Mathematisch-
Naturwissenschaftliche
Bibliothek

9

LUGOWSKI-WEINERT

GRUNDZÜGE DER ALGEBRA

TEIL I

MATHEMATISCH-NATURWISSENSCHAFTLICHE
BIBLIOTHEK

9

GRUNDZÜGE DER ALGEBRA

TEIL I

ALLGEMEINE GRUPPENTHEORIE

von

Dr. Herbert Lugowski und Dr. Hanns Joachim Weinert

Pädagogische Hochschule Potsdam

Mit 15 Abbildungen

B.G.TEUBNER VERLAGSGESELLSCHAFT · LEIPZIG

1 9 5 7

Lizenz-Nr. 294/375/48/57

Printed in Germany

Satz und Druck: (III/18/154) B.G.Teubner, Leipzig C1, Querstr.17 · 255

VORWORT

Die vorliegende Einführung in das Gedankengut der modernen Algebra wird drei aufeinander aufbauende Teile umfassen:

1. Allgemeine Gruppentheorie.
2. Allgemeine Ring- und Körpertheorie.
3. Auflösungstheorie algebraischer Gleichungen.

Sie entstand in gemeinsamer Arbeit aus Vorlesungen, die beide Verfasser seit 1951 an der Pädagogischen Hochschule Potsdam abgehalten haben, und erschien zunächst in einer Reihe von Lehrbriefen für das Fernstudium der Oberstufenlehrer. Gegenüber dieser ursprünglichen Form wurden zwar gewisse Abänderungen vorgenommen, ohne jedoch die Zielstellung solcher für das Selbststudium bestimmter Lehrbriefe aufzugeben, nämlich im wesentlichen ein Ersatz für die einführenden akademischen Vorlesungen zu sein.

Aus dieser Absicht erklärt sich auch die besondere Breite der Darstellung; der sich daraus ergebenden Gefahr der Unübersichtlichkeit versuchten die Verfasser durch eine strenge Gliederung und Systematisierung zu begegnen. So werden Definitionen, Sätze, Folgerungen bzw. Beispiele durchgehend mit D, S, F bzw. B und zwei nachfolgenden Nummern gekennzeichnet, von denen jeweils die erste die Nummer des Paragraphen, die zweite eine Durchnumerierung in jedem Paragraphen angibt.

Desgleichen sind die verhältnismäßig zahlreichen Aufgaben am Ende jedes Paragraphen beibehalten worden. Ihre Behandlung vor dem jeweiligen Weiterlesen ist sehr zu empfehlen, da ein Vertrautwerden mit den Begriffsbildungen der modernen Algebra wohl nur durch ständiges Anwenden und Üben möglich ist. Die vollständige Angabe sämtlicher Lösungen am Ende jedes Teiles wird dabei eine Hilfe sein. Auch geben die Aufgaben zusätzliche Beispiele sowie einige Ergänzungen zur Theorie.

An Vorkenntnissen werden (außer bei einzelnen erläuternden Beispielen) nur wenige Grundbegriffe der Mengenlehre vorausgesetzt, die jedoch auch einem nicht mit diesem Gebiet vertrauten Leser

ohne weiteres verständlich und einsichtig sind. Überdies findet man sie in einem Anhang erläuternd zusammengefaßt. Desgleichen werden die benötigten Aussagen der elementaren Zahlentheorie im laufenden Text mit entwickelt, zumal auf naheliegende zahlentheoretische Beispiele und Anwendungen wegen ihrer Einfachheit besonders gern zurückgegriffen wird. Die so vermittelten Kenntnisse ersetzen natürlich keineswegs ein systematisches Studium der elementaren Zahlentheorie selbst.

Die Verfasser möchten nicht versäumen, an dieser Stelle all denen ihren Dank auszusprechen, die an einer kritischen Durchsicht des Materials beteiligt waren, das diesen Bänden zugrunde liegt, insbesondere Herrn Prof. Dr. H. REICHARDT, Berlin, und Herrn Studienrat W. KLOBE, Erfurt. Desgleichen danken sie dem Verlag B. G. Teubner dafür, daß er es ermöglicht hat, diese Einführung in die Algebra einem breiteren Kreise mathematisch interessierter Leser zugänglich zu machen.

Potsdam, im Sommer 1956

H. LUGOWSKI H. J. WEINERT

INHALTSVERZEICHNIS

EINLEITUNG

Wie wohl bei kaum einer anderen mathematischen Disziplin hat sich die Auffassung über den Inhalt der Algebra im Laufe der historischen Entwicklung mehrfach gewandelt. Im ganzen kann man etwa vier Etappen unterscheiden, die wir hier kurz skizzieren wollen[1]).

1. Das Wort Algebra entstammt dem Titel „Hisâb aljabr w'almuqâbalah" eines Buches des berühmten choresmischen Mathematikers AL CHWÂRAZMÎ[2]). Aljabr w'almuqâbalah heißt etwa Ergänzung und Ausgleich und bedeutet in unserer heutigen Ausdrucksweise das Hinzufügen oder Weglassen eines konstanten Gliedes auf der einen Seite einer Gleichung durch „Ergänzung und Ausgleich" auf der anderen Seite. Vom Abendlande wurde dann das Wort „Aljabr" als Bezeichnung für die noch recht primitive, jeder Buchstaben- und Zeichensymbolik entbehrende Lehre über die Auflösung von Gleichungen übernommen.

2. Mit VIETA[3]) und DESCARTES[4]) beginnt die Symbolik unserer heutigen Buchstabenrechnung, an der auch LEIBNIZ[5]) und NEWTON[6]) noch Anteil haben. Erst mit ihr werden kompliziertere mathematische Ausdrücke übersichtlich, und ihre allgemeine Be-

---

1) Die folgende Darstellung lehnt sich an einen Vortrag an, der von B. N. DELAUNAY auf der Konferenz über „Algebra und Zahlentheorie" im September 1951 in Moskau gehalten wurde.

2) MUHAMED IBN MUSA AL CHWÂRAZMÎ wirkte um 810 bis 840 als Astronom am Hofe al Mamuns, des Sohnes von Harun al Raschid, in Bagdad.

3) FRANÇOIS VIÈTE (lat. VIETA), 1540 bis 1603, frz. Jurist und Mathematiker; führt allgemein Buchstaben für Unbekannte und Koeffizienten sowie die Zeichen „+", „—" und den Bruchstrich ein.

4) RENÉ DESCARTES (lat. CARTESIUS), 1596 bis 1650, frz. Philosoph und Mathematiker; setzt sich für VIETAS Symbolik ein und schafft heutige Bezeichnung der Potenzen.

5) GOTTFRIED WILHELM LEIBNIZ 1646 bis 1716, Politiker, Philosoph und Mathematiker; führt die Zeichen „·" und „:" ein und verallgemeinert die schon von FRANS VAN SCHOOTEN (1615 bis 1660) eingeführten Indizes; darüber hinaus verdankt man ihm die heute gebräuchliche Symbolik der Infinitesimalrechnung.

6) ISAAC NEWTON, 1643 bis 1727, engl. Physiker und Mathematiker; setzt die allgemeine Verwendung des schon 1557 von seinem Landsmann ROBERT RECORDE eingeführten Gleichheitszeichens durch.

handlung, einschließlich der Umformungsregeln für Gleichungen, grenzt sich gegenüber der Arithmetik ab, die es stets mit konkreten Zahlen zu tun hat. So überträgt sich der Name Algebra schließlich auf alles, was in der Mathematik mit Berechnungen nach Regeln zusammenhängt, die durch eingesetzte Zahlen realisiert werden können. Es ist dies mit anderen Worten die damals bekannte Buchstabenrechnung, soweit sie sich nicht auf Geometrie und Infinitesimalrechnung bezieht. Sie stimmt weitgehend mit der Algebra unserer heutigen Schulmathematik überein und hat ihren charakteristischen Niederschlag in dem Lehrbuch von EULER[1]) gefunden.

3. Am Ende des 18. Jahrhunderts tritt die Frage der Auflösung einer Gleichung n-ten Grades in einer Unbekannten so sehr in den Vordergrund, daß alles andere den Charakter von Hilfsmitteln für dieses schwere und tiefliegende Problem annimmt. Es hat bis zu seiner endgültigen Lösung nahezu 300 Jahre lang die hervorragendsten Mathematiker beschäftigt, von denen hier nur einige genannt seien. So gelingt schon den italienischen Mathematikern der Renaissance[2]) die allgemeine Lösung der Gleichungen 3. und 4. Grades. TSCHIRNHAUS[3]) und LAGRANGE[4]) bemühen sich um allgemeine Gesichtspunkte, insbesondere um die Zurückführung vorgelegter Gleichungen auf bereits lösbare Hilfsgleichungen, sogenannte Resolventen. GAUSS[5]) beweist den sogenannten Fundamentalsatz der Algebra, d. h. die Existenz der Wurzeln einer Gleichung innerhalb der Menge der komplexen Zahlen. DESCARTES, NEWTON, LAGRANGE, LOBATSCHEWSKI[6]) STURM[7]), SYLVESTER[8]) beschäftigen sich mit der Bestimmung der Anzahl und der approximativen Berechnung von reellen Wurzeln. ABEL[9]) zeigt, daß Gleichungen 5. und höheren Grades nicht allgemein durch Radikale

---

1) LEONHARD EULER, 1707 bis 1783, „Vollständige Anleitung zur Algebra", Petersburg 1770.

2) SCIPIONE DEL FERRO, 1465 bis 1526; NICCOLÒ TARTAGLIA, 1500 bis 1557; GERONIMO CARDANO, 1501 bis 1576; LUDOVICO FERRARI, 1522 bis 1565.

3) EHRENFRIED WALTER VON TSCHIRNHAUS, 1651 bis 1708.

4) JOSEPH LOUIS LAGRANGE, 1736 bis 1813.

5) CARL FRIEDRICH GAUSS, 1777 bis 1855.

6) NIKOLAUS IWAN LOBATSCHEWSKI, 1793 bis 1856.

7) JAQUES CHARLES FRANÇOIS STURM, 1803 bis 1855.

8) JAMES JOSEPH SYLVESTER, 1814 bis 1897.

9) NIELS HENRIK ABEL, 1802 bis 1829.

lösbar sind, während GALOIS[1]) durch die Einführung des Gruppenbegriffes das entscheidende Hilfsmittel zur Beherrschung dieses Problems schafft.

So versteht man über 100 Jahre lang unter Algebra im wesentlichen wieder Gleichungstheorie, wenn auch auf einer viel höheren Entwicklungsstufe als in der ersten Etappe und mit allen Hilfsmitteln der zweiten Etappe. Den mathematischen Inhalt dieser Epoche, den wir in den Lehrbüchern von SERRET, WEBER und PERRON[2]) dargestellt finden, bezeichnen wir heute meist als „klassische Algebra".

4. Die von der klassischen Algebra eingeführten Hilfsbegriffe wie Gruppe, Körper usw. zeigen in ihrer Weiterentwicklung, an der Mathematiker wie E. E. KUMMER (1810 bis 1893), L. KRONECKER (1823 bis 1891), R. DEDEKIND (1831 bis 1916), C. JORDAN (1838 bis 1922), O. HÖLDER (1859 bis 1937), und E. STEINITZ (1871 bis 1928) beteiligt sind, daß ihre Anwendungsmöglichkeiten viel weiter reichen, als zunächst angenommen werden konnte. Die in ihnen behandelten algebraischen Gesetzmäßigkeiten erstrecken sich nämlich auf zahlreiche Begriffsbildungen der übrigen mathematischen und naturwissenschaftlichen Disziplinen, wie etwa Vektoren, Tensoren, Transformationen, Lösungssysteme von Differentialgleichungen, rationale Funktionen usw.

So vollzieht sich mit Beginn unseres Jahrhunderts abermals eine radikale Umwälzung der Algebra. In Anlehnung an die vorhandenen konkreten Vorbilder werden nun die verschiedensten Systeme von Dingen mit abstrakt definierten Rechenverknüpfungen untersucht. Ausgehend vom allgemeinen Mengenbegriff entstehen so „algebraische Strukturen" wie Gruppe, Modul, Ring, Körper, hyperkomplexes System, Verband, deren Erforschung zur eigentlichen Aufgabe der Algebra geworden ist. Darum haben sich u. a. D. HILBERT (1862 bis 1943), EMMY NOETHER (1882 bis 1935) sowie die Mathematiker der Gegenwart P. S. ALEXANDROFF, E. ARTIN, R. BRAUER, H. HASSE, W. KRULL, A. G. KUROSCH, O. J. SCHMIDT, B. L. VAN DER WAERDEN verdient gemacht.

---

1) ÉVARISTE GALOIS, 1811 bis 1832.
2) I. A. SERRET, Handbuch der höheren Algebra, 2 Bände, deutsche Auflage Leipzig 1868; H. WEBER, Lehrbuch der Algebra, 2 Bände, Braunschweig 1896; O. PERRON, Algebra, 2 Bände, 3. Auflage Berlin 1951.

Selbstverständlich erfolgt von diesen abstrakten Begriffen aus wieder eine fruchtbare Durchdringung der klassischen Algebra. Damit entsteht die „moderne Algebra" in der Gestalt, wie sie heute an den Hochschulen gelehrt wird und wie sie zuerst in dem bekannten ausgezeichneten Lehrbuch von V. D. WAERDEN dargestellt wurde. Darüber hinaus gestatten die modernen algebraischen Begriffsbildungen eine weitgehende Anwendung in vielen anderen mathematischen Disziplinen. Sie lassen überall, nicht zuletzt auch in der Elementarmathematik, zusammenfassende, strukturelle Gesichtspunkte deutlich werden und allgemeine Überblicke gewinnen.

I. GRUNDBEGRIFFE DER GRUPPENTHEORIE

Wie alle algebraischen Strukturbegriffe stellt auch der Gruppenbegriff eine zusammenfassende Abstraktion gewisser Gesetzmäßigkeiten dar, die den verschiedensten mathematischen Gegenständen gemeinsam sind. Bei der Addition von Vektoren oder Matrizen, bei der Multiplikation aller möglichen Potenzen einer festen Zahl, bei der Nacheinanderausführung von Vertauschungen irgendwelcher Objekte (Permutationen) oder von geometrischen Abbildungen (etwa projektive, affine, kongruente Transformationen), überall treten – um zunächst nur einige Beispiele zu nennen – Operationen auf, die wie die Addition bzw. Multiplikation von Zahlen als eindeutige, assoziative Verknüpfungen aufgefaßt werden können und überdies in einem noch näher auszuführenden Sinne umkehrbar sind. Durch eine allgemeine Kennzeichnung solcher Operationen und die Untersuchung der für sie gültigen Gesetzmäßigkeiten gelingt es der Gruppentheorie, das ihnen Gemeinsame zu erfassen und so Überlegungen ein für allemal vorwegzunehmen, die sonst immer wieder für sich durchgeführt werden müßten.

Begriffsbildungen, die auf Grund einer glücklichen Ausgewogenheit zwischen inhaltlicher Struktur und umfangreicher Anwendbarkeit zu klärenden und ordnenden Prinzipien in fast allen mathematischen Disziplinen werden, sind natürlich das Ergebnis einer langen Entwicklung. Sie erstreckte sich beim Gruppenbegriff über einen Zeitraum von etwa 100 Jahren und war lange auf Gruppen von Permutationen beschränkt, bis man schrittweise immer weitergehende Anwendungsmöglichkeiten der so gefundenen Aussagen erkannte.

Die Fruchtbarkeit des so entstandenen Gruppenbegriffes, den wir im § 1 zunächst auf verschiedene Arten kennzeichnen, wird wohl schon die darauffolgende systematische Zusammenstellung von Beispielen deutlich machen, wobei wir auch auf die oben bereits erwähnten näher eingehen. Die weiteren Paragraphen dieses Kapitels entwickeln sodann die allgemeinen Grundlagen, auf denen

die Behandlung spezieller Gruppen im zweiten Kapitel und weitergehende Strukturuntersuchungen in den nächsten Kapiteln aufbauen können.

§ 1. Gruppen

Die Gruppentheorie betrachtet stets nur eine zwischen den Elementen einer Menge erklärte Operation oder Verknüpfung. Obgleich diese nach unseren einleitenden Bemerkungen in konkreten Fällen sehr verschiedener Art sein kann, ist es üblich, sie im allgemeinen als Multiplikation zu schreiben und auch die dabei geläufigen Bezeichnungen wie Faktor, Produkt usw. zu gebrauchen.

Definition **D (1.1)**

Eine nichtleere Menge von Elementen $a, b, c, \ldots$ heißt eine multiplikative Gruppe $\mathfrak{G}$, wenn in ihr eine als Multiplikation geschriebene Verknüpfung festgelegt ist, die folgenden Axiomen genügt:

M I: *Die Multiplikation ordnet je zwei in bestimmter Reihenfolge gegebenen Elementen $a \in \mathfrak{G}$ und $b \in \mathfrak{G}$ ein Element $c \in \mathfrak{G}$ eindeutig zu:*

$$a \cdot b = c.$$

Im allgemeinen ist das Produkt von der Reihenfolge der Faktoren abhängig[1]*).*

M II: *Die Multiplikation ist assoziativ:*

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

M III: *Die Multiplikation ist in $\mathfrak{G}$ in dem Sinne umkehrbar, daß zu beliebigen $a \in \mathfrak{G}$ und $b \in \mathfrak{G}$ die Gleichungen*

$$a \cdot x = b \text{ und } y \cdot a = b$$

mit $x \in \mathfrak{G}$ und $y \in \mathfrak{G}$ lösbar sind. Zu vorgegebenem Resultat der Multiplikation und einem vorgegebenen Faktor gibt es also in $\mathfrak{G}$ einen zum Produkt ergänzenden anderen Faktor (Möglichkeit der beiderseitigen Division).

---

1) Das Verknüpfungszeichen „$\cdot$“ wird oft weggelassen, wenn keine Mißverständnisse zu befürchten sind.

Insbesondere heißt eine Gruppe kommutativ oder abelsch[1]*, wenn darüber hinaus gilt:*

M IV: Die Multiplikation ist kommutativ:

$$a \cdot b = b \cdot a.$$

Man unterscheidet endliche und unendliche Gruppen im Einklang mit den Begriffen der Mengenlehre und nennt die Anzahl der Elemente die *Ordnung* der Gruppe.

Als Beispiel können zunächst die in B(2.1c) und B(2.2a) angegebenen multiplikativen Gruppen dienen. Weiterhin überzeugt man sich sofort, daß auch die in B(2.4c) genannten regulären Matrizen bezüglich der Matrizenmultiplikation den Axiomen *M I*, *M II*, *M III*, nicht aber dem Axiom *M IV* genügen. Wir werden übrigens in S(1.9) allgemein zeigen, daß die in B(2.4c) nachgewiesenen Aussagen $M\,III_1$ und $M\,III_2$ mit *M III* gleichwertig sind.

Selbstverständlich ist die Gruppenverknüpfung von der multiplikativen Schreibweise unabhängig. Gehen wir zur additiven Schreibweise über (vgl. D(1.11)), erhalten wir weitere Beispiele für (abelsche) Gruppen. Dazu betrachte man etwa B(2.1b), B(2.1c), B(2.3), B(2.4b).

Man verdeutliche sich auch die nachstehenden Folgerungen an einigen dieser Beispiele.

Das Assoziativgesetz *M II* sagt aus: Ein Produkt von drei Faktoren ist eindeutig durch die Angabe seiner Faktoren und deren Reihenfolge bestimmt; es ist unabhängig davon, welche Faktoren man zur Ausrechnung durch Klammern zusammenfaßt. Man kann also ein Produkt von drei Faktoren einfach durch $a \cdot b \cdot c$ angeben. Diese Aussage läßt sich auf endlich viele Faktoren ausdehnen:

Folgerung **F(1.2)**

Das Produkt einer beliebigen endlichen Anzahl von Gruppenelementen ist eindeutig durch die Angabe seiner Faktoren und deren Reihenfolge bestimmt:

$$a = a_1 \cdot a_2 \cdot \ldots \cdot a_n = \prod_{\nu=1}^{n} a_\nu .$$

Beweis

Dazu zeigt man, daß das Ergebnis bei beliebiger Zusammenfassung der Faktoren dem Ergebnis bei einer bestimmten Zusammenfassung gleich ist. Wir wenden vollständige Induktion nach der

1) Nach dem bereits in der Einleitung erwähnten Mathematiker N. H. ABEL.

Anzahl n der Faktoren an. Den Induktionsanfang gibt uns $M\,II$ mit $n = 3$.

Als Induktionsvoraussetzung nehmen wir an, die Behauptung sei für Produkte mit weniger als n Faktoren bereits bewiesen, so daß man in solchen auf die Beklammerung verzichten kann. Daher braucht man bei einem Produkt von n Faktoren nur noch die folgenden Beklammerungen zu unterscheiden:

$$\begin{aligned}
&(a_1) \cdot (a_2 \cdot a_3 \cdot \ldots \cdot a_{n-1} \cdot a_n),\\
&(a_1 \cdot a_2) \cdot (a_3 \cdot \ldots \cdot a_{n-1} \cdot a_n),\\
&\quad\vdots \qquad\qquad\qquad\quad \vdots\\
&(a_1 \cdot a_2 \cdot a_3 \cdot \ldots \cdot a_{n-1}) \cdot (a_n).
\end{aligned}$$

Wir zeigen, daß diese sämtlichen Ausdrücke mit dem ersten übereinstimmen. Ein beliebiger von ihnen sei:

$$(a_1 \cdot a_2 \cdot \ldots \cdot a_m) \cdot (a_{m+1} \cdot \ldots \cdot a_n).$$

Da nach Induktionsvoraussetzung ein Produkt von weniger als n Faktoren mit beliebiger Beklammerung berechnet werden kann, erhalten wir dafür:

$$(a_1 \cdot (a_2 \cdot \ldots \cdot a_m)) \cdot (a_{m+1} \cdot \ldots \quad a_n).$$

Unter Berücksichtigung von $M\,II$ ergibt sich:

$$(a_1) \cdot ((a_2 \cdot \ldots \cdot a_m) \cdot (a_{m+1} \cdot \ldots \cdot a_n)).$$

Erneute Anwendung der Induktionsvoraussetzung zeigt die Übereinstimmung mit:

$$(a_1) \cdot (a_2 \cdot \ldots \cdot a_n).$$

Wie man also auch die n Faktoren beim Ausrechnen zusammenfaßt, stets erhält man dasselbe Ergebnis. Wir können also wieder das Produkt ohne Beklammerung eindeutig angeben:

$$a_1 \cdot a_2 \cdot \ldots \cdot a_n.$$

qed.[1])

1) Das Ende eines Beweises kennzeichnen wir durch qed. als Abkürzung für quod erat demonstrandum (was zu zeigen war.)

Das Kommutativgesetz *M IV* sagt aus: In einer abelschen Gruppe ist ein Produkt aus zwei Faktoren eindeutig durch Angabe seiner Faktoren unabhängig von deren Reihenfolge bestimmt. Unter Verwendung von F (1.2) läßt sich diese Aussage auf beliebig viele Faktoren übertragen:

Folgerung **F (1.3)**

In einer abelschen Gruppe ist das Produkt einer beliebigen endlichen Anzahl von Gruppenelementen bereits durch die Angabe der Faktoren vollständig bestimmt.

Beweis

Nach F (1.2) ist in einer beliebigen Gruppe ein Produkt durch die Angabe seiner Faktoren und deren Reihenfolge bestimmt. Wir haben noch zu zeigen, daß in einer abelschen Gruppe auch die Angabe der Reihenfolge entfallen kann, d. h., es gilt:

$$a_1 \cdot a_2 \cdot \ldots \cdot a_n = a_{i_1} \cdot a_{i_2} \cdot \ldots \cdot a_{i_n},$$

wobei $i_1, i_2, \ldots, i_n$ eine beliebige Anordnung der Indizes $1, 2, \ldots, n$ bedeutet. Da jede Umordnung der Faktoren zurückzuführen ist auf eine Reihe von Vertauschungen zweier benachbarter Faktoren, genügt es nachzuweisen:

$$a_1 \ldots a_i a_{i+1} \ldots a_n = a_1 \ldots a_{i+1} a_i \ldots a_n.$$

Wegen F (1.2) folgt das aber aus *M IV* nach:

$$(a_1 \ldots a_{i-1})\ (a_i a_{i+1})\ (a_{i+2} \ldots a_n) = (a_1 \ldots a_{i-1})\ (a_{i+1} a_i)\ (a_{i+2} \ldots a_n)$$

qed.

Die Möglichkeit der beiderseitigen Division *M III* gestattet den Nachweis der Existenz gewisser besonders wichtiger Elemente in jeder Gruppe:

Satz **S (1.4)**

In jeder Gruppe $\mathfrak{G}$ *existiert ein eindeutig bestimmtes Einselement e mit der Eigenschaft:*

$$ea = ae = a \quad \textit{für alle } a \in \mathfrak{G}.$$

Man überzeuge sich von der Existenz eines Einselementes in den bereits erwähnten multiplikativen Gruppen. Die Notwendigkeit der in den Beweis eingehenden Überlegungen unterstreichen die in B(2.4d) angegebenen Gegenbeispiele.

Beweis

1. Wir zeigen zunächst die Existenz von mindestens einem *Linkseinselement* e_L in $\mathfrak{G}$ mit der Eigenschaft $e_L \cdot a = a$ für alle $a \in \mathfrak{G}$.

Wegen *M III* ist für ein festes $c \in \mathfrak{G}$ insbesondere die Gleichung

$$y \cdot c = c$$

mit $y \in \mathfrak{G}$ lösbar. Dieses Element y hat also bezüglich des festgewählten $c \in \mathfrak{G}$ bei der Multiplikation von links die gewünschte reproduzierende Eigenschaft. Ist nun a ein beliebiges Element aus $\mathfrak{G}$, kann man ebenfalls wegen *M III* die Gleichung

$$c \cdot x = a$$

mit $x \in \mathfrak{G}$ lösen, und es folgt unter Verwendung von *M II*:

$$ya = y(cx) = (yc)x = cx = a.$$

Somit reproduziert y bei der Multiplikation von links alle Elemente aus $\mathfrak{G}$. Also ist $y = e_L$ ein Element mit der verlangten Eigenschaft.

2. Analog folgt die Existenz von mindestens einem *Rechtseinselement* e_R in $\mathfrak{G}$ mit der Eigenschaft $a \cdot e_R = a$ für alle $a \in \mathfrak{G}$.

3. Jedes Linkseinselement $e_L \in \mathfrak{G}$ stimmt mit jedem Rechtseinselement $e_R \in \mathfrak{G}$ überein. Es gilt nämlich:

$$e_L e_R = e_R$$

$$e_L e_R = e_L,$$

wenn wir bei der ersten Gleichung die von links reproduzierende Eigenschaft von e_L, bei der zweiten Gleichung die von rechts reproduzierende Eigenschaft von e_R verwenden. Wegen *M I* ist $e_L = e_R$.

Das in 1. ermittelte Element stimmt daher mit dem in 2. ermittelten überein. Wir bezeichnen es mit e. Außer e gibt es in $\mathfrak{G}$ wegen 3. kein weiteres Links- oder Rechtseinselement.

qed.

Satz **S (1.5)**

In jeder Gruppe $\mathfrak{G}$ existiert zu jedem $a \in \mathfrak{G}$ ein eindeutig bestimmtes Inverses a^{-1} mit der Eigenschaft

$$a^{-1}a = aa^{-1} = e.$$

Beweis

1. Wir zeigen zunächst, daß in $\mathfrak{G}$ zu jedem $a \in \mathfrak{G}$ ein *Linksinverses* a_L^{-1} mit der Eigenschaft $a_L^{-1}a = e$ existiert. Ein solches findet man nämlich nach *M III* als Lösung der speziellen Gleichung

$$ya = e.$$

2. Analog ergibt sich, daß in $\mathfrak{G}$ zu jedem $a \in \mathfrak{G}$ ein *Rechtsinverses* a_R^{-1} mit der Eigenschaft $aa_R^{-1} = e$ existiert.

3. Jedes Linksinverse $a_L^{-1} \in \mathfrak{G}$ zu einem festen $a \in \mathfrak{G}$ stimmt mit jedem Rechtsinversen $a_R^{-1} \in \mathfrak{G}$ zu diesem $a \in \mathfrak{G}$ überein. Es gilt nämlich nach S (1.4) und *M II*

$$a_R^{-1} = ea_R^{-1} = \left(a_L^{-1}a\right)a_R^{-1} = a_L^{-1}\left(aa_R^{-1}\right) = a_L^{-1}e = a_L^{-1}.$$

Das in 1. ermittelte Element stimmt daher mit dem in 2. ermittelten überein und wird mit a^{-1} bezeichnet. Außer a^{-1} gibt es in $\mathfrak{G}$ wegen 3. kein weiteres Links- oder Rechtsinverses zu a

qed.

Die bereits genannten multiplikativen Gruppen liefern Beispiele für diesen Satz und die nachstehenden Folgerungen.

Folgerung **F (1.6)**

Es ist stets $(a^{-1})^{-1} = a$ und $(ab)^{-1} = b^{-1}a^{-1}$;

denn das ergibt sich wegen der Eindeutigkeit des Inversen zu jedem Element aus den Gleichungen

$$a^{-1}a = e \quad \text{und} \quad (ab)\,(b^{-1}a^{-1}) = e.$$

Folgerung **F (1.7)**

Die Lösungen $x \in \mathfrak{G}$ *bzw.* $y \in \mathfrak{G}$ *der Gleichungen* $ax = b$ *und* $ya = b$ *mit* $a \in \mathfrak{G}$ *und* $b \in \mathfrak{G}$ *lassen sich in der Gestalt angeben:*

$$x = a^{-1}b \quad bzw. \quad y = ba^{-1}.$$

Man überzeugt sich davon sofort durch Einsetzen in die Gleichungen (Probe). Darüber hinaus können wir über diese Lösungen folgende Eindeutigkeitsaussagen machen:

Satz **S (1.8)**

Die Lösungen $x \in \mathfrak{G}$ *bzw.* $y \in \mathfrak{G}$ *der Gleichungen* $ax = b$ *bzw.* $ya = b$ *mit* $a \in \mathfrak{G}$ *und* $b \in \mathfrak{G}$ *sind eindeutig bestimmt (Eindeutigkeit der beiderseitigen Division).*

Beweis

Aus $ax_1 = b$ und $ax_2 = b$ und der sich daraus ergebenden Gleichung

$$ax_1 = ax_2$$

folgt durch Multiplikation mit a^{-1} von links wie behauptet:

$$x_1 = x_2.$$

Entsprechend beweist man die Aussage für $ya = b$.

qed.

Die Eindeutigkeit der Division kann auch für eine Rechenoperation gelten, die nicht den Gruppenaxiomen genügt (etwa die Multiplikation der natürlichen Zahlen). Dies muß aber nicht der Fall sein, wie ein in B(2.4d) angegebenes Gegenbeispiel lehrt.

Wir haben bisher eine Gruppe mit Hilfe der drei Axiome *M I*, *M II* und *M III* gekennzeichnet. Es ist interessant und für den Nachweis der Gruppeneigenschaft einer Menge mit einer Verknüpfung oft sehr nützlich, daß man dieses Axiomensystem abändern kann. So ersieht man aus F(1.7) die Möglichkeit, das Axiom *M III* durch die Forderung der Existenz des Einselementes und des Inversen zu jedem Gruppenelement zu ersetzen. Wir können dies aber noch wesentlich verschärfen, indem wir nur die

Existenz eines Linkseinselementes und der zu ihm gehörigen Linksinversen zu jedem Gruppenelement fordern:

Satz **S (1.9)**

Das Axiomensystem D(1.1) *für Gruppen kann dahingehend abgeändert werden, daß man unter Beibehaltung der übrigen Axiome statt M III die folgenden Axiome M III$_1$ und M III$_2$ gleichzeitig fordert:*

M III$_1$: Es existiert wenigstens ein Linkseinselement $e \in \mathfrak{G}$ mit $ea = a$ für alle $a \in \mathfrak{G}$.

M III$_2$: Es existiert zu jedem $a \in \mathfrak{G}$ bezüglich dem in M III$_1$ genannten Linkseinselement e wenigstens ein Linksinverses $a^{-1} \in \mathfrak{G}$ mit $a^{-1}a = e$.

Das Axiomensystem *M I, M II, M III* ist aus strukturellen Gesichtspunkten vorzuziehen, da in ihm keine besonderen Eigenschaften einzelner Elemente eingehen. Dagegen macht es unsere Beispielsammlung deutlich, daß für den Nachweis der Gruppeneigenschaft das Axiomensystem *M I, M II, M III$_1$, M III$_2$* meist handlicher ist.

Beweis

Axiomensysteme sind genau dann gleichwertig, wenn sie wechselseitig auseinander abgeleitet werden können. Aus dem System *M I, M II, M III* folgt das System *M I, M II, M III$_1$, M III$_2$*, da wir in S(1.4) und S(1.5) sogar viel mehr aus *M I, M II, M III* geschlossen haben. Es bleibt zu zeigen, daß auch das Umgekehrte gilt. *M I* und *M II* kommen aber im neuen Axiomensystem selbst vor. Wir müssen also noch *M III* ableiten.

1. Das in *M III$_2$* geforderte Element a^{-1} erfüllt neben $a^{-1}a = e$ auch die Gleichung $aa^{-1} = e$. Es folgt nämlich unter Verwendung von *M II* und *M III$_1$*:

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

Nach *M III$_2$* existiert ein Element $(a^{-1})^{-1}$, welches die Gleichung

$$(a^{-1})^{-1} \cdot (a^{-1}) = e$$

erfüllt. Wir multiplizieren damit die vorhergehende Gleichung von links

$$(a^{-1})^{-1}\,[a^{-1}\,(aa^{-1})] = (a^{-1})^{-1}a^{-1}$$

und erhalten nach *M II*:

$$aa^{-1} = e.$$

2. Das in $M\,III_1$ geforderte Element e erfüllt neben $ea = a$ auch $ae = a$ für alle $a \in \mathfrak{G}$:

$$a = ea = (aa^{-1})\,a = a\,(a^{-1}a) = ae.$$

3. Damit löst das Element $x = a^{-1}b$ die Gleichung $ax = b$ und das Element $y = ba^{-1}$ die Gleichung $ya = b$, wie man durch Einsetzen nachweist:

$$ax = a\,(a^{-1}b) = (aa^{-1})\,b = eb = b$$
$$ya = (ba^{-1})\,a = b\,(a^{-1}a) = be = b.$$

Man beachte, daß bei diesen Rechnungen wesentlich die in 1. und 2. durchgeführten Überlegungen eingehen. qed.

Wir merken noch an, daß aus dem neuen Axiomensystem selbstverständlich mit $M\,III$ auch alle aus dem alten Axiomensystem abgeleiteten Aussagen folgen. Insbesondere gilt dies für die in den Sätzen S(1.4), S(1.5), S(1.8) enthaltenen Eindeutigkeitsaussagen. Ferner weisen wir auf eine zweite Abänderungsmöglichkeit des Axiomensystems für Gruppen hin, die entsteht, wenn man in $M\,III_1$ und $M\,III_2$ von S(1.9) anstatt der dort formulierten linksseitigen die entsprechenden rechtsseitigen Eigenschaften fordert.

Über das in S(1.9) Ausgesprochene hinaus wollen wir für *endliche* Gruppen noch ein weiteres Axiomensystem angeben. Es folgt dann nämlich aus der Eindeutigkeit der Division bereits die Möglichkeit der Division, d. h. aus der Aussage „Jede Gleichung $ax = b$ bzw. $ya = b$ hat *höchstens* eine Lösung" die Aussage „Jede Gleichung $ax = b$ bzw. $ya = b$ hat *mindestens* eine Lösung":

Satz **S (1.10)**

In dem Axiomensystem D(1.1) *kann für endliche Gruppen unter Beibehaltung der übrigen Axiome das Axiom M III durch das folgende Axiom M III* ersetzt werden:*

M III: Sind* $x_1 \in \mathfrak{G}$ *und* $x_2 \in \mathfrak{G}$ *Lösungen der Gleichung* $ax = b$ *mit* $a \in \mathfrak{G}$ *und* $b \in \mathfrak{G}$, *so folgt* $x_1 = x_2$.

Entsprechend:

Sind $y_1 \in \mathfrak{G}$ *und* $y_2 \in \mathfrak{G}$ *Lösungen der Gleichung* $ya = b$ *mit* $a \in \mathfrak{G}$ *und* $b \in \mathfrak{G}$, *so folgt* $y_1 = y_2$.

Von der Möglichkeit dieser Abänderung des Axiomensystems machen wir in B(2.8e) Gebrauch.

Beweis

Nach den am Anfang des Beweises von S(1.9) angestellten Überlegungen ist unter Berücksichtigung von S(1.8) nur noch *M III* aus *M I*, *M II*, *M III** abzuleiten.

Die Gruppe $\mathfrak{G}$ habe n Elemente, es sei a ein beliebiges von ihnen. Wir bilden die n Produkte ax, wo x alle Elemente aus $\mathfrak{G}$ durchläuft. Diese Produkte sind alle voneinander verschieden, da aus $ax_1 = ax_2$ wegen *M III** $x_1 = x_2$ folgt. Sie müssen also die ganze Gruppe ausmachen. Das heißt aber, daß jedes $b \in \mathfrak{G}$ in der Gestalt ax mit geeignetem $x \in \mathfrak{G}$ angegeben werden kann. Daher ist für beliebige $a \in \mathfrak{G}$, $b \in \mathfrak{G}$ die Gleichung $ax = b$ mit $x \in \mathfrak{G}$ lösbar. Entsprechend beweist man die Lösbarkeit der Gleichung $ya = b$.

qed.

In den bisherigen Betrachtungen haben wir uns einen ersten Überblick über den Gruppenbegriff verschafft. Ihr wesentlicher Inhalt war die Untersuchung einer beliebigen Verknüpfung, die den in D(1.1) genannten Forderungen genügt. Wir betonen, daß die dabei verwendete multiplikative Schreibweise keinerlei inhaltliche Bedeutung hat, sondern nur den axiomatisch festgelegten Eigenschaften der Verknüpfung Ausdruck verleiht. Prinzipiell kann jede andere Schreibweise gewählt werden, die das gleiche zu leisten vermag. Das ist der Fall, wenn wir die Verknüpfung als Addition schreiben. Allerdings pflegt man diese additive Schreibweise nur bei abelschen Gruppen, dort aber sehr häufig, zu verwenden[1]).

Wir wollen daher die gesamte bisher abgeleitete Theorie für additiv geschriebene abelsche Gruppen, die man auch Moduln nennt, übertragen. Bei dieser Übertragung ist zweierlei zu beachten. Erstens werden nämlich durch die Forderung der Kommutativität alle Aussagen vereinfacht, in denen die Reihenfolge der Gruppenelemente bei der Verknüpfung ursprünglich eine Rolle spielte. Dies hat mit der Schreibweise der Verknüpfung zunächst nichts zu tun und kann auch für multiplikativ geschriebene abelsche Gruppen durchgeführt werden. Zweitens ersetzt man die Multiplikation durch die Addition und damit alle multiplikativen Ausdrücke wie Faktor, Produkt usw. durch die entsprechenden additiven Bezeichnungen wie Summand, Summe usw.

1) Vgl. aber Anhang IIa.

Schließlich ist zu bemerken, daß es bei dieser „Übertragung" prinzipiell überflüssig ist, Beweise erneut zu führen, da diese von der gewählten Schreibweise der Verknüpfung unabhängig sind. Man kann natürlich alles für additiv geschriebene abelsche Gruppen neu entwickeln, ohne sich auf das Vorangegangene zu beziehen. Es ist aber gerade ein Kennzeichen der modernen Mathematik, gleiche, in verschiedenen konkreten Gestalten auftretende Beweisgänge nicht immer wieder, sondern in abstrakter Herauslösung ein für allemal durchzuführen.

Definition **D (1.11)**

Eine nichtleere Menge von Elementen $a, b, c, \ldots$ heißt eine additive abelsche Gruppe oder ein Modul $\mathfrak{G}$, wenn in ihr eine als Addition geschriebene Verknüpfung erklärt ist, die folgenden Axiomen genügt:

A I: *Die Addition ordnet je zwei Elementen $a \in \mathfrak{G}$ und $b \in \mathfrak{G}$ ein Element $c \in \mathfrak{G}$ eindeutig zu:*

$$a + b = c.$$

A II: *Die Addition ist assoziativ:*

$$(a + b) + c = a + (b + c).$$

A III: *Die Addition ist in $\mathfrak{G}$ in dem Sinne umkehrbar, daß zu beliebigen $a \in \mathfrak{G}$ und $b \in \mathfrak{G}$ die Gleichung*

$$a + x = b$$

mit $x \in \mathfrak{G}$ lösbar ist. Zu vorgegebenem Resultat der Addition und einem vorgegebenen Summanden gibt es also in $\mathfrak{G}$ einen zur Summe ergänzenden anderen Summanden (Möglichkeit der Subtraktion).

A IV: *Die Addition ist kommutativ:*

$$a + b = b + a.$$

Wie bei D (1.1) unterscheidet man endliche und unendliche Moduln.

Folgerung **F (1.12)**

In einem Modul ist die Summe einer beliebigen endlichen Anzahl von Elementen durch die Angabe der Summanden bestimmt:

$$a = a_1 + a_2 + \cdots + a_n = \sum_{\nu=1}^{n} a_\nu.$$

Satz **S (1.13)**

In jedem Modul $\mathfrak{G}$ *existiert ein eindeutig bestimmtes Nullelement* o *mit der Eigenschaft:*

$$a + o = a \quad \textit{für alle } a \in \mathfrak{G}.$$

Satz **S (1.14)**

In jedem Modul $\mathfrak{G}$ *existiert zu jedem* $a \in \mathfrak{G}$ *ein eindeutig bestimmtes entgegengesetztes Element* $(-a)$ *mit der Eigenschaft*

$$a + (-a) = o.$$

Folgerung **F (1.15)**

Es ist stets $-(-a) = a$ *und* $-(a + b) = (-a) + (-b)$.

Folgerung **F (1.16)**

Die Lösung $x \in \mathfrak{G}$ *der Gleichung* $a + x = b$ *mit* $a \in \mathfrak{G}$ *und* $b \in \mathfrak{G}$ *läßt sich in der Gestalt*

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

angeben, wofür man auch kürzer $x = b - a$ *schreibt.*

Satz **S (1.17)**

Die Lösung $x \in \mathfrak{G}$ *der Gleichung* $a + x = b$ *mit* $a \in \mathfrak{G}$ *und* $b \in \mathfrak{G}$ *ist eindeutig bestimmt (Eindeutigkeit der Subtraktion).*

Satz **S (1.18)**

Das Axiomensystem D (1.11) *für Moduln kann dahingehend abgeändert werden, daß man unter Beibehaltung der übrigen Axiome statt A III die folgenden Axiome* $A\,III_1$ *und* $A\,III_2$ *gleichzeitig fordert:*

$A\,III_1$: *Es existiert wenigstens ein Nullelement* $o \in \mathfrak{G}$ *mit* $a + o = a$ *für alle* $a \in \mathfrak{G}$.

$A\,III_2$: *Es existiert zu jedem* $a \in \mathfrak{G}$ *bezüglich dem in* $A\,III_1$ *genannten Nullelement* o *wenigstens ein entgegengesetztes Element* $(-a) \in \mathfrak{G}$ *mit* $a + (-a) = o$.

Satz **S (1.19)**

In dem Axiomensystem D(1.11) *kann für endliche Moduln unter Beibehaltung der übrigen Axiome das Axiom A III durch das folgende Axiom A III* ersetzt werden:*

A III: Sind* $x_1 \in \mathfrak{G}$ *und* $x_2 \in \mathfrak{G}$ *Lösungen der Gleichung* $a+x=b$ *mit* $a \in \mathfrak{G}$ *und* $b \in \mathfrak{G}$, *so folgt* $x_1 = x_2$.

Aufgaben zu § 1

1. Man führe den zweiten Schritt des Beweises von S(1.4) durch.
2. Man führe den zweiten Schritt des Beweises von S(1.5) durch.
3. Man verallgemeinere die Aussage $(ab)^{-1} = b^{-1}a^{-1}$ durch vollständige Induktion für eine beliebige endliche Anzahl von Faktoren.
4. Man beweise *M III** allein aus *M I*, *M II*, *M III* ohne Verwendung von S(1.4) und S(1.5).
5. Man überlege sich, wieso die in S(1.4) und S(1.5) enthaltenen Eindeutigkeitsaussagen erneut aus S(1.8) folgen.
6. Man beweise die nach S(1.9) stehende Bemerkung über die Abänderungsmöglichkeit des Axiomensystems für Gruppen.
7. Man überzeuge sich am Beispiel der natürlichen Zahlen mit der gewöhnlichen Multiplikation als Verknüpfung, daß auf die Voraussetzung „endliche Gruppe" in S(1.10) nicht verzichtet werden kann.
8. Man vergleiche alle Aussagen in Moduln mit den jeweils entsprechenden in multiplikativen Gruppen.
9. Man führe alle Beweise von F(1.12) ff unter Ausnutzung der Kommutativität in additiver Schreibweise erneut durch.

§ 2. Beispiele von Gruppen

Über die bereits in der Einleitung zu diesem Kapitel angegebene Zielstellung hinaus dient die folgende Beispielsammlung zur Festigung und Veranschaulichung der bisher entwickelten Begriffsbildungen. Zugleich benutzen wir die Gelegenheit, einige Tatsachen aus der Kombinatorik und der elementaren Zahlentheorie zusammenzustellen, die für den Aufbau der Gruppentheorie als Hilfsmittel Verwendung finden. Dagegen nehmen wir hier die Gültigkeit der üblichen Rechenregeln für (komplexe) Zahlen als gegeben an (vgl. auch Aufg. 1).

Zahlen **B (2.1)**

Wir betrachten Zahlenbereiche innerhalb der Menge der komplexen Zahlen mit der gewöhnlichen Addition bzw. Multiplikation als Verknüpfungsvorschrift.

a) Die Menge der natürlichen Zahlen bildet weder hinsichtlich der Addition noch hinsichtlich der Multiplikation eine Gruppe.

b) *Die Menge der ganzen Zahlen ist bezüglich der Addition eine unendliche abelsche Gruppe, also ein unendlicher Modul.* Das Nullelement und das zu einem Element entgegengesetzte Element decken sich mit den in der Arithmetik üblichen Begriffen. Mit der Multiplikation als Verknüpfung bilden die ganzen Zahlen dagegen keine Gruppe.

c) *Die Menge der rationalen, der reellen sowie der komplexen Zahlen bilden jeweils sowohl hinsichtlich der Addition als auch, allerdings unter Ausschluß der Null, hinsichtlich der Multiplikation unendliche abelsche Gruppen.* Für Nullelement, entgegengesetztes Element bzw. Einselement, inverses Element gilt das unter b) Gesagte analog.

Einheitswurzeln **B (2.2)**

Bekanntlich hat die Gleichung

$$x^n - 1 = 0$$

genau n verschiedene Wurzeln, die man als komplexe Zahlen wie folgt angeben kann:

$$\varepsilon_k = \cos\frac{2k\pi}{n} + i \cdot \sin\frac{2k\pi}{n} = e^{\frac{2k\pi i}{n}};$$

$$(k = 0, 1, \ldots, n-1).$$

Sie heißen n-te Einheitswurzeln und entsprechen den Eckpunkten eines dem Einheitskreis der komplexen Zahlenebene einbeschriebenen regelmäßigen n-Ecks (vgl. Abb. 1 für $n = 6$).

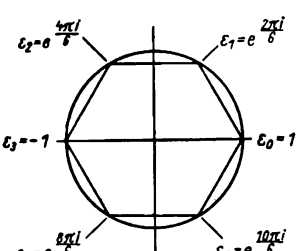


Abb. 1

a) *Die n-ten Einheitswurzeln bilden mit der für komplexe Zahlen erklärten Multiplikation eine abelsche Gruppe der Ordnung n.* Man sieht nämlich mit Hilfe des MOIVREschen Lehrsatzes sofort, daß Produkt und Quotient zweier n-ter Einheitswurzeln wieder eine solche sind. Die Eindeutigkeit, Assoziativität und Kommutativität der Multiplikation gilt für alle komplexen Zahlen und damit auch für die hier betrachteten Einheitswurzeln.

b) Die Gruppe der n-ten Einheitswurzeln hat die besondere Eigenschaft, daß alle ihre Elemente bereits als Potenzen einer geeigneten n-ten Einheitswurzel geschrieben werden können. Nach dem MOIVREschen Lehrsatz leistet das z. B.

$$\varepsilon_1 = \cos\frac{2\pi}{n} + i \cdot \sin\frac{2\pi}{n} = e^{\frac{2\pi i}{n}}$$

wegen

$$\varepsilon_1^1 = \varepsilon_1, \quad \varepsilon_1^2 = \varepsilon_2, \quad \varepsilon_1^3 = \varepsilon_3, \qquad \varepsilon_1^{n-1} = \varepsilon_{n-1}, \quad \varepsilon_1^n = \varepsilon_0.$$

Jede n-te Einheitswurzel, die auf diese Weise mit ihren Potenzen alle n-ten Einheitswurzeln liefert, heißt *primitive n-te Einheitswurzel.*

Vektoren **B (2.3)**

Wir schreiben die aus der analytischen Geometrie bekannten Vektoren des dreidimensionalen Raumes mit Hilfe orthogonaler Einheitsvektoren $\mathfrak{e}_1, \mathfrak{e}_2, \mathfrak{e}_3$ in der Form

$$\mathfrak{x} = x_1\mathfrak{e}_1 + x_2\mathfrak{e}_2 + x_3\mathfrak{e}_3,$$

wobei die Koordinaten x_1, x_2, x_3 von $\mathfrak{x}$ (unabhängig voneinander) beliebige reelle Werte annehmen.

a) *Die Menge aller Vektoren des dreidimensionalen Raumes bildet bezüglich der Vektoraddition einen Modul.* Die den Modulaxiomen entsprechenden Gesetzmäßigkeiten werden nämlich bereits in der elementaren Vektorrechnung nachgewiesen. Insbesondere ist das Nullelement der Vektor von der Länge 0, d. h. der Vektor

$$\mathfrak{o} = 0\mathfrak{e}_1 + 0\mathfrak{e}_2 + 0\mathfrak{e}_3,$$

und der zu $\mathfrak{x}$ entgegengesetzte Vektor $(-\mathfrak{x})$ der Vektor gleicher Länge und entgegengesetzter Richtung, d. h.

$$(-\mathfrak{x}) = (-x_1)\,\mathfrak{e}_1 + (-x_2)\,\mathfrak{e}_2 + (-x_3)\,\mathfrak{e}_3.$$

b) Entsprechendes gilt für alle Vektoren in einer Ebene bzw. auf einer Geraden wie überhaupt allgemein für alle Vektoren eines n-dimensionalen Raumes.

c) Dagegen bilden Vektoren sowohl hinsichtlich der skalaren als auch hinsichtlich der vektoriellen Produktbildung keine Gruppen (vgl. Aufg. 3).

Matrizen **B (2.4)**

Unter einer Matrix vom Typ (m, n) versteht man ein rechteckiges Zahlenschema

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

von m Zeilen und n Spalten. Die $m \cdot n$ Matrixelemente a_{ik} seien dabei im folgenden etwa als reelle Zahlen festgelegt.

a) Matrizen vom gleichen Typ können nach der Vorschrift

$$(a_{ik}) + (b_{ik}) = (a_{ik} + b_{ik})$$

addiert werden. Für die Erklärung der Multiplikation ist erforderlich, daß die Matrizen (a_{ik}) und (b_{ik}) verkettet sind, d. h., es muß die Spaltenanzahl von (a_{ik}) mit der Zeilenzahl von (b_{ik}) übereinstimmen. Die Vorschrift für die Multiplikation lautet:

$$(a_{ik}) \cdot (b_{ik}) = (\sum_h a_{ih} \cdot b_{hk}) .$$

b) *Die Menge aller Matrizen vom gleichen Typ (m, n) bilden bezüglich der Matrizenaddition einen Modul.*

Beweis

A I: Die Addition ist nach Definition eindeutig und ergibt stets eine Matrix vom gleichen Typ.

A II: Die Forderung des Assoziativgesetzes für die Matrizen reduziert sich vermöge der Definition der Addition für Matrizen auf die Forderung des Assoziativgesetzes für die Addition der Matrizenelemente, die erfüllt ist.

A III$_1$: Das Nullelement ist die Nullmatrix (a_{ik}) mit $a_{ik} = 0$ für alle i und k.

A III$_2$: Die zu (a_{ik}) entgegengesetzte Matrix $-(a_{ik})$ ist $(-a_{ik})$.

A IV: Hier gilt das Analoge wie bei *A II*. qed.

c) *Die Menge aller quadratischen Matrizen* (a_{ik}) *vom gleichen Typ* (n, n) *mit nichtverschwindender Determinante* $|(a_{ik})|$ *bildet eine multiplikative Gruppe, die sog. volle lineare Gruppe vom Grad n. Sie ist nicht kommutativ; ihre Elemente werden auch reguläre Matrizen genannt.*

Beweis

M I: Die Multiplikation ist nach Definition eindeutig und ergibt wieder eine quadratische Matrix von gleichem Typ. Ferner gewährleistet der Multiplikationssatz für Determinanten

$$|(a_{ik})| \cdot |(b_{ik})| = |(\sum_h a_{ih} \cdot b_{hk})|,$$

daß auch die Determinante der Produktmatrix nicht verschwindet.

M II: Die Produkte

$$[(a_{ik}) \cdot (b_{ik})] \cdot (c_{ik}) \quad \text{bzw.} \quad (a_{ik}) \cdot [(b_{ik}) \cdot (c_{ik})]$$

besitzen an jeder beliebigen Stelle i, k die Elemente:

$$\sum_j (\sum_h a_{ih} b_{hj}) c_{jk} \quad \text{bzw.} \quad \sum_h a_{ih} (\sum_j b_{hj} c_{jk}).$$

Diese sind nach den für reelle Zahlen geltenden Gesetzen gleich. Also gilt das Assoziativgesetz für die Multiplikation der Matrizen.

M III$_1$: Das Einselement ist die Einheitsmatrix $E = (\delta_{ik})$ mit[1])

$$\delta_{ik} = \begin{cases} 1 & \text{für} \quad i = k \\ 0 & \text{für} \quad i \neq k. \end{cases}$$

M III$_2$: Die zu (a_{ik}) inverse Matrix $(a_{ik})^{-1}$ ist die Matrix (b_{ik}) mit

$$b_{ik} = \frac{1}{|(a_{ik})|} \cdot A_{ki},$$

wo A_{ik} das Produkt aus $(-1)^{i+k}$ und dem Minor der Determinante $|(a_{ik})|$ ist, der durch Streichen der i-ten Zeile und der k-ten Spalte entsteht.

Für das Nichterfülltsein von *M IV* vergleiche Aufgabe 4. qed.

1) Man bezeichnet δ_{ik} auch als KRONECKER-Symbol.

d) Es ist bemerkenswert, daß die Moduleigenschaft bezüglich der Matrizenaddition für beliebige Matrizen vom gleichen Typ erfüllt ist, während die Gruppeneigenschaft bezüglich der Matrizenmultiplikation nicht so allgemein abgeleitet werden kann. Dies liegt daran, daß einmal eine Matrix als Gruppenelement mit sich selbst verkettet, also quadratisch sein muß. Zum andern lehrt die Matrizenrechnung, daß für die Invertierbarkeit einer quadratischen Matrix das Nichtverschwinden ihrer Determinante notwendig und hinreichend ist. Diese Forderung geht auch nur in den Beweis von $M\,III_2$ wesentlich ein.

Dies ist insofern lehrreich, als z. B. die Menge aller quadratischen Matrizen vom Typ (2,2) hinsichtlich der Multiplikation den Axiomen $M\,I$, $M\,II$, $M\,III_1$ genügt. Sie gleicht darin der Menge der natürlichen Zahlen und besitzt trotzdem hinsichtlich der Multiplikation Eigenschaften, die wir von der Zahlenrechnung her nicht kennen. Wir erläutern dies an einigen Beispielen. Sie zeigen, daß man bei den Beweisen in § 1 keine Vereinfachungen in Analogie zur Zahlenrechnung erwarten kann.

So ist z. B. möglich, daß

$$A X_1 = A X_2 \quad \text{mit} \quad X_1 \neq X_2$$

gilt im Gegensatz zu der in Gruppen erfüllten Aussage S(1.8). Man wähle nämlich etwa:

$$A = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, \quad X_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad X_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Weiterhin kann ein Element Y die Gleichung $YC = C$ für festes C erfüllen, ohne daß $YA = A$ für beliebiges A gilt (vgl. Beweis zu S(1.4)). Man wähle nämlich etwa:

$$C = \begin{pmatrix} c & 0 \\ 0 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Wir können sogar mit Hilfe dieser Matrizen eine Menge bilden, in der die Matrizenmultiplikation den Axiomen $M\,I$, $M\,II$ und $M\,III_1$ genügt, in der es aber nicht nur (wie $M\,III_1$ verlangt) ein, sondern sogar unendlich viele Linkseinselemente, dagegen kein Rechtseinselement gibt (vgl. Beweise zu S(1.4) und S(1.9)).

Dazu nehmen wir alle Matrizen, in denen die Elemente der zweiten Zeile $a_{21} = a_{22} = 0$ sind, die also die Gestalt

$$\begin{pmatrix} a_{11} & a_{12} \\ 0 & 0 \end{pmatrix}$$

haben. Das Produkt solcher Matrizen ist nämlich wieder eine Matrix dieser Gestalt, die Eindeutigkeit und Assoziativität der Multiplikation ist bei allen quadratischen Matrizen erfüllt. Dann sind aber in dieser Menge alle Matrizen der Form

$$\begin{pmatrix} 1 & x \\ 0 & 0 \end{pmatrix}$$

mit beliebigem x Linkseinselemente, denn es gilt offensichtlich

$$\begin{pmatrix} 1 & x \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a_{11} & a_{12} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ 0 & 0 \end{pmatrix}.$$

Es gibt dagegen kein Rechtseinselement in dieser Menge, denn das aus

$$\begin{pmatrix} a_{11} & a_{12} \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_{11}x & a_{11}y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ 0 & 0 \end{pmatrix}$$

entstehende Gleichungssystem

$$a_{11}x = a_{11}$$
$$a_{11}y = a_{12}$$

müßte bei festen x und y für alle möglichen Werte von a_{11} und a_{12} erfüllt sein.

Permutationen **B (2.5)**

Unter einer Permutation vom Grad n versteht man eine eineindeutige Abbildung einer endlichen Menge von n Elementen auf sich selbst. Der Einfachheit halber bezeichnen wir die Elemente dieser Menge mit den Zahlen $1, 2, \ldots, n$. Wir erhalten also eine Zuordnung der Art

$$1 \to i_1,\ 2 \to i_2,\ \ldots,\ n \to i_n,$$

wobei die $i_1, i_2, \ldots, i_n$ wieder genau die Zahlen $1, 2, \ldots, n$ sind, nur im allgemeinen in einer anderen Reihenfolge. In übersichtlicher Weise schreibt man eine solche Permutation

$$s = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}.$$

Zum Beispiel sind alle Permutationen der Zahlen 1, 2, 3:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Da es bei einer Permutation nur auf die Zuordnung ankommt, d. h. darauf, daß in der eben eingeführten Schreibweise unter jeder Zahl die ihr zugeordnete steht, ist diese Schreibweise von der Anordnung der Spalten unabhängig. So ist z. B. durch

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 2 & 1 \\ 2 & 1 & 3 \end{pmatrix}$$

stets dieselbe Permutation gekennzeichnet.

a) Als eineindeutige Abbildungen, bei denen Original- und Bildmenge übereinstimmen, lassen sich Permutationen der Zahlen $1, 2, \ldots, n$ nacheinander ausführen. Dabei entsteht jeweils wieder eine solche Abbildung, also eine Permutation der Zahlen $1, 2, \ldots, n$. Werden z. B. die beiden Permutationen

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

in der angegebenen Reihenfolge nacheinander ausgeführt, so geht die Zahl 1 durch die erste Permutation in die Zahl 2 und diese durch die zweite Permutation in die Zahl 3, insgesamt also die Zahl 1 in die Zahl 3 über. Entsprechend wird die 2 über die 1 auf die 2 und die 3 über die 3 auf die 1 abgebildet. Es entsteht als Ergebnis die Permutation

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Sind allgemein die beiden Permutationen

$$s_1 = \begin{pmatrix} 1 & 2 & & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \quad \text{und} \quad s_2 = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix}$$

gegeben, so formen wir zunächst zur besseren Übersichtlichkeit die zweite Permutation durch Spaltenvertauschung um:

$$s_2 = \begin{pmatrix} 1 & 2 & & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix} = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}.$$

Die Nacheinanderausführung von s_1 und s_2 ergibt dann ersichtlich die Permutation

$$\begin{pmatrix} 1 & 2 & & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}.$$

Man bezeichnet diese Nacheinanderausführung als Multiplikation der Permutationen und gebraucht entsprechend die Begriffe Faktor und Produkt:

$$\begin{pmatrix} 1 & 2 & & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \cdot \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ k_1 & k_2 & \dots & k_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}.$$

Es ist dabei aber streng auf die Reihenfolge der Faktoren zu achten, denn diese Produktbildung ist im allgemeinen nicht kommutativ. So ist in dem oben behandelten Beispiel

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

dagegen

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

b) *Die Menge aller Permutationen der Zahlen* $1, 2, \dots, n$ *bildet mit der unter* a) *erklärten Multiplikation als Verknüpfung eine Gruppe der Ordnung* $n!$.

Beweis

Nach den Ausführungen in a) ist nur noch zu zeigen:

M II: Es seien s_1, s_2, s_3 beliebige Permutationen, die durch Spaltenvertauschungen auf die Form

$$s_1 = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}, \quad s_2 = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}, \quad s_3 = \begin{pmatrix} j_1 & j_2 & \dots & j_n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}$$

gebracht werden können. Dann gilt:

$$s_1 \cdot s_2 = \begin{pmatrix} 1 & 2 & & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}, \quad s_2 \cdot s_3 = \begin{pmatrix} i_1 & i_2 & & j_n \\ k_1 & k_2 & \dots & k_n \end{pmatrix},$$

$$(s_1 \cdot s_2) \cdot s_3 = \begin{pmatrix} 1 & 2 & & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix} = s_1 \cdot (s_2 \cdot s_3).$$

M III$_1$: Die identische Permutation

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}$$

hat die Eigenschaften des Einselementes.

M III$_2$: Zu jeder Permutation

$$s = \begin{pmatrix} 1 & 2 & & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$$

existiert eine inverse Permutation

$$s^{-1} = \begin{pmatrix} i_1 & i_2 & & i_n \\ 1 & 2 & & n \end{pmatrix}.$$

Für die Behauptung über die Ordnung vergleiche Aufgabe 5.

qed.

c) Die Gruppe der $n!$ Permutationen der Zahlen $1, 2, \dots, n$ heißt die *symmetrische Gruppe* $\mathfrak{S}_n$. Sie hat ihren Namen von den sog. symmetrischen Funktionen in n Variablen; das sind solche

Funktionen $f(x_1, x_2, \ldots, x_n)$, die bei jeder Permutation der $x_1, x_2, \ldots, x_n$ in sich übergehen. Man sagt auch, die symmetrischen Funktionen gestatten die Anwendung aller Elemente der symmetrischen Gruppe. Zum Beispiel ist

$$f(x_1, x_2, x_3) = x_1x_2 + x_2x_3 + x_3x_1$$

eine symmetrische Funktion in drei Variablen (vgl. Aufg. 7).

d) Permutationen und aus ihnen gebildete Gruppen spielten in der Entwicklung der Gruppentheorie eine große Rolle. Bei ihrer Behandlung wurden bereits gruppentheoretische Betrachtungen durchgeführt, ohne daß der abstrakte Begriff der Gruppe vorlag. Dieser entstand erst viel später aus der Erkenntnis, daß wesentliche Teile der Theorie der Permutationsgruppen von der speziellen Eigenschaft ihrer Elemente, Permutationen zu sein, unabhängig sind. Ein von KRONECKER 1870 aufgestelltes System abstrakter Gruppenaxiome soll das erste dieser Art sein. Allerdings läßt sich jede endliche Gruppe durch eine ihr zugeordnete Permutationsgruppe beschreiben. Darauf gehen wir im Zusammenhang mit einer ausführlichen Behandlung der Permutationen später ein.

Transformationen **B (2.6)**

Die bei Permutationen übliche Beschränkung auf endliche Mengen abgebildeter Objekte hat den Vorteil, daß die Gesamtheit der Zuordnungen jeder Permutation explizit hingeschrieben werden kann. Der Inhalt unserer Überlegungen ist jedoch von dieser Voraussetzung nicht abhängig. Wir verallgemeinern sie daher und erklären:

Unter einer Transformation s versteht man eine eineindeutige Abbildung einer beliebigen Menge $\mathfrak{M}$ auf sich selbst. Wir kennzeichnen die Transformation s durch ihre Wirkung auf alle Elemente $a \in \mathfrak{M}$ und schreiben das a durch s zugeordnete Bild $s(a)$. Transformationen von $\mathfrak{M}$ sind also umkehrbar eindeutige Funktionen, deren Definitionsbereich und Wertevorrat mit $\mathfrak{M}$ zusammenfallen.

a) Als eineindeutige Abbildungen, bei denen Original- und Bildmenge übereinstimmen, lassen sich Transformationen einer Menge

nacheinander ausführen. Dabei entsteht jeweils wieder (genau) eine solche Abbildung, also eine Transformation dieser Menge.

Man bezeichnet diese Nacheinanderausführung als Multiplikation der Transformationen. Es ist also[1])

$$[s_1 \cdot s_2]\,(a) = s_2\,(s_1\,(a)).$$

Wie schon die Permutationen als spezielle Transformationen lehren, ist diese Produktbildung im allgemeinen nicht kommutativ.

b) *Die Menge* $\mathfrak{T}$ *aller Transformationen einer beliebigen Menge* $\mathfrak{M}$ *bildet mit der unter* a) *erklärten Multiplikation als Verknüpfung eine Gruppe.*

Beweis

Unter Berücksichtigung von a) bleibt nur noch zu zeigen:

M II: Es gilt

$$[s_1 \cdot s_2] \cdot s_3 = s_1 \cdot [s_2 \cdot s_3],$$

da beide Produkte auf jedes $a \in \mathfrak{M}$ die gleiche Wirkung haben:

$$[[s_1 \cdot s_2] \cdot s_3]\,(a) = s_3\,([s_1 \cdot s_2]\,(a)) = s_3\,(s_2\,(s_1\,(a))),$$
$$[s_1 \cdot [s_2 \cdot s_3]]\,(a) = [s_2 \cdot s_3]\,(s_1\,(a)) = s_3\,(s_2\,(s_1\,(a))).$$

$M\,III_1$: Durch die Vorschrift

$$e\,(a) = a \quad \text{für alle } a \in \mathfrak{M}$$

wird die identische Transformation e erklärt, die also jedes $a \in \mathfrak{M}$ auf sich selbst abbildet. e ist das Einselement von $\mathfrak{T}$:

$$e \cdot s = s \cdot e = s \quad \text{für alle } s \in \mathfrak{T}.$$

$M\,III_2$: Zu jedem $s \in \mathfrak{T}$ wird durch die Vorschrift

$$s^{-1}\,(s\,(a)) = a \quad \text{für alle } a \in \mathfrak{M}$$

eine zu s inverse Transformation s^{-1} erklärt, die die durch s bewirkte Abbildung rückgängig macht. Es gilt:

$$s \cdot s^{-1} = e.$$

qed.

1) Vgl. aber Anhang IIb.

Wir haben hier ein treffendes Beispiel für die Tatsache, daß in der Mathematik oft Verallgemeinerungen zur Vereinfachung der Begriffe und Beweise führen. Alle in die Beweise von B (2.5 b) eingehenden expliziten Rechnungen hätten wir uns nämlich ersparen können, da die eben angestellten allgemeinen Überlegungen erst recht für Permutationen gelten.

Geometrische Transformationen **B (2.7)**

Wir können die Ergebnisse des vorangehenden Beispiels insbesondere auf geometrische Überlegungen anwenden, wenn wir als Menge $\mathfrak{M}$ alle Punkte des dreidimensionalen Raumes (einschließlich seiner unendlich fernen Ebene) nehmen.

Freilich ist die Gesamtheit aller Transformationen von $\mathfrak{M}$ zu allgemein, um Gegenstand geometrischen Interesses zu sein. Man wird die Menge der zu betrachtenden Transformationen wenigstens dahingehend einschränken, daß man nur stetige Transformationen zuläßt. Darunter versteht man solche eineindeutigen Abbildungen des Raumes auf sich, die benachbarte Punkte wieder in benachbarte Punkte überführen. Diese Abbildungen bilden ebenfalls eine Gruppe und werden topologische Abbildungen genannt. Ihr Studium ist Gegenstand der Topologie.

Die Geometrie im eigentlichen Sinne macht weitere Einschränkungen.

a) Von den zu betrachtenden Transformationen des Raumes verlangt man die Eigenschaft, daß sie die Punkte jeder Geraden bzw. jeder Ebene wieder in die Punkte einer Geraden bzw. einer Ebene überführen (also lineare Gebilde gleicher Dimension aufeinander abbilden unter Erhaltung der Inzidenz, d. h. gegenseitiger Lagebeziehungen). Solche Transformationen heißen projektive Transformationen.

Zum Beispiel bilden projektive Transformationen ein Quadrat auf ein Viereck ab, das aber im allgemeinen weder parallele noch orthogonale noch gleichlange Seiten hat. Die projektiven Transformationen lassen also von allen Eigenschaften eines Quadrats nur die Viereckeigenschaft invariant.

Die Gesamtheit der projektiven Transformationen des Raumes bildet eine Gruppe, die sog. projektive Gruppe.

Beweis

M I: Die Nacheinanderausführung zweier projektiver Transformationen ergibt wieder eine solche. Da nämlich sowohl die erste als auch die zweite Transformation lineare Gebilde unter Erhaltung der Inzidenz in ebensolche überführt, so gilt dies auch für die gesamte Abbildung. Die Eindeutigkeit der Verknüpfung ist sogar für beliebige Transformationen erfüllt.

M II: Das assoziative Gesetz gilt ebenfalls sogar für beliebige Transformationen.

M III$_1$: Die in B(2.6b) erklärte identische Transformation ist offensichtlich projektiv.

M III$_2$: Desgleichen ist die in B(2.6b) für jede Transformation s erklärte inverse Transformation s^{-1} mit s ebenfalls projektiv. qed.

b) Besondere projektive Transformationen sind solche, die parallele Geraden wieder in parallele Geraden überführen. Sie werden affine Transformationen genannt. Ein Quadrat wird von ihnen auf ein Parallelogramm abgebildet, das aber im allgemeinen weder orthogonale noch gleichlange Seiten hat. Die affinen Transformationen lassen also von den Eigenschaften eines Quadrats nur die Parallelogrammeigenschaft invariant.

Die Gesamtheit der affinen Transformationen des Raumes bildet eine Gruppe, die sog. affine Gruppe. Der Beweis verläuft analog dem für die projektive Gruppe.

c) Besondere affine Transformationen sind solche, die orthogonale Geraden wieder in orthogonale Geraden überführen. Man bezeichnet sie als äquiforme Transformationen oder Ähnlichkeitstransformationen. Sie lassen nämlich nicht nur rechte, sondern überhaupt alle Winkel und damit alle Längenverhältnisse invariant. Diese Transformationen überführen jedes Quadrat wieder in ein Quadrat, im allgemeinen jedoch von anderer Seitenlänge. Die Ausführung einer solchen Transformation bedeutet also eine maßstäbliche Vergrößerung bzw. Verkleinerung. Analog zu a) und b) beweist man:

Die Gesamtheit der äquiformen Transformationen des Raumes bildet eine Gruppe, die sog. äquiforme Gruppe oder Hauptgruppe.

d) Besondere Ähnlichkeitstransformationen sind solche, die die Längen selbst invariant lassen, also die *kongruenten Transformationen*. Entsprechend dem bisher Ausgeführten bilden sie ebenfalls eine Gruppe, die sog. *Kongruenzgruppe*.

e) Besondere kongruente Transformationen sind solche, die jede Orientierung erhalten. Sie werden auch *Bewegungen* (im Gegensatz zu Umlegungen) genannt und bilden die sog. *Bewegungsgruppe*.

Die unter a) bis e) geschilderten Gruppen, deren jede die folgenden enthält, kennzeichnen den in der modernen Mathematik üblichen Aufbau der Geometrie. Er wurde zum ersten Male von F. KLEIN[1]) in dem bekannten *Erlanger Programm* aufgezeigt.

Auf die analytische Darstellung geometrischer Transformationen und ihren Zusammenhang mit der Matrizenrechnung kommen wir in § 14 zu sprechen.

Restklassen ganzer Zahlen **B (2.8)**

Jede positive ganze Zahl m gestattet, in der Menge der ganzen Zahlen eine Äquivalenzrelation zu erklären, die sog. Kongruenz modulo m:

Sind a und b ganze Zahlen, so nennt man a kongruent b modulo m genau dann, wenn die Differenz $a - b$ ein ganzzahliges Vielfaches gm von m ist. Man bezeichnet dies durch

$$a \equiv b \bmod m$$

oder kürzer

$$a \equiv b \ (m).$$

Die Kongruenz mod m ist tatsächlich eine Äquivalenzrelation, denn sie ist offensichtlich (vgl. Aufg. 8)

reflexiv: $a \equiv a \ (m)$,

symmetrisch: aus $a \equiv b \ (m)$ folgt $b \equiv a \ (m)$,

transitiv: aus $a \equiv b \ (m)$ und $b \equiv c \ (m)$ folgt $a \equiv c \ (m)$.

---

1) FELIX KLEIN, 1849 bis 1925, „Vergleichende Betrachtungen über neuere geometrische Forschungen", Erlangen 1872.

Wie aus der Mengenlehre bekannt ist, bewirkt jede in einer Menge erklärte Äquivalenzrelation eine Einteilung dieser Menge in Klassen zueinander äquivalenter Elemente. So entsteht durch die Kongruenz mod m die Einteilung der Menge der ganzen Zahlen in die sog. Restklassen mod m. Genau die in einer Restklasse mod m liegenden ganzen Zahlen sind also untereinander kongruent.

Wegen der Elementfremdheit der Klassen bestimmt jedes Element der Klasse eindeutig die Klasse, der es angehört. Die die ganze Zahl a enthaltende Restklasse mod m bezeichnen wir mit

$$[a] \bmod m.$$

Es entspricht der Kongruenz der Elemente

$$a \equiv b \bmod m$$

die Gleichheit der Restklassen

$$[a] = [b] \bmod m.$$

Der Name „Restklassen" stammt von einer anderen Definition der Kongruenz. Sie besagt, daß zwei Zahlen mod m kongruent sind, wenn sie bei der Division durch m den gleichen Rest lassen, und ist mit unserer Erklärung gleichwertig. Es folgt nämlich einmal aus

$$a = qm + r \quad \text{und} \quad b = q'm + r \quad \text{mit} \quad 0 \leq r < m,$$

daß die Differenz

$$a - b = (q - q')m$$

ein ganzzahliges Vielfaches von m ist. Umgekehrt ergibt sich aus

$$a - b = gm$$

durch Einsetzen in $a = qm + r$ mit $0 \leq r < m$, daß auch b bei Division durch m den gleichen Rest r läßt:

$$b = a - gm = (q - g)m + r.$$

Aus dieser Definition entnehmen wir sofort, daß es genau m verschiedene Restklassen mod m gibt:

$$[0], [1], \ldots, [m - 1].$$

Die Zahlen $0, 1, \ldots, m-1$ bilden also ein vollständiges Repräsentantensystem der Restklassen mod m, welches das kleinste nichtnegative Repräsentantensystem mod m genannt wird.

Das Studium der Restklassen und der Kongruenzrechnung ist ein wesentlicher Teil der elementaren Zahlentheorie, in dem gruppentheoretische Überlegungen eine wichtige Rolle spielen. Die folgende Einführung faßt das für die Gruppentheorie Benötigte zusammen.

a) In der Menge der Restklassen mod m führen wir durch

$$[a] + [b] = [a + b]$$

eine additive Verknüpfung ein. Auf diese Weise wird in der Tat den beiden Restklassen $[a]$ und $[b]$ eine eindeutig bestimmte Restklasse als Summe zugeordnet, die von der Wahl der Repräsentanten a und b unabhängig ist. Wir müssen also zeigen, daß aus

$$[a] = [a'] \text{ und } [b] = [b']$$

folgt

$$[a + b] = [a' + b'].$$

Gehen wir von der Gleichheit der Restklassen zur Kongruenz der Elemente über, so lautet diese Behauptung, daß aus

$$a \equiv a' \ (m) \text{ und } b \equiv b' \ (m)$$

folgt

$$a + b \equiv a' + b' \ (m).$$

Dies ist aber wegen

$$a = a' + gm \text{ und } b = b' + hm$$

und damit

$$a + b = a' + b' + (g + h)m$$

erfüllt.

Analog erklären wir in der Menge der Restklassen mod m durch

$$[a] \cdot [b] = [a \cdot b]$$

eine multiplikative Verknüpfung, die ebenfalls den beiden Restklassen $[a]$ und $[b]$ unabhängig von der Wahl der Repräsentanten a und b eine eindeutig bestimmte Restklasse als Produkt zuordnet (vgl. Aufg. 9).

b) *Die Menge der Restklassen mod m bildet bezüglich der in* a) *erklärten Addition einen Modul der Ordnung m, den sogenannten Restklassenmodul mod m.*

Beweis

Es bleibt nur zu zeigen:

A II: Die Assoziativität der Addition der ganzen Zahlen überträgt sich gemäß der Definition auf die Addition der Restklassen.

$A\ III_1$: Nullelement ist die Nullrestklasse [0].

$A\ III_2$: Die zur Restklasse $[a]$ entgegengesetzte Restklasse $-[a]$ ist $[-a]$.

A IV: Man schließt wie bei *A II*.

qed.

c) Bezüglich der in a) erklärten Multiplikation bilden auch die von [0] verschiedenen Restklassen mod m im allgemeinen keine Gruppe. Wir zeigen durch ein Beispiel, daß *M III** nicht erfüllt ist. Es ergibt sich nämlich mod 12:

$$[5] \cdot [4] = [2] \cdot [4] = [8], \text{ obwohl } [5] \neq [2].$$

d) Wir können jedoch ähnlich wie in B(2.4) eine Untermenge in der Menge der Restklassen mod m auszeichnen, die eine multiplikative Gruppe bildet.

Dazu erinnern wir zunächst an einige Begriffe aus der Teilbarkeitslehre ganzer Zahlen:

Eine ganze Zahl t heißt Teiler einer ganzen Zahl a (in Zeichen $t \mid a$), wenn es eine ganze Zahl x mit $a = t \cdot x$ gibt. Dann ist natürlich wegen $a = (-t)(-x)$ auch $-t$ ein Teiler von a, so daß man sich auf positive Teiler beschränken kann.

Damit ist klar, was unter einem gemeinsamen Teiler t zweier Zahlen a und b zu verstehen ist. Unter allen möglichen gemeinsamen Teilern ist der größte gemeinsame Teiler d von a und b (in Zeichen $d = (a, b)$) durch die beiden folgenden Forderungen eindeutig bestimmt:

1. d ist (positiver) gemeinsamer Teiler von a und b: $d \mid a$ und $d \mid b$.
2. Jeder gemeinsame Teiler t von a und b ist auch Teiler von d:
   Aus $t \mid a$ und $t \mid b$ folgt $t \mid d$.

Man überlegt sich dies am einfachsten, indem man jede der auftretenden Zahlen in ihre Primfaktoren zerlegt (vgl. Aufg. 11). Die dabei verwendete Existenz und Eindeutigkeit einer solchen Zerlegung ist ein wichtiger (und

durchaus nicht trivialer) Satz der elementaren Zahlentheorie, auf den wir uns hier jedoch ohne Beweis stützen. Übrigens wird sich ein solcher Beweis bei allgemeinen Betrachtungen im folgenden Band ohnehin mit ergeben.

Die angestrebte Auswahl gewisser Restklassen beruht auf folgendem Sachverhalt:

Alle Zahlen $a, a', \ldots$ einer Restklasse mod m haben mit m den gleichen größten gemeinsamen Teiler.

Beweis

Wir bezeichnen $(a, m) = d$ und $(a', m) = d'$. Aus $(a, m) = d$ folgt $d|a$ und $d|m$. Wegen

$$a' \equiv a \ (m), \text{ also } a' = a + gm$$

gilt dann auch $d|a'$. Mit $d|m$ ergibt sich daher $d|d'$. Umgekehrt folgt $d'|a'$ und $d'|m$ aus $(a', m) = d'$. Wegen

$$a = a' - gm$$

gilt dann auch $d'|a$. Mit $d'|m$ folgt dann auch $d'|d$. Also ist $d' = d$.

qed.

