P.S. Alexandroff

Einführung in die Gruppentheorie

Deutscher Verlag der Wissenschaften 1971
Übersetzung von Lothar Uhlig
MSB: Nr. 1
Abschrift und LaTex-Satz: 2020 https://mathematikalpha.de

Zum Geleit

Der Begriff der Gruppe ist so alt wie die Mathematik selbst. Ins mathematische Bewusstsein tritt er jedoch erst zu Beginn des 19. Jahrhunderts, als die Theorie der algebraischen Gleichungen mit E. Galois zur Entwicklung einer weitgespannten Theorie der Gruppen endlicher Ordnung Anlass gab.

Zugleich aber regte die invariantentheoretische Tendenz der Geometrie dazu an, einige spezielle unendliche Gruppen zu untersuchen, wodurch ein weiterer Ausbau der Gruppentheorie vollzogen wurde. Sie zeigte ferner die Möglichkeit, die neue Theorie auf viele Gebiete der Mathematik anzuwenden.

Aus einem solchen Wechselspiel gegenseitiger Anregungen entstand um 1920 zusammen mit einer Strukturumwandlung der Algebra und Geometrie in Verbindung mit dem Eingang mengentheoretischer Überlegungen in die Mathematik die selbständige Disziplin der Gruppentheorie.
Sie befasst sich nur mit ganz allgemeinen abstrakten Elementen oder Größen. Daher können durch sie - und darin liegt weiterhin ihre große Bedeutung - Aussagen, Methoden, u. a. aus verschiedensten Gebieten der Mathematik einerseits, aber andererseits auch solche, die weit außerhalb mathematischer Betrachtungen liegen, sofern diese nur die gleiche logische Struktur haben, vermöge eben dieser Struktur gemeinsam behandelt werden.
Damit werden durch die Gruppentheorie die Schlussweisen auf die begrifflich einfachsten Bestandteile zurückgeführt; sie dient dabei auch in sehr einfacher Weise dazu, zum axiomatischen Denken zu gelangen.

So ist schließlich die Gruppentheorie auch bestens dazu geeignet, in das mathematische Denken und das deduktive Schließen einzuführen. Daher ist es fast eine Selbstverständlichkeit, die Mathematische Schülerbücherei mit einem solchen Bändchen zu beginnen.
Das Heft von P. Alexandroff ist fachlich, didaktisch und methodisch ausgezeichnet dazu geeignet, einen Leser, der den Stoff bis zur neunten Klasse beherrscht, in das Wesen der Gruppentheorie einzuführen. Aber auch dem Studenten der Mathematik und der Naturwissenschaften der ersten Semester sei dieses Buch empfohlen.

Januar 1965
Dr. Ernst Hameister

Vorwort zur zweiten Auflage

Die erste Auflage dieses Buches erschien im Jahre 1938. Seitdem ist unsere algebraische Literatur durch bedeutende Werke wie "Höhere Algebra" und "Gruppentheorie" von A.G. Kurosch und durch die Vorlesungen über lineare Algebra von I.M. Gelfand und A.I. Malzew ergänzt werden.

Doch bleibt daneben die Forderung nach einer völlig elementaren Einführung in die Gruppentheorie, die gleichzeitig auch als elementare Einführung in die Algebra im weiteren Sinne des Wortes dienen könnte, bestehen.
Daher stimmte ich auch einer Neuauflage dieses Buches zu. Es dürfte angehende Mathematiker interessieren, die noch keine Hochschule besucht haben, es kann einem Lehrer die Kenntnisse auffrischen, die er sich auf einem pädagogischen Institut erworben hat.
Alle, die tiefer in die Gruppentheorie eindringen wollen, verweise ich auf die oben erwähnte Monographie von A.G. Kurosch.

Für diejenigen meiner Leser, für welche dieses Buch die erste mathematische Lektüre nach den Schulbüchern ist, möchte ich noch hinzufügen, dass die ganze Tragweite der Gruppentheorie erst in den Wechselbeziehungen mit anderen mathematischen Disziplinen (und gegenwärtig auch der Physik) zur Geltung kommt.

Daher empfehle ich diesen Lesern, sich mit den Elementen der höheren Algebra (nach dem erwähnten Lehrbuch von A.G. Kurosch) und mit der analytischen Geometrie (beispielsweise nach dem Lehrbuch von S.P. Finikow) vertraut zu machen. Danach kann man sich mit der linearen Algebra von I.M. Gelfand beschäftigen und sich auch mit meinem Buche "Was ist die sogenannte nichteuklidische Geometrie!" bekannt machen.

In allen diesen Büchern findet der Leser viele Anwendungen der Gruppentheorie. Die zweite Auflage dieses Buches unterscheidet sich von der ersten durch unwesentliche Änderungen, die in der Hauptsache auf die Beseitigung verschiedener Fehler der ersten Auflage zurückzuführen sind.

P. Alexandroff

Inhaltsverzeichnis

Einleitung

In der Schule vollzieht sich der Übergang von arithmetischen zu algebraischen Aufgaben dadurch, dass in den Aufgaben ebene (konkrete) Zahlen durch Buchstaben (allgemeine Zahlen, d.Ü.) ersetzt werden. Die Bezeichnung der Zahlen durch Buchstaben befreit uns von den speziellen gegebenen Zahlen, die in diesem oder jenem Problem auftreten, und lehrt uns, das Problem in allgemeiner Form, also für beliebige Zahlenwerte, welche die darin vorkommenden Größen annehmen können, zu lösen.

Dementsprechend lernt man auf der Schule in den ersten wichtigen Kapiteln der Algebra die Anwendung der Rechenoperationen auf Buchstabenausdrücke oder, was dasselbe ist, die Gesetze der sogenannten identischen Umformung algebraischer Ausdrücke. Wir wollen zunächst diesen Begriff erklären.

Jeder algebraische Ausdruck ist eine Gesamtheit von Buchstaben, die untereinander durch die algebraischen Operationszeichen verbunden sind. Dabei wollen wir der Einfachheit halber im Moment nur die Addition, Subtraktion und Multiplikation betrachten.
Der Sinn jedes algebraischen Ausdruckes ist folgender:

Ersetzt man die im Ausdruck vorkommenden Buchstaben durch Zahlen, so gibt er Art und Reihenfolge der Operationen an, die man an diesen Zahlen ausführen soll. Mit anderen Worten: jeder algebraische Ausdruck stellt ein gewisses in allgemeiner Form hingeschriebenes Rezept für eine gewöhnliche arithmetische Rechnung dar.
Die identische Umformung eines algebraischen Ausdruckes bedeutet den Übergang von einem Ausdruck zu einem anderen, der mit dem ersten durch folgende Beziehung zusammenhängt: Geben wir in beiden Ausdrücken für die Buchstaben völlig willkürliche Zahlwerte vor, aber so, dass ein und dieselben in beiden Ausdrücken vorkommenden Buchstaben stets ein und denselben Zahlwert erhalten, und führen wir dann die angegebenen Operationen aus, so liefern beide Ausdrücke ein und dasselbe Zahlenresultat.

Eine identische Umformung schreibt man als Gleichung zweier algebraischer Ausdrücke; diese Gleichung gilt bei beliebiger Ersetzung der in ihr vorkommenden Buchstaben (wie oben angegeben). Eine Gleichung dieser Form heißt bekanntlich Identität. Beispielsweise gilt

$$a - a = 0 \tag{1}$$

$$(a + b)c = ac + bc \tag{2}$$

Jede Identität drückt eine gewisse Eigenschaft der in ihr auftretenden Operationen aus. So besagt beispielsweise die Identität (1) folgendes:
Subtrahiert man von einer Zahl die gleiche Zahl, so erhält man immer ein und dasselbe Resultat, nämlich Null. Die Identität (2) beinhaltet folgende Eigenschaft der Operationen Addition und Multiplikation:
Das Produkt der Summe zweier Zahlen mit einer dritten Zahl ist gleich der Summe der Produkte jedes der Summanden mit dieser dritten Zahl.

Es gibt unendlich viele Identitäten. Jedoch kann man eine geringe Anzahl fundamentaler Identitäten ähnlich den oben angegebenen aufstellen derart, dass jede Identität eine Folgerung aus diesen fundamentalen Identitäten ist.

Jede algebraische Rechnung, also jede beliebig komplizierte identische Umformung eines algebraischen Ausdruckes in einen anderen, ist somit eine Kombination einer geringen Anzahl fundamentaler oder elementarer identischer Umformungen, die man in der elementaren Algebra

kurz unter den Namen Regeln zur Auflösung von Klammern, Vorzeichenregeln usw. zusammenfasst.

Führt man diese Kombinationen elementarer Umformungen aus, so darf man gewöhnlich auch vergessen, dass jeder Buchstabe im algebraischen Ausdruck nur ein Symbol, ein Zeichen ist, das eine gewisse Zahl bezeichnet:

Man führt, wie man sagt, die Rechnung mechanisch durch, vergisst die reale Bedeutung der in jedem Augenblick durchgeführten Umformung und befolgt lediglich die Regeln dieser Umformungen. So verfahren gewöhnlich auch praktisch die Mathematiker und Studenten. Doch kommt es dabei leider vor, dass diese reale Bedeutung der durchgeführten Umformungen überhaupt aus dem Bewusstsein schwindet.

Die mechanische Durchführung algebraischer Operationen hat auch noch eine andere, wesentlichere Seite. Sie läuft darauf hinaus, dass man unter den in einem algebraischen Ausdruck vorkommenden Buchstaben häufig keine Zahlen, sondern mancherlei andere Objekte mathematischer Untersuchung verstehen kann:
Nicht nur auf Zahlen, sondern auch auf andere Dinge kann man solche Operationen anwenden, die eine Reihe wichtiger Eigenschaften mit den algebraischen Operationen gemeinsam haben und die man daher naturgemäß Addition, Multiplikation usw. nennt.

Beispiele dafür werden wir sogleich angeben. So sind etwa die Kräfte in der Mechanik keine Zahlen, sondern sogenannte Vektoren, d.h. Größen, die nicht nur einen Zahlwert, sondern auch eine Richtung haben. Kräfte kann man addieren, und diese Addition besitzt die Haupteigenschaften der gewöhnlichen algebraischen Addition von Zahlen.
Dies führt dazu, dass man auf Kräfte auch die Subtraktion nach den Regeln der Algebra anwenden kann. Somit ist die Tragweite algebraischer Umformungen viel größer als die einer Schreibweise allgemeiner Operationen an Zahlen:

Die Algebra untersucht Rechnungen mit beliebigen Objekten, für welche Rechenoperationen definiert sind, die den wichtigsten algebraischen Axiomen genügen.

1 Der Begriff der Gruppe

1.1 Einleitende Beispiele

1.1.1 Operationen mit den ganzen Zahlen

Die Addition ganzer Zahlen[1] erfüllt folgende Bedingungen, die man als Axiome der Addition bezeichnet und die für alles folgende außerordentlich große Bedeutung haben:

I. Je zwei Zahlen kann man addieren (d.h., zu je zwei beliebigen Zahlen a und b existiert eine eindeutig bestimmte Zahl, die man als ihre Summe bezeichnet: $a + b$).

II. Das Gesetz der Assoziativität:
Für je drei beliebige Zahlen a, b, c gilt die Identität

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

III. Unter den Zahlen existiert eine bestimmte Zahl 0, die Null, welche so beschaffen ist, dass für jede Zahl a die Relation

$$a + 0 = a$$

erfüllt ist.

IV. Zu jeder Zahl a existiert eine sogenannte entgegengesetzte Zahl $-a$, die die Eigenschaft besitzt, dass die Summe $a + (-a)$ gleich Null ist:

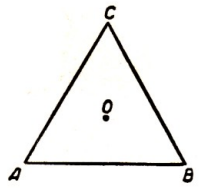
$$a + (-a) = 0$$

Schließlich ist noch eine besondere Bedingung erfüllt.
V. Das Gesetz der Vertauschbarkeit oder Kommutativität:

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

1.1.2 Die Drehungen eines gleichseitigen Dreiecks

Wir zeigen, dass man nicht nur Zahlen, sondern auch viele andere Dinge addieren kann, und zwar unter Beibehaltung der eben um geführten Bedingungen.



Erstes Beispiel. Wir betrachten alle möglichen Drehungen eines gleichzeitigen Dreiecks ABC um seinen Mittelpunkt O (Abb. 1). Dabei nennt man zwei Drehungen identisch, wenn sie sich lediglich um eine ganze Zahl vollständiger Drehungen voneinander unterscheiden (also um ein ganzzahliges Vielfaches von 360°). Man sieht leicht, dass von allen möglichen Drehungen des Dreiecks lediglich drei Drehungen des Dreieck in sich überführen, nämlich:

die Drehungen um 120°, 240° und die sogenannte Nulldrehung, die alle Eckpunkte und damit auch sämtliche Seiten des Dreiecks in ihrer Lage lässt.[2]

[1] Unter den ganzen Zahlen verstehen wir immer alle positiven und alle negativen ganzen Zahlen und außerdem die Zahl Null.

[2] Da eine Drehung um ein ganzzahliges Vielfaches von 360° offensichtlich jeden Eckpunkt in seine ursprüngliche Lage überführt, so definiert man diese Drehung als identisch mit der Nulldrehung; allgemein erklärt man zwei Drehungen als identisch, falls sie sich um eine ganze Zahl vollständiger Drehungen voneinander unterscheiden.

Die erste Drehung führt den Eckpunkt A in den Eckpunkt B, den Eckpunkt B in den Eckpunkt C, den Eckpunkt C in den Eckpunkt A über (sie vertauscht, wie man sagt, die Eckpunkte A, B, C in zyklischer Reihenfolge).
Die zweite Drehung führt A in C, B in A, C in B über, vertauscht also A, C, B zyklisch.

Jetzt führen wir folgende naturgemäße Definition ein:
Die Addition zweier Drehungen bedeute die Hintereinanderausführung der ersten und zweiten Drehung. Addiert man die Drehung um 120° zu sich selbst, so liefert sie die Drehung um 240°; fügt man ihr die Drehung um 240° hinzu, so ergibt sich die Drehung um 360°, also die Nulldrehung.
Zwei Drehungen um 240° liefern die Drehung um 480° = 360° + 120°, ihre Summe ist also die Drehung um 120°. Bezeichnen wir die Nulldrehung mit a_0 die Drehung um 120° mit a_1 die Drehung um 240° mit a_2, so erhalten wir folgende Relationen.

$$\begin{aligned} a_0 + a_0 = a_0 \quad &; \quad a_0 + a_1 = a_1 + a_0 = a_1 \\ a_0 + a_2 = a_2 + a_0 = a_2 \quad &; \quad a_1 + a_1 = a_2 \\ a_1 + a_2 = a_2 + a_1 = a_0 \quad &; \quad a_2 + a_2 = a_1 \end{aligned}$$

Also ist für je zwei Drehungen ihre Summe definiert. Man überzeugt sich leicht, dass diese Addition das assoziative und offensichtlich auch das kommutative Gesetz erfüllt. Weiter kommt unter diesen Drehungen die Nulldrehung a_0 vor, die die Bedingung

$$a + a_0 = a_0 + a = a$$

für jede Drehung a erfüllt.

