes $\boldsymbol{E}^n$ mit dem Zentrum o. Man diskutiere das Extremalproblem $\varrho(o, x) =$ Extremum unter der Nebenbedingung $x \in Q$.

Zum Abschluß dieses Paragraphen möchten wir noch mit einigen Bemerkungen auf das *Erlanger Programm* von Felix Klein [1] eingehen, das einen großen Einfluß auf die Entwicklung der Geometrie hatte. Die in diesen *„Vergleichenden Betrachtungen über neuere geometrische Forschungen"* aus dem Jahre 1872 aufgestellten Grundsätze lassen sich etwa folgendermaßen zusammenfassen:

I. *Zu jeder Geometrie gehört eine entsprechende Automorphismengruppe, die Gruppe derjenigen Transformationen des Raumes X, bei denen die gerade untersuchten geometrischen Eigenschaften ungeändert bleiben.*

II. *Es sei eine Transformationsgruppe gegeben; die geometrischen Eigenschaften der transformierten Gebilde sind dann gerade diejenigen, die bei allen Transformationen der Gruppe invariant bleiben.*

Im Sinne von I haben wir die affine Gruppe $\mathfrak{A}(n)$, die euklidische Gruppe $\mathfrak{E}(n)$ und die Gruppe $\mathfrak{SE}(n) := \boldsymbol{SO}(n) \cdot \mathfrak{T}(\boldsymbol{E}^n)$ der orientierungserhaltenden euklidischen Bewegungen gebildet, vgl. Folgerung 2.6, (2.39) und Satz 3.1. Man bemerkt die Inklusionen $\mathfrak{A}(n) \supset \mathfrak{E}(n) \supset \mathfrak{SE}(n)$. Den zweiten Grundsatz haben wir z. B. bei der Untersuchung der Quadriken angewandt: Die affine Geometrie der Quadriken bedeutet die Aufstellung eines vollständigen Invariantensystems gegenüber affinen Transformationen, und ihre euklidische Geometrie läuft auf ihre euklidische Klassifikation hinaus. Natürlich lassen sich viele geometrische Eigenschaften der Quadriken sowohl in der affinen als auch in der euklidischen Geometrie angeben, die hier nicht einmal erwähnt wurden; diese haben jedoch einen mehr speziellen und beschreibenden Charakter. Nach der Lösung des Klassifikationsproblems lassen sich viele Fragen über die gerade betrachteten geometrischen Objekte oft recht einfach beantworten, es ist als die Grundaufgabe der Geometrie einer Transformationsgruppe anzusehen (vgl. § 5.7).

Wir vergleichen nun verschiedene Geometrien derselben Objektmenge, d. h. Transformationsgruppen $[G, X]$, $[H, X]$ über derselben Menge X, wobei wir $G, H \subseteq S(X)$ annehmen können (Beispiel 1.4.1; man beachte, daß auch im allgemeinen Fall die Wirkung einer beliebigen Gruppe G über X nur über das Bild $\varphi(G)$ des die

Wirkung von G über X definierenden Homomorphismus φ (1.4.3) realisiert wird). Nach F. KLEIN gilt die leicht zu verifizierende Feststellung

III. *Ist für eine Grundmenge X von geometrischen Objekten die Gruppe $G \supset H$, so ist jede G-Invariante auch eine H-Invariante.*

Je größer die Gruppe einer Transformationsgruppe über X ist, desto allgemeiner ist ihre Geometrie und desto kleiner ist die Menge ihrer Invarianten. Zum Beispiel ist die affine Geometrie (bei $K = \mathbf{R}$) in diesem Sinne allgemeiner als die euklidische; in der euklidischen Geometrie sind die Hauptachsen einer Quadrik invariant, und in der affinen ist das nicht der Fall; z. B. sind alle Ellipsen affin, aber nicht euklidisch äquivalent. Zwischen der euklidischen und der affinen liegt die *äquiaffine Geometrie*; gibt man in einem affinen Raum eine Volumenfunktion vor, so wird die *äquiaffine Gruppe* als die Menge aller derjenigen affinen Transformationen f definiert, die die Volumenfunktion invariant lassen; diese Bedingung ist nach (5.7.32) äquivalent zu $N(a_f) = 1$. Hier wurde Grundsatz I angewandt. Nach Grundsatz II untersucht die äquiaffine Geometrie diejenigen Eigenschaften, die bei der äquiaffinen Gruppe invariant bleiben; natürlich ist jede affine Eigenschaft auch äquiaffin und euklidisch invariant, aber nicht umgekehrt (Grundsatz III).

Die Durchführung dieser Grundsätze benutzte F. KLEIN zur Einteilung der Geometrien nach ihren Bewegungsgruppen. Die Bedeutung dieser Prinzipien wird allerdings erst voll sichtbar, wenn man die Geometrie vom projektiven Standpunkt aus betreibt, den wir in Band 3 entwickeln wollen.

Eine konsequente Ausgestaltung der F. Kleinschen Gedanken in der modernen Terminologie führt auf die in § 1.5 behandelten Kategorien; als Geometrie einer Gruppe G kann man die Kategorie $\mathfrak{T}(G)$ der Transformationsgruppen $[G, X]$ (G fest) mit den G-Invarianten als Morphismen ansehen (Beispiel 1.5.4). Die vergleichenden Betrachtungen verschiedener Geometrien lassen sich in der Kategorie $\mathfrak{T}$ aller Transformationsgruppen mit den äquivarianten Morphismen, Beispiel 1.5.3, anstellen. Man erkennt schließlich, daß die zuerst im Erlanger Programm ausgeführten Betrachtungen eine weit über die Geometrie hinausreichende Bedeutung gewonnen haben: In jeder Kategorie gehört zu jeder Objektmenge X die Automorphismengruppe $\mathrm{Aut}(X)$, vgl. Satz 1.5.1, die eine Transformationsgruppe von X ist. Die Kategorien aber sind der sehr allgemeine Rahmen, in dem sich die Mathematik heute unterbringen läßt.