Daher ist der größte gemeinsame Teiler (a, m) eine Eigenschaft der Restklasse $[a] \bmod m$. Das ermöglicht es, insbesondere diejenigen Restklassen $[a] \bmod m$ zu betrachten, für die $(a, m) = 1$ gilt. Sie heißen prime Restklassen mod m.

e) *Die Menge der primen Restklassen mod m bildet bezüglich der in* a) *erklärten Multiplikation eine abelsche Gruppe, die sog. prime Restklassengruppe mod m.*

Beweis

M I: Wir wissen bereits, daß das Produkt zweier beliebiger Restklassen mod m wieder eine eindeutig bestimmte Restklasse mod m ist. Insbesondere ist das Produkt zweier primen Restklassen mod m wieder eine prime Restklasse mod m, denn das Produkt zweier zu m teilerfremden Zahlen ist selbst teilerfremd zu m.

M II: Die Assoziativität der Restklassenmultiplikation ergibt sich entsprechend wie in b) aus der Assoziativität der Multiplikation ganzer Zahlen.

*M III**: Da es nur m verschiedene Restklassen mod m gibt, ist die Menge der primen Restklassen mod m erst recht endlich. Nach S(1.10) genügt dann der Nachweis von *M III**. Wir nehmen also an, daß

$$[a] \cdot [x_1] = [a] \cdot [x_2], \text{ also } [ax_1] = [ax_2]$$

ist. Dann ist die Differenz

$$ax_1 - ax_2 = a(x_1 - x_2) = gm$$

ein ganzzahliges Vielfaches von m. Da nach Voraussetzung $(a, m) = 1$ gilt, folgt daraus $m \mid (x_1 - x_2)$, d. h. aber

$$[x_1] = [x_2].$$

M IV: Man schließt wie bei *M II*.

qed.

Der Spezialfall $m = p$ mit einer beliebigen Primzahl p ist notwendig und hinreichend dafür, daß alle von [0] verschiedenen Restklassen mod m prim sind. Genau in diesem Falle bilden die $m - 1$ von [0] verschiedenen Restklassen mod m eine multiplikative abelsche Gruppe.

f) Die Ordnung der primen Restklassengruppe mod m wird durch die Anzahl der zu m teilerfremden Zahlen gegeben, die kleiner als m sind. Man bezeichnet sie durch die sogenannte *EULERsche Funktion* $\varphi(m)$. In der Zahlentheorie leitet man unter Verwendung der Zerlegung von m in Primfaktoren,

$$m = p_1^{\mu_1} \cdot p_2^{\mu_2} \quad \cdot p_h^{\mu_h} \quad (p_i \neq p_j \text{ für } i \neq j),$$

für $\varphi(m)$ die Formel ab:

$$\varphi(m) = m \cdot \left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_h}\right) = p_1^{\mu_1 - 1} \ldots p_h^{\mu_h - 1} (p_1 - 1) \ldots (p_h - 1).$$

Zum Beispiel besitzt die prime Restklassengruppe mod 12 als Elemente die $\varphi(12) = \varphi(2^2 \cdot 3) = 4$ primen Restklassen mod 12:

$$[1], [5], [7], [11].$$

Aufgaben zu § 2

1. Man prüfe für alle Beispiele das Erfülltsein bzw. Nichterfülltsein der Gruppenaxiome nach, soweit dies im Text noch nicht ausdrücklich geschehen ist.
2. Die im Text angegebenen Beispiele erschöpfen keineswegs die Möglichkeit, Gruppen aus Zahlen zu bilden. So ist etwa die Menge aller geraden Zahlen ein Modul, die Menge aller Brüche, deren Zähler und Nenner ganzzahlige Potenzen von 2 sind, eine multiplikative abelsche Gruppe. Man prüfe diese Behauptungen nach und bilde ähnliche Beispiele.
3. Man begründe die in B(2.3c) aufgestellte Behauptung.
4. Auch die Multiplikation quadratischer Matrizen mit nichtverschwindender Determinante ist im allgemeinen nicht kommutativ. Man zeige dies durch Beispiele.
5. Es gibt genau $n!$ Permutationen der Zahlen $1, 2, \ldots, n$.
6. Die symmetrische Gruppe $\mathfrak{S}_n$ ist nur im Fall $n = 2$ abelsch.
7. Man zeige, daß die in B(2.5c) angegebene Funktion tatsächlich symmetrisch ist.
8. Man beweise die Reflexivität, Symmetrie und Transitivität der Kongruenz mod m.
9. Man zeige die Unabhängigkeit der Definition

$$[a] \cdot [b] = [a \cdot b]$$

von der Wahl der Repräsentanten a und b.

10. Man stelle die Restklassen mod 6 auf und veranschauliche sich die in B(2.8a) erklärten Verknüpfungen.
11. Unter Voraussetzung der Existenz und Eindeutigkeit der Primzerlegung positiver ganzer Zahlen zeige man, daß der größte gemeinsame Teiler $d = (a, b)$ durch die in B(2.8d) genannten beiden Forderungen eindeutig bestimmt ist.

§ 3. Potenzen von Gruppenelementen

Unter allen Produkten von Elementen einer Gruppe treten insbesondere solche auf, deren Faktoren alle übereinstimmen. In Anlehnung an die allgemein für derartige Produkte übliche Bezeichnung spricht man auch hier von Potenzen.

Der Leser vergegenwärtige sich für das Folgende die Potenzrechnung mit gewöhnlichen Zahlen. Sie beginnt mit der Einführung von Potenzen mit natürlichen Exponenten ≥ 2, für die gewisse Gesetze abgeleitet werden. Die „erste Erweiterung des Potenz-

begriffes" hat die Zulassung von beliebigen ganzzahligen Exponenten zum Ziel, wobei gefordert wird, daß die gleichen Gesetze gültig bleiben (Permanenzprinzip). Zur Erklärung von Potenzen mit negativen Exponenten benutzt man Quotienten. Die erweiterte Potenzrechnung führt daher nur aus solchen Zahlenbereichen nicht hinaus, in denen die Division uneingeschränkt ausführbar ist.

Die Behandlung der Potenzen von Gruppenelementen erfolgt völlig analog. Wegen der Gruppeneigenschaft *M III* erweist sich die Erweiterung des Potenzbegriffes auf negative Exponenten in Gruppen als immer durchführbar. Diese allgemeinen abstrakten Überlegungen umfassen natürlich den konkreten Fall aller derjenigen Zahlenbereiche, die multiplikative Gruppen sind. Die Allgemeinheit macht unsere Überlegungen jedoch nicht schwieriger. Sie würden, um exakt zu sein, in jedem einzelnen konkreten Falle entsprechend verlaufen müssen.

Definition **D (3.1)**

Ein Produkt von n gleichen Faktoren $a \in \mathfrak{G}$ *heißt n-te Potenz von a:*

$$a^n = \underbrace{a \cdot a \cdot \ldots \cdot a}_{n}.$$

Das Operationszeichen n ist dabei eine natürliche Zahl ≥ 2 *und wird als Exponent bezeichnet.*

Folgerung **F (3.2)**

In jeder Gruppe gelten die beiden Potenzgesetze:

$$I: \quad a^n \cdot a^m = a^{n+m}$$

$$II: \quad (a^n)^m = a^{n \cdot m}.$$

Dagegen gilt

$$III: \quad (ab)^n = a^n \cdot b^n$$

dann (und für alle n auch nur dann), wenn $ab = ba$ *ist, insbesondere also stets für abelsche Gruppen. Dabei sind n und m natürliche Zahlen* ≥ 2.

Dies ergibt sich unmittelbar aus D (3.1) allein unter Verwendung von *M I* und *M II* (vgl. Aufg. 1). Da die Definition D (3.1) ebenfalls von der Gültigkeit von *M III* unabhängig ist, hätten

wir also das bisher Gesagte auch für Mengen mit einer Verknüpfung aussprechen können, die nur *M I* und *M II* erfüllt. Dagegen werden wir ab jetzt die Voraussetzung, daß wir Potenzen von Gruppenelementen untersuchen, voll ausnützen. So stellen wir zunächst folgenden Zusammenhang zwischen Potenz- und Inversenbildung fest:

Folgerung **F (3.3)**

Das Inverse der n-ten Potenz ($n \geq 2$) *von* $a \in \mathfrak{G}$ *ist die n-te Potenz des Inversen* a^{-1} *von a:*

$$(a^n)^{-1} = (a^{-1})^n .$$

Beweis

Nach Definition des Inversen erfüllt $(a^n)^{-1}$ die Gleichung:

$$a^n \cdot (a^n)^{-1} = e .$$

Andererseits ergibt sich

$$a^n \cdot (a^{-1})^n = \underbrace{a\,a \ldots a}_{n} \cdot \underbrace{a^{-1}a^{-1} \ldots a^{-1}}_{n} = e$$

durch n-malige Anwendung von $a\,a^{-1} = e$. Aus der Eindeutigkeit des Inversen folgt die Behauptung.

qed.

Das zu jedem Gruppenelement a existierende Inverse wurde formal als a^{-1} bezeichnet. Es ist die eindeutig bestimmte Lösung der Gleichung $ax = e$ und hat mit dem in D (3.1) erklärten Potenzbegriff nichts zu tun. Um a^{-1} als Potenz von a auffassen zu können, müssen wir den Potenzbegriff dahingehend erweitern, daß sogar alle ganzen Zahlen als Exponenten zugelassen werden. Eine solche Erweiterung ist nur sinnvoll, wenn dabei die in F (3.2) genannten Gesetze gültig bleiben (Permanenzprinzip). Wir benutzen daher diese Gesetze als Anleitung für die angestrebte Erweiterung. In diesem Sinne werden uns schon durch das Potenzgesetz *I*

$$\text{wegen} \quad \left\{ \begin{array}{ll} a \cdot a & = a^2 \\ a \cdot a^{-1} & = e \\ a^n \cdot (a^n)^{-1} & = e \end{array} \right\} \quad \text{die Setzungen} \quad \left\{ \begin{array}{ll} a^1 & = a \\ a^0 & = e \\ a^{-n} & = (a^n)^{-1} \end{array} \right\} ,$$

letztere für $n \geq 2$, nahegelegt. Wir sprechen diese Setzungen als Definition aus und müssen selbstverständlich nachweisen, daß damit F (3.2) für den so erweiterten Potenzbegriff erhalten bleibt.

Definition **D (3.4)**

Wir erklären:

$$a^1 = a$$
$$a^0 = e$$
$$a^{-n} = (a^n)^{-1} \qquad (n \geq 2).$$

Die letzte Setzung in D (3.4) besagt im Zusammenhang mit F (3.3):

$$a^{-n} = (a^n)^{-1} = (a^{-1})^n.$$

Diese Gleichheiten gelten zunächst für $n \geq 2$, die erste wurde definiert, die zweite bewiesen. Wir zeigen als nächstes, daß sie für beliebige ganzzahlige Exponenten weitergelten.

Folgerung **F (3.5)**

Es ist $a^{-n} = (a^n)^{-1} = (a^{-1})^n$

für beliebiges ganzzahliges $n \gtrless 0$.

Beweis

1. Für $n \geq 2$ ist alles klar.
2. Das gleiche gilt nach D (3.4) für $n = 1$ und $n = 0$.
3. Für negative $n = -m$ $(m > 0)$ ist zu beweisen:

$$a^m = (a^{-m})^{-1} = (a^{-1})^{-m}.$$

Es ist aber

$$\begin{aligned}(a^{-1})^{-m} &= [(a^{-1})^m]^{-1} && \text{nach D (3.4), angewendet auf } (a^{-1}) \text{ und } m > 0,\\ &= [(a^m)^{-1}]^{-1} && \text{nach F (3.3), wegen } m > 0,\\ &= \begin{cases}[a^{-m}]^{-1} & \text{nach D (3.4), angewendet auf } a \text{ und } m > 0,\\ a^m & \text{nach F (1.6).}\end{cases}\end{aligned}$$

qed.

Satz **S (3.6)**

Die Potenzgesetze I, II, III bleiben gültig für alle nach D (3.4) *auftretenden ganzzahligen Exponenten.*

Beweis

Wir zeigen zuerst I, indem wir in der zu beweisenden Formel

$$a^n \cdot a^m = a^{n+m}$$

für n jede beliebige ganze Zahl zulassen und für m folgende Fallunterscheidungen durchführen:

1. Für $m = 0$, $m = +1$, $m = -1$ überzeugt man sich sofort von der Richtigkeit der Behauptung.

2. Für positive m führen wir vollständige Induktion von m auf $m+1$ durch. Der Induktionsanfang ist nach 1. mit $m = 1$ gegeben. Dann ist

$$\begin{aligned} a^n \cdot a^{m+1} &= a^n \cdot (a^m \cdot a^1) && \text{nach 1.} \\ &= (a^{n+m}) \cdot a^1 && \text{nach Induktionsvoraussetzung} \\ &= a^{(n+m)+1} && \text{nach 1.} \end{aligned}$$

3. Analog verfahren wir für negative $m = -s$ $(s > 0)$, indem wir vollständige Induktion von s auf $s+1$ durchführen. Der Induktionsanfang ist nach 1. mit $s = 1$ gegeben. Dann ist:

$$\begin{aligned} a^n \cdot a^{-(s+1)} &= a^n \cdot a^{-s-1} \\ &= a^n \cdot (a^{-s} \cdot a^{-1}) && \text{nach 1.} \\ &= (a^{n-s}) \cdot a^{-1} && \text{nach Induktionsvoraussetzung} \\ &= a^{(n-s)-1} && \text{nach 1.} \\ &= a^{n-(s+1)}. \end{aligned}$$

Beim Nachweis von II bedienen wir uns ähnlicher Schlüsse. Wir lassen in

$$(a^n)^m = a^{n \cdot m}$$

n jeden beliebigen ganzzahligen Wert annehmen und unterscheiden bezüglich m:

1. Für $m = 0$, $m = 1$, $m = -1$ folgt die Behauptung nach D (3.4) bzw. F (3.5).

2. Für positive m führt man vollständige Induktion durch, die dem Leser überlassen bleibt (vgl. Aufg. 3).

3. Für negative $m = -s$ $(s > 0)$ sei der Schluß von s auf $s+1$ hier noch einmal durchgeführt:

$$\begin{aligned}
(a^n)^{-(s+1)} &= (a^n)^{-s-1} \\
&= (a^n)^{-s} \cdot (a^n)^{-1} && \text{nach } I \\
&= a^{n(-s)}\,(a^n)^{-1} && \text{nach Induktionsvoraussetzung} \\
&= a^{n(-s)}\,a^{-n} && \text{nach F (3.5)} \\
&= a^{n(-s)-n} && \text{nach } I \\
&= a^{n(-s-1)} \\
&= a^{n(-(s+1))}.
\end{aligned}$$

Schließlich beweisen wir *III*. Für $n \geq 2$ und $n = -1$ ist dies schon geschehen. Die Fälle $n = 0$ und $n = 1$ ergeben sich aus D (3.4). Für $n \leq 2$, also $n = -s$ $(s \geq 2)$, führen wir die Behauptung mit Hilfe von F (3.5) auf die bereits gezeigten Fälle zurück:

$$\begin{aligned}
(a \cdot b)^{-s} &= [(a \cdot b)^{-1}]^s = [(b \cdot a)^{-1}]^s = [a^{-1} \cdot b^{-1}]^s = (a^{-1})^s \cdot (b^{-1})^s \\
&= a^{-s} \cdot b^{-s}.
\end{aligned}$$

Dabei haben wir die Vertauschbarkeit von a und b mehrfach benutzt. Diese Bedingung ist also hinreichend. Sie ist aber auch notwendig, wie der Fall $n = -1$ lehrt (vgl. Aufg. 4).

qed.

Entsprechend den Bemerkungen nach dem Beweis von S (1.10) ff. können wir die Potenzrechnung in die additive Schreibweise übertragen. In Moduln entspricht dem Begriff der Potenz der Begriff des Vielfachen:

Definition **D (3.7)**

Eine Summe von n gleichen Summanden $a \in \mathfrak{G}$ heißt Vielfaches von a:

$$na = \underbrace{a + a + \ldots + a}_{n}.$$

Das Operationszeichen n ist dabei eine natürliche Zahl ≥ 2.

Folgerung **F (3.8)**

In jedem Modul gelten die drei Gesetze:

$$\begin{aligned} I: &\quad na + ma = (n+m)\,a \\ II: &\quad m(na) = (m \cdot n)\,a \\ III: &\quad na + nb = n(a+b), \end{aligned}$$

wobei zunächst n und m natürliche Zahlen ≥ 2 *sind.*

Auch der Begriff des Vielfachen läßt sich für beliebige ganze Zahlen als Operationszeichen so erweitern, daß die Gesetze *I, II, III* gültig bleiben.

Definition **D (3.9)**

Wir erklären:

$$\begin{aligned} 1a &= a \\ 0a &= o \\ (-n)\,a &= -(na)\ (n \geq 1), \end{aligned}$$

wobei o das Nullelement des Moduls und $-(na)$ *das zu na entgegengesetzte Element bedeuten*[1]).

Entsprechend F (3.5) und S (3.6) erhalten wir:

Folgerung **F (3.10)**

Es ist $(-n)\,a = -(na) = n\,(-a)$

für beliebige ganzzahlige $n \gtrless 0$.

Satz **S (3.11)**

Die Gesetze I, II, III bleiben gültig für alle nach D (3.9) *auftretenden ganzzahligen Operationszeichen.*

Es sei ausdrücklich darauf hingewiesen, daß mit D (3.7) und D (3.9) nicht etwa zusätzlich zur additiven Verknüpfung des

1) Wenn eine Unterscheidung wünschenswert ist, bezeichnen wir die Zahl Null mit 0 im Gegensatz zum Nullelement *o* und entsprechend die Zahl Eins mit 1 im Gegensatz zum Einselement *e*.

Moduls eine neue (etwa multiplikative) Verknüpfung der Modulelemente untereinander erklärt wird. Vielmehr handelt es sich um eine eindeutig definierte „Operatoranwendung" der ganzen Zahlen auf die Modulelemente. Die ganzen Zahlen werden dabei zu einem „Operatorenbereich" für jeden Modul.

Dieser Sachverhalt erhält in der Gruppentheorie eine Verallgemeinerung, indem man für beliebige Gruppen die Anwendung beliebiger Operatorenbereiche mit analogen Gesetzmäßigkeiten definiert. Darauf kommen wir später zu sprechen.

Aufgaben zu § 3

1. Man beweise die Folgerung F(3.2).
2. Man führe einen zweiten Beweis für F(3.3) durch vollständige Induktion.
3. Man trage den fehlenden Schluß im Beweis von S(3.6) nach.
4. Zwei Gruppenelemente a und b erfüllen $ab = ba$ dann und nur dann, wenn das gleiche für ihre Inversen gilt.
5. Gruppenelemente, die als Potenzen eines festen Gruppenelementes geschrieben werden können, sind kommutativ multiplizierbar.
6. Für beliebige Gruppenelemente a und b gilt:

$$(ab)^{-n} = (b^{-1}a^{-1})^n.$$

   Man beweise diese Formel und verallgemeinere sie auf eine beliebige endliche Anzahl von Faktoren.
7. Man vergleiche alle Aussagen in Moduln mit den jeweils entsprechenden in multiplikativen Gruppen.
8. Man übertrage die Aussagen in Aufgabe 6 in additive Schreibweise.
9. Der Leser wird bemerkt haben, daß bei den letzten Betrachtungen in diesem Paragraphen die ganzen Zahlen in doppelter Bedeutung auftreten können, nämlich einmal mit den üblichen Rechengesetzen als Operatorenbereich für jeden Modul, zum anderen aber als einer von diesen Moduln selbst. Man überlege sich, daß in diesem Spezialfall durch D(3.7) und D(3.9) ausnahmsweise eine Verknüpfung zwischen Elementen derselben Menge erklärt wird. Diese stimmt, wenn sie auch einer ganz anderen Auffassung entspringt, mit der üblichen Multiplikation der ganzen Zahlen überein.
10. Der in B(2.3) erklärte Modul der Vektoren ist ein Beispiel eines Moduls, der nicht nur die ganzen Zahlen, sondern alle reellen Zahlen als Operatorenbereich mit den in F(3.8) genannten Gesetzen *I*, *II*, *III* gestattet.
11. Das gleiche gilt für den in B(2.4) erklärten Modul aller Matrizen vom Typ (n, m).

§ 4. Strukturtafel, Isomorphie

Wir lernen in diesem Paragraphen zunächst ein Hilfsmittel zur rechnerischen Beherrschung endlicher Gruppen kennen. Dabei werden wir von selbst auf den grundlegenden Begriff der Isomorphie geführt.

Eine Gruppe $\mathfrak{G}$ ist eine Menge, in der eine Verknüpfung erklärt ist, an die bestimmte Anforderungen gestellt sind. Im endlichen Falle können wir also die Elemente der Menge $\mathfrak{G}$ mit $a_1, a_2, \ldots, a_n$ in beliebiger Reihenfolge bezeichnen, für die Verknüpfung eine vollständige Rechentafel aufstellen und uns schließlich fragen, wie sich die an die Verknüpfung gestellten Anforderungen in der Rechentafel widerspiegeln.

Die zu konstruierende Rechentafel wird nach dem Mathematiker CAYLEY[1]) benannt.

Erklärung **D (4.1)**

Man erhält die *CAYLEYsche Strukturtafel* einer endlichen Gruppe $\mathfrak{G}$, indem man alle Gruppenelemente $a_1, a_2, \ldots, a_n$ wie unter *I.* in je einer Spalte und Zeile als Tafeleingänge schreibt und den Innenraum der so entstehenden Tabelle wie unter *II.* mit den n^2 Produkten (bzw. Summen) der Elemente ausfüllt:

I.

	a_1	a_2	. . .	a_n
a_1				
a_2				
a_n				

II.

	. . .	a_k	. . .
a_i	·····	$a_i a_k$	

1) ARTHUR CAYLEY, 1821 bis 1895.

Als Beispiel stellen wir die Strukturtafel der symmetrischen Gruppe $\mathfrak{S}_3$ mit den Elementen

$$s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad s_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad s_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$s_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad s_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad s_6 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

auf[1]:

	s_1	s_2	s_3	s_4	s_5	s_6
s_1	s_1	s_2	s_3	s_4	s_5	s_6
s_2	s_2	s_3	s_1	s_6	s_4	s_5
s_3	s_3	s_1	s_2	s_5	s_6	s_4
s_4	s_4	s_5	s_6	s_1	s_2	s_3
s_5	s_5	s_6	s_4	s_3	s_1	s_2
s_6	s_6	s_4	s_5	s_2	s_3	s_1

Folgerung **F (4.2)**

Den einzelnen Gruppeneigenschaften entsprechen die folgenden Gesetzmäßigkeiten der Strukturtafel:

M I bzw. *A I:* An jeder Stelle der Tafel steht ein eindeutig bestimmtes Element der Gruppe.

M III$_1$ bzw. *A III*$_1$*:* Es gibt wenigstens eine Zeile, die mit dem Tafeleingang übereinstimmt.

S(1.4) bzw. S(1.13)*:* Es gibt genau eine Zeile und eine Spalte, die mit dem entsprechenden Tafeleingang übereinstimmen. Bei der Wahl von $a_1 = e$ bzw. $a_1 = o$ sind dies die erste Zeile und erste Spalte, womit man die Tafeleingänge sparen kann.

---

1) Es versteht sich, daß die äußere Gestalt der Strukturtafel von der gewählten Numerierung der Gruppenelemente abhängig ist.

M III$_2$ bzw. *A III*$_2$: In jeder Spalte tritt das Eins- bzw. Nullelement mindestens einmal auf.

S(1.5) bzw. S(1.14): Das Eins- bzw. Nullelement tritt in jeder Zeile und in jeder Spalte genau einmal auf. Zeilen und Spalten, in deren Schnittpunkt e bzw. o steht, kennzeichnen zueinander inverse bzw. entgegengesetzte Elemente.

M III bzw. *A III*: In jeder Zeile und in jeder Spalte tritt jedes Gruppenelement mindestens einmal auf, weil sonst wenigstens eine Gleichung der Gestalt $ax = b$ oder $ya = b$ bzw. $a + x = b$ keine Lösung hätte.

*M III** bzw. *A III**: In jeder Zeile und jeder Spalte tritt jedes Gruppenelement höchstens einmal auf, weil sonst wenigstens eine Gleichung der Gestalt $ax = b$ oder $ya = b$ bzw. $a + x = b$ mindestens zwei verschiedene Lösungen hätte.

Bemerkung: Die beiden zuletzt genannten Eigenschaften der Strukturtafel folgen offensichtlich auseinander. Das bestätigt erneut die Gleichwertigkeit von *M III* und *M III** bzw. *A III* und *A III** für endliche Gruppen.

M IV bzw. *A IV*: Bei kommutativen Gruppen ist die Strukturtafel symmetrisch bezüglich der von links oben nach rechts unten verlaufenden Diagonalen.

Das assoziative Gesetz *M II* bzw. *A II* spiegelt sich in der Strukturtafel nicht unmittelbar wider. Wir geben ein Beispiel für eine Strukturtafel[1]), die allen bisher genannten Bedingungen genügt,

---

1) Es ist klar, daß man für jede Menge mit einer eindeutigen Verknüpfung ebenfalls eine Strukturtafel aufstellen kann,

aber in der zugrunde gelegten Menge eine Verknüpfung beschreibt, die nicht assoziativ ist:

	a_1	a_2	a_3	a_4	a_5	a_6
a_1	a_1	a_2	a_3	a_4	a_5	a_6
a_2	a_2	a_3	a_1	a_5	a_6	a_4
a_3	a_3	a_1	a_2	a_6	a_4	a_5
a_4	a_4	a_5	a_6	a_3	a_2	a_1
a_5	a_5	a_6	a_4	a_2	a_1	a_3
a_6	a_6	a_4	a_5	a_1	a_3	a_2

mit $(a_5 a_4)\, a_3 = a_2 a_3 = a_1$,

aber $a_5 (a_4 a_3) = a_5 a_6 = a_3$.

Das zeigt auch, daß *M II* bzw. *A II* nicht aus den übrigen Gruppenaxiomen abgeleitet werden kann.

Für das Folgende stützen wir uns auf weitere Beispiele. So bildet die Menge der vier Permutationen

$$s_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix},\ s_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix},\ s_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix},\ s_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

eine multiplikative abelsche Gruppe, die sog. *KLEINsche Vierergruppe* $\mathfrak{V}_4$. Zum Beweis der Gruppeneigenschaft stellen wir die Strukturtafel auf. Die Nachrechnung bleibt dem Leser überlassen:

	s_1	s_2	s_3	s_4
s_1	s_1	s_2	s_3	s_4
s_2	s_2	s_1	s_4	s_3
s_3	s_3	s_4	s_1	s_2
s_4	s_4	s_3	s_2	s_1

Wir stellen fest, daß alle in F (4.2) genannten Eigenschaften erfüllt sind. Da das assoziative Gesetz in B (2.5) für beliebige Permutationen bewiesen wurde, bilden also s_1, s_2, s_3, s_4 in der Tat eine multiplikative abelsche Gruppe.

Desgleichen bildet die Menge der Funktionen

$$f_1(x) = x, \quad f_2(x) = \frac{1}{x}, \quad f_3(x) = -x, \quad f_4(x) = -\frac{1}{x}$$

mit der Verknüpfung

$$[f_i \cdot f_k]\,(x) = f_k\,(f_i\,(x))$$

eine multiplikative abelsche Gruppe. Sie hat die Strukturtafel

	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

denn es ist z. B.

$$f_2 \cdot f_1 = f_1(f_2(x)) = f_1\left(\frac{1}{x}\right) = \frac{1}{x} = f_2$$

$$f_2 \cdot f_2 = f_2(f_2(x)) = f_2\left(\frac{1}{x}\right) = \frac{1}{\frac{1}{x}} = x = f_1$$

$$f_2 \cdot f_3 = f_3(f_2(x)) = f_3\left(\frac{1}{x}\right) = -\frac{1}{x} = f_4$$

$$f_2 \cdot f_4 = f_4(f_2(x)) = f_4\left(\frac{1}{x}\right) = -\frac{1}{\frac{1}{x}} = -x = f_3 \qquad \text{usw.}$$

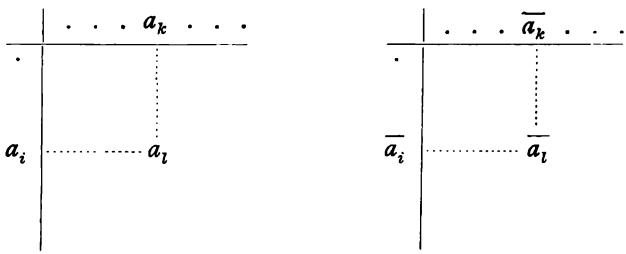
Aus der Strukturtafel ersehen wir wieder die Gültigkeit von *M I* und *M III*. Von *M II* könnten wir uns an dieser Stelle durch Ausrechnen von allen 4^3 Möglichkeiten überzeugen; wir werden aber sehen, wie wir die Gültigkeit von *M II* anders erschließen können (vgl. Aufg. 4).

Die beiden zuletzt aufgeführten Beispiele sind insofern interessant, als ihre Strukturtafeln, wenn man von der Art der Elemente absieht, übereinstimmen. Daher besteht in beiden Gruppen eine „strukturelle Gleichheit" in dem Sinne, daß sich die Verknüpfung in der einen Gruppe genauso vollzieht wie in der anderen. Diejenigen Eigenschaften, die sich nur daraus ergeben, wie die Gruppenelemente zu verknüpfen sind, gelten also für beide Gruppen gleichzeitig.

Ein derartiger Sachverhalt ist für die Untersuchung von Gruppen von großer Wichtigkeit. Wir stellen daher die wesentlichen Merk-

male fest, die die strukturelle Gleichheit zweier Gruppen allgemein kennzeichnen.

Es seien $\mathfrak{G}$ und $\overline{\mathfrak{G}}$ zwei endliche multiplikative Gruppen, deren Strukturtafeln in der eben beschriebenen Weise übereinstimmen. Damit ist also eine Numerierung der Elemente $a_1, a_2, \ldots, a_n$ aus $\mathfrak{G}$ und $\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n}$ aus $\overline{\mathfrak{G}}$ in der Art möglich, daß in beiden Strukturtafeln an gleichen Stellen gleiche Indizes auftreten:



Es existiert also eine eineindeutige Abbildung von $\mathfrak{G}$ auf $\overline{\mathfrak{G}}$ vermöge der Zuordnung

$$a_i \to \overline{a_i},$$

für welche die aus

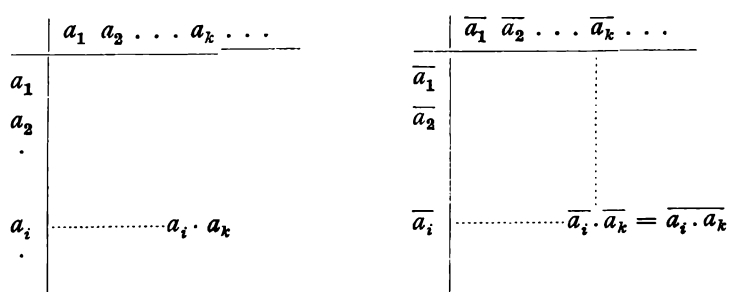
$$a_i \cdot a_k = a_l \to \overline{a_l} = \overline{a_i} \cdot \overline{a_k}$$

folgende Relation

$$\overline{a_i \cdot a_k} = \overline{a_i} \cdot \overline{a_k}$$

gilt.

Man sieht, daß umgekehrt zwei endliche Gruppen, für die eine solche Abbildung möglich ist, gleiche Strukturtafeln besitzen:



Die strukturelle Gleichheit zweier endlicher Gruppen kann also ebensogut durch die Gleichheit ihrer Strukturtafeln als auch durch die Existenz einer eineindeutigen relationstreuen Abbildung aufeinander gekennzeichnet werden. Relationstreue heißt dabei zunächst die Gültigkeit von

$$\overline{a_i \cdot a_k} = \overline{a_i} \cdot \overline{a_k} \text{ für alle } i \text{ und } k,$$

in Worten:

Bild des Produktes = Produkt der Bilder.

Im Falle zweier additiver Gruppen, für die offensichtlich die gleichen Überlegungen gelten, bedeutet Relationstreue entsprechend:

$$\overline{a_i + a_k} = \overline{a_i} + \overline{a_k} \text{ für alle } i \text{ und } k,$$

also:

Bild der Summe = Summe der Bilder.

Wir können sogar von der strukturellen Gleichheit einer additiven und einer multiplikativen Gruppe sprechen, wobei wir unter Relationstreue zu verstehen haben (vgl. Aufgaben 3 und 5):

$$\overline{a_i \cdot a_k} = \overline{a_i} + \overline{a_k}, \text{ falls } \mathfrak{G} \text{ multiplikativ, } \overline{\mathfrak{G}} \text{ additiv ist,}$$

$$\overline{a_i + a_k} = \overline{a_i} \cdot \overline{a_k}, \text{ falls } \mathfrak{G} \text{ additiv, } \overline{\mathfrak{G}} \text{ multiplikativ ist,}$$

jeweils für alle i und k;

also:

Bild des Produktes = Summe der Bilder

bzw.:

Bild der Summe = Produkt der Bilder.

Der Begriff der eineindeutigen relationstreuen Abbildung einer Gruppe auf eine andere, der natürlich von der Voraussetzung der Endlichkeit unabhängig ist, wird nun nicht nur eine Übertragung unserer bisherigen Betrachtungen auf beliebige Gruppen ermöglichen, sondern nimmt überhaupt eine zentrale Stellung in der Gruppentheorie ein. Wir legen daher (sogleich etwas allgemeiner) fest:

Definition **D (4.3)**

Es sei $\mathfrak{G}$ *eine beliebige, multiplikative oder additive Gruppe und* $\overline{\mathfrak{G}}$ *eine Menge, für deren Elemente eine eindeutige multiplikative oder additive Verknüpfung erklärt ist.*

Dann heißt $\mathfrak{G}$ *isomorph abgebildet auf* $\overline{\mathfrak{G}}$, *in Zeichen* $\mathfrak{G} \overset{\sim}{\longleftrightarrow} \overline{\mathfrak{G}}$; *wenn gilt:*

I: Es existiert eine eineindeutige Abbildung von $\mathfrak{G}$ *auf* $\overline{\mathfrak{G}}$ *vermöge der Zuordnung*

$$a \to \bar{a} \quad \text{mit} \quad a \in \mathfrak{G}, \bar{a} \in \overline{\mathfrak{G}}.$$

II: Diese Zuordnung ist relationstreu, was je nach Vorgabe der Verknüpfungen in $\mathfrak{G}$ *und* $\overline{\mathfrak{G}}$ *einer der vier Beziehungen entspricht:*

$$\left.\begin{aligned} \overline{a \quad b} &= \bar{a} \quad \bar{b} \\ \overline{a + b} &= \bar{a} + \bar{b} \\ \overline{a \quad b} &= \bar{a} + \bar{b} \\ \overline{a + b} &= \bar{a} \quad \bar{b} \end{aligned}\right\} \quad \textit{für alle } a \textit{ und } b \textit{ aus } \mathfrak{G}.$$

Man nennt die Abbildung selbst einen Isomorphismus, $\mathfrak{G}$ *das Original und* $\overline{\mathfrak{G}}$ *das isomorphe Bild*[1]).

Die Abschwächung der Voraussetzung über $\overline{\mathfrak{G}}$ in D(4.3) wird gerechtfertigt durch die

Folgerung **F (4.4)**

Das isomorphe Bild $\overline{\mathfrak{G}}$ *einer Gruppe* $\mathfrak{G}$ *ist selbst Gruppe. Insbesondere überträgt sich etwaige Kommutativität.*

Beweis

Wir führen den Beweis ohne Beschränkung der Allgemeinheit nur für den Fall, daß die Verknüpfungen in $\mathfrak{G}$ und $\overline{\mathfrak{G}}$ multiplikativ sind.

M I: Die für die Elemente von $\overline{\mathfrak{G}}$ erklärte eindeutige Verknüpfung führt aus $\overline{\mathfrak{G}}$ nicht heraus wegen

$$\bar{a} \cdot \bar{b} = \overline{a \cdot b} \in \overline{\mathfrak{G}}.$$

1) Für die Bezeichnung vgl. auch Anhang IIc.

M II: Das assoziative Gesetz in $\overline{\mathfrak{G}}$ folgt aus dem in $\mathfrak{G}$ durch mehrfache Anwendung der Relationstreue:

$$\overline{(a\,b)\,c} = \overline{a\,(b\,c)}$$

$$\overline{(a\,b)}\;\;\bar{c} = \bar{a} \cdot \overline{(b\,c)}$$

$$(\bar{a} \cdot \bar{b}) \cdot \bar{c} = \bar{a} \cdot (\bar{b} \cdot \bar{c})$$

M III: Zur Lösung der Gleichung

$$\bar{a} \cdot \bar{x} = \bar{b}$$

gehen wir auf die Originale a von $\bar{a}$ und b von $\bar{b}$ zurück. In $\mathfrak{G}$ ist aber die Gleichung $ax = b$ mit $x \in \mathfrak{G}$ lösbar. Das Bild $\bar{x}$ von x löst wegen $\overline{a \cdot x} = \bar{a} \cdot \bar{x} = \bar{b}$ die verlangte Gleichung. Entsprechend schließt man für

$$\bar{y} \cdot \bar{a} = \bar{b}.$$

Falls insbesondere $\mathfrak{G}$ kommutativ ist, folgt das gleiche für $\overline{\mathfrak{G}}$ wegen

$$\bar{a} \cdot \bar{b} = \overline{a \cdot b} = \overline{b \cdot a} = \bar{b} \cdot \bar{a}.$$

qed.

Definition **D (4.5)**

Zwei Gruppen heißen isomorph, wenn eine von ihnen auf die andere isomorph abgebildet werden kann.

Satz **S (4.6)**

Die in D (4.5) *erklärte Isomorphie ist eine Äquivalenzrelation und liefert daher eine Einteilung der Menge aller Gruppen in Klassen zueinander isomorpher Gruppen.*

Beweis

1. Reflexivität: Jede Gruppe $\mathfrak{G}$ ist zu sich selbst isomorph vermöge der Zuordnung $a \to a$ für alle $a \in \mathfrak{G}$.

2. Symmetrie: Es sei

$$\mathfrak{G} \overset{\sim}{\longleftrightarrow} \overline{\mathfrak{G}} \text{ vermöge der Zuordnung } a \longrightarrow \bar{a};$$

Dann ist auch

$$\overline{\mathfrak{G}} \overset{\sim}{\longleftrightarrow} \overline{\overline{\mathfrak{G}}} = \mathfrak{G} \text{ vermöge der Zuordnung } \bar{a} \longrightarrow \bar{\bar{a}} = a.$$

Diese Abbildung ist nämlich offensichtlich eineindeutig und auch relationstreu; denn einerseits folgt aus der Relationstreue der ursprünglichen Abbildung $a \cdot b = \overline{\overline{a \cdot b}} = \overline{\bar{a} \cdot \bar{b}}$, andererseits gilt $a \cdot b = \bar{\bar{a}} \cdot \bar{\bar{b}}$, also ergibt sich $\overline{\overline{a \cdot b}} = \bar{\bar{a}} \cdot \bar{\bar{b}}$.

3. Transitivität: Es sei

$$\mathfrak{G} \overset{\sim}{\longleftrightarrow} \bar{\mathfrak{G}} \text{ vermöge der Zuordnung } a \to \bar{a}$$

und

$$\mathfrak{G} \overset{\sim}{\longleftrightarrow} \bar{\bar{\mathfrak{G}}} \text{ vermöge der Zuordnung } \bar{a} \to \bar{\bar{a}};$$

dann ist auch

$$\mathfrak{G} \overset{\sim}{\longleftrightarrow} \bar{\bar{\mathfrak{G}}} \text{ vermöge der Zuordnung } a \to \bar{\bar{a}}.$$

Die Eineindeutigkeit der Abbildung von $\mathfrak{G}$ auf $\bar{\bar{\mathfrak{G}}}$ ist wieder klar: die Relationstreue folgt aus

$$\overline{\overline{a \cdot b}} = \overline{\bar{a} \cdot \bar{b}} = \bar{\bar{a}} \cdot \bar{\bar{b}}.$$

qed.

Folgerung **F (4.7)**

Endliche Gruppen sind genau dann isomorph, wenn ihre Strukturtafeln übereinstimmen.

Dies folgt sofort aus den Betrachtungen, die uns zu D(4.3) führten, und zeigt, daß die Isomorphie in der Tat die angestrebte Verallgemeinerung des Begriffes der strukturellen Gleichheit auf beliebige Gruppen ist. Insbesondere braucht man bei der Behandlung einzelner Gruppen zueinander isomorphe Gruppen nicht gesondert zu untersuchen. Wir führen daher den Begriff der *abstrakten Gruppe* ein als den allgemeinsten Vertreter einer Klasse zueinander isomorpher Gruppen. Die abstrakte Gruppe kennzeichnet die rein gruppenmäßige Struktur aller zu ihr isomorphen Gruppen, unabhängig von jeder darüber hinausgehenden besonderen Eigenschaft der Elemente aller dieser Gruppen.

Aufgaben zu § 4

1. Man stelle die Strukturtafel des Restklassenmoduls mod 5 auf und bediene sich dabei des kleinsten nicht-negativen Repräsentantensystems mod 5.
2. Man beweise die Isomorphie der primen Restklassengruppe mod 12 zur KLEINschen Vierergruppe durch Aufstellen der Strukturtafel.

3. Ebenso beweise man die Isomorphie der multiplikativen Gruppe der vierten Einheitswurzeln zum Restklassenmodul mod 4.

4. Stimmt die Strukturtafel einer endlichen Menge $\mathfrak{M}$, in der eine eindeutige Verknüpfung erklärt ist, mit der einer Gruppe $\mathfrak{G}$ überein, so ist $\mathfrak{M}$ gemäß den Überlegungen vor D(4.3) isomorphes Bild von $\mathfrak{G}$ und damit nach F(4.4) selbst Gruppe. Man zeige auf diese Weise, daß die Menge der Funktionen

$$f_1(\lambda) = \lambda, \qquad f_2(\lambda) = \frac{1}{1-\lambda}, \qquad f_3(\lambda) = \frac{\lambda - 1}{\lambda},$$

$$f_4(\lambda) = 1 - \lambda, \qquad f_5(\lambda) = \frac{1}{\lambda}, \qquad f_6(\lambda) = \frac{\lambda}{\lambda - 1}$$

mit der Verknüpfung

$$[f_i \cdot f_k](\lambda) = f_k(f_i(\lambda))$$

eine multiplikative Gruppe ist, da sie die gleiche Strukturtafel wie die symmetrische Gruppe $\mathfrak{S}_3$ hat. (Zur geometrischen Bedeutung dieser Ausdrücke können wir hier nur bemerken: Ist λ das Doppelverhältnis von vier Punkten, so geben die $f_i(\lambda)$ die Werte des Doppelverhältnisses dieser vier Punkte bei allen Vertauschungen ihrer Reihenfolge an.)

5. Die Zuordnung

$$x \to \bar{x} = \log x$$

vermittelt eine isomorphe Abbildung der multiplikativen Gruppe aller positiven reellen Zahlen auf die additive Gruppe aller reellen Zahlen.

6. Bei einem Isomorphismus $\mathfrak{G} \overset{\sim}{\leftarrow} \overline{\mathfrak{G}}$ zwischen multiplikativen Gruppen werden die Einselemente aufeinander abgebildet. Weiterhin gilt:

Bild des Inversen = Inverses des Bildes.

§ 5. Komplexe und Untergruppen

Wir wollen im folgenden Beziehungen untersuchen, die zwischen beliebigen Teilmengen von Elementen einer Gruppe bestehen. Solche Beziehungen sind uns schon durch die Mengenlehre gegeben und werden durch die Zeichen

$$=,\ \subseteq,\ \supseteq,\ <,\ >,\ \cap,\ \cup$$

ausgedrückt. Darüber hinaus gestattet jedoch die in der Gruppe erklärte Verknüpfung weitere Begriffsbildungen. Es ist daher auch üblich, in der Gruppentheorie die nichtleeren Teilmengen Komplexe zu nennen.

Definition **D (5.1)**

Aus zwei beliebigen Komplexen $\mathfrak{A}$ *und* $\mathfrak{B}$ *einer Gruppe* $\mathfrak{G}$ *entsteht durch die Bildung aller Produkte* $a \cdot b$ *mit* $a \in \mathfrak{A}$ *und* $b \in \mathfrak{B}$ *ein neuer Komplex von* $\mathfrak{G}$, *das eindeutig bestimmte Komplexprodukt* $\mathfrak{A} \cdot \mathfrak{B}$ *von* $\mathfrak{A}$ *und* $\mathfrak{B}$.

Bildet man alle Inversen a^{-1} *der Elemente* a *eines Komplexes* $\mathfrak{A}$ *von* $\mathfrak{G}$, *so erhält man wieder einen Komplex von* $\mathfrak{G}$, *den zu* $\mathfrak{A}$ *eindeutig bestimmten inversen Komplex* $\mathfrak{A}^{-1}$.

So besteht z. B. das Komplexprodukt der beiden Komplexe

$$\mathfrak{A} = \left\{ \begin{pmatrix} 123 \\ 123 \end{pmatrix}, \begin{pmatrix} 123 \\ 231 \end{pmatrix}, \begin{pmatrix} 123 \\ 213 \end{pmatrix} \right\} \quad \text{und} \quad \mathfrak{B} = \left\{ \begin{pmatrix} 123 \\ 312 \end{pmatrix}, \begin{pmatrix} 123 \\ 132 \end{pmatrix} \right\}$$

der symmetrischen Gruppe $\mathfrak{S}_3$ aus den folgenden Permutationen:

$$\begin{pmatrix} 123 \\ 123 \end{pmatrix} \cdot \begin{pmatrix} 123 \\ 312 \end{pmatrix} = \begin{pmatrix} 123 \\ 312 \end{pmatrix} \qquad \begin{pmatrix} 123 \\ 123 \end{pmatrix} \cdot \begin{pmatrix} 123 \\ 132 \end{pmatrix} = \begin{pmatrix} 123 \\ 132 \end{pmatrix}$$

$$\begin{pmatrix} 123 \\ 231 \end{pmatrix} \cdot \begin{pmatrix} 123 \\ 312 \end{pmatrix} = \begin{pmatrix} 123 \\ 123 \end{pmatrix} \qquad \begin{pmatrix} 123 \\ 231 \end{pmatrix} \cdot \begin{pmatrix} 123 \\ 132 \end{pmatrix} = \begin{pmatrix} 123 \\ 321 \end{pmatrix}$$

$$\begin{pmatrix} 123 \\ 213 \end{pmatrix} \cdot \begin{pmatrix} 123 \\ 312 \end{pmatrix} = \begin{pmatrix} 123 \\ 132 \end{pmatrix} \qquad \begin{pmatrix} 123 \\ 213 \end{pmatrix} \cdot \begin{pmatrix} 123 \\ 132 \end{pmatrix} = \begin{pmatrix} 123 \\ 312 \end{pmatrix}.$$

Also ist

$$\mathfrak{A} \cdot \mathfrak{B} = \left\{ \begin{pmatrix} 123 \\ 312 \end{pmatrix}, \begin{pmatrix} 123 \\ 123 \end{pmatrix}, \begin{pmatrix} 123 \\ 132 \end{pmatrix}, \begin{pmatrix} 123 \\ 321 \end{pmatrix} \right\}.$$

Ferner sind

$$\mathfrak{A}^{-1} = \left\{ \begin{pmatrix} 123 \\ 123 \end{pmatrix}, \begin{pmatrix} 123 \\ 312 \end{pmatrix}, \begin{pmatrix} 123 \\ 213 \end{pmatrix} \right\}$$

bzw.

$$\mathfrak{B}^{-1} = \left\{ \begin{pmatrix} 123 \\ 231 \end{pmatrix}, \begin{pmatrix} 123 \\ 132 \end{pmatrix} \right\}$$

die zu $\mathfrak{A}$ bzw. $\mathfrak{B}$ inversen Komplexe.

Folgerung **F (5.2)**

Für die in D(5.1) erklärten Begriffsbildungen gilt:

a) Die Komplexmultiplikation umfaßt die Multiplikation der Gruppenelemente, da jedes Gruppenelement für sich als Komplex aufgefaßt werden kann.

b) Die Komplexmultiplikation ist assoziativ:

$$(\mathfrak{A} \cdot \mathfrak{B}) \cdot \mathfrak{C} = \mathfrak{A} \cdot (\mathfrak{B} \cdot \mathfrak{C}),$$

da die ihr zugrunde liegende Multiplikation der Gruppenelemente assoziativ ist (vgl. Aufg. 3).

c) Aus dem gleichen Grunde ist die Komplexmultiplikation in nicht-abelschen Gruppen im allgemeinen nicht kommutativ. Besteht aber eine Gleichung

$$\mathfrak{A} \cdot \mathfrak{B} = \mathfrak{B} \cdot \mathfrak{A},$$

so sagt diese im Sinne der Gleichheitsdefinition für Mengen nur aus, daß jedes Produkt $a \cdot b \in \mathfrak{A} \cdot \mathfrak{B}$ gleich einem Produkt $b' \cdot a' \in \mathfrak{B} \cdot \mathfrak{A}$ ist und umgekehrt. Es kann dabei $a \neq a'$, $b \neq b'$ sein, d. h., aus $\mathfrak{A} \cdot \mathfrak{B} = \mathfrak{B} \cdot \mathfrak{A}$ folgt nur $a \cdot b = b' \cdot a'$, aber nicht notwendig $a \cdot b = b \cdot a$ (vgl. Aufg. 4).

d) Es gibt bezüglich der Komplexmultiplikation einen eindeutig bestimmten Einheitskomplex $\mathfrak{E}$, der nur aus dem Einselement $e \in \mathfrak{G}$ besteht:

$$\mathfrak{E} \cdot \mathfrak{A} = \mathfrak{A} \cdot \mathfrak{E} = \mathfrak{A}.$$

e) Es ist klar, daß stets $\mathfrak{A}^{-1} \cdot \mathfrak{A} \supseteq \mathfrak{E}$ gilt. Jedoch ist $\mathfrak{A}^{-1} \cdot \mathfrak{A} = \mathfrak{E}$ dann und nur dann, wenn $\mathfrak{A}$ und damit $\mathfrak{A}^{-1}$ nur aus einem Element bestehen. Die Behauptung mit „dann" folgt unmittelbar. Statt der Behauptung mit „nur dann" beweisen wir gleich weitergehend, daß es zu einem Komplex $\mathfrak{A}$, der wenigstens zwei verschiedene Elemente a und a' enthält, keinen Komplex $\mathfrak{B}$ gibt, der $\mathfrak{B} \cdot \mathfrak{A} = \mathfrak{E}$ erfüllt. Ist nämlich $b \in \mathfrak{B}$, so enthält $\mathfrak{B} \cdot \mathfrak{A}$ die Elemente $b \cdot a$ und $b \cdot a'$. Wegen *M III** ist $b \cdot a \neq b \cdot a'$; es können aber nicht $b \cdot a$ und $b \cdot a'$ in $\mathfrak{E}$ enthalten sein.

Die Menge aller Komplexe einer Gruppe $\mathfrak{G} \neq \mathfrak{E}$ bildet also selbst keine Gruppe, worauf man wegen b), d) und der in der Literatur üblichen, aber unglücklichen Bezeichnung „inverser Komplex" für den Komplex der Inversen eines Komplexes kommen könnte.

f) Der inverse Komplex des inversen Komplexes ist der ursprüngliche Komplex:

$$(\mathfrak{A}^{-1})^{-1} = \mathfrak{A}.$$

Dies ergibt sich aus der eindeutigen Bestimmtheit des Inversen von Gruppenelementen.

g) Aus $\mathfrak{A} \subseteq \mathfrak{B}$ folgt $\mathfrak{A} \cdot \mathfrak{C} \subseteq \mathfrak{B} \cdot \mathfrak{C}$ und $\mathfrak{C} \cdot \mathfrak{A} \subseteq \mathfrak{C} \cdot \mathfrak{B}$ für jeden Komplex $\mathfrak{C}$ der Gruppe.

h) Aus $\mathfrak{A} \subseteq \mathfrak{B}$ folgt $\mathfrak{A}^{-1} \subseteq \mathfrak{B}^{-1}$.

Nachdem wir diese einfachen Hilfsmittel bereitgestellt haben, kommen wir zu denjenigen Untersuchungen, die die Bedeutung des Komplexbegriffes für die Gruppentheorie ausmachen. Dazu beschäftigen wir uns insbesondere mit solchen Komplexen, die selbst Gruppeneigenschaft aufweisen:

Definition **D (5.3)**

Ein Komplex $\mathfrak{H}$ einer Gruppe $\mathfrak{G}$ heißt eine Untergruppe von $\mathfrak{G}$, wenn die Elemente von $\mathfrak{H}$ mit der in $\mathfrak{G}$ festgelegten Verknüpfungsvorschrift für sich die Gruppenaxiome erfüllen.

So ist z. B. die KLEINsche Vierergruppe eine Untergruppe der symmetrischen Gruppe $\mathfrak{S}_4$; weitere Beispiele entnimmt man mühelos aus B(2.1), B(2.2) und B(2.7) sowie den Aufgaben 10, 14, 15 und 16.

Nach D(5.3) ist klar, daß Untergruppen von Untergruppen selbst Untergruppen der ursprünglichen Gruppe sind. Weiterhin ergibt sich die sehr einfache, aber grundlegende

Folgerung **F (5.4)**

Das Einselement einer Gruppe $\mathfrak{G}$ stimmt mit dem Einselement jeder ihrer Untergruppen $\mathfrak{H}$ überein; ebenso ist das zu einem Element $a \in \mathfrak{H}$ inverse Element in $\mathfrak{H}$ gleich dem zu a inversen Element in $\mathfrak{G}$.

Beweis

Wir bezeichnen das eindeutig bestimmte Einselement von $\mathfrak{H}$ mit $e_{\mathfrak{H}}$, dasjenige von $\mathfrak{G}$ mit $e_{\mathfrak{G}}$. Für jedes Element $a \in \mathfrak{H}$ gilt dann:

$$e_{\mathfrak{H}} \cdot a = a$$

sowie

$$e_{\mathfrak{G}} \cdot a = a,$$

wenn wir berücksichtigen, daß wegen $\mathfrak{H} \subseteq \mathfrak{G}$ auch $a \in \mathfrak{G}$ ist. Betrachten wir beide Gleichungen in $\mathfrak{G}$, ergibt sich wegen *M III**:

$$e_{\mathfrak{H}} = e_{\mathfrak{G}}.$$

Analog schließt man für die Inversen (vgl. Aufg. 6). qed.

Jede Gruppe $\mathfrak{G}$ enthält zwei triviale Untergruppen, nämlich $\mathfrak{G}$ selbst und die nur aus dem Einselement e bestehende Einheitsgruppe $\mathfrak{E}$. Darüber hinaus kann man Kriterien angeben, welche Komplexe Untergruppen sind.

Satz **S (5.5)**

Damit ein Komplex $\mathfrak{H}$ einer Gruppe $\mathfrak{G}$ Untergruppe von $\mathfrak{G}$ ist, ist notwendig und hinreichend, daß

$$\mathfrak{H} \cdot \mathfrak{H} \subseteq \mathfrak{H} \quad \textit{und} \quad \mathfrak{H}^{-1} \subseteq \mathfrak{H}$$

gilt, d. h., daß $\mathfrak{H}$ mit zwei Elementen auch deren Produkt und zu jedem Element das Inverse enthält.

Beweis

Die Notwendigkeit dieser Bedingungen ist klar. Sie sind auch hinreichend, denn mit ihnen sind für $\mathfrak{H}$ bereits alle Gruppenaxiome erfüllt. So besagt $\mathfrak{H} \cdot \mathfrak{H} \subseteq \mathfrak{H}$, daß die Multiplikation aus $\mathfrak{H}$ nicht herausführt, als Multiplikation innerhalb $\mathfrak{G}$ ist sie eindeutig; beides zusammen ergibt *M I. M II* gilt in $\mathfrak{H}$, weil es in ganz $\mathfrak{G}$ gilt. $M\,III_2$ ist mit $\mathfrak{H}^{-1} \subseteq \mathfrak{H}$ erfüllt. Damit gilt $M\,III_1$ ebenfalls, weil mit $a \in \mathfrak{H}$, also $a^{-1} \in \mathfrak{H}$ auch $a^{-1} \cdot a = e \in \mathfrak{H}$. qed.

Die beiden Bedingungen aus S (5.5) kann man in eine einzige zusammenfassen:

Satz **S (5.6)**

Damit ein Komplex $\mathfrak{H}$ einer Gruppe $\mathfrak{G}$ Untergruppe von $\mathfrak{G}$ ist, ist notwendig und hinreichend, daß

$$\mathfrak{H} \cdot \mathfrak{H}^{-1} \subseteq \mathfrak{H}$$

gilt, d. h., daß $\mathfrak{H}$ mit zwei Elementen a, b auch das Produkt $a \cdot b^{-1}$ enthält.

Beweis

Wir zeigen, daß die Bedingung $\mathfrak{H} \cdot \mathfrak{H}^{-1} \subseteq \mathfrak{H}$ äquivalent ist zu den beiden Bedingungen von S(5.5). Einerseits folgt nämlich aus $\mathfrak{H} \cdot \mathfrak{H} \subseteq \mathfrak{H}$ und $\mathfrak{H}^{-1} \subseteq \mathfrak{H}$ durch Multiplikation der letzten Relation von links mit $\mathfrak{H}$ wegen F(5.2g)

$$\mathfrak{H} \cdot \mathfrak{H}^{-1} \subseteq \mathfrak{H} \cdot \mathfrak{H} \subseteq \mathfrak{H}.$$

Umgekehrt folgt aus $\mathfrak{H} \cdot \mathfrak{H}^{-1} \subseteq \mathfrak{H}$ wegen $\mathfrak{E} \subseteq \mathfrak{H} \cdot \mathfrak{H}^{-1} \subseteq \mathfrak{H}$ sofort

$$\mathfrak{E} \cdot \mathfrak{H}^{-1} = \mathfrak{H}^{-1} \subseteq \mathfrak{H}.$$

Daraus ergibt sich wegen F(5.2h) $\mathfrak{H} \subseteq \mathfrak{H}^{-1}$. Multiplikation von links mit $\mathfrak{H}$ liefert:

$$\mathfrak{H} \cdot \mathfrak{H} \subseteq \mathfrak{H} \cdot \mathfrak{H}^{-1} \subseteq \mathfrak{H}.$$

qed.

Folgerung **F(5.7)**

Eine Untergruppe $\mathfrak{H}$ von $\mathfrak{G}$ erfüllt sogar die Relationen:

$$\mathfrak{H} \cdot \mathfrak{H} = \mathfrak{H}, \quad \mathfrak{H}^{-1} = \mathfrak{H}, \quad \mathfrak{H} \cdot \mathfrak{H}^{-1} = \mathfrak{H}.$$

Als Kriterium für die Untergruppeneigenschaft genügen also entsprechend den Sätzen S(5.5) und S(5.6) die genannten Relationen mit dem Zeichen $\subseteq$. Sie gelten dann aber von selbst mit dem Gleichheitszeichen.

Beweis

Wegen $\mathfrak{H} \supseteq \mathfrak{E}$ folgt $\mathfrak{H} \cdot \mathfrak{H} \supseteq \mathfrak{E} \cdot \mathfrak{H} = \mathfrak{H}$; mit $\mathfrak{H} \cdot \mathfrak{H} \subseteq \mathfrak{H}$ gibt das $\mathfrak{H} \cdot \mathfrak{H} = \mathfrak{H}$. Die beiden Relationen $\mathfrak{H}^{-1} \subseteq \mathfrak{H}$ und $\mathfrak{H}^{-1} \supseteq \mathfrak{H}$ traten bereits im Beweis von S(5.6) auf. $\mathfrak{H} \cdot \mathfrak{H}^{-1} = \mathfrak{H}$ ist Folge der beiden anderen Relationen.

qed.

Für endliche Komplexe kann man das Kriterium S(5.5) wesentlich vereinfachen:

Satz **S(5.8)**

Damit ein endlicher Komplex $\mathfrak{H}$ einer Gruppe $\mathfrak{G}$ Untergruppe von $\mathfrak{G}$ ist, ist notwendig und hinreichend, daß

$$\mathfrak{H} \cdot \mathfrak{H} \subseteq \mathfrak{H}$$

gilt, d. h., daß $\mathfrak{H}$ mit je zwei Elementen auch ihr Produkt enthält.

Beweis

Nach S(1.10) bilden *M I*, *M II*, *M III** bereits ein Axiomensystem für endliche Gruppen. *M II* und *M III** sind aber für die Elemente von $\mathfrak{G}$, also erst recht für diejenigen von $\mathfrak{H}$ erfüllt. *M I* folgt aus $\mathfrak{H} \cdot \mathfrak{H} \subseteq \mathfrak{H}$ wie im Beweis von S(5.5). Damit ist gezeigt, daß die Bedingung $\mathfrak{H} \cdot \mathfrak{H} \subseteq \mathfrak{H}$ hinreichend ist; ihre Notwendigkeit ist klar.

qed.

Wir wollen schließlich noch ein Kriterium dafür angeben, daß ein beliebiger Komplex einer Gruppe in einer ihrer Untergruppen enthalten ist. Dieses Kriterium gilt dann erst recht für einzelne Gruppenelemente.

Satz **S (5.9)**

Damit ein Komplex $\mathfrak{A}$ einer Gruppe $\mathfrak{G}$ in einer Untergruppe $\mathfrak{H}$ von $\mathfrak{G}$ enthalten ist, ist notwendig und hinreichend, daß

$$\mathfrak{A} \cdot \mathfrak{H} = \mathfrak{H}$$

erfüllt ist. Das gleiche gilt für

$$\mathfrak{H} \cdot \mathfrak{A} = \mathfrak{H}.$$

Beweis

1. Wir gehen aus von $\mathfrak{A}\mathfrak{H} = \mathfrak{H}$. Wegen $\mathfrak{E} \subseteq \mathfrak{H}$ folgt

$$\mathfrak{A} = \mathfrak{A}\mathfrak{E} \subseteq \mathfrak{A}\mathfrak{H} = \mathfrak{H},$$

also $\mathfrak{A} \subseteq \mathfrak{H}$.

2. Umgekehrt sei $\mathfrak{A} \subseteq \mathfrak{H}$. Dann folgt einmal $\mathfrak{A}\mathfrak{H} \subseteq \mathfrak{H}\mathfrak{H} \subseteq \mathfrak{H}$, zum anderen $\mathfrak{A}^{-1} \subseteq \mathfrak{H}^{-1} \subseteq \mathfrak{H}$ und daher

$$\mathfrak{E} \subseteq \mathfrak{A}\mathfrak{A}^{-1} \subseteq \mathfrak{A}\mathfrak{H},$$

$$\mathfrak{H} = \mathfrak{E}\mathfrak{H} \subseteq \mathfrak{A}\mathfrak{H}\mathfrak{H} \subseteq \mathfrak{A}\mathfrak{H}.$$

Aus $\mathfrak{A}\mathfrak{H} \subseteq \mathfrak{H}$ und $\mathfrak{H} \subseteq \mathfrak{A}\mathfrak{H}$ folgt $\mathfrak{A}\mathfrak{H} = \mathfrak{H}$.

3. Analog schließt man für $\mathfrak{H}\mathfrak{A} = \mathfrak{H}$.

qed.

Wir wollen untersuchen, wann Komplexverknüpfungen von Untergruppen wieder Untergruppen ergeben. Es gelten folgende Aussagen:

Satz **S (5.10)**

Der Durchschnitt $\mathfrak{A} \cap \mathfrak{B} \cap \ldots$ *von beliebig vielen Untergruppen* $\mathfrak{A}, \mathfrak{B}, \ldots$ *einer Gruppe* $\mathfrak{G}$ *ist wieder Untergruppe von* $\mathfrak{G}$.

Beweis

Der Durchschnitt ist nicht leer, da jede Untergruppe $\mathfrak{A}, \mathfrak{B}, \ldots$ das Einselement e enthält. Ferner seien x und y zwei Elemente von $\mathfrak{A} \cap \mathfrak{B} \cap \ldots$, d. h., x und y sind beide in sämtlichen Komponenten des betrachteten Durchschnittes enthalten. Da alle Komponenten Untergruppen sind, sind auch $x \cdot y$ und x^{-1} in allen Komponenten enthalten. Damit ist aber nach S (5.5) $\mathfrak{A} \cap \mathfrak{B} \cap \ldots$ Untergruppe von $\mathfrak{G}$.

qed.

Bemerkung

Im Gegensatz zu S (5.10) ist im allgemeinen schon die Vereinigung $\mathfrak{A} \cup \mathfrak{B}$ von zwei Untergruppen nicht wieder Untergruppe (vgl. Aufg. 11).

Satz **S (5.11)**

Das Komplexprodukt $\mathfrak{A} \cdot \mathfrak{B}$ *zweier Untergruppen* $\mathfrak{A}$ *und* $\mathfrak{B}$ *einer Gruppe* $\mathfrak{G}$ *ist dann und nur dann Untergruppe von* $\mathfrak{G}$, *wenn gilt:*

$$\mathfrak{A} \cdot \mathfrak{B} = \mathfrak{B} \cdot \mathfrak{A}.$$

Beweis

Die Gesamtheit $(\mathfrak{A}\,\mathfrak{B})^{-1}$ aller Inversen $(ab)^{-1}$ von Elementen ab aus $\mathfrak{A}\,\mathfrak{B}$ ist die Gesamtheit aller $b^{-1}a^{-1}$, also $\mathfrak{B}^{-1}\mathfrak{A}^{-1}$. Sind nun $\mathfrak{A}$ und $\mathfrak{B}$ bei der Multiplikation vertauschbare Untergruppen, so folgt nach F (5.7):

$$(\mathfrak{A}\,\mathfrak{B})\,(\mathfrak{A}\,\mathfrak{B})^{-1} = \mathfrak{A}\,\mathfrak{B}\,\mathfrak{B}^{-1}\,\mathfrak{A}^{-1} = \mathfrak{A}\,\mathfrak{B}\,\mathfrak{B}\,\mathfrak{A} = \mathfrak{A}\,\mathfrak{B},$$

d. h., $\mathfrak{A}\mathfrak{B}$ erfüllt die Bedingung aus S (5.6) und ist Untergruppe. Ist umgekehrt $\mathfrak{A}\mathfrak{B}$ Untergruppe, erhält man mit einer analogen Überlegung:

$$\mathfrak{A}\mathfrak{B} = (\mathfrak{A}\mathfrak{B})^{-1} = \mathfrak{B}^{-1}\mathfrak{A}^{-1} = \mathfrak{B}\mathfrak{A}.$$

qed.

Zu einer weiteren Begriffsbildung führt uns der Gedanke, jeden Komplex einer Gruppe in eine möglichst kleine Untergruppe einzubetten.

Definition **D (5.12)**

Unter der von einem Komplex $\mathfrak{A}$ aus der Gruppe $\mathfrak{G}$ erzeugten Untergruppe $\langle\mathfrak{A}\rangle$ versteht man den Durchschnitt aller derjenigen Untergruppen von $\mathfrak{G}$, die $\mathfrak{A}$ enthalten.

Satz **S (5.13)**

Die von einem Komplex $\mathfrak{A}$ einer Gruppe $\mathfrak{G}$ erzeugte Untergruppe $\langle\mathfrak{A}\rangle$ enthält genau alle Produkte[1]*, die man mit je endlich vielen Elementen aus $\mathfrak{A}$ und $\mathfrak{A}^{-1}$ bilden kann. Sie ist in jeder Untergruppe $\mathfrak{H}$ von $\mathfrak{G}$ mit $\mathfrak{H} \supseteq \mathfrak{A}$ enthalten, ist also in diesem Sinne die kleinste Untergruppe, die $\mathfrak{A}$ umfaßt.*

Beweis

Die Menge der genannten Elemente bildet nach S (5.5) selbst eine Untergruppe $\mathfrak{U}$ von $\mathfrak{G}$. Offensichtlich gilt $\mathfrak{A} \subseteq \mathfrak{U}$. Damit ist $\mathfrak{U}$ eine der Komponenten des in D (5.12) erklärten Durchschnittes, also ist $\langle\mathfrak{A}\rangle \subseteq \mathfrak{U}$. Umgekehrt gilt $\langle\mathfrak{A}\rangle \supseteq \mathfrak{U}$, weil $\langle\mathfrak{A}\rangle \supseteq \mathfrak{A}$ nach D (5.12) und $\langle\mathfrak{A}\rangle$ Untergruppe ist, aus welcher Produkt- und Inversenbildung nicht herausführt.
Weiterhin ist $\langle\mathfrak{A}\rangle$ in jeder Untergruppe $\mathfrak{H}$ von $\mathfrak{G}$ mit $\mathfrak{H} \supseteq \mathfrak{A}$ enthalten, denn $\mathfrak{H}$ ist dann ja Komponente des Durchschnittes, der $\langle\mathfrak{A}\rangle$ gemäß D (5.12) definiert.

qed.

Im vorangehenden haben wir zu jedem Komplex $\mathfrak{A}$ mit $\langle\mathfrak{A}\rangle$ eine eindeutig bestimmte Untergruppe erklärt, die von $\mathfrak{A}$ erzeugt wird. Offenbar ist $\mathfrak{A} = \langle\mathfrak{A}\rangle$, falls $\mathfrak{A}$ selbst Untergruppe ist. Es erhebt sich nun die umgekehrte Frage, zu einer vorgegebenen Untergruppe $\mathfrak{H}$ Komplexe $\mathfrak{A}$ zu finden, die $\mathfrak{H}$ erzeugen, d. h. für die $\langle\mathfrak{A}\rangle = \mathfrak{H}$ gilt. Diese Aufgabe hat immer mehrere Lösungen, falls $\mathfrak{H}$ verschieden von der Einheitsgruppe $\mathfrak{E}$ ist. Dann erzeugt nämlich z. B. sowohl der Komplex $\mathfrak{H}$ selbst als auch der aus allen vom Einselement verschiedenen Elementen von $\mathfrak{H}$ bestehende Komplex die Gruppe $\mathfrak{H}$.

---

1) Dabei sind auch die Elemente von $\mathfrak{A}$ bzw. $\mathfrak{A}^{-1}$ selbst als „Produkte aus nur einem Faktor" mit gemeint.

Man kann diese Fragestellung dahingehend verschärfen, daß man zu einer Untergruppe $\mathfrak{H}$ ein möglichst kleines *Erzeugendensystem* sucht, d. h., einen Komplex $\mathfrak{A}$, der selbst noch die Gruppe $\mathfrak{H}$ erzeugt, jeder echte Teilkomplex von $\mathfrak{A}$ dagegen eine echte Untergruppe von $\mathfrak{H}$. Dieses Problem ist nicht immer lösbar, andererseits sind im Falle der Lösbarkeit meist mehrere Lösungen vorhanden. Wir haben hier eine tiefliegende und grundlegende Problemstellung der gesamten Mathematik vor uns, die wir jedoch nur in einigen wichtigen Spezialfällen ausführlicher behandeln können.

Es verbleibt die Aufgabe, die Ergebnisse dieses Paragraphen für additive abelsche Gruppen, d. h. für Moduln auszusprechen. Wir verzichten jedoch von nun an darauf, dies bis in alle Einzelheiten auszuführen, und beschränken uns auf die wichtigsten Begriffsbildungen und vielgebrauchte Sätze.

So entspricht dem Komplexprodukt die *Komplexsumme* $\mathfrak{A} + \mathfrak{B}$ und dem inversen Komplex der *entgegengesetzte Komplex* $(-\mathfrak{A})$. Im Gegensatz zur Komplexmultiplikation ist die Komplexaddition stets kommutativ. Die additiven Untergruppen bezeichnet man auch als *Untermoduln*. Zur Feststellung der Untermoduleigenschaft eines Komplexes $\mathfrak{H}$ ist das S(5.6) entsprechende Kriterium, daß $\mathfrak{H}$ mit zwei Elementen a und b auch die Differenz $a - b$ enthält, das wichtigste. Aus S(5.9) entnehmen wir, daß ein Komplex $\mathfrak{A}$ genau dann in einem Untermodul $\mathfrak{H}$ enthalten ist, wenn $\mathfrak{A} + \mathfrak{H} = \mathfrak{H}$ gilt. An Stelle des Kriteriums in S(5.11) tritt die Aussage, daß die Komplexsumme zweier Untermoduln stets selbst Untermodul ist. Zu einem Komplex $\mathfrak{A}$ existiert auch hier ein eindeutig bestimmter, von ihm erzeugter Untermodul $\langle\mathfrak{A}\rangle$, während die umgekehrte Fragestellung dieselbe Problematik wie bei multiplikativen Gruppen aufweist.

Aufgaben zu § 5

1. Wieviel Komplexe kann man mit den Elementen der Gruppe $\mathfrak{S}_3$ aufstellen?
2. Man bilde einige Beispiele für den Durchschnitt, die Vereinigung, das Komplexprodukt sowie für den inversen Komplex von Komplexen der Gruppe $\mathfrak{S}_3$.

3. Man gebe Beispiele für die Gültigkeit des Assoziativgesetzes der Komplexmultiplikation.

4. Man wähle zwei Komplexe $\mathfrak{A}$ und $\mathfrak{B}$ der Gruppe $\mathfrak{S}_3$ aus, die sich kommutativ multiplizieren, ohne daß dies für ihre Elemente der Fall ist.

5. Man zeige, daß stets $(\mathfrak{A} \cup \mathfrak{B}) \cdot \mathfrak{C} = \mathfrak{A}\mathfrak{C} \cup \mathfrak{B}\mathfrak{C}$ gilt, aber nur $(\mathfrak{A} \cap \mathfrak{B}) \cdot \mathfrak{C} \subseteq \mathfrak{A}\mathfrak{C} \cap \mathfrak{B}\mathfrak{C}$, und bilde Beispiele in $\mathfrak{S}_3$.

6. Man führe den zweiten Teil des Beweises von F(5.4) durch.

7. Man beweise S(5.6) ohne Verwendung der Komplexschreibweise, indem man auf die einzelnen Elemente zurückgeht.

8. Man beweise den zweiten Teil der Behauptung von S(5.9).

9. Man überlege sich, daß die in F(5.7) genannten Relationen $\mathfrak{H}\mathfrak{H} = \mathfrak{H}$ und $\mathfrak{H}\mathfrak{H}^{-1} = \mathfrak{H}$ unmittelbar aus S(5.9) folgen.

10. Man stelle sämtliche Untergruppen der Gruppe $\mathfrak{S}_3$ auf und prüfe die Kriterien S(5.5), S(5.6), F(5.7), S(5.8) sowie S(5.9) an Beispielen nach.

11. Man bestätige die Bemerkung nach S(5.10) durch ein Beispiel in $\mathfrak{S}_3$.

12. Man bilde ein Beispiel für S(5.11) in $\mathfrak{S}_3$.

13. Man gebe zu jeder echten Untergruppe von $\mathfrak{S}_3$ sämtliche Erzeugendensysteme an und für $\mathfrak{S}_3$ solche, die möglichst klein sind.

14. Im Modul $\mathfrak{G}$ der ganzen Zahlen wird jeder vom Nullmodul verschiedene Untermodul $\mathfrak{H}$ von einer positiven ganzen Zahl erzeugt, und zwar von der kleinsten positiven ganzen Zahl m, die in $\mathfrak{H}$ enthalten ist.

15. Im Modul aller Vektoren des dreidimensionalen Raumes bilden alle in einer Ebene bzw. in einer Geraden liegenden Vektoren Untermoduln.

16. Die in B(2.4) behandelte volle lineare Gruppe $\mathfrak{G}$ vom Grad n enthält u. a. folgende Untergruppen:

    a) Die Gruppe $\mathfrak{U}$ aller unimodularen Matrizen vom Typ (n, n), das sind diejenigen regulären Matrizen, deren Determinante den Wert ± 1 hat;

    b) die Gruppe $\mathfrak{U}_+$ aller eigentlich unimodularen Matrizen vom Typ (n, n), das sind diejenigen unimodularen Matrizen mit der Determinante $+1$;

    c) die Gruppe $\mathfrak{O}$ aller orthogonalen Matrizen vom Typ (n, n), das sind diejenigen regulären Matrizen, für die transponierte und inverse Matrix übereinstimmen (die zu einer Matrix A transponierte Matrix A^T entsteht bekanntlich dadurch, daß man die Zeilen als Spalten schreibt);

    d) die Gruppe $\mathfrak{O}_+$ aller eigentlich orthogonalen Matrizen vom Typ (n, n), das sind diejenigen orthogonalen Matrizen mit der Determinante $+1$.

    Man beweise in allen vier Fällen die Untergruppeneigenschaft und untersuche das Verhältnis dieser Untergruppen zueinander.

17. In der Gruppe $\mathfrak{T}$ aller Transformationen einer abzählbaren Menge $\mathfrak{M}$ bilden diejenigen, die nur endlich viele Elemente von $\mathfrak{M}$ verändern, eine Untergruppe, die sog. abzählbare symmetrische Gruppe $\mathfrak{S}_a$.

§ 6. Zyklische Gruppen

Im Anschluß an die am Ende des vorigen Paragraphen aufgeworfene Problemstellung beschäftigen wir uns mit solchen Gruppen, für die ein nur aus einem Element bestehendes Erzeugendensystem existiert.

Definition **D (6.1)**

Eine Gruppe $\mathfrak{G}$ *heißt zyklisch, wenn sie von einem Element* $a \in \mathfrak{G}$ *erzeugt werden kann. Man nennt* a *erzeugendes oder auch primitives Element von* $\mathfrak{G} = \langle a \rangle$.

Aus S(5.13) ergibt sich:

Folgerung **F (6.2)**

Eine zyklische Gruppe $\mathfrak{G} = \langle a \rangle$ *besteht aus genau allen Potenzen* a^i *mit ganzzahligen Exponenten* $i \gtreqless 0$; *daher ist eine zyklische Gruppe stets abelsch. In additiver Schreibweise entsprechen den Potenzen ganzzahlige Vielfache des erzeugenden Elementes.*

Wir haben bereits die folgenden Beispiele zyklischer Gruppen kennengelernt:

1. Die Gruppe der n-ten Einheitswurzeln mit den primitiven n-ten Einheitswurzeln als Erzeugenden.

2. Sämtliche echten Untergruppen der Gruppe $\mathfrak{S}_3$; die Erzeugenden wurden in Aufgabe 13 von § 5 bestimmt.

3. Den Modul der ganzen Zahlen, erzeugt von $(+1)$ oder (-1).

4. Den Restklassenmodul mod m, etwa erzeugt von der Restklasse [1].

Die Struktur zyklischer Gruppen ist besonders übersichtlich. Wir können zunächst eine grundlegende Unterscheidung durchführen:

Satz **S (6.3)**

Für eine zyklische Gruppe $\mathfrak{G} = \langle a \rangle$ *gibt es die beiden folgenden Möglichkeiten:*

a) *Die Potenzen von* a *sind alle voneinander verschieden. Dann ist* $\mathfrak{G}$ *eine unendliche zyklische Gruppe, auch freie zyklische Gruppe genannt. In diesem Falle heißt* a *ein Element von unendlicher Ordnung oder ein freies Element (Beispiel* 3).

b) *Die Potenzen von a sind nicht alle voneinander verschieden. Dann ist* $\mathfrak{G}$ *eine endliche zyklische Gruppe. Die Ordnung n von* $\mathfrak{G}$ *ist bestimmt durch die Gleichung* $a^n = e$ *mit minimalem Exponenten* $n > 0$, *und a heißt ein Element der Ordnung n* (*Beispiele* 1, 2, 4).

Beweis

a) Dieser Teil des Satzes ergibt sich unmittelbar aus F (6.2).

b) Nach Voraussetzung existieren wenigstens zwei übereinstimmende Potenzen $a^h = a^k$ mit $h \neq k$. Wir können ohne Beschränkung der Allgemeinheit $h > k$ annehmen. Dann folgt die Gleichung $a^{h-k} = e$ mit positivem Exponenten $h - k$. Es sei n der kleinste positive Exponent, für den eine solche Gleichung

$$a^n = e$$

gilt. Dann sind die Potenzen

$$a^0, a^1, a^2, \ldots, a^{n-1}$$

alle voneinander verschieden, denn aus $a^h = a^k$ mit $0 \leqq k < h < n$ würde sich $a^{h-k} = e$ mit $h - k < n$ im Widerspruch zur Wahl von n ergeben. Ferner ist jedes a^i gleich einer der Potenzen aus der obigen Reihe $a^0, a^1, \ldots, a^{n-1}$; denn schreibt man mit ganzen Zahlen g und r:

$$i = gn + r \quad \text{mit } 0 \leqq r < n,$$

so ist:

$$a^i = a^{gn+r} = (a^{gn})\, a^r = (a^n)^g\, a^r = e a^r = a^r.$$

qed.