Schließlich gibt es zu jeder der drei Drehungen eine entgegengesetzte, deren Summe mit der ursprünglichen die Nulldrehung ergibt. Die Nulldrehung ist offensichtlich zu sich selbst entgegengesetzt, $-a_0 = a_0$, da, $a_0 + a_0 = a_0$ ist; ferner ist $-a_1 = a_2$ und $-a_2 = -a_1$ (da $a_1 + a_2 = a_0$ ist). Daher erfüllt die Addition der Drehungen eines gleichseitigen Dreiecks alle vorhin formulierten Axiome der Addition.

Wir halten das Additionsgesetz der Drehungen noch einmal in übersichtlicher Weise in Form folgender Additionstafel fest:

	a_0	a_1	a_2
a_0	a_0	a_1	a_2
a_1	a_1	a_2	a_0
a_2	a_2	a_0	a_1

Die Summe zweier Elemente finden wir in dieser Tabelle an dem Schnittpunkt der dem ersten Element entsprechenden Zeile mit der dem zweiten Element entsprechenden Spalte.

Will man mit diesen Drehungen mechanisch rechnen, so nehme man einfach die drei Buchstaben a_0, a_1, a_2 und addiere sie gemäß der eben angegebenen Additionstafel. Von der Bedeutung dieser Buchstaben kann man dabei völlig absehen.

1.1.3 Die Kleinsche Vierergruppe

Zweites Beispiel. Wir betrachten die Gesamtheit der vier Buchstaben a_0, a_1, a_2, a_3, deren Addition durch folgende Tafel definiert ist:

Tafel II

	a_0	a_1	a_2	a_3
a_0	a_0	a_1	a_2	a_3
a_1	a_1	a_0	a_3	a_2
a_2	a_2	a_3	a_0	a_1
a_3	a_3	a_2	a_1	a_0

oder ausführlich:

$$\begin{aligned} a_0 + a_0 = a_0 \quad &; \quad a_0 + a_1 = a_1 + a_0 = a_1 \\ a_0 + a_2 = a_2 + a_0 = a_2 \quad &; \quad a_0 + a_3 = a_3 + a_0 = a_3 \\ a_1 + a_1 = a_0 \quad &; \quad a_2 + a_2 = a_0 \\ a_1 + a_2 = a_2 + a_1 = a_3 \quad &; \quad a_2 + a_3 = a_3 + a_2 = a_1 \\ a_1 + a_3 = a_3 + a_1 = a_2 \quad &; \quad a_3 + a_3 = a_0 \end{aligned}$$

Die Addition ist für je zwei beliebige aus der Menge dieser vier Buchstaben definiert. Man beweist sofort, dass diese Addition das assoziative und das kommutative Gesetz erfüllt. Der Buchstabe a_0 besitzt die Haupteigenschaft der Null: Die Summe zweier Summanden, von denen einer gleich a_0 ist, ist gleich dem anderen Summanden.

Es zeigt sich also, dass die Bedingungen I, II, III, V in dieser "Vierbuchstabenalgebraërfüllt sind. Um sich davon zu überzeugen, dass die Bedingung IV ebenfalls erfüllt ist, genügt der Hinweis auf

$$a_0 + a_0 = a_0 \quad ; \quad a_1 + a_1 = a_0 \quad ; \quad a_2 + a_2 = a_0 \quad ; \quad a_3 + a_3 = a_0$$

wonach jeder Buchstabe zu sich selbst entgegengesetzt ist (d.h bei Addition zu sich selbst Null ergibt).
Diese "Vierbuchstabenalgebra" könnte auf den ersten Blick als mathematische Spielerei, als Kurzweil ohne realen Inhalt erscheinen. In Wirklichkeit haben die durch Tafel II ausgedrückten Gesetze dieser Algebra, eine völlig reale Bedeutung, mit der wir uns in Kürze vertraut machen. Ich weise außerdem darauf hin, dass diese "Vierbuchstabenalgebra" auch in der höheren Algebra große Bedeutung besitzt. Sie heißt die Kleinsche Vierergruppe.[3]

1.1.4 Die Drehungen eines Quadrates

Drittes Beispiel. Eine weitere von der vorhergehenden verschiedene "Vierbuchstabenalgebra" kann man analog zu dem ersten Beispiel konstruieren. Wir betrachten ein Quadrat $ABCD$ und die Drehungen um seinen Mittelpunkt, die die Figur in sich überführen.

Wiederum identifizieren wir je zwei Drehungen, die sich um ein ganzzahliges Vielfaches von 360° unterscheiden. Wir haben also insgesamt vier Drehungen, nämlich die Nulldrehung, die Drehungen um 90°, um 180° und um 270°. Diese Drehungen bezeichnen wir in dieser Reihenfolge mit a_0, a_1, a_2, a_3.

Versteht man unter der Addition zweier Drehungen wieder ihre Hintereinanderausführung, so erhält man folgende zum ersten Beispiel völlig analoge Additionstafel:

[3] Nach dem großen deutschen Mathematiker Felix Klein (1849-1925).

	a_0	a_1	a_2	a_3
a_0	a_0	a_1	a_2	a_3
a_1	a_1	a_2	a_3	a_0
a_2	a_2	a_3	a_0	a_1
a_3	a_3	a_0	a_1	a_2

Auf die gleiche Weise wie im ersten Beispiel kann man Drehungen eines regelmäßigen Fünf-, Sechs- und allgemein eines n-Ecks betrachten. Es sei dem Leser selbst überlassen, die hierher gehört gen Überlegungen durchzuführen und die entsprechenden Additionstafeln zusammenzustellen.

1.2 Definition der Gruppe

Bevor wir in der Betrachtung einzelner Beispiele fortfahren, fassen wir die Ergebnisse aus den bereits untersuchten Beispielen zusammen und führen folgende grundlegende Definition ein.

Wir nehmen an, es sei eine gewisse endliche oder unendliche Menge[4] G vorgegeben; ferner nehmen wir an, für je zwei Elemente a und b der Menge G sei ein bestimmtes drittes Element dieser Menge definiert, das wir die Summe der Elemente a und b nennen und mit $a + b$ bezeichnen.
Schließlich nehmen wir an, diese Operation der Addition (also die Operation des Übergangs von zwei gegebenen Elementen a und b zum Element $a + b$) erfülle folgende Bedingungen:

I. Die Bedingung der Assoziativität.
Für je drei Elemente a, b, c der Menge G gilt die Relation

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

Dies bedeutet folgendes: Bezeichnen wir mit d das Element der Menge G, das die Summe der Elemente a und b ist, und entsprechend mit e des Element $b + c$ der Menge G, so sind $d + c$ und $a + e$ ein und dasselbe Element der Menge G.

II. Die Bedingung der Existenz einer neutralen Elementen.
Unter den Elementen der Menge G gibt es ein bestimmtes Element, das man neutrales Element nennt und mit 0 bezeichnet und das so beschaffen ist, dass bei beliebiger Wahl des Elemente a

$$a + 0 = 0 + a = a$$

gilt.

III. Die Bedingung der Existenz einer entgegengesetzten Elementes zu jedem vorgegebenen Element: Zu jedem vorgegebenen Element a der Menge G kann man ein Element $-a$ aus G finden, so dass

$$a + (-a) = (-a) + a = 0$$

gilt.
Eine Menge G mit einer in ihr definierten Operation der Addition, die die eben aufgezählten drei Bedingungen erfüllt, heißt eine Gruppe. Diese Bedingungen selbst heißen Axiome des Gruppenbegriffs oder kurz Gruppenaxiome.

[4] Siehe den Anhang am Schluss des Buches. Im folgenden wollen wir voraussetzen, dass der Leser den Inhalt dieses Anhangs vollkommen beherrscht.

Ist in einer Gruppe G außer den drei Gruppenaxiomen auch noch folgende Bedingung erfüllt:
IV. Die Bedingung der Vertauschbarkeit oder Kommutativität:

$$a + b = b + a$$

so heißt die Gruppe kommutativ oder Abelsch.[5]

Eine Gruppe heißt endlich, wenn sie aus endlich vielen Elementen besteht; andernfalls heißt sie unendlich. Die Anzahl der Elemente einer endlichen Gruppe bezeichnet man als ihre Ordnung.

Nachdem wir uns mit der Definition einer Gruppe vertraut gemacht haben, sehen wir, dass die Beispiele, die in den ersten beiden Paragraphen dieses Kapitels angegeben wurden, Beispiele für Gruppen sind. Wir haben also bisher folgende Gruppen kennengelernt:

1. die Gruppe der ganzen Zahlen;
2. die Gruppe der Drehungen eines gleichseitigen Dreiecks (diese Gruppe heißt auch zyklische Gruppe der Ordnung 3);
3. die Kleinsche Vierergruppe;
4. die Gruppe der Drehungen eines Quadrates (zyklische Gruppe der Ordnung 4).

Am Schluss des § 1 wurde noch die Drehungsgruppe eines regelmäßigen n-Ecks (zyklische Gruppe der Ordnung n) erwähnt.
Alle diese Gruppen sind kommutativ und mit Ausnahme der Gruppe der ganzen Zahlen endlich; diese ist offenbar unendlich.

1.3 Einfache Sätze über Gruppen

1.3.1 Die Addition beliebig, aber endlich vieler Gruppenelemente

Die erste Regel für die Auflösung von Klammern[6]

Das Assoziativitätsaxiom hat in der Gruppentheorie und damit auch in der gesamten Algebra sehr große Bedeutung: Dadurch kann man nicht nur die Summe zweier, sondern auch die Summe dreier und allgemein beliebig, aber endlich vieler Gruppenelemente definieren und zur Berechnung dieser Summen die üblichen Regeln für die Auflösung von Klammern anwenden.[7]

Sind nämlich beispielsweise drei Elemente a, b, c vorgegeben, so wissen wir vorläufig noch nicht, was die Addition dieser drei Elemente bedeutet; denn die Gruppenaxiome sprechen nur von der Summe zweier Summanden, und Ausdrücke der Form $a+b+c$ sind noch nicht definiert. Nun besagt aber die Bedingung der Assoziativität: Addieren wir einerseits die zwei Elemente a und $b+c$ und andererseits die beiden Elemente $a+b$ und c, so erhalten wir ein und dasselbe Element als ihre Summe.

Also lässt sich das Element, welches die Summe der beiden Elemente a und $b+c$ und ebenso die Summe der beiden Elemente $a+b$ und c ist, eindeutig als Summe der Elemente a, b, c (in der eben angegebenen Reihenfolge) definieren und wird deshalb einfach mit $a+b+c$ bezeichnet. Daher kann man die Gleichung

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

[5] Nach dem genialen norwegischen Mathematiker N. H. Abel (1802-1829)

[6] Möchte sich der Leser zunächst mit weiteren Beispielen von Gruppen beschäftigen, so kann er diesen Paragraphen überspringen und nach der Lektüre der Kapitel II-IV darauf zurückkommen.

[7] Dabei muss man nur beachten, dass man im Falle einer nicht kommutativen Gruppe die Reihenfolge der Summanden nicht ändern darf.

als Definition des Ausdruckes $a+b+c$ für die Summe der drei Elemente a, b, c betrachten.

Entsprechend kann man die Summe der vier Elemente a, b, c, d beispielsweise als $a+(b+c+d)$ definieren. Wir beweisen, dass dabei

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

gilt.
Nach dem eben Gesagten hat man zunächst

$$a+(b+c+d)=a+[b+(c+d)]$$

Für die drei Elemente a, b, $c+d$ gilt aber:

$$a+[b+(c+d)]=(a+b)+(c+d)$$

Andererseits gilt auch für die drei Elemente $a+b$, c, d:

$$(a+b)+(c+d)=[(a+b)+c]+d=(a+b+c)+d.$$

was zu beweisen wir.

Wir setzen nun voraus, die Summe von je $n-1$ Summanden sei bereits definiert; den definieren wir die Summe der n Summanden $1+...+a_n$ als $a_1+a_2+...+a_n$ und können damit den Ausdruck $a_1+...+a_n$ nach der Methode der vollständigen Induktion für beliebiges n als definiert ansehen.

Satz. Es sei n eine beliebige natürliche Zahl. Für jede natürliche Zahl[8] $m\leq n$ gilt die Identität

$$(a_1+...+a_m)+(a_{m+1}+...+a_n)=a_1+...+a_n \tag{1}$$

Beweis. Der Beweis wird nach der Methode der vollständigen Induktion geführt[9]:
Für $n=1$ besagt der Satz die Identität $a_1=a_1$. Wir nehmen nun an, er sei für $n\leq k-1$ gültig, und beweisen ihn für $n=k$. Wir betrachten zunächst den Fall $m=1$. Dann geht die Formel (1) über in

$$a_1+(a_2+...+a_k)=a_1+...+a_k$$

Dies ist aber gerade die Definition des Ausdruckes $a_1+...+a_k$. Also gilt für vorgegebenes $n=k$ und $m=1$ die Formel (1).

Jetzt wählen wir $n=k$ fest und nehmen an, unsere Formel sei für $m=q-1$ bewiesen; wir beweisen sie für $m=q$.
Da die Formel (1) für $m=n$ offensichtlich gilt, können wir $q<k$ voraussetzen. Da die Gültigkeit des Satzes für $n\leq k-1$ vorausgesetzt ist, gilt dann

$$(a_1+...+a_q)+(a_{q+1}+...+a_k)=[(a_1+...+a_{q-1})+a_q]+(a_{q+1}+...+a_k)$$

Die Bedingung der Assoziativität, angewendet auf die drei Elemente $(a_1+...+a_{q-1})$, a_q, $(a_{q+1}+...+a_k)$ ergibt

$$[(a_1+...+a_{q-1})+a_q]+(a_{q+1}+...+a_k)=(a_1+...+a_{q-1})+[a_q+(a_{q+1}+...+a_k)]$$

[8] Eine natürliche Zahl ist eine ganze positive Zahl.
[9] Es empfiehlt sich, den Beweis selbst durchzuführen und ihn dann erst mit dem nachfolgenden Text zu vergleichen.

Der Ausdruck rechts in eckigen Klammern ist nach Definition aber gleich

$$a_q + a_q + 1 + ... + a_k$$

Also gilt

$$(a_1 + ... + a_q) + (a_{q+1} + ... + a_k) = (a_1 + ... + a_{q-1}) + (a_q + ... + a_k)$$

Da aber die Formel (1) für $n = k$ und $m = q - 1$ als gültig vorausgesetzt wurde, ist die rechte Seite der letzten Gleichung gleich $a_1 + ... + a_k$. Somit gilt

$$(a_1 + ... + a_q) + (a_{q+1} + ... + a_k) = a_1 + ... + a_k$$

was zu beweisen war.