Literatur

Александров, П. С.

[1] Лекции по аналитической геометрии, пополненные необходимыми сведениями из алгебры с приложением собрания задач, снабженных решениями, составленного А. С. Пархоменко, Наука, Москва 1968.

Asser, G.

[1] Grundbegriffe der Mathematik, I. Mengen. Abbildungen. Natürliche Zahlen. 4. Aufl., VEB Deutscher Verlag der Wissenschaften, Berlin 1980.

Beiglböck, W. D.

[1] Lineare Algebra, Springer-Verlag, Berlin – Heidelberg – New York – Tokyo 1983.

Beresin, I. S., und N. P. Shidkow

[1] Numerische Methoden 2, VEB Deutscher Verlag der Wissenschaften, Berlin 1971 (Übersetzung aus dem Russischen).

Boseck, H.

[1] Einführung in die Theorie der linearen Vektorräume. VEB Deutscher Verlag der Wissenschaften, 5. Aufl., Berlin 1984.

Dieudonné, J.

[1] Algèbre linéaire et géométrie élémentaire, 3. éd., Hermann, Paris 1968 (russ. Ausgabe: Nauka, Moskau 1972).

Eisenreich, G.

[1] Lineare Algebra und analytische Geometrie, Akademie-Verlag, Berlin 1980.

Faddejew, D. K., und W. N. Faddejewa

[1] Numerische Methoden der linearen Algebra, 5. Aufl., VEB Deutscher Verlag der Wissenschaften, Berlin/Oldenburg-Verlag, München – Wien 1978 (Übersetzung aus dem Russischen).

Gantmacher, F. R.

[1] Matrizentheorie, VEB Deutscher Verlag der Wissenschaften, Berlin 1986 (Übersetzung aus dem Russischen).

Гельфанд, И. М.

[1] Лекции по линейной алгебре, Наука, Москва 1971.

Halmos, P. R.

[1] Finite-Dimensional Vector Spaces, 2. ed., D. van Nostrand Comp., Inc., Princeton (N. J.) – Toronto – London – New York 1958 (russ. Ausgabe: Gostechizdat, Moskau 1963).

Калужнин, Л. А.

[1] Введение в общую алгебру, Наука, Москва 1973.

KANTOR, I. L, und A. S. SOLODOWNIKOW

[1] Hyperkomplexe Zahlen, BSB Teubner Verlagsgesellschaft, Leipzig 1978 (Übersetzung aus dem Russischen).

KELLER, O.-H.

[1] Analytische Geometrie und lineare Algebra, VEB Deutscher Verlag der Wissenschaften, 3. Aufl., Berlin 1968.

KLAUA, D.

[1] Elementare Axiome der Mengenlehre, Akademie-Verlag, Berlin 1971.

[2] Grundbegriffe der axiomatischen Mengenlehre, Teil 1 und 2, Akademie-Verlag, Berlin 1973.

[3] Kardinal- und Ordinalzahlen, Teil I und II, Akademie-Verlag, Berlin 1974.

KLEIN, F.

[1] Vergleichende Betrachtungen über neuere geometrische Forschungen, Erlangen 1872. Mit historischen Bemerkungen von H. WUSSING herausgegeben in: Das Erlanger Programm, Ostwalds Klassiker der exakten Wissenschaften 253, Akademische Verlagsgesellschaft Geest & Portig K.-G., Leipzig 1974.

KOCHENDÖRFFER, R.

[1] Einführung in die Algebra, 4. Aufl., VEB Deutscher Verlag der Wissenschaften, Berlin 1974.

KOECHER, M.

[1] Lineare Algebra und analytische Geometrie, Grundwissen Mathematik Bd. 2, Springer-Verlag, Berlin – Heidelberg – New York – Tokyo 1983.

Кострикин, А. Г.

[1] Введение в алгебру, Наука, Москва 1977.

Кострикин, А. И., и Ю. И. Манин

[1] Линейная алгебра и геометрия, Изд-во МГУ, Москва 1980.

KUROSCH, A. G. (Курош, А. Г.)

[1] Gruppentheorie, Akademie-Verlag, Nachdruck, Berlin 1955 (Übersetzung aus dem Russischen; neue russ. Ausgabe: Nauka, Moskau 1967).

[2] Лекции по общей алгебре, Наука, Москва 1973.

[3] Общая алгебра, Наука, Москва 1974.

[4] Курс высшей алгебры, Наука, Москва 1971.

LANG, S.

[1] Algebra, Addison-Wesley Publ. Comp., Reading (Mass.) 1965 (russ. Ausgabe: Mir, Moskau 1968).

Мальцев, А. И.

[1] Основы линейной алгебре, Гостехиздат, Москва 1956.

PICKERT, G.

[1] Analytische Geometrie, Akademische Verlagsgesellschaft Geest & Portig K.-G., Leipzig 1953.

REICHARDT, H.

[1] Vorlesungen über Vektor- und Tensorrechnung, 2. Aufl., VEB Deutscher Verlag der Wissenschaften, Berlin 1968.

Шилов, Г. Е.

[1] Введение в теорию линейных пространств, Гостехиздат, Москва – Ленинград 1952.

SCHUBERT, H.

[1] Kategorien, Akademie-Verlag, Berlin 1970.

VAN DER WAERDEN, B. L.

[1] Algebra, Bd. I, 8. Aufl.; Bd. II, 5. Aufl., Springer-Verlag, Berlin – Heidelberg – New York 1971 bzw. 1967.

Namen- und Sachverzeichnis