Da jedes Element einer Gruppe eine zyklische Untergruppe erzeugt, können wir den Begriff der Ordnung eines Gruppenelementes für beliebige Gruppen übernehmen (vgl. Aufgaben 1 und 2):

Definition **D (6.4)**

Unter der Ordnung eines Elementes a einer Gruppe $\mathfrak{G}$ *versteht man die Ordnung der durch a eindeutig bestimmten zyklischen Untergruppe* $\langle a \rangle$ *von* $\mathfrak{G}$.

Folgerung **F (6.5)**

a) *Jedes Element* $b \neq e$ *einer unendlichen zyklischen Gruppe* $\langle a \rangle$ *ist von unendlicher Ordnung.*

b) *Jedes Element b einer endlichen zyklischen Gruppe* $\langle a \rangle$ *ist von endlicher Ordnung.*

Beweis

a) Wir betrachten die von $b = a^i$ erzeugte zyklische Gruppe und haben nach D(6.4) zu zeigen, daß sie unendlich ist. Wäre nun $b^h = b^k$ mit $h \neq k$, so folgt $a^{ih} = a^{ik}$ mit $ih \neq ik$ im Widerspruch zur Voraussetzung.

b) In diesem Falle haben wir die Endlichkeit von $\langle b \rangle$ nachzuweisen, die aber wegen $\langle b \rangle \leqq \langle a \rangle$ sofort aus der Endlichkeit von $\langle a \rangle$ folgt.

qed.

Die Potenzen von Gruppenelementen mit endlicher Ordnung unterliegen folgender Gesetzmäßigkeit:

Satz **S (6.6)**

Alle, und nur die Potenzen eines Gruppenelementes a der Ordnung n stimmen überein, deren Exponenten h und k sich um ein ganzzahliges Vielfaches n g von n unterscheiden, d. h. modulo n kongruent sind.

Beweis

Wenn $h - k = gn$ gilt, folgt $a^h = a^k$ wegen

$$a^{h-k} = a^{ng} = e.$$

Ist umgekehrt $a^h = a^k$ und setzt man $h - k = ng + r$ mit $0 \leqq r < n$, so muß wegen

$$e = a^{h-k} = a^{ng+r} = a^{ng}\, a^r = e\, a^r = a^r$$

und nach Wahl von n der Rest r verschwinden.

qed.

Alle zyklischen Gruppen sind bis auf Isomorphie durch besonders einfache Vertreter gekennzeichnet (vgl. Aufg. 4):

Satz **S (6.7)**

a) *Jede unendliche zyklische Gruppe $\langle a \rangle$ ist isomorph zur additiven Gruppe der ganzen Zahlen vermöge der Zuordnung*

$$a^i \to i.$$

b) *Jede endliche zyklische Gruppe $\langle a \rangle$ der Ordnung n ist isomorph zur additiven Restklassengruppe mod n vermöge der Zuordnung*

$$a^i \to [i] \bmod n.$$

Beweis

a) Die Zuordnung ist nach S(6.3) eineindeutig; wegen $a^i a^k = a^{i+k}$ besteht Relationstreue.

b) Man schließt wie unter a) mit Hilfe von S(6.6).

qed.

Folgerung **F (6.8)**

a) *Alle unendlichen zyklischen Gruppen sind untereinander isomorph. Es gibt also genau eine abstrakte zyklische Gruppe von unendlicher Ordnung. Man bezeichnet sie oft mit* $\mathfrak{Z}_\infty$.

b) *Alle endlichen zyklischen Gruppen der gleichen Ordnung n sind untereinander isomorph. Es gibt also genau eine abstrakte zyklische Gruppe der Ordnung n. Man bezeichnet sie oft mit* $\mathfrak{Z}_n$.

Wir untersuchen nunmehr Untergruppen zyklischer Gruppen und empfehlen dem Leser, sich alle Aussagen am Beispiele des (unendlichen) Moduls der ganzen Zahlen bzw. an der (endlichen) Gruppe der n-ten Einheitswurzeln (etwa für $n = 24$, vgl. Aufg. 6) zu veranschaulichen.

Satz **S (6.9)**

Alle Untergruppen einer zyklischen Gruppe $\mathfrak{G} = \langle a \rangle$ *sind selbst zyklisch. Für die Einheitsgruppe* $\mathfrak{E} \subseteq \mathfrak{G}$ *ist das trivial; jede andere Untergruppe* $\mathfrak{H} \subseteq \mathfrak{G}$ *kann von derjenigen Potenz* $a^m \in \mathfrak{H}$ *erzeugt werden, deren Exponent m positiv und minimal ist. Dabei gilt:*

a) *Ist* $\mathfrak{G}$ *eine unendliche zyklische Gruppe, so ist jede Untergruppe* $\mathfrak{H} \neq \mathfrak{E}$ *von* $\mathfrak{G}$ *ebenfalls unendlich.*

b) *Ist* $\mathfrak{G}$ *eine endliche zyklische Gruppe der Ordnung n, so ist für jede Untergruppe* $\mathfrak{H} \neq \mathfrak{E}$ *das oben festgelegte m ein (von n verschiedener) Teiler von n:*

$$n = m \cdot \nu,$$

wobei der Komplementärteiler ν *die Ordnung von* $\mathfrak{H}$ *angibt.*

Beweis

1. Wegen $\mathfrak{H}^{-1} \subseteq \mathfrak{H}$ muß jede Untergruppe $\mathfrak{H} \neq \mathfrak{E}$ wenigstens ein a^i mit $i > 0$ enthalten. Es sei m der kleinste positive Exponent aller $a^i \in \mathfrak{H}$. Für $m = 1$ ergibt sich aus $\mathfrak{H} = \mathfrak{G}$ unmittelbar die Behauptung. Für $m > 1$ zeigen wir $\mathfrak{H} = \langle a^m \rangle$. Klar ist

$\mathfrak{H} \supseteq \langle a^m \rangle$. Andererseits läßt sich jedes $a^i \in \mathfrak{H}$ als Potenz $(a^m)^g$ von a^m schreiben, denn aus $i = mg + r$ mit ganzzahligen g und r sowie $0 \leqq r < m$ folgt

$$a^r = a^{i-mg} = a^i (a^m)^{-g} \in \mathfrak{H},$$

also $r = 0$ nach Wahl von m.

2. Die Behauptung für a) ergibt sich unmittelbar aus F(6.5a). Im Falle b) zeigen wir, daß für jede Untergruppe $\mathfrak{H} = \langle a^m \rangle$ unter Berücksichtigung der Wahl von m die Gleichung $n = m \cdot \nu$ gilt. Setzt man nämlich $n = m \cdot \nu + r$ mit ganzen Zahlen ν und r, wo $0 \leqq r < m$, erhält man aus

$$a^r = a^{n-m\nu} = a^n (a^m)^{-\nu} = (a^n)^{-\nu} \in \mathfrak{H}$$

$r = 0$ wegen der Minimaleigenschaft von m. Damit enthält aber $\mathfrak{H} = \langle a^m \rangle$ genau die ν Elemente

$$a^m, a^{2m}, \ldots, a^{\nu m} = a^n = e.$$

qed.

Damit sind wir in der Lage, uns einen Überblick über sämtliche Untergruppen einer zyklischen Gruppe zu verschaffen:

Satz **S (6.10)**

a) *Ist* $\mathfrak{G} = \langle a \rangle$ *eine unendliche zyklische Gruppe, so sind* $\langle a^m \rangle$ *mit* $m = 1, 2, \ldots$ *genau alle ihre Untergruppen* $\mathfrak{H} \neq \mathfrak{E}$.

b) *Ist* $\mathfrak{G} = \langle a \rangle$ *eine endliche zyklische Gruppe der Ordnung* n *und durchläuft* $m > 0$ *alle (von* n *verschiedenen) Teiler von* n, *so sind* $\langle a^m \rangle$ *genau alle ihre Untergruppen* $\mathfrak{H} \neq \mathfrak{E}$. *Dabei ist* m *der in* S(6.9) *festgelegte minimale Exponent.*

Beweis

Nach S (6.9) werden auf diese Weise jedenfalls alle Untergruppen von $\mathfrak{G}$ erfaßt. Es bleibt also nur zu zeigen, daß die so erzeugten Untergruppen alle voneinander verschieden sind.

Im Falle a) folgt dies einfach daraus, daß $a^{m'}$ mit $0 < m' < m$ wegen S(6.3a) keine Potenz von a^m sein kann.

Im Falle b) ergibt sich $\langle a^m \rangle \neq \langle a^{m'} \rangle$ sofort aus S(6.9b), da mit m und m' auch die zugehörigen Untergruppenordnungen ν und ν' verschieden sind. Die Bemerkung über die Minimalität von m erhält man sofort, wenn man die Elemente von $\langle a^m \rangle$ wie am Ende des Beweises von S (6.9) aufschreibt.

qed.

Das erzeugende Element a^m der Untergruppe $\mathfrak{H} = \langle a^m \rangle$ war bisher geeignet gewählt worden. Wir bestimmen jetzt alle erzeugenden Elemente von $\mathfrak{H}$.

Satz **S (6.11)**

a) *In einer unendlichen zyklischen Gruppe* $\mathfrak{G} = \langle a \rangle$ *gilt* $\langle a^k \rangle = \langle a^m \rangle$ *dann und nur dann, wenn* $k = \pm m$ *ist.*

b) *In einer endlichen zyklischen Gruppe* $\mathfrak{G} = \langle a \rangle$ *der Ordnung n gilt* $\langle a^k \rangle = \langle a^m \rangle$ *mit einem positiven Teiler m von n dann und nur dann, wenn der größte gemeinsame Teiler* (k, n) *von k und n gleich m ist.*

Beweis

a) Aus $\langle a^k \rangle = \langle a^m \rangle$ folgt $a^k = (a^m)^g$ und $a^m = (a^k)^h$ mit ganzzahligen g und h. Damit ist nach S(6.3) $k = mg$ und $m = kh$, also $m = mgh$. Aus $gh = 1$ folgt $g = h = \pm 1$ und damit $k = \pm m$. Umgekehrt ist $\langle a^m \rangle = \langle a^{-m} \rangle$ nach S(5.13) klar.

b) Wir gehen zunächst wieder von $\langle a^k \rangle = \langle a^m \rangle$ aus und zeigen $(k, n) = m$. Da sich a^k als geeignete Potenz $(a^m)^g$ von a^m schreiben läßt, gilt nach S(6.6)

$$k = mg + nh \quad (g, h \text{ ganzzahlig}).$$

Daher folgt aus $m|n$ auch $m|k$, d. h., m ist gemeinsamer Teiler von n und k. Andererseits läßt sich auch a^m als geeignete Potenz $(a^k)^{g'}$ von a^k schreiben, was die Gleichung

$$m = kg' + nh' \quad (g', h' \text{ ganzzahlig})$$

zur Folge hat. Diese Gleichung lehrt, daß jeder gemeinsame Teiler von k und n auch in m aufgeht. Also ist m der größte gemeinsame Teiler von k und n.

Umgekehrt sei $\mathfrak{H} = \langle a^m \rangle$ und k eine ganze Zahl mit $(k, n) = m$. Nun läßt sich die von a^k erzeugte Untergruppe gemäß S(6.9) auch von einer Potenz $a^{m'}$ erzeugen, wobei m' ein Teiler von n ist. Nach dem schon bewiesenen Teil dieses Satzes gilt dabei $(k, n) = m'$. Wegen der eindeutigen Bestimmtheit des (positiven) größten gemeinsamen Teilers folgt also $m = m'$; mithin gilt:

$$\langle a^k \rangle = \langle a^{m'} \rangle = \langle a^m \rangle.$$

qed.

Wir wenden den vorangehenden Satz insbesondere für den Fall $m = 1$ an:

Folgerung **F (6.12)**

a) *Eine unendliche zyklische Gruppe* $\mathfrak{G} = \langle a \rangle$ *hat genau zwei erzeugende Elemente, nämlich* a *und* a^{-1}.

b) *Eine endliche zyklische Gruppe* $\mathfrak{G} = \langle a \rangle$ *der Ordnung* n *hat genau* $\varphi(n)$ *erzeugende Elemente, nämlich alle* a^k *mit* $(k, n) = 1$ *und* $k \leqq n$.

Wie bereits in F (6.2) erwähnt, haben wir bei additiven zyklischen Gruppen die Potenzen durch ganzzahlige Vielfache zu ersetzen. Eine additive zyklische Gruppe $\langle a \rangle$ ist daher endlich, wenn es eine positive ganze Zahl n gibt, die $na = o$ erfüllt. Die kleinste Zahl mit dieser Eigenschaft ist die Ordnung von a und $\langle a \rangle$. Mit diesen Begriffsbildungen gelten alle abgeleiteten Aussagen analog. So ergibt sich z. B. die Aussage von Aufgabe 14 aus § 5 unmittelbar aus S (6.10a).

Aufgaben zu § 6

1. Man bestimme die Ordnungen der Elemente der Gruppe $\mathfrak{S}_3$.
2. In jeder Gruppe ist das Einselement das einzige mit der Ordnung 1.
3. Bei einem Isomorphismus ist stets die Ordnung des Bildelementes gleich der Ordnung des Originalelementes.
4. Die folgenden Gruppen der Ordnung 6 sind zyklisch:
   a) die Gruppe der 6-ten Einheitswurzeln,
   b) die prime Restklassengruppe mod 7,
   c) die prime Restklassengruppe mod 9.
   Sie sind damit alle nach S (6.7) zum Restklassenmodul mod 6 isomorph. Man gebe unter Benutzung von Aufgabe 3 Zuordnungen an, die diese Isomorphien vermitteln, und vergleiche die Strukturtafeln.
5. Man überlege sich, daß bei der isomorphen Abbildung einer zyklischen Gruppe $\mathfrak{Z}_m$ auf den Restklassenmodul mod m die erzeugenden Elemente von $\mathfrak{Z}_m$ genau auf die primen Restklassen mod m abgebildet werden.
6. Man bestimme alle Untergruppen der zyklischen Gruppe $\mathfrak{Z}_{24}$ der Ordnung 24 und gebe alle Erzeugenden dieser Untergruppen an. Die Ergebnisse kann man sich an Hand der Gruppe der 24-ten Einheitswurzeln veranschaulichen, indem man die 24-ten Einheitswurzeln als komplexe Zahlen in der Gaussschen Ebene darstellt.
7. Mit Hilfe von S (6.11b) läßt sich leicht der folgende wichtige Satz der elementaren Zahlentheorie beweisen: Der größte gemeinsame Teiler $m = (k, n)$ läßt sich aus k und n mit ganzen Zahlen g und h linear kombinieren:
$$m = kg + nh.$$

§ 7. Nebenklassen

Wir untersuchen spezielle Komplexe in einer Gruppe, mit deren Hilfe eine Klasseneinteilung der Menge aller Gruppenelemente möglich ist. Auf diese Weise gelangen wir zu einigen grundlegenden Strukturaussagen über endliche Gruppen, insbesondere zu dem wichtigen Satz von LAGRANGE.

Definition **D (7.1)**

Das Komplexprodukt $a\mathfrak{H}$ eines Elementes a der Gruppe $\mathfrak{G}$ mit einer Untergruppe $\mathfrak{H} \subseteq \mathfrak{G}$ heißt die von a erzeugte Linksnebenklasse von $\mathfrak{H}$ in $\mathfrak{G}$. Entsprechend heißt $\mathfrak{H}a$ die von a erzeugte Rechtsnebenklasse von $\mathfrak{H}$ in $\mathfrak{G}$[1]).

Als Beispiele empfehlen wir die Aufstellung sämtlicher Links- bzw. Rechtsnebenklassen von allen möglichen Untergruppen in $\mathfrak{S}_3$, die für Aufgabe 1 ohnehin benötigt werden. Man überprüfe daran auch die nachstehende

Folgerung **F (7.2)**

Für zwei Linksnebenklassen gilt $a\mathfrak{H} = b\mathfrak{H}$ dann und nur dann, wenn $a^{-1}b \in \mathfrak{H}$ ist; andernfalls sind sie elementfremd. Entsprechendes gilt für Rechtsnebenklassen mit $ab^{-1} \in \mathfrak{H}$.

Beweis

Aus $a\mathfrak{H} = b\mathfrak{H}$ folgt $a^{-1}b\mathfrak{H} = \mathfrak{H}$ und damit nach S(5.9) $a^{-1}b \in \mathfrak{H}$ und umgekehrt. Zum Nachweis der Elementfremdheit von $a\mathfrak{H}$ und $b\mathfrak{H}$ für $a\mathfrak{H} \neq b\mathfrak{H}$ zeigen wir: Zwei Linksnebenklassen, die wenigstens ein Element gemeinsam haben, stimmen vollständig überein. Ist nämlich $x \in a\mathfrak{H} \wedge b\mathfrak{H}$, d. h. $x = ah_1 = bh_2$, so ergibt sich wegen $a^{-1}b = h_1h_2^{-1} \in \mathfrak{H}$ nach dem zuerst Bewiesenen $a\mathfrak{H} = b\mathfrak{H}$. Die Aussagen über die Rechtsnebenklassen beweist man analog.

qed.

---

1) In der (älteren) Literatur findet man auch die Bezeichnung „Nebengruppe" statt Nebenklasse. Diese Bezeichnung ist irreführend, da die Untergruppe $\mathfrak{H}$ die einzige Links- wie Rechtsnebenklasse von $\mathfrak{H}$ in $\mathfrak{G}$ ist, die Gruppeneigenschaft hat. Sie ist nämlich die einzige, die das Element e enthält.

Satz **S (7.3)**

Die voneinander verschiedenen Linksnebenklassen von $\mathfrak{H}$ in $\mathfrak{G}$ sind die Klassen einer Klasseneinteilung von $\mathfrak{G}$ im Sinne der Mengenlehre, der sog. Zerlegung von $\mathfrak{G}$ in Linksnebenklassen nach $\mathfrak{H}$:

$$\mathfrak{H} \cup a\mathfrak{H} \cup b\mathfrak{H} \cup c\mathfrak{H} \cup \ldots$$

mit $a \notin \mathfrak{H}$, $b \notin \mathfrak{H} \cup a\mathfrak{H}$, $c \notin \mathfrak{H} \cup a\mathfrak{H} \cup b\mathfrak{H}$, ... Ein vollständiges Repräsentantensystem für diese Klasseneinteilung ist etwa

$$\{e, a, b, c, \ldots\}.$$

Entsprechend erhält man die Zerlegung von $\mathfrak{G}$ in Rechtsnebenklassen nach $\mathfrak{H}$.

Beweis

Es ist nachzuweisen, daß die in der Behauptung konstruierte Vereinigungsmenge aus nichtleeren, untereinander elementfremden Komponenten besteht und alle Elemente von $\mathfrak{G}$ umfaßt. Aus $e \in \mathfrak{H}$ folgt sofort, daß die Komponenten nicht leer sind und jedes Element aus $\mathfrak{G}$ erfaßt wird. Die Elementfremdheit der Komponenten ergibt sich unmittelbar aus F (7.2).

qed.

Folgerung **F (7.4)**

Der Klasseneinteilung von $\mathfrak{G}$ in Linksnebenklassen nach $\mathfrak{H}$ entspricht nach F (7.2) *die Äquivalenzrelation:*

$$a \sim b \text{ dann und nur dann, falls } a^{-1}b \in \mathfrak{H}.$$

Sie wird linksseitige Äquivalenz nach $\mathfrak{H}$ genannt. Analog ist die rechtsseitige Äquivalenz nach $\mathfrak{H}$ mit $ab^{-1} \in \mathfrak{H}$ zu erklären.

Die Zerlegung der Gruppe $\mathfrak{G}$ in Linksnebenklassen nach einer Untergruppe $\mathfrak{H}$ ist im allgemeinen verschieden von der Zerlegung in Rechtsnebenklassen nach derselben Untergruppe $\mathfrak{H}$ (vgl. Aufgaben 1 und 2). Man kann aber, wie wir im folgenden zeigen, die in beiden Zerlegungen auftretenden Nebenklassen eineindeutig aufeinander beziehen. Insbesondere stimmt also im endlichen Falle die Anzahl der Linksnebenklassen mit der Anzahl der Rechtsnebenklassen überein.

Satz **S (7.5)**

Die Menge der Nebenklassen in der linksseitigen Zerlegung von $\mathfrak{G}$ *nach* $\mathfrak{H}$ *ist gleichmächtig der Menge der Nebenklassen in der rechtsseitigen Zerlegung von* $\mathfrak{G}$ *nach* $\mathfrak{H}$.

Beweis

Es genügt nachzuweisen, daß die Repräsentantensysteme gleichmächtig sind. Bildet nun

$$\{e, a, b, c, \ldots\}$$

ein vollständiges linksseitiges Repräsentantensystem, so ist

$$\{e, a^{-1}, b^{-1}, c^{-1}, \ldots\}$$

ein vollständiges rechtsseitiges Repräsentantensystem. In der zugehörigen Zerlegung

$$\mathfrak{H} \cup \mathfrak{H}a^{-1} \cup \mathfrak{H}b^{-1} \cup \mathfrak{H}c^{-1} \cup \ldots$$

ist nämlich jedes Gruppenelement $x \in \mathfrak{G}$ enthalten; denn aus $x^{-1} \in \mathfrak{G}$ und der Vollständigkeit des linksseitigen Repräsentantensystems $\{e, a, b, c, \ldots\}$ folgt $x^{-1} \in y\mathfrak{H}$ mit geeignetem y aus $\{e, a, b, c, \ldots\}$ und damit $x \in (y\mathfrak{H})^{-1} = \mathfrak{H}^{-1}y^{-1} = \mathfrak{H}y^{-1}$ mit y^{-1} aus $\{e, a^{-1}, b^{-1}, c^{-1}, \ldots\}$. Ferner sind alle in der obigen Zerlegung auftretenden Rechtsnebenklassen voneinander verschieden; denn aus $a\mathfrak{H} \neq b\mathfrak{H}$ folgt nach F (7.2) $a^{-1}b \notin \mathfrak{H}$, damit also $(a^{-1}b)^{-1} = (b^{-1})(a^{-1})^{-1} \notin \mathfrak{H}$ und daher ebenfalls nach F (7.2) $\mathfrak{H}b^{-1} \neq \mathfrak{H}a^{-1}$.

qed.

Definition **D (7.6)**

Die nach S (7.5) *eindeutig bestimmte Mächtigkeit der Menge aller in einer Zerlegung von* $\mathfrak{G}$ *nach* $\mathfrak{H}$ *auftretenden Nebenklassen (im endlichen Falle also deren Anzahl) heißt der Index von* $\mathfrak{H}$ *in* $\mathfrak{G}$ *und wird mit* $(\mathfrak{G}:\mathfrak{H})$ *bezeichnet.*

Die Ordnung der Gruppe $\mathfrak{G}$ ist also gleich dem Index $(\mathfrak{G}:\mathfrak{E})$ der Einheitsgruppe $\mathfrak{E}$ in $\mathfrak{G}$.

Die folgenden Aussagen formulieren wir für endliche Gruppen; sie können jedoch unter Verwendung des Begriffes der transfiniten Kardinalzahl auch für unendliche Gruppen ausgesprochen werden. Man veranschauliche sich das Folgende bis F (7.9) am Beispiele der symmetrischen Gruppe $\mathfrak{S}_3$.

Satz von LAGRANGE **S (7.7)**

Die Ordnung einer Untergruppe $\mathfrak{H}$ einer endlichen Gruppe $\mathfrak{G}$ ist ein Teiler der Ordnung von $\mathfrak{G}$; der Komplementärteiler ist der Index von $\mathfrak{H}$ in $\mathfrak{G}$:

$$(\mathfrak{G}:\mathfrak{E}) = (\mathfrak{G}:\mathfrak{H})\,(\mathfrak{H}:\mathfrak{E}).$$

Beweis

Wegen der Endlichkeit von $\mathfrak{G}$ sind erst recht alle Nebenklassen von $\mathfrak{G}$ nach $\mathfrak{H}$ endlich. Die Anzahl der Elemente in jeder Nebenklasse $a\mathfrak{H}$ stimmt mit der Ordnung von $\mathfrak{H}$ überein. Es enthält nämlich $a\mathfrak{H}$ genau die Elemente ah, wobei h genau alle Elemente von $\mathfrak{H}$ durchläuft, und es ist $ah \neq ah'$ für $h \neq h'$.
Daher folgt die Behauptung nach den vorhergehenden Sätzen durch Abzählen der Elemente in der linksseitigen Zerlegung von $\mathfrak{G}$ nach $\mathfrak{H}$:

$$\mathfrak{G} = \mathfrak{H} \cup a\mathfrak{H} \cup b\mathfrak{H} \cup \cdots \cup t\mathfrak{H}.$$

qed.

Für den Fall einer endlichen zyklischen Gruppe $\mathfrak{Z}_n$ ist diese Aussage bereits in S (6.9) enthalten, wobei man dort sogar weiß, daß es für jeden Teiler ν der Ordnung n wirklich eine und auch nur eine Untergruppe der Ordnung ν gibt (vgl. S (6.10)). Für beliebige endliche Gruppen können dagegen mehrere Untergruppen gleicher Ordnung (etwa in $\mathfrak{S}_3$) oder aber auch für bestimmte Teiler der Gruppenordnung gar keine Untergruppen dieser Ordnung existieren (etwa in der Gruppe $\mathfrak{A}_4$ für den Teiler 6, vgl. Aufg. 1 von § 11).

Folgerung **F (7.8)**

Die Ordnung eines Elementes a einer endlichen Gruppe $\mathfrak{G}$ ist ein Teiler der Gruppenordnung,

wie sich unmittelbar aus dem Satz von LAGRANGE mit $\mathfrak{H} = \langle a \rangle$ ergibt.

Folgerung **F (7.9)**

In einer Gruppe der Ordnung n gilt für jedes Element a die Gleichung $a^n = e$,

denn n ist nach F (7.8) Vielfaches der Ordnung von a.

Folgerung **F (7.10)**

Es gibt nur eine abstrakte Gruppe der Primzahlordnung p, nämlich die zyklische Gruppe $\mathfrak{Z}_p$.

Beweis

Hat $\mathfrak{G}$ die Ordnung p, so gibt es nach F(7.8) in $\mathfrak{G}$ außer dem Einselement e nur Elemente der Ordnung p. Jedes von diesen erzeugt bereits die gesamte Gruppe $\mathfrak{G}$. Die Gruppe ist also zyklisch.

qed.

Selbstverständlich übertragen sich wieder alle Aussagen auf Moduln unter Berücksichtigung der sich aus der Gültigkeit des kommutativen Gesetzes ergebenden Vereinfachungen. Man bezeichnet aber in additiver Schreibweise die Nebenklassen $a + \mathfrak{H} = \mathfrak{H} + a$ eines Untermoduls $\mathfrak{H}$ in $\mathfrak{G}$ im allgemeinen als *Restklassen modulo* $\mathfrak{H}$ und nennt die in F(7.4) angeführte Äquivalenzrelation *Kongruenz modulo* $\mathfrak{H}$. Wie wir sehen werden, handelt es sich dabei um eine Verallgemeinerung der Begriffsbildungen in B(2.8). Entsprechend benutzt man auch hier für modulo $\mathfrak{H}$ kongruente Elemente aus $\mathfrak{G}$ die Schreibweisen

$$a \equiv b \bmod \mathfrak{H} \quad \text{oder} \quad a \equiv b \ (\mathfrak{H}),$$

was also nach F(7.4) bedeutet, daß $a - b \in \mathfrak{H}$ ist.

Läßt sich insbesondere der Untermodul $\mathfrak{H} \subseteq \mathfrak{G}$ von einem Element $m \in \mathfrak{H}$ erzeugen, ist also $\mathfrak{H} = \langle m \rangle$ zyklisch, so nennt man die Kongruenz mod $\mathfrak{H}$ auch eine Kongruenz mod m und schreibt

statt	$a \equiv b \bmod \langle m \rangle$	bzw. $a \equiv b \ (\langle m \rangle)$
einfach	$a \equiv b \bmod m$	bzw. $a \equiv b \ (m)$.

Die Bedingung $a - b \in \langle m \rangle$ besagt in diesem Falle, daß $a - b$ ein ganzzahliges Vielfaches gm von m ist. Auch dies ist noch wesentlich allgemeiner als die in B(2.8) behandelte Kongruenz ganzer Zahlen, denn die hier betrachteten Kongruenzen sind durch $m \in \mathfrak{G}$ bestimmte Beziehungen zwischen den Elementen eines beliebigen Moduls $\mathfrak{G}$, für den die ganzen Zahlen nur die Rolle des Operatorenbereiches spielen.

Setzt man freilich den beliebigen Modul $\mathfrak{G}$ gleich dem der ganzen Zahlen, so deckt sich die hier allgemein erklärte Kongruenzrechnung mit der aus B(2.8). Dies liegt daran, daß im Modul der ganzen Zahlen jeder Untermodul zyklisch ist und von einer positiven ganzen Zahl erzeugt werden kann (vgl. § 5, Aufg. 14). Wir haben

damit die Kongruenzrechnung der elementaren Zahlentheorie weit allgemeineren gruppentheoretischen Überlegungen untergeordnet. Wie wir später sehen werden, sind auch die übrigen Aussagen aus B(2.8) nur Spezialfälle allgemeinerer Betrachtungen, so z. B. die Tatsache, daß die Restklassen ganzer Zahlen selbst einen Modul bilden (vgl. Kapitel III).

Aufgaben zu § 7

1. Man stelle zu jeder Untergruppe $\mathfrak{H}$ von $\mathfrak{S}_3$ die Zerlegung von $\mathfrak{S}_3$ sowohl in Links- als auch in Rechtsnebenklassen nach $\mathfrak{H}$ auf.
2. Man zerlege die prime Restklassengruppe mod 15 in Nebenklassen nach der von [4] erzeugten Untergruppe.
3. Ist $\mathfrak{G}$ eine von a erzeugte zyklische Gruppe und $\mathfrak{H}$ eine von der Einheitsgruppe verschiedene Untergruppe, die also nach S(6.9) von a^m mit minimalem m erzeugt werden kann, so ist der Index $(\mathfrak{G}:\mathfrak{H})$ gleich m. Man wende diese Aussage insbesondere auf den Modul der ganzen Zahlen an.
4. Wir haben in F(7.4) die Äquivalenzrelation als Folgerung aus der Klasseneinteilung S(7.3) erhalten. Man gehe den umgekehrten Weg.
5. Der Index $(\mathfrak{O}:\mathfrak{O}_+)$ der Gruppe $\mathfrak{O}_+$ der eigentlich orthogonalen Matrizen vom Typ (n, n) in der Gruppe $\mathfrak{O}$ der orthogonalen Matrizen vom gleichen Typ ist 2. Man beweise dies durch Herstellung der linksseitigen Zerlegung von $\mathfrak{O}$ nach $\mathfrak{O}_+$.
6. Es gibt bis auf Isomorphie genau je zwei Gruppen der Ordnung 4 und der Ordnung 6.
7. Man beweise den sog. kleinen FERMATschen Satz[1]) der elementaren Zahlentheorie:

$$a^{\varphi(m)} \equiv 1 \ (m) \quad \text{für } (a, m) = 1.$$

1) PIERRE DE FERMAT, 1601 bis 1665.

II. PERMUTATIONS- UND TRANSFORMATIONSGRUPPEN

Während unsere bisherigen Untersuchungen im wesentlichen allgemeine gruppentheoretische Aussagen zum Ziel hatten, gehen wir in diesem Kapitel näher auf bestimmte Gruppen und die Natur ihrer Elemente ein. Sie sind sowohl für Anwendungen der Gruppentheorie in anderen mathematischen Disziplinen als auch für die Gruppentheorie selbst von Bedeutung, zumal sie rechnerisch verhältnismäßig leicht zugängliche Beispiele in die Hand geben.

In den folgenden Kapiteln benötigen wir hauptsächlich die grundlegenden Aussagen über Permutationen und die von ihnen gebildeten Gruppen aus den §§ 8 bis 11; dagegen können die vertiefenden Betrachtungen im § 12 beim ersten Studium übergangen werden. Die abschließend behandelten geometrischen Transformationsgruppen verdienen Interesse um ihrer selbst willen.

§ 8. Darstellung endlicher Gruppen durch Permutationen

Wie wir schon einmal erwähnten, umfaßt das Studium der Permutationsgruppen bereits das Studium sämtlicher Gruppen von endlicher Ordnung. Dies liegt darin begründet, daß jede endliche Gruppe wenigstens einer Permutationsgruppe isomorph ist, oder mit anderen Worten, daß jede Klasse zueinander isomorpher endlicher Gruppen wenigstens eine Permutationsgruppe enthält. Wir leiten im folgenden einen von CAYLEY herrührenden Satz ab, der sogar die Konstruktion der in Rede stehenden Permutationsgruppe gestattet. Dabei behandeln wir ohne Beschränkung der Allgemeinheit nur multiplikative Gruppen.

Satz **S (8.1)**

Es sei $\mathfrak{G}$ eine beliebige endliche Gruppe mit den Elementen $a_1, a_2, \ldots, a_n$. Dann sind

$$s_i = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ a_1 a_i & a_2 a_i & \ldots & a_n a_i \end{pmatrix} \quad \text{mit } i = 1, \ldots, n$$

n Permutationen dieser Elemente, und $\mathfrak{G}$ ist isomorph zu der aus den Permutationen $s_1, s_2, \ldots, s_n$ bestehenden Permutationsgruppe $\mathfrak{P}$ vermöge der Zuordnung $a_i \to s_i$.

Beweis

1. Die erklärten s_i sind tatsächlich Permutationen, da wegen *M III** die Produkte $a_1 a_i, a_2 a_i, \ldots, a_n a_i$ wieder genau alle Elemente der Gruppe $\mathfrak{G}$ sind.

2. Nach F (4.5) genügt es zu zeigen, daß die Strukturtafeln der Menge $\mathfrak{P}$ dieser Permutationen und der Gruppe $\mathfrak{G}$ übereinstimmen. Die Permutation $s_i \in \mathfrak{P}$ überführt jedes Element $a_j \in \mathfrak{G}$ in das Element $a_j a_i$:

$$s_i (a_j) = a_j a_i .$$

Ist nun $a_i a_k = a_l$, so folgt für alle j:

$$s_l (a_j) = a_j a_l = a_j a_i a_k = s_k (a_j a_i) = s_k (s_i (a_j)) .$$

Dabei bedeutet $s_k (s_i (a_j))$, daß zuerst s_i auf a_j und dann s_k auf das Ergebnis $s_i (a_j)$ anzuwenden ist. Das ist aber nach der Definition der Multiplikation von Permutationen dasselbe, als ob man $s_i s_k$ auf a_j anwendet[1]). Daher ist $s_l = s_i s_k$; die Strukturtafeln von $\mathfrak{G}$ und $\mathfrak{P}$ sind also gleich. qed.

Selbstverständlich brauchen wir in den Permutationen $s_1, \ldots, s_n$ statt der Elemente von $\mathfrak{G}$ nur die entsprechenden Indizes einzutragen.

Aus S (8.1) erhält man unmittelbar:

Folgerung **F (8.2)**

Jede Gruppe der Ordnung n ist isomorph einer Untergruppe der symmetrischen Gruppe $\mathfrak{S}_n$.

---

1) Betrachtet man die Permutationen als Transformationen gemäß B (2.6), so entspricht unsere Überlegung der Formel: $s_k(s_i(a_j)) = [s_i s_k] (a_j)$.

Folgerung **F (8.3)**

Es gibt von jeder Ordnung n nur endlich viele zueinander nicht isomorphe Gruppen, mit anderen Worten, es gibt nur endlich viele Klassen zueinander isomorpher Gruppen der Ordnung n.

Letzteres folgt in diesem Zusammenhang daraus, daß die symmetrische Gruppe $\mathfrak{S}_n$ als endliche Gruppe nur endlich viele Untergruppen enthält. Doch hätten wir diese Aussage auch unabhängig von den Überlegungen dieses Paragraphen gewinnen können, da für die Strukturtafeln der genannten Gruppen rein kombinatorisch nur endlich viele Möglichkeiten in Frage kommen.

Wir bemerken noch, daß es oft möglich ist, zu $\mathfrak{G}$ isomorphe Gruppen von Permutationen zu finden, deren Grad kleiner ist als die Ordnung von $\mathfrak{G}$ (vgl. Aufg. 2). Es ist bis heute ein ungelöstes Problem, den dabei kleinstmöglichen Grad in seiner Abhängigkeit von der Ordnung von $\mathfrak{G}$ anzugeben.

Aufgaben zu § 8

1. Welche Zusammenhänge bestehen zwischen der CAYLEYschen Strukturtafel von $\mathfrak{G}$ und den in S(8.1) konstruierten Permutationen?
2. Die in § 4, Aufgabe 4 genannte Gruppe der Doppelverhältnisse ist nach S(8.1) durch Permutationen vom Grad 6 darzustellen. Da diese Gruppe andererseits isomorph zur Gruppe $\mathfrak{S}_3$ ist, haben wir damit ein Beispiel zu den Bemerkungen nach F(8.3).

§ 9. Zerlegung einer Permutation in Zyklen

Die in B(2.5) eingeführte Schreibweise von Permutationen läßt sie zwar als eineindeutige Abbildungen sehr deutlich erkennen, ist aber für das praktische Rechnen mit Permutationen etwas schwerfällig. Wir geben daher eine kürzere und handlichere Schreibweise an, die jede beliebige Permutation als Produkt besonders einfacher Permutationen kennzeichnet.

Definition **D (9.1)**

Eine Permutation z vom Grad n heißt zyklisch, wenn sie durch Vertauschung ihrer Spalten auf die folgende Gestalt gebracht werden kann:

$$z = \begin{pmatrix} i_1 & i_2 & \cdots & i_{r-1} & i_r & i_{r+1} & \cdots & i_n \\ i_2 & i_3 & \cdots & i_r & i_1 & i_{r+1} & \cdots & i_n \end{pmatrix}.$$

Eine solche Permutation führt also

$$i_1 \text{ in } i_2, \quad i_2 \text{ in } i_3, \qquad i_{r-1} \text{ in } i_r, \quad i_r \text{ in } i_1$$

über, während die Zahlen $i_{r+1}, \ldots, i_n$ in Ruhe bleiben. Wir vereinfachen die Schreibweise durch die Angabe von z als *r-gliedrigen Zyklus*

$$z = (i_1\, i_2 \ldots i_r),$$

in dem für $r > 1$ nur diejenigen Zahlen auftreten, die durch z tatsächlich geändert werden. Für $r = 1$ erhält man die identische Permutation, die sich D (9.1) als Spezialfall unterordnet und sich somit als eingliedriger Zyklus $e = (i_1)$ schreiben läßt.

Eine zyklische Permutation ist z. B.:

$$z = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 3 & 4 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 5 & 4 & 3 & 2 & 6 \\ 5 & 4 & 3 & 1 & 2 & 6 \end{pmatrix} = (1\ 5\ 4\ 3)$$

Die durch diese Permutation bewirkte Vertauschung der Zahlen 1, 5, 4, 3 kann man durch ein „zyklisches" Schema veranschaulichen, das sich natürlich auch für eine beliebige zyklische Permutation verallgemeinern läßt und die Unabhängigkeit von der Wahl der zuerst hingeschriebenen Zahl unterstreicht.

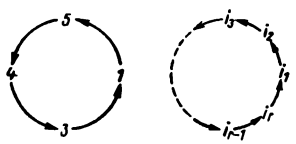


Abb. 2

Selbstverständlich ist nicht jede Permutation zyklisch. Es gilt aber:

Satz **S (9.2)**

Jede Permutation s läßt sich als Produkt elementfremder Zyklen schreiben[1]*). Diese Darstellung ist eindeutig bis auf die Reihenfolge der Faktoren. Wir bezeichnen sie als Hauptproduktdarstellung von s. In ihr treten für s ≠ e nur solche Zahlen auf, die durch s tatsächlich geändert werden.*

Beispiel: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 7 & 4 & 8 & 9 & 1 & 2 & 6 \end{pmatrix} = (1\ 3\ 7)(2\ 5\ 8)(6\ 9).$

1) Bei einer zyklischen Permutation besteht das „Produkt" nur aus einem Zyklus.

Beweis

1. Für die identische Permutation ist nichts zu beweisen. Jede andere Permutation s enthält Zahlen, die tatsächlich geändert werden; nur diese werden betrachtet.

2. Bei geeigneter Bezeichnung dieser Zahlen liefere die Permutation s zunächst die Zuordnungen

$$i_1 \to i_2, \quad i_2 \to i_3, \qquad\qquad i_{r-1} \to i_r, \quad i_r \to i_{r+1},$$

wobei i_{r+1} die erste wieder auftretende Zahl aus der Reihe der ihr vorangegangenen Zahlen sei. Dann ist $i_{r+1} = i_1$; denn wäre $i_{r+1} = i_\varrho$ mit $2 \leqq \varrho \leqq r$, so folgte wegen

$$i_r \to i_\varrho$$
$$i_{\varrho-1} \to i_\varrho$$

und wegen der Eineindeutigkeit der Zuordnung $i_r = i_{\varrho-1}$ mit $1 \leqq \varrho - 1 \leqq r - 1$ im Widerspruch zur Wahl von i_{r+1}. Durch die angegebenen Zuordnungen wird also ein Zyklus $(i_1 i_2 \ldots i_r)$ erklärt.

3. Wenn mit $i_1, i_2, \ldots, i_r$ bereits alle von s tatsächlich geänderten Zahlen erschöpft sind, ist s zyklisch und damit die Behauptung klar. Andernfalls existiert wenigstens eine noch nicht aufgetretene Zahl j_1, die nach den gleichen Überlegungen wie unter 2. eine Reihe von Zuordnungen

$$j_1 \to j_2, \quad j_2 \to j_3, \qquad\qquad j_{s-1} \to j_s, \quad j_s \to j_1$$

und damit einen Zyklus $(j_1 j_2 \ldots j_s)$ liefert.

Dabei sind die Zahlen j sämtlich verschieden von den Zahlen i. Würden nämlich die beiden Zyklen eine Zahl gemeinsam haben, so müßten wegen der Eindeutigkeit der durch s vermittelten Abbildung auch die in beiden Zyklen auf diese Zahlen nächstfolgenden Zahlen übereinstimmen. Setzt man diesen Schluß fort, erhält man die Gleichheit beider Zyklen im Widerspruch zur Wahl von j_1.

4. Falls noch weitere Zahlen vorhanden sind, bildet man einen dritten Zyklus usf. Das Verfahren bricht ab, da durch s nur endlich viele Zahlen geändert werden. Offensichtlich sind die Zyklen

durch
$$s = \begin{pmatrix} i_1\ i_2 \dots i_r\ j_1\ j_2 \dots j_s \dots \\ i_2\ i_3 \dots i_1\ j_2\ j_3 \dots j_1 \dots \quad \dots \end{pmatrix}$$
eindeutig bestimmt, und ihr Produkt
$$(i_1 i_2 \dots i_r)\ (j_1 j_2 \dots j_s)$$
vermittelt dieselbe Zuordnungsvorschrift wie s.

Da zwei Permutationen s_1 und s_2, von denen s_1 andere Zahlen als s_2 wirklich permutiert, kommutativ multiplizierbar sind (vgl. Aufg. 4), ist die Reihenfolge der Zyklen in der Produktdarstellung von s beliebig. qed.

Die Schreibweise von Permutationen als Produkt elementfremder Zyklen ist nicht nur übersichtlicher, sondern gewährt auch insbesondere beim Potenzieren Rechenvorteile:

Nach Definition ordnet ein Zyklus z jeder in ihm vorkommenden Zahl die jeweils erste nachfolgende Zahl zu. Führt man dies m-mal hintereinander aus, erhält man für die m-te Potenz z^m, daß sie jeder Zahl die jeweils m-te nachfolgende Zahl zuordnet. Der Leser verdeutliche sich dies an Hand des im Anschluß an D (9.1) eingeführten Schemas. Es brauchen dabei nicht alle Potenzen von z selbst zyklische Permutationen zu sein (vgl. Aufg. 5):

$z = (1\,2\,3\,4\,5)$	$z = (1\,2\,3\,4)$
$z^2 = (1\,3\,5\,2\,4)$	$z^2 = (1\,3)(2\,4)$
$z^3 = (1\,4\,2\,5\,3)$	$z^3 = (1\,4\,3\,2)$
$z^4 = (1\,5\,4\,3\,2)$	$z^4 = (1)$
$z^5 = (1)$	

Dagegen ist das Inverse einer zyklischen Permutation
$$z = (i_1 i_2 \dots i_r)$$
stets wieder eine zyklische Permutation, nämlich
$$z^{-1} = (i_r \dots i_2 i_1).$$

Nach der letzten Bemerkung im Beweis von S (9.2) übertragen sich diese Aussagen über zyklische Permutationen auf beliebige Permutationen in ihrer Hauptproduktdarstellung

gemäß:
$$s = z_1 z_2 \dots z_l$$
$$s^m = z_1^m z_2^m \dots z_l^m\ ;\quad s^{-1} = z_1^{-1} z_2^{-1} \dots z_l^{-1}.$$

Folgerung **F (9.3)**

Eine zyklische Permutation $z = (i_1 i_2 \ldots i_r)$ *hat die Ordnung* r.
Die Ordnung h *einer beliebigen Permutation* $s = z_1 z_2 \ldots z_l$ *ist gleich dem kleinsten gemeinsamen Vielfachen der Ordnungen* r_i *der einzelnen Zyklen* z_i *in der Hauptproduktdarstellung*

Beweis

Für einen einzelnen Zyklus folgt dies unmittelbar aus den obigen Bemerkungen. Weiterhin gilt für die Ordnung h

$$s^h = z_1^h z^h \ldots z_l^h = (1).$$

Damit ein Potenzprodukt elementfremder Zyklen gleich (1) ist, ist offensichtlich hinreichend, aber auch notwendig, daß jede Zyklenpotenz gleich (1) ist. Andernfalls könnte man nämlich zwei von (1) verschiedene Teilprodukte angeben, die zueinander invers sein müssen im Widerspruch zur Elementfremdheit aller Zyklen. Es muß also h ein Vielfaches von jedem r_i und damit das kleinste gemeinsame Vielfache aller r_i sein. qed.

Die Eindeutigkeit der in S (9.2) eingeführten Produktdarstellung sowie die bisher besprochenen Rechenvorteile beruhen wesentlich auf der Elementfremdheit der als Faktoren auftretenden Zyklen. Läßt man auch Produkte von Zyklen zu, die gleiche Zahlen enthalten[1]), kann man zu den verschiedensten Darstellungen gelangen. So überzeugt man sich z. B. sofort durch Ausmultiplikation, daß etwa die folgenden Produkte Zerlegungen derselben Permutation sind:

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 7 & 4 & 8 & 9 & 1 & 2 & 6 \end{pmatrix} \begin{cases} = (1\,3\,7)(2\,5\,8)(6\,9) \\ = (1\,3\,7\,8)(8\,1)(2\,5\,8\,6\,9)(6\,2) \\ = (1\,3)(1\,7)(2\,5)(2\,8)(6\,9). \end{cases}$$

---

1) Auch die Multiplikation solcher nichtelementfremder Zyklen ist übersichtlicher durchzuführen als die der ihnen entsprechenden ausführlich geschriebenen zyklischen Permutationen. In der Tat kommt es doch nur auf die wirklich veränderten Zahlen an, die ja gerade in den Zyklen auftreten;

z. B. $(1\,9\,5\,7)(7\,4\,5\,9) = (1\,7)(4\,5)$

wegen

$1 \to 9 \to 7$	$1 \to 7$
$7 \to 1$	$7 \to 1$
$4 \to 5$	$4 \to 5$
$5 \to 7 \to 4$	$5 \to 4$
$9 \to 5 \to 9$	$9 \to 9$.

Von diesen Darstellungen interessieren besonders diejenigen, deren Zyklen alle zweigliedrig sind.

Definition **D (9.4)**

Ein zweigliedriger Zyklus heißt eine Transposition.

Satz **S (9.5)**

Jede Permutation s läßt sich als Produkt nicht notwendig elementfremder Transpositionen schreiben.

Beweis

Jeder Zyklus in der Hauptproduktdarstellung von s läßt sich zerlegen gemäß

$$(i_1 i_2 \ldots i_r) = (i_1 i_2)\,(i_1 i_3) \ldots (i_1 i_r).$$ qed.

Die Schreibweise einer Permutation s als Produkt von Zyklen gestattet, unabhängig von der Elementfremdheit der verwendeten Faktoren, eine besonders einfache Berechnung eines Produktes der Gestalt

$$s_0^{-1} \cdot s \cdot s_0.$$

Man nennt diese Produktbildung die *Transformation der Permutation s mit der Permutation* s_0, eine Begriffsbildung, deren Bedeutung wir erst später kennenlernen werden (vgl. § 15).

Satz **S (9.6)**

Eine Permutation s in einer beliebigen Zyklendarstellung

$$s = z_1 z_2 \ldots z_k$$

wird transformiert mit der Permutation s_0, *indem man in jedem Zyklus die auftretenden Zahlen der Permutation* s_0 *unterwirft.*

Beispiel:

Wir wählen

$$s = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 4\,5\,6\,3\,2\,1 \end{pmatrix} \quad \text{und} \quad s_0 = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 6\,2\,1\,5\,4\,3 \end{pmatrix}, \quad \text{also} \quad s_0^{-1} = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 3\,2\,6\,5\,4\,1 \end{pmatrix}.$$

Dann ist die umständliche Multiplikation

$$s_0^{-1} s s_0 = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 3\,2\,6\,5\,4\,1 \end{pmatrix} \cdot \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 4\,5\,6\,3\,2\,1 \end{pmatrix} \cdot \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 6\,2\,1\,5\,4\,3 \end{pmatrix} = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 3\,4\,6\,2\,1\,5 \end{pmatrix}$$

nach diesem Satz zu ersetzen durch Anwendung von s_0 auf die Zahlen in $s = (1\,4\,3\,6)\,(2\,5)$, und man erhält unmittelbar:

$$s_0^{-1} s s_0 = (6\,5\,1\,3)\,(2\,4).$$

Beweis

Zunächst gilt:

$$s_0^{-1} s s_0 = s_0^{-1} z_1 s_0 \cdot s_0^{-1} z_2 s_0 \cdot \ldots \cdot s_0^{-1} z_k s_0,$$

d. h., jeder Zyklus z wird einzeln transformiert. Ist $z = (i_1 i_2 \ldots i_r)$, so bringen wir s_0 auf die Form

$$s_0 = \begin{pmatrix} i_1 & i_2 & \ldots & i_r & i_{r+1} & \ldots & i_n \\ j_1 & j_2 & \ldots & j_r & j_{r+1} & \ldots & j_n \end{pmatrix}$$

und erhalten:

$$s_0^{-1} z s_0 = \begin{pmatrix} j_1 j_2 \ldots j_r j_{r+1} \ldots j_n \\ i_1 i_2 \ldots i_r i_{r+1} \ldots i_n \end{pmatrix} \cdot (i_1 i_2 \ldots i_r) \cdot \begin{pmatrix} i_1 i_2 \ldots i_r i_{r+1} \ldots i_n \\ j_1 j_2 \ldots j_r j_{r+1} \ldots j_n \end{pmatrix}.$$

Offensichtlich ergibt dies die zyklische Permutation

$$s_0^{-1} z s_0 = (j_1 \; j_2 \ldots j_r).$$

Sie entsteht aus z auf die behauptete Weise. qed.

Aufgaben zu § 9

1. Alle Permutationen der Gruppe $\mathfrak{S}_3$ sind zyklisch.
2. Man schreibe die folgenden Permutationen als Produkt elementfremder Zyklen und bestimme jeweils ihre Ordnung:
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 2 & 6 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 5 & 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 3 & 6 & 5 & 1 & 9 & 7 & 8 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 7 & 4 & 9 & 2 & 1 & 5 & 8 \end{pmatrix}.$$
3. Man gebe sämtliche Elemente der Gruppe $\mathfrak{S}_4$ in Zyklenschreibweise an und bestimme jeweils die Elementordnung.
4. Man begründe die am Ende des Beweises von S(9.2) aufgestellte Behauptung.
5. Man gebe ein Kriterium dafür an, welche Potenzen einer zyklischen Permutation $z = (i_1 i_2 \ldots i_r)$ selbst zyklisch sind. Was gilt insbesondere, falls r eine Primzahl p ist? (Hinweis: Man überlege sich zuvor, daß z^m entweder wieder ein r-gliedriger Zyklus ist oder in eine Anzahl Zyklen gleicher Länge zerfällt.)
6. Eine Permutation
$$s = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$$
wird mit der Permutation s_0 transformiert, indem man beide Zeilen von s für sich der Permutation s_0 unterwirft.
7. Man transformiere die in Aufgabe 2 angegebenen Permutationen mit
$$s_0 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 4 & 1 & 5 \end{pmatrix} \quad \text{bzw.} \quad s_0 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 3 & 1 & 9 & 8 & 7 & 6 & 5 \end{pmatrix}$$
auf die in S(9.6) und Aufgabe 6 erklärte Weise und überzeuge sich durch direkte Ausmultiplikation von der Richtigkeit der Ergebnisse.

§ 10. Gerade und ungerade Permutationen

In der identischen Permutation können die Zahlen so angeordnet werden, daß sie oben und unten in der natürlichen Reihenfolge stehen. Bei jeder anderen Permutation wird man in jeder Anordnung der Spalten mindestens ein Paar von Spalten finden, in denen die Anordnung oben gegenläufig der Anordnung unten ist:

$$s = \begin{pmatrix} \dots i_\mu \dots i_\nu \dots \\ \dots j_\mu \dots j_\nu \dots \end{pmatrix} \quad \text{mit} \quad \begin{matrix} i_\mu < i_\nu \\ j_\mu > j_\nu \end{matrix} \text{ oder umgekehrt.}$$

Eine nähere Untersuchung dieser Verhältnisse führt zu der wichtigen Unterscheidung der Permutationen in gerade und ungerade.

Definition **D (10.1)**

Unter einer Inversion der Permutation s versteht man das Auftreten eines Spaltenpaares

$$\binom{i_\mu}{j_\mu}, \binom{i_\nu}{j_\nu} \quad \textit{mit} \quad i_\mu < i_\nu,\ j_\mu > j_\nu \quad \textit{oder umgekehrt.}$$

Am einfachsten festzustellen sind die Inversionen einer Permutation, wenn ihre obere Zeile in der natürlichen Reihenfolge $1, \dots, n$ angeordnet ist, denn dann ist eine Inversion gekennzeichnet durch ein Zahlenpaar in der unteren Zeile, das nicht in der natürlichen Reihenfolge auftritt, z. B.:

$$s = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 4\,3\,1\,5\,2 \end{pmatrix} \text{ hat 6 Inversionen: } \begin{matrix} 1\,2 & 1\,3 & 1\,5 & 2\,3 & 2\,5 & 4\,5 \\ 4\,3, & 4\,1, & 4\,2, & 3\,1, & 3\,2, & 5\,2. \end{matrix}$$

Satz **S (10.2)**

Eine beliebige Umordnung der Spalten einer Permutation s ändert die Anzahl der Inversionen nicht.

Beispiel:

$$s = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 4\,5\,2\,1\,6\,3 \end{pmatrix} \text{ hat 8 Inversionen: } \begin{matrix} 1\,3 & 1\,4 & 1\,6 & 2\,3 & 2\,4 & 2\,6 & 3\,4 & 5\,6 \\ 4\,2, & 4\,1, & 4\,3, & 5\,2, & 5\,1, & 5\,3, & 2\,1, & 6\,3. \end{matrix}$$

Wir ordnen die Spalten von s um:

$$s = \begin{pmatrix} 2\,4\,5\,6\,1\,3 \\ 5\,1\,6\,3\,4\,2 \end{pmatrix} \text{ hat 8 Inversionen: } \begin{matrix} 2\,4 & 2\,6 & 2\,3 & 4\,1 & 4\,3 & 5\,6 & 6\,1 & 1\,3 \\ 5\,1, & 5\,3, & 5\,2, & 1\,4, & 1\,2, & 6\,3, & 3\,4, & 4\,2. \end{matrix}$$

Beweis

Die in Rede stehende Umordnung kann als Permutation der Spalten von s aufgefaßt und damit nach S(9.5) auf eine Anzahl von Vertauschungen zweier Spalten von s zurückgeführt werden. Jede solche Vertauschung ist ihrerseits herstellbar durch eine Anzahl von Vertauschungen je zweier benachbarter Spalten von s. Bei jeder der zuletzt genannten Vertauschungen bleibt aber die Anzahl der Inversionen von s erhalten. Für das vertauschte Spaltenpaar ist das nach unserer Definition selbstverständlich, für die davor oder dahinter stehenden Spalten von s ändert sich aber die Reihenfolge zu den Spalten des vertauschten Paares nicht.

qed.

Damit ist die Anzahl der Inversionen einer Permutation unabhängig von der Reihenfolge ihrer Spalten festgelegt. Wir können daher folgende Klasseneinteilung vornehmen:

Definition **D (10.3)**

Eine Permutation heißt gerade (bzw. ungerade), wenn die Anzahl ihrer Inversionen gerade (bzw. ungerade) ist.

Wir stellen einige Kriterien auf, die unabhängig vom Abzählen der Inversionen festzustellen gestatten, ob eine Permutation gerade oder ungerade ist.

Zu diesem Zwecke betrachten wir das sogenannte *Differenzenprodukt in n Variablen* $x_1, x_2, \ldots, x_n$[1])

$$P = \prod_{\mu<\nu} (x_\mu - x_\nu) = (x_1 - x_2) \cdot (x_1 - x_3) \cdot \ldots \cdot (x_1 - x_n) \cdot (x_2 - x_3) \cdot \ldots \cdot (x_2 - x_n) \cdot \ldots \cdot (x_{n-1} - x_n).$$

Die $\binom{n}{2}$ Faktoren $(x_\mu - x_\nu)$ von P entsprechen in ihren Indizes genau den $\binom{n}{2}$ möglichen Spaltenpaaren $\binom{\mu}{i_\mu}, \binom{\nu}{i_\nu}$ von

$$s = \begin{pmatrix} 1 & \ldots & \mu & \ldots & \nu & \ldots & n \\ i_1 & \ldots & i_\mu & \ldots & i_\nu & \ldots & i_n \end{pmatrix}.$$

1) Das Differenzenprodukt P ist bekanntlich identisch mit der VANDERMONDEschen Determinante (ALEXANDRE TH. VANDERMONDE, 1735 bis 1796).

Unter der Anwendung von s auf P versteht man die Vertauschung der Variablen $x_1, x_2, \ldots, x_n$ in P gemäß s:

$$s(P) = \prod_{\mu<\nu} (x_{i_\mu} - x_{i_\nu}).$$

Wählen wir z. B. $n = 3$, also

$$P = (x_1 - x_2)\ (x_1 - x_3)\ (x_2 - x_3),$$

so ergibt sich

$$\text{mit } s = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}: \ s(P) = (x_2 - x_3)\ (x_2 - x_1)\ (x_3 - x_1) = P,$$

dagegen

$$\text{mit } s = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}: \ s(P) = (x_3 - x_2)\ (x_3 - x_1)\ (x_2 - x_1) = -P.$$

Satz **S (10.4)**

Für das Differenzenprodukt P in n Variablen gilt bei der Anwendung einer beliebigen Permutation s vom Grad n,

$$\textit{falls } s \textit{ gerade ist}: \quad s(P) = P,$$
$$\textit{falls } s \textit{ ungerade ist}: \quad s(P) = -P.$$

Beweis

Jeder Index in P tritt, abgesehen von der Stellung, genau $(n-1)$-mal auf. Dies gilt auch für $s(P)$, da s eine eineindeutige Abbildung der Indizes vermittelt. Es hat also $s(P)$ bis auf Vorzeichen genau die gleichen Faktoren wie P. Vorzeichenwechsel ergibt sich für einen Faktor genau dann, wenn der vordere Index größer als der hintere wird, d. h. also in der oben eingeführten Bezeichnung für den Fall

$$i_\mu > i_\nu.$$

Da nach Voraussetzung aber stets $\mu < \nu$ ist, entspricht jeder Inversion genau ein Vorzeichenwechsel. Unter Berücksichtigung von D (10.3) folgt damit die Behauptung.

qed.

Folgerung **F (10.5)**

Für die Multiplikation von Permutationen gelten die den Vorzeichenregeln der Zahlenrechnung entsprechenden Aussagen:

Das Produkt zweier gerader Permutationen ist gerade.

Das Produkt einer geraden Permutation mit einer ungeraden Permutation ist (unabhängig von der Reihenfolge) ungerade.

Das Produkt zweier ungerader Permutationen ist gerade.

Der Beweis ergibt sich nach S (10.4) unmittelbar durch die Nacheinanderanwendung beider Permutationen auf das Differenzenprodukt P.

Nach F (10.5) ist es naheliegend, ein *Vorzeichen* für Permutationen einzuführen gemäß

$$\operatorname{sgn}(s) = \begin{cases} +1, \text{ falls } s \text{ eine gerade Permutation ist,} \\ -1, \text{ falls } s \text{ eine ungerade Permutation ist.} \end{cases}$$

Satz **S (10.6)**

Es sei die Permutation s auf irgendeine Weise als Produkt von Transpositionen dargestellt. Dann ist die Anzahl der auftretenden Transpositionen gerade, wenn s gerade ist, und ungerade, wenn s ungerade ist.

Beweis

Wir bemerken zuvor, daß für jedes s nach S (9.5) wenigstens eine solche Darstellung existiert. Weiterhin werden wir zeigen, daß eine Transposition

$$(i_1\ i_2) = \begin{pmatrix} i_1 & i_2 & i_3 & \dots & i_n \\ i_2 & i_1 & i_3 & \dots & i_n \end{pmatrix}$$

ungerade ist, woraus sich dann die Behauptung nach F (10.5) ergibt. Nun liegt bei den beiden ersten Spalten eine Inversion vor, während je zwei Spaltenpaare

$$\binom{i_1}{i_2}, \binom{i_\nu}{i_\nu} \quad \text{und} \quad \binom{i_2}{i_1}, \binom{i_\nu}{i_\nu} \quad \text{mit } \nu = 3, \dots, n$$

entweder keine oder zwei Inversionen ergeben[1]). Das erstere tritt ein, wenn i_1 und i_2 entweder beide größer oder beide kleiner als i_ν sind, das letztere dagegen für die übrigen Fälle, für die man ohne Beschränkung der Allgemeinheit etwa $i_1 < i_\nu < i_2$ annehmen kann.

qed.

Satz **S (10.7)**

Es sei die Permutation s nach S (9.2) *in der Hauptproduktdarstellung gegeben, in der l Zyklen z_i von der Länge r_i auftreten, also insgesamt $r = r_1 + \ldots + r_l$ Zahlen von s wirklich geändert werden.*

Dann ist die natürliche Zahl $k = r - l$ gerade, wenn s gerade ist, und ungerade, wenn s ungerade ist.

Beweis

Wir benutzen S (10.6) und stützen uns auf die in S (9.5) angegebene Zerlegung. Danach entstehen aus jedem Zyklus z_i genau $r_i - 1$ Transpositionen. Das ergibt für $s = z_1 z_2 \ldots z_l$ eine Zerlegung in

$$k = (r_1 - 1) + (r_2 - 1) + \ldots + (r_l - 1) = r - l$$

Transpositionen.

qed.

Eine für praktische Anwendungen besonders elegante Form des Kriteriums S (10.7) ist unmittelbar ersichtlich:

Folgerung **F (10.8)**

Man zähle in der Hauptproduktdarstellung der Permutation s diejenigen Zyklen ab, die eine gerade Anzahl von Zahlen enthalten. Je nachdem, ob sich dabei eine gerade oder ungerade Zahl ergibt, ist s gerade oder ungerade.

---

1) Mit anderen Worten: Bei der Feststellung, ob eine gerade oder ungerade Anzahl von Inversionen vorliegt, brauchen Spalten, in denen oben und unten dieselbe Zahl steht, nicht berücksichtigt zu werden.

Dies gilt übrigens allgemein für jede Permutation, wie sich aus dem nachfolgenden Satz S(10.7) ergibt, der nämlich lehrt, daß in Ruhe gelassene Zahlen auf das Vorzeichen einer Permutation ohne Einfluß sind.

Aufgaben zu § 10

1. Man stelle das Vorzeichen der in Aufgabe 2 von § 9 angegebenen 4 Permutationen nach D(10.1), S(10.6) und S(10.7) bzw. F(10.8) fest.
2. Man zeige, daß bei der Multiplikation einer Permutation s mit einer Transposition t von rechts genau zwei Zahlen in der unteren Zeile von s vertauscht werden.
3. Mit Hilfe von Aufgabe 2 ist direkt aus D(10.1) das Kriterium S(10.6) neu abzuleiten.
4. Eine Permutation s und die zu ihr inverse Permutation s^{-1} haben dasselbe Vorzeichen.
5. Das Vorzeichen einer Permutation s stimmt mit dem Vorzeichen jeder Permutation überein, die aus s durch Transformation entsteht.

§ 11. Gruppen von Permutationen

Die in den beiden vorangegangenen Paragraphen zusammengestellten Hilfsmittel ermöglichen uns eine eingehendere Untersuchung der symmetrischen Gruppe $\mathfrak{S}_n$ sowie ihrer Untergruppen. Wegen der Endlichkeit von $\mathfrak{S}_n$ kann man nach S(5.8) als Kriterium für Untergruppen $\mathfrak{H} \cdot \mathfrak{H} \subseteq \mathfrak{H}$ verwenden, d. h. ein Komplex $\mathfrak{H} \subseteq \mathfrak{S}_n$ ist genau dann Untergruppe, wenn die Multiplikation nicht aus ihm herausführt.

Die Bestimmung aller möglichen Untergruppen von $\mathfrak{S}_n$ für beliebiges n ist ein sehr schwieriges Problem, das allgemein zu lösen noch nicht gelungen ist. Selbst über die Anzahl dieser Untergruppen kann man noch keine allgemeinen Aussagen machen. Dagegen lassen sich spezielle Untergruppen auch allgemein angeben:

Satz **S (11.1)**

Die Menge der Permutationen aus $\mathfrak{S}_n$, die r beliebig vorgegebene Zahlen aus $1, \ldots, n$ fest lassen, bilden eine Untergruppe von $\mathfrak{S}_n$. Auf diese Art entstehen $\binom{n}{r}$ verschiedene[1]*) Untergruppen, die alle zu $\mathfrak{S}_{n-r}$ isomorph sind.*

---

1) In dem Ausnahmefall $r = n - 1$ stimmen natürlich die $\binom{n}{n-1} = n$ zu $\mathfrak{S}_1$ isomorphen Untergruppen $\{(1)\}, \ldots, \{(n)\}$ überein.

Beweis

Der erste Teil der Behauptung ergibt sich nach dem oben genannten Kriterium unmittelbar, denn aus $s_1(\nu) = \nu$ und $s_2(\nu) = \nu$ folgt auch $[s_1 \cdot s_2](\nu) = \nu$ für jedes der festgelassenen ν aus $1, \ldots, n$.
Ferner lassen sich aus n Zahlen auf genau $\binom{n}{r}$ verschiedene Weisen r Zahlen auswählen, die fest bleiben sollen. Dabei wird jedesmal die Menge der $n - r$ anderen Zahlen eineindeutig auf sich abgebildet, wobei ersichtlich alle möglichen Abbildungen dieser Art vorkommen. Die Gruppe dieser Abbildungen unterscheidet sich also von $\mathfrak{S}_{n-r}$ nur durch die Bezeichnung der permutierten Zahlen.

qed.

Wenden wir diesen Satz insbesondere in der Art an, daß wir die letzten r Zahlen aus $1, 2, \ldots, n$ fest lassen, erhalten wir:

Folgerung **F (11.2)**

Die Gruppen $\mathfrak{S}_2, \mathfrak{S}_3, \ldots, \mathfrak{S}_{n-1}$ können als Untergruppen von $\mathfrak{S}_n$ *aufgefaßt werden.*

Weiterhin ist folgende allgemeine Aussage für Untergruppen aus $\mathfrak{S}_n$ möglich:

Satz **S (11.3)**

Eine Untergruppe $\mathfrak{H}$ *von* $\mathfrak{S}_n$ *enthält entweder nur gerade Permutationen, oder sie besteht aus gleich vielen geraden und ungeraden Permutationen.*

Beweis

$\mathfrak{H}$ enthalte k gerade und l ungerade Permutationen, die wir wie folgt schreiben:

$$g_1, \ldots, g_k; u_1, \ldots, u_l.$$

Für $l = 0$ ist nichts zu beweisen. Ist $l > 0$, so multiplizieren wir sämtliche Elemente mit u_l und erhalten wegen der Eindeutigkeit der Division wieder alle Elemente von $\mathfrak{H}$:

$$g_1 u_l, \ldots, g_k u_l; u_1 u_l, \ldots, u_l u_l.$$

Damit enthält $\mathfrak{H}$ nach F (10.5) l gerade und k ungerade Permutationen, woraus bereits $k = l$ folgt.

qed.

Wenden wir diesen Satz insbesondere auf $\mathfrak{S}_n$ selbst an, so ergibt sich unter erneuter Berücksichtigung von F(10.5):

Satz **S(11.4)**

$\mathfrak{S}_n$ enthält genau $\frac{n!}{2}$ gerade und $\frac{n!}{2}$ ungerade Permutationen[1]*. Die $\frac{n!}{2}$ geraden Permutationen bilden eine Untergruppe von $\mathfrak{S}_n$, die sogenannte alternierende Gruppe $\mathfrak{A}_n$.*

Die ungeraden Permutationen bilden im Gegensatz zu den geraden Permutationen keine Untergruppe. Das ergibt sich ebenfalls aus F(10.5) oder schon aus der Überlegung, daß die identische Permutation gerade ist.

Der gleiche Zusammenhang, der nach § 2 zwischen der symmetrischen Gruppe und den symmetrischen Funktionen besteht, trifft für die alternierende Gruppe und die alternierenden Funktionen zu. Letztere sind dadurch gekennzeichnet, daß sie bei einer beliebigen Permutation ihrer Variablen bis auf den Faktor ± 1 ungeändert bleiben. Diesem möglichen Vorzeichenwechsel entspringt die Bezeichnung „alternierend". Ein Beispiel für eine alternierende Funktion haben wir bereits in dem Differenzenprodukt kennengelernt, das alle geraden Permutationen gestattet, dagegen bei ungeraden Permutationen das Vorzeichen ändert.

Wir stellen für die symmetrische Gruppe und die alternierende Gruppe möglichst handliche Erzeugendensysteme auf:

Satz **S(11.5)**

Die Transpositionen der Gestalt $(1\ k)$ mit $k = 2, \ldots, n$ bilden ein Erzeugendensystem für $\mathfrak{S}_n$:

$$\mathfrak{S}_n = \langle (1\ 2), (1\ 3), \ldots, (1\ n) \rangle.$$

Beweis

Die Menge sämtlicher Transpositionen aus $\mathfrak{S}_n$ ist nach S(9.5) sicher Erzeugendensystem für $\mathfrak{S}_n$. Es muß also nur gezeigt werden, daß alle Transpositionen aus den oben angegebenen erzeugt werden können.

---

1) Es versteht sich, daß in S(11.4) wie auch in S(11.5) $n \geqq 2$ sein muß, entsprechend in S(11.6) $n \geqq 3$.

Für $n = 2$ ist nichts zu beweisen. Im Falle $n \geqq 3$ gilt aber für $i \neq j$, $i \geqq 2$, $j \geqq 2$:

$$(1i)\,(1j)\,(1i) = (ij).$$

qed.

Satz **S (11.6)**

Die dreigliedrigen Zyklen der Gestalt $(1\,2\,k)$ *mit* $k = 3, \ldots, n$ *bilden ein Erzeugendensystem für* $\mathfrak{A}_n$:

$$\mathfrak{A}_n = \langle (1\,2\,3), (1\,2\,4), \ldots, (1\,2\,n) \rangle.$$

Beweis

1. Wir zeigen zunächst, daß die Gesamtheit aller dreigliedrigen Zyklen als Erzeugendensystem für $\mathfrak{A}_n$ ausreicht. Nach S (10.6) ist jede Permutation aus $\mathfrak{A}_n$ als Produkt einer geraden Anzahl von Transpositionen darzustellen. Jedes Paar dieser Transpositionen kann durch dreigliedrige Zyklen ausgedrückt werden, nämlich

$$(i_1 i_2)\,(j_1 j_2) = (i_1 i_2 j_2)\,(i_1 j_1 j_2)$$

oder

$$(i_1 i_2)\,(i_1 i_3) = (i_1 i_2 i_3),$$

je nachdem, ob die beiden Transpositionen elementfremd sind oder eine gemeinsame Zahl enthalten.

2. Der Beweis erfolgt nun analog dem Beweis von S (11.5). Die Behauptung gilt für $\mathfrak{A}_3$ und, wie man leicht nachprüft[1]), für $\mathfrak{A}_4$. Im Falle $n \geqq 5$ stehen zunächst nach Voraussetzung und wegen

$$(12j)\,(12i)\,(12j)^{-1} = (1ij)$$

alle dreigliedrigen Zyklen zur Verfügung, in denen die 1 auftritt. Dann lassen sich aber mit vier voneinander verschiedenen Zahlen i, j, k, l aus $2, \ldots, n$ wegen

$$(1li)\,(1jk)\,(1il) = (ijk)$$

alle dreigliedrigen Zyklen aus dem angegebenen Erzeugendensystem bilden.

qed.

---

1) In $\langle (123), (124) \rangle$ liegen die Elemente (123), (124), (134) = $(123)^{-1}(124)$, (234) = $(123)(124)^{-1}$ und deren Inverse, also alle möglichen dreigliedrigen Zyklen aus $\mathfrak{S}_4$.

Aufgaben zu § 11

1. Man stelle alle Untergruppen der Permutationsgruppe $\mathfrak{S}_4$ auf und gebe minimale Erzeugendensysteme an. Es gibt einschließlich der trivialen Untergruppen 30 Stück; man führe den Vollständigkeitsbeweis.
2. Man drücke alle Elemente der Gruppe $\mathfrak{A}_4$ durch das in S(11.6) angegebene Erzeugendensystem aus.
3. Auch für die Elemente der abzählbaren symmetrischen Gruppe $\mathfrak{S}_a$ (vgl. Aufg. 17 von § 5) läßt sich ein Vorzeichen einführen, da jedes Element $s \in \mathfrak{S}$ als Element einer symmetrischen Gruppe $\mathfrak{S}_n$ mit hinreichend großem n aufgefaßt werden kann und dort $\operatorname{sgn}(s)$ erklärt ist.

   Man zeige: Die Gesamtheit der Elemente $s \in \mathfrak{S}_a$ mit $\operatorname{sgn}(s) = +1$ bildet eine Untergruppe von $\mathfrak{S}_a$, die sog. abzählbare alternierende Gruppe $\mathfrak{A}_a$.

§ 12. Transitivität und Primitivität von Permutationsgruppen[1])

Weitere Unterscheidungsmöglichkeiten von Permutationsgruppen ergeben sich, indem man die Wirkung aller Permutationen einer Gruppe $\mathfrak{P}$ auf die Menge $\mathfrak{M}$ der permutierten Elemente betrachtet. Der Leser mag sich die Überlegung wie bisher an dem konkreten Beispiel der Menge $\mathfrak{M} = \{1, 2, \ldots, n\}$ veranschaulichen. Wir führen in $\mathfrak{M}$ eine Äquivalenzrelation ein:

Definition **D (12.1)**

Es sei $\mathfrak{P}$ eine beliebige Permutationsgruppe und $\mathfrak{M}$ die Menge der von $\mathfrak{P}$ permutierten Elemente. Dann heißt $a \in \mathfrak{M}$ $\mathfrak{P}$-konjugiert zu $b \in \mathfrak{M}$, wenn es wenigstens eine Permutation $s \in \mathfrak{P}$ gibt mit

$$s(a) = b.$$

Folgerung **F (12.2)**

Die in D(12.1) *festgelegte Beziehung ist eine Äquivalenzrelation in $\mathfrak{M}$.*

Sie ist nämlich wegen $(1) \in \mathfrak{P}$ reflexiv, wegen $s^{-1} \in \mathfrak{P}$ symmetrisch und wegen $s_1 \cdot s_2 \in \mathfrak{P}$ transitiv.

---

1) Für ein eingehenderes Studium der Permutationsgruppen sind die Ausführungen dieses Paragraphen interessant und bedeutungsvoll, doch ist ihre Kenntnis für unsere folgenden Untersuchungen nicht erforderlich.

Definition **D (12.3)**

Die Klassen der Klasseneinteilung von $\mathfrak{M}$, die der in D (12.1) *festgelegten Äquivalenzrelation entspricht, heißen Transitivitätsgebiete.*

Insbesondere heißt die Permutationsgruppe $\mathfrak{P}$ transitiv über $\mathfrak{M}$, wenn $\mathfrak{M}$ selbst das einzige auftretende Transitivitätsgebiet ist, sonst intransitiv.

Eine Permutationsgruppe ist also genau dann transitiv über $\mathfrak{M}$, wenn zu jedem $a \in \mathfrak{M}$ und jedem $b \in \mathfrak{M}$ ein $s \in \mathfrak{P}$ mit $s(a) = b$ existiert. Wie aus den Eigenschaften der Äquivalenzrelation folgt, ist dafür hinreichend und notwendig, daß irgendein festes $a \in \mathfrak{M}$ durch Permutationen aus $\mathfrak{P}$ in alle $b \in \mathfrak{M}$ übergeführt wird. Dies erleichtert die Feststellung der Transitivität bzw. Intransitivität einer Permutationsgruppe wesentlich.

Beispiele:

Eine transitive Permutationsgruppe ist die in § 4 genannte KLEINsche Vierergruppe $\mathfrak{B}_4$ mit den Elementen

$$(1),\ (12)(34),\ (13)(24),\ (14)(23);$$

denn von diesen Permutationen wird der Reihe nach z. B. die Zahl $a = 1$ in 1, 2, 3 und 4 übergeführt. Die Menge $\mathfrak{M} = \{1, 2, 3, 4\}$ besteht also bezüglich $\mathfrak{B}_4$ aus genau einem Transitivitätsgebiet.

Dagegen ist die aus den Permutationen

$$(1),\ (12),\ (34),\ (12)(34)$$

bestehende Gruppe intransitiv, denn es gibt in ihr z. B. keine Permutation, die 1 in 3 überführt. Die Menge $\mathfrak{M} = \{1, 2, 3, 4\}$ zerfällt bezüglich dieser Permutationsgruppe in die zwei Transitivitätsgebiete $\{1, 2\}$ und $\{3, 4\}$.

Die beiden Beispiele sind insofern besonders interessant, als beide Gruppen zueinander isomorph sind. Das unterstreicht die Abhängigkeit der hier behandelten Begriffsbildungen von der konkreten Gestalt der Gruppenelemente.

Ferner sind sowohl $\mathfrak{S}_n$ als auch $\mathfrak{A}_n$ über $\mathfrak{M} = \{1, 2, \ldots, n\}$ transitiv. Dies folgt etwa daraus, daß beide Gruppen jedenfalls die folgenden Permutationen enthalten:

$$(1),\ (1\ 2\ n),\ (1\ 3\ n),\ \ldots,\ (1\ n{-}1\ n),\ (1\ n\ n{-}1).$$

Zur weiteren Untersuchung transitiver Permutationsgruppen benötigen wir eine bequeme Bezeichnung derjenigen Untergruppen, die einzelne Elemente von $\mathfrak{M}$ fest lassen (vgl. Aufg. 2).

Definition **D (12.4)**

Es sei $\mathfrak{P}$ eine Permutationsgruppe von $\mathfrak{M}$ und a ein beliebiges Element aus $\mathfrak{M}$. Dann nennt man die Untergruppe derjenigen Permutationen s mit $s(a) = a$ die Stabilitätsuntergruppe $\mathfrak{H}_a$ von $\mathfrak{P}$.

Satz **S (12.5)**

Man erhält jede Stabilitätsuntergruppe $\mathfrak{H}_b$ einer transitiven Permutationsgruppe $\mathfrak{P}$ durch Transformation einer fest vorgegebenen Stabilitätsuntergruppe $\mathfrak{H}_a$ mit einem geeigneten Element aus $\mathfrak{P}$:

$$\mathfrak{H}_b = s^{-1}\,\mathfrak{H}_a s \quad \textit{mit } s(a) = b.$$

Beweis

Nach D (12.4) enthält $\mathfrak{H}_a$ genau alle Permutationen aus $\mathfrak{P}$, die a festlassen. Zu beliebigem $b \in \mathfrak{M}$ existiert wegen der Transitivität von $\mathfrak{P}$ wenigstens ein $s \in \mathfrak{P}$ mit $s(a) = b$. Das Komplexprodukt $s^{-1}\,\mathfrak{H}_a s$ ist die Menge aller mit s transformierten Permutationen aus $\mathfrak{H}_a$. Da in der Hauptproduktdarstellung jeder Permutation aus $\mathfrak{H}_a$ das Element a nicht auftritt, gilt nach S (9.6) das gleiche für das Element b in den Permutationen von $s^{-1}\,\mathfrak{H}_a s$, d. h., man erhält

$$s^{-1}\,\mathfrak{H}_a s \subseteq \mathfrak{H}_b.$$

Geht man umgekehrt von $\mathfrak{H}_b$ aus mit $s^{-1}(b) = a$, so ergibt sich

$$s\,\mathfrak{H}_b s^{-1} \subseteq \mathfrak{H}_a$$

und damit

$$\mathfrak{H}_b \subseteq s^{-1}\,\mathfrak{H}_a s.$$

Das zeigt die behauptete Gleichheit.

qed.