1.3.2 Das neutrale Element

Die Bedingung für die Existenz eines neutralen Elementes lautet: In der Gruppe existiert ein gewisses Element 0 derart, dass für jedes Element a der Gruppe die Bedingung

$$a + 0 = 0 + a = a \tag{1}$$

erfüllt ist.
Diese Bedingung enthält keineswegs die Behauptung, dass es in der vorgelegten Gruppe kein zweites von 0 verschiedenes Element 0' mit derselben Eigenschaft

$$a + 0' = 0' + a = a \tag{1'}$$

für jedes a geben könnte.
Aus der folgenden etwas inhaltsreicheren Aussage ergibt sich, dass tatsächlich ein derartiges Element 0' nicht auftritt. Man bezeichnet sie oft als Satz von der Eindeutigkeit des neutralen Elementes.

Satz. Gibt es zu irgendeinem bestimmten Element a einer Gruppe G ein Element 0, das eine der Bedingungen

$$a + 0_a = a \qquad \text{oder} \qquad 0_a + a = a$$

erfüllt, so ist notwendigerweise

$$0_a = 0.$$

Beweis: Wir setzen zunächst voraus, es sei $a + 0_a = a$, und bemerken, dass für ein beliebiges Element b

$$b + 0_a = (b + 0) + 0_a$$

gilt. Ersetzt man dann 0 durch $(-a) + a$, so erhält man

$$b + 0_a = b + (-a) + a + 0_a = b + (-a) + (a + 0_a) = b + (-a) + a = b$$

Ebenso gilt:

$$0_a + b = (0 + 0_a) + b = (-a) + a + 0_a + b = (-a) + (a + 0_a) + b = (-a) + a + b = b$$

und somit für jedes b

$$b + 0_a = 0_a + b = b$$

Wählen wir nun insbesondere $b = 0$, so ergibt sich

$$0 + 0_a = 0 \tag{2}$$

Nach Definition des Elementes 0 gilt aber andererseits

$$0 + 0_a = 0_a \tag{3}$$

Aus den Gleichungen (2) und (3) folgt $0 = 0_a$, was zu beweisen war.
Ebenso kann man die Identität $0_a = 0$ aus der Voraussetzung $0_a + a = a$ folgern.

1.3.3 Das entgegengesetzte Element

Die Bedingung für die Existenz eines entgegengesetzten Elementes lautet: Zu jedem Element a existiert ein Element $-a$ derart, dass

$$(-a) + a = a + (-a) = 0$$

gilt.
Hier ist wiederum nur die Existenz des Elementes $-a$ behauptet, nicht aber seine Eindeutigkeit. Wir beweisen diese Eindeutigkeit durch den folgenden Satz.

Satz. Gibt es zu einem vorgegebenen Element a irgendein Element a', das eine der Bedingungen

$$a + a' = 0 \qquad \text{oder} \qquad a' + a = 0$$

erfüllt, so ist $a' = a$.

Beweis. Es sei $a + a' = 0$. Daraus folgt

$$(-a) + (a + a') = (-a) + 0 = -a \qquad \text{also} \qquad [(-a) + a] + a' = -a$$

$$\text{also} \qquad 0 + a' = -a \qquad \text{d.h.} \qquad a' = -a$$

Ganz analog kann man $a' = -a$ aus der Voraussetzung $a + a = 0$ herleiten.
Also existiert zu einem vorgegebenen a genau ein Element x, das der Gleichung $a + x = 0$ bzw. der Gleichung $x + a = 0$ genügt, nämlich das Element $x = -a$.

Betrachten wir jetzt das Element $-a$. Dann erfüllt das Element a die Gleichung $-a + a = 0$, ist also für das Element $-a$ gerade das Element $x = -(-a)$, von dem eben die Rede war. Also gilt

$$-(-a) = a$$

1.3.4 Die Subtraktion

Zweite Regel für die Auflösung von Klammern

Es seien zwei Elemente a und b der Gruppe G vorgegeben. Zu jedem der Elemente a und b gibt es ein entgegengesetztes Element $-a$ bzw. $-b$.
Die Summe des Elementes b und des Elementes $-a$ heißt Differenz[10] zwischen dem Element b (Minuend) und dem Element a (Subtrahend) und wird mit $b - a$ bezeichnet:

$$b + (-a) = b - a \tag{1}$$

[10] Mitunter "rechte Differenz". Siehe unten.

Daher ist diese Gleichung die Definition der Differenz $b-a$, d.h. die Definition der Subtraktion als einer Rechenoperation, durch welche eben die Differenz der Elemente b und a bestimmt ist.

Auf Grund des assoziativen Gesetzes und der Definition des Elementes $-a$ gilt

$$(b-a)+a=[b+(-a)]+a=b+(-a+a)=b \tag{2}$$

der Minuend ist also gleich der Summe der Differenz und des Subtrahenden.[11] Mit anderen Worten: $b-a$ ist eine Lösung der Gleichung

$$x+a=b \tag{3}$$

Sie ist auch die einzige; denn ist das Element c eine Lösung der Gleichung (3), so ist $c+a=b$, das bedeutet

$$c+a+(-a)=b+(-a) \qquad \text{also} \qquad c=b+(-a)=b-a$$

Ebenso hat die Gleichung

$$a+x=b \tag{4}$$

das Element $-a+b$ als einzige Lösung.

Bemerkung. Manchmal bezeichnet man die Lösung der Gleichung (3), also das Element $b-a=b+(-a)$, als rechte und die Lösung der Gleichung (4), also das Element, $-a+b$ als linke Differenz der Elemente b und a. Für kommutative Gruppen fallen natürlich diese beiden Differenzbegriffe zusammen.
Folgerung. Ist $a+b=a+c$ oder $b+a=c+a$, so ist $b=c$.

Die Haupteigenschaft der Subtraktion wird durch die Formel

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

ausgedrückt.
Wir erinnern an folgendes: $-b-a$ bezeichnet $-b+(-a)$, also die Summe der zwei Elemente $-b$ und $-a$.

Das Element $-(a+b)$ ist nämlich das eindeutig bestimmte Element x der Gruppe, das der Bedingung

$$a+b+x=0 \tag{5}$$

genügt. Nun gilt aber

$$a+b+[(-b)+(-a)]=a+[b+(-b)]+(-a)=a+0+(-a)=a+(-a)=0$$

Somit erfüllt das Element $x=-b+(-a)=-b-a$ gerade die Bedingung (5), also ist tatsächlich $-(a+b)=-b-a$.

Durch vollständige Induktion erhalten wir daraus das allgemeine Resultat

$$-(a_1+...+a_n)=-a_n-a_{n-1}-...-a_1$$

[11] In nichtkommutativen Gruppen ist die Summe $b+(a-b)$ im allgemeinen nicht gleich a. Dies ist in der Gruppentheorie sehr wesentlich.

wobei die rechte Seite das Element

$$(-a_n) + (-a_{n-1}) + ... + (-a_1)$$

Daraus folgt nach Definition der Subtraktion:

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

und allgemein

$$c - (a_1 + ... + a_n) = c - a_n - a_{n-1} - ... - a_1 \tag{6}$$

In kommutativen Gruppen ist die Reihenfolge der Summanden gleichgültig, und wir können schreiben

$$c - (a_1 + ... + a_n) = c - a_1 - ... - a_n \tag{6'}$$

Formel (1) in Abschnitt 1 und Formel (6') enthält die übliche Regel der elementaren Algebra für das Auflösen von Klammern bei Addition und Subtraktion.

1.3.5 Bemerkungen über die Gruppenaxiome

Wir haben uns nicht die Aufgabe gestellt, eine möglichst geringe Anzahl von Forderungen anzugeben, die für die Definition des Begriffes der Gruppe ausreichen. Wir haben verlangt, dass das neutrale Element die Forderungen

$$a + 0 = 0 + a = a$$

erfüllt und dass das zu einem beliebigen Element a entgegengesetzte Element $-a$ die Bedingungen $a + (-a) = (-a) + a = 0$ erfüllt.
Indessen genügt es, auf Grund des in den Abschnitten 2 und 3 dieses Paragraphen Bewiesenen, nur eine der Bedingungen $a + 0 = a$ oder $0 + a = a$, und ebenso nur eine der Bedingungen $a + (-a) = 0$ oder $(-a) + a = 0$ zu fordern.

Schließlich erwähnen wir noch, dass in der Definition einer Gruppe (§ 2) die Axiome II und III, also die Bedingungen der Existenz eines neutralen Elementes und der eines entgegengesetzten zu jedem vorgegebenen Element, durch ein einziges Axiom ersetzt werden können, nämlich durch das folgende:

Die Bedingung der unbeschränkten Ausführbarkeit der Subtraktion.
Zu je zwei Elementen a und b kann man Elemente x und y finden derart, dass $a + x = b$ und $y + a = b$ ist.

Die Durchführung des Beweises überlassen wir dem Leser (er kann ihn auch beispielsweise in dem Buch "Gruppentheorie"von A.G. Kurosch) nachlesen.

2 Permutationsgruppen

2.1 Definition der Permutationsgruppen

Sitzen die drei Personen Martin, Kurt und Peter in dieser Reihenfolge von links nach rechts auf einer Bank, so können sie sich auf sechs verschiedene Arten umgruppieren, nämlich, wenn immer von links nach rechts aufgezählt wird, so:

(1) Martin, Kurt, Peter; (2) Martin, Peter, Kurt; (3) Kurt, Martin, Peter; (4) Kurt, Peter, Martin; (5) Peter, Martin, Kurt; (6) Peter, Kurt, Martin.

Der Übergang von einer beliebigen Sitzfolge zu einer anderen heißt Permutation. Eine Permutation schreibt man folgendermaßen:

Martin, Kurt, Peter;
Kurt, Peter, Martin

dies soll bedeuten, dass Kurt Martins Platz, Peter Kurts Platz und Martin Peters Platz einnimmt.

In diesem Sinne kann man von Permutationen beliebiger Gegenstände sprechen. Da hierbei die besondere Natur der zu permutierenden Gegenstände unwesentlich ist, werden diese Gegenstände meist durch Ziffern bezeichnet, und man spricht von einer Permutation von Ziffern. Somit kann man mit den drei Ziffern 1, 2, 3 folgende Permutationen vornehmen:

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

Jede Permutation drückt aus, dass an Stelle der in der oberen Zeile stehenden Ziffern die darunter geschriebenen der unteren Zeile treten. Die erste Permutation

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

nennt man die identische, in ihr bleibt jede Ziffer unverändert an ihrem Platz. Die zweite Permutation

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

besteht darin, dass die Ziffer 1 festbleibt, die Ziffer 3 auf den Platz der Ziffer 2 und die Ziffer 2 an die Stelle der Ziffer 3 tritt; entsprechendes gilt für die anderen Permutationen.

Die allgemeine Form einer Permutation der n Ziffern $1, 2, ..., n$ lautet:

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

Hier sind i_1, i_2, ..., i_n insgesamt wieder die Ziffern $1, 2, ..., n$, lediglich in anderer Reihenfolge. Wir betrachten zum Beispiel

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix}$$

Hier ist offensichtlich $n = 5$, $i_1 = 3$, $i_2 = 1$, $i_3 = 4$, $i_4 = 5$, $i_5 = 2$.
Bekanntlich gestatten n Ziffern $n!$ Permutationen.

Wir wenden uns wieder den Permutationen von drei Ziffern zu. Die Addition zweier Permutationen soll die Hintereinanderausführung der ersten und der zweiten bedeuten. Dadurch ergibt sich wieder eine Permutation, die man als die Summe der zwei vorgegebenen bezeichnet.

Wir addieren beispielsweise die Permutationen

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

Durch die erste Permutation wird die Eine mit der Zwei vertauscht, bei der zweiten Permutation bleibt diese Zwei fest, also geht nach Hintereinanderausführung beider Permutationen die Eins in die Zwei über. Entsprechend geht bei der Hintereinanderausführung der beiden Permutationen die Zwei in die Drei und die Drei in die Eins über. Daher gilt

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

Auf dieselbe Weise addiert man zwei beliebige Permutationen. Um die Resultate aller dieser Additionen bequem aufschreiben zu können, führen wir folgende Bezeichnungen ein:

$$P_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$
$$P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

P_0 heißt die identische Permutation. Dann erhalten wir folgende Additionstafel:

Erster Summand	Zweiter Summand					
	P_0	P_1	P_2	P_3	P_4	P_5
P_0	P_0	P_1	P_2	P_3	P_4	P_5
P_1	P_1	P_0	P_3	P_2	P_5	P_4
P_2	P_2	P_4	P_0	P_5	P_1	P_3
P_3	P_3	P_5	P_1	P_4	P_0	P_2
P_4	P_4	P_2	P_5	P_0	P_3	P_1
P_5	P_5	P_3	P_4	P_1	P_2	P_0

Um die Summe zweier Permutationen zu finden, beispielsweise $P_2 + P_4$ muss man die Zeile nehmen, in deren Überschrift ("erster Summand") die erste Permutation steht (in unserem Falle P_2), und die Spalte, in deren Überschrift ("zweiter Summand") die zweite Permutation steht (in unserem Falle P_4). Im Schnittpunkt der gewählten Zeile mit der gewählten Spalte steht die gesuchte Summe: $P_2 + P_4 = P_1$.

Wir führen die Rechnung ausführlich durch:

$$P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad ; \qquad P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

nach derselben Überlegung wie bei Gleichung (1) gilt

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

also ist tatsächlich $P_2 + P_4 = P_1$.
Dem Leser bleibt es überlassen, auf diese Weise die gesamte Additionstafel nachzuprüfen.
Man überzeugt sich sofort davon, dass diese Addition das assoziative Gesetz erfüllt.

Das neutrale Element (die "Null") ist offensichtlich die identische Permutation

$$P_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

Schließlich existiert zu jeder Permutation die entgegengesetzte, die, zu ihr summiert, die identische Permutation liefert: Die zu einer vorgegebenen entgegengesetzte Permutation bringt alle in der gegebenen Permutation geänderten Ziffern an ihren alten Platz zurück. So gilt zum Beispiel

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

Um in der Additionstafel sofort die zu einer vorgegebenen entgegengesetzte Permutation zu finden, muss man in der zur vorgegebenen Permutation gehörigen Zeile das Element P_0 suchen; die Überschrift der zu diesem P_0, gehörigen Spalte ist dann gerade die gesuchte entgegengesetzte.
Wie man leicht sieht, gilt:

$$-P_0 = P_0; -P_1 = P_1; -P_2 = P_2; -P_3 = P_4; -P_4 = P_3; -P_5 = P_5$$

Also erfüllt die Addition der Permutationen sämtliche Gruppenaxiome. Die Gesamtheit aller Permutationen von drei Elementen ist somit eine Gruppe. Wir bezeichnen sie mit S_3.

Die Gruppe S_3 ist endlich, von der Ordnung 6. Sie ist nicht kommutativ. Beispielsweise gilt nämlich: $P_2 + P_3 = P_5$, $P_3 + P_2 = P_1$.