Satz **S (12.6)**

Es sei $\mathfrak{H}_a$ eine Stabilitätsuntergruppe der transitiven Permutationsgruppe $\mathfrak{P}$. Dann überführen genau die Permutationen jeder Rechtsnebenklasse $\mathfrak{H}_a \cdot s$ von $\mathfrak{H}_a$ in $\mathfrak{P}$ das Element a in das Element $s(a)$.

Beweis

Es sei $h_a \cdot s$ eine beliebige Permutation aus $\mathfrak{H}_a \cdot s$. Dann ist

$$[h_a \cdot s]\,(a) = s\,(h_a\,(a)) = s\,(a).$$

Andererseits sei s' eine beliebige Permutation aus $\mathfrak{P}$ mit

$$s'(a) = s(a).$$

Wir zeigen, daß dann s' in $\mathfrak{H}_a \cdot s$ enthalten ist. Es gilt nämlich

$$s^{-1}(s'(a)) = s^{-1}(s(a))$$

und daher

$$[s' \cdot s^{-1}](a) = a.$$

Daraus folgt

$$s' \cdot s^{-1} \in \mathfrak{H}_a, \text{ also } s' \in \mathfrak{H}_a \cdot s.$$

qed.

Aus der Zerlegung von $\mathfrak{P}$ in Rechtsnebenklassen nach $\mathfrak{H}_a$ ergibt sich damit die wichtige

Folgerung **F (12.7)**

Der Index $(\mathfrak{P}:\mathfrak{H}_a)$ *jeder Stabilitätsuntergruppe* $\mathfrak{H}_a$ *einer transitiven Permutationsgruppe* $\mathfrak{P}$ *ist gleich der Anzahl der Elemente von* $\mathfrak{M}$.

Falls eine Permutationsgruppe $\mathfrak{P}$ über der Menge $\mathfrak{M}$ transitiv ist, erhalten wir vermöge D (12.1) keine echte Klasseneinteilung von $\mathfrak{M}$. Es ist aber unter Umständen möglich, dann auf andere Weise zu einer Klasseneinteilung in $\mathfrak{M}$ zu gelangen, die ihrerseits wieder Eigenschaften der transitiven Permutationsgruppe $\mathfrak{P}$ kennzeichnet. Wir bezeichnen dazu mit $s(\mathfrak{M}_1)$ die Menge aller der durch $s \in \mathfrak{P}$ gelieferten Bilder der Elemente einer beliebigen Untermenge $\mathfrak{M}_1 \subseteq \mathfrak{M}$.

Definition **D (12.8)**

Eine Untermenge $\mathfrak{M}_1$ *von* $\mathfrak{M}$ *heißt Primitivitätsgebiet*[1]) *bezüglich der über* $\mathfrak{M}$ *transitiven Permutationsgruppe* $\mathfrak{P}$, *wenn* $\mathfrak{M}_1$ *die beiden Bedingungen erfüllt:*

1. $\mathfrak{M}_1$ *enthält mindestens zwei Elemente.*
2. *Es ist entweder* $s(\mathfrak{M}_1) \subseteq \mathfrak{M}_1$ *oder* $s(\mathfrak{M}_1)$ *elementfremd zu* $\mathfrak{M}_1$ *für* $s \in \mathfrak{P}$.

Es bildet also jede Permutation $s \in \mathfrak{P}$ entweder alle Elemente eines Primitivitätsgebietes $\mathfrak{M}_1$ wieder auf $\mathfrak{M}_1$ oder alle Elemente

1) Die Bezeichnung ist in der Literatur nicht feststehend. So werden Primitivitätsgebiete oft Imprimitivitätsgebiete wie übrigens auch Transitivitätsgebiete teilweise Intransitivitätsgebiete genannt.

von $\mathfrak{M}_1$ auf Elemente ab, die nicht in $\mathfrak{M}_1$ enthalten sind. Offensichtlich ist $\mathfrak{M}$ selbst Primitivitätsgebiet bezüglich $\mathfrak{P}$; daneben kann es aber auch echte Untermengen von $\mathfrak{M}$ mit dieser Eigenschaft geben. So haben wir z. B. in der Menge $\mathfrak{M} = \{1, 2, 3, 4\}$ bezüglich $\mathfrak{P} = \mathfrak{B}_4$ außer $\mathfrak{M}$ die folgenden sechs Primitivitätsgebiete:

$$\{1, 2\},\ \{1, 3\},\ \{1, 4\},\ \{3, 4\},\ \{2, 4\},\ \{2, 3\}.$$

Es liegen nämlich etwa die Bilder von 1 und 2 bei (1) und bei (12) (34) wieder in $\{1, 2\}$, bei (13) (24) und bei (14) (23) aber außerhalb von $\{1, 2\}$.

In Verallgemeinerung des Begriffes der Stabilitätsuntergruppe, die ein einzelnes Element aus $\mathfrak{M}$ invariant läßt, ist jetzt diejenige Untergruppe zu betrachten, die ein ganzes Primitivitätsgebiet $\mathfrak{M}_1$ in sich überführt. Offensichtlich bilden nämlich alle Permutationen $h \in \mathfrak{P}$ mit (vgl. Aufg. 9)

$$h(\mathfrak{M}_1) = \mathfrak{M}_1$$

eine Untergruppe $\mathfrak{H}$ von $\mathfrak{P}$, wofür wir

$$\mathfrak{H}(\mathfrak{M}_1) = \mathfrak{M}_1$$

schreiben. Wir vermerken, daß $\mathfrak{H}$ sämtliche Stabilitätsuntergruppen $\mathfrak{H}_a$ mit $a \in \mathfrak{M}_1$ enthält.

Satz **S (12.9)**

Es sei $\mathfrak{M}_1$ ein Primitivitätsgebiet von $\mathfrak{M}$ bezüglich der transitiven Permutationsgruppe $\mathfrak{P}$ und $\mathfrak{H}$ die eben erklärte Untergruppe von $\mathfrak{P}$ mit $\mathfrak{H}(\mathfrak{M}_1) = \mathfrak{M}_1$.

Dann überführen die Permutationen jeder Rechtsnebenklasse $\mathfrak{H} \cdot s$ von $\mathfrak{H}$ in $\mathfrak{P}$ die Elemente aus $\mathfrak{M}_1$ in die Elemente aus $s(\mathfrak{M}_1)$. Dabei ist $s(\mathfrak{M}_1)$ elementfremd zu $s'(\mathfrak{M}_1)$ für alle $s' \notin \mathfrak{H} \cdot s$ und $s(\mathfrak{M}_1)$ ebenfalls Primitivitätsgebiet von $\mathfrak{M}$ bezüglich $\mathfrak{P}$.

Beweis

Sei $h \cdot s$ eine beliebige Permutation aus $\mathfrak{H} \cdot s$. Dann ist

$$[h \cdot s]\,(\mathfrak{M}_1) = s(h(\mathfrak{M}_1)) = s(\mathfrak{M}_1).$$

Den zweiten Teil der Behauptung beweisen wir indirekt. Wäre etwa

$$s'(a_1) = s(b_1) \quad \text{mit } a_1 \in \mathfrak{M}_1,\ b_1 \in \mathfrak{M}_1,$$

so folgt

$$s^{-1}(s'(a_1)) = s^{-1}(s(b_1))$$
$$[s'\,s^{-1}](a_1) = b_1,$$

also ist $s'\,s^{-1} \in \mathfrak{H}$ und damit $s' \in \mathfrak{H} \cdot s$ im Widerspruch zur Voraussetzung.

Es ist $s(\mathfrak{M}_1)$ ebenfalls Primitivitätsgebiet. Ist nämlich x eine beliebige Permutation aus $\mathfrak{P}$, so ist

$$x(s(\mathfrak{M}_1)) = [sx](\mathfrak{M}_1) \begin{cases} = \mathfrak{M}_1 \text{ für } sx \in \mathfrak{H}, \\ \text{elementfremd zu } \mathfrak{M}_1 \text{ sonst,} \end{cases}$$

letzteres nach dem zuvor Bewiesenen. qed.

Folgerung **F (12.10)**

Mit den Bezeichnungen aus S (12.9) *sei*

$$\mathfrak{P} = \mathfrak{H} \cup \mathfrak{H} \cdot s_2 \cup \quad \cup \mathfrak{H} \cdot s_l$$

die Zerlegung von $\mathfrak{P}$ in Rechtsnebenklassen nach $\mathfrak{H}$. Dann entspricht ihr eine Klasseneinteilung von $\mathfrak{M}$

$$\mathfrak{M} = \mathfrak{M}_1 \cup s_2(\mathfrak{M}_1) \cup \ldots \cup s_l(\mathfrak{M}_1)$$

in $l = (\mathfrak{P}:\mathfrak{H})$ Primitivitätsgebiete bezüglich $\mathfrak{P}$. Letztere enthalten gleich viele Elemente, es ist also der Index von $\mathfrak{H}$ in $\mathfrak{P}$ ein Teiler der Anzahl der Elemente von $\mathfrak{M}$.

Beweis

Es bleibt nur die Aussage über die Anzahl der Elemente jeder Klasse zu zeigen. Diese folgt aber unmittelbar aus der Eineindeutigkeit der durch Permutationen vermittelten Abbildungen. qed.

Die Klasseneinteilung von $\mathfrak{M}$ in Primitivitätsgebiete bezüglich $\mathfrak{P}$ ist nicht notwendig eindeutig, da sie von der Wahl von $\mathfrak{M}_1$ abhängen kann. So gestattet die Menge $\mathfrak{M} = \{1, 2, 3, 4\}$ bezüglich $\mathfrak{P} = \mathfrak{B}_4$ in Abhängigkeit von $\mathfrak{M}_1$ die folgenden Klasseneinteilungen:

$\mathfrak{M}_1 = \{1, 2, 3, 4\}$: $\mathfrak{M} = \{1, 2, 3, 4\}$
$\mathfrak{M}_1 = \{1, 2\}$ oder $\mathfrak{M}_1 = \{3, 4\}$: $\mathfrak{M} = \{1, 2\} \cup \{3, 4\}$
$\mathfrak{M}_1 = \{1, 3\}$ oder $\mathfrak{M}_1 = \{2, 4\}$: $\mathfrak{M} = \{1, 3\} \cup \{2, 4\}$
$\mathfrak{M}_1 = \{1, 4\}$ oder $\mathfrak{M}_1 = \{2, 3\}$: $\mathfrak{M} = \{1, 4\} \cup \{2, 3\}$.

Die jeweils zugehörigen Untergruppen $\mathfrak{H}$ und die in F(12.10) aufgeführten Zerlegungen von $\mathfrak{P}$ nach $\mathfrak{H}$ sind in gleicher Reihenfolge:

$$\mathfrak{H} = \mathfrak{V}_4 \qquad \mathfrak{V}_4 = \mathfrak{H}$$
$$\mathfrak{H} = \{(1), (12)(34)\} \qquad \mathfrak{V}_4 = \mathfrak{H} \cup \mathfrak{H} \cdot (13)(24)$$
$$\mathfrak{H} = \{(1), (13)(24)\} \qquad \mathfrak{V}_4 = \mathfrak{H} \cup \mathfrak{H} \cdot (14)(23)$$
$$\mathfrak{H} = \{(1), (14)(23)\} \qquad \mathfrak{V}_4 = \mathfrak{H} \cup \mathfrak{H} \cdot (12)(34).$$

Die Primitivitätsgebiete jeder solchen Klasseneinteilung werden also bei allen Permutationen aus $\mathfrak{P}$ untereinander permutiert. Umgekehrt ist offensichtlich, daß jede Einteilung von $\mathfrak{M}$ in elementfremde Untermengen mit mindestens zwei Elementen, die bei allen Permutationen von $\mathfrak{P}$ untereinander permutiert werden, eine solche Klasseneinteilung in Primitivitätsgebiete liefert. Es werden damit ja sogar für jede dieser Untermengen die in D(12.8) festgelegten Eigenschaften gefordert.

Definition **D (12.11)**

Die transitive Permutationsgruppe $\mathfrak{P}$ heißt primitiv über $\mathfrak{M}$, falls $\mathfrak{M}$ das einzige Primitivitätsgebiet von $\mathfrak{M}$ bezüglich $\mathfrak{P}$ ist, sonst imprimitiv.

Eine echte Klasseneinteilung in Primitivitätsgebiete ist also genau für imprimitive Permutationsgruppen möglich. $\mathfrak{V}_4$ ist ein Beispiel einer imprimitiven Gruppe. Dagegen sind $\mathfrak{S}_n$ und $\mathfrak{A}_n$ stets primitiv über $\mathfrak{M} = \{1, 2, \ldots, n\}$. Wäre nämlich die echte Untermenge $\mathfrak{M}_1 = \{a, b, \ldots\}$ von $\mathfrak{M}$ ein Primitivitätsgebiet und $x \notin \mathfrak{M}_1$, so würde $(abx) \in \mathfrak{A}_n < \mathfrak{S}_n$ die Zahl a in die Zahl $b \in \mathfrak{M}_1$, aber die Zahl b in die Zahl $x \notin \mathfrak{M}_1$ überführen im Widerspruch zu D(12.8).

Wir geben schließlich ein Kriterium dafür, daß eine transitive Permutationsgruppe $\mathfrak{P}$ über $\mathfrak{M}$ imprimitiv ist.

Satz **S (12.12)**

Es sei $\mathfrak{P}$ eine über $\mathfrak{M}$ transitive Permutationsgruppe und $\mathfrak{H}_a$ die Stabilitätsuntergruppe eines beliebigen Elementes $a \in \mathfrak{M}$. Dann ist $\mathfrak{P}$ imprimitiv über $\mathfrak{M}$ genau dann, wenn eine echte Untergruppe $\mathfrak{H} < \mathfrak{P}$ existiert, die ihrerseits $\mathfrak{H}_a$ echt enthält:

$$\mathfrak{H}_a < \mathfrak{H} < \mathfrak{P}.$$

Beweis

1. Ist $\mathfrak{P}$ imprimitiv, so liegt nach F(12.10) a in einem Primitivitätsgebiet $\mathfrak{M}_1 < \mathfrak{M}$, und $\mathfrak{H}$ ist die dazu vor S(12.9) konstruierte

Untergruppe. Aus F (12.10) folgt $\mathfrak{H} < \mathfrak{P}$. Andererseits kann $\mathfrak{H}$ nicht mit $\mathfrak{H}_a$ zusammenfallen. Es gibt nämlich wenigstens eine Permutation $h \in \mathfrak{P}$, die a in ein anderes Element von $\mathfrak{M}_1$ überführt. Nach D (12.8) gilt dann $h(\mathfrak{M}_1) \leqq \mathfrak{M}_1$ und somit $h \in \mathfrak{H}$, aber $h \notin \mathfrak{H}_a$.

2. Existiert umgekehrt eine Untergruppe $\mathfrak{H}$ mit $\mathfrak{H}_a < \mathfrak{H} < \mathfrak{P}$, so ist die Gesamtheit $\mathfrak{H}(a)$ der Bilder von a bei Anwendung aller Permutationen $h \in \mathfrak{H}$ ein Primitivitätsgebiet $\mathfrak{M}_1 < \mathfrak{M}$. $\mathfrak{M}_1$ enthält nämlich a und darüber hinaus noch wenigstens ein Element $b \neq a$, weil sonst $\mathfrak{H} = \mathfrak{H}_a$ wäre. Ferner ist $\mathfrak{M}_1 < \mathfrak{M}$, denn sonst müßte jedes Element aus $\mathfrak{M}$ als $h(a)$ mit $h \in \mathfrak{H}$ geschrieben werden können. Daraus folgte aber nach S (12.6), daß $\mathfrak{H}$ aus jeder Rechtsnebenklasse $\mathfrak{H}_a \cdot s$ von $\mathfrak{H}_a$ in $\mathfrak{P}$ wenigstens ein Element und damit wegen $\mathfrak{H}_a < \mathfrak{H}$ sämtliche Rechtsnebenklassen enthalten würde, also $\mathfrak{H} \geqq \mathfrak{P}$ im Widerspruch zu $\mathfrak{H} < \mathfrak{P}$.

Wir müssen noch die zweite Eigenschaft aus D (12.8) für $\mathfrak{M}_1$ nachweisen. Nun ist einerseits

$$\mathfrak{H}(\mathfrak{M}_1) = \mathfrak{H}(\mathfrak{H}(a)) = [\mathfrak{H}\mathfrak{H}](a) = \mathfrak{H}(a) = \mathfrak{M}_1.$$

Andererseits hat für jedes $s \in \mathfrak{P}$ mit $s \notin \mathfrak{H}$ stets $s(\mathfrak{M}_1)$ mit $\mathfrak{M}_1$ kein Element gemeinsam. Denn würde

$$s(m_1) = m_1' \text{ mit } m_1 \in \mathfrak{M}_1,\ m_1' \in \mathfrak{M}_1$$

vorkommen, so folgt wegen $m_1 = h(a)$ und $m_1' = h'(a)$ mit $h \in \mathfrak{H}$ und $h' \in \mathfrak{H}$:

$$s(h(a)) = [hs](a) = h'(a)$$

$$[hsh'^{-1}](a) = a$$

$$[hsh'^{-1}] \in \mathfrak{H}_a < \mathfrak{H},$$

und damit ist $s = h^{-1}(hsh'^{-1})h'$ ein Produkt von Elementen aus $\mathfrak{H}$ im Widerspruch zu $s \notin \mathfrak{H}$. qed.

Man kann also nicht nur aus den Primitivitätsgebieten die zugehörigen Untergruppen $\mathfrak{H}$ konstruieren, sondern auch von diesen Untergruppen mit $\mathfrak{H}_a < \mathfrak{H} < \mathfrak{P}$ ausgehend die Primitivitätsgebiete erhalten. Weiterhin muß offensichtlich die Eigenschaft, daß eine echte Zwischengruppe existiert, für alle Stabilitätsuntergruppen einer transitiven Permutationsgruppe $\mathfrak{P}$ gleichzeitig erfüllt sein oder für keine. Dies ist wieder eine die Permutationsgruppen selbst betreffende Aussage, die aus der Betrachtung der Menge der permutierten Elemente $\mathfrak{M}$ gewonnen wurde. Desgleichen

kann man aus S(12.12) schließen, daß zwischen $\mathfrak{S}_{n-1}$ und $\mathfrak{S}_n$ und ebenso zwischen $\mathfrak{A}_{n-1}$ und $\mathfrak{A}_n$ keine echte Zwischengruppe existiert (Aufg. 11).

Aufgaben zu § 12

1. Welche Untergruppen der Gruppe $\mathfrak{S}_4$ sind über $\mathfrak{M} = \{1, 2, 3, 4\}$ transitiv, welche intransitiv? Im zweiten Falle gebe man die Transitivitätsgebiete an.
2. Es sei $\mathfrak{P}$ eine beliebige Permutationsgruppe der Menge $\mathfrak{M}$. Dann bilden alle Elemente aus $\mathfrak{P}$ mit $s(a) = a$ eine Untergruppe.
3. Für $\mathfrak{P} = \mathfrak{S}_4$ ist $\mathfrak{H}_4 = \mathfrak{S}_3$. Man konstruiere nach S(12.5) $\mathfrak{H}_1, \mathfrak{H}_2, \mathfrak{H}_3$.
4. Man zerlege $\mathfrak{S}_4$ in Rechtsnebenklassen nach $\mathfrak{H}_4 = \mathfrak{S}_3$ und veranschauliche S(12.6) und F(12.7).
5. Man untersuche die über $\mathfrak{M} = \{1, 2, 3, 4\}$ transitiven Untergruppen der $\mathfrak{S}_4$ (vgl. Aufg. 1) hinsichtlich ihrer Primitivitätsgebiete.
6. Die Permutationen

   (1), (145)(236), (154)(263), (12)(35)(46), (13)(24)(56), (16)(25)(34)

   bilden eine Untergruppe $\mathfrak{P}$ der symmetrischen Gruppe $\mathfrak{S}_6$. Man beweise, daß sie transitiv und imprimitiv über $\mathfrak{M} = \{1, 2, 3, 4, 5, 6\}$ ist, und gebe sämtliche Klasseneinteilungen von $\mathfrak{M}$ in Primitivitätsgebiete an.
7. Zu den in Aufgabe 6 festzustellenden Primitivitätsgebieten gebe man die zugehörigen Untergruppen $\mathfrak{H}$ an. Man veranschauliche sich die Aussage über $(\mathfrak{P} : \mathfrak{H})$ in F(12.10).
8. Die Vollständigkeit der Lösung der vorigen Aufgabe überprüfe man mit Hilfe von S(12.12).
9. Man begründe, warum aus $h(\mathfrak{M}_1) \subseteq \mathfrak{M}_1$ stets $h(\mathfrak{M}_1) = \mathfrak{M}_1$ folgt (Bezeichnung wie im Text).
10. $\mathfrak{P}$ sei die Untergruppe $\langle (13), (14)(23) \rangle$ der symmetrischen Gruppe $\mathfrak{S}_4$. Man veranschauliche S(12.12) an sämtlichen Stabilitätsuntergruppen.
11. Man beweise die im Text im Anschluß an S(12.12) formulierten Behauptungen.

§ 13. Gruppen von Deckabbildungen geometrischer Gebilde

Die folgenden Betrachtungen beschäftigen sich mit Symmetrieeigenschaften geometrischer Gebilde. Dazu stellen wir uns ein geometrisches Gebilde G als starren Körper vor (unabhängig von der Dimension) und untersuchen, auf welche verschiedene Weisen G in den ursprünglich von ihm eingenommenen Raum eingefügt werden kann. Man denke etwa an einen Würfel, der in ein genau pas-

sendes Futteral hineinzulegen ist, oder an ein aus einem Blatt Papier ausgeschnittenes Quadrat, das in den entstandenen Ausschnitt einzupassen ist. Die verschiedenen dabei möglichen Lagen bezeichnen wir als *Symmetrielagen* des Gebildes G, den Übergang von einer zur anderen als *Deckabbildung* von G. Bei einer nichtidentischen Deckabbildung von G bleibt entweder eine *Symmetrieachse* oder ein *Symmetriepunkt* oder kein Punkt in Ruhe.

Für sehr viele geometrische Gebilde gibt es nur eine Symmetrielage und damit nur die identische Deckabbildung. Jedoch gestatten gerade die wichtigsten geometrischen Gebilde mehrere Symmetrielagen (etwa Würfel, Quader, Quadrat, gleichschenkliges und gleichseitiges Dreieck) oder sogar unendlich viele Symmetrielagen (etwa Kugel, Zylinder, Kegel, Kreis, Gerade) und damit entsprechend viele Deckabbildungen. Von ihrem rein geometrischen Interesse abgesehen sind diese Untersuchungen insbesondere für die Kristallographie wichtig, sie gestatten jedoch auch die Anwendung mathematischer Methoden auf Probleme der bildenden Kunst, wie z. B. Mustergestaltung und Ornamentik.

Jede Deckabbildung eines geometrischen Gebildes G bildet die Gesamtheit aller Punkte dieses Gebildes eineindeutig auf sich selbst ab. Unter allen möglichen eineindeutigen Abbildungen der Menge $\mathfrak{M}$ dieser Punkte auf sich selbst sind sie dadurch ausgezeichnet, daß sie die gegenseitige Lage der Punkte zueinander invariant lassen. Die Menge der Deckabbildungen von G ist also ein Komplex $\mathfrak{A}$ in der Gruppe $\mathfrak{T}$ aller Transformationen von $\mathfrak{M}$ (vgl. B (2.6)).

Satz **S (13.1)**

Die Gesamtheit $\mathfrak{A}$ aller Deckabbildungen eines geometrischen Gebildes G bildet mit der für Transformationen erklärten Verknüpfung (Nacheinanderausführung) eine Gruppe.

Beweis

Der Gedanke, die Gesamtheit der Deckabbildungen $\mathfrak{A}$ als Komplex einer Transformationsgruppe aufzufassen, erleichtert nach S (5.5) den Beweis, da wir nur $\mathfrak{A} \cdot \mathfrak{A} \subseteq \mathfrak{A}$ und $\mathfrak{A}^{-1} \subseteq \mathfrak{A}$ zu zeigen brauchen. Die Nacheinanderausführung zweier Deckabbildungen von G entspricht aber stets dem Übergang von einer Symmetrielage von G zu einer anderen, also wieder einer Deckabbildung von G, d. h. $\mathfrak{A} \cdot \mathfrak{A} \subseteq \mathfrak{A}$. Wenn weiterhin eine beliebige Deck-

abbildung das Gebilde G aus einer ersten Symmetrielage in eine zweite überführt, so ist der Übergang von der zweiten Symmetrielage in die erste die zur genannten Deckabbildung inverse Deckabbildung. Die Nacheinanderausführung beider ergibt nämlich offensichtlich die identische Deckabbildung. Damit gilt auch $\mathfrak{A}^{-1} \leqq \mathfrak{A}$. qed.

Wir merken an, daß man den Beweis auch mühelos ohne Verwendung des Transformationsbegriffes direkt durchführen kann (vgl. Aufg. 2).

Zunächst untersuchen wir solche geometrischen Gebilde, deren Deckabbildungen eine endliche Gruppe bilden.

Gleichseitiges Dreieck **B (13.2)**

Ein gleichseitiges Dreieck hat sechs voneinander verschiedene Symmetrielagen $L_1, \ldots, L_6$ (vgl. Abb. 3). Wir können sie dadurch abzählen, daß jeder der drei Eckpunkte nach oben genommen werden kann und dabei noch je zwei Lagen für die beiden anderen

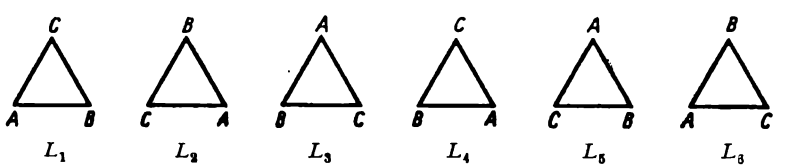


Abb. 3

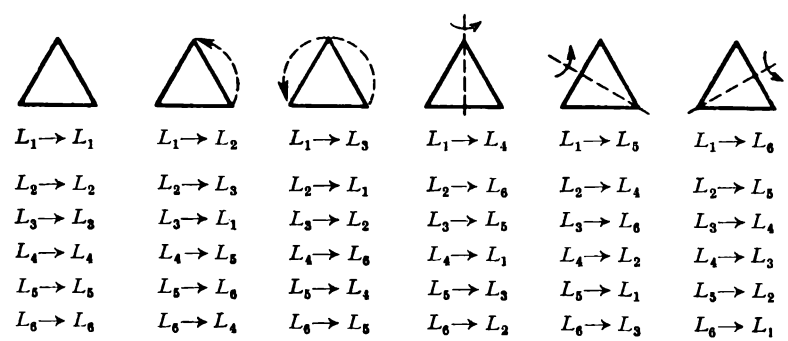


Abb. 4

Eckpunkte möglich sind. Wir haben damit zur Kennzeichnung der Deckabbildungen sechs Ausgangslagen und sechs Endlagen zur Verfügung. Es entstehen jedoch nicht $6 \cdot 6$, sondern nur 6 verschiedene Deckabbildungen, weil jede Bewegung des (starren) Dreiecks von 6 verschiedenen Ausgangslagen her beschrieben werden kann. Zum Beispiel wird die identische Deckabbildung durch $L_i \to L_i$ für $i = 1, \ldots, 6$ gekennzeichnet. Es genügt also zur Charakterisierung dieser sechs Deckabbildungen, von einer beliebig gewählten festen Lage auszugehen (vgl. Abb. 4).

Man kann diese Deckabbildungen wie folgt beschreiben:

$L_1 \to L_1$ als die identische Deckabbildung e.

$L_1 \to L_2$ als eine Drehung d des Dreiecks um den Schwerpunkt (Symmetriepunkt) mit einem Drehwinkel von $\frac{2\pi}{3}$ in mathematisch positivem Sinne.

$L_1 \to L_3$ als eine ebensolche Drehung um $2 \cdot \frac{2\pi}{3}$, die also gleich $d \cdot d = d^2$ ist.

$L_1 \to L_4$ als eine Umklappung (Spiegelung) u_1 um die Seitenhalbierende (Symmetrieachse) der Seite AB; für

$L_1 \to L_5$ als u_2 und

$L_1 \to L_6$ als u_3 gilt Entsprechendes.

Nach S(13.1) bilden diese sechs Deckabbildungen eine Gruppe $\mathfrak{D}_3$. Die von d und d^2 erzeugten zyklischen Untergruppen von der Ordnung 3 fallen zusammen:

$$\langle d \rangle = \langle d^2 \rangle = \{ d, d^2, d^3 = e \}.$$

Jede der drei Umklappungen erzeugt eine zyklische Gruppe der Ordnung 2:

$$\langle u_i \rangle = \{ u_i, u_i^2 = e \} \quad \text{für } i = 1, 2, 3.$$

Die Gruppe $\mathfrak{D}_3$ selbst ist vermöge der Zuordnungen

$$e \to (1), \quad d \to (123), \quad d^2 \to (132),$$
$$u_1 \to (12), \quad u_2 \to (13), \quad u_3 \to (23)$$

isomorph zur symmetrischen Gruppe $\mathfrak{S}_3$. Man erhält dies sofort, wenn man die Eckpunkte A, B, C des Dreieckes der Reihe nach als 1, 2, 3 bezeichnet und die Deckabbildungen als Permutationen

der Eckpunkte auffaßt. Diese Permutationen und ihre Nacheinanderausführungen beschreiben dann genau den gleichen Sachverhalt wie die Deckabbildungen.

Für die folgenden Verallgemeinerungen ist es am besten, die Gruppe $\mathfrak{D}_3$ durch die Erzeugung $\langle d, u\rangle$ zu beschreiben, wobei d ein primitives Element der zyklischen Gruppe aller Drehungen und u eine beliebige Umklappung ist. $\mathfrak{D}_3 = \langle d, u\rangle$ folgt sofort durch Abzählen der Elemente in der Zerlegung in Nebenklassen nach $\langle d\rangle$:

$$\mathfrak{D}_3 = \langle d\rangle \cup \langle d\rangle \cdot u.$$

Diese Erzeugung ist auch geometrisch evident. Wir können nämlich ein aus einem Blatt herausgeschnittenes Dreieck mit der ursprünglich von oben sichtbaren Fläche nach oben oder nach unten in den Ausschnitt einpassen. Diese beiden prinzipiellen Möglichkeiten bewirkt bereits eine beliebige Umklappung; von ihnen aus gelangt man allein durch Drehungen zu allen sechs Symmetrielagen.

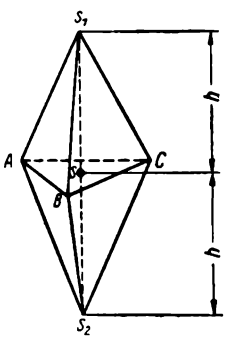


Abb. 5

Man kann sich das zuletzt Gesagte auch veranschaulichen, indem man statt der Deckabbildungen des Dreiecks die einer symmetrischen Doppelpyramide mit diesem Dreieck als Grundfläche betrachtet (vgl. Abb. 5). Ihre Symmetrielagen und Deckabbildungen stimmen offensichtlich mit denen des Dreiecks überein. Den Drehungen des Dreiecks um den Symmetriepunkt S entsprechen die der Doppelpyramide um die Symmetrieachse S_1S_2. Mit den Umklappungen ist die Vertauschung der Spitzen S_1 und S_2 verbunden. Setzen wir die Höhe $2h$ der Doppelpyramide gleich Null, so erhalten wir das Ausgangsdreieck als Spezialfall.

Regelmäßiges n-Eck **B (13.3)**

Die in B (13.2) entwickelten Gedankengänge lassen sich ohne weiteres auf ein beliebiges regelmäßiges n-Eck ($n \geqq 3$) ausdehnen.

Man nennt die Gruppe aller Deckabbildungen eines regelmäßigen n-Ecks die *Diedergruppe* $\mathfrak{D}_n$ [1]. Sie entspricht der Gruppe der

1) Der Name erklärt sich daraus, daß man das n-Eck als einen „Körper" auffaßt, der von zwei ebenen Flächenstücken („Di-eder") begrenzt wird.

Deckabbildungen einer symmetrischen Doppelpyramide mit dem regelmäßigen n-Eck als Grundfläche[1]) (vgl. Abb. 6 für $n = 6$). Die Gruppe $\mathfrak{D}_n$ enthält $2n$ Elemente, nämlich die n Elemente einer zyklischen Gruppe von Drehungen um die Winkel 0, $\frac{2\pi}{n}$, $2 \cdot \frac{2\pi}{n}$, $(n-1) \cdot \frac{2\pi}{n}$ sowie n Umklappungen (Spiegelungen). Die Drehungen erfolgen um den Schwerpunkt S des n-Ecks bzw. um die Symmetrieachse S_1S_2 der Pyramide, während die Symmetrieachsen der Umklappungen

für ungerades n durch jeden der n Eckpunkte zum Mittelpunkt der gegenüberliegenden Seiten verlaufen,

für gerades n zur Hälfte durch gegenüberliegende Eckpunkte, zur Hälfte durch gegenüberliegende Seitenmittelpunkte bestimmt sind.

Alle Symmetrieachsen gehen stets durch den Schwerpunkt S.

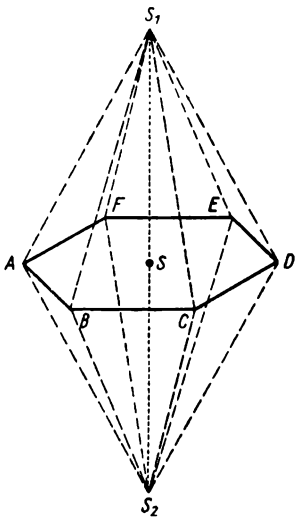


Abb. 6

Die Gruppe $\mathfrak{D}_n$ kann wieder mit Hilfe eines primitiven Elementes d der zyklischen Gruppe der Drehungen und einer Umklappung u erzeugt werden:

$$\mathfrak{D}_n = \langle d, u \rangle = \langle d \rangle \cup \langle d \rangle \cdot u.$$

Sie ist isomorph zu einer Untergruppe der symmetrischen Gruppe $\mathfrak{S}_n$; es entspricht nämlich jeder Deckabbildung eine bestimmte Permutation der Eckpunkte des regelmäßigen n-Ecks. Wegen $n! > 2n$ für $n > 3$ handelt es sich bis auf den Fall $n = 3$ um echtes Enthaltensein.

---

1) Für $n = 4$ entsteht bei geeigneter Höhe der Doppelpyramide das Oktaeder, dessen Deckabbildungen wir in B(13.6) behandeln. Dieser Spezialfall sei hier ausgeschlossen.

Aus den Betrachtungen von B (13.2) ergibt sich noch eine weitere, die Deckabbildungen eines beliebigen geometrischen Gebildes betreffende Verallgemeinerung:

Satz **S (13.4)**

Die Anzahl der Deckabbildungen eines geometrischen Gebildes G *stimmt mit der Anzahl der möglichen Symmetrielagen von* G *überein. Man kann zu ihrer Beschreibung von einer beliebig gewählten festen Lage ausgehen.*

Besonders interessante endliche Deckabbildungsgruppen besitzen die bekannten fünf regelmäßigen Polyeder.

Regelmäßiges Tetraeder **B (13.5)**

Ein regelmäßiges Tetraeder hat zwölf Symmetrielagen, deren Abzählung man vornimmt, indem jeder der vier Eckpunkte als oberer (vgl. Abb. 7) gewählt wird, wobei je noch drei Symmetrielagen der Figur möglich sind. Um die zwölf Deckabbildungen zu charakterisieren, können wir nach S (13.4) von der in Abb. 7 gewählten Lage ausgehen.

Um die Symmetrieachse AS_A sind die Drehungen um die Winkel $0, \frac{2\pi}{3}$ und $2 \cdot \frac{2\pi}{3}$ Deckabbildungen. Entsprechendes gilt für Drehungen um die Symmetrieachsen BS_B, CS_C und DS_D. Diese vier Symmetrieachsen gehen durch einen Eckpunkt und den Schwerpunkt der gegenüberliegenden Fläche des Tetraeders, weshalb man sie auch als Flächenmittellinien bezeichnet. In der Kristallographie werden sie aus verständlichem Grunde dreizählige Symmetrieachsen genannt. Abgesehen von der dabei viermal auftretenden identischen Deckabbildung sind die bisher genannten Deckabbildungen untereinander verschieden, da die zugehörigen Symmetrieachsen jeweils durch einen anderen festen Eckpunkt gehen. Wir haben also damit insgesamt neun verschiedene Deckabbildungen gekennzeichnet.

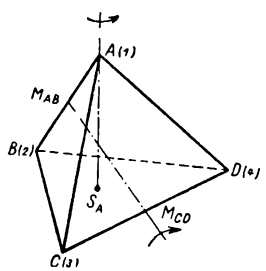


Abb. 7

Die drei noch fehlenden erhalten wir, wenn wir als Symmetrieachsen die sogenannten Kantenmittellinien verwenden. Sie gehen durch die Mittelpunkte einander gegenüberliegender Kanten ($M_{AB}M_{CD}$, $M_{AC}M_{BD}$, $M_{AD}M_{BC}$) und sind zweizählige Symmetrieachsen, da sie nur Drehungen um die Winkel 0 und $\frac{2\pi}{2}$ gestatten. Außer der dreimal auftretenden identischen Deckabbildung erhalten wir damit tatsächlich drei verschiedene Deckabbildungen, da sie z. B. den Punkt A in der angegebenen Reihenfolge in den Punkt B bzw. C bzw. D überführen. Sie sind auch von den übrigen neun verschieden, da sie im Gegensatz zu diesen keinen Eckpunkt der Figur fest lassen.

Die aus den eben aufgeführten 12 Deckabbildungen bestehende Gruppe wird *Tetraedergruppe* genannt. Sie kann von zwei Elementen erzeugt werden, und zwar von einer beliebigen der acht (nichttrivialen) Drehungen um eine der dreizähligen Symmetrieachsen und einer beliebigen der drei (nichttrivialen) Drehungen um eine der zweizähligen Symmetrieachsen. Der Beweis wird besonders einfach, wenn man die Isomorphie der Tetraedergruppe $\mathfrak{G}$ zur alternierenden Gruppe $\mathfrak{A}_4$ benutzt, die uns auch das Aufsuchen sämtlicher Untergruppen von $\mathfrak{G}$ erleichtert. Diese Isomorphie ergibt sich daraus, daß die zwölf von den Deckabbildungen vermittelten Permutationen der mit 1, 2, 3, 4 bezeichneten Eckpunkte A, B, C, D des Tetraeders eine Untergruppe der Ordnung 12 in der symmetrischen Gruppe $\mathfrak{S}_4$, also die alternierende Gruppe $\mathfrak{A}_4$ bilden. Den Untergruppen der $\mathfrak{A}_4$ entsprechen folgende Untergruppen von $\mathfrak{G}$:

a) $\{(1), (12)(34)\}$: Zyklische Gruppe der Drehungen um $M_{AB}M_{CD}$
$\{(1), (13)(24)\}$: Zyklische Gruppe der Drehungen um $M_{AC}M_{BD}$
$\{(1), (14)(23)\}$: Zyklische Gruppe der Drehungen um $M_{AD}M_{BC}$

b) KLEINsche Vierergruppe: Zusammengenommen ergeben die obigen Gruppen eine zu $\mathfrak{B}_4$ isomorphe Untergruppe von $\mathfrak{G}$. Ihre Deckabbildungen sind dadurch gekennzeichnet, daß sie entweder alle Eckpunkte in Ruhe lassen oder alle Eckpunkte verändern.

c) $\{(1), (234), (243)\}$: Zyklische Gruppe der Drehungen um AS_A
$\{(1), (134), (143)\}$: Zyklische Gruppe der Drehungen um BS_B
$\{(1), (124), (142)\}$: Zyklische Gruppe der Drehungen um CS_C
$\{(1), (123), (132)\}$: Zyklische Gruppe der Drehungen um DS_D

Weil damit bereits alle Untergruppen der $\mathfrak{A}_4$ aufgezählt sind, fällt jede von einer Drehung der Ordnung 2 und einer Drehung der Ordnung 3 erzeugte Untergruppe mit $\mathfrak{G}$ zusammen.

Würfel und regelmäßiges Oktaeder **B (13.6)**

Würfel und Oktaeder sind zueinander duale dreidimensionale Figuren[1]). Das bedeutet, daß man jedem Würfel in der in Abb. 8 angegebenen Weise ein Oktaeder und entsprechend jedem Oktaeder einen Würfel einbeschreiben kann. Symmetrielagen und Deckabbildungen dieser beiden Figuren entsprechen damit einander eineindeutig, so daß es genügte, nur eine von beiden zu betrachten. Es ist aber vorteilhaft, sich bei den Untersuchungen je nach Bedarf auf die Würfel- oder Oktaedervorstellung zu stützen.

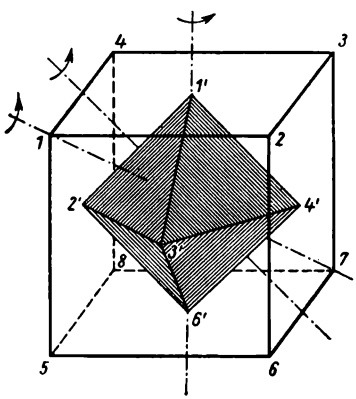


Abb. 8

Zur Abzählung der Symmetrielagen der in Abb. 8 ineinandergezeichneten Figuren benutzen wir das Oktaeder. Für jeden der 6 Eckpunkte als oberen Punkt gibt es genau 4 voneinander verschiedene, also insgesamt 24 Symmetrielagen. Ihnen entsprechen nach S(13.4) 24 Deckabbildungen, deren Gruppe $\mathfrak{G}$ man meist als *Oktaedergruppe* bezeichnet. Wir beschreiben die Deckabbildungen nach zyklischen Untergruppen geordnet.

Durch je zwei gegenüberliegende Eckpunkte des Oktaeders, etwa 1′ und 6′ (d. h. durch die Mittelpunkte gegenüberliegender Flächen des Würfels), geht eine vierzählige Symmetrieachse (Raumdiagonale des Oktaeders). Drehungen um die Winkel $0, \frac{2\pi}{4}, 2 \cdot \frac{2\pi}{4}$ und $3 \cdot \frac{2\pi}{4}$ liefern außer der identischen noch drei weitere Deck-

1) Das Dualitätsprinzip im Raume besagt, daß jede Inzidenzen (vereinigte Lagen) betreffende Aussage richtig bleibt, wenn man in ihr das Wort Punkt durch das Wort Ebene, das Wort Gerade durch das Wort Gerade und das Wort Ebene durch das Wort Punkt ersetzt. Da das Tetraeder zu sich selbst dual ist, gibt eine Berücksichtigung der Dualität in B(13.5) nichts Neues.

abbildungen, womit wir insgesamt $3 \cdot 3 + 1 = 10$ verschiedene Deckabbildungen gekennzeichnet haben. Sie liegen in drei zyklischen Gruppen der Ordnung 4.

Durch je zwei gegenüberliegende Eckpunkte des Würfels, etwa 1 und 7 (d. h. durch die Mittelpunkte gegenüberliegender Flächen des Oktaeders), geht eine dreizählige Symmetrieachse (Raumdiagonale des Würfels). Drehungen um die Winkel 0, $\frac{2\pi}{3}$ und $2 \cdot \frac{2\pi}{3}$ liefern außer der identischen noch zwei weitere Deckabbildungen, d. h. insgesamt 8 untereinander vershciedene, bisher noch nicht aufgeführte Deckabbildungen. Sie liegen in vier zyklischen Gruppen der Ordnung 3.

Die noch fehlenden 6 Deckabbildungen sind die nichttrivialen Drehungen um 6 zweizählige Symmetrieachsen, die durch die Mittelpunkte je zweier gegenüberliegender Kanten sowohl des Würfels wie des Oktaeders verlaufen, etwa durch $M_{1,4}\, M_{6,7}$. Sie liegen also in sechs zyklischen Gruppen der Ordnung 2.

Die mit den Deckabbildungen verbundenen Permutationen der Eckpunkte des Würfels lehren die Isomorphie der Gruppe $\mathfrak{G}$ zu einer Untergruppe der symmetrischen Gruppe $\mathfrak{S}_8$, die der Eckpunkte des Oktaeders die Isomorphie von $\mathfrak{G}$ zu einer Untergruppe der symmetrischen Gruppe $\mathfrak{S}_6$. Wir zeigen, daß $\mathfrak{G}$ isomorph zur symmetrischen Gruppe $\mathfrak{S}_4$ ist. Dazu bezeichnen wir die vier Raumdiagonalen $D_{1,7}$, $D_{2,8}$, $D_{3,5}$, $D_{4,6}$ des Würfels der Reihe nach mit D_1, D_2, D_3, D_4 und betrachten die durch die Deckabbildungen hervorgerufenen Permutationen dieser Diagonalen, was für einige Deckabbildungen in der folgenden Tabelle zusammengestellt ist.

Untergruppe von $\mathfrak{G}$	Beschrieben als Untergr. von $\mathfrak{S}_8$	Beschrieben als Untergr. von $\mathfrak{S}_6$	Beschrieben als Untergr. von $\mathfrak{S}_4$
Drehungen um $1'6'$	$\langle(1234)(5678)\rangle$	$\langle(2345)\rangle$	$\langle(1234)\rangle$
Drehungen um $D_{1,7}$	$\langle(245)(386)\rangle$	$\langle(123)(456)\rangle$	$\langle(243)\rangle$
Drehungen um $M_{1,4}\, M_{6,7}$	$\langle(14)(28)(35)(67)\rangle$	$\langle(12)(35)(46)\rangle$	$\langle(14)\rangle$

Es bleibt noch nachzuweisen, daß die den 24 Deckabbildungen von $\mathfrak{G}$ entsprechenden Permutationen der vier Diagonalen tat-

sächlich gerade die Elemente der $\mathfrak{S}_4$ sind. Dazu betrachten wir die Untergruppe $\langle (1234), (243) \rangle$, deren Elemente nach obiger Tabelle als Permutationen der vier Diagonalen auftreten. Nach F (7.8) hat diese Untergruppe mindestens die Ordnung $4 \cdot 3 = 12$. Da sie aber offensichtlich nicht die $\mathfrak{A}_4$ ist, folgt mit $\langle (1234), (243) \rangle = \mathfrak{S}_4$ die Behauptung.

Regelmäßiges Dodekaeder und Ikosaeder **B (13.7)**

Die Betrachtungen über Dodekaeder (Abb. 9a) und Ikosaeder (Abb. 9b) verlaufen entsprechend denen in B (13.6), wenn sie auch wesentlich komplizierter sind. Die Abzählung der Symmetrielagen der

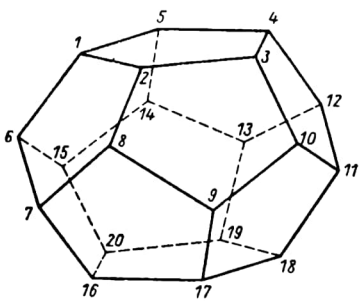


Abb. 9a

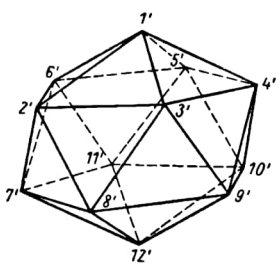


Abb. 9b

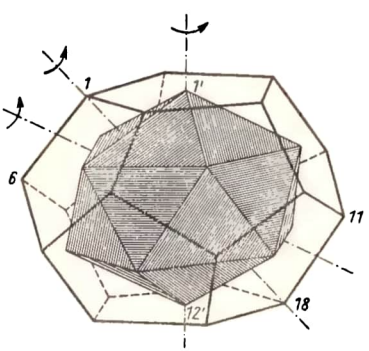


Abb. 9c

in Abb. 9c ineinandergezeichneten dualen Figuren ergibt für jeden oberen Punkt des Ikosaeders 5 verschiedene und somit insgesamt $12 \cdot 5 = 60$ Lagen. Die Gruppe $\mathfrak{G}$ der Deckabbildungen enthält also 60 Elemente; es ist üblich, sie als *Ikosaedergruppe* zu bezeichnen. Wir beschreiben die Deckabbildungen wieder nach zyklischen Untergruppen geordnet,

Durch je zwei gegenüberliegende Eckpunkte des Ikosaeders, etwa 1′ und 12′ (d. h. durch die Mittelpunkte gegenüberliegender Flächen des Dodekaeders), geht eine fünfzählige Symmetrieachse. Drehungen um die Winkel 0, $\frac{2\pi}{5}$, $2\cdot\frac{2\pi}{5}$, $3\cdot\frac{2\pi}{5}$ und $4\cdot\frac{2\pi}{5}$ liefern außer der identischen noch vier weitere Deckabbildungen, womit insgesamt $6\cdot 4+1=25$ verschiedene Deckabbildungen gekennzeichnet sind. Sie liegen in sechs zyklischen Gruppen der Ordnung 5.

Durch je zwei gegenüberliegende Eckpunkte des Dodekaeders, etwa 1 und 18 (d. h. durch die Mittelpunkte gegenüberliegender Flächen des Ikosaeders), geht eine dreizählige Symmetrieachse. Drehungen um die Winkel 0, $\frac{2\pi}{3}$ und $2\cdot\frac{2\pi}{3}$ liefern außer der identischen noch zwei weitere Deckabbildungen, d. h. insgesamt 20 untereinander verschiedene, bisher noch nicht aufgeführte Deckabbildungen. Sie liegen in zehn zyklischen Gruppen der Ordnung 3.

Die noch fehlenden 15 Deckabbildungen sind die nichttrivialen Drehungen um 15 zweizählige Symmetrieachsen, die durch die Mittelpunkte je zweier gegenüberliegender Kanten sowohl des Dodekaeders wie des Ikosaeders verlaufen, etwa durch $M_{1,6}$ und $M_{11,18}$. Sie liegen also in 15 zyklischen Gruppen der Ordnung 2.

Es ist wieder klar, daß die Ikosaedergruppe zu je einer Untergruppe der symmetrischen Gruppen $\mathfrak{S}_{20}$ und $\mathfrak{S}_{12}$ isomorph ist, was zu ihrem Studium jedoch kaum handliche Hilfsmittel liefert. Wichtig ist die Tatsache, daß die Ikosaedergruppe isomorph zur alternierenden Gruppe $\mathfrak{A}_5$ ist.

Der Grundgedanke des entsprechenden Beweises in B(13.6) war der, daß vier Figuren (nämlich die Würfeldiagonalen) in die Grundfigur eingezeichnet und deren Permutationen den Deckabbildungen eineindeutig zugeordnet wurden. Wir haben also hier fünf solche Figuren zu finden, die bei den Deckabbildungen des Ikosaeders ineinander übergeführt werden, wobei diese Permutationen der fünf Figuren genau die Elemente der $\mathfrak{A}_5$ ergeben müssen. Dies leisten fünf Oktaeder, die auf die folgende Weise dem Ikosaeder einbeschrieben werden.

Man geht von einem beliebigen Paar gegenüberliegender (also paralleler) Kanten des Ikosaeders aus. Zu diesem gibt es genau

zwei weitere solche Paare, die untereinander und zu dem ersten Paar senkrecht sind. Die Mittelpunkte dieser sechs Kanten bilden die Eckpunkte eines Oktaeders (vgl. Abb. 10). Aus den Symmetrieeigenschaften des Ikosaeders folgt, daß man von jedem Paar

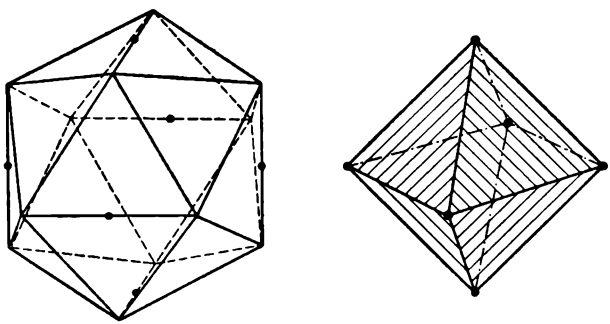


Abb. 10

gegenüberliegender Kanten ausgehen und somit insgesamt $30:6=5$ verschiedene Oktaeder einbeschreiben kann. Wir bezeichnen sie mit $O_1, O_2, \ldots, O_5$.

Offensichtlich entspricht nun jeder Deckabbildung des Ikosaeders eine Permutation der fünf Oktaeder. Alle so vermittelten Permutationen der $O_1, \ldots, O_5$ bilden eine Untergruppe $\mathfrak{U}$ der symmetrischen Gruppe $\mathfrak{S}_5$, die höchstens 60 verschiedene Permutationen enthalten kann. Wir zeigen, daß diese Untergruppe die $\mathfrak{A}_5$ enthält, woraus $\mathfrak{U}=\mathfrak{A}_5$ folgt.

Dazu beweisen wir, daß jeder dreigliedrige Zyklus $(O_i\, O_j\, O_k)$ in $\mathfrak{U}$ enthalten ist (vgl. S(11.6)): Die Mittelpunkte der Kanten jeder Ikosaederfläche gehören, da diese Kanten nicht senkrecht aufeinander stehen, zu drei verschiedenen Oktaedern. Aus Symmetriegründen gibt es dabei zu jedem Tripel O_i, O_j, O_k wenigstens eine Ikosaederfläche, deren Kantenmittelpunkte gerade Eckpunkte von O_i, O_j und O_k sind. Die Drehungen um die durch den Mittelpunkt dieser Fläche gehende dreizählige Symmetrieachse liefern bereits die Permutationen $(O_i\, O_j\, O_k)$ bzw. $(O_i\, O_k\, O_j)$ der Oktaeder O_i, O_j, O_k.

Auf die Aufzählung der 59 verschiedenen Untergruppen der Ikosaedergruppe bzw. der $\mathfrak{A}_5$ wollen wir hier verzichten. Wir vermerken

nur, daß es unter anderem fünf Untergruppen der Ordnung 12 gibt, deren Elemente dadurch charakterisiert sind, daß sie jeweils eines der fünf einbeschriebenen Oktaeder in sich überführen.

Schließlich untersuchen wir einige geometrische Gebilde, deren Deckabbildungen unendliche Gruppen bilden. Da wir dabei die geometrischen Sachverhalte als bekannt voraussetzen dürfen, beschränken wir uns im folgenden auf eine mehr referierende Darstellung.

Gerade, Kreis, Doppelkegel **B (13.8)**

Die unendlich vielen Symmetrielagen einer Geraden und die ihnen entsprechenden Deckabbildungen entstehen durch alle möglichen Verschiebungen der Geraden in sich und Umklappung dieser Geraden um jeden beliebigen ihrer Punkte. Die Gruppe $\mathfrak{G}$ aller Deckabbildungen ist nicht kommutativ, wie man sich durch Nacheinanderausführung einer beliebigen Verschiebung und einer beliebigen Umklappung in beiden Reihenfolgen überlegt. Dagegen bilden die Verschiebungen eine kommutative Untergruppe $\mathfrak{H} \leqq \mathfrak{G}$. Sie ist nämlich isomorph zur additiven Gruppe der reellen Zahlen, da man jede Verschiebung nach Länge und Richtung durch eine reelle Zahl kennzeichnen kann; der Nacheinanderausführung der Verschiebungen entspricht dann offensichtlich die Addition der zugehörigen reellen Zahlen. Weiterhin ist jede Umklappung durch eine fest vorgegebene Umklappung u mit nachfolgender Verschiebung zu beschreiben. Dies lehrt die Zerlegung

$$\mathfrak{G} = \mathfrak{H} \cup u \cdot \mathfrak{H}.$$

Für den Kreis und damit für den Doppelkegel gilt genau das Entsprechende, wobei die Umklappungen um einen beliebigen Durchmessers des Kreises erfolgen und mit den reellen Zahlen in der von der Trigonometrie her gewohnten Art modulo 2π zu rechnen ist.

Kreis und Doppelkegel stehen dabei in dem gleichen Verhältnis wie regelmäßiges n-Eck und die darüber errichtete Doppelpyramide und können als Grenzfall dieser Figuren für $n \to \infty$ aufgefaßt werden.

Ebene **B (13.9)**

Für die Ebene gibt es die folgenden Arten von Deckabbildungen: die Parallelverschiebungen der Ebene in sich in einer beliebigen

Richtung um eine beliebige Strecke, die Drehungen der Ebene in sich um jeden ihrer Punkte als Zentrum um jeden Winkel, die Umklappungen der Ebene um jede in ihr liegende Gerade und die aus je einer Umklappung und Parallelverschiebung zusammengesetzten Gleitspiegelungen. Sie zusammen bilden die Gruppe der Deckabbildungen dieser Ebene, aufgefaßt als geometrisches Gebilde des dreidimensionalen Raumes. Diese Gruppe entspricht natürlich der Kongruenzgruppe dieser Ebene, aufgefaßt als zweidimensionaler Raum, worauf wir im nächsten Paragraphen mit zu sprechen kommen.

Kugel **B (13.10)**

Die Deckabbildungen einer Kugel sind alle möglichen Drehungen um alle möglichen Durchmesser der Kugel. Die Gruppe der Deckabbildungen der Kugel fällt also mit der Drehungsgruppe der Kugel zusammen. Alle ihre Elemente können aus den Drehungen um zwei orthogonale Durchmesser zusammengesetzt werden. Untergruppen sind u. a. die Deckabbildungsgruppen aller regelmäßigen geometrischen Gebilde.

Aufgaben zu § 13

1. Man zeige, daß bei nichtidentischen Deckabbildungen eines geometrischen Gebildes G die Gesamtheit aller eventuell in Ruhe bleibenden Punkte von G entweder nur aus einem Punkt besteht (Symmetriepunkt) oder eine Gerade ist (Symmetrieachse).
2. Der Beweis von S(13.1) ist nach den Bemerkungen im Text erneut durchzuführen.
3. Welche Struktur hat die Gruppe der Deckabbildungen eines gleichschenkligen, aber nicht gleichseitigen Dreiecks?
4. Man beweise, daß die Gruppe der Deckabbildungen eines von einem Quadrat verschiedenen Rechtecks bzw. die einer symmetrischen Doppelpyramide mit diesem Rechteck als Grundfläche isomorph zur KLEINschen Vierergruppe $\mathfrak{V}_4$ ist. Das gleiche gilt für die Gruppe der Deckabbildungen eines Quaders mit nichtquadratischen Seitenflächen.
5. Man bestimme die zur Diedergruppe $\mathfrak{D}_4$ isomorphen Untergruppen von $\mathfrak{S}_4$.
6. Man beschreibe die den Untergruppen der symmetrischen Gruppe $\mathfrak{S}_4$ entsprechenden Untergruppen der Oktaedergruppe.
7. Man kennzeichne die Struktur der Gruppe der Deckabbildungen eines Kegels.
8. In welchem Verhältnis stehen die Gruppen der Deckabbildungen von Doppelkegel, Zylinder und Rotationsellipsoid?
9. Man kennzeichne die in B(13.9) beschriebenen Deckabbildungen durch die Anzahl ihrer Fixpunkte.

§ 14. Gruppen geometrischer Transformationen

In diesem Paragraphen gehen wir nochmals auf die bereits in B(2.7) zusammengestellten Transformationsgruppen des Erlanger Programms ein. Die analytische Darstellung der betreffenden Transformationen steht in einem engen Zusammenhang mit der Matrizen- und Vektorrechnung, die ihre praktische Handhabung wesentlich erleichtert und darüber hinaus Einsichten in die Struktur der genannten Gruppen ermöglicht.

Dazu beschreiben wir den dreidimensionalen Raum mit Hilfe homogener Koordinaten, d. h., wir kennzeichnen jeden Punkt P durch ein Quadrupel (x_1, x_2, x_3, x_4) reeller Zahlen, wobei jeweils diejenigen Quadrupel als nicht verschieden angesehen werden, die durch Multiplikation der Koordinaten mit einem konstanten Faktor $\lambda \neq 0$ auseinander hervorgehen; das Quadrupel $(0, 0, 0, 0)$ ist ausgeschlossen. Bekanntlich kann man sich solche Koordinaten aus den üblichen kartesischen Koordinaten (x, y, z) entstanden denken, wenn man jedes Quadrupel (x_1, x_2, x_3, x_4) mit $x_4 \neq 0$ als Repräsentant von $\left(\frac{x_1}{x_4}, \frac{x_2}{x_4}, \frac{x_3}{x_4}\right)$ ansieht. Die Quadrupel (x_1, x_2, x_3, x_4) mit $x_4 = 0$ stellen dann die sog. uneigentlichen oder unendlich fernen Punkte des Raumes dar.

a) Eine *projektive Transformation* ist gemäß unserer Definition eine solche eineindeutige Abbildung der Punkte des Raumes aufeinander, die unter Erhaltung der Inzidenz lineare Gebilde in lineare Gebilde überführt[1]). *Jede solche Transformation kann nun mit Hilfe einer nichtsingulären Matrix von Typ* (4,4) *beschrieben werden und umgekehrt, wobei jeweils Matrizen der Form* (a_{ik}) *und* $\lambda(a_{ik}) = (\lambda a_{ik})$, *die also durch Multiplikation mit einem konstanten Faktor* $\lambda \neq 0$ *auseinander hervorgehen, als gleichwertig anzusehen sind:*

$$(*) \qquad \bar{x}_k = \sum_{i=1}^{4} x_i a_{ik} \qquad (k = 1, \ldots, 4).$$

1) Man beachte, daß wir unter projektiven Transformationen nur die sog. „Kollineationen" verstehen (die jeweils Gebilde gleicher Dimension aufeinander abbilden) und die auf Grund des Dualitätsprinzips auch möglichen „Korrelationen" beiseite lassen (die im dreidimensionalen Fall Punkte und Ebenen wechselseitig aufeinander abbilden).

Unter Verwendung der Multiplikationsvorschrift verketteter Matrizen können wir mit $\bar{\mathfrak{x}} = (\bar{x}_1, \bar{x}_2, \bar{x}_3, \bar{x}_4)$, $\mathfrak{x} = (x_1, x_2, x_3, x_4)$ und $A = (a_{ik})$ dafür auch schreiben:

$$\bar{\mathfrak{x}} = \mathfrak{x} A .$$

Dann bestimmt sich $\mathfrak{x} = \bar{\mathfrak{x}} A^{-1}$ unter Verwendung von $A^{-1} = (\hat{a}_{ik})$ als

$$x_k = \sum_{i=1}^{4} \bar{x}_i \hat{a}_{ik} \qquad (k = 1, \ldots, 4) .$$

Wir zeigen zunächst, daß (*) in der Tat eine projektive Transformation darstellt. Die Gesamtheit aller Punkte $\mathfrak{x} = (x_1, x_2, x_3, x_4)$ einer Ebene (u_1, u_2, u_3, u_4), die also der Gleichung $\sum x_k u_k = 0$ genügen, geht nämlich wieder in die Gesamtheit der Punkte $\bar{\mathfrak{x}} = (\bar{x}_1, \bar{x}_2, \bar{x}_3, \bar{x}_4)$ einer Ebene $(\bar{u}_1, \bar{u}_2, \bar{u}_3, \bar{u}_4)$ über:

$$0 = \sum_k x_k u_k = \sum_k \left(\sum_i \bar{x}_i \hat{a}_{ik}\right) u_k = \sum_i \bar{x}_i \left(\sum_k \hat{a}_{ik} u_k\right) = \sum_i \bar{x}_i \bar{u}_i$$

mit

$$\bar{u}_i = \sum_k \hat{a}_{ik} u_k .$$

Umgekehrt hat der analytische Ausdruck jeder projektiven Transformation

$$x_i \to \bar{x}_i = f_i(x_1, x_2, x_3, x_4) \qquad (i = 1, \ldots, 4)$$

die obige Gestalt (*), wie man erkennt, wenn man Bildebenen $\bar{x}_i = \text{const.}$ betrachtet. Jede der zugehörigen vier Originalebenen wird dann nämlich durch die Gleichung

$$f_i(x_1, x_2, x_3, x_4) = \text{const.}$$

dargestellt, d. h., $f_i(x_1, x_2, x_3, x_4)$ muß ein linearer homogener Ausdruck in x_1, x_2, x_3, x_4 sein.

Die Gleichwertigkeit von (a_{ik}) und (λa_{ik}) in den Transformationsgleichungen (*) folgt daraus, daß ja sowohl die x_i als auch die $\bar{x}_k$ jeweils nur bis auf einen solchen konstanten Faktor bestimmt sind.

Für die Brauchbarkeit der damit nachgewiesenen analytischen Darstellung ist es wesentlich, daß der Nacheinanderausführung zweier projektiver Transformationen

$$\bar{x}_k = \sum_i x_i a_{ik} \qquad \text{bzw.} \quad \bar{\mathfrak{x}} = \mathfrak{x} A ,$$

$$\bar{\bar{x}}_l = \sum_k \bar{x}_k b_{kl} \qquad \text{bzw.} \quad \bar{\bar{\mathfrak{x}}} = \bar{\mathfrak{x}} B$$

das Produkt $C = (c_{il}) = AB$ der zugeordneten Matrizen entspricht:

$$\bar{\bar{x}}_l = \sum_k \left(\sum_i x_i a_{ik}\right) b_{kl} \qquad \text{bzw.} \quad \bar{\bar{\mathfrak{x}}} = (\mathfrak{x} A)\, B$$

$$= \sum_i x_i \left(\sum_k a_{ik} b_{kl}\right) \qquad = \mathfrak{x}(A\,B)$$

$$= \sum_i x_i c_{il} \qquad = \mathfrak{x} C .$$

Mit den erst im nächsten Kapitel zu behandelnden Begriffsbildungen läßt sich der gesamte Sachverhalt wie folgt zusammenfassen: Die projektive Gruppe ist vermöge (*) homomorphes Bild der vollen linearen Gruppe vom Grad 4, und zwar ist sie isomorph zur Faktorgruppe dieser Gruppe nach demjenigen Normalteiler, der aus allen Diagonalmatrizen $\lambda \cdot E = (\lambda \cdot \delta_{ik})$ besteht (vgl. Aufg. 1 von § 17 und S(18.11)).

b) Die *affinen Transformationen* sind unter den eben behandelten projektiven Transformationen durch die Erhaltung der Parallelität ausgezeichnet. Sie müssen also unendlich ferne Punkte wieder in unendlich ferne Punkte überführen, d. h., aus $x_4 = 0$ muß $\bar{x}_4 = 0$ folgen. In (*) hat daher die vierte Gleichung die Gestalt $\bar{x}_4 = a_{44} x_4$; also entsprechen den affinen Transformationen Matrizen der Form

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & 0 \\ a_{21} & a_{22} & a_{22} & 0 \\ a_{31} & a_{32} & a_{33} & 0 \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix}.$$

Um hiervon zu der für affine Transformationen üblichen inhomogenen Schreibweise zu gelangen, normiert man a_{44} auf 1 und ebenso die Quadrupel (x_1, x_2, x_3, x_4) und $(\bar{x}_1, \bar{x}_2, \bar{x}_3, \bar{x}_4)$, die nicht unendlich ferne Punkte darstellen, auf $(x_1, x_2, x_3, 1)$ bzw. $(\bar{x}_1, \bar{x}_2, \bar{x}_3, 1)$. Damit gehen die Gleichungen (*) über in

$$\bar{x}_1 = x_1 a_{11} + x_2 a_{21} + x_3 a_{31} + a_{41}$$

$$\bar{x}_2 = x_1 a_{12} + x_2 x_{22} + x_3 a_{32} + a_{42}$$

$$\bar{x}_3 = x_1 a_{13} + x_2 a_{23} + x_3 a_{33} + a_{43}$$

$$\bar{x}_4 = x_4 = 1,$$

wofür man unter Verwendung der Abkürzungen

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \qquad \begin{aligned} \mathfrak{x} &= (x_1, x_2, x_3), \\ \bar{\mathfrak{x}} &= (\bar{x}_1, \bar{x}_2, \bar{x}_3), \\ \mathfrak{a} &= (a_{41}, a_{42}, a_{43}) \end{aligned}$$

übersichtlich schreiben kann:

$$\bar{\mathfrak{x}} = \mathfrak{x}A + \mathfrak{a}.$$

Man erhält also alle affinen Transformationen, indem man in dieser Gleichung A alle Matrizen der vollen linearen Gruppe vom Grad 3 *und* $\mathfrak{a}$ *alle dreidimensionalen Vektoren durchlaufen läßt* (man beachte, daß über den willkürlichen Faktor $\lambda \neq 0$ in der homogenen Schreibweise beim Übergang zu inhomogenen Koordinaten durch die Setzung $a_{44} = 1$ verfügt wurde). Geometrisch bilden dabei die Transformationen $\bar{\mathfrak{x}} = \mathfrak{x}A$ die (zur multiplikativen vollen linearen Gruppe isomorphe) Untergruppe derjenigen affinen Transformationen, die den Ursprung in Ruhe lassen, während die Transformationen $\bar{\mathfrak{x}} = \mathfrak{x} + \mathfrak{a}$ die (zur additiven Gruppe aller Vektoren isomorphe) Untergruppe der Translationen liefern.

c) Die *Ähnlichkeitstransformationen* sind solche affinen Transformationen, die rechte Winkel invariant lassen. Da dies Translationen $\mathfrak{a}$ selbstverständlich erfüllen, können wir uns, wie auch im folgenden, auf die Diskussion der Transformationen von der Gestalt $\bar{\mathfrak{x}} = \mathfrak{x}A$ beschränken. Zur Charakterisierung der Orthogonalität verwenden wir dabei das Verschwinden des Skalarprodukts (unter Bezug auf ein orthonormiertes Koordinatensystem)

$$\mathfrak{x}\mathfrak{y}^{\mathrm{T}} = (x_1, x_2, x_3) \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = x_1 y_1 + x_2 y_2 + x_3 y_3$$

zweier Vektoren $\mathfrak{x}$ und $\mathfrak{y}$[1]). Es muß also aus $\mathfrak{x}\mathfrak{y}^{\mathrm{T}} = 0$ stets folgen

$$\bar{\mathfrak{x}}\bar{\mathfrak{y}}^{\mathrm{T}} = \mathfrak{x}AA^{\mathrm{T}}\mathfrak{y}^{\mathrm{T}} = 0.$$

1) Die Beschränkung der betrachteten affinen Transformationen auf solche, die den Ursprung in Ruhe lassen, gestattet es, jeden Punkt mit dem vom Ursprung zu ihm führenden Ortsvektor zu identifizieren. Dadurch betrachtet man natürlich nur Orthogonalitätsverhältnisse im Ursprung, was aber ausreicht. Es entspricht nämlich jedem rechten Winkel ein solcher mit parallelen Schenkeln durch den Ursprung, und wenn dieser bei der Transformation wieder in einen rechten Winkel übergeführt wird, so wegen der Erhaltung der Parallelität auch jener.

Dafür ist jedenfalls hinreichend, daß die Matrix AA^{T} die Gestalt λE hat. Diese Bedingung ist aber auch notwendig. Wäre nämlich $AA^{\mathrm{T}} = C \neq \lambda E$, so gibt es sicher einen Vektor $\mathfrak{x}$ derart, daß $\mathfrak{x}$ und $\mathfrak{x}C$ verschiedene Richtung haben. Mit einem zu $\mathfrak{x}$, aber nicht zu $\mathfrak{x}C$ orthogonalen Vektor $\mathfrak{y}$ erhalten wir $\mathfrak{x}\mathfrak{y}^{\mathrm{T}} = 0$, dagegen $\bar{\mathfrak{x}}\bar{\mathfrak{y}}^{\mathrm{T}} = \mathfrak{x}C\mathfrak{y}^{\mathrm{T}} \neq 0$.

Die Ähnlichkeitstransformationen, die den Ursprung in Ruhe lassen, entsprechen also genau den durch die Bedingung $AA^{\mathrm{T}} = \lambda E$ ausgewählten Matrizen. Sie unterscheiden sich von orthogonalen Matrizen, die sogar der Forderung $AA^{\mathrm{T}} = E$ genügen (vgl. den folgenden Abschnitt), nur um einen skalaren Faktor $\sqrt{\lambda}$.

d) Die für *kongruente Transformationen* hinzukommende Forderung der Längentreue läuft analog den eben durchgeführten Überlegungen auf die Invarianz des Skalarprodukts

$$\mathfrak{x}\mathfrak{x}^{\mathrm{T}} = \bar{\mathfrak{x}}\bar{\mathfrak{x}}^{\mathrm{T}} = \mathfrak{x}AA^{\mathrm{T}}\mathfrak{x}^{\mathrm{T}},$$

also auf $AA^{\mathrm{T}} = E$ hinaus.

Die kongruenten Transformationen, die den Ursprung in Ruhe lassen, sind also gerade durch die orthogonalen Matrizen gekennzeichnet; die von ihnen gebildete Gruppe ist daher isomorph zur orthogonalen Gruppe $\mathfrak{O}$.

Zur geometrischen Bedeutung dieser Transformationen sei bemerkt, daß (vgl. Aufg. 16 zu § 5) für die Determinante einer orthogonalen Matrix $|A| = +1$ oder $|A| = -1$ gilt. Im ersten Fall ist die entsprechende Transformation eine reine Drehung um den Ursprung, im zweiten Fall kommt noch eine Umlegung (Orientierungsänderung) hinzu. Das ergibt sich einfach daraus, daß sich der Inhalt eines Parallelepipeds mit der Determinante der Transformationsmatrix multipliziert (vgl. Aufg. 1). Insbesondere lehrt jetzt Aufgabe 5 von § 7, daß jede solche Umlegung durch Nacheinanderausführung einer festgewählten Umlegung und einer Drehung zu erhalten ist.

e) Aus dem zuletzt Gesagten ergibt sich: *Die Gruppe der orientierungstreuen kongruenten Transformationen (Bewegungen), die den Ursprung in Ruhe lassen, ist isomorph zur eigentlich orthogonalen Gruppe $\mathfrak{O}_+$.*

Es versteht sich, daß die in diesem Paragraphen durchgeführten Überlegungen mit entsprechenden Vereinfachungen im zwei- bzw. eindimensionalen Raum ebenso verlaufen; desgleichen kann man sie für n-dimensionale Räume verallgemeinern.

Aufgaben zu § 14

1. Man beweise, daß sich der Rauminhalt

$$I = \begin{vmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{vmatrix}$$

eines von drei Punkten $\mathfrak{x} = (x_1, x_2, x_3)$, $\mathfrak{y} = (y_1, y_2, y_3)$, $\mathfrak{z} = (z_1, z_2, z_3)$ und dem Ursprung aufgespannten Parallelepipeds bei einer affinen Transformation $\bar{\mathfrak{x}} = \mathfrak{x}A + \mathfrak{a}$ mit $|A|$ multipliziert.

2. Unter Verwendung von 1. kennzeichne man die geometrische Bedeutung der unimodularen bzw. eigentlich unimodularen Gruppe.

III. HOMOMORPHE ABBILDUNGEN

Wir wenden uns nunmehr wieder direkt der Theorie beliebiger Gruppen zu und setzen damit die Betrachtungen des ersten Kapitels fort. Leitgedanke der Untersuchungen wird der Abbildungsbegriff sein, der in der Gruppentheorie eine zentrale Rolle spielt. Dabei werden wir an die im § 4 behandelten isomorphen Abbildungen anknüpfen und empfehlen deshalb, sich den Inhalt dieses Paragraphen nochmals zu vergegenwärtigen. Allerdings gestattet die Isomorphie bloß, Gruppen gleicher Struktur zu vergleichen, und dient somit eigentlich nur zur näheren Festlegung des Untersuchungsobjektes der Gruppentheorie. Dagegen wird ein allgemeinerer Abbildungsbegriff (Homomorphie, § 18) ermöglichen, Gruppen verschiedener Struktur zueinander in Beziehung zu setzen und daraus Aussagen über die betrachteten Gruppen zu gewinnen.

§ 15. Automorphismen

Wir untersuchen solche Isomorphismen, bei denen Original und Bild die gleiche Gruppe sind.

Definition **D (15.1)**

Jeder Isomorphismus, der eine (eineindeutige, relationstreue) Abbildung einer Gruppe $\mathfrak{G}$ *auf sich selbst vermittelt, heißt ein Automorphismus von* $\mathfrak{G}$.

Offensichtlich ist die identische Abbildung jeder Gruppe auf sich selbst, bei der also Original und Bild elementweise übereinstimmen, stets ein Automorphismus. Für die meisten Gruppen gibt es aber neben diesem identischen Automorphismus noch andere Automorphismen, was wir hier jedoch nur für einige Beispiele nachweisen. Dazu ermitteln wir sämtliche Automorphismen der symmetrischen Gruppe $\mathfrak{S}_3$, der Kleinschen Vierergruppe $\mathfrak{V}_4$ und der zyklischen Gruppe $\mathfrak{Z}_n$. Unsere Überlegungen haben natürlich von

vornherein zu berücksichtigen, daß bei einem Isomorphismus und damit auch bei einem Automorphismus nur Elemente gleicher Ordnung aufeinander abgebildet werden können; insbesondere ist also stets das Einselement dem Einselement zuzuordnen (vgl. Aufgabe 6 von § 4 und Aufgabe 2 und 3 von § 6). Die Beachtung dieser notwendigen Bedingungen schaltet von vornherein eine Reihe vergeblicher Ansätze aus und systematisiert unsere Betrachtungen.

Symmetrische Gruppe $\mathfrak{S}_3$ **B (15.2)**

Ein nichtidentischer Automorphismus der Gruppe $\mathfrak{S}_3$ wird etwa gegeben durch die Zuordnung

$$\begin{aligned}
(1) &\to \overline{(1)} = (1)\\
(123) &\to \overline{(123)} = (132)\\
(132) &\to \overline{(132)} = (123)\\
(12) &\to \overline{(12)} = (12)\\
(13) &\to \overline{(13)} = (23)\\
(23) &\to \overline{(23)} = (13).
\end{aligned}$$

Sie vermittelt nämlich nach Konstruktion eine eineindeutige Abbildung der Gruppe $\mathfrak{S}_3$ auf sich selbst. Die Berücksichtigung der oben genannten notwendigen Bedingungen gewährleistet selbstverständlich noch nicht die Relationstreue

$$\overline{a \cdot b} = \bar{a} \cdot \bar{b}$$

für beliebige Elemente a und b aus $\mathfrak{S}_3$. Zu ihrem Beweis könnte man sich auf F (4.7) stützen und die Übereinstimmung der beiden Strukturtafeln

	(1)	(123)	(132)	(12)	(13)	(23)
(1)						
(123)						
(132)	. . . . .					(23)
(12)						
(13)						
(23)						

	$\overline{(1)}$	$\overline{(123)}$	$\overline{(132)}$	$\overline{(12)}$	$\overline{(13)}$	$\overline{(23)}$
$\overline{(1)}$						
$\overline{(123)}$						.
$\overline{(132)}$	. .					$\overline{(23)}$
$\overline{(12)}$						
$\overline{(13)}$						
$\overline{(23)}$						

zeigen. Das erforderte die Berechnung aller möglichen Produkte gemäß dem Beispiel

$$\overline{(132)} \cdot \overline{(13)} = (123) \cdot (23) = (13) = \overline{(23)}.$$

Diese Rechenarbeit ersparen wir uns aber durch folgende theoretische Überlegung: Die angegebene Abbildung kommt doch offensichtlich dadurch zustande, daß die permutierten Ziffern 1 und 2 miteinander vertauscht werden. Da es aber bei einer Permutation auf die Bezeichnung der permutierten Objekte nicht ankommt, unterscheidet sich die Gruppe

$$\{\overline{(1)}, \overline{(123)}, \ldots, \overline{(23)}\}$$

von der ursprünglichen nur durch die Schreibweise, nicht aber in ihrer Struktur.

Dieses Verfahren gestattet sofort, sechs verschiedene Automorphismen $\sigma_1, \ldots, \sigma_6$ (einschließlich des identischen) anzugeben, da es sechs Möglichkeiten gibt, die Ziffern 1, 2, 3 auf die drei permutierten Objekte zu verteilen. Die Bilder bei diesen Automorphismen sind:

	bei σ_1	bei σ_2	bei σ_3	bei σ_4	bei σ_5	bei σ_6
(1) →	(1)	(1)	(1)	(1)	(1)	(1)
(123) →	(123)	(123)	(123)	(132)	(132)	(132)
(132) →	(132)	(132)	(132)	(123)	(123)	(123)
(12) →	(12)	(23)	(13)	(12)	(23)	(13)
(13) →	(13)	(12)	(23)	(23)	(13)	(12)
(23) →	(23)	(13)	(12)	(13)	(12)	(23)

Die Permutationen von drei Elementen spielen bei diesen Betrachtungen eine mehrfache Rolle:

1. Einmal bilden sie die Gruppe $\mathfrak{S}_3$, deren Automorphismen wir aufstellen.

2. Durch Permutation der permutierten Objekte, d. h. durch Ziffernvertauschung innerhalb der unter 1. genannten Permutationen, erhalten wir die sechs Automorphismen unserer Tabelle.

3. Die drei Transpositionen der Gruppe $\mathfrak{S}_3$ werden bei diesen sechs Automorphismen auf alle sechs möglichen Arten permutiert.

Aus der letzten Feststellung folgt, daß mit den angegebenen sechs Automorphismen alle überhaupt möglichen Automorphismen der Gruppe $\mathfrak{S}_3$ erfaßt sind. Da sich nämlich jeder dreigliedrige Zyklus s als Produkt $s = t_1 \cdot t_2$ zweier Transpositionen t_1 und t_2 schreiben läßt, bestimmt die Zuordnung der Transpositionen gemäß

$$\bar{s} = \overline{t_1 \cdot t_2} = \bar{t}_1 \cdot \bar{t}_2$$

auch die Zuordnung der dreigliedrigen Zyklen. Nach unserer allgemeinen Vorbemerkung können nun bei einem Automorphismus die Transpositionen als Elemente der Ordnung 2 nur einander zugeordnet werden. Alle Möglichkeiten dieser Art sind aber in unserer Tabelle nach 3. erschöpft.

KLEINsche Vierergruppe $\mathfrak{V}_4$ **B (15.3)**

Bei allen Automorphismen der Gruppe $\mathfrak{V}_4$ muß das Einselement sich selbst zugeordnet werden. Die übrigen drei Gruppenelemente haben aber alle die gleiche Ordnung 2, können also auf insgesamt sechs verschiedene Weisen einander zugeordnet werden:

(1) →	(1)	(1)	(1)	(1)	(1)	(1)
(12)(34)→	(12)(34)	(14)(23)	(13)(24)	(12)(34)	(14)(23)	(13)(24)
(13)(24)→	(13)(24)	(12)(34)	(14)(23)	(14)(23)	(13)(24)	(12)(34)
(14)(23)→	(14)(23)	(13)(24)	(12)(34)	(13)(24)	(12)(34)	(14)(23)

Jede dieser sechs möglichen Zuordnungen vermittelt tatsächlich einen Automorphismus der Gruppe $\mathfrak{V}_4$. Auch hier läßt sich der rechnerische Nachweis der Relationstreue umgehen, indem man eine allgemeine Überlegung anstellt. Es lassen sich nämlich alle Produktbildungen zweier Faktoren durch die folgenden Feststellungen kennzeichnen, die von den in der Tabelle angegebenen Vertauschungen der Elemente der Ordnung 2 unabhängig sind:

1. Das Einselement als Faktor wirkt stets reproduzierend.

2. Ein Element der Ordnung 2 mit sich selbst multipliziert ergibt das Einselement.

3. Das Produkt zweier verschiedener Elemente der Ordnung 2 ist das dritte Element der Ordnung 2.

Zyklische Gruppe $\mathfrak{Z}_n$ **B (15.4)**

Es sei $\mathfrak{Z}_n = \langle a \rangle$ eine zyklische Gruppe der Ordnung n. Da bei einem Automorphismus stets Elemente gleicher Ordnung aufeinander abgebildet werden, ist dem primitiven Element a wieder ein primitives Element a^k mit $(k, n) = 1$ zuzuordnen (vgl. F (6.12 b)). Damit sind $\varphi(n)$ verschiedene Zuordnungen

$$a \to \overline{a} = a^k$$

für a mit zu n teilerfremden Exponenten k aus der Reihe $1, \ldots, n$ möglich. Jede von ihnen kennzeichnet einen durch

$$a^i \to \overline{a^i} = (a^i)^k = (a^k)^i \quad \text{für alle } i$$

beschriebenen Automorphismus. Wegen $\langle a \rangle = \langle a^k \rangle$ handelt es sich nämlich offensichtlich um eine eineindeutige Abbildung von $\mathfrak{Z}_n$ auf sich, die relationstreu ist wegen

$$\overline{a^i \cdot a^j} = \overline{a^{i+j}} = a^{(i+j)k} = a^{ik} \cdot a^{jk} = \overline{a^i} \cdot \overline{a^j}$$

In den vorangehenden Beispielen haben wir die Existenz nichtidentischer Automorphismen für eine Anzahl Gruppen nachgewiesen und darüber hinaus alle Automorphismen der betrachteten Gruppen aufgestellt. Wir beschäftigen uns nunmehr allgemein mit der Menge Φ aller Automorphismen einer Gruppe $\mathfrak{G}$. Diese Menge Φ ist ein Komplex der Gruppe $\mathfrak{T}$ aller eineindeutigen Abbildungen von $\mathfrak{G}$ auf sich selbst, der durch die Forderung der Relationstreue gekennzeichnet wird. Es ist von größter Wichtigkeit, daß die Menge Φ aller Automorphismen von $\mathfrak{G}$ mit der in $\mathfrak{T}$ erklärten Verknüpfung (Nacheinanderausführung) selbst eine Gruppe ist, die sogenannte *Automorphismengruppe* der Gruppe $\mathfrak{G}$. Wie wir schon hier bemerken wollen, bilden die (noch genauer festzulegenden) Automorphismen anderer algebraischer Strukturen ebenfalls Gruppen, die sogenannten Automorphismengruppen dieser Strukturen. Diese Feststellung charakterisiert sowohl den historischen Ursprung der Gruppentheorie als auch ihre entscheidende Bedeutung für die Algebra.

Satz **S (15.5)**

Die Menge Φ aller Automorphismen einer Gruppe $\mathfrak{G}$ ist selbst eine Gruppe. Als Verknüpfung dient die Nacheinanderausführung der durch die Automorphismen bewirkten Abbildungen.

Beweis

Fassen wir die Menge Φ als Komplex der Gruppe $\mathfrak{T}$ aller eineindeutigen Abbildungen von $\mathfrak{G}$ auf sich selbst auf, ist nach S(5.5) nur zu zeigen, daß das Produkt zweier Automorphismen und das Inverse jedes Automorphismus wieder Automorphismen sind. Unter Verwendung einer anderen Schreibweise als in B(2.6) führen wir jedoch den Beweis der Gruppeneigenschaft von Φ direkt, d. h. ohne Bezugnahme auf $\mathfrak{T}$.

Wir bezeichnen nämlich die Automorphismen mit griechischen Buchstaben $\sigma_1, \sigma_2, \sigma_3, \ldots$ und die Anwendung eines Automorphismus σ auf ein Element $a \in \mathfrak{G}$ durch

$$a \to \sigma(a) = a^{\sigma}.$$

Damit gehen wir also von der in B(2.6) eingeführten Funktionsschreibweise zu einer Exponentenschreibweise über[1]).

M I: Das Produkt $\sigma_1 \cdot \sigma_2$ zweier Automorphismen σ_1 und σ_2 ist wieder ein eindeutig bestimmter Automorphismus; denn führt man zwei eineindeutige Abbildungen von $\mathfrak{G}$ auf sich nacheinander aus, erhält man wieder eine solche Abbildung, und aus der Relationstreue von σ_1 und σ_2

$$(a\,b)^{\sigma_1} = a^{\sigma_1} b^{\sigma_1} \quad \text{und} \quad (a\,b)^{\sigma_2} = a^{\sigma_2} b^{\sigma_2}$$

für beliebige Elemente a und b aus $\mathfrak{G}$ folgt die Relationstreue von $\sigma_1 \cdot \sigma_2$:

$$(a\,b)^{[\sigma_1 \cdot \sigma_2]} = ((a\,b)^{\sigma_1})^{\sigma_2} = (a^{\sigma_1} b^{\sigma_1})^{\sigma_2} = (a^{\sigma_1})^{\sigma_2} (b^{\sigma_1})^{\sigma_2}$$
$$= a^{[\sigma_1 \cdot \sigma_2]}\, b^{[\sigma_1 \cdot \sigma_2]}.$$

M II: Der Beweis der Assoziativität in B(2.6b) überträgt sich in Exponentenschreibweise wie folgt:

$$a^{[\sigma_1 \cdot \sigma_2] \cdot \sigma_3} = (a^{\sigma_1 \cdot \sigma_2})^{\sigma_3} = ((a^{\sigma_1})^{\sigma_2})^{\sigma_3} = (a^{\sigma_1})^{\sigma_2 \cdot \sigma_3} = a^{\sigma_1 \cdot [\sigma_2 \cdot \sigma_3]}.$$

---

1) Die Exponentenschreibweise vermeidet die im Anhang IIb ausführlich auseinandergesetzte Vertauschung bei der Produktbildung:

Aus $[\sigma_1 \cdot \sigma_2](a) = \sigma_2(\sigma_1(a))$ wird $a^{[\sigma_1 \cdot \sigma_2]} = (a^{\sigma_1})^{\sigma_2}$

$M\,III_1$: Der identische Automorphismus ε ist gekennzeichnet durch

$$a^{\varepsilon} = a \quad \text{für alle } a \in \mathfrak{G}$$

und wirkt daher auf jeden Automorphismus reproduzierend:

$$a^{\sigma\cdot\varepsilon} = (a^{\sigma})^{\varepsilon} = a^{\sigma}$$

$M\,III_2$: Zu jedem Automorphismus σ wird durch die Vorschrift

$$(a^{\sigma})^{\sigma^{-1}} = a \quad \text{für alle } a \in \mathfrak{G}$$

ein zu σ inverser Automorphismus σ^{-1} erklärt; denn σ^{-1} macht offensichtlich die eineindeutige Abbildung σ rückgängig, und aus der Relationstreue von σ

$$(ab)^{\sigma} = a^{\sigma} b^{\sigma}$$

folgt die Relationstreue von σ^{-1}

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

qed.

Die Struktur der Automorphismengruppe jedes unserer Beispiele ergibt sich gemäß folgenden Überlegungen:

B (15.3)

Die Automorphismengruppe $\Phi_{\mathfrak{V}_4}$ der KLEINschen Vierergruppe $\mathfrak{V}_4$ ist isomorph zur symmetrischen Gruppe $\mathfrak{S}_3$. Von allen möglichen $4!$ eineindeutigen Abbildungen der vier Gruppenelemente der $\mathfrak{V}_4$ sind nämlich genau diejenigen Automorphismen, die das Einselement von $\mathfrak{V}_4$ fest lassen. Diese bilden aber nach S (11.1) eine zu $\mathfrak{S}_{4-1} = \mathfrak{S}_3$ isomorphe Untergruppe.

B (15.2)

Die Automorphismengruppe $\Phi_{\mathfrak{S}_3}$ der symmetrischen Gruppe $\mathfrak{S}_3$ ist isomorph zu eben dieser Gruppe $\mathfrak{S}_3$. Das ist in zweifacher Hinsicht bemerkenswert. Einmal nämlich wird damit gezeigt, daß eine Gruppe der Struktur nach Automorphismengruppe von sich selbst sein kann, zum anderen, daß zueinander nicht isomorphe Gruppen, etwa $\mathfrak{S}_3$ und $\mathfrak{V}_4$, isomorphe Automorphismengruppen besitzen können.

Den Beweis für $\Phi_{\mathfrak{S}_3} \xleftrightarrow{\sim} \mathfrak{S}_3$ kann man etwa über die Zuordnung der Automorphismen zu den ihnen entsprechenden Permutationen der drei Transpositionen von $\mathfrak{S}_3$ führen. Wir werden aber bald Hilfsmittel kennenlernen, die in diesem Falle einen einfacheren Beweis ermöglichen.

B (15.4)

Die Automorphismengruppe $\Phi_{\mathfrak{Z}_n}$ der zyklischen Gruppe $\mathfrak{Z}_n = \langle a \rangle$ ist isomorph zur primen Restklassengruppe mod n vermöge der Zuordnung

$$\sigma_k \to \overline{\sigma_k} = [k] \bmod n,$$

wobei wir unter σ_k den durch

$$a \to a^k = a^{\sigma_k} \text{ mit } (k, n) = 1$$

vermittelten Automorphismus von $\mathfrak{Z}_n$ verstehen. Die Zahlen k können etwa durch Vertreter aus dem kleinsten, nichtnegativen Repräsentantensystem mod n angegeben werden. Wegen $(k, n) = 1$ durchlaufen die Indizes k von σ_k nur die $\varphi(n)$ zu n teilerfremden Zahlen von 1 bis n. Damit ist die angegebene Zuordnung eineindeutig.

Zum Beweis der Relationstreue zeigen wir, daß dem Produkt zweier Automorphismen σ_k und σ_l das Produkt ihrer Indizes entspricht:

$$a^{\sigma_k \cdot \sigma_l} = \left(a^{\sigma_k}\right)^{\sigma_l} = \left(a^k\right)^l = a^{k \cdot l} = a^{\sigma_{k \cdot l}},$$

also ist

$$\overline{\sigma_k} \cdot \overline{\sigma_l} = [k] \cdot [l] = [k \cdot l] = \overline{\sigma_{k \cdot l}} = \overline{\sigma_k \cdot \sigma_l}.$$

Wir verallgemeinern noch den bei $\Phi_{\mathfrak{Z}_4}$ verwendeten Beweisgedanken (vgl. Aufg. 5):

Folgerung **F (15.6)**

Die Ordnung der Automorphismengruppe einer endlichen Gruppe der Ordnung n ist ein Teiler von $(n-1)!$

Zur weiteren Untersuchung von Automorphismengruppen benötigen wir eine Begriffsbildung, von der wir bereits einen Spezialfall in § 9 kennengelernt haben:

Definition **D (15.7)**

Sind x und a Elemente einer Gruppe $\mathfrak{G}$, so versteht man unter der Transformation von x mit a die Produktbildung

$$a^{-1}xa.$$

Satz **S (15.8)**

Durch Transformation aller Elemente $x \in \mathfrak{G}$ mit einem festen Element $a \in \mathfrak{G}$ entsteht vermöge der Zuordnung

$$x \to \bar{x} = a^{-1}xa$$

ein Automorphismus von $\mathfrak{G}$.

Beweis

Nach Definition wird jedem Element $x \in \mathfrak{G}$ eindeutig ein Bild $\bar{x} \in \mathfrak{G}$ zugeordnet. Die Zuordnung ist eineindeutig, da aus $a^{-1}xa = a^{-1}ya$ stets $x = y$ folgt. Sie vermittelt eine Abbildung von $\mathfrak{G}$ auf sich selbst, weil jedes beliebige Element $y \in \mathfrak{G}$ als Bild, nämlich von aya^{-1} auftritt. Schließlich besteht Relationstreue wegen

$$\bar{x} \cdot \bar{y} = a^{-1}xa \cdot a^{-1}ya = a^{-1}xya = \overline{x \cdot y}.$$

qed.

Dieser Satz gibt Anlaß zu einer Einteilung aller Automorphismen einer Gruppe in zwei Klassen:

Definition **D (15.9)**

Ein Automorphismus einer Gruppe $\mathfrak{G}$ heißt innerer Automorphismus von $\mathfrak{G}$, wenn es ein Element $a \in \mathfrak{G}$ gibt, so daß alle Bilder $\bar{x}$ durch Transformation der Originale x mit diesem Element a entstehen. Jeder andere Automorphismus heißt äußerer Automorphismus von $\mathfrak{G}$.

Der identische Automorphismus ist stets ein innerer Automorphismus, denn er kann durch die Zuordnung

$$x \to e^{-1}xe = x$$

gewonnen werden. Für abelsche Gruppen existiert nur dieser innere

Automorphismus (es ist dann ja $a^{-1}xa = a^{-1}ax = x$), so daß alle sonst noch vorhandenen Automorphismen einer abelschen Gruppe äußere Automorphismen sind (vgl. B(15.3) und B(15.4)). Andererseits können alle Automorphismen einer Gruppe innere Automorphismen sein. Das trifft z. B. für die in B(15.2) aufgestellten Automorphismen der symmetrischen Gruppe $\mathfrak{S}_3$ zu; denn man erhält $\sigma_1, \ldots, \sigma_6$, indem man der Reihe nach alle Elemente von $\mathfrak{S}_3$ mit $s_1 = (1)$, $s_2 = (123)$, $s_3 = (132)$, $s_4 = (12)$, $s_5 = (13)$, $s_6 = (23)$ transformiert. Nach S (9.6) kann man ja die Transformation einer Permutation s mit der Permutation s_0 einfach so durchführen, daß man in einer Zyklendarstellung von s die auftretenden Zahlen gemäß s_0 permutiert. Auf genau diese Weise haben wir aber der Reihe nach die sechs Automorphismen der Gruppe $\mathfrak{S}_3$ aufgestellt. Damit können wir den noch ausstehenden Beweis der Isomorphie $\Phi_{\mathfrak{S}_3} \overset{\sim}{\leftarrow} \mathfrak{S}_3$ vermöge der Zuordnung $\sigma_i \to s_i$ leicht erbringen. Es ist ja

$$x^{\sigma_i} = s_i^{-1} x s_i \qquad (i = 1, \ldots, 6),$$

und damit folgt aus $s_i s_j = s_k$ auch $\sigma_i \sigma_j = \sigma_k$ wegen

$$x^{\sigma_i \sigma_j} = (x^{\sigma_i})^{\sigma_j} = (s_i^{-1} x s_i)^{\sigma_j} = s_j^{-1}(s_i^{-1} x s_i)\, s_j = (s_i s_j)^{-1} x (s_i s_j)$$
$$= s_k^{-1} x s_k = x^{\sigma_k}.$$

Über diese beiden extremen Fälle hinaus, daß die Menge der inneren Automorphismen einer Gruppe die ganze Automorphismengruppe erschöpft oder sich auf deren Einheitsgruppe reduziert, gilt allgemein:

Satz **S (15.10)**

Die Menge Φ' der inneren Automorphismen einer Gruppe $\mathfrak{G}$ ist eine Untergruppe der Automorphismengruppe Φ von $\mathfrak{G}$.

Beweis

Das Produkt zweier innerer Automorphismen σ_a und σ_b ist wegen

$$x^{\sigma_a \sigma_b} = (x^{\sigma_a})^{\sigma_b} = (a^{-1} x a)^{\sigma_b} = b^{-1}(a^{-1} x a)\, b = (ab)^{-1} x (ab)$$

wieder ein innerer Automorphismus. Desgleichen ist zu σ_a der durch Transformation mit a^{-1} entstehende innere Automorphismus $\sigma_{a^{-1}}$ invers zu σ_a:

$$(x^{\sigma_a})^{\sigma_{a^{-1}}} = (a^{-1} x a)^{\sigma_{a^{-1}}} = (a^{-1})^{-1}(a^{-1} x a)\, a^{-1} = x.$$

Damit ist die Untergruppeneigenschaft von Φ' gezeigt. qed.

Aufgaben zu § 15

1. Man bestimme sämtliche Automorphismen der zyklischen Gruppen $\mathfrak{Z}_2$ und $\mathfrak{Z}_{12}$ sowie der unendlichen zyklischen Gruppe $\mathfrak{Z}_\infty$.
2. Der Übergang zum konjugiert-komplexen Wert bewirkt einen Automorphismus sowohl der additiven als auch der multiplikativen Gruppe der komplexen Zahlen.
3. Man kennzeichne die Automorphismen der additiven Gruppe der reellen Zahlen.
4. Die Automorphismengruppe Φ einer Gruppe $\mathfrak{G}$ ist eine *echte* Untergruppe der Gruppe $\mathfrak{T}$ aller eineindeutigen Abbildungen von $\mathfrak{G}$ auf sich.
5. Man beweise F(15.6).
6. Man stelle alle inneren Automorphismen der Gruppe $\langle(13), (14)(23)\rangle$ auf und ermittele die Struktur der Gruppe dieser Automorphismen.

§ 16. Konjugierte Elemente und Untergruppen[1])

Wir haben die in D(15.7) erklärte Transformation von x mit a bisher unter dem Gesichtspunkt betrachtet, daß in

$$a^{-1}xa$$

bei festem $a \in \mathfrak{G}$ das Element x die Gruppe $\mathfrak{G}$ durchläuft, und erhielten damit einen inneren Automorphismus von $\mathfrak{G}$. Es liegt nun die umgekehrte Betrachtungsweise nahe, bei festem $x \in \mathfrak{G}$ das Element a die Gruppe $\mathfrak{G}$ durchlaufen zu lassen, d. h. also, alle Bilder von x bei sämtlichen inneren Automorphismen zu untersuchen. Das wird uns weitere Einsichten in die Struktur der Gruppe $\mathfrak{G}$ liefern, die letzten Endes mit der Frage zusammenhängen, welche Elemente von $\mathfrak{G}$ untereinander kommutativ multiplizierbar sind. Für abelsche Gruppen werden daher die folgenden Überlegungen im allgemeinen trivial werden.

Definition **D (16.1)**

Zwei Elemente x und y der Gruppe $\mathfrak{G}$ heißen konjugiert in $\mathfrak{G}$, wenn sie durch wenigstens einen inneren Automorphismus von $\mathfrak{G}$ ineinander übergeführt werden:

$$y = a^{-1}xa \quad \textit{und damit} \quad x = (a^{-1})^{-1}ya^{-1}.$$

Es ist meist üblich, den genauer kennzeichnenden Zusatz „in $\mathfrak{G}$" wegzulassen, da es sich im allgemeinen von selbst versteht, auf welche Gruppe Bezug genommen wird.

1) Beim ersten Studium dieses Kapitels genügt eine Kenntnisnahme von D(16.1), S(16.2), D(16.10), S(16.11).

Satz **S (16.2)**

Die Untermengen zueinander konjugierter Elemente bilden eine Klasseneinteilung von $\mathfrak{G}$. *Sie besteht für* $\mathfrak{G} \neq \mathfrak{E}$ *aus mindestens zwei Klassen.*

Beweis

Wir zeigen, daß die in D(16.1) zwischen den Elementen von $\mathfrak{G}$ erklärte Beziehung eine Äquivalenzrelation ist. Sie ist nämlich reflexiv, weil der identische Automorphismus ein innerer Automorphismus ist. Die Symmetrie der Beziehung, die auf der Existenz des inversen inneren Automorphismus beruht, wurde bereits in der Definition ausgesprochen. Die Beziehung ist schließlich transitiv, denn aus

$$y = a^{-1} x a \quad \text{und} \quad z = b^{-1} y b$$

folgt

$$z = b^{-1} (a^{-1} x a)\, b = (a b)^{-1} x (a b).$$

Die Aussage über die Anzahl der Klassen folgt daraus, daß das Einselement $e \in \mathfrak{G}$ bei allen Automorphismen auf sich selbst abgebildet wird und daher eine Klasse für sich bildet. Wenn $\mathfrak{G}$ nicht nur aus dem Einselement besteht, muß also mindestens noch eine weitere Klasse vorhanden sein.

qed.

Wie man sich sofort überzeugt, zerfällt z. B. die symmetrische Gruppe $\mathfrak{S}_3$ in drei Klassen zueinander konjugierter Elemente:

$$\mathfrak{S}_3 = \{(1)\} \cup \{(123), (132)\} \cup \{(12), (13), (23)\}.$$

Dagegen ist für jede abelsche Gruppe eine solche Klasseneinteilung insofern trivial, als jedes Gruppenelement bei inneren Automorphismen nur auf sich selbst abgebildet wird, also jede Klasse nur aus einem Element besteht.

Aus D(16.1) erhält man unmittelbar (vgl. Aufg. 3 von § 6):

Folgerung **F (16.3)**

Zueinander konjugierte Gruppenelemente haben die gleiche Ordnung.

Jedoch folgt aus der Übereinstimmung der Ordnung von Gruppenelementen im allgemeinen nicht, daß diese Elemente zuein-

ander konjugiert sind (vgl. etwa Aufg. 1). Weiterhin ergibt sich aus S (9.6) für jede Permutationsgruppe $\mathfrak{P}$:

Folgerung **F (16.4)**

Zueinander in $\mathfrak{P}$ konjugierte Permutationen haben gleichartige Zyklendarstellungen.

Auch diese Aussage ist im allgemeinen nicht umkehrbar (vgl. ebenfalls Aufg. 1), wohl aber für die symmetrische Gruppe $\mathfrak{S}_n$ (vgl. Aufg. 2).

Um uns einen Überblick über die in einer Gruppe $\mathfrak{G}$ zu einem festen Element $x \in \mathfrak{G}$ konjugierten Elemente zu verschaffen und insbesondere ihre Anzahl zu bestimmen, untersuchen wir, welche $a \in \mathfrak{G}$ durch Transformation von x jeweils dasselbe $y \in \mathfrak{G}$ liefern:

$$y = a^{-1} x a.$$

Dafür betrachten wir zunächst den Spezialfall $y = x$, d. h., wir fragen nach allen $a \in \mathfrak{G}$, die mit x vertauschbar sind:

$$x = a^{-1} x a, \quad \text{also } ax = xa \text{ für festes } x \in \mathfrak{G}.$$

Definition **D (16.5)**

Die Menge aller mit einem festen Element $x \in \mathfrak{G}$ vertauschbaren Elemente $a \in \mathfrak{G}$ heißt der Normalisator $\mathfrak{V}_x$ von x in $\mathfrak{G}$.

Folgerung **F (16.6)**

Der Normalisator $\mathfrak{V}_x$ von $x \in \mathfrak{G}$ ist eine Untergruppe von $\mathfrak{G}$. Er enthält mindestens die von x erzeugte zyklische Gruppe $\langle x \rangle$.

Beweis

Es seien a_1 und a_2 zwei beliebige Elemente aus $\mathfrak{V}_x$. Mit

$$a_1 x = x a_1 \quad \text{und} \quad a_2 x = x a_2$$

gilt dann auch

$$a_1 a_2 x = x a_1 a_2 \text{ sowie } x a_1^{-1} = a_1^{-1} x.$$

Dies zeigt die Untergruppeneigenschaft von $\mathfrak{V}_x$. Da jede zyklische Gruppe abelsch ist, folgt $\langle x \rangle \leqq \mathfrak{V}_x$.

qed.

Damit erhalten wir als Ergebnis für den allgemeinen Fall:

Satz **S (16.7)**

Alle und nur die Elemente einer Rechtsnebenklasse $\mathfrak{B}_x \cdot b$ *von* $\mathfrak{B}_x$ *in* $\mathfrak{G}$ *liefern durch Transformation von* x *das gleiche (zu* x *konjugierte) Element, d. h., es gilt*

$$a^{-1}xa = b^{-1}xb \quad \textit{genau dann, wenn} \quad a \in \mathfrak{B}_x \cdot b.$$

Insbesondere ist daher die Anzahl[1]) *der verschiedenen zu* x *konjugierten Elemente gleich der Anzahl der verschiedenen Rechtsnebenklassen von* $\mathfrak{B}_x$ *in* $\mathfrak{G}$, *also gleich dem Index* $(\mathfrak{G} : \mathfrak{B}_x)$.

Beweis

Die Gleichung $a^{-1}xa = b^{-1}xb$ ist offensichtlich gleichwertig mit der Gleichung $xab^{-1} = ab^{-1}x$ und diese wiederum nach D (16.5) mit $ab^{-1} \in \mathfrak{B}_x$, also mit $a \in \mathfrak{B}_x \cdot b$.

qed.

So sind z. B. die Indizes der Normalisatoren der Elemente aus der Gruppe $\mathfrak{S}_3$

$$\begin{aligned}
\mathfrak{B}_{(1)} &= \mathfrak{S}_3 && (\mathfrak{S}_3 : \mathfrak{B}_{(1)}) = 1\\
\mathfrak{B}_{(123)} &= \mathfrak{B}_{(132)} = \mathfrak{A}_3, && (\mathfrak{S}_3 : \mathfrak{B}_{(123)}) = 2\\
\mathfrak{B}_{(12)} &= \{(1), (12)\} && (\mathfrak{S}_3 : \mathfrak{B}_{(12)}) = 3\\
\mathfrak{B}_{(13)} &= \{(1), (13)\} && (\mathfrak{S}_3 : \mathfrak{B}_{(13)}) = 3\\
\mathfrak{B}_{(23)} &= \{(1), (23)\} && (\mathfrak{S}_3 : \mathfrak{B}_{(23)}) = 3
\end{aligned}$$

in Übereinstimmung mit der Anzahl der Elemente der einzelnen Klassen.

Im Zusammenhang mit D(16.5) gelangt man noch zu einer weiteren Begriffsbildung, wenn man an Stelle der Vertauschbarkeit mit einem Element die mit allen Gruppenelementen fordert:

Definition **D (16.8)**

Die Menge aller mit allen Elementen $x \in \mathfrak{G}$ *vertauschbaren Elemente* $a \in \mathfrak{G}$ *heißt das Zentrum* $\mathfrak{Z}$ *von* $\mathfrak{G}$.

---

1) Im unendlichen Falle ist unter gleicher Anzahl natürlich die Gleichmächtigkeit der betrachteten Mengen zu verstehen.

Ein Element $a \in \mathfrak{G}$ liegt also genau dann im Zentrum, wenn sein Normalisator $\mathfrak{N}_a$ gleich der gesamten Gruppe $\mathfrak{G}$ ist. Weiterhin gilt:

Folgerung **F (16.9)**

Das Zentrum $\mathfrak{Z}$ einer Gruppe $\mathfrak{G}$ ist der Durchschnitt $\mathfrak{D}$ der Normalisatoren aller Elemente aus $\mathfrak{G}$ und damit Untergruppe von $\mathfrak{G}$.

Beweis

Die Elemente des Durchschnittes $\mathfrak{D}$ sind enthalten in allen Normalisatoren und damit vertauschbar mit allen Gruppenelementen; daher ist $\mathfrak{D} \leqq \mathfrak{Z}$. Umgekehrt ist jedes Element des Zentrums mit jedem Gruppenelement vertauschbar, liegt also in allen Normalisatoren und damit in deren Durchschnitt; das zeigt $\mathfrak{Z} \leqq \mathfrak{D}$.

qed.

So ist z. B. das Zentrum von $\mathfrak{S}_3$ gleich der Einheitsgruppe, das Zentrum jeder abelschen Gruppe gleich der ganzen Gruppe (und umgekehrt), schließlich das Zentrum der Gruppe $\langle (13), (14)(23) \rangle$ gleich der nichttrivialen Untergruppe $\{(1), (13)(24)\}$.

Im folgenden erweitern wir unsere Betrachtungen auf Untergruppen, d. h., wir untersuchen nicht nur die Bilder einzelner Elemente, sondern die Bilder von Untergruppen $\mathfrak{H} \leqq \mathfrak{G}$ bei inneren Automorphismen von $\mathfrak{G}$.

Als eine eineindeutige relationstreue Abbildung bewirkt jeder Isomorphismus einer Gruppe $\mathfrak{G}$ auf eine Gruppe $\overline{\mathfrak{G}}$ erst recht eine eineindeutige relationstreue Abbildung, also einen Isomorphismus jeder Untergruppe $\mathfrak{H} \leqq \mathfrak{G}$ auf eine Bildmenge $\overline{\mathfrak{H}} \leqq \overline{\mathfrak{G}}$, die nach F (4.4) eine Untergruppe von $\overline{\mathfrak{G}}$ ist. So wird insbesondere bei jedem Automorphismus von $\mathfrak{G}$ eine Untergruppe $\mathfrak{H} \leqq \mathfrak{G}$ wieder auf eine Untergruppe von $\mathfrak{G}$ isomorph abgebildet, die natürlich nicht mit $\mathfrak{H}$ übereinzustimmen braucht. Diese Überlegungen sind besonders wichtig für innere Automorphismen:

Definition **D (16.10)**

Zwei Untergruppen $\mathfrak{H}$ und $\mathfrak{H}^*$ der Gruppe $\mathfrak{G}$ heißen konjugiert (in $\mathfrak{G}$), wenn sie durch wenigstens einen inneren Automorphismus von $\mathfrak{G}$ ineinander übergeführt werden:

$$\mathfrak{H}^* = a^{-1}\,\mathfrak{H}\,a \quad \textit{und damit} \quad \mathfrak{H} = (a^{-1})^{-1}\,\mathfrak{H}^*\,a^{-1}.$$

Satz **S (16.11)**

Die Einteilung aller Untergruppen von $\mathfrak{G}$ in Klassen zueinander konjugierter Untergruppen ist eine Klasseneinteilung der Menge aller Untergruppen, die für $\mathfrak{G} \neq \mathfrak{E}$ wenigstens aus zwei Klassen besteht.

Der Beweis, daß die in D (16.10) zwischen den Untergruppen von $\mathfrak{G}$ erklärte Beziehung eine Äquivalenzrelation ist, verläuft völlig analog dem Beweis von S (16.2). Entsprechendes gilt für die Behauptung über die Anzahl der Klassen.

So liegen die sechs Untergruppen der Gruppe $\mathfrak{S}_3$ in vier Klassen konjugierter Untergruppen:

$$\{(1)\} = \mathfrak{E}$$
$$\{(1), (12)\} = \mathfrak{H}_1,\ \{(1), (13)\} = \mathfrak{H}_2,\ \{(1), (23)\} = \mathfrak{H}_3$$
$$\{(1), (123), (132)\} = \mathfrak{A}_3$$
$$\{(1), (123), (132), (12), (13), (23)\} = \mathfrak{S}_3.$$

Die F (16.3) entsprechende Aussage, daß konjugierte Untergruppen gleiche Ordnung haben, versteht sich bei ihrer Isomorphie von selbst. Ferner erhalten wir in Analogie zu D (16.5), F (16.6), S (16.7) unter Verwendung des Komplexproduktes:

Definition **D (16.12)**

Die Menge aller mit einer Untergruppe $\mathfrak{H} \leqq \mathfrak{G}$ vertauschbaren Elemente $a \in \mathfrak{G}$ heißt der Normalisator $\mathfrak{N}_{\mathfrak{H}}$ von $\mathfrak{H}$ in $\mathfrak{G}$:

$$a\mathfrak{H} = \mathfrak{H}a\ ^{1}).$$

Folgerung **F (16.13)**

Der Normalisator $\mathfrak{N}_{\mathfrak{H}}$ von $\mathfrak{H} \leqq \mathfrak{G}$ ist eine Untergruppe von $\mathfrak{G}$. Er enthält mindestens die Gruppe $\mathfrak{H}$ selbst.

Beweis

Es seien a_1 und a_2 bzw. a beliebige Elemente aus $\mathfrak{N}_{\mathfrak{H}}$. Mit

$$a_1\mathfrak{H} = \mathfrak{H}a_1 \quad \text{und} \quad a_2\mathfrak{H} = \mathfrak{H}a_2 \quad \text{bzw.} \quad a\mathfrak{H} = \mathfrak{H}a$$

gilt dann auch

$$a_1a_2\mathfrak{H} = \mathfrak{H}a_1a_2 \quad \text{bzw.} \quad \mathfrak{H}a^{-1} = a^{-1}\mathfrak{H}.$$

1) Genau die Elemente $a \in \mathfrak{N}_{\mathfrak{H}}$ vermitteln also durch Transformation eine Abbildung von $\mathfrak{H}$ auf sich selbst. Jede solche Transformation bewirkt damit einen Automorphismus von $\mathfrak{H}$, der also durch einen inneren Automorphismus von $\mathfrak{G}$ induziert wird, aber selbst kein innerer Automorphismus von $\mathfrak{H}$ zu sein braucht.

Also ist $\mathfrak{V}_{\mathfrak{H}}$ Untergruppe von $\mathfrak{G}$. Für $h \in \mathfrak{H}$ gilt aber stets $h\mathfrak{H} = \mathfrak{H}h$, also ist jedes h aus $\mathfrak{H}$ enthalten in $\mathfrak{V}_{\mathfrak{H}}$. qed.

Satz **S (16.14)**

Alle und nur die Elemente einer Rechtsnebenklasse $\mathfrak{V}_{\mathfrak{H}} \cdot b$ von $\mathfrak{V}_{\mathfrak{H}}$ in $\mathfrak{G}$ liefern durch Transformation von $\mathfrak{H}$ die gleiche (zu $\mathfrak{H}$ konjugierte) Untergruppe, d. h., es gilt

$$a^{-1}\mathfrak{H}a = b^{-1}\mathfrak{H}b \quad \text{genau dann, wenn} \quad a \in \mathfrak{V}_{\mathfrak{H}} \cdot b.$$

Insbesondere ist daher die Anzahl der verschiedenen zu $\mathfrak{H}$ konjugierten Untergruppen gleich der Anzahl der verschiedenen Rechtsnebenklassen von $\mathfrak{V}_{\mathfrak{H}}$ in $\mathfrak{G}$, also gleich dem Index $(\mathfrak{G} : \mathfrak{V}_{\mathfrak{H}})$.

Der Beweis von S (16.7) läßt sich mit Ersetzung von $x \in \mathfrak{G}$ durch $\mathfrak{H} \leqq \mathfrak{G}$ auf Grund der für die Komplexmultiplikation gültigen Rechenregeln wörtlich übertragen.

So gilt z. B. für die Normalisatoren der Untergruppen von $\mathfrak{S}_3$

$$\begin{aligned}
\mathfrak{V}_{\mathfrak{E}} &= \mathfrak{S}_3, & (\mathfrak{S}_3 : \mathfrak{V}_{\mathfrak{E}}) &= 1 \\
\mathfrak{V}_{\mathfrak{H}_1} &= \mathfrak{H}_1, & (\mathfrak{S}_3 : \mathfrak{V}_{\mathfrak{H}_1}) &= 3 \\
\mathfrak{V}_{\mathfrak{H}_2} &= \mathfrak{H}_2, & (\mathfrak{S}_3 : \mathfrak{V}_{\mathfrak{H}_2}) &= 3 \\
\mathfrak{V}_{\mathfrak{H}_3} &= \mathfrak{H}_3, & (\mathfrak{V}_3 : \mathfrak{V}_{\mathfrak{H}_3}) &= 3 \\
\mathfrak{V}_{\mathfrak{A}_3} &= \mathfrak{S}_3, & (\mathfrak{S}_3 : \mathfrak{V}_{\mathfrak{A}_3}) &= 1 \\
\mathfrak{V}_{\mathfrak{S}_3} &= \mathfrak{S}_3, & (\mathfrak{S}_3 : \mathfrak{V}_{\mathfrak{S}_3}) &= 1,
\end{aligned}$$

was wieder mit der Anzahl der konjugierten Untergruppen jeder Klasse übereinstimmt.

Aus S (16.14) ergibt sich noch eine für sich interessante Feststellung:

Folgerung **F (16.15)**

Eine Klasse konjugierter echter Untergruppen einer endlichen Gruppe $\mathfrak{G}$ erschöpft mit ihren Elementen niemals ganz $\mathfrak{G}$.

Beweis

Es sei $\mathfrak{H}$ eine echte Untergruppe von $\mathfrak{G}$. Dann gilt wegen $\mathfrak{H} \leqq \mathfrak{V}$

$$(\mathfrak{G} : \mathfrak{V}_{\mathfrak{H}})\,(\mathfrak{V}_{\mathfrak{H}} : \mathfrak{H})\,(\mathfrak{H} : \mathfrak{E}) = (\mathfrak{G} : \mathfrak{E}),$$

also ist erst recht

$$(\mathfrak{G} : \mathfrak{V}_{\mathfrak{H}})\,(\mathfrak{H} : \mathfrak{E}) \leq (\mathfrak{G} : \mathfrak{E}).$$

Da die zu $\mathfrak{H}$ konjugierten Untergruppen die gleiche Ordnung wie $\mathfrak{H}$ haben, gibt die linke Seite der letzten Relation nach S(16.14) an, wieviel Gruppenelemente die Menge der zu $\mathfrak{H}$ konjugierten Untergruppen enthielte, wenn dabei kein Gruppenelement in mehr als einer konjugierten Untergruppe auftreten würde. Selbst dann wäre die Anzahl der in dieser Menge überhaupt enthaltenen Gruppenelemente höchstens gleich der Anzahl aller Gruppenelemente. Für $(\mathfrak{G}:\mathfrak{N}_{\mathfrak{H}}) > 1$ wird aber das Einselement mindestens zweimal gezählt, womit für diesen Fall die Behauptung bewiesen ist. Für $(\mathfrak{G}:\mathfrak{N}_{\mathfrak{H}}) = 1$ tritt aber nur eine zu sich selbst konjugierte Untergruppe auf, die wegen der Voraussetzung $\mathfrak{H} < \mathfrak{G}$ nicht alle Elemente von $\mathfrak{G}$ enthält.

qed.

Abschließend bemerken wir, daß man unsere Betrachtungen über konjugierte Gruppenelemente und konjugierte Untergruppen zusammenfassen und verallgemeinern kann, indem man konjugierte Komplexe behandelt. Man untersucht dann also beliebige Untermengen und ihre Bilder bei inneren Automorphismen und erfaßt damit erst recht konjugierte Elemente und konjugierte Untergruppen. D(16.1) und D(16.10), S(16.2) und S(16.11), D(16.5) und D(16.12), die in F(16.6) und F(16.13) genannte Gruppeneigenschaft sowie S(16.7) und S(16.14) werden dann zu Spezialfällen der entsprechenden Aussagen über konjugierte Komplexe.

Aufgaben zu § 16

1. Man zerlege die Gruppe $\langle (13), (14)(23)\rangle$ in Klassen konjugierter Elemente.
2. Jede Klasse konjugierter Elemente der symmetrischen Gruppe $\mathfrak{S}_n$ besteht aus genau den Elementen, die in der Hauptproduktdarstellung eine gleichartige Zyklenzerlegung haben. Dieser Satz gilt nicht mehr für echte Untergruppen von $\mathfrak{S}_n$.
3. Das Komplexprodukt zweier Klassen konjugierter Elemente besteht stets aus der Vereinigung von Klassen konjugierter Elemente.
4. Bilden wir zu einer Klasse konjugierter Elemente den inversen Komplex, so ist dieser wieder eine Klasse konjugierter Elemente.
5. Man bestimme die Normalisatoren aller Elemente der Gruppe $\langle (13), (14)(23)\rangle$.
6. Man zeige für eine endliche Gruppe $\mathfrak{G}$: Die Anzahl der Elemente einer beliebigen Klasse konjugierter Elemente ist ein Teiler des Index $(\mathfrak{G}:\mathfrak{Z})$ des Zentrums $\mathfrak{Z}$ von $\mathfrak{G}$.

7. Für die Elemente a des Zentrums $\mathfrak{Z}$ einer Gruppe $\mathfrak{G}$ gilt sowohl, daß sie durch Transformation identische Automorphismen bewirken, als auch, daß sie bei allen inneren Automorphismen auf sich selbst abgebildet werden. Jedes Zentrumselement bildet also für sich eine Klasse konjugierter Elemente. Man nennt sie deshalb auch *invariante Elemente.*

8. Das Zentrum der symmetrischen Gruppe $\mathfrak{S}_n$ $(n \geq 3)$ ist gleich der Einheitsgruppe.

9. Das Zentrum der vollen linearen Gruppe $\mathfrak{G}$ besteht aus allen skalaren Vielfachen $\lambda E = \lambda(\delta_{ik})$ der Einheitsmatrix $(\lambda \neq 0)$.

10. Man teile die 30 Untergruppen der symmetrischen Gruppe $\mathfrak{S}_4$ in Klassen konjugierter Untergruppen ein und veranschauliche sich F(16.15).

11. Alle Stabilitätsuntergruppen einer transitiven Permutationsgruppe sind zueinander konjugiert.

§ 17. Normalteiler

Für die von uns angestrebte Verallgemeinerung des Isomorphiebegriffes spielen diejenigen Untergruppen eine ausschlaggebende Rolle, die für sich selbst schon eine Klasse konjugierter Untergruppen bilden.

Definition **D (17.1)**

Eine Untergruppe $\mathfrak{N}$ einer Gruppe $\mathfrak{G}$ heißt Normalteiler von $\mathfrak{G}$, wenn sie bei allen inneren Automorphismen von $\mathfrak{G}$ auf sich selbst abgebildet wird:

$$\mathfrak{N} = a^{-1}\mathfrak{N}a \quad \textit{für alle } a \in \mathfrak{G}.$$

Die Invarianz eines Normalteilers von $\mathfrak{G}$ gegenüber allen inneren Automorphismen von $\mathfrak{G}$ erklärt die für ihn auch gebräuchliche Bezeichnung *invariante Untergruppe.* Die Einheitsgruppe $\mathfrak{E}$ und die gesamte Gruppe $\mathfrak{G}$ sind selbstverständlich stets Normalteiler von $\mathfrak{G}$. Weiterhin ist in einer abelschen Gruppe jede Untergruppe Normalteiler. Wegen der großen Wichtigkeit von Normalteilern stellen wir zunächst einige charakterisierende Eigenschaften zusammen, die ebenso zur Definition des Normalteilers dienen können.

Satz **S (17.2)**

Für die Normalteilereigenschaft einer Untergruppe $\mathfrak{N}$ von $\mathfrak{G}$ ist jede der folgenden Aussagen notwendig und hinreichend:

a) *Jede Linksnebenklasse $a\mathfrak{N}$ stimmt mit der entsprechenden Rechtsnebenklasse $\mathfrak{N}a$ von $\mathfrak{N}$ in $\mathfrak{G}$ überein:*

$$a\mathfrak{N} = \mathfrak{N}a \quad \text{für alle } a \in \mathfrak{G}.$$

b) *$\mathfrak{N}$ enthält alle zu ihr konjugierten Untergruppen*[1]*:*

$$\mathfrak{N} \supseteq a^{-1}\mathfrak{N}a \quad \text{für alle } a \in \mathfrak{G}.$$

c) *$\mathfrak{N}$ besteht aus vollständigen Klassen zueinander konjugierter Elemente aus $\mathfrak{G}$, d.h., mit jedem Element aus $\mathfrak{N}$ sind auch alle zu ihm konjugierten Elemente in $\mathfrak{N}$ enthalten:*

$$\text{Aus } n \in \mathfrak{N} \text{ folgt } a^{-1}na \in \mathfrak{N} \text{ für alle } a \in \mathfrak{G}.$$

d) *$\mathfrak{N}$ besitzt ein Erzeugendensystem, das aus vollständigen Klassen $\mathfrak{K}_1, \mathfrak{K}_2, \ldots$ zueinander konjugierter Elemente besteht:*

$$\mathfrak{N} = \langle \mathfrak{K}_1, \mathfrak{K}_2, \ldots \rangle.$$

e) *Der Normalisator $\mathfrak{B}_{\mathfrak{N}}$ von $\mathfrak{N}$ in $\mathfrak{G}$ ist die gesamte Gruppe $\mathfrak{G}$:*

$$\mathfrak{B}_{\mathfrak{N}} = \mathfrak{G}.$$

Beweis

a) Die Gleichwertigkeit von $\mathfrak{N} = a^{-1}\mathfrak{N}a$ und $a\mathfrak{N} = \mathfrak{N}a$ folgt unmittelbar durch Multiplikation mit a bzw. a^{-1}.

b) Die Notwendigkeit der unter b) genannten Bedingung ist klar. Wir zeigen, daß sie auch hinreichend ist, also aus $\mathfrak{N} \supseteq a^{-1}\mathfrak{N}a$ für alle $a \in \mathfrak{G}$ stets $\mathfrak{N} = a^{-1}\mathfrak{N}a$ für alle $a \in \mathfrak{G}$ folgt. Multipliziert man nämlich die erste Relation von links mit a und von rechts mit a^{-1}, so erhält man

$$a\mathfrak{N}a^{-1} \supseteq \mathfrak{N} \quad \text{für alle } a \in \mathfrak{G}.$$

Ersetzt man a durch a^{-1}, das ja mit a ebenso alle Gruppenelemente durchläuft, so ergibt sich

$$a^{-1}\mathfrak{N}a \supseteq \mathfrak{N} \quad \text{für alle } a \in \mathfrak{G},$$

woraus zusammen mit der ursprünglichen Relation die Behauptung folgt.

---

1) Das ist eine für die praktische Nachprüfung vorteilhafte Abschwächung der Bedingung aus D(17.1). Desgleichen wird das Kriterium c) oft verwendet, während d) und e) von untergeordneter Bedeutung sind.

c) Diese Aussage ergibt sich unmittelbar durch Übertragung der Komplexaussage in b) auf die einzelnen Gruppenelemente.

d) Jeder Normalteiler besitzt mindestens ein solches Erzeugendensystem, da er nach c) aus vollständigen Klassen konjugierter Elemente besteht und diese trivialerweise ein Erzeugendensystem bilden. Gilt umgekehrt $\mathfrak{N} = \langle \mathfrak{K}_1, \mathfrak{K}_2, \ldots \rangle$, so besteht $\mathfrak{N}$ wegen der in den Aufgaben 3 und 4 von § 16 genannten Aussagen aus vollständigen Klassen konjugierter Elemente, was nach c) die Normalteilereigenschaft von $\mathfrak{N}$ zeigt.

e) Die Gleichung $\mathfrak{V}_{\mathfrak{N}} = \mathfrak{G}$ ist nur eine andere Formulierung von a) mit Hilfe des in D (16.12) erklärten Begriffes des Normalisators einer Untergruppe.

qed.

Beispiele:

Die drei Normalteiler der symmetrischen Gruppe $\mathfrak{S}_3$, nämlich $\mathfrak{E}$, $\mathfrak{A}_3$ und $\mathfrak{S}_3$, haben wir bereits als die nur zu sich selbst konjugierten Untergruppen im Anschluß an S (16.11) kennengelernt.

Die symmetrische Gruppe $\mathfrak{S}_4$ besitzt vier Normalteiler: $\mathfrak{E}$, $\mathfrak{V}_4$, $\mathfrak{A}_4$, $\mathfrak{S}_4$. Für $\mathfrak{A}_4$ folgt das schon daraus, daß sie die einzige Untergruppe der Ordnung 12 ist, also nur zu sich selbst konjugiert sein kann. $\mathfrak{V}_4$ besteht außer dem Einselement gerade aus den Permutationen, deren Hauptproduktdarstellungen die Gestalt $(i_1 i_2)(j_1 j_2)$ haben. Sie enthält damit nach S (9.6) zu jedem Element alle konjugierten Elemente, ist also nach S (17.2 c) Normalteiler. Jede andere Untergruppe der $\mathfrak{S}_4$ verstößt gegen die Bedingung in S (17.2 c). Man prüft das am zweckmäßigsten unter Verwendung von Aufg. 2 in § 16 nach oder benutzt Aufg. 10 in § 16.

Für die Feststellung der Normalteilereigenschaft einer Untergruppe ist folgende hinreichende Bedingung oft nützlich:

Folgerung **F (17.3)**

Eine Untergruppe $\mathfrak{N} \leqq \mathfrak{G}$ *mit dem Index* $(\mathfrak{G}:\mathfrak{N}) = 2$ *ist Normalteiler von* $\mathfrak{G}$.

Beweis

Wir zeigen $a\mathfrak{N} = \mathfrak{N}a$ für alle $a \in \mathfrak{G}$. Für $a \in \mathfrak{N}$ ist dies trivial. Für jedes andere $a \in \mathfrak{G}$ ist aber $a\mathfrak{N}$ wegen $(\mathfrak{G}:\mathfrak{N}) = 2$ die einzige noch vorhandene Linksnebenklasse von $\mathfrak{N}$ in $\mathfrak{G}$ und entsprechend

$\mathfrak{N}a$ die einzige noch vorhandene Rechtsnebenklasse. Wegen der Klasseneinteilung

$$\mathfrak{G} = \mathfrak{N} \cup a\mathfrak{N} = \mathfrak{N} \cup \mathfrak{N}a$$

stimmen beide überein. qed.

So ist z. B. die alternierende Gruppe $\mathfrak{A}_n$ stets Normalteiler der symmetrischen Gruppe $\mathfrak{S}_n$. Wir wollen hier nur bemerken, daß die symmetrische Gruppe $\mathfrak{S}_n$ für $n \geqq 5$ auch nur die Normalteiler $\mathfrak{E}$, $\mathfrak{A}_n$ und $\mathfrak{S}_n$ und die alternierende Gruppe $\mathfrak{A}_n$ nur die Normalteiler $\mathfrak{E}$ und $\mathfrak{A}_n$ besitzt. Letzteres ist für die Auflösungstheorie algebraischer Gleichungen von einschneidender Bedeutung, worauf wir später zurückkommen.

Der Normalteilerbegriff ist, wie aus der Definition hervorgeht, ein Relativbegriff zwischen zwei Gruppen. Die Eigenschaft einer Gruppe $\mathfrak{N}$, Normalteiler zu sein, bezieht sich stets auf eine bestimmte sie enthaltende Gruppe $\mathfrak{G}$. So ist z. B. die Gruppe $\mathfrak{A}_3$ Normalteiler in der Gruppe $\mathfrak{S}_3$, dagegen nicht mehr in der die Gruppe $\mathfrak{S}_3$ umfassenden Gruppe $\mathfrak{S}_4$. Es gilt jedoch:

Satz **S (17.4)**

Es sei $\mathfrak{N}$ Normalteiler von $\mathfrak{G}$. Dann ist $\mathfrak{N}$ auch Normalteiler jeder $\mathfrak{N}$ umfassenden Untergruppe $\mathfrak{H}$ von $\mathfrak{G}$.

Beweis

Aus $\mathfrak{N} = a^{-1}\mathfrak{N}a$ für alle $a \in \mathfrak{G}$ folgt erst recht $\mathfrak{N} = a^{-1}\mathfrak{N}a$ für alle $a \in \mathfrak{H} \subseteq \mathfrak{G}$.

qed.

So ist z. B. die Gruppe $\mathfrak{V}_4$ nicht nur Normalteiler von $\mathfrak{S}_4$, sondern auch von $\mathfrak{A}_4$ und den drei Untergruppen der $\mathfrak{S}_4$ von der Ordnung 8.

Wir können uns diese Verhältnisse durch einen sog. Graph veranschaulichen (vgl. Abb. 11). Aus der Normalteilereigenschaft bei ① folgt also die bei ②. Das ist aber auch das einzige, was in dieser Hinsicht allgemein ausgesagt werden kann. Man beachte daher:

1. Aus der Normalteilereigenschaft bei ① folgt nicht notwendig die bei ③. So ist z. B. $\mathfrak{N} = \mathfrak{V}_4$ Normalteiler von $\mathfrak{G} = \mathfrak{S}_4$, aber $\mathfrak{H} = \langle (13), (14)(23) \rangle$ mit $\mathfrak{V}_4 \lhd \mathfrak{H} \lhd \mathfrak{S}_4$ nicht Normalteiler von $\mathfrak{S}_4$.

2. Aus der Normalteilereigenschaft bei ② und ③ folgt nicht notwendig die bei ①. So ist z. B. $\mathfrak{N} = \langle (12)(34) \rangle$ Normalteiler von $\mathfrak{H} = \mathfrak{V}_4$ und $\mathfrak{V}_4$ wiederum Normalteiler von $\mathfrak{G} = \mathfrak{S}_4$, aber nicht $\langle (12)(34) \rangle$ Normalteiler von $\mathfrak{S}_4$.

3. Damit kann man erst recht die Normalteilereigenschaft bei ① nicht aus der bei ② oder aus der bei ③ folgern.

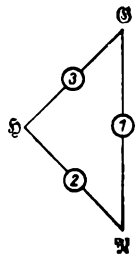


Abb. 11

Schließlich untersuchen wir, welche Komplexverknüpfungen von Normalteilern wieder Normalteiler ergeben.

Satz **S (17.5)**

Der Durchschnitt $\mathfrak{N}_1 \wedge \mathfrak{N}_2$ *zweier Normalteiler* $\mathfrak{N}_1$ *und* $\mathfrak{N}_2$ *von* $\mathfrak{G}$ *ist selbst Normalteiler von* $\mathfrak{G}$.

Beweis

$\mathfrak{N}_1 \wedge \mathfrak{N}_2$ ist nach S (5.10) Untergruppe von $\mathfrak{G}$. Da $\mathfrak{N}_1$ und $\mathfrak{N}_2$ aus vollständigen Klassen konjugierter Elemente bestehen, gilt dies wegen der Elementfremdheit der Klassen auch für den Durchschnitt $\mathfrak{N}_1 \wedge \mathfrak{N}_2$ (Kennzeichnung von Normalteilern nach S (17.2 c)).

qed.

Satz **S (17.6)**

Das Komplexprodukt $\mathfrak{N}_1 \cdot \mathfrak{N}_2$ *zweier Normalteiler* $\mathfrak{N}_1$ *und* $\mathfrak{N}_2$ *von* $\mathfrak{G}$ *ist selbst Normalteiler von* $\mathfrak{G}$.

Beweis

Für jedes Element $n_1 \in \mathfrak{N}_1$ gilt $n_1 \mathfrak{N}_2 = \mathfrak{N}_2 n_1$ und damit erst recht $\mathfrak{N}_1 \mathfrak{N}_2 = \mathfrak{N}_2 \mathfrak{N}_1$; also ist nach S (5.11) $\mathfrak{N}_1 \mathfrak{N}_2$ Untergruppe von $\mathfrak{G}$. Die Normalteilereigenschaft folgt aus:

$$a \mathfrak{N}_1 \mathfrak{N}_2 = \mathfrak{N}_1 a \mathfrak{N}_2 = \mathfrak{N}_1 \mathfrak{N}_2 a \quad \text{für alle } a \in \mathfrak{G}$$

(Kennzeichnung von Normalteilern nach S (17.2 a)).

qed.

Bemerkung

Die Vereinigung zweier Normalteiler von $\mathfrak{G}$ ist dagegen im allgemeinen kein Normalteiler von $\mathfrak{G}$, da sie nicht einmal Untergruppe zu sein braucht.

Als Beispiel für diese beiden Sätze betrachten wir die Gruppe $\mathfrak{G} = \langle (13), (14)(23) \rangle$ mit den nichttrivialen Normalteilern

$$\left.\begin{aligned} \mathfrak{N}_1 &= \{(1), (13)(24), (1234)\ (1432)\} \\ \mathfrak{N}_2 &= \{(1), (13)(24), (13), (24)\} \\ \mathfrak{N}_3 &= \{(1), (13)(24), (12)(34), (14)(23)\} \end{aligned}\right\} \text{Index } (\mathfrak{G}:\mathfrak{N}_i) = 2$$

$$\mathfrak{N}_4 = \{(1), (13)(24)\}.$$

Der Durchschnitt irgend zwei dieser Normalteiler ist stets gleich $\mathfrak{N}_4$, also ebenfalls Normalteiler von $\mathfrak{G}$. Entsprechendes gilt für die Komplexprodukte wegen

$$\mathfrak{N}_1\mathfrak{N}_2 = \mathfrak{N}_1\mathfrak{N}_3 = \mathfrak{N}_2\mathfrak{N}_3 = \mathfrak{G},$$
$$\mathfrak{N}_1\mathfrak{N}_4 = \mathfrak{N}_1,\ \mathfrak{N}_2\mathfrak{N}_4 = \mathfrak{N}_2,\ \mathfrak{N}_3\mathfrak{N}_4 = \mathfrak{N}_3.$$

Daß man die Voraussetzungen in beiden Sätzen nicht abschwächen kann, indem man nur von einer der beiden Untergruppen $\mathfrak{N}_1$ und $\mathfrak{N}_2$ die Normalteilereigenschaft fordert, zeigen wir durch folgende Gegenbeispiele. So sind etwa der Durchschnitt

$$\mathfrak{B}_4 \cap \{(1), (12), (34), (12)(34)\} = \{(1), (12)(34)\}$$

und das Komplexprodukt

$$\mathfrak{B}_4 \cdot \{(1), (13)\} = \langle (13), (14)(23) \rangle$$

nicht Normalteiler der symmetrischen Gruppe $\mathfrak{S}_4$, obwohl $\mathfrak{B}_4$ ein solcher ist.

Aufgaben zu § 17

1. Die multiplikative Gruppe $\mathfrak{G}$ aller regulären Matrizen vom Typ (n, n) mit reellen Zahlen als Matrizenelementen hat u. a. als Normalteiler die Untermenge aller Matrizen, deren Determinanten gleich 1 bzw. ± 1 sind oder auch derjenigen Matrizen, die ein skalares Vielfaches $\lambda E = (\lambda \delta_{ik})$ der Einheitsmatrix sind $(\lambda \neq 0)$.
2. Das Zentrum $\mathfrak{Z}$ von $\mathfrak{G}$ ist stets Normalteiler von $\mathfrak{G}$ und von jedem Normalisator $\mathfrak{B}_x$ von $x \in \mathfrak{G}$ bzw. $\mathfrak{B}_\mathfrak{H}$ von $\mathfrak{H} \subseteq \mathfrak{G}$ (Beispiele liefert die oben behandelte Gruppe $\mathfrak{G} = \langle (13), (14)(23) \rangle$ mit $\mathfrak{Z} = \mathfrak{N}_4$).
3. Die von $a \in \mathfrak{G}$ erzeugte zyklische Gruppe $\langle a \rangle$ ist Normalteiler des Normalisators $\mathfrak{B}_a$ von a. Entsprechend ist die Untergruppe $\mathfrak{H} \subseteq \mathfrak{G}$ Normalteiler des Normalisators $\mathfrak{B}_\mathfrak{H}$ von $\mathfrak{H}$.
4. Die Gruppe Φ' der inneren Automorphismen von $\mathfrak{G}$ ist Normalteiler der Automorphismengruppe Φ von $\mathfrak{G}$.
5. Der Durchschnitt aller Untergruppen einer Klasse konjugierter Untergruppen von $\mathfrak{G}$ ist Normalteiler von $\mathfrak{G}$.

6. Das Komplexprodukt $\mathfrak{H}\mathfrak{N}$ einer Untergruppe $\mathfrak{H} \subseteq \mathfrak{G}$ mit einem Normalteiler $\mathfrak{N}$ von $\mathfrak{G}$ ist Untergruppe von $\mathfrak{G}$.
7. Unter Verwendung von F(17.3) zeige man: Die abzählbare alternierende Gruppe $\mathfrak{A}_a$ ist Normalteiler der abzählbaren symmetrischen Gruppe $\mathfrak{S}_a$.

§ 18. Homomorphie

Die Isomorphie zwischen zwei Gruppen $\mathfrak{G}$ und $\overline{\mathfrak{G}}$ ist durch zwei Eigenschaften gekennzeichnet:

I: Es besteht eine eineindeutige Abbildung von $\mathfrak{G}$ auf $\overline{\mathfrak{G}}$.

II: Diese Abbildung ist relationstreu (vgl. D(4.3)).

Dabei bezieht sich die Aussage *I* nur auf die von den Gruppenelementen aus $\mathfrak{G}$ und $\overline{\mathfrak{G}}$ gebildeten Mengen, dagegen die Aussage *II* auf die in $\mathfrak{G}$ und $\overline{\mathfrak{G}}$ erklärten Verknüpfungen. Es liegt nahe, die unter *I* genannte rein mengentheoretische Forderung abzuschwächen. Das führt auf den für die Abbildungen von Gruppen zentralen Begriff der Homomorphie.

Definition **D (18.1)**

Es sei $\mathfrak{G}$ eine Gruppe und $\overline{\mathfrak{G}}$ eine Menge, für deren Elemente eine eindeutige Verknüpfung erklärt ist. Ohne Beschränkung der Allgemeinheit schreiben wir die Verknüpfung sowohl in $\mathfrak{G}$ als auch in $\overline{\mathfrak{G}}$ multiplikativ.

Dann heißt $\mathfrak{G}$ homomorph abgebildet auf $\overline{\mathfrak{G}}$, in Zeichen $\mathfrak{G} \xrightarrow{\sim} \overline{\mathfrak{G}}$, wenn gilt:

I: Es existiert eine eindeutige Abbildung von $\mathfrak{G}$ auf $\overline{\mathfrak{G}}$ vermöge der Zuordnung

$$a \to \bar{a} \quad \text{mit} \quad a \in \mathfrak{G},\ \bar{a} \in \overline{\mathfrak{G}}.$$

II: Diese Zuordnung ist relationstreu:

$$\overline{a \cdot b} = \bar{a} \cdot \bar{b}.$$

Man nennt die Abbildung selbst einen Homomorphismus, $\mathfrak{G}$ das Original und $\overline{\mathfrak{G}}$ das homomorphe Bild.

Folgerung **F (18.2)**

Das homomorphe Bild $\overline{\mathfrak{G}}$ einer Gruppe $\mathfrak{G}$ ist selbst Gruppe. Insbesondere überträgt sich etwaige Kommutativität.

Wir können den Beweis für F (18.2) in völliger Analogie zu dem von F (4.4) führen, da alle in ihm verwendeten Schlüsse von der eindeutigen Bestimmtheit des Originales zu jedem Bild (die bei einem Isomorphismus, nicht aber notwendig bei einem Homomorphismus vorliegt) unabhängig sind.

Folgerung **F (18.3)**

Es sei die Gruppe $\mathfrak{G}$ homomorph abgebildet auf die Gruppe $\overline{\mathfrak{G}}$. Dann läßt sich über die Abbildung einzelner Elemente folgendes aussagen:

a) *Das Bild des Einselementes $e \in \mathfrak{G}$ ist das Einselement $\bar{e} \in \overline{\mathfrak{G}}$.*

b) *Das Bild des zu $a \in \mathfrak{G}$ inversen Elementes a^{-1} ist das Inverse $\bar{a}^{-1}$ des Bildes $\bar{a} \in \overline{\mathfrak{G}}$ von a:*

$$\overline{(a^{-1})} = (\bar{a})^{-1}.$$

c) *Das Bild $\bar{a} \in \overline{\mathfrak{G}}$ eines Elementes $a \in \mathfrak{G}$ von endlicher Ordnung n hat als Ordnung einen Teiler m von n.*

Beweis

a) Aus $ea = a$ für alle $a \in \mathfrak{G}$ folgt $\overline{ae} = \bar{e} \cdot \bar{a} = \bar{a}$ für alle $\bar{a} \in \overline{\mathfrak{G}}$.

b) Die Behauptung ergibt sich aus $\overline{(a^{-1})}\,\bar{a} = \overline{(a^{-1})}\,\bar{a} = \bar{e}$.

c) Aus $\overline{(a^n)} = (\bar{a})^n = \bar{e}$ folgt $m \mid n$ nach S (6.6).

qed.

Beispiele **B (18.4)**

a) Es sei $\mathfrak{G} = \mathfrak{S}_n$ $(n > 2)$ und $\overline{\mathfrak{G}} = \{+1, -1\}$. Ordnet man jeder Permutation $s \in \mathfrak{S}_n$ ihr „Vorzeichen" zu

$$s \to \bar{s} = \operatorname{sgn}(s) = \begin{cases} +1, \text{ falls } s \text{ eine gerade Permutation ist,} \\ -1, \text{ falls } s \text{ eine ungerade Permutation ist,} \end{cases}$$

so vermittelt dies eine homomorphe Abbildung $\mathfrak{G} \xrightarrow{\sim} \overline{\mathfrak{G}}$. Die Zuordnung liefert nämlich eine eindeutige Abbildung von $\mathfrak{G}$ auf $\overline{\mathfrak{G}}$, die nach F (10.5) relationstreu ist:

$$\bar{s}_1 \cdot \bar{s}_2 = \operatorname{sgn}(s_1) \cdot \operatorname{sgn}(s_2) = \operatorname{sgn}(s_1 \cdot s_2) = \overline{s_1 \cdot s_2}.$$

b) Es sei $\mathfrak{G}$ die Gruppe aller regulären Matrizen vom Typ (n, n) mit reellen Zahlen als Matrizenelementen und $\overline{\mathfrak{G}}$ die multiplikative Gruppe der von Null verschiedenen reellen Zahlen. Wir ordnen jeder Matrix $A \in \mathfrak{G}$ ihre Determinante $|A| = \overline{A} \in \overline{\mathfrak{G}}$ zu. Diese Abbildung ist eindeutig und erschöpft mit ihren Bildern ganz $\overline{\mathfrak{G}}$, da jede reelle Zahl $a \neq 0$ wenigstens als Bild der Diagonalmatrix

$$A = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ & 1 & \\ 0 & & a \end{pmatrix} \to \overline{A} = |A| = a$$

auftritt. Die Relationstreue ergibt sich aus

$$\overline{A} \cdot \overline{B} = |A| \cdot |B| = |AB| = \overline{AB}.$$

Damit ist $\mathfrak{G}$ homomorph abgebildet auf $\overline{\mathfrak{G}}$.

c) Es sei $\mathfrak{G}$ der Modul der ganzen Zahlen und $\overline{\mathfrak{G}}$ der Restklassenmodul mod 5 (vgl. B(2.8b)). Als Bild ordnen wir jeder ganzen Zahl diejenige Restklasse mod 5 zu, in der sie selbst enthalten ist,

$$a \to \bar{a} = [a],$$

also ausführlich:

$$\begin{array}{lllll} -5 \searrow & -4 \searrow & -3 \searrow & -2 \searrow & -1 \searrow \\ 0 \to [0], & +1 \to [1], & +2 \to [2], & +3 \to [3], & +4 \to [4], \\ +5 \nearrow & +6 \nearrow & +7 \nearrow & +8 \nearrow & +9 \nearrow \end{array}$$

Diese Zuordnung vermittelt eine eindeutige Abbildung von $\mathfrak{G}$ auf $\overline{\mathfrak{G}}$, da jede ganze Zahl genau in einer Restklasse mod 5 liegt. Die Relationstreue ist nach Definition der Restklassenaddition

$$\bar{a} + \bar{b} = [a] + [b] = [a + b] = \overline{a + b}$$

erfüllt.

Auf die gleiche Weise kann man jeden Restklassenmodul mod m als homomorphes Bild des Moduls der ganzen Zahlen gewinnen. Damit ergibt sich die Moduleigenschaft des Restklassenmoduls mod m unmittelbar aus F(18.2), so daß sich von unserem jetzt gewonnenen Standpunkt der konkrete Nachweis in B(2.8b) erübrigt.

Wir gehen wieder zu allgemeinen Betrachtungen über und stellen zunächst fest, daß jeder Isomorphismus erst recht ein Homomorphismus und jeder eineindeutige Homomorphismus ein Isomorphismus ist. Dabei haben wir bisher beide Begriffe als „*Abbildungen auf*" festgelegt. Die Vorstellung, daß das homomorphe bzw. isomorphe Bild $\overline{\mathfrak{G}}$ von $\mathfrak{G}$ in einer Menge $\mathfrak{G}^*$ enthalten ist, führt dazu, diese Begriffe auch als „*Abbildungen in*" aufzufassen. Die sich daraus ergebenden vier Kombinationen werden noch verdoppelt, wenn man die Möglichkeit $\mathfrak{G}^* = \mathfrak{G}$, also $\overline{\mathfrak{G}} \subseteq \mathfrak{G}$ berücksichtigt. Wir stellen diese acht Kombinationen in einer Tabelle zusammen und geben gleichzeitig die gebräuchlichen Bezeichnungen für die auf diese Weise definierten Begriffe an:

Definition **D (18.5)**

Relationstreue Abbildung	*von* $\mathfrak{G}$ *auf* $\overline{\mathfrak{G}}$ *bzw. von* $\mathfrak{G}$ *in* $\overline{\mathfrak{G}}$
eindeutig $\mathfrak{G} \xrightarrow{\sim} \overline{\mathfrak{G}} \subseteq \mathfrak{G}^*$	*Homomorphismus*
insbes. $\overline{\mathfrak{G}} = \mathfrak{G}$ *bzw.* $\mathfrak{G}^* = \mathfrak{G}$	*Endomorphismus*
eineindeutig $\mathfrak{G} \xleftrightarrow{\sim} \overline{\mathfrak{G}} \subseteq \mathfrak{G}^*$	*Isomorphismus*
insbes. $\overline{\mathfrak{G}} = \mathfrak{G}$ *bzw.* $\mathfrak{G}^* = \mathfrak{G}$	*Automorphismus bzw. Meromorphismus*

Beispiele:

Die in B(18.4a) genannte Abbildung ist ein *Homomorphismus von* $\mathfrak{S}_n$ *auf* $\overline{\mathfrak{G}} = \{+1, -1\}$, dagegen ein *Homomorphismus von* $\mathfrak{S}_n$ *in* die multiplikativ verknüpfte Menge der rationalen Zahlen.

Wegen der Isomorphie der multiplikativen Gruppen $\{+1, -1\}$ und $\{(1), (12)\}$, die ja beide isomorph zur zyklischen Gruppe $\mathfrak{Z}_2$ sind, können wir als Bilder bei der obigen Abbildung $+1$ durch (1) und -1 durch (12) ersetzen. Das liefert einen *Endomorphismus von* $\mathfrak{S}_n$ *in* $\mathfrak{S}_n$.

Zum Beispiel wird dieser Endomorphismus für die Gruppe $\mathfrak{S}_3$ durch die Zuordnung gegeben:

$$\begin{matrix}(1)\\(123)\\(132)\end{matrix}\begin{matrix}\searrow\\\to\\\nearrow\end{matrix}(1),\qquad \begin{matrix}(12)\\(13)\\(23)\end{matrix}\begin{matrix}\searrow\\\to\\\nearrow\end{matrix}(12).$$

Ein *Endomorphismus einer Gruppe* $\mathfrak{G}$ *auf* sich selbst, der kein Automorphismus ist, kann natürlich nur bei unendlichen Gruppen auftreten. (Für ein Beispiel vergleiche man etwa das Lehrbuch von KUROSCH, § 18.)

Die Kennzeichnung der Deckabbildungen eines regelmäßigen Tetraeders durch die Permutationen der Eckpunkte ist ein *Isomorphismus der Tetraedergruppe* $\mathfrak{G}$ *auf* die alternierende Gruppe $\mathfrak{A}_4$ und ein *Isomorphismus von* $\mathfrak{G}$ *in* die symmetrische Gruppe $\mathfrak{S}_4$.

Die Zuordnung $a \to 2a$ liefert einen Isomorphismus des Moduls der ganzen Zahlen auf den Modul der geraden Zahlen, also einen Isomorphismus in sich selbst, d. h. einen *Meromorphismus* (vgl. Aufg. 1). Beispiele für *Automorphismen* haben wir in § 15 kennengelernt.

Wir haben dabei alle Beispiele in dem Sinne charakteristisch gegeben, daß sie nicht schon unter speziellere Begriffe fallen. Überdies verdeutlichen die Beispiele die Möglichkeit, bei Strukturuntersuchungen im allgemeinen die „Abbildungen in" durch „Abbildungen auf" zu beschreiben.

Im Gegensatz zu den isomorphen Abbildungen liefern die homomorphen Abbildungen keine Äquivalenzrelation, da aus der Existenz einer homomorphen Abbildung $\mathfrak{G}$ auf $\overline{\mathfrak{G}}$ nicht (wie bei der symmetrischen Beziehung der Isomorphie) auf die Existenz einer solchen von $\overline{\mathfrak{G}}$ auf $\mathfrak{G}$ geschlossen werden kann. Dagegen gilt:

Folgerung **F (18.6)**

Es sei $\mathfrak{G}$ *homomorph abgebildet auf* $\overline{\mathfrak{G}}$ *und* $\overline{\mathfrak{G}}$ *homomorph abgebildet auf* $\overline{\overline{\mathfrak{G}}}$. *Dann ist* $\overline{\overline{\mathfrak{G}}}$ *auch homomorphes Bild von* $\mathfrak{G}$:

$$\textit{Aus } \mathfrak{G} \xrightarrow{\sim} \overline{\mathfrak{G}} \textit{ und } \overline{\mathfrak{G}} \xrightarrow{\sim} \overline{\overline{\mathfrak{G}}} \textit{ folgt } \mathfrak{G} \xrightarrow{\sim} \overline{\overline{\mathfrak{G}}}.$$

Der Beweis dieser Folgerung entspricht wieder dem Beweis der Transitivität isomorpher Abbildungen in S (4.6).

Die nachfolgenden Untersuchungen zeigen, daß man sich eine Übersicht über sämtliche (strukturell verschiedenen) homomorphen Bilder einer Gruppe verschaffen kann. Wir kommen damit zu dem wichtigen Homomorphiesatz für Gruppen, den wir in mehreren Schritten beweisen.

Satz **S (18.7)**

Jede homomorphe Abbildung einer Gruppe $\mathfrak{G}$ auf eine Gruppe $\overline{\mathfrak{G}}$ vermittelt eine Klasseneinteilung von $\mathfrak{G}$ in Klassen $\mathfrak{A}, \mathfrak{B}, \ldots$ solcher Elemente von $\mathfrak{G}$, die auf dasselbe Bild von $\overline{\mathfrak{G}}$ abgebildet werden:

$$\mathfrak{A}\left\{\begin{array}{ccc} a & \searrow & \\ a' & \to & \bar{a}, \\ & \nearrow & \end{array}\right. \qquad \mathfrak{B}\left\{\begin{array}{ccc} b & \searrow & \\ b' & \to & \bar{b}, \\ & \nearrow & \end{array}\right.$$

Wir nennen die Klassen $\mathfrak{A}, \mathfrak{B}, \ldots$ kurz „Klassen bildgleicher Elemente".

Beweis

Nach Konstruktion sind die Klassen $\mathfrak{A}, \mathfrak{B}, \ldots$ nicht leer und erschöpfen ganz $\mathfrak{G}$. Aus der Eindeutigkeit der Abbildung folgt ihre Elementfremdheit.

qed.

Satz **S (18.8)**

Die Klasse $\mathfrak{N}$ derjenigen Elemente $n, n', \ldots$ von $\mathfrak{G}$, die bei einem Homomorphismus $\mathfrak{G} \xrightarrow{\sim} \overline{\mathfrak{G}}$ auf das Einselement $\bar{e} \in \overline{\mathfrak{G}}$ abgebildet werden, ist ein Normalteiler von $\mathfrak{G}$; dieser durch $\mathfrak{G} \xrightarrow{\sim} \overline{\mathfrak{G}}$ eindeutig bestimmte Normalteiler $\mathfrak{N}$ heißt der Kern des Homomorphismus. Die übrigen Klassen bildgleicher Elemente von $\mathfrak{G}$ sind genau die Nebenklassen von $\mathfrak{G}$ nach $\mathfrak{N}$.

Beweis

1. $\mathfrak{N}$ ist Untergruppe von $\mathfrak{G}$: Es wird nämlich mit n und n' auch das Produkt nn' wegen

$$\overline{nn'} = \bar{n} \cdot \overline{n'} = \bar{e} \cdot \bar{e} = \bar{e}$$

auf $\bar{e} \in \overline{\mathfrak{G}}$ abgebildet. Das gleiche gilt für das Inverse n^{-1} von n wegen

$$\overline{(n^{-1})} = (\bar{n})^{-1} = (\bar{e})^{-1} = \bar{e}.$$

2. $\mathfrak{N}$ ist Normalteiler von $\mathfrak{G}$: Dazu zeigen wir daß mit n auch alle zu n konjugierten Elemente $a^{-1}na$ in $\mathfrak{N}$ liegen (Normalteilereigenschaft S(17.2c)):

$$\overline{a^{-1}na} = \overline{a^{-1}} \cdot \bar{n} \cdot \bar{a} = \bar{a}^{-1} \cdot \bar{e} \cdot \bar{a} = \bar{a}^{-1} \cdot \bar{a} = \bar{e}.$$

3. Alle Elemente $a \cdot n$ einer Linksnebenklasse $a\mathfrak{N}$ haben das gleiche Bild $\bar{a} \in \overline{\mathfrak{G}}$:

$$\overline{an} = \bar{a} \cdot \bar{n} = \bar{a} \cdot \bar{e} = \bar{a}.$$

4. Zwei Elemente a und a' aus $\mathfrak{G}$, die das gleiche Bild $\bar{a} = \overline{a'}$ aus $\overline{\mathfrak{G}}$ haben, liegen in der gleichen Linksnebenklasse von $\mathfrak{G}$ nach $\mathfrak{N}$:

$$\overline{a^{-1}a'} = \overline{a^{-1}} \cdot \overline{a'} = \bar{a}^{-1}\bar{a} = \bar{e}.$$

Es gilt also $a^{-1}a' \in \mathfrak{N}$, woraus nach F(7.4) die Behauptung folgt.

Mit 3. und 4. ist die Übereinstimmung der in S(18.7) erklärten Klasseneinteilung mit der Klasseneinteilung von $\mathfrak{G}$ in Linksnebenklassen von $\mathfrak{G}$ nach $\mathfrak{N}$ gezeigt, die wegen der Normalteilereigenschaft von $\mathfrak{N}$ mit der Einteilung von $\mathfrak{G}$ in Rechtsnebenklassen von $\mathfrak{G}$ nach $\mathfrak{N}$ zusammenfällt. qed.

Dieser Satz lehrt, daß zu jeder homomorphen Abbildung $\mathfrak{G} \xrightarrow{\sim} \overline{\mathfrak{G}}$ ein eindeutig bestimmter Normalteiler als Kern gehört, der mit seinen Nebenklassen gerade die Klassen der bei diesem Homomorphismus bildgleichen Originale kennzeichnet. Es liegt umgekehrt der Gedanke nahe, zu jedem Normalteiler von $\mathfrak{G}$ und der durch ihn in $\mathfrak{G}$ bestimmten Klasseneinteilung in Nebenklassen eine homomorphe Abbildung zu konstruieren.