2.2 Der Begriff der Untergruppe

2.2.1 Erläuterung um Beispiel der Permutationsgruppen

1. Beispiele und Definition

Naturgemäß fragt man sich nun: Ist es möglich, eine Gruppe zu erhalten, die nicht aus allen, sondern nur aus gewissen Permutationen von drei Ziffern besteht, und gelten bei Beschränkung auf dieses Teilsystem wiederum dieselben Gesetze der Addition ? Man überzeugt sich leicht davon, dass das möglich ist.

Betrachten wir zum Beispiel das Elementpaar P_0 und P_1. Aus der Additionstafel entnimmt man

$$P_0 + P_0 = P_0; P_0 + P_1 = P_1; P_1 + P_0 = P_1; P_1 + P_1 = P_0$$

Wir sehen, dass alle Gruppenaxiome erfüllt sind, insbesondere ist $-P_0 = P_0$ und $-P_1 = P_1$. Das bedeutet, dass die beiden Elemente P_0 und P_1 eine Gruppe bilden, die ein Teil der Gruppe aller Permutationen von drei Ziffern ist.

Ebenso überzeugt man sich davon, dass auch das Paar der Elemente P_0 und P_2 seinerseits eine Gruppe bildet wie euch das Paar P_0 und P_5.
Das Paar P_0 und P_3 und auch das Paar P_0 und P_4 bilden keine Gruppen, da $P_3 + P_3 = P_4$, d.h. die Summe des Elementes P_3 mit sich selbst kein Element unseres Paares ist.

Diese einfachen Überlegungen rechtfertigen die Einführung folgender allgemeinen Definition:

Ist irgendeine Gruppe G gegeben und ist die Menge H, die aus gewissen Elementen unserer Gruppe G besteht, bei den in G bestehenden Additionsgesetzen eine Gruppe, so heißt H Untergruppe der Gruppe G.

Daher ist jedes der Elementpaare (P_0, P_1), (P_0, P_2), (P_0, P_5) eine Untergruppe der Ordnung 2 der Gruppe S_3. Andere Untergruppen der Ordnung 2 hat die Gruppe S_3 nicht:

Aus der Definition der Untergruppe folgt, dass jede Untergruppe H der Gruppe G das neutrale Element der Gruppe G enthalten muss; also hat jede Untergruppe der Ordnung 2 der Gruppe S_3 die Form (P_0, P_i), wobei i eine der Zahlen 1, 2, 3, 4, 5 ist. Wir haben aber gesehen, dass i weder gleich 3 noch gleich 4 sein kann, somit bleiben nur die betrachteten Untergruppen

$$(P_0, P_1); (P_0, P_2); (P_0, P_5)$$

In der Gruppe S_3 gibt es auch eine aus drei Elementen bestehende Untergruppe (eine Untergruppe der Ordnung 3). Dies ist die Untergruppe (P_0, P_3, P_4). Der Leser möge sich davon überzeugen, dass diese die einzige in S_3 enthaltene Untergruppe der Ordnung 3 ist. Untergruppen der Ordnungen 4 und 5 kommen in der Gruppe S_3 überhaupt nicht vor.[12]

Somit gibt es folgende Untergruppen der Gruppe S_3: Drei Untergruppen der Ordnung 2, nämlich (P_0, P_1), (P_0, P_2), (P_0, P_5); eine Untergruppe der Ordnung 3, nämlich (P_0, P_3, P_4). Auf die gleiche Weise, wie wir die Gruppe S_3 untersucht haben, kann man auch die Gruppe S_4 untersuchen, die aus allen Permutationen von vier Ziffern besteht.
Die Gruppe S_4 hat die Ordnung $1 \cdot 2 \cdot 3 \cdot 4 = 24$.
Allgemein bilden für beliebiges n die Permutationen von n Ziffern die Gruppe S_n der Ordnung $1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$.

Die Additionsgesetze sind in allen diesen Gruppen die gleichen: Die Addition zweier Permutationen von n Ziffern bedeutet das Hintereinanderausführen dieser Permutationen, in der Reihenfolge von links nach rechts.
Wir bemerken schließlich, dass man die Gruppe S_n aller Permutationen von n Elementen oft auch als symmetrische Gruppe der Permutationen von n Elementen bezeichnet. Jede Untergruppe der Gruppe S_n heißt Permutationsgruppe.

2.2.2 Bedingung, dass eine Teilmenge einer Gruppe eine Untergruppe ist

Um nachzuweisen, dass eine gewisse Teilmenge H einer Gruppe G eine Untergruppe ist, benutzt man zweckmäßigerweise folgenden allgemeinen Satz:

Eine Teilmenge H einer Gruppe G ist dann und nur dann eine Untergruppe der Gruppe G, wenn folgende Bedingungen erfüllt sind:
1. Die Summe zweier Elemente a und b von H (im Sinne der in G definierten Addition) ist ein Element der Menge H.
2. Das neutrale Element der Gruppe G ist Element der Menge H.
3. Das entgegengesetzte Element jedes Elementes der Menge H ist Element der Menge H.

[12] Davon kann man sich überzeugen durch eine Untersuchung der 10 Teilmengen der Gruppe S_3, die das Element P_0 enthalten und aus vier Elementen bestehen, sowie der 5 Teilmengen, die einschließlich P_0 fünf Elemente enthalten. Das Fehlen von Untergruppen der Ordnung 4 und 5 in der Gruppe S_3 folgt aber unmittelbar aus dem nachstehenden allgemeinen Satz, der später bewiesen wird (Kapitel VIII): Die Ordnung jeder Untergruppe H einer endlichen Gruppe G ist ein Teiler der Ordnung der Gruppe G.

Zum Beweis genügt es, zu bemerken, dass unsere Bedingungen gerade die Forderungen ausdrücken, dass die Einschränkung auf H der in G definierten Addition alle Axiome des Gruppenbegriffes erfüllt.
Das assoziative Gesetz braucht man nicht zu fordern: Dieses ist für die Addition beliebiger Elemente der Menge G erfüllt, insbesondere also auch in dem Spezialfall, dass diese Elemente der Menge H angehören.

2.3 Permutationen als Abbildungen einer endlichen Menge auf sich

Gerade und ungerade Permutationen[13]

1. Wir haben den Begriff der Permutation in der elementaren und etwas primitiven Weise untersucht, wie man dies gewöhnlich macht. Wenn man sich nicht vor allgemein-mathematischen Redewendungen fürchtet, kann man eine Permutation von n Elementen einfach als eine eineindeutige Abbildung f der Menge der vorgegebenen n Elemente auf sich definieren.

Wir nehmen an, unsere Elemente seien die Zahlen $1, 2, 3, ..., n$; dann ist eine Permutation

$$\begin{pmatrix} 1 & 2 & 3 & ... & n \\ a_1 & a_2 & a_3 & ... & a_n \end{pmatrix}$$

als eine Funktion

$$a_k = f(k) \qquad ; \qquad k = 1, 2, ..., n$$

gegeben, wobei sowohl die Argument- als auch die Funktionswerte die Zahlen $1, 2, 3, ..., n$ sind. Für zwei verschiedene Argumentwerte sind die Funktionswerte immer verschieden. Insbesondere ist eine Permutation vollständig bestimmt, wenn für jedes k der Wert $f(k)$, also a_k bekannt ist.

Daraus folgt, dass es völlig unwesentlich ist, in welcher Reihenfolge die Zahlen in der oberen Zeile geschrieben sind: Wichtig ist lediglich, dass unter der Zahl k das entsprechende a_k geschrieben steht.
Beispielsweise stellen

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} 3 & 4 & 5 & 2 & 1 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}$$

zwei Schreibweisen ein und derselben Permutation dar. Diese im Grunde selbstverständliche Bemerkung kann man auch so formulieren:
Es sei die Permutation

$$A = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ a_1 & a_2 & a_3 & ... & a_n \end{pmatrix} \tag{1}$$

vorgegeben. Ist dann

$$P = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ p_1 & p_2 & p_3 & ... & p_n \end{pmatrix} \tag{2}$$

irgendeine Permutation derselben Zahlen $1, 2, 3, ..., n$, so lässt sich die Permutation (1) auch in der Form

$$\begin{pmatrix} p_1 & p_2 & p_3 & ... & p_n \\ a_{p_1} & a_{p_2} & a_{p_3} & ... & a_{p_n} \end{pmatrix} \tag{1}$$

[13] Der Leser, dem dieser Paragraph Schwierigkeiten bereitet. kann ihn bei der ersten Lektüre fortlassen und braucht lediglich vor Kapitel VI darauf zurückzukommen. Vor der Lektüre dieses Paragraphen muss der Leser jedenfalls mit dem gesamten Anhang vertraut sein, der am Schluss des Buches angefügt ist.

schreiben.

2. Gerade und ungerade Permutationen. Es sei die Permutation

$$A = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ a_1 & a_2 & a_3 & ... & a_n \end{pmatrix} \tag{1}$$

vorgegeben.
Wir betrachten eine beliebige Menge, die aus irgend zwei der Zahlen $1, 2, 3, ..., n$ besteht, und nennen diese beiden Zahlen i und k. Diese Menge heißt Zahlenpaar[14] Sie ist das Paar, das aus den Elementen i und k besteht und mit (i, k) bezeichnet wird. Bekanntlich ist die Anzahl aller Paare, die man aus n vorgegebenen Elementen bilden kann, gleich [15]

$$\binom{n}{k} = \frac{n(n-1)}{1 \cdot 2}$$

Das Paar, das aus den Elementen i und k besteht, heißt regulär in bezug auf die Permutation A, wenn die Differenzen $i - k$ und $a_i - a_k$ ein und dasselbe Vorzeichen haben. Dies bedeutet:

Ist $i < k$, so muss $a_i < a_k$ sein, ist $i > k$, so muss $a_i > a_k$ sein. Anderenfalls sagt man; dass unser Paar in bezug auf die Permutation irregulär ist oder eine Inversion bildet. Wenn folglich das Paar (i, k) eine Inversion bildet, so gilt entweder $i < k$ und $a_i > a_k$ oder umgekehrt $i > k$ und $a_i < a_k$.

Wir betrachten als Beispiel die Permutationen der Gruppe S_3. In der Permutation $P_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ gibt es keine einzige Inversion, alle Paare sind regulär.
In der Permutation $P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ gibt es die einzige Inversion $(2, 3)$.
In der Permutation $P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ gibt es die einzige Inversion $(1, 2)$.
In der Permutation $P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ gibt es zwei Inversionen $(1, 3)$ und $(1, 2)$.
In der Permutation $P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ gibt es zwei Inversionen $(1, 3)$ und $(2, 3)$.
In der Permutation $P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ gibt es drei Inversionen $(1, 2)$, $(1, 3)$ und $(2, 3)$.

Definition. Eine Permutation, die eine gerade Anzahl von Inversionen enthält, heißt gerade Permutation; eine Permutation, die eine ungerade Anzahl von Inversionen enthält, heißt ungerade Permutation.

Wir haben gesehen, dass die geraden Permutationen P_0, P_3 und P_4 in der Gruppe S_3 eine Untergruppe bilden. Wir stellen uns jetzt die Aufgabe, zu beweisen, dass dies für jede Gruppe S_n gilt.

[14] Hier wird mit dem Begriff des Paares keine Voraussetzung über die Reihenfolge der Elemente des Paares verbunden: (i, k) und (k, i) sind zwei Schreibweisen ein und desselben Paares. Die Elementpaare, die man aus vorgegebenen Elementen herausgreifen kann, heißen auch Kombinationen 2. Klasse der Elemente.

[15] Die Kombinationen k-ter Klasse von n Elementen sind die sämtlichen aus k Elementen bestehenden Teilmengen der Menge von n Elementen. Diese Methode erlaubt es übrigens, die logische Unzulänglichkeit zu vermeiden, die beim Schulunterricht in Kombinatorik oft begangen wird.

Der Beweis stützt sich auf einige Vorbemerkungen, zu denen wir jetzt übergehen.
Unter dem Signum der Permutation A verstehen wir die Zahl $+1$, wenn die Permutation A gerade, und die Zahl -1, wenn sie ungerade ist.
Abweichend vom üblichen Sprachgebrauch bezeichnen wir jetzt als Signum einer rationalen Zahl r bei $r > 0$ die Zahl $+1$, bei $r < 0$ die Zahl -1 und bei $r = 0$ die Zahl 0.
Das Signum der Zahl r bezeichnen wir mit $(\text{sgn}r)$.

Bei diesen Bezeichnungen ist klar, dass das Signum der Permutation A gleich ist dem Produkt der Sigma aller $\frac{n(n-1)}{2}$ Zahlen $\frac{i-k}{a_i-a_k}$; dabei wird der Bruch

$$\frac{i-k}{a_i-a_k} = \frac{k-i}{a_k-a_i}$$

Paar, das den Zahlen $1, 2, 3, ..., n$ entnommen ist, nur einmal gebildet. Diese Bemerkung benutzen wir zum Beweis des folgenden Satzes:

Das Signum der Summe zweier Permutationen ist gleich dem Produkt der Sigma der Summanden.

Es seien zwei Permutationen vorgegeben:

$$A = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ a_1 & a_2 & a_3 & ... & a_n \end{pmatrix} \quad , \quad B = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ b_1 & b_2 & b_3 & ... & b_n \end{pmatrix}$$

Ihre Summe ist offensichtlich die Permutation

$$A + B = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ b_{a_1} & b_{a_2} & b_{a_3} & ... & b_{a_n} \end{pmatrix} \tag{1}$$

Das Signum von A ist gleich dem Produkt der Sigma aller

$$\frac{i-k}{a_i-a_k}$$

Das Signum von B ist gleich dem Produkt der Sigma aller

$$\frac{i-k}{b_i-b_k}$$

Da man aber auch

$$B = \begin{pmatrix} a_1 & a_2 & a_3 & ... & a_n \\ b_{a_1} & b_{a_2} & b_{a_3} & ... & b_{a_n} \end{pmatrix}$$

schreiben kann, so gilt:
Das Signum von B ist gleich dem Produkt der Sigma aller $\frac{a_i-a_k}{b_{a_i}-b_{a_k}}$. Daraus folgt sofort:

$$\begin{aligned}(\text{sgn}A)\cdot(\text{sgn}B) &= \text{Produkt aller } \left(\text{sgn}\frac{i-k}{a_i-a_k}\right)\cdot\left(\text{sgn}\frac{a_i-a_k}{b_{a_i}-b_{a_k}}\right) \\ &= \text{Produkt aller } \left(\text{sgn}\frac{i-k}{a_i-a_k}\cdot\frac{a_i-a_k}{b_{a_i}-b_{a_k}}\right) \\ &= \text{Produkt aller } \left(\text{sgn}\frac{i-k}{b_{a_i}-b_{a_k}}\right)\end{aligned}$$

Das letzte Produkt ist aber das Signum der Permutation

$$\begin{pmatrix} a_1 & a_2 & a_3 & ... & a_n \\ b_{a_1} & b_{a_2} & b_{a_3} & ... & b_{a_n} \end{pmatrix}$$

also der Permutation $A + B$, was zu beweisen war.

Alle dem bewiesenen Satz folgt unmittelbar: Die Summe zweier gleichartiger Permutationen[16] ist eine gerade, hingegen die Summe zweier ungleichartiger Permutationen[17] eine ungerade Permutation.

Die identische Permutation enthält keine einzige Inversion und ist folglich eine gerade Permutation. Ferner ist

$$A + (-A) = 0$$

also ist die Summe einer vorgegebenen Permutation A und der ihr entgegengesetzten eine gerade Permutation. Daraus folgt nach dem eben Bewiesenen, dass eine Permutation und die ihr entgegengesetzte jeweils zur selben Klasse gehören.

Somit gilt: Die Summe zweier gerader Permutationen ist eine gerade Permutation, die identische Permutation ist eine gerade Permutation, die entgegengesetzte einer geraden Permutation ist eine gerade Permutation.
Daraus folgt, dass die Gesamtheit aller geraden Permutationen von n Elementen eine Untergruppe der Gruppe S_n aller überhaupt möglichen Permutationen von n Elementen ist. Die Gruppe der geraden Permutationen von n Elementen heißt alternierende (d.h. vorzeichenändernde) Permutationsgruppe von n Elementen und wird mit A_n bezeichnet.

Satz. Die Ordnung der Gruppe A_n ist gleich $n!$.

Mit anderen Worten, in der Gruppe A_n kommt gerade die Hälfte aller Permutationen von n Elementen vor. Um sich davon zu überzeugen, genügt es, eine eineindeutige Beziehung zwischen der Menge aller geraden und der Menge aller ungeraden Permutationen von n Elementen herzustellen. Diese Beziehung stellt man her, indem man irgendeine bestimmte ungerade Permutation P wählt und jeder geraden Permutation A die Permutation $P + A$ zuordnet. Auf diesem Wege erhält man:

1. Jeder geraden Permutation entspricht eine ungerade Permutation.
2. Zwei verschiedenen geraden Permutationen entsprechen verschiedene ungerade Permutationen.
3. Jede ungerade Permutation B ist einer (und nur einer) geraden Permutation zugeordnet, nämlich der Permutation $-P + B$.

Somit ist dies eine eineindeutige Zuordnung zwischen der Menge aller geraden und der Menge aller ungeraden Permutationen.

[16] Also die Summe zweier gerader oder zweier ungerader Permutationen
[17] Also die Summe einer geraden und einer ungeraden oder einer ungeraden und einer geraden Permutation

3 Einige allgemeine Bemerkungen über Gruppen

Der Begriff des Isomorphismus

3.1 Die „additive“ und die „multiplikative“ Terminologie in der Gruppentheorie

Die Hauptbestandteile des Gruppenbegriffs sind:

a) Die Menge der Gegenstände (Zahlen, Permutationen, Drehungen usw.), welche die Elemente der Gruppe ausmachen;

b) eine bestimmte Operation oder Verknüpfung, die wir Addition nennen und die es gestattet, zu je zwei Elementen a und b unserer Gruppe ein drittes Element $a + b$ derselben Gruppe zu finden.

Wir haben das Wort Addition zur Bezeichnung der in unserer Gruppe vorliegenden Verknüpfung gewählt. Selbstverständlich hat die Wahl dieses oder eines anderen Wortes im Grunde keinen Einfluss.
Für jede Gruppe könnte man ebenso von der Multiplikation ihrer Elemente sprechen statt von ihrer Addition, indem man nicht die additive, sondern die multiplikative Terminologie benutzt. Mit der additiven Schreibweise einer Gruppe sind wir bereits vertraut.

Jetzt wollen wir überlegen, wie sich die Gruppenaxiome in multiplikativer Schreibweise ausdrücken lassen.
Zunächst fordern wir, dass für je zwei Elemente a und b unserer Menge G (siehe Kap. I, § 2) eindeutig das Element $a \cdot b$, das Produkt der beiden Elemente a und b, definiert ist.
Die Gruppenaxiome selbst erhalten dann folgende Gestalt.
I. Die Bedingung der Assoziativität:

$$(ab)c = a(bc).$$

II. Die Bedingung der Existenz eines neutralen Elementes.
Unter den Elementen von G gibt es ein eindeutig bestimmtes Element, das wir neutrales Element nennen und mit e (Eins) bezeichnen derart, dass $ae = a = ea$ bei beliebiger Wahl des Elementes a gilt.

III. Die Bedingung der Existenz eines inversen Elementes zu jedem vorgegebenen Element.
Zu jedem vorgegebenen Element a der Menge G kann man ein und nur ein Element a^{-1} derselben Menge G finden, so dass

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

gilt.
Wir sehen: Wird die in einer vorgegebenen Gruppe definierte und ursprünglich als Addition bezeichnete Verknüpfung als Multiplikation aufgefasst, so ist es sinnvoll, das neutrale Element Null in Eins umzubenennen und von inversen Elementen (a^{-1}) statt von entgegengesetzten $(-a)$ zu sprechen.

Historisch ist diese "multiplikative" Terminologie die erste; sie wird gegenwärtig von fast allen Autoren benutzt. In manchen Fällen ist die additive, in anderen Fällen die multiplikative Schreibweise vorzuziehen. Schließlich gibt es Fälle, in denen beide gleich bequem sind.

Ein Beispiel, bei dem natürlich die additive Schreibweise am bequemsten ist, stellt die Gruppe der ganzen Zahlen dar: Die Gruppenoperation ist hier die übliche arithmetische Addition, das neutrale Element die arithmetische Null; der Begriff der entgegengesetzten Zahl hat hier seinen üblichen arithmetischen Sinn.

Man kann einwenden, dass es ungewohnt und unbequem sei, die übliche arithmetische Addition in Multiplikation, die Null in Eins usw. umzubenennen.
Jedoch muss dem Leser klar sein, dass diese Umbenennung, von allen ihren Unbequemlichkeiten abgesehen, durchaus möglich ist und jedenfalls solange auf keinerlei Widerspruch führt, wie wir uns auf das Studium nur der Gruppe der ganzen Zahlen beschränken, also eine einzige Operation unter den ganzen Zahlen betrachten, nämlich die arithmetische Addition.
Würden wir neben der arithmetischen Addition auch noch die im elementaren, arithmetischen Sinne des Wortes verstandene Multiplikation betrachten, so ergäbe die vorhin besprochene Umbenennung der Addition in Multiplikation natürlich eine gänzlich undurchsichtige Terminologie.

Als Beispiel einer Gruppe, für die umgekehrt die multiplikative Sprechweise passender ist, betrachten wir die Gruppe R, die aus allen positiven und negativen rationalen Zahlen[18], also aus allen von Null verschiedenen rationalen Zahlen besteht. Als Gruppenoperation in der Gruppe R verwenden wir die übliche arithmetische Multiplikation. Sie ist bekanntlich assoziativ. Die gewöhnliche Eins erfüllt hinsichtlich dieser Operation die Bedingung II:

$$a \cdot 1 = a \qquad \text{für beliebiges } a$$

Schließlich existiert für jedes Element der Menge R (also für jede rationale Zahl $a \neq 0$) eine rationale Zahl $a^{-1} = \frac{1}{a} \neq 0$, die der Bedingung $a \cdot a^{-1} = 1$ genügt. Also sind sämtliche Gruppenaxiome erfüllt, d.h., die von Null verschiedenen rationalen Zahlen bilden bezüglich der arithmetischen Multiplikation eine Gruppe.
Wegen $ab = ba$ ist diese Gruppe kommutativ. Sie enthält als Untergruppe die Gruppe aller positiven rationalen Zahlen ($a > 0$). Bei diesen Gruppen benutzt man natürlich die multiplikative Schreibweise.

Der Leser möge sich davon überzeugen, dass die negativen rationalen Zahlen bezüglich der gewöhnlichen arithmetischen Multiplikation keine Gruppe bilden.
Auch die Gesamtheit aller rationalen Zahlen (einschließlich der Null) bildet keine Gruppe bezüglich der arithmetischen Multiplikation, da keine zur Null inverse Zahl existiert. Hingegen ist, wie man leicht sieht, die Menge aller rationalen Zahlen eine Gruppe R bezüglich der arithmetischen Addition. In dieser Gruppe ist als Untergruppe die Gruppe der ganzen Zahlen enthalten.

Abschließend bemerken wir zu diesen Fragen der Terminologie, dass es bei Permutationsgruppen keinen ernsthaften Grund dafür gibt, die additive der multiplikativen Schreibweise oder umgekehrt vorzuziehen. Bei der multiplikativen Schreibweise erhält jedoch einer der Sätze des vorigen Kapitels eine symmetrische Gestalt, nämlich:
Das Signum des Produktes zweier Permutationen ist gleich dem Produkt ihrer Sigma.

Gegenwärtig geht man immer mehr dazu über, die kommutativen Gruppen in der additiven Schreibweise zu behandeln; doch haben wir eben eine Ausnahme dieser Regel kennengelernt, als wir von der Gruppe der von Null verschiedenen rationalen Zahlen sprachen. In diesem Buche wollen wir auch bei den nichtkommutativen Gruppen die additive Schreibweise beibehalten.

[18] Als rationale Zahlen erklärt man alle ganzen Zahlen sowie alle Brüche p/q (p, q ganz, $q \neq 0$).

3.2 Isomorphe Gruppen

Wir betrachten einerseits die Drehungsgruppe R, eines gleichseitigen Dreiecks (Kap. I, § l) und andererseits die in der Gruppe aller Permutationen von drei Ziffern enthaltene Untergruppe A_3, die aus den drei Elementen P_0, P_3, P_4 (Kap. II, § 2) besteht. Wir bezeichnen die Elemente der Gruppe R_3 mit a_0, a_1, a_2. Wir stellen jetzt zwischen den Elementen der Gruppe R_3 und den Elementen der Gruppe A_3 folgende eineindeutige Zuordnung her:

$$a_0 \longleftrightarrow P_0, \qquad a_1 \longleftrightarrow P_3, \qquad a_2 \longleftrightarrow P_4$$

Diese Zuordnung ist additionsinvariant in folgendem Sinne:
Kann in R_3 irgendein Element als Summe zweier Elemente aus R_3 geschrieben werden, gilt also etwa $a_0 + a_1 = a_1$ oder $a_1 + a_1 = a_2$ oder $a_1 + a_2 = a_0$, und ersetzt man jedes Element der erhaltenen Gleichungen durch die entsprechenden Elemente aus A_3 so bleibt die Gleichung in A_3 gültig.

Wir sehen, dass die Gruppen R_3 und A_3, obwohl sie aus Elementen verschiedener Natur bestehen (die eine Gruppe besteht aus Drehungen eines Dreiecks und die andere aus Permutationen von Ziffern), gleiche Struktur haben: Die Additionstafeln dieser Gruppen unterscheiden sich lediglich durch die Bezeichnungen. Ändern wir also die Bezeichnungen, benennen wir also die Elemente um, so erhalten wir identische Gruppentafeln.

Gruppen, deren Additionstafeln bei geeigneter Wahl der Elementbezeichnung identisch werden, heißen isomorphe Gruppen.
Der übliche Begriff des Isomorphismus ist etwas anders erklärt. Die "Umbenennung" der Elemente in der Additionstafel, von der in dieser Definition des Isomorphismus die Rede ist, besteht im wesentlichen darin, dass eine eineindeutige Zuordnung zwischen den Elementen der beiden Gruppen hergestellt wird. Wir geben dementsprechend jetzt eine Definition des Isomorphismus, die unmittelbar vom Begriff der eineindeutigen Abbildung ausgeht.

Definition I. Es sei eine eineindeutige Zuordnung

$$g \longleftrightarrow g'$$

zwischen der Menge aller Elemente der Gruppe G und der Menge aller Elemente der Gruppe G' vorgegeben. Wir wollen sagen, dass diese Zuordnung eine isomorphe Zuordnung (oder ein Isomorphismus) zwischen den beiden Gruppen ist, wenn die Bedingung der Invarianz der Addition erfüllt ist; diese lautet:
Gilt eine beliebige Relation der Form

$$g_1 + g_2 = g_3$$

zwischen den Elementen einer Gruppe, beispielsweise G, so ist auch die Relation richtig, die man erhält, wenn man die Elemente g_1, g_2, g_3 der Gruppe G durch die ihnen in der Gruppe G' zugeordneten Elemente g_1', g_2', g_3' ersetzt:

$$g_1' + g_2' = g_3'$$

Definition II. Zwei Gruppen heißen isomorph, wenn man zwischen ihnen eine isomorphe Zuordnung herstellen kann.

Anmerkung. Fordert man, dass aus $g_1 + g_2 = g_3$ in der Gruppe G stets $g_1' + g_2' = g_3'$ für

die den Elementen g_1, g_2, g_3 entsprechenden Elemente der Gruppe G' folgt, so gilt auch die umgekehrte Behauptung, nämlich:
Gilt für irgend drei Elemente g'_1, g'_2, g'_3 der Gruppe G' die Relation

$$g'_1 + g'_2 = g'_3$$

so ist für die den Elementen g'_1, g'_2, g'_3 entsprechenden Elemente g_1, g_2, g_3 der Gruppe G auch die Relation

$$g_1 + g_2 = g_3 \tag{1}$$

erfüllt. Würde nämlich die Relation (1) nicht gelten, so wäre also

$$g_1 + g_2 = g_4 \neq g_3$$

Wegen der eineindeutigen Zuordnung zwischen G und G' entspräche dem Element g_4 der Gruppe G in der Gruppe G' ein Element g'_4, das von g'_3 verschieden wäre; nach unserer Voraussetzung muss aus

$$g_1 + g_2 = g_4$$

die Gleichung

$$g'_1 + g'_2 = g'_4$$

folgen, im Widerspruch zu

$$g'_1 + g'_2 = g'_3$$

Satz. Bei der isomorphen Abbildung

$$g \longleftrightarrow g'$$

der Gruppe G auf die Gruppe G' entspricht dem neutralen Element der einen Gruppe das neutrale Element der anderen Gruppe. Jedes Paar entgegengesetzter Elemente der einen Gruppe entspricht einem Paar entgegengesetzter Elemente der anderen Gruppe.

Es sei also g' das neutrale Element der Gruppe G und bei der gegebenen isomorphen Zuordnung zwischen den Gruppen G und G' entspreche ihm das Element g'_0 der Gruppe G'.
Wir beweisen, dass g'_0 das neutrale Element der Gruppe G' ist. Da g' das neutrale Element der Gruppe G ist, so gilt für jedes Element g derselben Gruppe

$$g + g' = g$$

Wegen der isomorphen Abbildung $g \longleftrightarrow g'$ gilt:

$$g' + g'_0 = g'$$

also ist g'_0 das neutrale Element der Gruppe G'.