Satz **S (18.9)**

a) *Faßt man die Nebenklassen $a\mathfrak{N} = [a]$ eines Normalteilers $\mathfrak{N}$ von $\mathfrak{G}$ als Elemente einer neuen Menge auf, so bildet diese Menge mit der Komplexmultiplikation als Verknüpfung eine Gruppe, die sog. Faktorgruppe $\mathfrak{G}/\mathfrak{N}$ von $\mathfrak{G}$ nach $\mathfrak{N}$. Die Ordnung der Faktorgruppe $\mathfrak{G}/\mathfrak{N}$ ist der Index $(\mathfrak{G}:\mathfrak{N})$.*

b) *Die Gruppe $\mathfrak{G}$ wird auf die Faktorgruppe $\mathfrak{G}/\mathfrak{N}$ homomorph abgebildet vermöge der Zuordnung $a \to [a]$. Der Kern dieses Homomorphismus ist $\mathfrak{N}$, die Abbildung selbst nennt man auch den natürlichen Homomorphismus von $\mathfrak{G}$ bezüglich $\mathfrak{N}$.*

Beweis

a) Die Gruppeneigenschaft von $\mathfrak{G}/\mathfrak{N}$ folgt nach F(18.2), wenn b) gezeigt ist. Die Aussage über die Ordnung versteht sich von selbst.

b) Die Zuordnung $a \to [a]$ bildet jedes Element von $\mathfrak{G}$ auf diejenige Nebenklasse ab, in der es selbst enthalten ist. Sie vermittelt eine eindeutige Abbildung von $\mathfrak{G}$ auf die Menge der Nebenklassen, denn jedes Element aus $\mathfrak{G}$ liegt in genau einer Nebenklasse. Ferner ist die Abbildung relationstreu wegen $\mathfrak{N}b = b\mathfrak{N}$ für alle $b \in \mathfrak{G}$:

$$[a] \cdot [b] = a\mathfrak{N} \cdot b\mathfrak{N} = ab\mathfrak{N}\mathfrak{N} = ab\mathfrak{N} = [a \cdot b].$$

Das Einselement der Faktorgruppe ist $\mathfrak{N} = [e]$; also werden genau die Elemente von $\mathfrak{N}$ auf das Einselement von $\mathfrak{G}/\mathfrak{N}$ abgebildet.

qed.

Wir weisen schließlich nach, daß alle homomorphen Bilder, die durch Homomorphismen mit gleichem Kern $\mathfrak{N}$ geliefert werden, zueinander isomorph sind.

Satz **S (18.10)**

Es sei $\mathfrak{G} \xrightarrow{\sim} \overline{\mathfrak{G}}$ *eine homomorphe Abbildung vermöge der Zuordnung* $a \to \bar{a}$ *mit dem Kern* $\mathfrak{N}$. *Dann ist* $\overline{\mathfrak{G}}$ *isomorph zur Faktorgruppe* $\mathfrak{G}/\mathfrak{N}$ *vermöge der Zuordnung* $\bar{a} \to [a] = \varphi(\bar{a})$.
Umgekehrt ist jedes isomorphe Bild $\overline{\mathfrak{G}}$ *der Faktorgruppe* $\mathfrak{G}/\mathfrak{N}$ *ein homomorphes Bild von* $\mathfrak{G}$.

Beweis

Die Eineindeutigkeit der Zuordnung φ zwischen den Elementen von $\overline{\mathfrak{G}}$ und den Nebenklassen von $\mathfrak{G}/\mathfrak{N}$ wurde bereits in S(18.8) nachgewiesen. Die Relationstreue dieser Zuordnung folgt aus der Relationstreue des natürlichen Homomorphismus $\mathfrak{G} \xrightarrow{\sim} \mathfrak{G}/\mathfrak{N}$ und der Relationstreue der vorgegebenen homomorphen Abbildung $\mathfrak{G} \xrightarrow{\sim} \overline{\mathfrak{G}}$ wegen:

$$\varphi(\bar{a}) \cdot \varphi(\bar{b}) = [a] \cdot [b] = [ab] = \varphi(\overline{ab}) = \varphi(\bar{a} \cdot \bar{b}).$$

Die Umkehrung ergibt sich unmittelbar aus F(18.6).

qed.

Den Inhalt der letzten vier Sätze pflegt man in seinen wesentlichen Zügen zusammenzufassen im

Homomorphiesatz für Gruppen **S (18.11)**

Jede Gruppe $\overline{\mathfrak{G}}$, auf die die Gruppe $\mathfrak{G}$ homomorph abgebildet ist, ist isomorph einer Faktorgruppe $\mathfrak{G}/\mathfrak{N}$, wobei der Normalteiler $\mathfrak{N}$ von $\mathfrak{G}$ der Kern des Homomorphismus ist. Andererseits ist jede Faktorgruppe $\mathfrak{G}/\mathfrak{N}$ von $\mathfrak{G}$ nach einem Normalteiler $\mathfrak{N}$ von $\mathfrak{G}$ homomorphes Bild von $\mathfrak{G}$.

Folgerung **F (18.12)**

a) *Ein Homomorphismus $\mathfrak{G} \xrightarrow{\sim} \overline{\mathfrak{G}}$ ist dann und nur dann ein Isomorphismus, wenn der Kern $\mathfrak{N}$ gleich der Einheitsgruppe $\mathfrak{E} \leqq \mathfrak{G}$ ist.*

b) *Das homomorphe Bild $\overline{\mathfrak{G}}$ einer Gruppe $\mathfrak{G}$ ist dann und nur dann gleich der Einheitsgruppe $\overline{\mathfrak{E}}$, wenn der Kern $\mathfrak{N}$ des Homomorphismus $\mathfrak{G} \xrightarrow{\sim} \overline{\mathfrak{G}}$ gleich der Gruppe $\mathfrak{G}$ ist.*

Beweis

a) Es sei $\mathfrak{N} = \mathfrak{E}$. Dann besteht jede Nebenklasse von $\mathfrak{G}$ nach $\mathfrak{N}$ nur aus einem Element, also ist $\mathfrak{G}/\mathfrak{N} = \mathfrak{G}/\mathfrak{E} = \mathfrak{G}$. Also ist wegen S (18.10) $\overline{\mathfrak{G}} \xleftrightarrow{\sim} \mathfrak{G}$. Umgekehrt folgt aus $\mathfrak{G} \xleftrightarrow{\sim} \overline{\mathfrak{G}}$, daß wegen der Eineindeutigkeit dieser Abbildung nur ein Element aus $\mathfrak{G}$ auf das Einselement $\bar{e} \in \overline{\mathfrak{G}}$ abgebildet wird. Damit ergibt sich nach F (18.3) $\mathfrak{N} = \mathfrak{E}$.

b) Es sei $\mathfrak{N} = \mathfrak{G}$. Dann besteht $\overline{\mathfrak{G}} \xleftarrow{\sim} \mathfrak{G}/\mathfrak{N} = \mathfrak{G}/\mathfrak{G}$ nur aus einem Element und ist also die Einheitsgruppe. Ist umgekehrt $\overline{\mathfrak{G}} = \overline{\mathfrak{E}}$, besteht wegen $\overline{\mathfrak{G}} \xleftarrow{\sim} \mathfrak{G}/\mathfrak{N}$ die Faktorgruppe $\mathfrak{G}/\mathfrak{N}$ nur aus einem Element, woraus bereits $\mathfrak{N} = \mathfrak{G}$ folgt. qed.

Die Bedeutung des Homomorphiesatzes beruht u. a. darauf, daß mit allen Normalteilern einer Gruppe auch sämtliche homomorphen Bilder der Gruppe ihrer Struktur nach bekannt sind. So hat etwa die symmetrische Gruppe $\mathfrak{S}_4$ vier Normalteiler und damit genau vier strukturell verschiedene homomorphe Bilder (vgl. Aufg. 3):

$$\mathfrak{N} = \mathfrak{E} \qquad \mathfrak{S}_4 \xrightarrow{\sim} \mathfrak{S}_4$$
$$\mathfrak{N} = \mathfrak{V}_4\colon \quad \mathfrak{S}_4 \xrightarrow{\sim} \mathfrak{S}_4/\mathfrak{V}_4 \xleftrightarrow{\sim} \mathfrak{S}_3$$
$$\mathfrak{N} = \mathfrak{A}_4\colon \quad \mathfrak{S}_4 \xrightarrow{\sim} \mathfrak{S}_4/\mathfrak{A}_4 \xleftrightarrow{\sim} \mathfrak{S}_2$$
$$\mathfrak{N} = \mathfrak{S}_4\colon \quad \mathfrak{S}_4 \xrightarrow{\sim} \mathfrak{E}.$$

Neben der Beschreibung einzelner homomorpher Bilder von Gruppen findet der Homomorphiesatz aber vor allem bei allgemeinen Strukturüberlegungen Anwendung. So wird er auch im folgenden immer wieder herangezogen werden, ohne daß wir freilich seine Anwendungsmöglichkeiten irgendwie erschöpfen können.

Für das praktische Rechnen in Faktorgruppen sind die folgenden Bemerkungen nützlich. Die Elemente der Faktorgruppe $\mathfrak{G}/\mathfrak{N}$ sind die Nebenklassen des Normalteilers $\mathfrak{N}$ von $\mathfrak{G}$, als Verknüpfung dient die Komplexmultiplikation. Anstatt nun die Klassen dieser Klasseneinteilung von $\mathfrak{G}$ zu betrachten, kann man gemäß F (7.4) zu den einzelnen Elementen von $\mathfrak{G}$ übergehen; der Gleichheit zweier Klassen $a\mathfrak{N} = a'\mathfrak{N}$ entspricht dabei die Äquivalenz $a \sim a'$ der in ihnen enthaltenen Elemente. (Links- und Rechtsnebenklassen nach einem Normalteiler brauchen wir ja ebensowenig zu unterscheiden wie links- und rechtsseitige Äquivalenz nach diesem Normalteiler.) Bei diesem Übergang wird aus der Komplexmultiplikation der Nebenklassen die gewöhnliche Gruppenverknüpfung der Elemente, wobei wegen

$$a\mathfrak{N} \cdot b\mathfrak{N} = ab\mathfrak{N}$$

gilt: Aus $a \sim a'$ und $b \sim b'$ folgt $ab \sim a'b'$.

Wählt man also ein vollständiges Repräsentantensystem für die Nebenklassen von $\mathfrak{G}$ nach $\mathfrak{N}$ aus, so kann man die Produkte der Repräsentanten bis auf Äquivalenz in diesem Repräsentantensystem angeben, und diese Darstellung der Faktorgruppe ist von der Wahl des Repräsentantensystems unabhängig.

Beispiel:

Wir betrachten die Faktorgruppe $\mathfrak{G}/\mathfrak{N}$ mit $\mathfrak{G} = \langle (13), (14)(23)\rangle$ und $\mathfrak{N} = \langle (13)(24)\rangle$. Sie hat die folgenden vier Nebenklassen als Elemente:

$$\begin{aligned}
(1)\,\mathfrak{N} &= \{(1), (13)(24)\} &&= \mathfrak{K}_1\\
(13)\,\mathfrak{N} &= \{(13), (24)\} &&= \mathfrak{K}_2\\
(12)(34)\,\mathfrak{N} &= \{(12)(34), (14)(23)\} &&= \mathfrak{K}_3\\
(1234)\,\mathfrak{N} &= \{(1234), (1432)\} &&= \mathfrak{K}_4.
\end{aligned}$$

Die Komplexmultiplikation als Verknüpfung liefert die Strukturtafel:

$\mathfrak{K}_1$	$\mathfrak{K}_2$	$\mathfrak{K}_3$	$\mathfrak{K}_4$
$\mathfrak{K}_2$	$\mathfrak{K}_1$	$\mathfrak{K}_4$	$\mathfrak{K}_3$
$\mathfrak{K}_3$	$\mathfrak{K}_4$	$\mathfrak{K}_1$	$\mathfrak{K}_2$
$\mathfrak{K}_4$	$\mathfrak{K}_3$	$\mathfrak{K}_2$	$\mathfrak{K}_1$.

Gehen wir von der Gleichheit der Klassen zur Äquivalenz der Elemente über, so können wir die Klassen etwa der Reihe nach durch die Elemente (1), (13), (12)(34), (1234) repräsentieren. Mit diesen Elementen rechnen wir wie mit Elementen aus $\mathfrak{G}$, ersetzen jedoch aus dem Repräsentantensystem herausführende Produkte durch äquivalente Elemente aus dem Repräsentantensystem, z. B.

$$(13)\cdot(12)(34) = (1432) \sim (1234).$$

Damit können wir die Strukturtafel der Klassen ersetzen durch eine Strukturtafel der Repräsentanten:

(1)	(13)	(12)(34)	(1234)
(13)	(1)	(1234)	(12)(34)
(12)(34)	(1234)	(1)	(13)
(1234)	(12)(34)	(13)	(1).

Selbstverständlich sind die in dieser Strukturtafel auftretenden Elemente abhängig von der Wahl des Repräsentantensystems. So könnte z. B. überall (14)(23) an Stelle von (12)(34) stehen. Von dieser Möglichkeit abgesehen, für die Klassen verschiedene Repräsentanten zu wählen, stimmen jedoch alle diese Strukturtafeln mit der zuerst angegebenen Strukturtafel überein.

Unter Umständen ist es möglich, ein vollständiges Repräsentantensystem zu finden, dessen Elemente eine Untergruppe von $\mathfrak{G}$ bilden. Dies ist für das praktische Rechnen besonders vorteilhaft, da dann keine Produkte aus dem Repräsentantensystem herausführen und das Ersetzen durch äquivalente Elemente wegfällt (vgl. Aufg. 3).

Abschließend ist wieder zu betonen, daß wie alle unsere Überlegungen auch der Inhalt dieses Paragraphen von der multiplikativen Schreibweise unabhängig ist. So treten ja auch in den Beispielen einige additive Gruppen auf. Wir überlassen es dem Leser, sämtliche Aussagen nochmals für Moduln $\mathfrak{G}$ zu formulieren. Dabei ist die Vereinfachung zu berücksichtigen, daß es sich in diesem Falle um abelsche Gruppen handelt und also jeder Untermodul Normalteiler ist. Es kann daher jeder Untermodul $\mathfrak{H}$ als Kern eines Homomorphismus auftreten und nach jedem Untermodul $\mathfrak{H}$ eine Faktorgruppe $\mathfrak{G}/\mathfrak{H}$ gebildet werden. Analog der

Bezeichnung der Nebenklassen von $\mathfrak{H}$ in $\mathfrak{G}$ als Restklassen modulo $\mathfrak{H}$ (vgl. Ende § 7) nennt man die Faktorgruppe $\mathfrak{G}/\mathfrak{H}$ im allgemeinen den *Restklassenmodul von* $\mathfrak{G}$ *modulo* $\mathfrak{H}$. Die der Klasseneinteilung von $\mathfrak{G}$ nach $\mathfrak{H}$ entsprechende Äquivalenzrelation hatten wir bereits in § 7 als Kongruenz modulo $\mathfrak{H}$ eingeführt. Sie gestattet wieder, Rechnungen im Restklassenmodul mit Hilfe eines vollständigen Repräsentantensystems durchzuführen.

Als Beispiel gehen wir nochmals auf den Fall ein, daß $\mathfrak{G}$ der Modul der ganzen Zahlen ist. Nach Aufg. 14 von § 5 sind seine sämtlichen Untermoduln zyklisch und werden von einer nichtnegativen ganzen Zahl erzeugt. Die bereits in B(2.8) besprochenen Restklassenmoduln mod m ordnen sich damit unseren allgemeinen Begriffen unter (vgl. auch B(18.4c)). Ferner hatten wir schon am Ende von § 7 erkannt, daß die Kongruenz ganzer Zahlen nichts anderes ist als die zu der Restklasseneinteilung von $\mathfrak{G}$ nach einem Untermodul $\langle m \rangle$ gehörige Äquivalenzrelation. Jetzt sehen wir, daß die Addition von Kongruenzen als repräsentantenweises Rechnen im Restklassenmodul ebenfalls in umfassendere Zusammenhänge eingeordnet ist. Einen entsprechenden Sachverhalt werden wir auch für die Multiplikation von Kongruenzen später kennenlernen.

Aufgaben zu § 18

1. Man zeige, daß die Zuordnung $a \to 2a$ einen Isomorphismus des Moduls $\mathfrak{G}$ der ganzen Zahlen auf den Modul $\overline{\mathfrak{G}}$ der geraden Zahlen vermittelt.
2. Man bestimme zu jedem Homomorphismus in B(18.4) den Kern $\mathfrak{N}$.
3. Man beweise: $\mathfrak{S}_4/\mathfrak{B}_4 \overset{\sim}{\longleftrightarrow} \mathfrak{S}_3$, $\mathfrak{S}_4/\mathfrak{A}_4 \overset{\sim}{\longleftrightarrow} \mathfrak{S}_2$.
4. Man bilde alle Faktorgruppen von $\mathfrak{G} = \langle (13), (14)(23) \rangle$.
5. Es bezeichne $\mathfrak{G}_1$ bzw. $\mathfrak{G}_2$ bzw. $\mathfrak{G}_3$ die multiplikative Gruppe der von Null verschiedenen komplexen bzw. reellen bzw. rationalen Zahlen. Man bilde die Faktorgruppen $\mathfrak{G}_1/\mathfrak{G}_2$ bzw. $\mathfrak{G}_2/\mathfrak{G}_3$ und beschreibe ihre Elemente.
6. Man beschreibe die in der Trigonometrie übliche Rechnung mit Winkelargumenten modulo 2π als repräsentantenweises Rechnen in einem Restklassenmodul.
7. Das homomorphe Bild einer zyklischen Gruppe $\langle a \rangle$ ist selbst zyklisch; insbesondere ist ein solcher Homomorphismus allein durch die Zuordnung der primitiven Elemente festgelegt.
8. Alle zyklischen Gruppen sind homomorphe Bilder der unendlichen zyklischen Gruppe.

9. In Verallgemeinerung von B(15.4) zeige man: Sämtliche Endomorphismen einer zyklischen Gruppe $\mathfrak{Z}_n = \langle a \rangle$ der Ordnung n entstehen vermöge der Zuordnungen

$$a^i \to \overline{a^i} = (a^i)^\lambda \quad \begin{cases} \text{für alle } i \\ \text{mit festem } \lambda = 0, 1, \ldots, n-1. \end{cases}$$

10. Die Gruppe Φ' der inneren Automorphismen einer Gruppe $\mathfrak{G}$ ist isomorph zur Faktorgruppe $\mathfrak{G}/\mathfrak{Z}$ von $\mathfrak{G}$ nach ihrem Zentrum $\mathfrak{Z}$. So ist z.B. die Gruppe der inneren Automorphismen der Gruppe $\langle (13), (14)(23) \rangle$ isomorph zur Gruppe $\mathfrak{A}_4$ in Übereinstimmung mit Aufg. 6 von § 15 und obiger Aufg. 4. Entsprechend folgt $\Phi' \mathfrak{S}_n \overset{\sim}{\longleftarrow} \mathfrak{S}_n$ gemäß Aufg. 8 von § 16 (vgl. auch B(15.2)).

§ 19. Untergruppen bei homomorphen Abbildungen

Um weitere Einsichten in die wechselseitigen Zusammenhänge von Bild und Original bei homomorphen Abbildungen von Gruppen zu gewinnen, fragen wir insbesondere danach, wie sich Untergruppen bei solchen Abbildungen verhalten. Nach F(18.2) ergibt sich zunächst unmittelbar:

Satz **S(19.1)**

Bei einem Homomorphismus $\mathfrak{G} \overset{\sim}{\longrightarrow} \overline{\mathfrak{G}}$ *wird jede Untergruppe* $\mathfrak{H} \leqq \mathfrak{G}$ *auf eine Untergruppe* $\overline{\mathfrak{H}} \leqq \overline{\mathfrak{G}}$ *abgebildet.*

Als Beispiel bilden wir $\mathfrak{G} = \mathfrak{S}_4$ homomorph auf $\overline{\mathfrak{G}} = \mathfrak{S}_3$ ab vermöge der Zuordnung (vgl. Aufg. 3 von § 18):

$$\begin{array}{ll} (1) & \searrow \\ (12)(34) & \to \\ (13)(24) & \to \\ (14)(23) & \nearrow \end{array} (1), \qquad \begin{array}{ll} (123) & \searrow \\ (243) & \to \\ (142) & \to \\ (134) & \nearrow \end{array} (123), \qquad \begin{array}{ll} (132) & \searrow \\ (143) & \to \\ (234) & \to \\ (124) & \nearrow \end{array} (132),$$

$$\begin{array}{ll} (12) & \searrow \\ (34) & \to \\ (1423) & \to \\ (1324) & \nearrow \end{array} (12), \qquad \begin{array}{ll} (13) & \searrow \\ (1432) & \to \\ (24) & \to \\ (1234) & \nearrow \end{array} (13), \qquad \begin{array}{ll} (23) & \searrow \\ (1243) & \to \\ (1342) & \to \\ (14) & \nearrow \end{array} (23).$$

Es sei zunächst $\mathfrak{H} = \langle (1324) \rangle = \{(1), (12)(34), (1324), (1423)\}$. Dann ist das Bild $\overline{\mathfrak{H}} = \{(1), (12)\}$ von $\mathfrak{H}$ eine Untergruppe von $\overline{\mathfrak{G}}$. Das Beispiel lehrt darüber hinaus, daß verschiedene Untergruppen

von $\mathfrak{G}$ durchaus das gleiche Bild $\overline{\mathfrak{H}} \leqq \overline{\mathfrak{G}}$ haben können. So werden die folgenden Untergruppen ebenfalls auf $\overline{\mathfrak{H}}$ abgebildet:

$$\{(1), (12)\},\ \{(1), (34)\},\ \{(1), (12)(34), (12), (34)\},$$
$$\{(1), (12)(34), (13)(24), (14)(23), (12), (34), (1324), (1423)\}.$$

Von diesen fünf auf $\overline{\mathfrak{H}}$ abgebildeten Untergruppen ist die letzte dadurch ausgezeichnet, daß sie alle Originale von Elementen aus $\overline{\mathfrak{H}}$ und damit die übrigen Untergruppen sowie überdies den Kern $\mathfrak{N} = \mathfrak{V}_4$ des Homomorphismus $\mathfrak{S}_4 \xrightarrow{\sim} \mathfrak{S}_3$ enthält. Dies führt uns zur folgenden allgemeinen Aussage:

Satz **S (19.2)**

Bei einem Homomorphismus $\mathfrak{G} \xrightarrow{\sim} \overline{\mathfrak{G}}$ mit dem Kern $\mathfrak{N}$ ist das vollständige Original einer Untergruppe $\overline{\mathfrak{H}} \leqq \overline{\mathfrak{G}}$, also der Komplex aller derjenigen Elemente von $\mathfrak{G}$, die auf Elemente von $\overline{\mathfrak{H}}$ abgebildet werden, eine Untergruppe $\mathfrak{K} \leqq \mathfrak{G}$. Man erhält $\mathfrak{K}$ aus jeder Untergruppe $\mathfrak{H} \leqq \mathfrak{G}$ mit dem Bild $\overline{\mathfrak{H}} \leqq \overline{\mathfrak{G}}$ vermöge

$$\mathfrak{K} = \mathfrak{H} \cdot \mathfrak{N}.$$

Das vollständige Original $\mathfrak{K}$ von $\overline{\mathfrak{H}}$ enthält alle Untergruppen $\mathfrak{H} \leqq \mathfrak{G}$, die bei $\mathfrak{G} \xrightarrow{\sim} \overline{\mathfrak{G}}$ auf $\overline{\mathfrak{H}} \leqq \overline{\mathfrak{G}}$ abgebildet werden, und ist von allen diesen Untergruppen die einzige, die den Kern $\mathfrak{N}$ des Homomorphismus umfaßt.

Beweis

Es seien a und b Elemente des vollständigen Originals $\mathfrak{K}$ von $\overline{\mathfrak{H}}$. Dann gilt wegen $a \to \bar{a} \in \overline{\mathfrak{H}}$ und $\bar{b} \in \overline{\mathfrak{H}}$ auch

$$a b^{-1} \to \overline{a b^{-1}} = \bar{a} \bar{b}^{-1} \in \overline{\mathfrak{H}},$$

d. h. $a b^{-1} \in \mathfrak{K}$. Nach S (5.5) ist $\mathfrak{K}$ also Untergruppe von $\mathfrak{G}$.

Es sei ferner $\mathfrak{H}$ irgendeine Untergruppe von $\mathfrak{G}$ mit dem Bild $\overline{\mathfrak{H}} \leqq \overline{\mathfrak{G}}$. Dann hat jedes Element $\bar{h} \in \overline{\mathfrak{H}}$ wenigstens ein Original $h \in \mathfrak{H}$, und alle in $\mathfrak{G}$ liegenden Originale von $\bar{h}$ bei $\mathfrak{G} \xrightarrow{\sim} \overline{\mathfrak{G}}$ sind nach S (18.8) genau die Vereinigung aller Produkte $h\mathfrak{N}$ mit $h \in \mathfrak{H}$, also das Komplexprodukt $\mathfrak{H}\mathfrak{N}$.

Daß $\mathfrak{K}$ alle auf $\overline{\mathfrak{H}}$ abgebildeten Untergruppen $\mathfrak{H}$ enthält, ist begrifflich klar, folgt aber auch aus $\mathfrak{K} = \mathfrak{H}\mathfrak{N}$ wegen $e \in \mathfrak{N}$. Desgleichen ergibt sich $\mathfrak{N} \subseteq \mathfrak{K}$ aus $\mathfrak{K} = \mathfrak{H}\mathfrak{N}$ wegen $e \in \mathfrak{H}$. Jede andere Untergruppe $\mathfrak{H}$ mit dem Bild $\overline{\mathfrak{H}}$ und $\mathfrak{N} \subseteq \mathfrak{H}$ stimmt nach S(5.9) wegen $\mathfrak{K} = \mathfrak{H}\mathfrak{N} = \mathfrak{H}$ mit $\mathfrak{K}$ überein. qed.

Wir haben damit eine eineindeutige Zuordnung zwischen den Untergruppen $\overline{\mathfrak{H}} \subseteq \overline{\mathfrak{G}}$ und denjenigen Untergruppen $\mathfrak{H} \subseteq \mathfrak{G}$ hergestellt, die als vollständige Originale den Kern $\mathfrak{N}$ des Homomorphismus $\mathfrak{G} \xrightarrow{\sim} \overline{\mathfrak{G}}$ enthalten. Insbesondere ergibt sich:

Folgerung **F (19.3)**

Sämtliche Untergruppen $\overline{\mathfrak{H}}$ einer Gruppe $\overline{\mathfrak{G}}$, auf die eine Gruppe $\mathfrak{G}$ mit dem Kern $\mathfrak{N}$ homomorph abgebildet ist, erhält man bereits als Bilder derjenigen Untergruppen $\mathfrak{H} \subseteq \mathfrak{G}$, die den Kern $\mathfrak{N}$ umfassen.

Wir sind bisher von einem Homomorphismus $\mathfrak{G} \xrightarrow{\sim} \overline{\mathfrak{G}}$ mit dem Kern $\mathfrak{N}$ ausgegangen und haben die dadurch bewirkten homomorphen Abbildungen der Untergruppen $\mathfrak{H} \xrightarrow{\sim} \overline{\mathfrak{H}}$ betrachtet. Nach dem Homomorphiesatz muß nun auch $\overline{\mathfrak{H}}$ isomorph zu einer Faktorgruppe der Gruppe $\mathfrak{H}$ nach einem bestimmten Normalteiler von $\mathfrak{H}$ sein:

Satz **S (19.4)**

Die durch den Homomorphismus $\mathfrak{G} \xrightarrow{\sim} \overline{\mathfrak{G}}$ mit dem Kern $\mathfrak{N}$ bewirkte homomorphe Abbildung der Untergruppe $\mathfrak{H} \xrightarrow{\sim} \overline{\mathfrak{H}}$ hat den Kern $\mathfrak{H} \cap \mathfrak{N}$. Es ist also

$$\overline{\mathfrak{H}} \xleftrightarrow{\sim} \mathfrak{H}/(\mathfrak{H} \cap \mathfrak{N}).$$

Beweis

Der Kern des Homomorphismus $\mathfrak{H} \xrightarrow{\sim} \overline{\mathfrak{H}}$ besteht genau aus den Elementen von $\mathfrak{G}$, die auf das Einselement $\bar{e} \in \overline{\mathfrak{H}} \subseteq \overline{\mathfrak{G}}$ abgebildet werden. Das sind aber genau diejenigen Elemente von $\mathfrak{G}$, die sowohl in $\mathfrak{H}$ als auch in $\mathfrak{N}$, also in $\mathfrak{H} \cap \mathfrak{N}$ liegen. qed.

Damit haben wir insbesondere bewiesen, daß der Durchschnitt irgendeiner Untergruppe von $\mathfrak{G}$ mit einem Normalteiler von $\mathfrak{G}$ stets Normalteiler dieser Untergruppe ist (vgl. auch Aufg. 2). Die Anwendung von S(19.4) auf eine beliebige Untergruppe und das voll-

ständige Original ihres Bildes ergibt den für strukturelle Untersuchungen tragenden

1. Isomorphiesatz **S (19.5)**

Es sei $\mathfrak{G}$ eine Gruppe, $\mathfrak{H}$ eine Untergruppe von $\mathfrak{G}$ und $\mathfrak{N}$ ein Normalteiler von $\mathfrak{G}$. Dann ist

$$\mathfrak{H}\mathfrak{N}/\mathfrak{N} \xleftrightarrow{\sim} \mathfrak{H}/(\mathfrak{H} \cap \mathfrak{N}).$$

Beweis

Wir bilden $\mathfrak{G}$ mit dem Kern $\mathfrak{N}$ homomorph auf $\overline{\mathfrak{G}}$ und damit $\mathfrak{H}$ auf $\overline{\mathfrak{H}} \subseteq \overline{\mathfrak{G}}$ ab. Damit erhalten wir nach S(19.4) einerseits

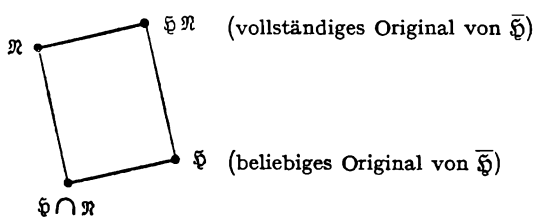
$$\overline{\mathfrak{H}} \xleftrightarrow{\sim} \mathfrak{H}/(\mathfrak{H} \cap \mathfrak{N}).$$

Wenden wir andererseits S(19.4) auf das in S(19.2) bestimmte vollständige Original $\mathfrak{K} = \mathfrak{H}\mathfrak{N}$ von $\overline{\mathfrak{H}}$ an, ergibt sich wegen $\mathfrak{N} \subseteq \mathfrak{K}$:

$$\overline{\mathfrak{H}} \xleftrightarrow{\sim} \mathfrak{K}/(\mathfrak{K} \cap \mathfrak{N}) = \mathfrak{H}\mathfrak{N}/\mathfrak{N}.$$

Aus der Transitivität der Isomorphie folgt die Behauptung. qed.

Zur besseren Einprägung veranschaulichen wir den 1. Isomorphiesatz und seinen Beweisgedanken wieder durch einen Graph:



Die stark ausgezogenen Striche bedeuten dabei nicht nur Untergruppen-, sondern sogar Normalteilereigenschaft. Die beiden Faktorgruppen sind zu $\overline{\mathfrak{H}}$ und damit zueinander isomorph. Über eine weitere Aussage an Hand dieses Graph vergleiche man Aufg. 5.

Als Beispiel wählen wir wie oben $\mathfrak{G} = \mathfrak{S}_4$, $\mathfrak{H} = \langle(1324)\rangle$ und $\mathfrak{N} = \mathfrak{V}_4$. Dann gilt

$$\mathfrak{H}\mathfrak{N} = \langle(12), (14)(23)\rangle, \quad \mathfrak{H} \cap \mathfrak{N} = \{(1), (12)(34)\},$$

und die Faktorgruppen $\mathfrak{H}\mathfrak{N}/\mathfrak{N}$ und $\mathfrak{H}/(\mathfrak{H} \cap \mathfrak{N})$ sind beide isomorph zur zyklischen Gruppe $\mathfrak{Z}_2$.

Wir vermerken noch, daß der 1. Isomorphiesatz für den Fall $\mathfrak{N} \leqq \mathfrak{H}$ zu der Trivialität $\mathfrak{H}/\mathfrak{N} \longleftrightarrow \mathfrak{H}/\mathfrak{N}$ ausartet. Im obigen Graph fallen dann die beiden stark ausgezogenen Strecken zusammen.

Es ist nun wichtig, daß sich nicht nur die Untergruppeneigenschaft, sondern sogar die Normalteilereigenschaft bei homomorphen Abbildungen überträgt:

Satz **S (19.6)**

a) *Bei einem Homomorphismus* $\mathfrak{G} \longrightarrow \overline{\mathfrak{G}}$ *wird jeder Normalteiler* $\mathfrak{H}$ *von* $\mathfrak{G}$ *auf einen Normalteiler* $\overline{\mathfrak{H}}$ *von* $\overline{\mathfrak{G}}$ *abgebildet.*

b) *Umgekehrt ist das vollständige Original* $\mathfrak{K}$ *eines Normalteilers* $\overline{\mathfrak{H}}$ *von* $\overline{\mathfrak{G}}$ *ein Normalteiler von* $\mathfrak{G}$.

Beweis

Wegen S(19.1) und S(19.2) brauchen wir in beiden Fällen nur noch die Normalteilereigenschaft nachzuweisen und benutzen dazu S(17.2c).

a) $\overline{\mathfrak{H}}$ enthält mit jedem Element $\bar{h}$ auch alle zu ihm konjugierten Elemente. Es ist nämlich für alle $\bar{a} \in \overline{\mathfrak{G}}$

$$\bar{a}^{-1}\bar{h}\bar{a} = \overline{a^{-1}ha}$$

das Bild eines Elementes $a^{-1}ha$ des Normalteilers $\mathfrak{H}$ von $\mathfrak{G}$.

b) $\mathfrak{K}$ enthält mit jedem Element k auch alle zu ihm konjugierten Elemente. Es wird nämlich für alle $a \in \mathfrak{G}$ jedes $a^{-1}ka$ wegen

$$\overline{a^{-1}ka} = \bar{a}^{-1}\bar{k}\bar{a}$$

auf ein Element des Normalteilers $\overline{\mathfrak{H}}$ von $\overline{\mathfrak{G}}$ abgebildet, gehört also zum vollständigen Original $\mathfrak{K}$. qed.

Wenden wir unsere Überlegungen insbesondere auf den natürlichen Homomorphismus $\mathfrak{G} \longrightarrow \hat{\mathfrak{G}} = \mathfrak{G}/\mathfrak{N}$ an, so besteht das vollständige Original $\mathfrak{K}$ jeder Untergruppe $\hat{\mathfrak{H}} \leqq \hat{\mathfrak{G}}$ aus vollständigen Nebenklassen von $\mathfrak{N}$ in $\mathfrak{G}$, und diese Nebenklassen sind genau die Elemente von $\hat{\mathfrak{H}}$.

Umgekehrt enthält jede Untergruppe $\mathfrak{H} \leqq \mathfrak{G}$, die aus vollständigen Nebenklassen von $\mathfrak{N}$ in $\mathfrak{G}$ besteht, mit dem Einselement auch $\mathfrak{N}$

und ist also vollständiges Original derjenigen Untergruppe $\hat{\mathfrak{H}}$, die gerade diese Nebenklassen als Elemente enthält. Die auf diese Weise einander eineindeutig entsprechenden Untergruppen $\hat{\mathfrak{H}} \leqq \hat{\mathfrak{G}}$ und $\mathfrak{H} \leqq \mathfrak{G}$ entstehen also auseinander, indem man die $\hat{\mathfrak{H}}$ bildenden Nebenklassen von $\mathfrak{G}$ nach $\mathfrak{N}$ in ihre einzelnen Elemente zerlegt oder umgekehrt die Elemente von $\mathfrak{H}$ zu vollständigen Nebenklassen von $\mathfrak{G}$ nach $\mathfrak{N}$ zusammenfaßt. Nach S(19.6) erhält man dabei insbesondere aus Normalteilern in beiden Richtungen ebenfalls Normalteiler.

Wendet man auf das so bestimmte vollständige Original $\mathfrak{H}$ von $\hat{\mathfrak{H}}$ S(19.4) an, erhält man wegen $\mathfrak{N} \leqq \mathfrak{H}$ nicht nur

$$\hat{\mathfrak{H}} \overset{\sim}{\longleftarrow} \mathfrak{H}/\mathfrak{N},$$

sondern sogar

$$\hat{\mathfrak{H}} = \mathfrak{H}/\mathfrak{N}.$$

$\hat{\mathfrak{H}}$ und $\mathfrak{H}/\mathfrak{N}$ bestehen dann nämlich aus genau denselben Nebenklassen von $\mathfrak{N}$ in $\mathfrak{G}$.

Als Beispiel wählen wir wieder $\mathfrak{G} = \mathfrak{S}_4$ und $\mathfrak{N} = \mathfrak{B}_4$, betrachten jedoch als homomorphes Bild nicht die Gruppe $\mathfrak{G} = \mathfrak{S}_3$, sondern die nach dem Homomorphiesatz zu ihr isomorphe Faktorgruppe $\hat{\mathfrak{G}} = \mathfrak{S}_4/\mathfrak{B}_4$:

$$\begin{matrix}(1)\\(12)(34)\\(13)(24)\\(14)(23)\end{matrix}\ \begin{matrix}\searrow\\\rightarrow\\\rightarrow\\\nearrow\end{matrix}\ [(1)] = (1)\cdot\mathfrak{B}_4; \qquad \begin{matrix}(123)\\(243)\\(142)\\(134)\end{matrix}\ \begin{matrix}\searrow\\\rightarrow\\\rightarrow\\\nearrow\end{matrix}\ [(123)] = (123)\cdot\mathfrak{B}_4;$$

$$\begin{matrix}(132)\\(143)\\(234)\\(124)\end{matrix}\ \begin{matrix}\searrow\\\rightarrow\\\rightarrow\\\nearrow\end{matrix}\ [(132)] = (132)\cdot\mathfrak{B}_4; \qquad \begin{matrix}(12)\\(34)\\(1423)\\(1324)\end{matrix}\ \begin{matrix}\searrow\\\rightarrow\\\rightarrow\\\nearrow\end{matrix}\ [(12)] = (12)\cdot\mathfrak{B}_4:$$

$$\begin{matrix}(13)\\(1432)\\(24)\\(1234)\end{matrix}\ \begin{matrix}\searrow\\\rightarrow\\\rightarrow\\\nearrow\end{matrix}\ [(13)] = (13)\cdot\mathfrak{B}_4; \qquad \begin{matrix}(23)\\(1243)\\(1342)\\(14)\end{matrix}\ \begin{matrix}\searrow\\\rightarrow\\\rightarrow\\\nearrow\end{matrix}\ [(23)] = (23)\cdot\mathfrak{B}_4;$$

Eine Untergruppe $\hat{\mathfrak{H}} \leqq \hat{\mathfrak{G}}$ ist etwa $\{[(1)], [(123)], [(132)]\}$. Lösen wir diese Nebenklassen in ihre Elemente auf, so erhalten wir $\mathfrak{A}_4$ als vollständiges Original von $\hat{\mathfrak{H}}$. Umgekehrt entsteht $\hat{\mathfrak{H}}$ durch Zusammenfassen der Elemente von $\mathfrak{A}_4 \supseteqq \mathfrak{N} = \mathfrak{V}_4$ in Nebenklassen, und es ist $\hat{\mathfrak{H}} = \mathfrak{A}_4/\mathfrak{V}_4$. Dabei folgt die Normalteilereigenschaft von $\hat{\mathfrak{H}}$ in $\hat{\mathfrak{G}}$ aus der von $\mathfrak{A}_4$ in $\mathfrak{S}_4$ und umgekehrt.

Abschließend behandeln wir noch zwei zusammenhängende Aussagen, die aus der in F(18.6) gezeigten Transitivität homomorpher Abbildungen entspringen und an die Überlegungen in S(18.8) bzw. S(18.9) anknüpfen.

Satz **S(19.7)**

Es sei $\mathfrak{G}$ homomorph abgebildet auf $\overline{\mathfrak{G}}$ mit dem Normalteiler $\mathfrak{N}$ von $\mathfrak{G}$ als Kern und $\overline{\mathfrak{G}}$ homomorph abgebildet auf $\overline{\overline{\mathfrak{G}}}$ mit dem Normalteiler $\overline{\mathfrak{H}}$ von $\overline{\mathfrak{G}}$ als Kern.

Dann ist $\mathfrak{G}$ homomorph abgebildet auf $\overline{\overline{\mathfrak{G}}}$, wobei der Kern dieses Homomorphismus das vollständige Original $\mathfrak{K}$ von $\overline{\mathfrak{H}}$ ist.

Beweis

Wegen F(18.6) bleibt nur die Aussage über den Kern $\mathfrak{K}$ nachzuweisen. Er ist bestimmt als die Gesamtheit aller derjenigen Elemente von $\mathfrak{G}$, die bei $\mathfrak{G} \xrightarrow{\sim} \overline{\overline{\mathfrak{G}}}$ das Einselement $\overline{\overline{e}} \in \overline{\overline{\mathfrak{G}}}$ zum Bilde haben. Da sich $\mathfrak{G} \xrightarrow{\sim} \overline{\overline{\mathfrak{G}}}$ gemäß $\mathfrak{G} \xrightarrow{\sim} \overline{\mathfrak{G}} \xrightarrow{\sim} \overline{\overline{\mathfrak{G}}}$ zusammensetzt, werden aber genau die Elemente von $\mathfrak{K} \leqq \mathfrak{G}$ über $\overline{\mathfrak{H}} \leqq \overline{\mathfrak{G}}$ auf $\overline{\overline{e}} \in \overline{\overline{\mathfrak{G}}}$ abgebildet. qed.

Wir bemerken noch, daß man den Kern des Homomorphismus $\overline{\mathfrak{G}} \xrightarrow{\sim} \mathfrak{G}$ als vollständiges Original von $\overline{\mathfrak{H}}$ nach S(19.2) mit Hilfe eines beliebigen Originals $\mathfrak{H}$ von $\overline{\mathfrak{H}}$ in der Form $\mathfrak{K} = \mathfrak{H}\mathfrak{N}$ gewinnen kann. Ferner ergibt sich aus S(19.7) erneut die in S(19.6b) ausgesprochene Übertragung der Normalteilereigenschaft von $\overline{\mathfrak{H}}$ auf das vollständige Original $\mathfrak{K}$ von $\overline{\mathfrak{H}}$.

Aufbauend auf S(19.7) erhalten wir den

2. Isomorphiesatz **S(19.8)**

Sei $\mathfrak{G}$ eine Gruppe, $\mathfrak{H}$ ein Normalteiler von $\mathfrak{G}$ und $\mathfrak{N} \leqq \mathfrak{H}$ ein Normalteiler von $\mathfrak{G}$. Dann ist

$$(\mathfrak{G}/\mathfrak{N})/(\mathfrak{H}/\mathfrak{N}) \xleftrightarrow{\sim} \mathfrak{G}/\mathfrak{H}.$$

Beweis

Es gilt:

$$\mathfrak{G} \xrightarrow{\sim} \hat{\mathfrak{G}} = \mathfrak{G}/\mathfrak{N} \quad \text{mit} \quad \mathfrak{H} \xrightarrow{\sim} \hat{\mathfrak{H}} = \mathfrak{H}/\mathfrak{N}.$$

Nach S(19.6a) ist $\hat{\mathfrak{H}}$ Normalteiler von $\hat{\mathfrak{G}}$. Wir können also weiterhin abbilden

$$\hat{\mathfrak{G}} \xrightarrow{\sim} \hat{\mathfrak{G}}/\hat{\mathfrak{H}} = (\mathfrak{G}/\mathfrak{N})\,/\,(\mathfrak{H}/\mathfrak{N})$$

und S(19.7) anwenden. Danach ist $\hat{\mathfrak{G}}/\hat{\mathfrak{H}}$ homomorphes Bild von $\mathfrak{G}$ mit dem Kern $\mathfrak{K} = \mathfrak{H}\mathfrak{N} = \mathfrak{H}$ (wegen $\mathfrak{N} \leqq \mathfrak{H}$), also nach S(18.9) isomorph zur Faktorgruppe $\mathfrak{G}/\mathfrak{H}$. qed.

So ist z.B. $\mathfrak{S}_4 \xrightarrow{\sim} \mathfrak{S}_3$ mit dem Kern $\mathfrak{B}_4$, $\mathfrak{S}_3 \xrightarrow{\sim} \mathfrak{S}_2$ mit dem Kern $\mathfrak{A}_3$ und in Übereinstimmung mit S(19.7) $\mathfrak{S}_4 \xrightarrow{\sim} \mathfrak{S}_2$ mit dem Kern $\mathfrak{A}_4 = \mathfrak{B}_4 \cdot \mathfrak{A}_3$. Der 2. Isomorphiesatz spiegelt sich wider in

$$(\mathfrak{S}_4/\mathfrak{B}_4)/(\mathfrak{A}_4/\mathfrak{B}_4) \xleftarrow{\sim} \mathfrak{S}_4/\mathfrak{A}_4,$$

denn es ist wegen $\mathfrak{S}_4/\mathfrak{B}_4 \xleftarrow{\sim} \mathfrak{S}_3$ und $\mathfrak{A}_4/\mathfrak{B}_4 \xleftarrow{\sim} \mathfrak{A}_3$ sowohl $(\mathfrak{S}_4/\mathfrak{B}_4)\,/\,(\mathfrak{A}_4/\mathfrak{B}_4)$ als auch $\mathfrak{S}_4/\mathfrak{A}_4$ isomorph zur zyklischen Gruppe $\mathfrak{Z}_2$.

Aufgaben zu § 19

1. Man bestimme die vollständigen Originale aller Untergruppen der Gruppe $\mathfrak{S}_3$ bei der homomorphen Abbildung $\mathfrak{S}_4 \xrightarrow{\sim} \mathfrak{S}_3$.
2. Man beweise direkt: Es sei $\mathfrak{H}$ eine Untergruppe der Gruppe $\mathfrak{G}$ und $\mathfrak{N}$ ein Normalteiler von $\mathfrak{G}$. Dann ist $\mathfrak{H} \cap \mathfrak{N}$ Normalteiler von $\mathfrak{H}$.
3. Man zeige die Isomorphie $\mathfrak{S}_4/\mathfrak{B}_4 \xleftarrow{\sim} \mathfrak{S}_3$ mit Hilfe des 1. Isomorphiesatzes.
4. Man veranschauliche sich den 2. Isomorphiesatz mit Hilfe der Gruppe $\mathfrak{G} = \langle (13), (14)(23) \rangle$, indem man geeignete Normalteiler dieser Gruppe wählt.
5. Für endliche Gruppen gilt mit den Bezeichnungen von S(19.5):

$$(\mathfrak{H}\mathfrak{N} : \mathfrak{H}) = (\mathfrak{N} : (\mathfrak{N} \cap \mathfrak{H})).$$

IV. EINIGE WICHTIGE STRUKTURAUSSAGEN ÜBER GRUPPEN

Aus der Fülle der über die bisher entwickelten allgemeinen Grundlagen hinausgehenden Untersuchungen, die den Inhalt der Gruppentheorie ausmachen, können wir abschließend lediglich ein spezielles Teilgebiet herausgreifen. Dabei bestimmt sich unsere Auswahl im Hinblick auf den Problemkreis, aus dem ja die Gruppentheorie überhaupt hervorgegangen ist: der Frage nach der Auflösbarkeit algebraischer Gleichungen. Allerdings können wir auf diese Anwendung erst später zu sprechen kommen, während wir hier nur die erforderlichen gruppentheoretischen Hilfsmittel darlegen. In ihrem Mittelpunkt steht der Begriff der „Auflösbarkeit" einer Gruppe, der aus der Betrachtung von Normalreihen und Kompositionsreihen abgeleitet wird, die auch für viele andere Untersuchungen grundlegend sind.

§ 20. Maximale Normalteiler, einfache Gruppen

Zu den angekündigten gruppentheoretischen Überlegungen benötigt man die folgenden Begriffsbildungen:

Definition **D (20.1)**

Ein echter Normalteiler $\mathfrak{M}$ *einer Gruppe* $\mathfrak{G}$ *heißt maximaler Normalteiler von* $\mathfrak{G}$, *wenn für jeden Normalteiler* $\mathfrak{N}$ *von* $\mathfrak{G}$ *mit* $\mathfrak{M} \subseteqq \mathfrak{N} \subseteqq \mathfrak{G}$ *entweder* $\mathfrak{M} = \mathfrak{N}$ *oder* $\mathfrak{N} = \mathfrak{G}$ *gilt.*

Ein Normalteiler $\mathfrak{M} < \mathfrak{G}$ wird also maximal genannt, wenn in $\mathfrak{G}$ kein weiterer Normalteiler $\mathfrak{N}$ mit $\mathfrak{M} < \mathfrak{N} < \mathfrak{G}$ existiert. So ist etwa die alternierende Gruppe $\mathfrak{A}_4$ maximaler Normalteiler der symmetrischen Gruppe $\mathfrak{S}_4$, die KLEINsche Vierergruppe ein solcher von $\mathfrak{A}_4$, nicht aber von $\mathfrak{S}_4$.

Man beachte, daß eine Gruppe mehrere maximale Normalteiler haben kann, so etwa die Gruppe $\langle (13), (14)(23) \rangle$ die drei Untergruppen der Ordnung 4.

Definition **D (20.2)**

Eine Gruppe $\mathfrak{G}$ heißt einfach, wenn sie nur die trivialen Normalteiler $\mathfrak{E}$ und $\mathfrak{G}$ besitzt[1]).

Naheliegende Beispiele für einfache Gruppen sind die zyklischen Gruppen von Primzahlordnung, da sie nach dem Satz von LAGRANGE (S (7.7)) nur die trivialen Untergruppen $\mathfrak{E}$ und $\mathfrak{Z}_p$ enthalten (vgl. auch S (20.6)). Ferner haben wir bereits in § 17 erwähnt, daß für $n \geqq 5$ die alternierende Gruppe $\mathfrak{A}_n$ nur die trivialen Normalteiler besitzt, also einfach ist. Wir werden diese bedeutsame Aussage am Ende dieses Paragraphen beweisen.

Den Zusammenhang zwischen den eben erklärten Begriffen vermittelt der

Satz **S (20.3)**

Die Faktorgruppe $\mathfrak{G}/\mathfrak{M}$ ist genau dann einfach und verschieden von der Einheitsgruppe, wenn $\mathfrak{M}$ ein maximaler Normalteiler von $\mathfrak{G}$ ist.

Beweis

Zunächst folgt aus $\mathfrak{M} < \mathfrak{G}$ offensichtlich $\mathfrak{G}/\mathfrak{M} \neq \mathfrak{E}$ und umgekehrt. Weiterhin erhält man nach S (19.6) sämtliche Normalteiler von $\mathfrak{G}/\mathfrak{M}$ als die homomorphen Bilder derjenigen Normalteiler $\mathfrak{N}$ von $\mathfrak{G}$, die $\mathfrak{M}$ umfassen. Aus der Maximalität von $\mathfrak{M}$ folgt, daß für $\mathfrak{N}$ nur $\mathfrak{M}$ und $\mathfrak{G}$ in Frage kommen, also $\mathfrak{G}/\mathfrak{M}$ nur sich selbst und die Einheitsgruppe als Normalteiler enthält. Ist umgekehrt letzteres der Fall, so gibt es in $\mathfrak{G}$ außer $\mathfrak{G}$ und $\mathfrak{M}$ keine Normalteiler, die $\mathfrak{M}$ umfassen.

qed.

Als nächstes zeigen wir einen Satz über das Komplexprodukt zweier maximaler Normalteiler, der zu einer oft nützlichen Isomorphieaussage führt:

Satz **S (20.4)**

Für das Produkt zweier verschiedener maximaler Normalteiler $\mathfrak{M}_1$ und $\mathfrak{M}_2$ von $\mathfrak{G}$ gilt $\mathfrak{M}_1 \mathfrak{M}_2 = \mathfrak{G}$.

1) Wir bemerken, daß für abelsche Gruppen jede Untergruppe Normalteiler ist und demzufolge eine einfache abelsche Gruppe nur sich selbst und die Einheitsgruppe als Untergruppe hat.

Beweis

$\mathfrak{M}_1\mathfrak{M}_2$ ist nach S(17.6) Normalteiler von $\mathfrak{G}$ und enthält offensichtlich sowohl $\mathfrak{M}_1$ als auch $\mathfrak{M}_2$. Wäre $\mathfrak{M}_1\mathfrak{M}_2$ verschieden von $\mathfrak{G}$, so müßte es sowohl gleich $\mathfrak{M}_1$ (wegen der Maximalität von $\mathfrak{M}_1$) als auch gleich $\mathfrak{M}_2$ (wegen der Maximalität von $\mathfrak{M}_2$) sein im Widerspruch zu $\mathfrak{M}_1 \neq \mathfrak{M}_2$. qed.

Damit erhält man aus dem 1. Isomorphiesatz (S(19.5)):

Folgerung **F(20.5)**

Sind $\mathfrak{M}_1$ und $\mathfrak{M}_2$ verschiedene maximale Normalteiler von $\mathfrak{G}$, so gilt:

$$\mathfrak{G}/\mathfrak{M}_1 \xleftarrow{\sim} \mathfrak{M}_2/\mathfrak{M}_1 \cap \mathfrak{M}_2).$$

Abschließend gehen wir auf die bereits als Beispiel erwähnten einfachen Gruppen näher ein:

Satz **S(20.6)**

Die Einheitsgruppe und die (zyklischen) Gruppen von Primzahlordnung sind die einzigen abelschen Gruppen, die einfach sind.

Beweis

Nach dem Vorausgegangenen bleibt nur zu zeigen, daß jede einfache abelsche Gruppe von der angegebenen Art ist. Jedenfalls ist eine zyklische Gruppe nach S(6.12) nur dann einfach, wenn sie von endlicher Ordnung n und n gleich 1 oder eine Primzahl ist. Eine nichtzyklische abelsche Gruppe enthält aber stets eine nichttriviale zyklische Untergruppe, ist also nicht einfach. qed.

Satz **S(20.7)**

Die alternierende Gruppe $\mathfrak{A}_n$ ist für $n \geqq 5$ einfach[1]).

Beweis

a) Wir zeigen zunächst, daß ein von der Einheitsgruppe verschiedener Normalteiler $\mathfrak{N}$ von $\mathfrak{A}_n$ wenigstens einen dreigliedrigen Zyklus $(a\,b\,c)$ enthält. Hier wie im folgenden bedeuten dabei $a, b, c, \ldots$ Zahlen aus der Reihe $1, 2, \ldots, n$. Nach Voraussetzung enthält $\mathfrak{N}$

1) Der folgende Beweis gilt ohne jede Änderung auch für die abzählbare alternierende Gruppe $\mathfrak{A}_\rho$.

eine Permutation $s \neq (1)$, die wir in ihre Hauptproduktdarstellung zerlegen. Nach der Länge der auftretenden Zyklen führen wir Fallunterscheidungen durch.

1. $s \in \mathfrak{N}$ enthalte wenigstens einen Zyklus mit mindestens vier Elementen:

$$s = (abcd \ldots) \ldots .$$

Transformiert man s mit der in $\mathfrak{A}_n$ liegenden Permutation $s_0 = (bcd)$, so erhält man die in $\mathfrak{A}_n$ zu s konjugierte Permutation

$$s' = s_0^{-1} s s_0 = (acdb \ldots) \ldots ,$$

die also nach S(17.2c) in dem Normalteiler $\mathfrak{N}$ liegt. Das Produkt

$$s' s^{-1} = (acdb \ldots)(\ldots dcba) = (abd)$$

liefert bereits einen in $\mathfrak{N}$ enthaltenen dreigliedrigen Zyklus.

2. $s \in \mathfrak{N}$ bestehe nur aus zwei- und dreigliedrigen Zyklen, wobei zunächst wirklich zweigliedrige Zyklen vorkommen sollen. Da s gerade ist, müssen diese paarweise auftreten, d. h., s ist von der Form:

$$s = (ab)(cd) \ldots .$$

Entsprechend den Überlegungen unter 1. transformieren wir s mit $s_0 = (abc)$ und erhalten als weitere Permutation von $\mathfrak{N}$

$$s' = s_0^{-1} s s_0 = (bc)(ad) \ldots .$$

Damit liegt auch

$$s'' = s' s^{-1} = (bc)(ad) \ldots \ldots (dc)(ba) = (bd)(ac)$$

in $\mathfrak{N}$. Da nach Voraussetzung $n \geqq 5$ ist, existiert ein von a, b, c, d verschiedenes Element e und damit in $\mathfrak{A}_n$ die Permutation $s_1 = (ace)$. Nochmalige Transformation liefert:

$$s''' = s_1^{-1} s'' s_1 = (bd)(ce) \in \mathfrak{N},$$

und damit ergibt sich

$$s'' s''' = (bd)(ac)(bd)(ce) = (aec) \in \mathfrak{N}.$$

3. Es bleibt als letztes der Fall, daß alle Faktoren von $s \in \mathfrak{N}$ dreigliedrige Zyklen sind:

$$s = (abc)(def) \ldots .$$

Wir transformieren wieder mit $s_0 = (cde)$ und erhalten

$$s' = s_0^{-1} s s_0 = (abd)(ecf) \ldots \in \mathfrak{N}.$$

Das Produkt

$$s' s^{-1} = (abd)\,(ecf) \ldots\ldots (fed)\,(cba) = (bfdce)$$

ist aber ein in $\mathfrak{N}$ enthaltener fünfgliedriger Zyklus, womit wir diesen letzten Fall auf den ersten zurückgeführt haben.

b) Nunmehr können wir den Beweis rasch zu Ende führen, indem wir zeigen, daß für $n \geqq 5$ jeder Normalteiler $\mathfrak{N}$ von $\mathfrak{A}_n$, der einen dreigliedrigen Zyklus $s = (abc)$ enthält, jeden dreigliedrigen Zyklus (xyz) enthält und somit nach S(11.6) mit $\mathfrak{A}_n$ zusammenfällt. Dazu betrachten wir die beiden in $\mathfrak{S}_n$ sicher vorhandenen Permutationen

$$s_0 = \begin{pmatrix} a\,b\,c\,d\,e\ldots \\ x\,y\,z\,u\,v\ldots \end{pmatrix}, \qquad s_1 = \begin{pmatrix} a\,b\,c\,d\,e\ldots \\ x\,y\,z\,v\,u\ldots \end{pmatrix}.$$

Sie gehen auseinander durch Multiplikation mit der Transposition (uv) hervor, haben also verschiedene Vorzeichen. Daher liegt eine von ihnen, etwa s_0, in $\mathfrak{A}_n$. Die Transformation von s mit s_0 ergibt schon den verlangten dreigliedrigen Zyklus

$$s_0^{-1} s s_0 = (xyz) \in \mathfrak{N}.$$ qed.

Folgerung **F (20.8)**

Die symmetrische Gruppe $\mathfrak{S}_n$ hat für $n \geqq 5$ genau die Normalteiler $\mathfrak{S}_n$, $\mathfrak{A}_n$ und $\mathfrak{E}$.

Beweis

Es sei $\mathfrak{N}$ ein Normalteiler von $\mathfrak{S}_n$ mit $\mathfrak{S}_n > \mathfrak{N} > \mathfrak{E}$. Dann ist auch $\mathfrak{N}^* = \mathfrak{N} \wedge \mathfrak{A}_n$ Normalteiler von $\mathfrak{S}_n$ (vgl. S(17.5)) und damit erst recht von $\mathfrak{A}_n$ (vgl. S(17.4)). Also folgt nach S(20.7) $\mathfrak{N}^* = \mathfrak{A}_n$ oder $\mathfrak{N}^* = \mathfrak{E}$. Im ersten Falle erhalten wir $\mathfrak{N} \geqq \mathfrak{A}_n$, also $\mathfrak{N} = \mathfrak{A}_n$ (vgl. S(11.3)). Der zweite Fall ist unmöglich, da dann $\mathfrak{N}$ (wiederum nach S(11.3)) nur aus der identischen Permutation und einer weiteren ungeraden Permutation u bestehen würde; zufolge der Normalteilereigenschaft von $\mathfrak{N}$ müßte $s^{-1} u s = u$, d. h. $us = su$ für alle $s \in \mathfrak{S}_n$ gelten im Widerspruch dazu, daß das Zentrum von $\mathfrak{S}_n$ die Einheitsgruppe ist (vgl. Aufg. 8 von § 16). qed.

Aufgaben zu § 20

1. Jeder Normalteiler $\mathfrak{N}$ von $\mathfrak{G}$, dessen Index $(\mathfrak{G}\colon \mathfrak{N})$ eine Primzahl ist, ist maximal.
2. Man veranschauliche sich S(20.4) und F(20.5) am Beispiele der Gruppe
$$\mathfrak{G} = \langle (13),\ (14)(23) \rangle.$$

§ 21. Normalreihen und Kompositionsreihen

Reihen einander enthaltender Untergruppen werden bei den verschiedensten gruppentheoretischen Überlegungen herangezogen. Für den hier auszuwählenden Teil dieser Betrachtungen ist es am zweckmäßigsten, den Begriff der Normalreihe zugrunde zu legen.

Definition **D (21.1)**

Unter einer Normalreihe einer Gruppe $\mathfrak{G}$ nach einem Normalteiler $\mathfrak{N}$ von $\mathfrak{G}$ versteht man eine endliche Reihe von Untergruppen

$$\mathfrak{G} = \mathfrak{G}_0 \supseteq \mathfrak{G}_1 \supseteq \ldots \supseteq \mathfrak{G}_l = \mathfrak{N},$$

in der jede Untergruppe $\mathfrak{G}_\nu$ Normalteiler der vorangehenden Untergruppe $\mathfrak{G}_{\nu-1}$ ist. Die Faktorgruppen $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ heißen die Faktoren der Normalreihe, deren Anzahl l man die Länge der Normalreihe nennt.

Insbesondere spricht man schlechthin von einer Normalreihe von $\mathfrak{G}$, wenn $\mathfrak{N}$ gleich der Einheitsgruppe $\mathfrak{E}$ ist:

$$\mathfrak{G} = \mathfrak{G}_0 \supseteq \mathfrak{G}_1 \supseteq \ldots \supseteq \mathfrak{G}_l = \mathfrak{E}.$$

Man beachte dabei, daß von jeder der Untergruppen $\mathfrak{G}_\nu$ nur die Normalteilereigenschaft bezüglich der vorangehenden Untergruppe $\mathfrak{G}_{\nu-1}$, nicht aber bezüglich der ganzen Gruppe $\mathfrak{G}$ gefordert wird. Desgleichen ist zu bemerken, daß eine Normalreihe ein Glied mehr hat, als ihre Länge angibt.

So hat z. B. die Normalreihe von $\mathfrak{S}_4$

$$\mathfrak{S}_4 \supseteq \mathfrak{B}_4 \supseteq \langle (12)(34) \rangle \supseteq \mathfrak{E}$$

vier Glieder, während ihre Länge gemäß der Anzahl der Faktoren

$$\mathfrak{S}_4/\mathfrak{B}_4, \quad \mathfrak{B}_4/\langle (12)(34) \rangle, \quad \langle (12)(34) \rangle/\mathfrak{E}$$

gleich $l = 3$ ist. Weiterhin ist $\langle (12)(34) \rangle$ wohl Normalteiler in $\mathfrak{B}_4$, aber nicht in $\mathfrak{S}_4$. Natürlich hätte man auch als eine Normalreihe von $\mathfrak{S}_4$ angeben können

$$\mathfrak{S}_4 \supseteq \mathfrak{A}_4 \supseteq \mathfrak{B}_4 \supseteq \langle (12)(34) \rangle \supseteq \mathfrak{E}$$

oder auch

$$\mathfrak{S}_4 \supseteq \mathfrak{A}_4 \supseteq \mathfrak{A}_4 \supseteq \mathfrak{B}_4 \supseteq \langle (12)(34) \rangle \supseteq \mathfrak{E}.$$

Allgemein nennt man die durch Hinzufügen weiterer Glieder entstehende Normalreihe eine *Verfeinerung* der ursprünglichen Normalreihe und unterscheidet gemäß obigen Beispielen *Normalreihen ohne Wiederholungen* und *Normalreihen mit Wiederholungen.*

Ferner kann man mit Hilfe der Isomorphie der Faktoren einen Isomorphiebegriff für Normalreihen einführen:

Definition **D (21.2)**

Zwei Normalreihen heißen isomorph, in Zeichen

$$[\mathfrak{G}_0 \geqq \mathfrak{G}_1 \geqq \cdots \geqq \mathfrak{G}_l] \overset{\sim}{\longleftrightarrow} [\mathfrak{H}_0 \geqq \mathfrak{H}_1 \geqq \cdots \geqq \mathfrak{H}_l],$$

wenn die Faktoren $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ der einen Reihe zu den Faktoren $\mathfrak{H}_{\mu-1}/\mathfrak{H}_\mu$ der anderen Reihe in einer geeigneten Reihenfolge isomorph sind.

So sind z. B. die beiden folgenden Normalreihen der zyklischen Gruppe $\mathfrak{Z}_{36}$ zueinander isomorph:

$$[\mathfrak{Z}_{36} \geqq \mathfrak{Z}_{18} \geqq \mathfrak{Z}_3 \geqq \mathfrak{E}] \overset{\sim}{\longleftrightarrow} [\mathfrak{Z}_{36} \geqq \mathfrak{Z}_{12} \geqq \mathfrak{Z}_4 \geqq \mathfrak{E}].$$

Es gelten nämlich zwischen den Faktoren die Isomorphien

$$\mathfrak{Z}_{36}/\mathfrak{Z}_{18} \overset{\sim}{\longleftrightarrow} \mathfrak{Z}_{12}/\mathfrak{Z}_6$$
$$\mathfrak{Z}_{18}/\mathfrak{Z}_3 \overset{\sim}{\longleftrightarrow} \mathfrak{Z}_6/\mathfrak{E}$$
$$\mathfrak{Z}_3/\mathfrak{E} \overset{\sim}{\longleftrightarrow} \mathfrak{Z}_{36}/\mathfrak{Z}_{12}.$$

Wir bemerken noch, daß man von zwei isomorphen Normalreihen mit Wiederholungen offenbar durch Streichen der überflüssigen Glieder zu zwei Normalreihen ohne Wiederholungen übergehen kann, ohne die Isomorphie zu zerstören.

Die entscheidende Bedeutung dieser Begriffsbildungen liegt nun in der zuerst von O. SCHREIER[1]) in dieser allgemeinen Form ausgesprochenen Tatsache, daß zwei beliebige Normalreihen einer Gruppe $\mathfrak{G}$ nach einem Normalteiler $\mathfrak{N}$ stets zu zwei isomorphen Normalreihen von $\mathfrak{G}$ nach $\mathfrak{N}$ verfeinert werden können.

Der Beweis dieses Strukturs atzes ist ein wesentliches Ziel des vorliegenden Paragraphen. Dabei zeigen wir zunächst, daß man die zwar auch im folgenden als Hilfsmittel benötigten Normalreihen nach einem Normalteiler stets wieder durch Normalreihen schlechthin ersetzen kann.

1) OTTO SCHREIER, 1901 bis 1929.

Satz **S (21.3)**

Jede Normalreihe von $\mathfrak{G}$ nach einem Normalteiler $\mathfrak{N}$ ist isomorph zu einer Normalreihe schlechthin:

$$[\mathfrak{G} \supseteq \mathfrak{G}_1 \supseteq \ldots \supseteq \mathfrak{G}_l = \mathfrak{N}] \longleftrightarrow [\mathfrak{G}/\mathfrak{N} \supseteq \mathfrak{G}_1/\mathfrak{N} \supseteq \ldots \supseteq \mathfrak{N}/\mathfrak{N} = \mathfrak{E}]$$

Beweis

Wir bemerken zunächst, daß nach S (17.4) $\mathfrak{N}$ als Normalteiler von $\mathfrak{G}$ erst recht Normalteiler von jedem $\mathfrak{G}_\nu$ ist und daß entsprechend unseren Überlegungen über den natürlichen Homomorphismus im Anschluß an S (19.6) die entstehenden Faktorgruppen in der Tat ineinander enthalten sind. Insbesondere ist nach S (19.6) $\mathfrak{G}_\nu/\mathfrak{N}$ Normalteiler von $\mathfrak{G}_{\nu-1}/\mathfrak{N}$.

Die Isomorphie der so konstruierten Normalreihe zu der vorgegebenen lehrt der 2. Isomorphiesatz (S (19.8)), dem zufolge die Faktoren beider Reihen paarweise zueinander isomorph sind:

$$\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu \longleftrightarrow (\mathfrak{G}_{\nu-1}/\mathfrak{N})\,/\,(\mathfrak{G}_\nu/\mathfrak{N}).$$

qed.

Als Beispiel betrachten wir die Normalreihe

$$\mathfrak{S}_4 \supseteq \mathfrak{A}_4 \supseteq \mathfrak{B}_4,$$

die zu der Normalreihe

$$\mathfrak{S}_4/\mathfrak{B}_4 \supseteq \mathfrak{A}_4/\mathfrak{B}_4 \supseteq \mathfrak{B}_4/\mathfrak{B}_4,$$

d. h. zu

$$\mathfrak{S}_3 \supseteq \mathfrak{A}_3 \supseteq \mathfrak{E}$$

isomorph ist.

Zur Vorbereitung des Hauptsatzes von O. SCHREIER benötigen wir noch den

Satz **S (21.4)**

Liegen zwei isomorphe Normalreihen vor

$$[\mathfrak{G} = \mathfrak{G}_0 \supseteq \mathfrak{G}_1 \supseteq \ldots \supseteq \mathfrak{G}_l = \mathfrak{E}] \longleftrightarrow [\mathfrak{H} = \mathfrak{H}_0 \supseteq \mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{H}_l = \mathfrak{E}],$$

so kann man zu jeder Verfeinerung der einen eine isomorphe Verfeinerung der anderen angeben.

Beweis

Jede Verfeinerung der ersten Reihe entsteht durch sukzessives Einschalten eines weiteren Gliedes $\mathfrak{G}^*$, etwa zwischen $\mathfrak{G}_{\nu-1}$ und

$\mathfrak{G}_\nu$. Die so entstehende Normalreihe $\mathfrak{G}_{\nu-1} \supseteq \mathfrak{G}^* \supseteq \mathfrak{G}_\nu$ von $\mathfrak{G}_{\nu-1}$ nach $\mathfrak{G}_\nu$ ist gemäß S(21.3) isomorph zur Normalreihe

$$(*) \qquad \mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu \supseteq \mathfrak{G}^*/\mathfrak{G}_\nu \supseteq \mathfrak{G}_\nu/\mathfrak{G}_\nu = \mathfrak{E}.$$

Nun existiert nach Voraussetzung zu dem Faktor $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ der ersten Reihe ein geeigneter Faktor $\mathfrak{H}_{\mu-1}/\mathfrak{H}_\mu$ der zweiten Reihe mit

$$\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu \overset{\sim}{\longleftrightarrow} \mathfrak{H}_{\mu-1}/\mathfrak{H}_\mu .$$

Die bei dieser Isomorphie den Untergruppen $\mathfrak{G}^*/\mathfrak{G}_\nu$ und $\mathfrak{G}_\nu/\mathfrak{G}_\nu = \mathfrak{E}$ von $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ entsprechenden Untergruppen von $\mathfrak{H}_{\mu-1}/\mathfrak{H}_\mu$ bestehen aus vollständigen Nebenklassen von $\mathfrak{H}_{\mu-1}$ nach $\mathfrak{H}_\mu$ und sind damit selbst Faktorgruppen ihrer vollständigen Originale $\mathfrak{H}^*$ und $\mathfrak{H}_\mu$ (beim natürlichen Homomorphismus $\mathfrak{H}_{\mu-1} \overset{\sim}{\longrightarrow} \mathfrak{H}_{\mu-1}/\mathfrak{H}_\mu$). Da sich bei der Isomorphie auch Normalteilereigenschaften übertragen, erhalten wir eine zu (*) isomorphe Normalreihe

$$\mathfrak{H}_{\mu-1}/\mathfrak{H}_\mu \supseteq \mathfrak{H}^*/\mathfrak{H}_\mu \supseteq \mathfrak{H}_\mu/\mathfrak{H}_\mu = \mathfrak{E},$$

die wiederum nach S(21.3) isomorph ist zu der Normalreihe

$$\mathfrak{H}_{\mu-1} \supseteq \mathfrak{H}^* \supseteq \mathfrak{H}_\mu$$

von $\mathfrak{H}_{\mu-1}$ nach $\mathfrak{H}_\mu$. Das Einsetzen dieser Teilreihe ergibt eine zu der Verfeinerung der ersten Reihe isomorphe Verfeinerung der zweiten Reihe.

qed.

Hauptsatz über Normalreihen von O. SCHREIER **S (21.5)**

Zwei beliebige Normalreihen einer Gruppe $\mathfrak{G}$

$$\mathfrak{G} \supseteq \mathfrak{G}_1 \supseteq \mathfrak{G}_2 \supseteq \ldots \supseteq \mathfrak{G}_l = \mathfrak{E}, \quad \mathfrak{G} \supseteq \mathfrak{H}_1 \supseteq \mathfrak{H}_2 \supseteq \ldots \supseteq \mathfrak{H}_k = \mathfrak{E}$$

besitzen stets isomorphe Verfeinerungen:

$$[\mathfrak{G} \supseteq \ldots \supseteq \mathfrak{G}_1 \supseteq \ldots \supseteq \mathfrak{G}_2 \supseteq \ldots\ldots \supseteq \mathfrak{E}]$$
$$\overset{\sim}{\longleftrightarrow} [\mathfrak{G} \supseteq \ldots \supseteq \mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{H}_2 \supseteq \ldots\ldots \supseteq \mathfrak{E}].$$

Beweis

a) *Die Behauptung gilt für* $k = 1$, *l beliebig.*

In diesem Falle ist nämlich die zweite Reihe von der Form

$$\mathfrak{G} \supseteq \mathfrak{E}$$

und damit die erste Reihe selbst die gesuchte Verfeinerung der zweiten Reihe.

b) *Beweis für $k = 2$, l beliebig (durch vollständige Induktion nach l).*

Die Richtigkeit für $k = 2$, $l = 1$ (Induktionsanfang) ist entsprechend a) unmittelbar klar. Wir nehmen also an, daß die Behauptung für $l - 1$ richtig ist und zeigen ihre Gültigkeit für l. Die beiden Gruppen

$$\mathfrak{D} = \mathfrak{G}_1 \cap \mathfrak{H}_1, \quad \mathfrak{P} = \mathfrak{G}_1 \mathfrak{H}_1$$

sind nach S(17.5) bzw. S(17.6) Normalteiler von $\mathfrak{G}$. Weiterhin folgt nach S(17.4) die Normalteilereigenschaft von $\mathfrak{D}$ in $\mathfrak{G}_1$ und $\mathfrak{H}_1$ sowie von $\mathfrak{G}_1$ und $\mathfrak{H}_1$ in $\mathfrak{P}$. Dies werden wir benutzen, um weitere Normalreihen aufzustellen, deren geschickte Kombination die Behauptung ergeben wird. So können wir zunächst nach Induktionsvoraussetzung zu den beiden Normalreihen von den Längen $l - 1$ und 2

$$\mathfrak{G}_1 \supseteq \mathfrak{G}_2 \supseteq \ldots \supseteq \mathfrak{G}_l = \mathfrak{E}, \qquad \mathfrak{G}_1 \supseteq \mathfrak{D} \supseteq \mathfrak{E}$$

isomorphe Verfeinerungen finden:

$$(*) \quad [\mathfrak{G}_1 \supseteq \ldots \supseteq \mathfrak{G}_2 \supseteq \ldots \ldots \supseteq \mathfrak{E}] \overset{\sim}{\longleftrightarrow} [\mathfrak{G}_1 \supseteq \ldots \supseteq \mathfrak{D} \supseteq \ldots \supseteq \mathfrak{E}].$$

Weiterhin sind die beiden folgenden Normalreihen zueinander isomorph:

$$(**) \qquad [\mathfrak{P} \supseteq \mathfrak{G}_1 \supseteq \mathfrak{D} \supseteq \mathfrak{E}] \overset{\sim}{\longleftrightarrow} [\mathfrak{P} \supseteq \mathfrak{H}_1 \supseteq \mathfrak{D} \supseteq \mathfrak{E}];$$

der Faktor $\mathfrak{D}/\mathfrak{E}$ tritt nämlich in beiden auf, während die anderen Faktoren nach dem 1. Isomorphiesatz isomorph sind:

$$\mathfrak{P}/\mathfrak{G}_1 \overset{\sim}{\longleftrightarrow} \mathfrak{H}_1/\mathfrak{D}, \quad \mathfrak{P}/\mathfrak{H}_1 \overset{\sim}{\longleftrightarrow} \mathfrak{G}_1/\mathfrak{D}.$$

Die rechte Seite von (*) ergibt eine Verfeinerung der linken Seite von (**), zu der nach S(21.4) eine isomorphe Verfeinerung der rechten Seite von (**) existiert:

$$[\mathfrak{P} \supseteq \mathfrak{G}_1 \supseteq \quad \supseteq \mathfrak{D} \supseteq \ldots \supseteq \mathfrak{E}]$$
$$\overset{\sim}{\longleftrightarrow} [\mathfrak{P} \supseteq \ldots \supseteq \mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{D} \supseteq \ldots \supseteq \mathfrak{E}].$$

Berücksichtigt man hier links die Isomorphie (*), so folgt

$$[\mathfrak{P} \supseteq \mathfrak{G}_1 \supseteq \ldots \supseteq \mathfrak{G}_2 \supseteq \ldots \ldots \supseteq \mathfrak{E}]$$
$$\overset{\sim}{\longleftrightarrow} [\mathfrak{P} \supseteq \ldots \supseteq \mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{D} \supseteq \ldots \supseteq \mathfrak{E}].$$

Daraus erhalten wir aber die verlangten isomorphen Verfeinerungen der ursprünglichen Normalreihen:

$$[\mathfrak{G} \supseteq \mathfrak{P} \supseteq \mathfrak{G}_1 \supseteq \ldots \supseteq \mathfrak{G}_2 \supseteq \ldots \ldots \supseteq \mathfrak{E}]$$
$$\overset{\sim}{\longleftrightarrow} [\mathfrak{G} \supseteq \mathfrak{P} \supseteq \ldots \supseteq \mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{D} \supseteq \ldots \supseteq \mathfrak{E}].$$

c) *Beweis für k beliebig, l beliebig (durch vollständige Induktion nach k).*

Wir benutzen das unter b) Gezeigte als Induktionsanfang und nehmen die Richtigkeit unserer Behauptung für $k-1$ an. Zunächst bilden wir aus den drei Gliedern $\mathfrak{G}$, $\mathfrak{H}_1$ und $\mathfrak{E}$ der zweiten Reihe die Normalreihe $\mathfrak{G} \supseteq \mathfrak{H}_1 \supseteq \mathfrak{E}$. Diese Reihe und die erste Normalreihe haben nach b) isomorphe Verfeinerungen:

$$(*)\ [\mathfrak{G} \supseteq \ldots \supseteq \mathfrak{G}_1 \supseteq \ldots \ldots \supseteq \mathfrak{E}] \overset{\sim}{\longleftrightarrow} [\mathfrak{G} \supseteq \ldots \supseteq \mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{E}].$$

Nunmehr wenden wir die Induktionsvoraussetzung auf die Teilreihe $\mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{E}$ auf der rechten Seite von (*) und auf die Teilreihe $\mathfrak{H}_1 \supseteq \mathfrak{H}_2 \supseteq \ldots \supseteq \mathfrak{H}_k = \mathfrak{E}$ der Länge $k-1$ an. Danach existieren für diese beiden Reihen isomorphe Verfeinerungen:

$$(**)\quad [\mathfrak{H}_1 \supseteq \ldots\ldots \supseteq \mathfrak{E}] \overset{\sim}{\longleftrightarrow} [\mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{H}_2 \supseteq \ldots\ldots \supseteq \mathfrak{E}].$$

Die linke Seite von (**) ergibt eine Verfeinerung der rechten Seite von (*), zu der nach S(21.4) eine isomorphe Verfeinerung der linken Seite von (*) existiert:

$$[\mathfrak{G} \supseteq \ldots\ldots \supseteq \mathfrak{G}_1 \supseteq \ldots\ldots\ldots \supseteq \mathfrak{E}] \overset{\sim}{\longleftrightarrow} [\mathfrak{G} \supseteq \ldots \supseteq \mathfrak{H}_1 \supseteq \ldots\ldots\ldots \supseteq \mathfrak{E}].$$

Ersetzen wir hier schließlich noch auf der rechten Seite die Teilreihe $\mathfrak{H}_1 \supseteq \ldots \ldots \supseteq \mathfrak{E}$ durch die zu ihr nach (**) isomorphe Reihe $\mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{H}_2 \supseteq \ldots\ldots \supseteq \mathfrak{E}$, so erhalten wir die behaupteten Verfeinerungen der ursprünglichen Normalreihen:

$$[\mathfrak{G} \supseteq \ldots\ldots \supseteq \mathfrak{G}_1 \supseteq \ldots\ldots\ldots \supseteq \mathfrak{E}] \overset{\sim}{\longleftrightarrow} [\mathfrak{G} \supseteq \ldots \supseteq \mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{H}_2 \supseteq \ldots\ldots \supseteq \mathfrak{E}].$$

qed.