Es sei g_1 und g_2 ein Paar entgegengesetzter Elemente der Gruppe G:

$$g_1 + g_2 = g_0$$

(wobei g_0 wie früher das neutrale Element der Gruppe G ist). Daraus folgt

$$g'_1 + g'_2 = g'_0$$

Da g'_0 das neutrale Element der Gruppe G' ist, sind also g'_1 und g'_2 entgegengesetzte Elemente von G'.

Übungen. 1. Man zeige, dass die Gruppe, die aus den beiden Elementen a_0 und a_1 mit der Additionstafel

	a_0	a_1
a_0	a_0	a_1
a_1	a_1	a_0

besteht, isomorph zur Gruppe der Drehungen eines Intervalls (um seinen Mittelpunkt) ist.

2. Man beweise, dass sämtliche Gruppen der Ordnung 2 zueinander isomorph sind.

3. Man beweise, dass alle Gruppen der Ordnung 3 zueinander isomorph sind.

Lösung. Es seien a_0, a_1, a_2 die Elemente einer Gruppe; es sei a_0 das Nullelement. Dann gilt

$$a_0 + a_0 = a_0 \qquad ; \qquad a_0 + a_1 = a_1 \qquad ; \qquad a_0 + a_2 = a_2$$

Es kann nicht $a_1 + a_1 = a_1$ sein, da dann $a_1 = a_0$ wäre. Also ist

$$a_1 + a_1 = a_2$$

Analog schließt man

$$a_1 + a_2 \neq a_2 \qquad \text{und} \qquad a_1 + a_2 \neq a_1$$

Daraus schließen wir, dass

$$a_1 + a_2 = a_0$$

gilt. Ebenso ergibt sich $a_2 + a_1 = a_0$. Schließlich ist

$$a_2 + a_2 \neq a_2$$

(da sonst $a_2 = a_0$ gelten würde) und $a_2 + a_2 \neq a_0$, (da $a_1 + a_2 = a_0$ ist). Also gilt

$$a_2 + a_2 = a_1$$

Somit ist für Gruppen der Ordnung 3 nur eine einzige Additionstafel möglich, nämlich

	a_0	a_1	a_2
a_0	a_0	a_1	a_2
a_1	a_1	a_2	a_0
a_2	a_2	a_0	a_1

4. Man beweise, dass jede kommutative Gruppe der Ordnung 4 entweder der Kleinschen Vierergruppe oder der Drehungsgruppe eines Quadrates isomorph ist (diese beiden Gruppen sind nicht zueinander isomorph).

5. Es ist zu beweisen, dass die Gruppe aller positiven Zahlen (mit der arithmetischen Multiplikation als Gruppenoperation) isomorph ist der Gruppe aller reellen Zahlen (mit der arithmetischen Addition als Gruppenoperation). Hinweis: Die isomorphe Abbildung wird durch den Logarithmus vermittelt.

3.3 Der Satz von Cayley

Wir beschließen dieses Kapitel mit dem Beweis des folgenden Satzes, der von Cayley[19] gefunden wurde.

[19]Der englische Mathematiker Cayley (geb. 1821, gest. 1895) war einer der Begründer der Gruppentheorie

Satz. Jede endliche Gruppe ist einer gewissen Permutationsgruppe isomorph.

Beweis. Es sei G eine endliche Gruppe, n ihre Ordnung,

$$a_1, a_2, ..., a_n$$

ihre Elemente, unter diesen sei a_1 das neutrale Element. Wir schreiben für jedes $i = 1, 2, 3, ..., n$ die Elemente

$$a_1 + a_i, \qquad a_2 + a_i, \qquad ..., \qquad a_n + a_i$$

auf. Bei festem i sind jedesmal alle diese Elemente verschieden; ihre Anzahl ist jedesmal gleich n; jedesmal sind es also dieselben Elemente a_1, a_2, ..., a_n, lediglich in anderer Reihenfolge. Es sei

$$a_1 + a_i = a_{i_1}, \quad a_2 + a_i = a_{i_2}, \quad ..., \quad a_n + a_i = a_{i_n}$$

Also entspricht dem Element a_i die Permutation

$$P_i = \begin{pmatrix} a_1 & a_2 & ... & a_n \\ a_1 + a_i & a_2 + a_i & ... & a_n + a_i \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & ... & a_n \\ a_{i_1} & a_{i_2} & ... & a_{i_n} \end{pmatrix}$$

oder auch die Permutation

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

die sich von der Permutation P_i nur dadurch unterscheidet, dass in P_i die Elemente der Gruppe G selbst, in P_i' dagegen die diesen Elementen eineindeutig entsprechenden Indizes permutiert werden.

Bei $i \neq k$, d.h. $a_i \neq a_k$ ist auch $P_i \neq P_k$; denn unter dem Element a_1 steht in der Permutation P_i das Element $a_1 + a_i = a_i$, in P_k jedoch $a_1 + a_k = a_k$.
Wir haben somit eine eineindeutige Zuordnung zwischen den Elementen a_1, a_2, ..., a_n der Gruppe G und den Permutationen P_1, P_2, ..., P_n hergestellt.

Jetzt müssen wir beweisen, dass erstens die Permutationen P_1, P_2, ..., P_n bezüglich der Addition von Permutationen eine Gruppe bilden und dass zweitens diese Gruppe zur Gruppe G isomorph ist.
Wir bemerken zunächst:

1. Unter den Permutationen P_1, P_2, ..., P_n ist die identische Permutation enthalten.
Da nämlich a_1 nach Voraussetzung das neutrale Element der Gruppe G ist, so ist die Permutation

$$P_1 = \begin{pmatrix} a_1 & a_2 & ... & a_n \\ a_1 + a_1 & a_2 + a_1 & ... & a_n + a_1 \end{pmatrix}$$

die identische Permutation.
Weiter beweisen wir: Ist $a_k = a_i + a_k$, so auch $P_k = P_i + P_k$. Zunächst bemerken wir, dass

$$\begin{pmatrix} a_1 & a_2 & ... & a_n \\ a_1 + a_k & a_2 + a_k & ... & a_n + a_k \end{pmatrix}$$

und

$$\begin{pmatrix} a_1 + a_i & a_2 + a_i & ... & a_n + a_i \\ a_1 + a_i + a_k & a_2 + a_i + a_k & ... & a_n + a_i + a_k \end{pmatrix}$$

zwei Schreibweisen ein und derselben Permutation P_k darstellen. Beide Schreibweisen zeigen, dass jedem Element a der Gruppe G bei der Zuordnung das Element $a + a_k$ derselben Gruppe entspricht.
Also können wir schreiben:

$$P_k = \begin{pmatrix} a_1 + a_i & a_2 + a_i & ... & a_n + a_i \\ a_1 + a_i + a_k & a_2 + a_i + a_k & ... & a_n + a_i + a_k \end{pmatrix}$$

Hieraus ersieht man, dass die Permutation

$$P_i + P_k = \begin{pmatrix} a_1 & a_2 & ... & a_n \\ a_1 + a_i & a_2 + a_i & ... & a_n + a_i \end{pmatrix} + \begin{pmatrix} a_1 + a_i & a_2 + a_i & ... & a_n + a_i \\ a_1 + a_i + a_k & a_2 + a_i + a_k & ... & a_n + a_i + a_k \end{pmatrix}$$

nach der allgemeinen Definition der Addition von Permutationen mit der Permutation

$$\begin{pmatrix} a_1 & a_2 & ... & a_n \\ a_1 + a_i + a_k & a_2 + a_i + a_k & ... & a_n + a_i + a_k \end{pmatrix}$$

identisch ist. Wegen $a_i + a_k = a_k$ gilt

$$\begin{pmatrix} a_1 & a_2 & ... & a_n \\ a_1 + a_i + a_k & a_2 + a_i + a_k & ... & a_n + a_i + a_k \end{pmatrix} = P_k$$

d.h. $P_i + P_k = P_k$.
Dieses Ergebnis lässt sich so formulieren:

IIa. Der Summe zweier Elemente der Gruppe G entspricht die Summe der diesen Elementen zugeordneten Permutationen.
Daraus folgt:

IIb. Die Summe je zweier beliebiger Permutationen aus der Gesamtheit der Permutationen P_1, P_2, ..., P_n ist eine der Permutationen P_1, P_2, ..., P_n.

Wir betrachten die Permutation P_i das Element a_i und das Element $-a_i = a_k$. Da $a_i + a_k = a_1$ ist, so ist nach dem eben Bewiesenen $P_i + P_k = P_1$; P_1 aber ist, wie wir gesehen haben, die identische Permutation, also ist $P_k = -P_i$.
Also gilt:

III. Die Permutation $-P_i$, ist für beliebiges $i = l, 2, ..., n$ eine der Permutationen P_1, P_2, ..., P_n. Aus IIb, I und III folgt, dass die Gesamtheit der Permutationen P_1, P_2, ..., P_n bei der gewöhnlichen Definition der Addition von Permutationen eine Gruppe ist.

Aus IIa folgt, dass diese Gruppe isomorph zur Gruppe G ist.
Der Cayleysche Satz ist damit bewiesen.

4 Zyklische Untergruppen einer vorgegebenen Gruppe

4.1 Die von einem vorgegebenen Element einer gegebenen Gruppe erzeugte Untergruppe

Es sei a ein willkürliches Element einer Gruppe G. Wir addieren es zu sich selbst, bilden also das Element $a + a$. Dieses Element bezeichnen wir mit $2a$. Ich betone: $2a$ ist lediglich eine Bezeichnung des Elementes $a + a$, keinesfalls ist dabei von der Multiplikation des Elementes a mit 2 die Rede.
Ebenso bezeichnen wir $a + a + a$ mit $3a$, allgemein setzen wir

$$\underbrace{a + a + ... + a}_{n-\text{mal}} = na$$

Wir betrachten ferner das Element $-a$ und bezeichnen nacheinander

$$\begin{aligned} (-a) + (-a) \quad & \text{mit} \quad -2a; \\ (-a) + (-a) + (-a) \quad & \text{mit} \quad -3a; \\ & \ldots \\ \underbrace{(-a) + (-a) + ... + (-a)}_{n-\text{mal}} \quad & \text{mit} \quad -na. \end{aligned}$$

Diese Bezeichnungen werden dadurch gerechtfertigt, dass tatsächlich

$$na + (-na) = 0$$

gilt. Zum Beweis dieser Behauptung bemerken wir zunächst, dass sie im Falle $n = 1$ offenbar richtig ist (dies folgt aus der Definition von $-a$). Wir nehmen an, sie sei für $n - 1$ richtig, und beweisen unter dieser Voraussetzung ihre Gültigkeit für n. Es gilt

$$na + (-na) = [a + (n-1)a] + [-(n-1)a + (-a)] = a + (n-1)a + [-(n-1)a] + (-a)$$

Nach unserer Annahme ist aber die geschweifte Klammer gleich Null, also gilt

$$na + (-na) = a + 0 + (-a) = a + (-a) = 0$$

was zu beweisen war.
Wir haben den Ausdruck na für beliebiges positives und beliebiges negatives n definiert. Wir setzen schließlich definitionsgemäß $0a = 0$ (wobei 0 links die Zahl Null und 0 rechts das neutrale Element der Gruppe G bedeutet).

Es seien jetzt p und q zwei ganze Zahlen.
Aus unserer Definition folgt, dass für beliebige ganze p und q gilt

$$pa + qa = (p + q)a$$

Wir erhalten folgendes Resultat:
Die Menge $H(a)$ der Elemente einer Gruppe G, die man in der Form na mit ganzem n darstellen kann, bildet bezüglich der in der Gruppe G definierten Addition eine Gruppe $H(a)$.

Es gilt nämlich:
1. Die Summe zweier Elemente, die zu $H(a)$ gehören, ist wieder ein Element von $H(a)$;
2. die Null gehört zu $H(a)$;
3. zu jedem Element ma aus $H(a)$ gibt es ein Element $-ma$, das ebenfalls zu $H(a)$ gehört.

Also ist $H(a)$ eine Untergruppe von G. Diese Untergruppe bezeichnet man als die von dem Element a erzeugte Untergruppe der Gruppe G.

4.2 Endliche und unendliche zyklische Gruppen

Die Gruppe $H(a)$ haben wir definiert als die Gruppe, die aus all denjenigen Elementen der Gruppe G besteht, die in der Form ma darstellbar sind. Wir haben aber noch nicht die Frage gestellt:
Ergeben zwei Schreibweisen m_1a und m_2a mit verschiedenen ganzen m_1 und m_2 immer zwei verschiedene Elemente der Gruppe G, oder kann es eintreten, dass $m_1a = m_2a$ ist, während m_1 und m_2 verschieden sind ?

Damit wollen wir uns jetzt befassen. Es mögen zwei voneinander verschiedene ganze Zahlen m_1 und m_2 existieren, für die $m_1a = m_2a$ ist. Addiert man auf beiden Seiten der letzten Gleichung das Element $-m_1a$, so erhält man:

$$0 = (m_2 - m_1)a$$

Folglich existiert eine ganze Zahl m mit

$$ma = 0$$

Da aus $ma = 0$ auch $-ma = 0$ folgt, kann man stets voraussetzen, die Zahl m in der Gleichung sei positiv.
Wir wählen jetzt unter allen natürlichen Zahlen, die der Bedingung $ma = 0$ genügen, die kleinste und bezeichnen sie mit α. Es gilt

$$a \neq 0, \quad 2a \neq 0, \quad ..., \quad (\alpha - 1)a \neq 0, \quad \alpha a = 0$$

Wir beweisen, dass sämtliche Elemente

$$0 = 0a, a, 2a, ..., (\alpha - 1)a \tag{1}$$

voneinander verschieden sind. Würde nämlich

$$pa = qa \qquad \text{mit} \qquad 0 \leq p < q \leq \alpha - 1$$

gelten, so erhielten wir, wenn wir auf beiden Seiten der letzten Gleichung $-pa$ hinzufügen würden,

$$(q - p)a = 0$$

Dies widerspräche aber der Definition der Zahl α, da nach unseren Bedingungen

$$0 < q - p \leq \alpha - 1$$

gilt. Also sind alle Elemente (1) voneinander verschieden. Wir beweisen, dass die gesamte Gruppe $H(a)$ durch die Elemente (1) erschöpft wird, dass also für beliebiges ganzzahliges m gilt:

$$ma = ra \qquad \text{mit} \qquad 0 \leq r \leq \alpha - 1$$

Dazu teilen wir m durch α und stellen m in folgender Form dar:

$$m = q\alpha + r \tag{2}$$

wobei q der Quotient und r der Rest ist, der der Bedingung

$$0 \leq r < \alpha$$

genügt[20]. Dann gilt

$$ma = (q\alpha + r)a = q\alpha \cdot a + ra$$

und wegen ,

$$q\alpha \cdot a = q(\alpha a) = q \cdot 0 = 0 \qquad \text{auch} \qquad ma = ra$$

Existieren also zwei Zahlen m_1 und m_2, mit $m_1 a = m_2 a$, so gibt es eine natürliche Zahl α derart, dass jede Gruppe $H(a)$ durch die α untereinander verschiedenen Elemente

$$0, a, 2a, ..., (\alpha - 1)a \tag{1}$$

erschöpft wird; es gilt dann $\alpha a = 0$ und allgemeiner folgender Sachverhalt:
Die Folge

$$..., -ma, ..., -a, 0, a, ..., ma, ...$$

ist eine nach rechts und links fortgesetzte unendliche Wiederholung ihres "Abschnittes" (I). In der Tat gilt:

$$\begin{aligned}
(\alpha + 1)a &= \alpha a + a = a; \\
(\alpha + 2)a &= \alpha a + 2a = 2a; \\
&... \\
(2\alpha - 1)a &= \alpha a + (\alpha - 1)a = (\alpha - 1)a; \\
2\alpha a &= 0 \\
(2\alpha + 1)a &= a \qquad \text{usw.}
\end{aligned}$$

und ebenso in der linken Hälfte:

$$\begin{aligned}
-a &= \alpha a - a = (\alpha - 1)a; \\
-2a &= \alpha a - 2a = (\alpha - 2)a; \\
&... \\
-(\alpha - 1)a &= \alpha a - (\alpha - 1)a = a; \\
-\alpha a &= 0 \qquad \text{usw.}
\end{aligned}$$

Um das Element der Gruppe $H(a)$ zu finden, das wir als Summe

$$\underbrace{a + a + ... + a}_{n-\text{mal}} = ma \quad \text{bzw.} \quad \underbrace{(-a) + (-a) + ... + (-a)}_{n-\text{mal}} = -ma$$

erhalten, müssen wir m bzw. $-m$ durch a dividieren. Der nichtnegative Rest r, den man bei dieser Division erhält, genügt der Bedingung $0 \leq r \leq \alpha - 1$ und ergibt:

$$ma = ra$$

Daraus wird auch klar, wie die Elemente der Gruppe $H(a)$ zu addieren sind:

$$pa + qa = (p + q)a = ra$$

[20] Auch für negatives m ist der Rest r bei der Division durch $a > 0$ stets nicht negativ zu nehmen. Ist nämlich m negativ, so wird $-m$ positiv und kann in der Form $-m = q'a + r'$ geschrieben werden, wobei q' und r' nicht negativ sind. Für $r' > 0$ gilt $m = -q'\alpha - r' = -(q' + 1)\alpha + (\alpha - r')$.

Dabei heißt bei der Division der negativen Zahl m durch die positive Zahl an die Zahl $-(q' + l)$ der Quotient und die positive Zahl $r = \alpha - r' < \alpha$ der Rest.

wobei r der Rest der Division von $p+q$ durch a ist.

Wir betrachten jetzt ein regelmäßiges α-Eck. Der Zentriwinkel, zu dem eine Seite unseres Vielecks die Basis bildet, ist

$$\phi = \frac{2\pi}{\alpha}$$

Das Vieleck kommt bei Drehungen um die Winkel 0 (identische Drehung), ϕ, 2ϕ, ..., $(\alpha-1)\phi$ mit sich selbst zur Deckung.
Identifiziert man Drehungen, die sich voneinander um ein ganzes Vielfaches einer vollen unterscheiden, so führen nur Drehungen um Vielfache von ϕ das Vieleck in die gleiche Lage über.
Die Summe der Drehungen um die Winkel $p\phi$ und $q\phi$ ist dabei gleich der Drehung um den Winkel $r\phi$, wobei r der Rest der Division von $p+q$ durch a ist.

Wir sehen: Ordnet man der Drehung des Vielecks um den Winkel $m\phi$ das Element in ma der Gruppe $H(a)$ zu, so erhält man eine isomorphe Abbildung der Gruppe $H(a)$ auf die Gruppe der Drehungen des regelmäßigen α-Ecks.

Gruppen, die den Drehungsgruppen regelmäßiger Vielecke isomorph sind, heißen endliche zyklische Gruppen.

Ist also $m_1 a = m_2 a$ für gewisse m_1 und m_2, so ist die Gruppe $H(a)$ eine endliche zyklische Gruppe.
Die Additionstafeln für die zyklischen Gruppen der Ordnung 3 und 4 wurden in § 1 beschrieben (erstes und drittes Beispiel). Die Additionstafel für eine zyklische Gruppe der Ordnung m hat die Gestalt:

	a_0	a_1	a_2	a_3	...	a_{m-1}
a_0	a_0	a_1	a_2	a_3	...	a_{m-1}
a_1	a_1	a_2	a_3	a_4	...	a_0
a_2	a_2	a_3	a_4	a_5	...	a_1
a_3	a_3	a_4	a_5	a_6	...	a_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	...	$\vdots$
a_{m-3}	a_{m-3}	a_{m-2}	a_{m-1}	a_0	...	a_{m-4}
a_{m-2}	a_{m-2}	a_{m-1}	a_0	a_1	...	a_{m-3}
a_{m-1}	a_{m-1}	a_0	a_1	a_2	...	a_{m-2}

Diese Additionstafel kann man als zweite Definition einer zyklischen Gruppe der Ordnung m auffassen.

Wir haben den Fall untersucht, dass für ein vorgegebenes Element a der Gruppe G zwei verschiedene ganze Zahlen m_1 und m_2 mit der Eigenschaft $m_1 a = m_2 a$ existieren.
Wir betrachten jetzt den Fall, dass keine zwei solche Zahlen vorhanden, also alle Elemente

$$..., -ma, -(m-1)a, ..., -3a, -2a, -a, 0, a, 2a, 3a, ..., ma, ... \tag{2}$$

verschieden sind. Dann besteht zwischen den Elementen (2) und den ganzen Zahlen eine eineindeutige Zuordnung: Dem Element ma entspricht die ganze Zahl m und umgekehrt. Bei

$$m_1 a + m_2 a = m_3 a \qquad \text{gilt auch} \qquad m_1 + m_2 = m_3$$

Diese eineindeutige Zuordnung ist also ein Isomorphismus zwischen der Untergruppe $H(a)$ und der Gruppe aller ganzen Zahlen.

Gruppen, die zur Gruppe der ganzen Zahlen isomorph sind, nennt man unendliche zyklische Gruppen.

Da ferner zwei Gruppen A und B, die zu ein und derselben Gruppe C isomorph sind, offensichtlich untereinander isomorph sind, so sind alle unendlichen zyklischen Gruppen untereinander isomorph. Ebenso sind auch alle endlichen zyklischen Gruppen ein und derselben Ordnung m untereinander isomorph. Wir fassen die Überlegungen dieses Paragraphen zusammen.

Satz. Jedes von Null verschiedene Element a einer Gruppe G erzeugt eine endliche oder unendliche zyklische Gruppe $H(a)$. Die Ordnung der Gruppe $H(a)$ heißt auch Ordnung des Elementes a.

Schließlich können wir endliche oder unendliche zyklische Gruppen auch so definieren: Eine Gruppe heißt zyklisch, wenn sie von einem ihrer Elemente erzeugt wird.

4.3 Erzeugendensysteme

Wir kehren jetzt zur zyklischen Gruppe $H(a)$ zurück, die von dem Element a der Gruppe G erzeugt wird. Das Element a erzeugt die Gruppe $H(a)$ in dem Sinne, dass jedes ihrer Elemente Summe von Summanden ist, deren jeder gleich a oder $-a$ ist.
"Das Element a erzeugt die Gruppe $H(a)$"besagt das gleiche wie "Das Element a ist erzeugendes Element der Gruppe $H(a)$".

Jedoch ist nicht jede Gruppe zyklisch, nicht jede Gruppe wird von einem einzigen Element erzeugt:
Nichtzyklische Gruppen werden nicht von einem, sondern von mehreren, manchmal von unendlich vielen Elementen erzeugt. Der Begriff eines erzeugenden Elementes führt auf den Begriff des Erzeugendensystems[21].

Definition. Eine Menge E von Elementen einer Gruppe G heißt Erzeugendensystem dieser Gruppe, wenn jedes Element der Gruppe die Summe endlich vieler Summanden ist, deren jeder entweder selbst Element von E oder zu einem Element der Menge E entgegengesetzt ist.

Beispiel. Wir betrachten die Ebene mit einem in ihr gewählten kartesischen Koordinatensystem. Wir bezeichnen mit G die Menge der Punkte $P = (x, y)$, deren beide Koordinaten x und y ganze Zahlen sind. Wir stellen folgende Additionsregel für die Punkte auf: Summe der beiden Punkte $P_1 = (x_1, y_1)$ und $P_2 = (x_2, y_2)$ ist der Punkt $P_3 = (x_3, y_3)$ mit den Koordinaten $x_3 = x_1 + x_2$ und $y_3 = y_1 + y_2$.

Man sieht sofort, dass bezüglich der so definierten Addition die Menge G eine abelsche Gruppe bildet (siehe Kap. I, § 2, IV) und dass die Punkte $(0; 1)$ und $(1; 0)$ ein Erzeugendensystem dieser Gruppe sind.

Bemerkung. Ist der Leser mit dem Begriff der komplexen Zahl vertraut, so kann er leicht zeigen, dass die eben konstruierte Gruppe isomorph zur Gruppe der ganzen komplexen Zahlen ist (mit der Addition als Gruppenoperation). Dabei heißt eine komplexe Zahl $x + iy$ ganz, wenn x und y ganze Zahlen sind.

Aufgabe. Man beweise, dass jedes System von natürlichen Zahlen, deren größter gemeinsamer Teiler gleich Eins ist, ein Erzeugendensystem der Gruppe der ganzen Zahlen ist.

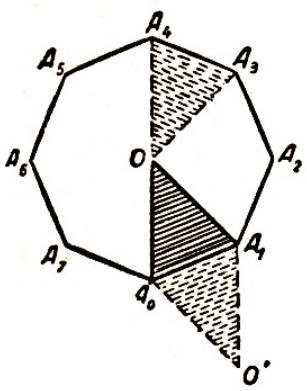
[21] Offensichtlich ist die Gesamtheit aller Elemente jeder Gruppe ein (triviales) Erzeugendensystem dieser Gruppe. Also besitzt jede Gruppe ein Erzeugendensystem.

5 Einfache Bewegungsgruppen

5.1 Beispiele und Definition von Kongruenzgruppen geometrischer Figuren

1. Kongruenzen regelmäßiger Vielecke in ihren Ebenen

Eine umfangreiche und sehr wichtige Klasse von Gruppen, die sowohl endliche als auch unendliche Gruppen enthält, bilden die "Kongruenzgruppen" geometrischer Figuren.
Unter einer Kongruenz einer gegebenen geometrischen Figur F versteht man eine Bewegung von F (im Raume oder in der Ebene), die F in sich überführt, also die Figur F mit sich selbst zur Deckung bringt.



Wir haben uns bereits mit einfachen Kongruenzgruppen vertraut gemacht, nämlich mit den Drehungsgruppen regelmäßiger Vielecke.
Es sei in der Ebene das regelmäßige Vieleck $A_0A_1A_2...A_n$ (Abb. 2), zum Beispiel das regelmäßige Achteck $A_0A_1A_2A_3A_4A_5A_6A_7A_8$ vorgegeben (die Eckpunkte seien alle in einer Richtung durchnummeriert, beispielsweise entgegen dem Uhrzeigersinn).
Gesucht sind diejenigen Bewegungen des Vielecks in seiner Ebene, die es mit sich selbst zur Deckung bringen.

Bei diesen Bewegungen muss jeder Eckpunkt des Vielecks in einen Eckpunkt, jede Seite in eine Seite und der Mittelpunkt O des Vielecks in sich selbst übergehen. Bei einer bestimmten Bewegung möge der Eckpunkt A_0 beispielsweise in A_k übergeben (in der Abbildung ist $k = 4$).

Dann muss die Seite A_0A_1 entweder in die Seite A_kA_{k+1} oder in die Seite A_kA_{k-1} übergehen. Ginge die Seite A_0A_1 in die Seite A_kA_{k-1} über, so auch das Dreieck A_0A_1O in das Dreieck $A_kA_{k-1}O$.
Dieses Dreieck könnte man durch Bewegung in seiner Ebene in die Lage A_0A_1O' überführen, die durch Spiegelung des Dreiecks A_0A_1O an seiner Seite A_0A_1 herzustellen ist. Damit hätte man gezeigt, dass man das Dreieck A_0A_1O durch eine Bewegung innerhalb seiner Ebene in sein Spiegelbild überführen könnte, was unmöglich ist.[22]

Also muss die Seite A_0A_1 in die Seite A_kA_{k+1} übergehen. Genauso überzeugt man sich davon, dass die Seite A_1A_2 in $A_{k+1}A_{k+2}$ übergeht, die Seite A_2A_3 in $A_{k+2}A_{k+3}$, usw.
Mit anderen Worten, die Bewegung ist eine Drehung des Vielecks in seiner Ebene um den Winkel $k\frac{2\pi}{n}$. Also gilt:

Jede Kongruenz eines regelmäßigen n-Ecks in seiner Ebene ist eine Drehung des Vielecks um den Winkel $k\frac{2\pi}{n}$, wobei k eine ganze Zahl ist.
Es gibt daher n derartige Kongruenzen. Diese Drehungen bilden, wie wir wissen, eine Gruppe.

2. Kongruenzen eines regelmäßigen Vielecks im dreidimensionalen Raum

Die vorigen Überlegungen haben wir unter der wesentlichen Voraussetzung durchgeführt, dass lediglich Kongruenzen eines Vielecks in seiner Ebene betrachtet wurden.

[22] Der strenge Beweis dieser Unmöglichkeit, die eine der grundlegenden Tatsachen der Geometrie der Ebene ist, würde den Rahmen dieses Buches überschreiten.

Untersuchen wir Kongruenzen eines n-Ecks im Raume, so kommen zu den bisherigen Drehungen noch "Umklappungen" des Vielecks hinzu, also Drehungen um einen Winkel von 180° um die Symmetrieachsen des Vielecks.

Ein regelmäßiges n-Eck besitzt n Symmetrieachsen: Bei geradem n sind die $\frac{n}{2}$ Geraden, die die Paare gegenüberliegender Eckpunkte, sowie die $\frac{n}{2}$ Geraden, die die Mittelpunkte gegenüberliegender Seiten verbinden, die Symmetrieachsen.
Bei ungeradem n sind die Symmetrieachsen durch die Geraden gegeben, die einen Eckpunkt mit dem Mittelpunkt der gegenüberliegenden Seite des Vielecks verbinden. Der Beweis dafür, dass diese n Drehungen und n Umklappungen eines regelmäßigen n-Ecks alle Kongruenzen des n-Ecks, d.h. alle Bewegungen im Raume, die das Vieleck in sich überführen, erschöpfen, ist im wesentlichen in den Überlegungen des § 3 dieses Kapitels enthalten.

Es mag dem Leser überlassen bleiben, zum besseren Verständnis dieses Paragraphen später noch einmal auf ihn zurückzukommen sowie überhaupt über alle mit den Kongruenzen eines regelmäßigen Vielecks zusammenhängenden Fragen dann noch einmal nachzudenken.