Wir wenden dieses Ergebnis insbesondere auf solche Normalreihen an, die keiner Verfeinerung mehr fähig sind:

Definition **D (21.6)**

Unter einer Kompositionsreihe einer Gruppe $\mathfrak{G}$ versteht man eine Normalreihe ohne Wiederholungen, die sich nicht mehr verfeinern läßt, ohne daß dabei Wiederholungen auftreten. Die Faktoren einer Kompositionsreihe heißen Kompositionsfaktoren.

Aus der Eigenschaft des maximalen Normalteilers und S (20.3) ergibt sich unmittelbar:

Folgerung **F (21.7)**

Eine Normalreihe (ohne Wiederholungen) einer Gruppe $\mathfrak{G}$

$$\mathfrak{G} = \mathfrak{G}_0 > \mathfrak{G}_1 > \ldots > \mathfrak{G}_l = \mathfrak{E}$$

ist genau dann Kompositionsreihe, wenn jedes $\mathfrak{G}_\nu$ *maximaler Normalteiler von* $\mathfrak{G}_{\nu-1}$ *ist, d. h., wenn die Faktoren* $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ *einfache Gruppen sind.*

Beispiele:

Die Gruppen $\mathfrak{S}_2$ und $\mathfrak{S}_3$ haben nur je eine Kompositionsreihe:

$$\mathfrak{S}_2 > \mathfrak{E}; \quad \mathfrak{S}_3 > \mathfrak{A}_3 > \mathfrak{E}.$$

Die Gruppe $\mathfrak{S}_4$ hat die drei Kompositionsreihen:

$$\mathfrak{S}_4 > \mathfrak{A}_4 > \mathfrak{B}_4 > \mathfrak{Z}_2 > \mathfrak{E},$$

wobei für $\mathfrak{Z}_2$ jeweils eine der drei Untergruppen von $\mathfrak{B}_4$ zu setzen ist.

Die Gruppe $\mathfrak{S}_n$ mit $n \geqq 5$ hat dagegen nach S (20.7) nur die Kompositionsreihe [1])

$$\mathfrak{S}_n > \mathfrak{A}_n > \mathfrak{E}.$$

Die zyklische Gruppe der Ordnung 12 hat die folgenden Kompositionsreihen:

$$\mathfrak{Z}_{12} > \mathfrak{Z}_6 > \mathfrak{Z}_3 > \mathfrak{E}$$
$$\mathfrak{Z}_{12} > \mathfrak{Z}_6 > \mathfrak{Z}_2 > \mathfrak{E}$$
$$\mathfrak{Z}_{12} > \mathfrak{Z}_4 > \mathfrak{Z}_2 > \mathfrak{E}.$$

Offensichtlich hat jede endliche Gruppe wenigstens eine Kompositionsreihe. Dagegen gibt es unendliche Gruppen, die überhaupt keine Kompositionsreihe besitzen, wie z. B. die unendliche zyklische Gruppe (vgl. Aufg. 3).

---

1) Entsprechend hat die abzählbare symmetrische Gruppe $\mathfrak{S}_\alpha$ die Kompositionsreihe $\mathfrak{S}_\alpha > \mathfrak{A}_\alpha > \mathfrak{E}$.

Liegen mehrere Kompositionsreihen einer Gruppe vor, so müßten sich diese nach dem Satz von O. SCHREIER zu isomorphen Normalreihen verfeinern lassen, und dies, gemäß unserer Bemerkung im Anschluß an D (21.2), sogar ohne Wiederholungen. Das ist aber bei Kompositionsreihen nicht mehr möglich, d. h., sie müssen von vornherein isomorph sein. Somit ergibt sich aus dem Satz von O. SCHREIER unmittelbar der

Satz von JORDAN-HÖLDER **S (21.8)**

Je zwei Kompositionsreihen einer Gruppe $\mathfrak{G}$ *sind isomorph.*

Man kann also bei einer Gruppe $\mathfrak{G}$, die überhaupt eine Kompositionsreihe besitzt, schlechthin von den Kompositionsfaktoren von $\mathfrak{G}$ sprechen. So sind z. B. die Kompositionsfaktoren der zyklischen Gruppe $\mathfrak{Z}_{12}$ der Struktur nach gegeben durch

$$\mathfrak{Z}_2, \mathfrak{Z}_2, \mathfrak{Z}_3$$

unabhängig davon, welche der drei Kompositionsreihen man betrachtet.

Weiterhin folgt sofort aus dem Satz von O. SCHREIER der

Satz **S (21.9)**

Wenn eine Gruppe $\mathfrak{G}$ *überhaupt eine Kompositionsreihe besitzt, so läßt sich jede (wiederholungsfreie) Normalreihe zu einer Kompositionsreihe verfeinern; insbesondere gibt es durch jeden Normalteiler von* $\mathfrak{G}$ *eine Kompositionsreihe.*

Aufgaben zu § 21

1. Als Beispiel zum Satz von O. SCHREIER stelle man zu den beiden Normalreihen der unendlichen zyklischen Gruppe $\langle a \rangle$

$$\langle a \rangle \supset \langle a^{12} \rangle \supset \langle a^{60} \rangle \supset \mathfrak{E}, \qquad \langle a \rangle \supset \langle a^{10} \rangle \supset \mathfrak{E}$$

isomorphe Verfeinerungen her.

2. Man lege durch die beiden Untergruppen $\mathfrak{Z}_8$ und $\mathfrak{Z}_6$ der zyklischen Gruppe $\mathfrak{Z}_{24}$ je eine Kompositionsreihe und gebe die zugehörigen Kompositionsfaktoren an.

3. Jede abelsche Gruppe, die eine Kompositionsreihe besitzt, ist endlich. Insbesondere besitzt also die unendliche zyklische Gruppe keine Kompositionsreihe.

§ 22. Auflösbare Gruppen

Wie wir später behandeln werden, kann man die Frage nach der Auflösbarkeit algebraischer Gleichungen (im Sinne der Angabe geschlossener Lösungsausdrücke, wie für die Gleichungen 3. Grades durch die Cardanoschen Formeln) zurückführen auf die Fragestellung, ob die Kompositionsreihen gewisser endlicher Gruppen Kompositionsfaktoren von Primzahlordnung besitzen.

Dies ist der Anlaß zu der folgenden Definition, die auch unendliche Gruppen einbegreift:

Definition **D (22.1)**

Eine Gruppe $\mathfrak{G}$ heißt auflösbar, wenn sie eine Normalreihe mit abelschen Faktoren besitzt.

Folgerung **F (22.2)**

In einer auflösbaren Gruppe $\mathfrak{G}$ läßt sich jede Normalreihe zu einer Normalreihe mit abelschen Faktoren verfeinern.

Beweis

Es sei $\mathfrak{G} = \mathfrak{H}_0 \supseteq \mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{H}_k = \mathfrak{E}$ eine beliebige Normalreihe von $\mathfrak{G}$ und $\mathfrak{G} = \mathfrak{G}_0 \supseteq \mathfrak{G}_1 \supseteq \ldots \supseteq \mathfrak{G}_l = \mathfrak{E}$ die nach D (22.1) existierende Normalreihe mit abelschen Faktoren. Nach dem Satz von O. SCHREIER besitzen beide Reihen isomorphe Verfeinerungen, womit unsere Behauptung darauf hinausläuft, daß jede Verfeinerung der zweiten Reihe wieder eine Normalreihe mit abelschen Faktoren liefert.

Schaltet man aber zwischen $\mathfrak{G}_{\nu-1}$ und $\mathfrak{G}_\nu$ ein Glied $\mathfrak{G}^*$ ein, so sind mit $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ auch $\mathfrak{G}_{\nu-1}/\mathfrak{G}^*$ und $\mathfrak{G}^*/\mathfrak{G}_\nu$ abelsche Gruppen. Für $\mathfrak{G}^*/\mathfrak{G}_\nu$ ist dies als Untergruppe von $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ klar; $\mathfrak{G}_{\nu-1}/\mathfrak{G}^*$ ist aber nach dem 2. Isomorphiesatz

$$(\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu)/(\mathfrak{G}^*/\mathfrak{G}_\nu) \xleftrightarrow{\sim} \mathfrak{G}_{\nu-1}/\mathfrak{G}^*$$

isomorph zur Faktorgruppe einer abelschen Gruppe, also ebenfalls abelsch.

qed.

Satz **S (22.3)**

Eine endliche Gruppe $\mathfrak{G} \neq \mathfrak{E}$ ist genau dann auflösbar, wenn die Kompositionsfaktoren von $\mathfrak{G}$ Primzahlordnung haben[1]).

Beweis

Die Bedingung ist offensichtlich hinreichend. Sie ist aber auch notwendig. Nach F (22.2) müssen nämlich auch die Faktoren der nicht mehr (wiederholungsfrei) zu verfeinernden Kompositionsreihen abelsch sein. Als einfache abelsche Gruppen sind die Kompositionsfaktoren aber gemäß S (20.6) von Primzahlordnung.

qed.

Beispiele:

Selbstverständlich sind alle abelschen Gruppen auflösbar. Ferner sind entsprechend den in § 21 angegebenen Kompositionsreihen die symmetrischen Gruppen $\mathfrak{S}_n$ für $n \leqq 4$ auflösbar, dagegen für $n \geqq 5$ nicht auflösbar.

Als Beispiel einer unendlichen auflösbaren Gruppe nennen wir die Gruppe $\mathfrak{O}$ aller orthogonalen Matrizen vom Typ (2,2) mit reellen Zahlen als Matrizenelementen. $\mathfrak{O}$ hat als Normalteiler die Gruppe $\mathfrak{O}_+$ aller orthogonalen Matrizen mit der Determinante 1, da nach Aufg. 5 von § 7 der Index $(\mathfrak{O}:\mathfrak{O}_+) = 2$ ist. $\mathfrak{O}_+$ ist als Gruppe aller Drehungen einer Ebene um einen festen Punkt eine abelsche Gruppe, also ist

$$\mathfrak{O} > \mathfrak{O}_+ > \mathfrak{E}$$

eine Normalreihe mit abelschen Faktoren.

Weiterhin sind alle Gruppen von Primzahlpotenzordnung auflösbar, was sich später für die Lösbarkeit geometrischer Konstruktionsaufgaben mit Zirkel und Lineal als bedeutungsvoll erweisen wird. Zum Beweis dieser Aussage benötigen wir

Satz **S (22.4)**

Enthält eine Gruppe $\mathfrak{G}$ einen auflösbaren Normalteiler $\mathfrak{N}$ mit auflösbarer Faktorgruppe $\mathfrak{G}/\mathfrak{N}$, so ist $\mathfrak{G}$ ebenfalls auflösbar.

---

1) Da eine Gruppe von Primzahlordnung zyklisch ist, nennt man die endlichen auflösbaren Gruppen teilweise auch *metazyklisch*.

Beweis

Nach Voraussetzung existieren sowohl für $\mathfrak{G}/\mathfrak{N}$ als auch für $\mathfrak{N}$ Normalreihen mit abelschen Faktoren:

$$\mathfrak{G}/\mathfrak{N} \supseteq \mathfrak{G}_1/\mathfrak{N} \supseteq \ldots \supseteq \mathfrak{N}/\mathfrak{N} \quad \text{bzw.} \quad \mathfrak{N} \supseteq \mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{E}.$$

Die erste dieser Reihen ist gemäß S(21.3) durch eine isomorphe Normalreihe von $\mathfrak{G}$ nach $\mathfrak{N}$ zu ersetzen, so daß man mit der zweiten Reihe zusammen eine Normalreihe von $\mathfrak{G}$ mit abelschen Faktoren erhält:

$$\mathfrak{G} \supseteq \mathfrak{G}_1 \supseteq \ldots \supseteq \mathfrak{N} \supseteq \mathfrak{H}_1 \supseteq \ldots \supseteq \mathfrak{E}.$$

qed.

Satz **S (22.5)**

Jede Gruppe $\mathfrak{G}$ von Primzahlpotenzordnung p^n ist auflösbar.

Beweis

a) Wir zeigen zunächst, daß eine Gruppe $\mathfrak{G}$ der Ordnung $p^n > 1$ ein von der Einheitsgruppe verschiedenes Zentrum $\mathfrak{Z}$ besitzt. Dazu benutzen wir, daß die mit allen Elementen von $\mathfrak{G}$ vertauschbaren Elemente von $\mathfrak{G}$ nur zu sich selbst konjugiert sind (vgl. Aufg. 7 von § 16), und zählen alle Elemente von $\mathfrak{G}$ ab, jeweils zusammengefaßt zu Klassen konjugierter Elemente.

Nun ist die Anzahl der Elemente einer solchen Klasse nach S(16.7) und S(16.2) stets ein echter Teiler der Gruppenordnung, also in unserem Falle eine der Zahlen

$$1, p, p^2, \ldots, p^{n-1}.$$

Wir bezeichnen mit a_i die Anzahl der Klassen, die aus p^i Elementen bestehen, und erhalten damit

$$p^n = a_0 \cdot 1 + a_1 \cdot p + a_2 \cdot p^2 + \ldots + a_{n-1} \cdot p^{n-1}.$$

Als Anzahl der Klassen, die nur aus einem Element bestehen, ist a_0 die gesuchte Ordnung des Zentrums $\mathfrak{Z}$ und natürlich $a_0 \neq 0$. Obige Gleichung lehrt $a_0 \equiv 0\ (p)$, also ist $a_0 \geqq p$ (vgl. als Beispiel die Gruppe $\langle (13), (14)(23) \rangle$ der Ordnung 2^3).

b) Die eigentliche Behauptung zeigen wir durch vollständige Induktion nach n. Für $n = 1$ ist sie klar; wir beweisen sie für einen beliebigen Exponenten n unter der Annahme ihrer Richtigkeit für alle kleineren Exponenten.

Dazu schalten wir das Zentrum $\mathfrak{Z}$ als Zwischengruppe ein, das nach a) nicht mit $\mathfrak{E}$ zusammenfällt:

$$\mathfrak{G} \supseteq \mathfrak{Z} > \mathfrak{E}.$$

Nun ist $\mathfrak{Z}$ Normalteiler in $\mathfrak{G}$ und als abelsche Gruppe auflösbar; desgleichen ist $\mathfrak{G}/\mathfrak{Z}$ nach Induktionsvoraussetzung auflösbar, denn die Ordnung von $\mathfrak{G}/\mathfrak{Z}$ ist als Index $(\mathfrak{G}:\mathfrak{Z})$ ein echter Teiler von p^n. Damit sind die Voraussetzungen von S (22.4) erfüllt, woraus unsere Behauptung folgt.

qed.

Abschließend zeigen wir, daß sich die Auflösbarkeit einer Gruppe sowohl auf ihre Untergruppen als auch auf ihre homomorphen Bilder überträgt.

Satz **S (22.6)**

Mit der Gruppe $\mathfrak{G}$ ist jede Faktorgruppe $\mathfrak{G}/\mathfrak{N}$ auflösbar.

Beweis

Gemäß F (22.2) existiert zur Normalreihe $\mathfrak{G} \supseteq \mathfrak{N} \supseteq \mathfrak{E}$ eine Verfeinerung

$$\mathfrak{G} \supseteq \ldots \supseteq \mathfrak{N} \supseteq \ldots \supseteq \mathfrak{E}$$

mit abelschen Faktoren. Damit hat aber auch $\mathfrak{G}/\mathfrak{N}$ eine Normalreihe mit abelschen Faktoren, nämlich die zu der Teilreihe $\mathfrak{G} \supseteq \ldots \supseteq \mathfrak{N}$ nach S (21.3) isomorphe Reihe

$$\mathfrak{G}/\mathfrak{N} \supseteq \ldots \supseteq \mathfrak{N}/\mathfrak{N}.$$

qed.

Satz **S (22.7)**

Mit der Gruppe $\mathfrak{G}$ ist jede Untergruppe $\mathfrak{H} \subseteq \mathfrak{G}$ auflösbar.

Beweis

a) Zum Beweis benötigen wir die folgende allgemeine Aussage über Normalreihen: Zu jeder Normalreihe

$$\mathfrak{G} = \mathfrak{G}_0 \supseteq \mathfrak{G}_1 \supseteq \ldots \supseteq \mathfrak{G}_l = \mathfrak{E}$$

von $\mathfrak{G}$ existiert eine Normalreihe der Untergruppe $\mathfrak{H}$ derart, daß ihre Faktoren zu Untergruppen der Faktoren $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ isomorph sind.

Man erhält die verlangte Normalreihe durch Durchschnittsbildung:

$$\mathfrak{H} = (\mathfrak{H} \cap \mathfrak{G}_0) \supseteq (\mathfrak{H} \cap \mathfrak{G}_1) \supseteq \ldots \supseteq (\mathfrak{H} \cap \mathfrak{G}_l) = \mathfrak{E}.$$

Zunächst ist tatsächlich $\mathfrak{H} \cap \mathfrak{G}_\nu$ Normalteiler in $\mathfrak{H} \cap \mathfrak{G}_{\nu-1}$, denn $\mathfrak{H} \cap \mathfrak{G}_\nu$ ist Durchschnitt der Untergruppe $\mathfrak{H} \cap \mathfrak{G}_{\nu-1}$ von $\mathfrak{G}_{\nu-1}$ und des Normalteilers $\mathfrak{G}_\nu$ von $\mathfrak{G}_{\nu-1}$ (vgl. Aufg. 2 von § 19). Weiterhin gilt nach dem 1. Isomorphiesatz

$$(\mathfrak{H} \cap (\mathfrak{G}_{\nu-1})/(\mathfrak{H} \cap \mathfrak{G}_\nu)$$
$$= (\mathfrak{H} \cap \mathfrak{G}_{\nu-1})/((\mathfrak{H} \cap \mathfrak{G}_{\nu-1}) \cap \mathfrak{G}_\nu) \longleftrightarrow ((\mathfrak{H} \cap \mathfrak{G}_{\nu-1}) \cdot \mathfrak{G}_\nu)/\mathfrak{G}_\nu$$

(man ersetze in der Bezeichnung von S (19.5) $\mathfrak{G}$ durch $\mathfrak{G}_{\nu-1}$, $\mathfrak{H}$ durch $\mathfrak{H} \cap \mathfrak{G}_{\nu-1}$ und $\mathfrak{N}$ durch $\mathfrak{G}_\nu$). Die rechts auftretende Faktorgruppe ist aber wegen $(\mathfrak{H} \cap \mathfrak{G}_{\nu-1}) \cdot \mathfrak{G}_\nu \subseteq \mathfrak{G}_{\nu-1}$ Untergruppe von $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$, womit die Isomorphie der Faktoren $(\mathfrak{H} \cap \mathfrak{G}_{\nu-1})/(\mathfrak{H} \cap \mathfrak{G}_\nu)$ der konstruierten Normalreihe von $\mathfrak{H}$ zu Untergruppen der behaupteten Art gezeigt ist.

b) Ist daher $\mathfrak{G}$ eine Gruppe, die eine Normalreihe mit abelschen Faktoren besitzt, so gilt das gleiche für jede Untergruppe $\mathfrak{H} \subseteq \mathfrak{G}$.

qed.

Aufgaben zu § 22

1. In Verallgemeinerung von Aufgabe 3 aus § 21 beweise man: Jede auflösbare Gruppe $\mathfrak{G}$, die eine Kompositionsreihe besitzt, ist endlich.
2. Man gebe die Kompositionsfaktoren einer Gruppe $\mathfrak{G}$ von Primzahlpotenzordnung p^n an.

§ 23. Kommutatorgruppen

Nach dem Vorangegangenen ist es von Interesse, ob vorgegebene Faktorgruppen kommutativ sind oder nicht. Die Begriffsbildungen dieses Paragraphen gestatten diesbezügliche Entscheidungen und werden damit zu einem bedeutungsvollen Hilfsmittel für alle Betrachtungen, welche die Auflösbarkeit von Gruppen betreffen. Ihre Verwendung ermöglicht teilweise überraschend elegante Beweisführungen, so daß sogar oft das weiter unten abgeleitete Kriterium S (23.8) als Definition der Auflösbarkeit an die Spitze gestellt wird.

Definition **D (23.1)**

Es seien a und b Elemente einer Gruppe $\mathfrak{G}$. Dann bezeichnet man als Kommutator von a und b das Produkt:

$$a^{-1}b^{-1}\,a\,b = c.$$

Die Bezeichnung erklärt sich daraus, daß der „Kommutator" gemäß

$$ab = ba \cdot c$$

ein Ausdruck ist für die Verschiedenheit der beiden Produkte ab und ba, also für die jeweilige Abweichung vom kommutativen Gesetz; er ist genau dann gleich e, wenn a und b vertauschbar sind.

Wie man unmittelbar sieht, ist der Kommutator von b und a das Inverse des Kommutators von a und b.

Im folgenden spielt die Gesamtheit $\mathfrak{C}$ der Kommutatoren aller möglichen Elementenpaare bzw. die von ihr erzeugte Gruppe eine wesentliche Rolle:

Definition **D (23.2)**

Die in der Gruppe $\mathfrak{G}$ von dem Komplex $\mathfrak{C}$ aller Kommutatoren erzeugte Untergruppe $\mathfrak{G}' = \langle \mathfrak{C} \rangle$ heißt die Kommutatorgruppe von $\mathfrak{G}$. Sie wird auch als die erste Ableitung von $\mathfrak{G}$ bezeichnet.

So ist z. B. die Kommutatorgruppe $\mathfrak{S}_3'$ der symmetrischen Gruppe $\mathfrak{S}_3$ die alternierende Gruppe $\mathfrak{A}_3$. Es kommen nämlich als Kommutatoren (und damit als Elemente der von ihnen erzeugten Gruppe) gemäß F (10.5) nur gerade Permutationen in Frage, da a und a^{-1} sowie b und b^{-1} gleiches Vorzeichen haben. Andererseits tritt etwa (123) als Kommutator auf:

$$(13)^{-1}\,(132)^{-1}\,(13)\,(132) = (123).$$

Ferner ist natürlich für eine abelsche Gruppe $\mathfrak{G}$ stets $\mathfrak{G}' = \mathfrak{E}$ und umgekehrt, so daß für abelsche Gruppen die folgenden Aussagen trivial werden.

Satz **S (23.3)**

Die Faktorgruppe $\mathfrak{G}/\mathfrak{N}$ einer Gruppe $\mathfrak{G}$ nach einem Normalteiler $\mathfrak{N}$ ist genau dann abelsch, wenn $\mathfrak{N}$ die Kommutatorgruppe $\mathfrak{G}'$ umfaßt.

Beweis

Gleichwertig mit der Bedingung $\mathfrak{N} \geqq \mathfrak{G}'$ ist offenbar die Bedingung $\mathfrak{N} \geqq \mathfrak{C}$. Genau in diesem Falle werden aber alle Kommu-

tatoren auf das Einselement $\mathfrak{N} = [e]$ von $\mathfrak{G}/\mathfrak{N}$ abgebildet, so daß alle Abweichungen von der Kommutativität

$$ab = ba \cdot c$$

in der Faktorgruppe $\mathfrak{G}/\mathfrak{N}$ verschwinden:

$$[a][b] = [b][a].$$

qed.

Betrachten wir nun die Gesamtheit der so gekennzeichneten Normalteiler von $\mathfrak{G}$ mit abelscher Faktorgruppe, so führt die Durchschnittsbildung aus ihr nicht heraus, und insbesondere ist der Durchschnitt aller dieser Normalteiler der kleinste Normalteiler mit abelscher Faktorgruppe. Er fällt mit der Kommutatorgruppe $\mathfrak{G}'$ selbst zusammen, denn es gilt:

Satz **S (23.4)**

Die Kommutatorgruppe $\mathfrak{G}'$ ist Normalteiler von $\mathfrak{G}$.

Beweis

Unter Verwendung der Normalteilereigenschaft S(17.2d) genügt es nachzuweisen, daß das Erzeugendensystem $\mathfrak{C}$ von $\mathfrak{G}'$ aus vollständigen Klassen zueinander konjugierter Elemente besteht. Dies ist aber der Fall, da auch alle konjugierten Elemente $x^{-1}cx$ eines Kommutators $c = a^{-1}b^{-1}ab$ in $\mathfrak{C}$ enthalten sind; $x^{-1}cx$ ist nämlich der Kommutator von $x^{-1}ax$ und $x^{-1}bx$:

$$(x^{-1}ax)^{-1} \cdot (x^{-1}bx)^{-1} \cdot (x^{-1}ax) \cdot (x^{-1}bx) = x^{-1}(a^{-1}b^{-1}ab)x.$$

qed.

Damit können wir folgende Verschärfung von S(23.3) aussprechen:

Satz **S (23.5)**

Jede Untergruppe $\mathfrak{H}$ von $\mathfrak{G}$, welche die Kommutatorgruppe $\mathfrak{G}'$ enthält, ist Normalteiler von $\mathfrak{G}$.

Beweis

Beim natürlichen Homomorphismus

$$\mathfrak{G} \xrightarrow{\sim} \mathfrak{G}/\mathfrak{G}'$$

erfährt $\mathfrak{H}$ die Abbildung (vgl. § 19)

$$\mathfrak{H} \xrightarrow{\sim} \hat{\mathfrak{H}} = \mathfrak{H}/\mathfrak{G}'.$$

Nun ist $\mathfrak{H}/\mathfrak{G}'$ als Untergruppe der gemäß S(23.4) abelschen Gruppe $\mathfrak{G}/\mathfrak{G}'$ Normalteiler von $\mathfrak{G}/\mathfrak{G}'$, also ihr vollständiges Original nach S(19.6) ebenfalls Normalteiler von $\mathfrak{G}$. Dieses vollständige Original ist aber $\mathfrak{H}$, da es den Kern $\mathfrak{G}'$ enthält (vgl. S(19.2)).

qed.

Diese Strukturaussagen erleichtern es u. a. wesentlich, die Kommutatorgruppe $\mathfrak{G}'$ einer Gruppe $\mathfrak{G}$ aufzusuchen. So ist z. B. $\mathfrak{S}_4' = \mathfrak{A}_4$, denn es ist gewiß $\mathfrak{S}_4' \neq \mathfrak{E}$, aber auch $\mathfrak{S}_4' \neq \mathfrak{S}_4$, da $\mathfrak{A}_4$ ein Normalteiler mit abelscher Faktorgruppe ist; schließlich ist auch $\mathfrak{S}_4' \neq \mathfrak{V}_4$, da die drei $\mathfrak{V}_4$ enthaltenden Gruppen der Ordnung 8 nicht Normalteiler von $\mathfrak{S}_4$ sind.

Es liegt nun nahe, von der Kommutatorgruppe $\mathfrak{G}'$ einer Gruppe $\mathfrak{G}$ erneut die Kommutatorgruppe $(\mathfrak{G}')'$ zu bilden, danach deren Kommutatorgruppe usw.

Definition **D (23.6)**

Die Kommutatorgruppe $(\mathfrak{G}')'$ *der ersten Ableitung* $\mathfrak{G}'$ *von* $\mathfrak{G}$ *wird die zweite Ableitung* $\mathfrak{G}''$ *von* $\mathfrak{G}$ *genannt. Entsprechend heißt* $(\mathfrak{G}'')'$ *die dritte Ableitung* $\mathfrak{G}'''$ *von* $\mathfrak{G}$ *und allgemein* $(\mathfrak{G}^{(\nu-1)})'$ *die* ν*-te Ableitung* $\mathfrak{G}^{(\nu)}$ *von* $\mathfrak{G}$.

Zur Vereinfachung der Ausdrucksweise bezeichnet man auch die Gruppe $\mathfrak{G}$ selbst als ihre nullte Ableitung $\mathfrak{G}^{(0)}$.

Satz **S (23.7)**

a) *Für jede Untergruppe* $\mathfrak{H}$ *von* $\mathfrak{G}$ *gilt*

$$\mathfrak{H}' \subseteq \mathfrak{G}' \quad \textit{und allgemeiner} \quad \mathfrak{H}^{(\nu)} \subseteq \mathfrak{G}^{(\nu)}.$$

b) *Für jede Faktorgruppe* $\mathfrak{G}/\mathfrak{N}$ *von* $\mathfrak{G}$ *gilt*

$$(\mathfrak{G}/\mathfrak{N})' = \mathfrak{G}'\mathfrak{N}/\mathfrak{N} \quad \textit{und allgemeiner} \quad (\mathfrak{G}/\mathfrak{N})^{(\nu)} = \mathfrak{G}^{(\nu)}\mathfrak{N}/\mathfrak{N}.$$

Beweis

a) Zunächst ist $\mathfrak{H}' \subseteq \mathfrak{G}'$ unmittelbar klar, da alle Kommutatoren von Elementen aus $\mathfrak{H}$ erst recht solche von Elementen aus $\mathfrak{G}$ sind. Durch vollständige Induktion von $\nu - 1$ auf ν erhält man aus $\mathfrak{H}^{(\nu-1)} \subseteq \mathfrak{G}^{(\nu-1)}$ unter Verwendung des Induktionsanfanges

$$\mathfrak{H}^{(\nu)} = (\mathfrak{H}^{(\nu-1)})' \subseteq (\mathfrak{G}^{(\nu-1)})' = \mathfrak{G}^{(\nu)}.$$

b) Hierfür zeigen wir zunächst, daß die Bildung der Kommutatorgruppe und die homomorphe Abbildung vertauschbare Operationen sind, d. h., bei $\mathfrak{G} \xrightarrow{\sim} \overline{\mathfrak{G}}$ gilt

$$\mathfrak{G}' \xrightarrow{\sim} \overline{\mathfrak{G}'} = (\overline{\mathfrak{G}})'$$

Es sind nämlich die Bilder von Kommutatoren von Elementen aus $\mathfrak{G}$

$$a^{-1}b^{-1}ab \to \overline{a^{-1}b^{-1}ab} = (\bar{a})^{-1}(\bar{b})^{-1}\bar{a}\bar{b}$$

Kommutatoren von Elementen aus $\overline{\mathfrak{G}}$, woraus $\overline{\mathfrak{G}'} \leqq (\overline{\mathfrak{G}})'$ folgt. Umgekehrt kann man offensichtlich zu jedem Kommutator von Elementen aus $\overline{\mathfrak{G}}$ einen Kommutator von Elementen aus $\mathfrak{G}$ finden, dessen Bild er ist, woraus entsprechend $\overline{\mathfrak{G}'} \geqq (\overline{\mathfrak{G}})'$ folgt.

Diese Aussage übertragen wir durch vollständige Induktion auf beliebig hohe Ableitungen. Es gelte also bereits

$$\mathfrak{G}^{(\nu-1)} \xrightarrow{\sim} \overline{\mathfrak{G}^{(\nu-1)}} = (\overline{\mathfrak{G}})^{(\nu-1)}.$$

Durch Anwendung des Induktionsanfanges auf $\mathfrak{G}^{(\nu-1)}$ (man ersetze oben $\mathfrak{G}$ durch $\mathfrak{G}^{(\nu-1)}$) erhält man

$$\mathfrak{G}^{(\nu)} = (\mathfrak{G}^{(\nu-1)})' \xrightarrow{\sim} \overline{(\mathfrak{G}^{(\nu-1)})'} = (\overline{\mathfrak{G}^{(\nu-1)}})',$$

also nach Induktionsvoraussetzung weiter

$$(\overline{\mathfrak{G}^{(\nu-1)}})' = ((\overline{\mathfrak{G}})^{(\nu-1)})' = (\overline{\mathfrak{G}})^{(\nu)}.$$

Das Resultat

$$\mathfrak{G}^{(\nu)} \xrightarrow{\sim} \overline{\mathfrak{G}^{(\nu)}} = (\overline{\mathfrak{G}})^{(\nu)}$$

entspricht aber bereits unserer Behauptung, da beim natürlichen Homomorphismus $\mathfrak{G} \xrightarrow{\sim} \overline{\mathfrak{G}} = \mathfrak{G}/\mathfrak{N}$ das Bild $\overline{\mathfrak{G}^{(\nu)}}$ der Untergruppe $\mathfrak{G}^{(\nu)}$ gleich der Faktorgruppe $\mathfrak{G}^{(\nu)}\mathfrak{N}/\mathfrak{N}$ ist. qed.

Bereits im Anschluß an S (23.7a) kann man das eingangs erwähnte Kriterium für die Auflösbarkeit einer Gruppe gewinnen:

Satz **S (23.8)**

Eine Gruppe $\mathfrak{G}$ ist genau dann auflösbar, wenn unter ihren Ableitungen die Einheitsgruppe $\mathfrak{E}$ auftritt. Ist dabei k die kleinste Zahl mit $\mathfrak{G}^{(k)} = \mathfrak{E}$, so ist

$$\mathfrak{G} = \mathfrak{G}^{(0)} \supset \mathfrak{G}' \supset \mathfrak{G}'' \supset \ldots \supset \mathfrak{G}^{(k)} = \mathfrak{E}$$

eine Normalreihe ohne Wiederholungen mit abelschen Faktoren.

Beweis

Es sei $\mathfrak{G}$ eine auflösbare Gruppe und

$$\mathfrak{G} = \mathfrak{G}_0 \supseteq \mathfrak{G}_1 \supseteq \ldots \supseteq \mathfrak{G}_l = \mathfrak{E}$$

eine Normalreihe mit abelschen Faktoren. Wir zeigen durch vollständige Induktion von $l-1$ auf l, daß $\mathfrak{G}^{(l)} = \mathfrak{E}$ ist, indem wir dies bereits für alle auflösbaren Gruppen als richtig annehmen, die eine solche Normalreihe mit weniger als l Faktoren besitzen. Den Induktionsanfang liefert die Einheitsgruppe $\mathfrak{G}_0 = \mathfrak{G}^{(0)} = \mathfrak{E}$.

Aus der Kommutativität von $\mathfrak{G}/\mathfrak{G}_1$ folgt nach S (23.3)

$$\mathfrak{G}_1 \supseteq \mathfrak{G}'$$

und damit nach S (23.7a)

$$\mathfrak{G}_1^{(l-1)} \supseteq (\mathfrak{G}')^{(l-1)} = \mathfrak{G}^{(l)}.$$

Nun ist aber $\mathfrak{G}_1$ eine auflösbare Gruppe, die eine Normalreihe mit abelschen Faktoren von der Länge $l-1$ besitzt, also gilt nach Induktionsvoraussetzung $\mathfrak{G}_1^{(l-1)} = \mathfrak{E}$; damit ist aber erst recht

$$\mathfrak{G}^{(l)} = \mathfrak{E}.$$

Zum Beweis der Umkehrung sowie der ergänzenden Behauptungen betrachten wir die Reihe aller Ableitungen von $\mathfrak{G}$

$$\mathfrak{G} = \mathfrak{G}^{(0)} \supseteq \mathfrak{G}' \supseteq \mathfrak{G}'' \supseteq \ldots.$$

Zufolge S (23.4) ist dabei stets $\mathfrak{G}^{(\nu)}$ Normalteiler in $\mathfrak{G}^{(\nu-1)}$. Da nun nach Voraussetzung unter den Ableitungen von $\mathfrak{G}$ die Einheitsgruppe $\mathfrak{G}^{(k)} = \mathfrak{E}$ auftritt, bricht die obige Reihe ab, ist also eine Normalreihe von $\mathfrak{G}$. Ihre Faktoren $\mathfrak{G}^{(\nu-1)}/\mathfrak{G}^{(\nu)}$ sind nach S (23.3) abelsch. Insbesondere ist bei minimaler Wahl von k diese Reihe wiederholungsfrei, da beim sukzessiven Bilden der Ableitungen von $\mathfrak{G}$ aus $\mathfrak{G}^{(\nu)} = \mathfrak{G}^{(\nu-1)}$ offensichtlich $\mathfrak{G}^{(\nu+1)} = \mathfrak{G}^{(\nu)}$ und damit die Gleichheit aller weiteren Glieder der Reihe folgt.

qed.

Als Beispiel für dieses Kriterium geben wir die Reihe der Ableitungen für die symmetrischen Gruppen an (vgl. auch Aufg. 2):

$$\mathfrak{S}_3 > \mathfrak{S}_3' = \mathfrak{A}_3 > \mathfrak{S}_3'' = \mathfrak{E},$$
$$\mathfrak{S}_4 > \mathfrak{S}_4' = \mathfrak{A}_4 > \mathfrak{S}_4'' = \mathfrak{V}_4 > \mathfrak{S}_4''' = \mathfrak{E},$$
$$\mathfrak{S}_n > \mathfrak{S}_n' = \mathfrak{S}_n'' = \ldots = \mathfrak{A}_n \quad \text{für } n \geq 5.$$

Ferner stimmt die im § 22 für die Gruppe $\mathfrak{D}$ aller orthogonalen Matrizen vom Typ (2,2) angegebene Normalreihe mit abelschen Faktoren mit der Reihe der Ableitungen von $\mathfrak{D}$ überein (vgl. Aufgabe 4):

$$\mathfrak{D} > \mathfrak{D}' = \mathfrak{D}_+ > \mathfrak{D}'' = \mathfrak{E}.$$

Vor allen Dingen ist aber der in S(23.8) angegebene Zusammenhang zwischen der Auflösbarkeit einer Gruppe und der Reihe ihrer Ableitungen zur Gewinnung allgemeiner Aussagen für auflösbare Gruppen von Wert. Wir müssen uns hier allerdings darauf beschränken, dies durch einen zweiten Beweis der uns bereits bekannten Sätze S(22.6) und S(22.7) deutlich zu machen.

Erneuter Beweis von S(22.6):

Nach S(23.8) ist nur zu zeigen, daß unter den Ableitungen von $\mathfrak{G}/\mathfrak{N}$ die Einheitsgruppe $\mathfrak{N}/\mathfrak{N}$ auftritt. Aus $\mathfrak{G}^{(l)} = \mathfrak{E}$ folgt aber nach S(23.7b)

$$(\mathfrak{G}/\mathfrak{N})^{(l)} = \mathfrak{G}^{(l)}\mathfrak{N}/\mathfrak{N} = \mathfrak{N}/\mathfrak{N}.$$

Erneuter Beweis von S(22.7):

Aus $\mathfrak{G}^{(l)} = \mathfrak{E}$ folgt wieder unmittelbar nach S(23.7a)

$$\mathfrak{H}^{(l)} = \mathfrak{E} \quad \text{wegen} \quad \mathfrak{H}^{(l)} \subseteq \mathfrak{G}^{(l)}.$$

Aufgaben zu § 23

1. Statt der Gleichung $ab = ba \cdot c$ könnte man zur Kennzeichnung der Abweichung vom kommutativen Gesetz auch jede der Gleichungen

$$ab = c_1 \cdot ba, \quad ab \cdot c_2 = ba, \quad c_3 \cdot ab = ba$$

verwenden und damit entsprechend „Kommutatoren" definieren, wie das zum Teil auch in der Literatur üblich ist.
Man drücke c_1, c_2, c_3 durch den in D(23.1) festgelegten Kommutatorbegriff aus und begründe, warum die Willkürlichkeit dieser Wahl für die Begriffsbildung der Kommutatorgruppe bedeutungslos ist.

2. Mit Hilfe der allgemeinen Aussagen des Textes bestimme man die Kommutatorgruppe der symmetrischen Gruppe $\mathfrak{S}_n$ für $n \geq 5$.
3. Ebenso ermittle man die Kommutatorgruppe von $\mathfrak{G} = \langle (13), (14)(23) \rangle$.
4. Man beweise die im Text angegebenen Behauptungen über die Ableitungen von $\mathfrak{O}$ (unter Heranziehung der geometrischen Bedeutung der in Frage kommenden Matrizen).
5. Mit Hilfe von S(23.8) beweise man erneut S(22.4).

LÖSUNGEN DER AUFGABEN

Zu § 1

1. Der verlangte Beweis verläuft unter Vertauschung der Seiten genau wie der im Text durchgeführte: Für ein festes $c \in \mathfrak{G}$ gibt es ein $y \in \mathfrak{G}$ mit

$$c \cdot y = c.$$

Ein beliebiges Element $a \in \mathfrak{G}$ kann als Produkt

$$x \cdot c = a$$

mit $x \in \mathfrak{G}$ geschrieben werden. Damit wird

$$a \cdot y = (x \cdot c) \cdot y = x \cdot (c \cdot y) = x \cdot c = a,$$

d. h., $y = e_R$ reproduziert bei Multiplikation von rechts alle Elemente aus $\mathfrak{G}$.

2. Für diesen Beweis gilt Entsprechendes. Wir gehen hier wie im folgenden auf Aufgaben, deren Lösungen sich unmittelbar in Analogie zum Text ergeben, nicht mehr näher ein.

3. Es sei bereits $(a_1 \cdot a_2 \cdot \ldots \cdot a_n)^{-1} = a_n^{-1} \cdot \ldots \cdot a_2^{-1} \cdot a_1^{-1}$ nachgewiesen. Dann gilt nach F(1.2) und F(1.6)

$$(a_1 a_2 \ldots a_n a_{n+1})^{-1} = ((a_1 a_2 \ldots a_n)\, a_{n+1})^{-1} = a_{n+1}^{-1}\,(a_1 a_2 \ldots a_n)^{-1}$$

und damit nach Induktionsvoraussetzung und F(1.2) weiter

$$= a_{n+1}^{-1}(a_n^{-1} \ldots a_2^{-1} a_1^{-1}) = a_{n+1}^{-1}\, a_n^{-1} \ldots a_2^{-1} a_1^{-1}.$$

4. Wir zeigen, daß aus $a x_1 = a x_2 = b$ ohne Verwendung von S(1.4) und S(1.5) $x_1 = x_2$ folgt. Nach *M III* existieren nämlich in $\mathfrak{G}$ Lösungen y und z der Gleichungen

$$x_1 = y\, b \quad \text{und} \quad x_2 = x_1 z.$$

Dann ist aber

$$x_1 = y\, b = y\,(a x_2) = (y a)\, x_2 = (y a)\,(x_1 z)$$
$$= (y\,(a x_1))\, z = (y b)\, z = x_1 z = x_2.$$

Analog beweist man die Behauptung für $y_1 a = y_2 a = b$.

5. Einselement und Inverses sind Lösungen von speziellen Gleichungen der Gestalt $a x = b$ bzw. $y a = b$ und als solche nach S(1.8) eindeutig bestimmt.

6. Die hierzu erforderlichen Überlegungen unterscheiden sich von den im Text durchgeführten nur durch die Vertauschung der Seiten.

7. Die natürlichen Zahlen erfüllen mit der gewöhnlichen Multiplikation als Verknüpfung nach den Grundgesetzen der Arithmetik *M I*, *M II* und *M III**. Würde nun S(1.10) auch für unendliche Mengen gelten, müßten die natürlichen Zahlen eine multiplikative Gruppe bilden. Sie erfüllen aber *M III* offensichtlich nicht.

8. Man achte bei der Durchführung insbesondere auf die Entsprechung von $\cdot$ und $+$, $\prod$ und $\sum$, e und o, a^{-1} und $(-a)$ sowie auf die Vereinfachungen, die sich aus der Gültigkeit des kommutativen Gesetzes ergeben.

9. Für F(1.12) sind die gleichen Schritte wie bei F(1.2) und F(1.3) unter Ersetzung von $\cdot$ durch $+$ durchzuführen.

Zum Beweis von S(1.13) gewährleistet zunächst *A III* die Existenz eines $y \in \mathfrak{G}$ mit

$$c + y = c$$

für ein festes $c \in \mathfrak{G}$. Jedes andere Element $a \in \mathfrak{G}$ läßt sich dann wieder nach *A III* als Summe

$$a = x + c$$

mit $x \in \mathfrak{G}$ schreiben. Dann ist wegen

$$a + y = x + c + y = x + c = a$$

$y = o$ ein Element mit der verlangten Eigenschaft. Aus

$$o_1 + o_2 = o_1$$
$$o_1 + o_2 = o_2$$

folgt die Eindeutigkeit.

Die Existenz von $(-a)$ in S(1.14) folgt unmittelbar aus *A III*. Die Eindeutigkeit ergibt sich aus

$$(-a)_1 = o + (-a)_1 = ((-a)_2 + a) + (-a)_1 = (-a)_2 + (a + (-a)_1)$$
$$= (-a)_2 + o = (-a)_2.$$

F(1.15) und F(1.16) lassen sich aus F(1.6) und F(1.7) ohne weiteres entnehmen. Desgleichen folgt aus $a + x_1 = a + x_2$ durch Addition von $(-a)$ sofort $x_1 = x_2$ und damit S(1.17).

Bei S(1.18) genügt wieder, aus *A III*$_1$ und *A III*$_2$ das Axiom *A III* herzuleiten. Das Element $x = (-a) + b$ löst aber offensichtlich die Gleichung $a + x = b$. Um schließlich in S(1.19) für endliche Moduln aus der Eindeutigkeitsaussage *A III** die Existenzaussage *A III* zu erhalten, verwendet man die Summen $a + x$, in denen x alle Elemente von $\mathfrak{G}$ durchläuft. Sie sind wegen *A III** sämtlich verschieden und machen gerade den ganzen Modul aus, so daß jede Gleichung $a + x = b$ mit $x \in \mathfrak{G}$ lösbar ist.

Zu § 2

1. B(2.1) und B(2.2): Die Durchführung der verlangten Nachweise versteht sich von selbst, wenn wir uns auf die Grundgesetze der Arithmetik stützen, und wird hier wie im folgenden nicht näher angegeben. (Siehe z. B. v. MANGOLDT-KNOPP „Einführung in die höhere Mathematik", S. Hirzel Verlag, Leipzig 1954, Bd. 1 S. 110ff.; A. VOGEL „Klassische Grundlagen der Analysis", S. Hirzel Verlag, Leipzig 1952, S. 4ff.)

B(2.3): Für die Grundlagen der Vektorrechnung siehe z. B. das in der gleichen Reihe erschienene Buch von M. HIEKE.

B(2.7): Die Gruppeneigenschaft ist jeweils entsprechend dem Hinweis im Text wie unter a) nachzuprüfen.

2. Weitere Beispiele:
a) Der Modul aller ganzzahligen Vielfachen einer beliebigen Zahl.
b) Die multiplikative abelsche Gruppe aller Potenzen einer beliebigen Zahl mit ganzzahligen Exponenten.

3. Das skalare Produkt zweier Vektoren ist nach Definition kein Vektor, also ist schon *M I* nicht erfüllt. Das vektorielle Produkt erfüllt zwar *M I*, dagegen nicht *M II*.

4. Man wähle etwa die Matrizen

$$\begin{pmatrix} 1 & 1 & & & 0 \\ 1 & 0 & & & \\ & & 1 & & \\ & & & \ddots & \\ 0 & & & & 1 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} 1 & 0 & & & 0 \\ 1 & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ 0 & & & & 1 \end{pmatrix}.$$

5. Der Satz gilt für $n = 1$. Wir führen vollständige Induktion von n auf $n + 1$ durch. Die Permutationen der Zahlen 1, 2, ..., $n + 1$ haben die Gestalt

$$s = \begin{pmatrix} 1 & 2 & \dots & n & n+1 \\ i_1 & i_2 & \dots & i_n & i_{n+1} \end{pmatrix}.$$

Nach Induktionsvoraussetzung gibt es für $i_1 = 1$ genau $n!$ Anordnungen von $i_2, \dots, i_{n+1}$, entsprechend für $i_1 = 2, \dots, i_1 = n + 1$. Das ergibt insgesamt $(n + 1) \cdot n! = (n + 1)!$ verschiedene Permutationen, womit alle Möglichkeiten erschöpft sind.

6. Im Falle $n = 2$ ist die Behauptung klar, für $n = 3$ wurde sie im Text durch ein Beispiel bewiesen. Dieser Beweis überträgt sich auf beliebiges $n > 3$, denn unter allen Permutationen der Zahlen 1, 2, ..., n befinden sich insbesondere die Permutationen

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 1 & 3 & 4 & \dots & n \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 3 & 1 & 4 & \dots & n \end{pmatrix}.$$

7. Die Elemente der symmetrischen Gruppe $\mathfrak{S}_3$ sind:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Ihre Anwendung auf $f(x_1, x_2, x_3) = x_1 x_2 + x_2 x_3 + x_3 x_1$ ergibt der Reihe nach:

$$\begin{aligned} x_1 x_2 + x_2 x_3 + x_3 x_1 &= f(x_1, x_2, x_3) \\ x_2 x_3 + x_3 x_1 + x_1 x_2 &= f(x_1, x_2, x_3) \\ x_3 x_1 + x_1 x_2 + x_2 x_3 &= f(x_1, x_2, x_3) \\ x_2 x_1 + x_1 x_3 + x_3 x_2 &= f(x_1, x_2, x_3) \\ x_3 x_2 + x_2 x_1 + x_1 x_3 &= f(x_1, x_2, x_3) \\ x_1 x_3 + x_3 x_2 + x_2 x_1 &= f(x_1, x_2, x_3). \end{aligned}$$

8. Es gilt:
$a - a = 0 \cdot m$;
aus $a - b = g \cdot m$ folgt $b - a = (-g) \cdot m$;
aus $a - b = g \cdot m$ und $b - c = g' \cdot m$ folgt $a - c = (g + g') \cdot m$.

9. Es ist zu zeigen, daß aus $[a] = [a']$ und $[b] = [b']$ folgt $[a \cdot b] = [a' \cdot b']$, d. h., daß sich $ab \equiv a'b' \ (m)$ aus $a \equiv a' \ (m)$ und $b \equiv b' \ (m)$ ergibt. Wegen $a = a' + gm$ und $b = b' + hm$ ist aber $ab = a'b' + (a'h + b'g + hgm)m$.

10. Die Restklassen mod 6 bestehen aus den Zahlen:

[0],	[1],	[2],	[3],	[4],	[5]
.	.	.	.	.	.
.	.	.	.	.	.
− 12	− 11	− 10	− 9	− 8	− 7
− 6	− 5	− 4	− 3	− 2	− 1
0	+ 1	+ 2	+ 3	+ 4	+ 5
+ 6	+ 7	+ 8	+ 9	+ 10	+ 11
+ 12	+ 13	+ 14	+ 15	+ 16	+ 17

wobei insbesondere die Zahlen 0, 1, 2, 3, 4, 5 das kleinste nicht-negative Repräsentantensystem mod 6 bilden. Die Unabhängigkeit der Verknüpfungen von der Wahl der Repräsentanten zeigt sich z. B. bei

$$[3] + [4] = [3 + 4] = [7] = [1]$$
$$[15] + [-2] = [15 - 2] = [13] = [1]$$

bzw. in Kongruenzschreibweise

$$3 + 4 \equiv 7 \equiv 1 \quad (6)$$
$$15 - 2 \equiv 13 \equiv 1 \quad (6)$$

sowie bei

$$[3] \cdot [4] = [3 \cdot 4] = [12] = [0]$$
$$[15] \cdot [-2] = [15 \cdot (-2)] = [-30] = [0]$$

bzw.

$$3 \cdot 4 \equiv 12 \equiv 0 \quad (6)$$
$$15 \quad (-2) \equiv -30 \equiv 0 \quad (6).$$

11. Jeder Teiler t einer Zahl a entsteht aus der Zerlegung von a in Primfaktoren durch Auswahl eines Teilproduktes dieser Primfaktoren. Entsprechend ist jeder gemeinsame Teiler von a und b ein gemeinsames Teilprodukt der Zerlegungen von a und b, also der größte gemeinsame Teiler $d = (a, b)$ das größtmögliche Teilprodukt dieser Art. Damit erfüllt d nicht nur trivialer Weise 1., sondern auch 2. Genügt umgekehrt eine positive ganze Zahl diesen beiden Forderungen, so ist sie wegen 1. gemeinsamer Teiler von a und b und wegen 2. der größte unter allen, da ja jeder andere gemeinsame Teiler ein Faktor von ihr ist.

Zu § 3

1. Die beiden Gesetze *I* und *II* ergeben sich unmittelbar durch Abzählen der Faktoren. Daß für *III* die Vertauschbarkeit der Faktoren a und b hinreichend ist, ist ebenfalls klar. Sie ist auch notwendig, denn schon für $n = 2$ folgt aus
$$(ab)^2 = ab\,ab = a^2 b^2$$
durch Multiplikation mit a^{-1} von links und b^{-1} von rechts
$$ba = ab.$$

2. Es gelte als Induktionsvoraussetzung $(a^n)^{-1} = (a^{-1})^n$. Dann wird
$$(a^{-1})^{n+1} = (a^{-1})^n \cdot (a^{-1}) = (a^n)^{-1} \cdot a^{-1}$$
und nach F(1.6)
$$(a^n)^{-1} \cdot a^{-1} = (a \cdot a^n)^{-1} = (a^{n+1})^{-1}.$$
Als Induktionsanfang prüft man entweder die Formel für $n = 2$ direkt nach oder benützt aus D(3.4) $a^1 = a$ für $n = 1$.

3. Es ist
$$(a^n)^{m+1} = (a^n)^m \cdot (a^n) = a^{nm} \cdot a^n = a^{nm+n} = a^{n(m+1)}.$$

4. Aus $ab = ba$ folgt $(ab)^{-1} = (ba)^{-1}$ und damit nach F(1.6)
$$b^{-1}a^{-1} = a^{-1}b^{-1}$$
und umgekehrt.

5. $a^n a^m = a^{n+m} = a^{m+n} = a^m a^n$.

6. $(ab)^{-n} = [(ab)^{-1}]^n = (b^{-1}a^{-1})^n$. Durch vollständige Induktion folgt $(abc \ldots k)^{-n} = (k^{-1} \ldots c^{-1}b^{-1}a^{-1})^n$.

7. Man beachte die Wechselbeziehung von „Potenz" und „Vielfachem".

8. $(-n) \cdot [a + b + c + \cdots + k] = n[(-a) + (-b) + (-c) + \cdots + (-k)]$.

9. Hinweis: Die Erklärung der Multiplikation ganzer Zahlen als „Rechenoperation zweiter Stufe" entspricht einer Operatoranwendung der bereits additiv verknüpfbaren ganzen Zahlen auf sich selbst.

10. Es sei $\mathfrak{x} = x_1\mathfrak{e}_1 + x_2\mathfrak{e}_2 + x_3\mathfrak{e}_3$ ein beliebiger Vektor und r eine beliebige reelle Zahl. Dann ist
$$r\mathfrak{x} = (r \cdot x_1)\,\mathfrak{e}_1 + (r \cdot x_2)\,\mathfrak{e}_2 + (r \cdot x_3)\,\mathfrak{e}_3$$
wieder ein dem Modul angehörender Vektor, dessen Länge die r-fache Länge von $\mathfrak{x}$ ist. Für diese Operatoranwendung gilt, wie durch Ausrechnung folgt:
$$I: \quad r\mathfrak{x} + s\mathfrak{x} = (r + s)\,\mathfrak{x}$$
$$II: \quad r(s\mathfrak{x}) = (r \cdot s)\mathfrak{x}$$
$$III: \quad r\mathfrak{x} + r\mathfrak{y} = r(\mathfrak{x} + \mathfrak{y}).$$

11. Mit der Operatoranwendung $r(a_{ik}) = (r \cdot a_{ik})$ verläuft alles wie bei 10.

Zu § 4

1.
0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

2.
1	5	7	11
5	1	11	7
7	11	1	5
11	7	5	1

3.
1	i	−1	−i	0 1 2 3
i	−1	−i	1	1 2 3 0
−1	−i	1	i	2 3 0 1
−i	1	i	−1	3 0 1 2

4. Die Strukturtafel für die Gruppe $\mathfrak{S}_3$ ist im Text angegeben.

5. *I*: Die Eineindeutigkeit der Zuordnung und der durch sie gegebenen Abbildung der genannten Mengen aufeinander ist eine Eigenschaft der Funktion $\bar{x} = \log x$ (vgl. Abb. 12).

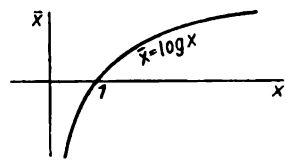


Abb. 12

II: Die Zuordnung ist relationstreu wegen

$$\overline{x_1 \cdot x_2} = \log (x_1 \cdot x_2) = \log x_1 + \log x_2 = \overline{x_1} + \overline{x_2}.$$

6. Es sei e Einselement von $\mathfrak{G}$, also $ea = a$ für alle $a \in \mathfrak{G}$. Dann ist wegen $\bar{e}\,\bar{a} = \bar{e} \cdot \bar{a} = \bar{a}$ für alle $\bar{a} \in \overline{\mathfrak{G}}$ das Bild $\bar{e}$ von e Einselement von $\overline{\mathfrak{G}}$. Ferner ist $(\bar{a})^{-1} = \overline{(a^{-1})}$ wegen $\overline{(a^{-1})}\,\bar{a} = \overline{(a^{-1})} \cdot \bar{a} = \bar{e}$.

Zu § 5

1. $\binom{6}{1} + \binom{6}{2} + \binom{6}{3} + \binom{6}{4} + \binom{6}{5} + \binom{6}{6} = 63$.

2. Mit den Bezeichnungen wie im Beispiel nach D(4.1) sei

$$\mathfrak{A} = \{s_1, s_2, s_3\} \text{ und } \mathfrak{B} = \{s_3, s_4\}.$$

Dann ist:

$\mathfrak{A} \cap \mathfrak{B} = \{s_3\}$, $\mathfrak{A} \cup \mathfrak{B} = \{s_1, s_2, s_3, s_4\}$, $\mathfrak{A} \cdot \mathfrak{B} = \{s_1, s_2, s_3, s_4, s_5, s_6\}$,

$\mathfrak{A}^{-1} = \{s_1, s_2, s_3\}$; $\mathfrak{B}^{-1} = \{s_2, s_4\}$.

3. $\mathfrak{A}$ bestehe aus s_1, s_2, s_3; $\mathfrak{B}$ aus s_4, s_5; $\mathfrak{C}$ aus s_2, s_3. Dann ist:

$$\mathfrak{A} \cdot \mathfrak{B} = \{s_4, s_5, s_6\}, \quad (\mathfrak{A} \cdot \mathfrak{B}) \cdot \mathfrak{C} = \{s_4, s_5, s_6\}$$

und

$$\mathfrak{B} \cdot \mathfrak{C} = \{s_4, s_5, s_6\}, \quad \mathfrak{A} \cdot (\mathfrak{B} \cdot \mathfrak{C}) = \{s_4, s_5, s_6\}.$$

4. Man wähle $\mathfrak{A}$ und $\mathfrak{B}$ wie in 3. Dann gilt $\mathfrak{A} \cdot \mathfrak{B} = \mathfrak{B} \cdot \mathfrak{A}$, während z. B. $s_2 s_4 \neq s_4 s_2$ ist.

5. Die erste Relation ist richtig, da auf beiden Seiten genau die Elemente stehen, deren rechter Faktor aus $\mathfrak{C}$ und deren linker Faktor aus $\mathfrak{A}$ oder $\mathfrak{B}$ entnommen sind.

Die linke Seite der zweiten Relation besteht aus genau den Elementen, deren rechter Faktor in $\mathfrak{C}$ und deren linker Faktor sowohl in $\mathfrak{A}$ als auch in $\mathfrak{B}$ liegen. Diese Elemente sind aber offensichtlich in der rechten Seite dieser Relation enthalten.

Daß das Gleichheitszeichen nicht zu gelten braucht, zeigt folgendes Beispiel:

Es sei $\mathfrak{A} = \{s_1, s_4\}$, $\mathfrak{B} = \{s_4, s_6\}$, $\mathfrak{C} = \{s_1, s_6\}$. Dann ist:

$$(\mathfrak{A} \cup \mathfrak{B}) \cdot \mathfrak{C} = \{s_1, s_3, s_4, s_6\}, \qquad \mathfrak{A}\mathfrak{C} \cup \mathfrak{B}\mathfrak{C} = \{s_1, s_3, s_4, s_6\}$$

und

$$(\mathfrak{A} \cap \mathfrak{B}) \cdot \mathfrak{C} = \{s_3, s_4\}, \qquad \mathfrak{A}\mathfrak{C} \cap \mathfrak{B}\mathfrak{C} = \{s_1, s_3, s_4, s_6\}.$$

6. Es sei a beliebig aus $\mathfrak{H}$. Das zu a gehörige Inverse innerhalb $\mathfrak{H}$ sei $a_{\mathfrak{H}}^{-1}$, innerhalb $\mathfrak{G}$ sei es $a_{\mathfrak{G}}^{-1}$. Dann gelten die Gleichungen

$$a \cdot a_{\mathfrak{H}}^{-1} = e_{\mathfrak{H}}$$

$$a \cdot a_{\mathfrak{G}}^{-1} = e_{\mathfrak{G}}.$$

Wegen $e_{\mathfrak{H}} = e_{\mathfrak{G}}$ folgt, indem wir beide Gleichungen in $\mathfrak{G}$ betrachten, nach *MIII** $a_{\mathfrak{H}}^{-1} = a_{\mathfrak{G}}^{-1}$.

7. Es ist die Äquivalenz der Bedingung (*) $ab^{-1} \in \mathfrak{H}$
mit den Bedingungen (**) $ab \in \mathfrak{H}$
(***) $a^{-1} \in \mathfrak{H}$
für alle $a \in \mathfrak{H}$ und $b \in \mathfrak{H}$ zu zeigen:

Einerseits folgt aus (*), angewendet auf $a = b$, daß $aa^{-1} = e \in \mathfrak{H}$. Nochmals (*) angewendet auf $e \in \mathfrak{H}$ und $a \in \mathfrak{H}$ ergibt $ea^{-1} = a^{-1} \in \mathfrak{H}$ also (***). Ferner ist mit a und b, wie eben gezeigt, auch a und b^{-1} und daher nach (*) $a(b^{-1})^{-1} = ab \in \mathfrak{H}$.

Andererseits liefert (***), angewendet auf $b \in \mathfrak{H}$, daß auch $b^{-1} \in \mathfrak{H}$ und damit nach (**) $ab^{-1} \in \mathfrak{H}$ für alle $a \in \mathfrak{H}$ und $b \in \mathfrak{H}$.

8. Der verlangte Beweis verläuft völlig analog zu dem im Text angegebenen.

9. Man setze in $\mathfrak{H}\mathfrak{A} = \mathfrak{H}$ für $\mathfrak{A}$ einmal $\mathfrak{H}$, einmal $\mathfrak{H}^{-1}$.

10. Die Untergruppen der $\mathfrak{S}_3$ sind:

$$\{s_1\}, \{s_1, s_4\}, \{s_1, s_5\}, \{s_1, s_6\}, \{s_1, s_2, s_3\} \text{ und } \mathfrak{S}_3 \text{ selbst.}$$

Als Beispiel für S (5.9) wähle man etwa $\mathfrak{H} = \{s_1, s_2, s_3\}$, $\mathfrak{A} = \{s_2, s_3\}$.

11. Man wähle $\mathfrak{A} = \{s_1, s_2, s_3\}$ und $\mathfrak{B} = \{s_1, s_4\}$.

12. Man wähle $\mathfrak{A}$ und $\mathfrak{B}$ wie in Aufgabe 11; es ergibt sich $\mathfrak{A}\mathfrak{B} = \mathfrak{B}\mathfrak{A} = \mathfrak{S}_3$.

13. $\{s_1\} = \langle s_1 \rangle$;

$\{s_1, s_4\} = \langle s_1, s_4 \rangle = \langle s_4 \rangle$, analog $\{s_1, s_5\}$, $\{s_1, s_6\}$;

$\{s_1, s_2, s_3\} = \langle s_1, s_2, s_3 \rangle = \langle s_1, s_2 \rangle = \langle s_1, s_3 \rangle = \langle s_2, s_3 \rangle = \langle s_2 \rangle = \langle s_3 \rangle$;

$$\begin{aligned}\mathfrak{S}_3 &= \langle s_4, s_5 \rangle = \langle s_4, s_6 \rangle = \langle s_5, s_6 \rangle \\ &= \langle s_2, s_4 \rangle = \langle s_2, s_5 \rangle = \langle s_2, s_6 \rangle \\ &= \langle s_3, s_4 \rangle = \langle s_3, s_5 \rangle = \langle s_3, s_6 \rangle.\end{aligned}$$

14. Es sei a ein beliebiges Element von $\mathfrak{H}$. Ohne Beschränkung der Allgemeinheit können wir a positiv wählen, da mit a auch $(-a)$ in $\mathfrak{H}$ enthalten ist und umgekehrt. Wir subtrahieren so oft m von a, bis ein Rest r mit $0 \leqq r < m$ bleibt: $\quad a - qm = r.$

Der nichtnegative ganzzahlige Operator q gibt an, wie oft m subtrahiert wurde. Diese Operation führt aus dem Untermodul $\mathfrak{H}$ nicht heraus, so daß auch $r \in \mathfrak{H}$ ist. Aus der Voraussetzung über m folgt $r = 0$.

15. Entsprechend S(5.6) genügt es zu zeigen, daß mit je zwei Vektoren auch ihre Differenz in der als Untermodul nachzuweisenden Menge enthalten ist. Das ist aber offensichtlich erfüllt.

16. a) Wir benutzen S(5.5) und zeigen, daß das Produkt zweier Matrizen mit Determinante ± 1 sowie das Inverse einer solchen Matrix wieder eine Matrix mit Determinante ± 1 ist. Ersteres folgt aus

$$|A \cdot B| = |A| \cdot |B|$$

unmittelbar, letzteres aus

$$|A^{-1}| = |A|^{-1} \text{ wegen } |AA^{-1}| = |A| \cdot |A^{-1}| = |E|.$$

b) Man schließt wie unter a).

c) Hier benutzt man die Formeln:

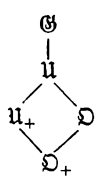
$$(AB)^T = B^T A^T = B^{-1} A^{-1} = (AB)^{-1},$$
$$(A^{-1})^T = (A^T)^T = A = (A^{-1})^{-1}.$$

d) Alle orthogonalen Matrizen sind unimodular wegen

$$|E| = |AA^{-1}| = |AA^T| = |A| \cdot |A^T| = |A|^2.$$

Damit gilt $\mathfrak{O}_+ = \mathfrak{O} \cap \mathfrak{U}$, womit nach S(5.10) die Untergruppeneigenschaft von $\mathfrak{O}_+$ bereits gezeigt ist.

Das Verhältnis der genannten Untergruppen zueinander spiegelt das nebenstehende leicht verständliche Schema wider.



17. Die Behauptung ergibt sich sofort mit Hilfe von S(5.5), denn sind a und b zwei Transformationen, die nur endlich viele Elemente wirklich verändern, so gilt das gleiche offenbar auch für ab und a^{-1}.

Zu § 6

1. Es haben der Reihe nach die Elemente $s_1, s_2, \ldots, s_6$ die Ordnungen 1, 3, 3, 2, 2, 2.

2. Aus $a^1 = e$ folgt $a = e$ unmittelbar.

3. Es sei $\mathfrak{G} \overset{\sim}{\longleftrightarrow} \overline{\mathfrak{G}}$ und $\bar{a} \in \overline{\mathfrak{G}}$ das Bild des Elementes $a \in \mathfrak{G}$. Dann wird $\langle a \rangle$ nach F(4.4) auf eine Untergruppe $\overline{\mathfrak{H}} \leqq \overline{\mathfrak{G}}$ abgebildet mit $\bar{a} \in \overline{\mathfrak{H}}$. Vermöge der Relationstreue gilt

$$a^k \to \overline{(a^k)} = (\bar{a})^k,$$

also $\overline{\mathfrak{H}} = \langle \bar{a} \rangle$. Die Gleichmächtigkeit von $\langle a \rangle$ und $\langle \bar{a} \rangle$ zeigt die Behauptung.

4.

0	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4

Restklassenmodul mod 6 mit dem erzeugenden Element [1]

ε^0	ε^1	ε^2	ε^3	ε^4	ε^5
ε^1	ε^2	ε^3	ε^4	ε^5	ε^0
ε^2	ε^3	ε^4	ε^5	ε^0	ε^1
ε^3	ε^4	ε^5	ε^0	ε^1	ε^2
ε^4	ε^5	ε^0	ε^1	ε^2	ε^3
ε^5	ε^0	ε^1	ε^2	ε^3	ε^4

Gruppe der 6-ten Einheitswurzeln mit der primitiven Einheitswurzel ε

1	3	2	6	4	5
3	2	6	4	5	1
2	6	4	5	1	3
6	4	5	1	3	2
4	5	1	3	2	6
5	1	3	2	6	4

Prime Restklassengruppe mod 7 mit dem erzeugenden Element [3]

1	2	4	8	7	5
2	4	8	7	5	1
4	8	7	5	1	2
8	7	5	1	2	4
7	5	1	2	4	8
5	1	2	4	8	7

Prime Restklassengruppe mod 9 mit dem erzeugenden Element [2]

5. Man verwende Aufgabe 3.

6. $\mathfrak{Z}_{24} = \{a^0, a^1, \ldots, a^{23}\} = \langle a\rangle = \langle a^5\rangle = \langle a^7\rangle = \langle a^{11}\rangle = \langle a^{13}\rangle = \langle a^{17}\rangle = \langle a^{19}\rangle = \langle a^{23}\rangle$

$\mathfrak{Z}_{12} = \{a^0, a^2, \ldots, a^{22}\} = \langle a^2\rangle = \langle a^{10}\rangle = \langle a^{14}\rangle = \langle a^{22}\rangle$

$\mathfrak{Z}_8 = \{a^0, a^3, \ldots, a^{21}\} = \langle a^3\rangle = \langle a^9\rangle = \langle a^{15}\rangle = \langle a^{21}\rangle$

$\mathfrak{Z}_6 = \{a^0, a^4, \ldots, a^{20}\} = \langle a^4\rangle = \langle a^{20}\rangle$

$\mathfrak{Z}_4 = \{a^0, a^6, \ldots, a^{18}\} = \langle a^6\rangle = \langle a^{18}\rangle$

$\mathfrak{Z}_3 = \{a^0, a^8, a^{16}\} = \langle a^8\rangle = \langle a^{16}\rangle$

$\mathfrak{Z}_2 = \{a^0, a^{12}\} = \langle a^{12}\rangle$

$\mathfrak{Z}_1 = \{a^0\} = \langle a^0\rangle$.

7. Es sei $(k, n) = m$ und ohne Beschränkung der Allgemeinheit $k < n$. Nach F(6.8b) gibt es eine zyklische Gruppe $\mathfrak{Z}_n = \langle a\rangle$ der Ordnung n. Dann erzeugen nach S(6.11b) die Elemente a^m und a^k die gleiche Untergruppe:

$$\langle a^m\rangle = \langle a^k\rangle.$$

Daher ist $(a^k)^g = a^m$ mit geeignetem ganzzahligem g. Daraus folgt nach S(6.6) $m \equiv kg\ (n)$, also

$$m = kg + nh \text{ mit ganzzahligen } g \text{ und } h.$$

Zu § 7

1. $\mathfrak{H} = \{s_1\}$: $\mathfrak{S}_3 = s_1 \cup s_2 \cup \dots \cup s_6$.

$\mathfrak{H} = \{s_1, s_4\}$: $\mathfrak{S}_3 = \mathfrak{H} \cup s_2\mathfrak{H} \cup s_3\mathfrak{H} = \{s_1, s_4\} \cup \{s_2, s_6\} \cup \{s_3, s_5\}$
$= \mathfrak{H} \cup \mathfrak{H}s_2 \cup \mathfrak{H}s_3 = \{s_1, s_4\} \cup \{s_2, s_5\} \cup \{s_3, s_6\}$

$\mathfrak{H} = \{s_1, s_5\}$: $\mathfrak{S}_3 = \mathfrak{H} \cup s_2\mathfrak{H} \cup s_3\mathfrak{H} = \{s_1, s_5\} \cup \{s_2, s_4\} \cup \{s_3, s_6\}$
$= \mathfrak{H} \cup \mathfrak{H}s_2 \cup \mathfrak{H}s_3 = \{s_1, s_5\} \cup \{s_2, s_6\} \cup \{s_3, s_4\}$

$\mathfrak{H} = \{s_1, s_6\}$: $\mathfrak{S}_3 = \mathfrak{H} \cup s_2\mathfrak{H} \cup s_3\mathfrak{H} = \{s_1, s_6\} \cup \{s_2, s_5\} \cup \{s_3, s_4\}$
$= \mathfrak{H} \cup \mathfrak{H}s_2 \cup \mathfrak{H}s_3 = \{s_1, s_6\} \cup \{s_2, s_4\} \cup \{s_3, s_5\}$

$\mathfrak{H} = \{s_1, s_2, s_3\}$: $\mathfrak{S}_3 = \mathfrak{H} \cup s_4\mathfrak{H} = \{s_1, s_2, s_3\} \cup \{s_4, s_5, s_6\}$
$= \mathfrak{H} \cup \mathfrak{H}s_4 = \{s_1, s_2, s_3\} \cup \{s_4, s_5, s_6\}$

$\mathfrak{H} = \mathfrak{S}_3$: $\mathfrak{S}_3 = \mathfrak{S}_3$.

2. Es sei $\mathfrak{G}$ die prime Restklassengruppe mod 15; dann gilt:

$$\mathfrak{G} = \{[1], [4]\} \cup \{[2], [8]\} \cup \{[7], [13]\} \cup \{[11], [14]\}.$$

3. Es genügt nachzuweisen, daß die Elemente $a^0, a^1, \dots, a^{m-1}$ ein vollständiges Repräsentantensystem der Nebenklassen von $\mathfrak{H}$ in $\mathfrak{G}$ bilden, also

$$\mathfrak{G} = \mathfrak{H} \cup a\mathfrak{H} \cup a^2\mathfrak{H} \cup \dots \cup a^{m-1}\mathfrak{H}$$

gilt. Ein beliebiges Element $a^k \in \mathfrak{G}$ läßt sich aber wegen $k = mg + r$ mit $0 \leq r < m - 1$ schreiben in der Form

$$a^k = a^r a^{mg} \in a^r\mathfrak{H}.$$

Für den Modul $\mathfrak{G}$ der ganzen Zahlen erhält man wieder m als die Anzahl der Restklassen mod m

$$\mathfrak{G} = [0] \cup [1] \cup \dots \cup [m-1] = \langle m\rangle \cup 1 + \langle m\rangle \cup \dots \cup (m-1) + \langle m\rangle,$$

da ja m die kleinste positive Zahl des Untermoduls $\langle m\rangle$ ist.

4. Wir erklären in $\mathfrak{G}$ eine Beziehung mit Hilfe einer Untergruppe $\mathfrak{H}$ durch

$$a \sim b \text{ dann und nur dann, falls } a^{-1}b \in \mathfrak{H}.$$

Diese Beziehung ist eine Äquivalenzrelation, denn sie ist

1. reflexiv — wegen $a^{-1}a = e \in \mathfrak{H}$, also $a \sim a$;
2. symmetrisch, — da mit $a^{-1}b \in \mathfrak{H}$ auch $(a^{-1}b)^{-1} = b^{-1}a \in \mathfrak{H}$ gilt, also aus $a \sim b$ folgt $b \sim a$;
3. transitiv, — da mit $a^{-1}b \in \mathfrak{H}$ und $b^{-1}c \in \mathfrak{H}$ auch $(a^{-1}b)(b^{-1}c) = a^{-1}c \in \mathfrak{H}$ gilt, also aus $a \sim b$ und $b \sim c$ folgt $a \sim c$.

Diese Äquivalenzrelation liefert nach F(7.2) eine Klasseneinteilung von $\mathfrak{G}$ in Linksnebenklassen von $\mathfrak{H}$ in $\mathfrak{G}$. Sie stimmt mit der in S(7.3) geschilderten überein. Die Überlegung mit $ab^{-1} \in \mathfrak{H}$ verläuft entsprechend.

5. Es gilt $\mathfrak{O} = \mathfrak{O}_+ \bigcup A \cdot \mathfrak{O}_+$, wobei A eine orthogonale Matrix mit der Determinante -1 ist. Dazu ist zu zeigen, daß sich jede orthogonale Matrix B mit negativer Determinante als Produkt einer festen Matrix A dieser Art mit einer geeigneten Matrix C aus $\mathfrak{O}_+$ schreiben läßt. Wir wählen

$$A = \begin{pmatrix} 0 & 1 & & & 0 \\ 1 & 0 & & & \\ & & 1 & & \\ & & & \ddots & \\ 0 & & & & 1 \end{pmatrix};$$

offensichtlich ist $|A| = -1$ und $A = A^T = A^{-1}$. Aus $B = (b_{ik})$ bilden wir durch Vertauschung der ersten beiden Zeilen die Matrix

$$C = \begin{pmatrix} b_{21} & b_{22} & \cdots & b_{2n} \\ b_{11} & b_{12} & \cdots & b_{1n} \\ b_{31} & b_{32} & \cdots & b_{3n} \\ & & \vdots & \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix}$$

und erhalten $B = A \cdot C$. Wegen $AB = A\,AC = C$ ist C als Produkt orthogonaler Matrizen selbst orthogonal und hat nach Konstruktion die Determinante $+1$.

Für die geometrische Bedeutung dieses Sachverhaltes verweisen wir auf § 14.

6. Es sei $\mathfrak{G}$ eine Gruppe der Ordnung 4 und $a \in \mathfrak{G}$ ein Element höchster Ordnung. Diese muß nach dem Satz von LAGRANGE ein Teiler von 4, also 4 oder 2 sein (das Einselement e ist das einzige Element der Ordnung 1). Im ersten Falle ist $\mathfrak{G} \overset{\sim}{\longleftrightarrow} \mathfrak{Z}_4$. Im zweiten Falle haben alle Elemente außer e die Ordnung 2. Dies legt in der Strukturtafel bereits folgendes fest:

	e	a	b	c
e	e	a	b	c
a	a	e		
b	b		e	
c	c			e.

Unter Berücksichtigung von F(4.2) stellt man rasch fest, daß die angefangene Strukturtafel nur auf eine Weise (entsprechend $\mathfrak{Z}_4$) ausgefüllt werden kann.

Durch ähnliche Überlegungen zeigt man, daß für die Ordnung 6 nur die Strukturen der Gruppen $\mathfrak{Z}_6$ und $\mathfrak{S}_3$ in Frage kommen.

7. Die Behauptung ergibt sich unmittelbar durch Anwendung von F(7.9) auf die prime Restklassengruppe mod m.

Zu § 8

1. Die untere Zeile von s_i ist die i-te Spalte der Strukturtafel von $\mathfrak{G}$.

2. Man erhält die folgenden Zuordnungen:

$$f_1 \to s_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} \qquad f_4 \to s_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 5 & 1 & 3 & 2 \end{pmatrix}$$

$$f_2 \to s_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \end{pmatrix} \qquad f_5 \to s_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 6 & 2 & 1 & 3 \end{pmatrix}$$

$$f_3 \to s_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 6 & 4 & 5 \end{pmatrix} \qquad f_6 \to s_6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$

Zu § 9

1. (1), (123), (132), (12), (13), (23).

2. (134256), (14)(26)(35), (1246)(798), (137)(26)(598) mit den Ordnungen 6, 2, 12, 6.

3. Element der Ordnung 1: (1);

   Elemente der Ordnung 2: (12), (13), (14), (23), (24), (34), (12)(34), (13)(24), (14)(23);

   Elemente der Ordnung 3: (123), (132), (124), (142), (134), (143), (234), (243);

   Elemente der Ordnung 4: (1234), (1432), (1324), (1423), (1342), (1243).

4. Die durch s_1 und s_2 gegebenen Zuordnungsvorschriften sind unabhängig von der Reihenfolge ihrer Ausführung.

5. z^m ist genau für den Fall $(r, m) = 1$ bzw. $(r, m) = r$ zyklisch, also für $r = p$ für alle m.

   Beweis:

   Genau für $(r, m) = r$ ist m ein Vielfaches von r und damit $z^m = (1)$, also zyklisch.

   Genau für $(r, m) = 1$ ist nach F(6.11) z^m erzeugendes Element von $\langle z \rangle$. Es muß also mit z auch z^m die Ordnung r haben; dies tritt nach unserem Hinweis und F(9.3) dann und nur dann ein, wenn z^m selbst ein r-gliedriger Zyklus ist.

6. Es sei

$$s = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}, \qquad s_0 = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix} = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ k_1 & k_2 & \dots & k_n \end{pmatrix};$$

dann ist

$$s_0^{-1} s\, s_0 = \begin{pmatrix} j_1 j_2 \dots j_n \\ 1\ 2 \dots n \end{pmatrix} \begin{pmatrix} 1\ 2 \dots n \\ i_1 i_2 \dots i_n \end{pmatrix} \begin{pmatrix} i_1 i_2 \dots i_n \\ k_1 k_2 \dots k_n \end{pmatrix} = \begin{pmatrix} j_1 j_2 \dots j_n \\ k_1 k_2 \dots k_n \end{pmatrix}$$

7. (624315), (64)(35)(21), (4218)(756), (437)(28)(956).

Zu § 10

1. Die angegebenen Permutationen sind alle ungerade.

2. $s \cdot t = \begin{pmatrix} \dots i_\mu \dots i_\nu \dots \\ \dots j_\mu \dots j_\nu \dots \end{pmatrix} \begin{pmatrix} j_\mu\, j_\nu \\ j_\nu\, j_\mu \end{pmatrix} = \begin{pmatrix} \dots i_\mu \dots i_\nu \dots \\ \dots j_\nu \dots j_\mu \dots \end{pmatrix}$

3. Es genügt zu zeigen, daß jeder Multiplikation einer Permutation s mit einer Transposition t von rechts einer Vorzeichenänderung entspricht. Dazu stützt man sich auf Aufgabe 2 und weist nach, daß die dort beschriebene Vertauschung die Anzahl der Inversionen um eine ungerade Zahl ändert. Zur Vereinfachung der Fallunterscheidungen geben wir s in der Gestalt an

$$s = \begin{pmatrix} 1 & \dots & \mu & \dots & \nu & \dots & n \\ i_1 & \dots & i_\mu & \dots & i_\nu & \dots & i_n \end{pmatrix}.$$

Wir untersuchen zunächst das Spaltenpaar $\begin{pmatrix} \mu \\ i_\mu \end{pmatrix}, \begin{pmatrix} \nu \\ i_\nu \end{pmatrix}$.

Falls zwischen diesen Spalten Inversion besteht, wird sie durch Vertauschung von i_μ mit i_ν aufgehoben, sonst entsteht eine neue Inversion.

Die Anzahl der durch alle anderen Spaltenpaare gebildeten Inversionen von s wird durch die Vertauschung von i_μ mit i_ν nur um eine gerade Anzahl abgeändert. Dies läßt sich bereits durch Betrachtung der beiden Spaltenpaare

$$\begin{pmatrix} \xi \\ i_\xi \end{pmatrix}, \begin{pmatrix} \mu \\ i_\mu \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} \xi \\ i_\xi \end{pmatrix}, \begin{pmatrix} \nu \\ i_\nu \end{pmatrix}$$

mit beliebigem ξ, verschieden von μ und ν, nachweisen. Man muß dazu die Stellung der Spalte $\begin{pmatrix} \xi \\ i_\xi \end{pmatrix}$ sowie die Größenbeziehung zwischen i_ξ, i_μ und i_ν beachten.

4. Aus D(10.3) folgt unmittelbar $\operatorname{sgn}(s) = \operatorname{sgn}(s^{-1})$.

5. Man wende Aufgabe 4 und F(10.5) auf $s^{-1} s\, s_0$ an oder schließe mit S(9.6) und S(10.7).

Zu § 11

1. $\{(1)\}$

$$\left.\begin{array}{l}\{(1),(12)\}=\langle(12)\rangle\\ \{(1),(13)\}=\langle(13)\rangle\\ \{(1),(14)\}=\langle(14)\rangle\\ \{(1),(23)\}=\langle(23)\rangle\\ \{(1),(24)\}=\langle(24)\rangle\\ \{(1),(34)\}=\langle(34)\rangle\\ \{(1),(12)(34)\}=\langle(12)(34)\rangle\\ \{(1),(13)(24)\}=\langle(13)(24)\rangle\\ \{(1),(14)(23)\}=\langle(14)(23)\rangle\end{array}\right\}\overset{\sim}{\longleftrightarrow}\mathfrak{Z}_2$$

$$\left.\begin{array}{l}\{(1),(123),(132)\}=\langle(123)\rangle\\ \{(1),(124),(142)\}=\langle(124)\rangle\\ \{(1),(134),(143)\}=\langle(134)\rangle\\ \{(1),(234),(243)\}=\langle(234)\rangle\end{array}\right\}\overset{\sim}{\longleftrightarrow}\mathfrak{Z}_3$$

$$\left.\begin{array}{l}\{(1),(1234),(13)(24),(1432)\}=\langle(1234)\rangle\\ \{(1),(1324),(12)(34),(1423)\}=\langle(1324)\rangle\\ \{(1),(1342),(14)(23),(1243)\}=\langle(1342)\rangle\end{array}\right\}\overset{\sim}{\longleftrightarrow}\mathfrak{Z}_4$$

$$\{(1),(12)(34),(13)(24),(14)(23)\}=\langle(12)(34),(13)(24)\rangle=\mathfrak{B}_4$$

$$\left.\begin{array}{l}\{(1),(12),(34),(12)(34)\}=\langle(12),(34)\rangle\\ \{(1),(13),(24),(13)(24)\}=\langle(13),(24)\rangle\\ \{(1),(14),(23),(14)(23)\}=\langle(14),(23)\rangle\end{array}\right\}\overset{\sim}{\longleftrightarrow}\mathfrak{V}_4$$

$$\{(1),(12),(13),(23),(123),(132)\}=\langle(12),(13)\rangle=\mathfrak{S}_3$$

$$\left.\begin{array}{l}\{(1),(12),(14),(24),(124),(142)\}=\langle(12),(14)\rangle\\ \{(1),(13),(14),(34),(134),(143)\}=\langle(13),(14)\rangle\\ \{(1),(23),(24),(34),(234),(243)\}=\langle(23),(24)\rangle\end{array}\right\}\overset{\sim}{\longleftrightarrow}\mathfrak{S}_3$$

$$\left.\begin{array}{l}\{(1),(13),(24),(12)(34),(13)(24),(14)(23),(1234),(1432)\}\\ \qquad=\langle(13),(14)(23)\rangle\\ \{(1),(12),(34),(12)(34),(13)(24),(14)(23),(1324),(1423)\}\\ \qquad=\langle(12),(13)(24)\rangle\\ \{(1),(14),(23),(12)(34),(13)(24),(14)(23),(1243),(1342)\}\\ \qquad=\langle(14),(12)(34)\rangle\end{array}\right\}\text{ Zueinander isomorph}$$

$$\left\{\begin{array}{l}(1),(12)(34),(13)(24),(14)(23),\\ (123),(132),(134),(143),(234),(243),(124),(142)\end{array}\right\}=\langle(123),(124)\rangle=\mathfrak{A}_4$$

$$\{(1),\ldots,(1243)\}=\langle(12),(13),(14)\rangle=\mathfrak{S}_4.$$

Wir führen den Vollständigkeitsbeweis nach steigender Untergruppenordnung n und stützen uns insbesondere auf den Satz von LAGRANGE. Für $n=1$, $n=2$, $n=3$ sind mit den angegebenen zyklischen Gruppen offensichtlich alle Möglichkeiten erschöpft. Desgleichen haben wir bei $n=4$ alle möglichen zyklischen Untergruppen angegeben, andere Untergruppen der Ordnung 4 können neben (1) nur Elemente der Ordnung 2 enthalten. Man überprüft leicht, daß sämtliche Kombinationsmöglichkeiten erschöpft sind.

Zyklische Gruppen mit größerer Ordnung kann es nicht geben.

Untergruppen der Ordnung 6 können nicht nur aus geraden Permutationen bestehen. Wegen der Inversenbildung müssen nämlich Dreierzyklen immer paarweise auftreten. Würde nun eine Untergruppe der Ordnung 6 vier Dreierzyklen enthalten, die wir ohne Beschränkung der Allgemeinheit (Ziffernvertauschung!) als (123), (132), (124), (142) annehmen können, so wären nach S(11.6) bereits alle Elemente der $\mathfrak{A}_4$ enthalten. Es bleibt damit nur die Möglichkeit, daß sie

$$(1),\ (12)(34),\ (13)(24),\ (14)(23)$$

und zwei Dreierzyklen enthält. Das wäre aber eine Gruppe der Ordnung 6, die die $\mathfrak{B}_4$ von der Ordnung 4 als Untergruppe hätte.

Untergruppen der Ordnung 6 müssen also drei ungerade Permutationen enthalten. Viererzyklen können es wegen der Ordnung nicht sein. Sie müssen also drei verschiedene Transpositionen enthalten. Damit entsteht aber nach S(11.5) entweder die $\mathfrak{S}_4$ oder eine zu $\mathfrak{S}_3$ isomorphe Gruppe. Von letzteren gibt es aber nach S(11.1) genau vier Stück.

Untergruppen der Ordnung 8 müssen aus vier geraden und vier ungeraden Permutationen bestehen. Andernfalls hätte nämlich die $\mathfrak{A}_4$ von der Ordnung 12 eine Untergruppe von der Ordnung 8. Die geraden Elemente müssen die der $\mathfrak{B}_4$ sein, weil ein Dreierzyklus die Ordnung 3 hat. Nehmen wir als ungerade Permutation einen Viererzyklus hinzu, entsteht stets eine der drei angegebenen Gruppen. Andernfalls müßten wir vier Transpositionen dazu nehmen, was aber stets die $\mathfrak{S}_4$ ergeben würde.

Für $n = 12$ genügt der Nachweis, daß nur gerade Permutationen auftreten können. Andernfalls würde nämlich eine Untergruppe $\mathfrak{H}$ sechs gerade und sechs ungerade Permutationen enthalten, deren Durchschnitt mit $\mathfrak{A}_4$ eine Untergruppe von $\mathfrak{S}_4$ aus sechs geraden Permutationen ergäbe, im Widerspruch zu unserer obigen Feststellung.

2. $(1) = (123)^3$ $\quad (124) = (124)$
$(12)(34) = (123)(124)^2(123)$ $\quad (142) = (124)^2$
$(13)(24) = (124)(123)$ $\quad (134) = (123)^2(124)$
$(14)(23) = (123)(124)$ $\quad (143) = (124)^2(123)$
$(123) = (123)$ $\quad (234) = (123)(124)^2$
$(132) = (123)^2$ $\quad (243) = (124)(123)^2$

3. Da die Menge der Elemente $s \in \mathfrak{S}_a$ mit $\operatorname{sgn}(s) = +1$ unendlich ist, haben wir gemäß S(5.5) nachzuprüfen, daß sowohl die Produkt- als auch die Inversenbildung nicht aus dieser Menge herausführt. Dafür können wir uns aber auf F(10.5) und Aufgabe 4 von §10 berufen, indem wir in einer symmetrischen Gruppe $\mathfrak{S}_n$ mit hinreichend hohem n arbeiten.

Zu § 12

1. Transitiv sind folgende Untergruppen: $\mathfrak{B}_4$, die zyklischen Untergruppen der Ordnung 4, die Untergruppen der Ordnung 8, $\mathfrak{A}_4$ und $\mathfrak{S}_4$.

   Die Transitivitätsgebiete der übrigen Gruppen geben wir nur durch charakteristische Beispiele an:

$\{(1)\}$	$\mathfrak{M} = \{1\} \cup \{2\} \cup \{3\} \cup \{4\}$
$\{(1), (12)\}$	$\mathfrak{M} = \{1, 2\} \cup \{3\} \cup \{4\}$
$\{(1), (12)(34)\}$	$\mathfrak{M} = \{1, 2\} \cup \{3, 4\}$
$\{(1), (123), (132)\}$	$\mathfrak{M} = \{1, 2, 3\} \cup \{4\}$
$\{(1), (12), (34), (12)(34)\}$:	$\mathfrak{M} = \{1, 2\} \cup \{3, 4\}$
$\mathfrak{S}_3$	$\mathfrak{M} = \{1, 2, 3\} \cup \{4\}$

2. Der Beweis wurde für den Spezialfall $\mathfrak{P} = \mathfrak{S}_n$ und $\mathfrak{M} = \{1, 2, \ldots, n\}$ bereits geführt (vgl. S(11.1)). Der hier verlangte Beweis beruht auf den gleichen Schlüssen:
   a) $\mathfrak{H} \cdot \mathfrak{H} \subseteq \mathfrak{H}$ genügt als Kriterium,
   b) aus $s_1(a) = a$, $s_2(a) = a$ folgt $[s_1 \cdot s_2](a) = a$.

3. Mit $s = (14)$ bzw. $s = (24)$ bzw. $s = (34)$ erhält man

$$\mathfrak{H}_1 = (14)^{-1}\,\mathfrak{H}_4\,(14) = \{(1), (42), (43), (23), (423), (432)\}$$
$$\mathfrak{H}_2 = (24)^{-1}\,\mathfrak{H}_4\,(24) = \{(1), (14), (13), (43), (143), (134)\}$$
$$\mathfrak{H}_3 = (34)^{-1}\,\mathfrak{H}_4\,(34) = \{(1), (12), (14), (24), (124), (142)\}.$$

4. Es ist $\mathfrak{S}_4 = \mathfrak{H}_4 \cup \mathfrak{H}_4\,(14) \cup \mathfrak{H}_4\,(24) \cup \mathfrak{H}_4\,(34)$ mit den Elementen

	(1)	(14)	(24)	(34)
	(12)	(124)	(142)	(12)(34)
	(13)	(134)	(13)(24)	(143)
	(23)	(14)(23)	(234)	(243)
	(123)	(1234)	(1423)	(1243)
	(132)	(1324)	(1342)	(1432),
wobei	$4 \to 4$	$4 \to 1$	$4 \to 2$	$4 \to 3$.

   Ferner gilt $(\mathfrak{S}_4 : \mathfrak{H}_4) = 4$ in Übereinstimmung mit der Anzahl der Elemente von $\mathfrak{M} = \{1, 2, 3, 4\}$.

5. Außer der bereits im Text behandelten Gruppe $\mathfrak{B}_4$ sind die drei zyklischen Untergruppen der Ordnung 4 und die drei Untergruppen der Ordnung 8 imprimitiv, jeweils mit den nichttrivialen Primitivitätsgebieten $\{1, 3\}$, $\{2, 4\}$ für die erste und $\{1, 2\}$, $\{3, 4\}$ für die zweite sowie $\{1, 4\}$, $\{2, 3\}$ für die dritte der in den Lösungen zu Aufgabe 1 von § 11 angegebenen Gruppen. Die beiden anderen transitiven Untergruppen $\mathfrak{A}_4$ und $\mathfrak{S}_4$ sind primitiv (vgl. Text nach D(12.11)).

6. Wir vermerken nur zur Orientierung, daß die angegebene Gruppe zur symmetrischen Gruppe $\mathfrak{S}_3$ isomorph ist.

   Die Transitivität ist klar, da z. B. die 1 in jedes andere Element von $\mathfrak{M}$ übergeführt wird. Außer dem trivialen Fall $\mathfrak{M}_1 = \mathfrak{M}$ existieren folgende Klasseneinteilungen von $\mathfrak{M}$ in Primitivitätsgebiete:

   $\mathfrak{M}_1 = \{1, 2\}$ oder $\{3, 4\}$ oder $\{5, 6\}$: $\mathfrak{M} = \{1, 2\} \cup \{3, 4\} \cup \{5, 6\}$
   $\mathfrak{M}_1 = \{1, 3\}$ oder $\{2, 5\}$ oder $\{4, 6\}$: $\mathfrak{M} = \{1, 3\} \cup \{2, 5\} \cup \{4, 6\}$
   $\mathfrak{M}_1 = \{1, 6\}$ oder $\{2, 4\}$ oder $\{3, 5\}$ $\mathfrak{M} = \{1, 6\} \cup \{2, 4\} \cup \{3, 5\}$
   $\mathfrak{M}_1 = \{1, 4, 5\}$ oder $\{2, 3, 6\}$: $\mathfrak{M} = \{1, 4, 5\} \cup \{2, 3, 6\}$

7. Zu $\{1, 2\}$ bzw. $\{4, 6\}$ bzw. $\{3, 5\}$ gehört $\mathfrak{H} = \{(1), (12)(35)(46)\}$, $(\mathfrak{P}:\mathfrak{H}) = 3$.
   Zu $\{3, 4\}$ bzw. $\{2, 5\}$ bzw. $\{1, 6\}$ gehört $\mathfrak{H} = \{(1), (16)(25)(34)\}$, $(\mathfrak{P}:\mathfrak{H}) = 3$.
   Zu $\{5, 6\}$ bzw. $\{1, 3\}$ bzw. $\{2, 4\}$ gehört $\mathfrak{H} = \{(1), (13)(24)(56)\}$, $(\mathfrak{P}:\mathfrak{H}) = 3$.
   Zu $\{1, 4, 5\}$ gehört
   Zu $\{2, 3, 6\}$ gehört
   $\mathfrak{H} = \{(1), (145)(236), (154)(263)\}$, $(\mathfrak{P}:\mathfrak{H}) = 2$.

8. Die Stabilitätsuntergruppen aller sechs Elemente sind sämtlich gleich der Gruppe $\mathfrak{E} = \{(1)\}$. Aus der Isomorphie von $\mathfrak{P}$ zu $\mathfrak{S}_3$ folgt, daß oben alle nur möglichen Zwischengruppen und die ihnen zugeordneten Primitivitätsgebiete auftreten.

9. Es bestehe das Primitivitätsgebiet $\mathfrak{M}_1$ aus m Elementen. Dann enthält auch $h(\mathfrak{M}_1)$ genau m Elemente wegen der Eineindeutigkeit der durch h gelieferten Abbildung. Aus $h(\mathfrak{M}_1) \subseteq \mathfrak{M}_1$ ergibt sich damit $h(\mathfrak{M}_1) = \mathfrak{M}_1$.

10. Die Stabilitätsuntergruppen der einzelnen Elemente sind:

$$\mathfrak{H}_1 = \mathfrak{H}_3 = \{(1), (24)\}, \mathfrak{H}_2 = \mathfrak{H}_4 = \{(1), (13)\}.$$

    Als einzige echte Zwischengruppe kommt nur

$$\mathfrak{H} = \{(1), (13), (24), (13)(24)\}$$

    und diese für alle vier Stabilitätsuntergruppen gemeinsam in Frage. Sie erzeugt auch die bereits unter 5. angegebenen Primitivitätsgebiete $\{1, 3\}$ und $\{2, 4\}$.

11. Es ist $\mathfrak{S}_{n-1}$ die zum Element $n \in \mathfrak{M} = \{1, 2, \ldots, n\}$ gehörige Stabilitätsuntergruppe $\mathfrak{H}_n$ von $\mathfrak{S}_n$. Da $\mathfrak{S}_n$ primitiv über $\mathfrak{M}$ ist, existiert nach S(12.12) keine echte Zwischengruppe.

    Entsprechend schließt man mit $\mathfrak{A}_{n-1} = \mathfrak{H}_n$ von $\mathfrak{A}_n$.

Zu § 13

1. Falls nur ein Punkt fest bleibt, ist nichts zu beweisen. Mit zwei Punkten bleibt aber wegen der Starrheit von G die durch sie bestimmte Gerade fest. Würde noch ein weiterer nicht auf dieser Gerade liegender

Punkt fest bleiben, folgt nach der gleichen Überlegung, daß ganz G in Ruhe bleibt, also die identische Abbildung vorliegt.

2. Die Überlegungen verlaufen völlig parallel zu den in B(2.6) durchgeführten. Man erklärt zunächst das Produkt zweier Deckabbildungen von G als Nacheinanderausführung und zeigt, daß das Produkt eine eindeutig bestimmte Deckabbildung von G ist. Die Assoziativität entspricht dem eindeutigen Ergebnis dreier in fester Reihenfolge ausgeführter Deckabbildungen. Die Existenz der identischen und aller inversen Deckabbildungen ist nach den Ausführungen im Text klar.

3. Diese Gruppe besteht aus der identischen Abbildung und einer Umklappung, hat also die Struktur der $\mathfrak{Z}_2$.

4. Der Beweis ergibt sich sofort, wenn man die vier Eckpunkte des Rechteckes mit 1, 2, 3, 4 bezeichnet und die Permutationen betrachtet, die durch die vier möglichen Deckabbildungen vermittelt werden. Beim Quader denke man sich eine symmetrische Doppelpyramide eingezeichnet.

5. Die Diedergruppe $\mathfrak{D}_4$ ist isomorph zu jeder der drei in der $\mathfrak{S}_4$ enthaltenen Untergruppen der Ordnung 8. Man verdeutliche sich dies durch eine Zeichnung und geeignete Numerierung der Eckpunkte des Grundquadrates.

6. $\langle(1)\rangle$ entspricht der identischen Deckabbildung.

$\left.\begin{matrix}\langle(12)\rangle \\ \vdots \\ \langle(34)\rangle\end{matrix}\right\}$ entsprechen den sechs zyklischen Untergruppen der Ordnung 2, deren Elemente die Drehungen um die sechs zweizähligen Symmetrieachsen sind.

$\left.\begin{matrix}\langle(123)\rangle \\ \vdots \\ \langle(234)\rangle\end{matrix}\right\}$ entsprechen den vier zyklischen Untergruppen der Ordnung 3, deren Elemente die Drehungen um die vier dreizähligen Symmetrieachsen sind.

$\left.\begin{matrix}\langle(1234)\rangle \\ \langle(1324)\rangle \\ \langle(1342)\rangle\end{matrix}\right\}$ entsprechen den drei zyklischen Untergruppen der Ordnung 4, deren Elemente die Drehungen um die drei vierzähligen Symmetrieachsen sind.

$\left.\begin{matrix}\langle(12)(34)\rangle \\ \langle(13)(24)\rangle \\ \langle(14)(23)\rangle\end{matrix}\right\}$ entsprechen den Untergruppen der Ordnung 2 der eben aufgeführten drei zyklischen Gruppen der Ordnung 4.

Die $\mathfrak{V}_4$ und je eine der drei zu ihr isomorphen Untergruppen sind als Untergruppen je einer der drei Untergruppen der Ordnung 8 aufzufassen. Diese sind aber nach Aufgabe 5 isomorph zu $\mathfrak{D}_4$. Ihre Untergruppen lassen sich durch Auszeichnung eines der drei Kantenquadrate des Oktaeders leicht kennzeichnen. Die $\mathfrak{S}_3$ und die drei zu ihr isomorphen Untergruppen entsprechen denjenigen Untergruppen der Oktaedergruppe, die eine Würfeldiagonale fest lassen. Schließlich besteht die zur $\mathfrak{A}_4$ isomorphe Untergruppe aus allen Drehungen um dreizählige Symmetrieachsen sowie aus den Drehungen um $\frac{2\pi}{2}$ um vierzählige Symmetrieachsen.

7. Die Gruppe der Deckabbildungen eines Kegels ist eine unendliche zyklische Gruppe. Sie ist isomorph zu der Drehungsgruppe eines Kreises.

8. Diese Gruppen sind zueinander isomorph, da die genannten geometrischen Gebilde unter Entsprechung sämtlicher Symmetrien wechselseitig ineinander gezeichnet werden können.

9. Die Umklappungen haben unendlich viele Fixpunkte, die Drehungen genau einen, alle anderen nichtidentischen Deckabbildungen keinen Fixpunkt (vgl. auch 1.).

Zu § 14

1. Da eine Parallelverschiebung $\mathfrak{a}$ keinen Einfluß hat, genügt es, die Transformation $\bar{\mathfrak{x}} = \mathfrak{x}A$ zu betrachten.

   Fassen wir I als Determinante der Matrix

$$\begin{pmatrix} \mathfrak{x} \\ \mathfrak{y} \\ \mathfrak{z} \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{pmatrix}$$

   auf, ergibt sich die Behauptung unmittelbar aus:

$$\begin{pmatrix} \bar{\mathfrak{x}} \\ \bar{\mathfrak{y}} \\ \bar{\mathfrak{z}} \end{pmatrix} = \begin{pmatrix} \mathfrak{x}A \\ \mathfrak{y}A \\ \mathfrak{z}A \end{pmatrix} = \begin{pmatrix} \mathfrak{x} \\ \mathfrak{y} \\ \mathfrak{z} \end{pmatrix} A .$$

2. Berücksichtigt man, daß sich der Rauminhalt jedes Parallelepipeds aus solchen mit einem Eckpunkt im Ursprung kombinieren läßt, ergibt sich aus 1. unmittelbar: Transformationen $\bar{\mathfrak{x}} = \mathfrak{x}A + \mathfrak{a}$ mit unimodularen Matrizen A ergeben inhaltstreue affine Transformationen, und zwar liegt im Falle $|A| = +1$ eine „eigentlich" inhaltstreue Transformation vor, während im Falle $|A| = -1$ Orientierungswechsel eintritt.

Zu § 15

1. a) $\mathfrak{Z}_2$ hat nur den identischen Automorphismus. (Diese Gruppe ist, wie wir hier nur vermerken wollen, die einzige Gruppe mit dieser Eigenschaft; vgl. das genannte Lehrbuch von KUROSCH, S. 89.)

   b) $\mathfrak{Z}_{12} = \langle a \rangle$ besitzt folgende vier Automorphismen (vgl. B(15.4)):

$$\begin{array}{llll} a \to a, & a \to a^5, & a \to a^7, & a \to a^{11} \\ a^2 \to a^2, & a^2 \to a^{10}, & a^2 \to a^2, & a^2 \to a^{10} \\ a^3 \to a^3, & a^3 \to a^3, & a^3 \to a^9, & a^3 \to a^9 \\ \vdots & \vdots & \vdots & \vdots \end{array}$$

   c) Da erzeugendes Element stets wieder auf erzeugendes Element abgebildet werden muß, gibt es nur zwei Automorphismen von $\mathfrak{Z}_\infty = \langle a \rangle$:

$$\begin{array}{ll} a \to a, & a \to a^{-1} \\ a^i \to a^i, & a^i \to (a^{-1})^i = a^{-i} \\ \vdots & \vdots \end{array}$$

   Die Relationstreue folgt aus der Isomorphie von $\langle a \rangle$ und $\langle a^{-1} \rangle$ zum Modul der ganzen Zahlen.

2. Es bezeichne $\overline{a + bi} = a - bi$ das Bild von $a + bi$ beim Übergang zum konjugiert komplexen Wert. Dieser Übergang bewirkt offensichtlich eine eineindeutige Abbildung der genannten Gruppen auf sich. Die Relationstreue folgt unmittelbar aus den für komplexe Zahlen gültigen Rechenregeln.

3. Wir bezeichnen die eineindeutigen Abbildungen der additiven Gruppe $\mathfrak{G}$ der reellen Zahlen auf sich selbst, also die eineindeutigen Funktionen, deren Definitionsbereich und Wertevorrat aus allen reellen Zahlen besteht, mit $f(x)$. Unter diesen sind genau diejenigen Automorphismen von $\mathfrak{G}$, für die gilt:

$$f(a + b) = f(a) + f(b).$$

Es ist interessant, daß die stetigen Funktionen dieser Art genau alle durch den Koordinatenursprung gehenden Geraden darstellen. Aus der Relationstreue und der Stetigkeit folgt nämlich der Reihe nach:

$$f(0) = 0$$

$$r \cdot f(x) = f(r \cdot x) \text{ für alle reellen } r \text{ und } x$$

$$\lim_{h \to 0} \frac{f(x + h) - f(x)}{h} = \lim_{h \to 0} \frac{f(h \cdot 1)}{h} = f(1) \text{ unabhängig von } x.$$

Für die Existenz unstetiger Funktionen dieser Art vgl. etwa E. Kamke, Mengenlehre, Sammlung Göschen Bd. 999, Kap. IV, § 12.

4. Die Behauptung folgt aus der Tatsache, daß das Einselement von $\mathfrak{G}$ bei Automorphismen stets in sich selbst übergeführt wird.

5. Die Gruppe $\mathfrak{T}$ aller eineindeutigen Abbildungen von $\mathfrak{G}$ auf sich ist isomorph zur Gruppe $\mathfrak{S}_n$. Da das Einselement von $\mathfrak{G}$ bei einem Automorphismus in Ruhe bleibt, kann die Automorphismengruppe Φ von $\mathfrak{G}$ nach S(11.1) nur isomorph zu einer Untergruppe von $\mathfrak{S}_{n-1}$ sein.

6. Die Gruppe $\langle (13), (14)(23) \rangle$ hat vier innere Automorphismen, die von je zwei Gruppenelementen durch Transformation bestimmt werden.

	$a = (1)$ oder $a = (13)(24)$	$a = (13)$ oder $a = (24)$	$a = (12)(34)$ oder $a = (14)(23)$	$a = (1234)$ oder $a = (1432)$
$a^{-1}(1)a =$	(1)	(1)	(1)	(1)
$a^{-1}(13)a =$	(13)	(13)	(24)	(24)
$a^{-1}(24)a =$	(24)	(24)	(13)	(13)
$a^{-1}(12)(34)a =$	(12)(34)	(14)(23)	(12)(34)	(14)(23)
$a^{-1}(13)(24)a =$	(13)(24)	(13)(24)	(13)(24)	(13)(24)
$a^{-1}(14)(23)a =$	(14)(23)	(12)(34)	(14)(23)	(12)(34)
$a^{-1}(1234)a =$	(1234)	(1432)	(1432)	(1234)
$a^{-1}(1432)a =$	(1432)	(1234)	(1234)	(1432)

Die Gruppe der inneren Automorphismen ist isomorph zur Gruppe $\mathfrak{V}_4$.

Zu § 16

1. Die fünf Klassen konjugierter Elemente in $\langle (13), (14)(23) \rangle$ sind:

   (1)
   (13)(24)
   (12)(34), (14)(23)
   (13), (24)
   (1234), (1432)

   } Gleichartige Zyklendarstellung! } Gleiche Ordnung!

2. Dies folgt unmittelbar aus S(9.6), da die Gruppe $\mathfrak{S}_n$ alle Permutationen von n Zahlen enthält und damit der Übergang von

$$s = (i_1 i_2 \dots i_r)(j_1 j_2 \dots j_s) \dots$$

   zu beliebigem

$$s' = (i_1' i_2' \dots i_r')(j_1' j_2' \dots j_s') \dots$$

   durch Transformation mit

$$s_0 = \begin{pmatrix} i_1 & i_2 & \dots & i_r & j_1 & j_2 & \dots & j_s \\ i_1' & i_2' & \dots & i_r' & j_1' & j_2' & \dots & j_s' \end{pmatrix} \in \mathfrak{S}_n$$

   möglich ist. Eine echte Untergruppe braucht jedoch s_0 nicht zu enthalten; vgl. auch obiges Beispiel.

3. Es seien $\mathfrak{K}_1$ und $\mathfrak{K}_2$ die beiden fraglichen Klassen und $x_1 \in \mathfrak{K}_1$, $x_2 \in \mathfrak{K}_2$. Wir zeigen, daß $\mathfrak{K}_1 \cdot \mathfrak{K}_2$ mit $x_1 \cdot x_2$ auch alle zu $x_1 \cdot x_2$ konjugierten Elemente enthält. Das folgt aus

$$a^{-1}(x_1 \cdot x_2)\, a = (a^{-1} x_1 a) \cdot (a^{-1} x_2 a) \in \mathfrak{K}_1 \cdot \mathfrak{K}_2$$

   für alle $a \in \mathfrak{G}$.

4. Es sei $\mathfrak{K}$ eine Klasse konjugierter Elemente und $x \in \mathfrak{K}$. Wir zeigen, daß $\mathfrak{K}^{-1}$ mit x^{-1} auch alle zu x^{-1} konjugierten Elemente enthält. Es gilt nämlich für alle $a \in \mathfrak{G}$:

$$a^{-1}(x^{-1})\, a = (a^{-1} x a)^{-1} \in \mathfrak{K}^{-1}.$$

5. $\mathfrak{B}_{(1)} = \mathfrak{B}_{(13)(24)} = \langle (13), (14)(23) \rangle$
   $\mathfrak{B}_{(13)} = \mathfrak{B}_{(24)} = \{(1), (13)(24), (13), (24)\}$
   $\mathfrak{B}_{(12)(34)} = \mathfrak{B}_{(14)(23)} = \{(1), (13)(24), (12)(34), (14)(23)\}$
   $\mathfrak{B}_{(1234)} = \mathfrak{B}_{(1432)} = \{(1), (13)(24), (1234), (1432)\}$

6. Die Behauptung folgt nach S(16.7) und $\mathfrak{Z} \leqq \mathfrak{B}_x$ für jedes $x \in \mathfrak{G}$ durch zweimalige Anwendung des Satzes von LAGRANGE:

$$(\mathfrak{G} : \mathfrak{Z})\,(\mathfrak{Z} : \mathfrak{E}) = (\mathfrak{G} : \mathfrak{B}_x)\,(\mathfrak{B}_x : \mathfrak{E}) = (\mathfrak{G} : \mathfrak{B}_x)\,(\mathfrak{B}_x : \mathfrak{Z})\,(\mathfrak{Z} : \mathfrak{E}).$$

7. Aus $ax = xa$ für $a \in \mathfrak{Z}$ und alle $x \in \mathfrak{G}$ folgt sowohl $x = a^{-1} x a$ als auch $a = x^{-1} a x$.

8. Der Beweis folgt unmittelbar aus den Aufgaben 7 und 2.

9. Offenbar gilt $\lambda E \cdot X = X \cdot \lambda E$ für alle $X \in \mathfrak{G}$. Ist umgekehrt

$$A \cdot X = X \cdot A \text{ für alle } X \in \mathfrak{G},$$

so hat die Matrix A die angegebene Gestalt. Aus

$$\sum_h a_{ih} x_{hl} = \sum_k x_{ik} a_{kl} \quad \text{für alle } i, l$$

folgt nämlich durch Spezialisierungen von X in der Form

$$x_{jl} = \begin{cases} 1 \text{ für festes } j \text{ und } l \\ 0 \text{ sonst} \end{cases}$$

die Beziehung

$$a_{ij} = \begin{cases} a_{ll} \text{ für } i = j \\ 0 \text{ sonst.} \end{cases}$$

10. Nur zu sich selbst konjugiert sind:

$\mathfrak{E}$, $\mathfrak{B}_4$, $\mathfrak{A}_4$, $\mathfrak{S}_4$.

Zueinander konjugiert sind:

1. Die sechs zyklischen Gruppen, die von einer Transposition erzeugt werden.
2. Die drei weiteren Gruppen der Ordnung 2.
3. Die vier zyklischen Gruppen der Ordnung 3.
4. Die drei zyklischen Gruppen der Ordnung 4.
5. Die drei zur $\mathfrak{B}_4$ isomorphen Gruppen.
6. Die $\mathfrak{S}_3$ und die drei zu ihr isomorphen Gruppen.
7. Die drei Gruppen der Ordnung 8.

Es gibt also insgesamt 11 Klassen zueinander konjugierter Untergruppen. Keine dieser Klassen mit Ausnahme der nur aus $\mathfrak{S}_4$ bestehenden erschöpft mit ihren Elementen ganz $\mathfrak{S}_4$.

11. Man vergleiche S(12.5).

Zu § 17

1. In den ersten beiden Fällen wurde die Untergruppeneigenschaft schon in Aufgabe 16 von § 5 angegeben. Die Normalteilereigenschaft folgt nach S(17.2c) aus der Relation

$$|A^{-1}BA| = |A^{-1}|\,|B|\,|A| = |A^{-1}|\,|A|\,|B| = |B|,$$

die für alle $A \in \mathfrak{G}$ und sogar für beliebige quadratische Matrizen B gilt. Die Aussage über die dritte Menge ist unmittelbar klar und überdies nach Aufgabe 9 von § 16 ein Beispiel für die nachstehende Aufgabe.

2. Die Normalteilereigenschaft von $\mathfrak{Z}$ folgt unmittelbar aus der Definition des Zentrums: $a\mathfrak{Z} = \mathfrak{Z}a$ für alle $a \in \mathfrak{G}$. Die restliche Behauptung ergibt sich wegen $\mathfrak{Z} \subseteq \mathfrak{B}_x$ bzw. $\mathfrak{Z} \subseteq \mathfrak{B}_{\mathfrak{H}}$ nach S(17.4).

3. Es ist zunächst $\langle a\rangle x = x\langle a\rangle$ für alle $x \in \mathfrak{B}_a$ zu zeigen. Nach Definition von $\mathfrak{B}_a$ ist aber $ax = xa$ und damit $xa^{-1} = a^{-1}x$ für alle $x \in \mathfrak{B}_a$. Durch vollständige Induktion ergibt sich aus diesen beiden Gleichungen $a^n x = xa^n$ für alle $x \in \mathfrak{B}_a$ mit beliebigen ganzzahligen Exponenten n. Dann gilt aber erst recht $\langle a\rangle x = x\langle a\rangle$.

   Der zweite Teil der Behauptung folgt nach Definition von $\mathfrak{B}_\mathfrak{H}$, denn es gilt ja $x\mathfrak{H} = \mathfrak{H}x$ für alle $x \in \mathfrak{B}_\mathfrak{H}$.

4. Wir zeigen (vgl. S(17.2c)) $\sigma^{-1}\alpha\sigma \in \Phi'$ für alle $\sigma \in \Phi$ und einen beliebigen inneren Automorphismus $\alpha \in \Phi'$ mit $x^\alpha = a^{-1}xa$ für $x \in \mathfrak{G}$. Es ist nämlich:

$$x^{\sigma^{-1}\alpha\sigma} = \left((x^{\sigma^{-1}})^\alpha\right)^\sigma = \left(a^{-1}x^{\sigma^{-1}}a\right)^\sigma = (a^{-1})^\sigma \cdot (x^{\sigma^{-1}})^\sigma \cdot a^\sigma.$$

   Wegen $(a^{-1})^\sigma = (a^\sigma)^{-1}$ (Bild des Inversen = Inverses des Bildes) und $(x^{\sigma^{-1}})^\sigma = x$ (nach Definition des inversen Automorphismus) folgt daher:

$$x^{\sigma^{-1}\alpha\sigma} = (a^\sigma)^{-1}xa^\sigma.$$

   Dies ist aber wieder ein innerer Automorphismus, der durch Transformation von x mit $a^\sigma \in \mathfrak{G}$ entsteht.

5. Der genannte Durchschnitt ist wieder Untergruppe und besteht aus vollständigen Klassen konjugierter Gruppenelemente (vgl. Beweis zu S(17.5)).

6. Für jedes $h \in \mathfrak{H} \subseteq \mathfrak{G}$ gilt $h\mathfrak{N} = \mathfrak{N}h$, also ist erst recht $\mathfrak{H}\mathfrak{N} = \mathfrak{N}\mathfrak{H}$. Damit folgt die Behauptung nach S(5.11) (vgl. auch den Beweis von S(17.6), wo die Normalteilereigenschaft von $\mathfrak{N}_1$ beim Beweis der Untergruppeneigenschaft von $\mathfrak{N}_1\mathfrak{N}_2$ nicht eingeht).

7. Es sei $t = (i_1 i_2)$ eine beliebige Transposition aus $\mathfrak{S}_a$. Dann gilt

$$\mathfrak{S}_a = \mathfrak{A}_a \cup t\mathfrak{A}_a;$$

   denn jedes Element $s \in \mathfrak{S}_a$ mit $\operatorname{sgn}(s) = -1$ läßt sich schreiben in der Form

$$s = t^2 s = t(ts) \in t\mathfrak{A}_a.$$

   Wir bemerken noch, daß man natürlich die Normalteilereigenschaft von $\mathfrak{A}_a$ auch ohne Verwendung von F(17.3) etwa nach dem Kriterium S(17.2b) mit Hilfe von F(10.5) zeigen kann; die Aussage $(\mathfrak{S}_a : \mathfrak{A}_a) = 2$ ist aber auch für sich von Interesse (vgl. z. B. § 21).

Zu § 18

1. Die Zuordnung vermittelt nach Definition eine eindeutige Abbildung von $\mathfrak{G}$ auf $\overline{\mathfrak{G}}$. Sie ist eineindeutig, da aus $2a = 2b$ stets $a = b$ folgt. Die Relationstreue folgt aus dem Distributivgesetz für ganze Zahlen.

2. a) $\mathfrak{N} = \mathfrak{A}_n$;

   b) $\mathfrak{N}$ ist die Untergruppe der Matrizen A mit $|A| = 1$;

   c) $\mathfrak{N} = \langle 5\rangle$ bzw. $\mathfrak{N} = \langle m\rangle$.

3. Die behaupteten Isomorphien folgen daraus, daß man die Elemente von $\mathfrak{S}_3$ bzw. $\mathfrak{S}_2$ als vollständiges Repräsentantensystem von $\mathfrak{S}_4/\mathfrak{V}_4$ bzw. $\mathfrak{S}_4/\mathfrak{A}_4$ verwenden kann.

4. Mit den Bezeichnungen in § 17 gilt:

$$\mathfrak{G}/\mathfrak{N}_1 \xleftarrow{\sim} \mathfrak{G}/\mathfrak{N}_2 \xleftarrow{\sim} \mathfrak{G}/\mathfrak{N}_3 \xleftarrow{\sim} \mathfrak{Z}_2;\ \mathfrak{G}/\mathfrak{N}_4 \xleftarrow{\sim} \mathfrak{V}_4.$$

5. Jede Nebenklasse von $\mathfrak{G}_1$ nach $\mathfrak{G}_2$ besteht aus genau denjenigen von Null verschiedenen komplexen Zahlen $z = re^{i\varphi}$, die bei beliebigem Betrag r das gleiche Argument φ haben. In der GAUSSschen Zahlenebene liegen sie jeweils auf einer durch den Nullpunkt gehenden Geraden Die Multiplikation in der Faktorgruppe $\mathfrak{G}_1/\mathfrak{G}_2$ entspricht der Addition der Argumente.

   Die Nebenklassen von $\mathfrak{G}_2$ nach $\mathfrak{G}_3$ bestehen jeweils aus denjenigen Irrationalitäten, deren Quotient rational ist (insbesondere bilden die rationalen Zahlen selbst eine Nebenklasse). Die Zahlengerade wird von den Zahlen jeder Nebenklasse dicht, aber nicht stetig bedeckt.

6. Es handelt sich um den Restklassenmodul des Moduls der reellen Zahlen nach dem von 2π erzeugten zyklischen Untermodul. Als vollständiges Repräsentantensystem wählt man im allgemeinen alle reellen Zahlen x mit $0 \leq x < 2\pi$ oder teilweise auch mit $-\pi < x \leq \pi$.

   Bei allen Winkelfunktionen liefern Argumente, die in der gleichen Restklasse liegen, denselben Funktionswert; für die Funktionen tg x und ctg x gilt dies sogar bezüglich des Restklassenmoduls nach dem von π erzeugten Untermodul.

7. Die Behauptung folgt aus der Relationstreue der homomorphen Abbildung. Es ist nämlich das Bild $\overline{a^n}$ jedes a^n wegen $\overline{a^n} = \bar{a}^n$ eine Potenz von $\bar{a}$.

8. Nach S(6.7) ist jede endliche zyklische Gruppe der Ordnung n isomorph dem Restklassenmodul mod n und dieser homomorphes Bild des zu $\mathfrak{Z}_\infty$ isomorphen Moduls der ganzen Zahlen. Die Behauptung folgt damit aus F(18.6).

9. a) Jede der angegebenen Zuordnungen liefert tatsächlich einen Endomorphismus von $\mathfrak{Z}_n$; es handelt sich nämlich offensichtlich um eindeutige Abbildungen von $\mathfrak{Z}_n$ in $\mathfrak{Z}_n$, die relationstreu sind wegen

$$\overline{a^i \cdot a^j} = \overline{a^{i+j}} = a^{(i+j)\lambda} = a^{i\lambda} \cdot a^{j\lambda} = \overline{a^i} \cdot \overline{a^j}.$$

   b) Mehr als diese n Endomorphismen kann es aber nicht geben, da nach Aufg. 7 homomorphe Abbildungen einer zyklischen Gruppe bereits durch das Bild des erzeugenden Elementes festgelegt sind und mehr als n Bilder a^λ für a nicht zur Verfügung stehen.

10. Das Zentrum $\mathfrak{Z}$ enthält nach Definition genau die Elemente $a \in \mathfrak{G}$, die durch Transformation den identischen Automorphismus von $\mathfrak{G}$ bewirken. Wir zeigen zunächst, daß genau die Elemente jeder Nebenklasse

$\mathfrak{Z} \cdot b$ von $\mathfrak{G}$ nach $\mathfrak{Z}$ durch Transformation ein und denselben inneren Automorphismus von $\mathfrak{G}$ liefern. Es gilt nämlich für ein beliebiges $ab \in \mathfrak{Z} \cdot b$:

$$y = (ab)^{-1} x (ab) = b^{-1} (a^{-1} x a)\, b = b^{-1} x b \text{ für alle } x \in \mathfrak{G},$$

und umgekehrt folgt aus

$$b_1^{-1} x b_1 = b_2^{-1} x b_2 \text{ für alle } x \in \mathfrak{G}$$

wegen

$$b_2 b_1^{-1} x = x b_2 b_1^{-1} \text{ für alle } x \in \mathfrak{G},$$

daß $b_2 b_1^{-1} \in \mathfrak{Z}$ und damit nach F(7.4) b_1 und b_2 in derselben Nebenklasse von $\mathfrak{Z}$ in $\mathfrak{G}$ liegen. Somit ist eine eineindeutige Zuordnung aller voneinander verschiedenen Nebenklassen $\mathfrak{Z} \cdot b$ von $\mathfrak{G}$ nach $\mathfrak{Z}$ auf die Menge aller voneinander verschiedenen inneren Automorphismen $x^{\sigma_b} = b^{-1} x b$ (für alle $x \in \mathfrak{G}$) gegeben:

$$\sigma_b \to \mathfrak{Z} \cdot b.$$

Die Relationstreue dieser Zuordnung entspricht der Tatsache, daß sich sowohl die Nebenklassen als auch die Automorphismen repräsentantenweise multiplizieren:

$$\mathfrak{Z} b_1\, \mathfrak{Z} b_2 = \mathfrak{Z} b_1 b_2$$

$$x^{[\sigma_{b_1} \sigma_{b_2}]} = b_2^{-1} (b_1^{-1} x b_1)\, b_2 = (b_1 b_2)^{-1} x (b_1 b_2) = x^{\sigma_{b_1 b_2}}.$$

Zu § 19

1. Die vollständigen Originale $\mathfrak{R}$ der Untergruppen $\bar{\mathfrak{H}} \leqq \mathfrak{S}_3$ sind:

$$\begin{aligned}
&\bar{\mathfrak{H}} = \mathfrak{S}_3 \quad ; \ \mathfrak{R} = \mathfrak{S}_3 \cdot \mathfrak{V}_4 \quad = \mathfrak{S}_4 \\
&\bar{\mathfrak{H}} = \mathfrak{A}_3 \quad ; \ \mathfrak{R} = \mathfrak{A}_3 \cdot \mathfrak{V}_4 \quad = \mathfrak{A}_4 \\
&\bar{\mathfrak{H}} = \langle (12) \rangle ; \ \mathfrak{R} = \langle (12) \rangle \cdot \mathfrak{V}_4 = \langle (12), (13)(24) \rangle \\
&\bar{\mathfrak{H}} = \langle (13) \rangle ; \ \mathfrak{R} = \langle (13) \rangle \cdot \mathfrak{V}_4 = \langle (13), (14)(23) \rangle \\
&\bar{\mathfrak{H}} = \langle (23) \rangle ; \ \mathfrak{R} = \langle (23) \rangle \cdot \mathfrak{V}_4 = \langle (23), (12)(34) \rangle \\
&\bar{\mathfrak{H}} = \mathfrak{E} \quad ; \ \mathfrak{R} = \mathfrak{E} \cdot \mathfrak{V}_4 \quad = \mathfrak{V}_4.
\end{aligned}$$

Damit ist eine eineindeutige Zuordnung hergestellt zwischen allen Untergruppen der $\mathfrak{S}_3$ und sämtlichen Untergruppen von $\mathfrak{S}_4$, die $\mathfrak{V}_4$ enthalten.

2. Wegen S(5.10) bleibt nur die Normalteilereigenschaft von $\mathfrak{H} \cap \mathfrak{N}$ nachzuweisen. Mit jedem Element $x \in \mathfrak{H} \cap \mathfrak{N}$ ist auch $h^{-1} x h \in \mathfrak{H} \cap \mathfrak{N}$ für jedes $h \in \mathfrak{H}$; denn wegen $x \in \mathfrak{H}$ ist $h^{-1} x h \in \mathfrak{H}$, und da $\mathfrak{N}$ Normalteiler von $\mathfrak{G}$ ist, folgt aus $x \in \mathfrak{N}$ auch $h^{-1} x h \in \mathfrak{N}$, mithin wie behauptet $h^{-1} x h \in \mathfrak{H} \cap \mathfrak{N}$ (Kennzeichnung von Normalteilern nach S(17.2c)).

3. Man setze $\mathfrak{G} = \mathfrak{S}_4$, $\mathfrak{H} = \mathfrak{S}_3$ und $\mathfrak{N} = \mathfrak{V}_4$. Dann ist $\mathfrak{H} \cdot \mathfrak{N} = \mathfrak{S}_4$ und $\mathfrak{H} \cap \mathfrak{N} = \mathfrak{E}$. Also folgt nach dem 1. Isomorphiesatz:

$$\mathfrak{H}\mathfrak{N}/\mathfrak{N} = \mathfrak{S}_4/\mathfrak{V}_4 \xleftarrow{\sim} \mathfrak{S}_3 = \mathfrak{H}/\mathfrak{H} \cap \mathfrak{N}) .$$

4. Jede Untergruppe $\mathfrak{H}$ der Ordnung 4 von $\mathfrak{G} = \langle (13), (14)(23) \rangle$ ist Normalteiler von $\mathfrak{G}$ und enthält das Zentrum $\mathfrak{Z} = \langle (13)(24) \rangle$, das ebenfalls Normalteiler von $\mathfrak{G}$ ist. In Übereinstimmung mit dem 2. Isomorphiesatz gilt stets

$$(\mathfrak{G}/\mathfrak{Z})/(\mathfrak{H}/\mathfrak{Z}) \xleftarrow{\sim} \mathfrak{G}/\mathfrak{H} ;$$

denn sowohl $(\mathfrak{G}/\mathfrak{Z})/(\mathfrak{H}/\mathfrak{Z})$ als auch $\mathfrak{G}/\mathfrak{H}$ ist isomorph zur zyklischen Gruppe der Ordnung 2.

5. Es ist $(\mathfrak{H}\mathfrak{N}:\mathfrak{N}) \cdot (\mathfrak{N}:(\mathfrak{N} \cap \mathfrak{H})) = (\mathfrak{H}\mathfrak{N}:\mathfrak{H}) \cdot (\mathfrak{H}:(\mathfrak{N} \cap \mathfrak{H}))$. Aus dem 1. Isomorphiesatz folgt die Behauptung wegen $(\mathfrak{H}\mathfrak{N}:\mathfrak{N}) = (\mathfrak{H}:(\mathfrak{N} \cap \mathfrak{H}))$.

Zu § 20

1. Die Behauptung ergibt sich unmittelbar aus S(20.3), da die Faktorgruppe $\mathfrak{G}/\mathfrak{N}$ Primzahlordnung hat, also einfach ist.

2. Daß das Komplexprodukt je zweier der im Text genannten maximalen Normalteiler mit $\mathfrak{G}$ zusammenfällt, ergibt sich durch Ausrechnung. Als Beispiel für F(20.5) wählen wir:

$$\mathfrak{M}_1 = \{(1), (13)(24), (1234), (1432)\},$$
$$\mathfrak{M}_2 = \{(1), (13)(24), (13), (24)\},$$

also

$$\mathfrak{M}_1 \cap \mathfrak{M}_2 = \{(1), (13)(24)\},$$

und erhalten in der Tat

$$\mathfrak{G}/\mathfrak{M}_1 \xleftarrow{\sim} \mathfrak{M}_2/\mathfrak{M}_1 \cap \mathfrak{M}_2) ,$$

da beide Seiten isomorph zu $\mathfrak{Z}_2$ sind.

Zu § 21

1. Isomorphe Verfeinerungen sind etwa

$$\langle a \rangle \supset \langle a^2 \rangle \supset \langle a^{12} \rangle \supset \langle a^{60} \rangle \supset \mathfrak{E},$$
$$\langle a \rangle \supset \langle a^5 \rangle \supset \langle a^{10} \rangle \supset \langle a^{60} \rangle \supset \mathfrak{E};$$

ihre Faktoren haben nämlich (bis auf die Reihenfolge) die Struktur

$$\mathfrak{Z}_2, \mathfrak{Z}_6, \mathfrak{Z}_5, \mathfrak{Z}_\infty .$$

2. Durch $\mathfrak{Z}_8$: $\mathfrak{Z}_{24} \supset \mathfrak{Z}_8 \supset \mathfrak{Z}_4 \supset \mathfrak{Z}_2 \supset \mathfrak{E}$.

Durch $\mathfrak{Z}_6$: $\mathfrak{Z}_{24} \supset \mathfrak{Z}_{12} \supset \mathfrak{Z}_6 \supset \mathfrak{Z}_3 \supset \mathfrak{E}$ oder $\mathfrak{Z}_{24} \supset \mathfrak{Z}_{12} \supset \mathfrak{Z}_6 \supset \mathfrak{Z}_2 \supset \mathfrak{E}$.

Die Kompositionsfaktoren sind bis auf Isomorphie und Reihenfolge:

$$\mathfrak{Z}_3, \mathfrak{Z}_2, \mathfrak{Z}_2, \mathfrak{Z}_2 .$$

3. Es sei $\mathfrak{G}$ eine abelsche Gruppe mit einer Kompositionsreihe

$$\mathfrak{G} = \mathfrak{G}_0 > \mathfrak{G}_1 > \ldots > \mathfrak{G}_l = \mathfrak{E}.$$

Die Kompositionsfaktoren $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ sind als Faktorgruppen abelscher Gruppen abelsch, nach F(21.7) einfach und damit gemäß S(20.6) von endlicher Ordnung. Also sind sämtliche Indizes $(\mathfrak{G}_{\nu-1}:\mathfrak{G}_\nu)$ endlich. Ihr Produkt ist aber die Ordnung von $\mathfrak{G}$.

Zu § 22

1. Nach F(22.2) läßt sich jede Normalreihe von $\mathfrak{G}$ zu einer solchen mit abelschen Faktoren verfeinern, so daß also auch jede Kompositionsreihe von vornherein nur abelsche Kompositionsfaktoren hat.
Damit verläuft der Beweis weiter wie zu Aufgabe 3 von § 21.

2. Die Kompositionsfaktoren sind nach S(22.5) und S(22.3) zyklische Gruppen von Primzahlordnung; also tritt wegen $(\mathfrak{G}:\mathfrak{E}) = p^n$ genau n-mal der Kompositionsfaktor $\mathfrak{Z}_p$ auf.

Zu § 23

1. Nach unserer Definition ist

$$c_1 = aba^{-1}b^{-1} \text{ der Kommutator von } a^{-1} \text{ und } b^{-1},$$
$$c_2 = b^{-1}a^{-1}ba \text{ der Kommutator von } b \text{ und } a,$$
$$c_3 = bab^{-1}a^{-1} \text{ der Kommutator von } b^{-1} \text{ und } a^{-1}.$$

Es würde also jede dieser anderen im Prinzip möglichen Festlegungen des Kommutatorbegriffes zum gleichen Komplex $\mathfrak{C}$ aller Kommutatoren führen.

2. Zunächst ist $\mathfrak{A}_n$ Normalteiler in $\mathfrak{S}_n$ mit abelscher Faktorgruppe, also gilt $\mathfrak{S}_n' \subseteq \mathfrak{A}_n$ nach S(23.3). $\mathfrak{S}_n' \neq \mathfrak{E}$ ist wieder klar; also folgt $\mathfrak{S}_n' = \mathfrak{A}_n$, da weitere Normalteiler gemäß F(20.8) nicht existieren.

3. Da sämtliche Faktorgruppen von $\mathfrak{G}$ mit Ausnahme von $\mathfrak{G}/\mathfrak{E}$ abelsch sind, enthalten alle Normalteiler $\mathfrak{N}_i \neq \mathfrak{E}$ von $\mathfrak{G}$ die Kommutatorgruppe $\mathfrak{G}'$; also ist

$$\mathfrak{G}' = \{(1), (13)(24)\}.$$

4. Bereits in § 22 wurde festgestellt, daß $\mathfrak{D}_+$ Normalteiler in $\mathfrak{D}$ mit abelscher Faktorgruppe ist. Es ist also (nach S(23.3)) $\mathfrak{D}' \subseteq \mathfrak{D}_+$. Wir zeigen umgekehrt $\mathfrak{D}_+ \subseteq \mathfrak{D}'$.
Es läßt sich nämlich jedes Element $C \in \mathfrak{D}_+$ als Kommutator eines Elementes $U \in \mathfrak{D}$ und eines Elementes $D \in \mathfrak{D}_+ \subseteq \mathfrak{D}$ schreiben:

$$C = U^{-1}D^{-1}UD.$$

Dies ergibt sich aus folgendem geometrischem Sachverhalt: Führt man die Drehung D um den Winkel φ und eine beliebige, aber feste Umklappung U in verschiedener Reihenfolge nacheinander aus, so erhält

man als Abweichung C dieser beiden Abbildungen eine Drehung um den Winkel 2φ. Es läßt sich also jede vorgegebene Drehung auf diese Weise darstellen.

Unter Verwendung von

$$D = \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix} \quad \text{und} \quad U = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

entspricht dem die Rechnung

$$\begin{aligned} C &= U^{-1} D^{-1} U D \\ &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix} \\ &= \begin{pmatrix} \cos^2\varphi - \sin^2\varphi & 2\cos\varphi \cdot \sin\varphi \\ -2\cos\varphi \cdot \sin\varphi & \cos^2\varphi - \sin^2\varphi \end{pmatrix} \\ &= \begin{pmatrix} \cos 2\varphi & \sin 2\varphi \\ -\sin 2\varphi & \cos 2\varphi \end{pmatrix}. \end{aligned}$$

Der Rest der Behauptung ist trivial, da $\mathfrak{D}_+$ abelsch ist und somit $\mathfrak{D}'' = \mathfrak{D}' = \mathfrak{E}$ gilt.

5. Die Voraussetzungen von S(22.4) bedeuten nach S(23.8)

$$\mathfrak{N}^{(h)} = \mathfrak{E} \quad \text{und} \quad (\mathfrak{G}/\mathfrak{N})^{(k)} = \mathfrak{N}/\mathfrak{N}.$$

Zunächst folgt aus letzterem nach S(23.7b)

$$\mathfrak{G}^{(k)}\mathfrak{N}/\mathfrak{N} = \mathfrak{N}/\mathfrak{N} \quad \text{und damit} \quad \mathfrak{G}^{(k)}\mathfrak{N} = \mathfrak{N}.$$

Daher ist $\mathfrak{G}^k \leqq \mathfrak{N}$, mithin unter Verwendung von S(23.7a)

$$\mathfrak{G}^{(k+h)} \leqq \mathfrak{N}^{(h)} = \mathfrak{E}, \quad \text{also} \quad \mathfrak{G}^{(k+h)} = \mathfrak{E}.$$

ANHANG I

Zusammenstellung der verwendeten Begriffsbildungen aus der Mengenlehre

Mengenbildung

Unter einer Menge $\mathfrak{M}$ versteht man die Zusammenfassung verschiedener (mathematischer) Objekte zu einer Gesamtheit. Diese Objekte werden die Elemente der Menge genannt. Mit

$$a \in \mathfrak{M} \quad \text{bzw.} \quad a \notin \mathfrak{M}$$

bezeichnet man, daß a Element von $\mathfrak{M}$ ist bzw. daß a nicht Element von $\mathfrak{M}$ ist. Weiterhin bedeutet

$$\{a, b, \ldots\}$$

die aus den Elementen $a, b, \ldots$ bestehende Menge. Insbesondere versteht man unter der leeren Menge oder Nullmenge Ø eine Menge, die kein Element enthält.

Nach diesem sog. naiven Standpunkt ist also eine Menge bereits erklärt, wenn von jedem (in Frage kommenden) Objekt feststeht, ob es Element dieser Menge ist oder nicht. Allerdings müssen zur Vermeidung von Paradoxien die zur Auswahl stehenden Objekte bereits vor der Mengenbildung und unabhängig von dieser fixiert sein. Unter Beachtung dessen können die Objekte sogar ihrerseits Mengen sein, d. h. Mengen als Elemente von „Mengen höherer Stufe" aufgefaßt werden.

Beispiele wie etwa die Menge aller natürlichen Zahlen, aller Primzahlen oder aller geraden Zahlen usw. liegen unmittelbar auf der Hand. Zur Veranschaulichung mengentheoretischer Begriffsbildungen werden oft ebene Punktmengen innerhalb geschlossener Kurven verwendet.

Ober- und Untermengen

Eine Menge $\mathfrak{M}_1$ enthält oder umfaßt eine Menge $\mathfrak{M}_2$ (in Zeichen $\mathfrak{M}_1 \supseteq \mathfrak{M}_2$), wenn jedes Element von $\mathfrak{M}_2$ auch Element von $\mathfrak{M}_1$ ist. $\mathfrak{M}_2$ heißt dann entsprechend enthalten in $\mathfrak{M}_1$ ($\mathfrak{M}_2 \subseteq \mathfrak{M}_1$), und man nennt $\mathfrak{M}_2$ Teil- oder Untermenge von $\mathfrak{M}_1$, $\mathfrak{M}_1$ Ober-

menge von $\mathfrak{M}_2$. Die Nullmenge wird als Untermenge jeder Menge aufgefaßt.

Gilt sowohl $\mathfrak{M}_1 \supseteq \mathfrak{M}_2$ als auch $\mathfrak{M}_1 \subseteq \mathfrak{M}_2$, so enthalten beide Mengen die gleichen Elemente und werden als gleich bezeichnet. ($\mathfrak{M}_1 = \mathfrak{M}_2$, andernfalls $\mathfrak{M}_1 \neq \mathfrak{M}_2$).

Insbesondere spricht man bei $\mathfrak{M}_1 \supseteq \mathfrak{M}_2$ und $\mathfrak{M}_1 \neq \mathfrak{M}_2$ von echtem Enthaltensein und schreibt dafür $\mathfrak{M}_1 \supset \mathfrak{M}_2$. In diesem Falle gibt es also wenigstens ein Element a mit $a \in \mathfrak{M}_1$, aber $a \notin \mathfrak{M}_2$.

So ist z. B. die Menge der Primzahlen echte Untermenge der Menge der natürlichen Zahlen, während die Menge aller Lösungen der Gleichung $x^2 - 4 = 0$ und die Menge $\{2, -2\}$ gleich sind.

Vereinigung und Durchschnitt von Mengen

Die Vereinigungsmenge $\mathfrak{M}_1 \cup \mathfrak{M}_2$ zweier Mengen $\mathfrak{M}_1$ und $\mathfrak{M}_2$ besteht aus allen Elementen, die in $\mathfrak{M}_1$ oder in $\mathfrak{M}_2$, d. h. in (wenigstens) einer dieser Mengen enthalten sind.

Der Durchschnitt $\mathfrak{M}_1 \cap \mathfrak{M}_2$ zweier Mengen $\mathfrak{M}_1$ und $\mathfrak{M}_2$ besteht aus allen Elementen, die in $\mathfrak{M}_1$ und in $\mathfrak{M}_2$, d. h. in beiden Mengen enthalten sind.

Vereinigungs- und Durchschnittsbildung sind beide kommutativ und assoziativ und wechselseitig distributiv:

$$\mathfrak{M}_1 \cup \mathfrak{M}_2 = \mathfrak{M}_2 \cup \mathfrak{M}_1, \quad (\mathfrak{M}_1 \cup \mathfrak{M}_2) \cup \mathfrak{M}_3 = \mathfrak{M}_1 \cup (\mathfrak{M}_2 \cup \mathfrak{M}_3),$$
$$\mathfrak{M}_1 \cap \mathfrak{M}_2 = \mathfrak{M}_2 \cap \mathfrak{M}_1, \quad (\mathfrak{M}_1 \cap \mathfrak{M}_2) \cap \mathfrak{M}_3 = \mathfrak{M}_1 \cap (\mathfrak{M}_2 \cap \mathfrak{M}_3),$$
$$\mathfrak{M}_1 \cap (\mathfrak{M}_2 \cup \mathfrak{M}_3) = (\mathfrak{M}_1 \cap \mathfrak{M}_2) \cup (\mathfrak{M}_1 \cap \mathfrak{M}_3,$$
$$\mathfrak{M}_1 \cup (\mathfrak{M}_2 \cap \mathfrak{M}_3) = (\mathfrak{M}_1 \cup \mathfrak{M}_2) \cap (\mathfrak{M}_1 \cup \mathfrak{M}_3).$$

Weiterhin gilt:

$$\mathfrak{M}_1 \cup \mathfrak{M}_2 \supseteq \mathfrak{M}_1, \quad \mathfrak{M}_1 \cup \mathfrak{M}_2 \supseteq \mathfrak{M}_2;$$
$$\mathfrak{M}_1 \cap \mathfrak{M}_2 \subseteq \mathfrak{M}_1, \quad \mathfrak{M}_1 \cap \mathfrak{M}_2 \subseteq \mathfrak{M}_2),$$
$$\mathfrak{M}_1 \cup \mathfrak{M}_2 = \mathfrak{M}_1 \text{ genau dann, wenn } \mathfrak{M}_2 \subseteq \mathfrak{M}_1;$$
$$\mathfrak{M}_1 \cap \mathfrak{M}_2 = \mathfrak{M}_1 \text{ genau dann, wenn } \mathfrak{M}_2 \supseteq \mathfrak{M}_1.$$

Insbesondere heißen zwei Mengen $\mathfrak{M}_1$ und $\mathfrak{M}_2$ disjunkt oder elementfremd, wenn ihr Durchschnitt leer ist: $\mathfrak{M}_1 \cap \mathfrak{M}_2 = \emptyset$.

Zur Veranschaulichung diene die Vereinigung bzw. der Durchschnitt zweier ebener Punktmengen:

Abb. 13

Differenzmenge

Die Differenzmenge $\mathfrak{M}_1 \setminus \mathfrak{M}_2$ enthält genau die Elemente von $\mathfrak{M}_1$, die nicht in $\mathfrak{M}_2$ liegen.

Veranschaulichung:

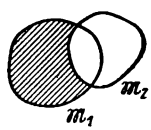


Abb. 14

Produktmenge

Unter der Produktmenge $\mathfrak{M}_1 \times \mathfrak{M}_2$ zweier Mengen $\mathfrak{M}_1$ und $\mathfrak{M}_2$ versteht man die Menge aller geordneten Elementenpaare (a_1, a_2) mit $a_1 \in \mathfrak{M}_1$, $a_2 \in \mathfrak{M}_2$. Dabei sind natürlich alle Paare (a_1, a_2) und (b_1, b_2) als voneinander verschieden zu betrachten, falls nicht $a_1 = b_1$ und $a_2 = b_2$ gilt.

Diese Begriffsbildung liegt z. B. den bekannten Erweiterungskonstruktionen von Zahlenbereichen mit Hilfe von Zahlenpaaren zugrunde. Desgleichen kann man die Punkte einer Ebene als die Produktmenge der von den beiden Achsen gebildeten Punktmenge ansehen.
Insbesondere gestattet sie eine präzise Fassung des Begriffes der algebraischen Operation bzw. Verknüpfung in einer Menge $\mathfrak{M}$ als einer eindeutigen Abbildung von $\mathfrak{M} \times \mathfrak{M}$ in $\mathfrak{M}$ (vgl. weiter unten).

Äquivalenzrelation und Klasseneinteilung

Zwischen den Elementen einer Menge $\mathfrak{M}$ bestehe eine Beziehung $\sim$ derart, daß für je zwei Elemente a und b aus $\mathfrak{M}$ entweder $a \sim b$ oder $a \nsim b$ gilt. Eine solche Beziehung heißt eine Äquivalenzrelation in $\mathfrak{M}$, wenn sie reflexiv ($a \sim a$), symmetrisch (aus $a \sim b$ folgt $b \sim a$) und transitiv (aus $a \sim b$ und $b \sim c$ folgt $a \sim c$) ist.

Faßt man jeweils zueinander äquivalente Elemente von $\mathfrak{M}$ zu Untermengen zusammen, erhält man eine Klasseneinteilung von $\mathfrak{M}$, d. h. eine Aufteilung aller Elemente von $\mathfrak{M}$ in nichtleere, elementfremde, als Klassen bezeichnete Untermengen.

Beweis: Es bezeichne $[a]$ die Untermenge aller zu $a \in \mathfrak{M}$ äquivalenten Elemente von $\mathfrak{M}$. Diese Untermengen sind wegen $a \sim a$, also $a \in [a]$, nicht leer und erschöpfen ganz $\mathfrak{M}$. Es bleibt zu zeigen, daß diese Untermengen zueinander elementfremd sind, d. h. entweder $[a] = [b]$ oder $[a] \cap [b] = \emptyset$ gilt. Entweder ist das letztere der Fall, oder es gibt ein Element $c \in \mathfrak{M}$ mit $c \in [a]$ und $c \in [b]$, also $c \sim a$ und $c \sim b$, woraus man unter Verwendung der Symmetrie und Transitivität $a \sim b$ schließt. Dann ist aber jedes Element $x \in [a]$ wegen $x \sim a$, also $x \sim b$ auch Element von $[b]$ und umgekehrt jedes Element $y \in [b]$ wegen $y \sim b$, also $y \sim a$, auch Element von $[a]$, d. h. $[a] = [b]$.

Umgekehrt erhält man aus jeder solchen Klasseneinteilung von $\mathfrak{M}$ eine Äquivalenzrelation, indem man genau die in einer Klasse liegenden Elemente als zueinander äquivalent bezeichnet.

Beweis: Wegen der Elementfremdheit der Klassen, die ganz $\mathfrak{M}$ erschöpfen, steht von je zwei Elementen a und b aus $\mathfrak{M}$ fest, daß entweder $a \sim b$ oder $a \nsim b$ gilt. Der Reflexivität, Symmetrie und Transitivität dieser Beziehung entsprechen dann die folgenden trivialen Aussagen:

Jedes a liegt in der Klasse, in der es liegt.

Wenn a in der gleichen Klasse liegt wie b, so auch b in der gleichen Klasse wie a.

Wenn a in der gleichen Klasse wie b und b in der gleichen Klasse wie c liegt, so auch a in der gleichen Klasse wie c.

Unter einem vollständigen Repräsentantensystem für eine Klasseneinteilung einer Menge $\mathfrak{M}$ versteht man eine Untermenge von $\mathfrak{M}$, die aus jeder Klasse genau ein Element enthält.

Die naheliegendste Äquivalenzrelation ist die Gleichheit im Sinne der Identität; bei der zugehörigen Klasseneinteilung besteht jede Klasse nur aus einem Element.

Weiterhin ist die Einteilung aller ganzen Zahlen in gerade und ungerade Zahlen eine Klasseneinteilung, die zugehörige Äquivalenzrelation wird als Kongruenz modulo 2 bezeichnet. Als vollständiges Repräsentantensystem können etwa die Zahlen 0 und 1 dienen.

Weitere Beispiele für Äquivalenzrelationen sind etwa die geometrischen Kongruenzen ebener Figuren, die Ähnlichkeit, die Affinität usw.

Abbildung von Mengen

Eine eindeutige Abbildung f einer Menge $\mathfrak{M}_1$ in eine Menge $\mathfrak{M}_2$ ordnet jedem Element a_1 aus $\mathfrak{M}_1$ als Original genau ein Element $a_2 = f(a_1)$ aus $\mathfrak{M}_2$ als Bild zu. Dabei ist es zugelassen, daß einerseits mehrere Originale das gleiche Bild haben und andererseits die Menge $f(\mathfrak{M}_1)$ aller Bilder eine echte Untermenge von $\mathfrak{M}_2$ ist.

Eine Abbildung von $\mathfrak{M}_1$ in $\mathfrak{M}_2$ heißt eineindeutig (umkehrbar eindeutig), wenn jedem Bild genau ein Original entspricht.

Insbesondere spricht man von eindeutigen bzw. eineindeutigen Abbildungen von $\mathfrak{M}_1$ auf $\mathfrak{M}_2$, wenn $f(\mathfrak{M}_1) = \mathfrak{M}_2$ ist, also jedes Element von $\mathfrak{M}_2$ als Bild eines Elementes aus $\mathfrak{M}_1$ auftritt.

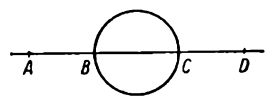


Abb. 15

Die vier Kombinationsmöglichkeiten dieser Begriffe lassen sich an der nebenstehenden Figur veranschaulichen. Durch senkrechte Parallelprojektion erhält man eine eindeutige (aber nicht eineindeutige) Abbildung des Kreises auf den Durchmesser BC bzw. in die Strecke AD und eine eineindeutige Abbildung etwa des oberen Halbkreises auf BC bzw. in AD.

Gleichmächtigkeit und Kardinalzahlen

Man nennt zwei Mengen $\mathfrak{M}_1$ und $\mathfrak{M}_2$ gleichmächtig, wenn sie eineindeutig aufeinander abgebildet werden können. Die Gleichmächtigkeit ist reflexiv, symmetrisch und transitiv, also eine Äquivalenzrelation. Die Klassen der ihr entsprechenden Klasseneinteilung werden Kardinalzahlen genannt und jeweils durch einen beliebigen Vertreter, d. h. durch eine Menge der entsprechenden Mächtigkeit repräsentiert.

Insbesondere heißt eine Menge endlich, wenn sie einem Abschnitt der Menge der natürlichen Zahlen (d. h. allen natürlichen Zahlen, die kleiner als eine feste natürliche Zahl sind) gleichmächtig ist. Für endliche Mengen entspricht der Kardinalzahlbegriff dem üblichen Begriff der Anzahl der Elemente dieser Menge. Die nicht endlichen Kardinalzahlen werden auch transfinite Kardinalzahlen genannt. Unter ihnen ist von besonderer Wichtigkeit die Klasse der zur Menge der natürlichen Zahlen gleichmächtigen Mengen, die man abzählbare Mengen nennt. Als Beispiel für eine überabzählbare Menge erwähnen wir nur die Menge der reellen Zahlen.

ANHANG II

Einige Bemerkungen zu Bezeichnungsfragen

a) *Additive Schreibweise von nichtabelschen Gruppen*

In der genannten Einführung in die Gruppentheorie von P. S. ALEXANDROFF wird entgegen dem im allgemeinen üblichen Gebrauch die additive Schreibweise konsequent auch für nichtabelsche Gruppen angewendet.

b) *Multiplikation von Transformationen, insbesondere Permutationen*

Wir haben das Produkt von Transformationen in B(2.6) in der Schreibweise

$$[s_1 \cdot s_2]\,(a) = s_2\,(s_1\,(a))$$

eingeführt. Diese hat den Vorteil, daß bei der Produktbildung $s_1 s_2$ die zuerst anzuwendende Transformation als erster Faktor steht, wofür der Nachteil entsteht, daß in der angegebenen Formel die Reihenfolge auf der rechten Seite vertauscht wird.

Es ist oft üblich, in einer anderen Weise zu verfahren und das Produkt durch

$$[s_1 \cdot s_2]\,(a) = s_1\,(s_2\,(a))$$

zu erklären. Die auf beiden Seiten gleiche Reihenfolge ist, besonders beim Auftreten mehrerer Faktoren, vorteilhafter. Man muß dann aber berücksichtigen, daß der zuletzt stehende Faktor die zuerst anzuwendende Transformation ist.

Insbesondere gilt dies für Permutationen, bei denen gerade bei der konkreten Berechnung durch unsere Gewohnheit, von links oben nach rechts unten zu lesen, die erstgenannte Schreibweise die suggestivere ist. Aus diesem Grunde ist sie bei uns gewählt worden.

In der anderen Schreibweise wäre zur Bildung des Produktes der beiden Permutationen

$$s_1 = \begin{pmatrix} 1 & 2 & & n \\ i_1 & i_2 & & i_n \end{pmatrix} \quad \text{und} \quad s_2 = \begin{pmatrix} 1 & 2 & & n \\ j_1 & j_2 & & j_n \end{pmatrix}$$

im Gegensatz zu B(2.5) zunächst s_1 umzuformen,

$$s_1 = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} = \begin{pmatrix} j_1 & j_2 & \dots & j_n \\ l_1 & l_2 & \dots & l_n \end{pmatrix}$$

und dann zu schreiben

$$s_1 \cdot s_2 = \begin{pmatrix} j_1 & j_2 & \dots & j_n \\ l_1 & l_2 & \dots & l_n \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & & n \\ l_1 & l_2 & \dots & l_n \end{pmatrix}.$$

Wir geben eine Übersicht über die Verwendung der einzelnen Schreibweisen in der von uns genannten Literatur.

1. Unsere Schreibweise stimmt überein mit: ALEXANDROFF, BAUMGARTNER, HASSE, HAUPT, KOCHENDÖRFFER, KUROSCH, SPECHT, SPEISER; Enzyklopädie der Elementarmathematik.

2. Die gegenteilige Schreibweise benutzen: PICKERT, TSCHEBOTAROW, VAN DER WAERDEN, ZASSENHAUS.

c) *Kennzeichnung der eineindeutigen Zuordnung*

Die dem Isomorphiebegriff zugrundeliegende eineindeutige Zuordnung der Elemente haben wir mit

$$a \to \bar{a}$$

bezeichnet. Da man sowohl vom Original a eindeutig zum Bild $\bar{a}$ als auch vom Bild $\bar{a}$ eindeutig zum Original a kommt, könnte man zu der Bezeichnung $a \longleftrightarrow \bar{a}$ veranlaßt werden, die überdies mit der Bezeichnung $\mathfrak{G} \overset{\sim}{\longleftrightarrow} \overline{\mathfrak{G}}$ korrespondieren würde. Dies ist auch dann ohne Gefahr, wenn $\mathfrak{G}$ und $\overline{\mathfrak{G}}$ kein Element gemeinsam haben. Sonst aber kann Verwirrung entstehen, wie wir durch ein Beispiel zeigen:

Wir bilden die zyklische Gruppe $\mathfrak{Z}_5 = \langle a \rangle$ der Ordnung 5 isomorph auf sich selbst ab vermöge der Zuordnung

$$a \to a^3,\ a^2 \to a,\ a^3 \to a^4,\ a^4 \to a^2,\ a^5 \to a^5.$$

Schreibt man jedoch Doppelpfeile, so entsteht z. B.

$$a^3 \longleftrightarrow a^4,\ a^4 \longleftrightarrow a^2,$$

so daß nur noch die Stellung zwischen Original und Bild zu unterscheiden gestattet. Das ist aber sehr bedenklich.

Der gleiche Einwand trifft natürlich zunächst auch auf die Bezeichnung $\mathfrak{G} \overset{\sim}{\longleftrightarrow} \bar{\mathfrak{G}}$ zu, wenn man sie für eine bestimmte isomorphe Abbildung von $\mathfrak{G}$ auf $\bar{\mathfrak{G}}$ gebraucht. Andererseits bedeutet aber das Vorliegen einer solchen Abbildung gerade die Isomorphie zwischen $\mathfrak{G}$ und $\bar{\mathfrak{G}}$, so daß „$\overset{\sim}{\longleftrightarrow}$" zugleich ein Zeichen für die Isomorphie als Äquivalenzrelation, also für eine symmetrische Beziehung wird. Das scheint uns die Verwendung dieses Zeichens überhaupt wie auch in beiden Bedeutungen zu rechtfertigen, zumal aus dem Zusammenhang stets hervorgeht, ob ein bestimmter Isomorphismus oder die Isomorphie schlechthin gemeint ist. Für letztere steht in der Literatur übrigens auch das Zeichen $\cong$.

VERZEICHNIS EINIGER LEHRBÜCHER

Allgemeine Lehrbücher

1. H. HASSE, Höhere Algebra, Teil I, II; 3. Auflage, Sammlung Göschen 931/932; Walter de Gruyter, Berlin 1951.
2. O. HAUPT, Einführung in die Algebra, Teil I, 3. Auflage 1956; Teil II, 2. Auflage 1954; Akademische Verlagsgesellschaft Leipzig.
3. R. KOCHENDÖRFFER, Einführung in die Algebra; Deutscher Verlag der Wissenschaften, Berlin 1955.
4. W. KRULL, Elementare und klassische Algebra vom modernen Standpunkt I, 2. Auflage, Sammlung Göschen 930; Walter de Gruyter, Berlin 1952.
5. G. PICKERT, Einführung in die höhere Algebra; Vandenhoeck & Ruprecht, Göttingen 1951.
6. N. TSCHEBOTAROW, Grundzüge der Galoisschen Theorie, Deutsche Ausgabe 1950; P. Noordhoff N. V., Groningen — Djakarta.
7. B. L. VAN DER WAERDEN, Algebra, Neuauflage von „Moderne Algebra", Teil I, 4. Auflage 1955; Teil II, 3. Auflage 1955; Julius Springer, Berlin.

Lehrbücher über Gruppentheorie

8. P. S. ALEXANDROFF, Einführung in die Gruppentheorie, Deutsche Ausgabe; Deutscher Verlag der Wissenschaften, Berlin 1954.
9. L. BAUMGARTNER, Gruppentheorie, 2. Auflage, Sammlung Göschen 837; Walter de Gruyter, Berlin 1949.
10. A. G. KUROSCH, Gruppentheorie, Deutsche Ausgabe; Akademie-Verlag, Berlin 1953.
11. W. SPECHT, Gruppentheorie; Julius Springer, Berlin 1956.
12. A. SPEISER, Die Theorie der Gruppen von endlicher Ordnung, 3. Auflage; Julius Springer, Berlin 1937.
13. H. ZASSENHAUS, Lehrbuch der Gruppentheorie; B. G. Teubner, Leipzig 1937.

Ferner sei verwiesen auf

14. Enzyklopädie der Elementarmathematik (Redaktion: P. S. ALEXANDROFF, A. I. MARKUSCHEWITSCH, A. J. CHINTSCHIN), Deutsche Ausgabe; Band I, 1954; Band II, 1956; Deutscher Verlag der Wissenschaften, Berlin.

SACHVERZEICHNIS