3. Allgemeine Definition der Kongruenzgruppe einer gegebenen Figur im Raume oder in der Ebene

Es sei im Raume oder in der Ebene eine Figur F vorgegeben. Wir betrachten sämtliche Kongruenzen dieser Figur, d.h. sämtliche Bewegungen im Raume oder in der Ebene, die diese Figur mit sich selbst zur Deckung bringen.

Als Summe $g_1 + g_2$ zweier Kongruenzen g_1 und g_2 definieren wir die Bewegung, die durch Hintereinanderausführung der Drehung g_1 und der Drehung g_2, in dieser Reihenfolge entsteht. Offensichtlich ist auch die Bewegung $g_1 + g_2$ unter der Voraussetzung eine Kongruenz der Figur F, dass die Bewegungen g_1 und g_2 es sind.

Die Gesamtheit aller Kongruenzen der Figur F bildet bei der eben definierten Operation der Addition eine Gruppe. Die Addition von Bewegungen erfüllt nämlich das assoziative Gesetz. Weiter gibt es in der Gesamtheit der Kongruenzen eine Null oder "identische" Kongruenz, nämlich die "Ruhe", also die Bewegung, die jeden Punkt der Figur fest lässt.
Schließlich existiert zu jeder Kongruenz g die ihr entgegengesetzte $-g$ (sie bewegt jeden Punkt aus der Lage, in der er sich nach der Drehung g befand, in die Ausgangslage zurück).

5.2 Die Bewegungsgruppe einer Geraden, eines Kreises, einer Ebene

Die Bewegungsgruppen regelmäßiger Vielecke sind endlich. In diesem Kapitel werden wir noch andere endliche Kongruenzgruppen kennenlernen, nämlich die Kongruenzgruppen gewisser Vielflache. Zunächst aber geben wir einige Beispiele unendlicher Kongruenzgruppen.

Das erste Beispiel bildet die Gruppe aller Kongruenzen einer Geraden in irgendeiner durch sie hindurchgehenden Ebene. Diese Gruppe besteht aus Verschiebungen der Geraden in sich (Kongruenzen erster Art) und aus Drehungen der Geraden in der gewählten Ebene um Winkel von 180° um einen beliebigen ihrer Punkte (Kongruenzen zweiter Art).

Die Gruppe der Kongruenzen einer Geraden ist nichtkommutativ.
Um sich davon zu überzeugen, genügt es, zwei Kongruenzen zu addieren, von denen die eine erster und die andere zweiter Art ist:

Das Resultat dieser Addition ändert sich bei Änderung der Reihenfolge der Summanden[23]. Offensichtlich kann man alle Kongruenzen zweiter Art erhalten, indem man zu jeder möglichen Verschiebung der Geraden eine beliebige Drehung um 180°, also eine Drehung um 180° um einen bestimmten, aber willkürlich gewählten Punkt dieser Geraden, addiert.

Die Verschiebungen der Geraden in sich bilden eine Untergruppe in der Gruppe ihrer sämtlichen Kongruenzen. Diese Verschiebungen sind die einzigen Bewegungen der Geraden in sich. Jeder Verschiebung der Geraden in sich entspricht in eindeutiger Weise eine reelle Zahl, die Länge und Richtung der Verschiebung der Geraden in sich kennzeichnet. Daraus schließt man leicht, dass die Gruppe aller Verschiebungen einer Geraden in sich der Gruppe der reellen Zahlen (mit der gewöhnlichen arithmetischen Addition als Gruppenoperation) isomorph ist.

Als zweites Beispiel betrachten wir die Gruppe aller Kongruenzen eines Kreises in seiner Ebene. Diese Gruppe besteht aus allen möglichen Drehungen des Kreises in seiner Ebene um seinen Mittelpunkt, wobei wie immer Drehungen um Winkel, die Vielfache von 2π sind, als identisch angesehen werden[24].

Jedem Element unserer Gruppe entspricht auf diese Weise ein bestimmter Winkel ϕ. Misst man diesen Winkel im Bogenmaß, so erhält man eine reelle Zahl x. Da aber Winkel, die sich um ganzzahlige Vielfache von 2π unterscheiden, ein und dieselbe Drehung des Kreises definieren, so entspricht jedem Element der Drehungsgruppe des Kreises nicht nur diese eine Zahl x, sondern auch alle Zahlen der Form $x + 2\pi k$, wobei k eine beliebige ganze Zahl ist.

Andererseits entspricht jeder reellen Zahl eine eindeutig bestimmte Drehung des Kreises, nämlich die Drehung um den Winkel, dessen Bogenlänge gleich x ist.
Daher kann man zwischen den Drehungen eines Kreises und den reellen Zahlen folgende Zuordnung treffen: Jeder reellen Zahl x entspricht eine einzige wohlbestimmte Drehung, nämlich die Drehung um den Winkel x. Umgekehrt ist aber jede Drehung nicht nur einer, sondern unendlich vielen reellen Zahlen zugeordnet, die sich alle um ganzzahlige Vielfache von 2π unterscheiden.

Die Gruppe der Drehungen eines Kreises bezeichnet man mit dem griechischen Buchstaben κ ("Kappa") vom Worte $\kappa\upsilon\kappa\lambda o\varsigma$ (Cyclos), das "Kreis" bedeutet.

Als drittes Beispiel wählen wir die Gruppe aller Bewegungen einer Ebene in sich. Und zwar betrachten wir dazu die Ebene nicht in einem, sondern in zwei Exemplaren, deren erstes unbeweglich ist, während man das andere bewegen, genauer, auf dem ersten gleiten lassen kann.
Die erste, unbewegliche Ebene können wir uns als einen nach allen Seiten unendlich ausgedehnten Tisch vorstellen, die zweite, bewegliche als Scheibe, die ebenfalls nach allen Seiten unendlich ausgedehnt ist und auf diesem Tische liegt. Wir meinen also die Gesamtheit der möglichen Bewegungen der Scheibe, bei denen sie stets auf dem Tische liegenbleibt[25].

In der Gruppe aller Bewegungen einer Ebene in sich gibt es unendlich viele Untergruppen. Unter ihnen nennen wir vor allem die unendlich vielen Drehungsgruppen:
Die Gesamtheit aller Drehungen der Ebene um einen beliebigen, aber festen ihrer Punkte bildet eine Gruppe,und jede dieser Gruppen ist, wie man leicht sieht, der Gruppe κ isomorph.

[23] Es bleibe dem Leser überlassen, sich davon zu überzeugen, indem er zwei beliebige, aber bestimmte Kongruenzen erster und zweiter Art nimmt und ihre Summe für die eine und die andere Reihenfolge der Summanden bildet

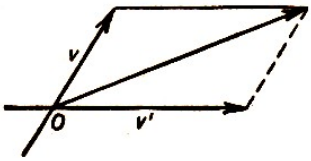
[24] Falls dem Leser der Sinn der nun folgenden Überlegungen nicht verständlich wird, kann er gleich zu dem folgenden Beispiel übergehen und erst nach Lektüre des Kap. VIII darauf zurückkommen.

[25] Es ist also insbesondere eine Drehung der Scheibe um eine auf dem Tisch liegende Achse nicht gestattet.

Folglich sind insbesondere alle diese Gruppen kommutativ. Neben den Drehungsgruppen gibt es in der Gruppe sämtlicher Bewegungen der Ebene in sich die Untergruppen der Parallelverschiebung längs verschiedener Geraden:
Bei vorgegebener Geraden g kann man die Ebene längs dieser Geraden verschieben, wobei die Gerade g und alle zu ihr parallelen Geraden in sich übergehen. Für diese Verschiebungen längs der Geraden g sind zwei entgegengesetzte Richtungen möglich.
Ihre Gesamtheit bildet eine Gruppe, die Gruppe der Verschiebungen oder Parallelverschiebungen der Ebene längs einer vorgegebenen Geraden; sie ist offensichtlich eine Untergruppe der Gruppe aller Bewegungen der Ebene in sich.

Jede Verschiebung längs einer Geraden g ist charakterisiert durch Größe und Richtung einer bestimmten Strecke v, die auf der Geraden g liegt und von einem ein für allemal fest gewählten Punkt O dieser Geraden aus abgetragen ist (Abb. 3).

Diese Strecke v durchläuft der Punkt O bei unserer Verschiebung. Daraus folgt, dass die Gruppe alter Verschiebungen der Ebene längs einer vorgegebenen Geraden g isomorph zur Gruppe aller reellen Zahlen ist (mit der üblichen Addition als Gruppenoperation).



Wir betrachten zwei Bewegungen v und v' der Ebene längs zweier nichtparalleler Geraden g und g' (Abb. 4).

Die Hintereinanderausführung dieser beiden Verschiebungen ergibt dasselbe Resultat wie die Verschiebung der Ebene längs der Diagonalen des aus den Verschiebungen gebildeten Parallelogramms; Länge und Richtung dieser Diagonalen ist dabei durch Länge und Richtung der Strecken v und v' festgelegt ("Parallelogrammregel" oder Addition von Vektoren).[26]

Also ist die Summe zweier beliebiger Parallelverschiebungen der Ebene wieder eine Parallelverschiebung der Ebene. Sie hängt nicht von der Reihenfolge der Summanden ab. Daraus folgt:
Die Gesamtheit aller Parallelverschiebungen der Ebene längs aller möglichen Geraden ist eine kommutative Untergruppe der Gruppe der Bewegungen der Ebene in sich.

Übungen.

1. Man beweise, dass die Gruppe aller Parallelverschiebungen der Ebene zur Gruppe der komplexen Zahlen mit der üblichen Addition als Gruppenoperation isomorph ist.

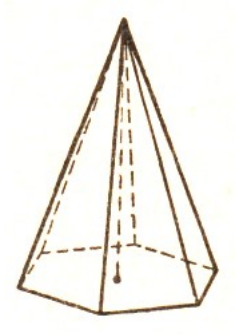
2. Man beweise, dass die Gesamtheit aller Drehungen der Ebene in sich (um alle möglichen Punkte der Ebene) keine Gruppe bildet.

Sämtliche eben betrachteten Gruppen, nämlich die Bewegungsgruppe einer Geraden, eines Kreises und einer Ebene, haben folgendes gemeinsam:
Alle diese Gruppen bestehen aus Bewegungen der entsprechenden Gebilde in sich. Mit anderen Worten, während jeder Bewegung bleiben die betreffenden Gebilde, der Kreis, die Gerade, die Ebene, vollkommen sie selbst. Diese Eigenschaft besteht nicht mehr bei den Kongruenzen regelmäßiger Vielecke.
Bei ihnen stimmt zwar die endgültige Lage der bewegten Figur mit der ursprünglichen überein,

[26] Zwei Verschiebungen längs zweier paralleler Geraden sind offensichtlich auch Verschiebungen längs einer Geraden (nämlich längs einer beliebigen der beiden vorgegebenen Geraden oder ebensogut längs einer beliebigen dritten zu ihnen parallelen).

aber die Zwischenlagen, die die Figur im Bewegungsprozess durchläuft, unterscheiden sich von ihrer ursprünglichen und ihrer endgültigen. Gleiches gilt auch bei den Bewegungen von Vielflachen, zu denen wir sogleich übergehen.

5.3 Die Drehungsgruppen einer regelmäßigen Pyramide und einer Doppelpyramide

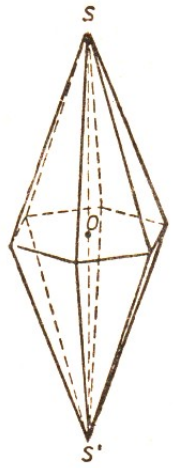


1. Die Pyramide

Die Gruppe der Drehungen einer regelmäßigen (Abb. 5) n-eckigen Pyramide um ihre Achse ist offensichtlich isomorph der Drehungsgruppe eines regelmäßigen in seiner Grundfläche liegenden n-Ecks. Diese Gruppe ist daher zyklisch von der Ordnung n.
Man überzeugt sich leicht davon, dass die Drehungen der Pyramide um ihre Achse (um die Winkel 0, $\frac{2\pi}{n}$, ..., $(n-1)\frac{2\pi}{n}$) alle Bewegungen erschöpfen, die die Pyramide mit sich selbst zur Deckung bringen.

2. Die Doppelpyramide (das Dieder)

Wir definieren jetzt die Kongruenzgruppe eines Körpers, der unter dem Namen "regelmäßige n-eckige Doppelpyramide"oder n-eckiges Dieder bekannt ist (Abb. 6).



Dieser Körper besteht aus einer regelmäßigen n-eckigen Pyramide und ihrem Spiegelbild an der Grundfläche.
Wir wollen beweisen, dass die Kongruenzgruppe des Dieders aus folgenden Elementen besteht:

1. den Drehungen um die Pyramidenachse (um die Winkel 0, $\frac{2\pi}{n}$, ..., $(n-1)\frac{2\pi}{n}$)
2. den sogenannten Umklappungen, also den Drehungen um den Winkel π um jede der Symmetrieachsen der "Diedergrundfläche", d.h. des regelmäßigen Vielecks, das beide Pyramiden zur gemeinsamen Grundfläche haben, über der das Dieder errichtet ist.
Wie wir gesehen haben, gibt es n solcher Symmetrieachsen, so dass es also n Bewegungen zweiter Art gibt.

Die Anzahl aller dieser Bewegungen ist daher gleich $2n$. Um uns davon zu überzeugen, dass es, abgesehen von $n = 4$, keine anderen Bewegungen gibt, die das n-eckige Dieder in sich selbst überführen, stellen wir zunächst fest, dass bei $n \neq 4$ jede Kongruenz des Dieders entweder die Punkte S und S' festlassen (Kongruenzen erster Art) oder ihre Plätze vertauschen muss (Kongruenzen zweiter Art).

Ferner muss bei diesen Bewegungen die Grundfläche des Dieders in sich selbst übergehen. Schließlich bemerken wir, dass die Addition (also die Hintereinanderausführung) zweier Kongruenzen erster Art eine Kongruenz erster Art, die Addition einer Kongruenz erster mit einer Kongruenz zweiter Art eine Kongruenz zweiter Art und die Addition zweier Kongruenzen zweiter Art eine Kongruenz erster Art ergibt.

Dabei hängt die Summe zweier Kongruenzen, von denen eine erster und die andere zweiter Art ist, von der Reihenfolge der Summanden ab: Ist a eine Kongruenz erster und b eine Kongruenz zweiter Art, so ist $a + b = b - a$.

Wir betrachten zunächst Kongruenzen erster Art. Bei diesen Kongruenzen wird die Grundfläche nicht geklappt, verbleibt also in ihrer Ebene. Sie erfährt daher lediglich eine Drehung um einen der Winkel

$$0, \frac{2\pi}{n}, ..., (n-1)\frac{2\pi}{n}$$

Alle Bewegungen des Dieders sind daher Drehungen um die Diederachse um einen dieser Winkel.
Also gibt es genau n Kongruenzen erster Art (einschließlich der identischen Kongruenz, d.h. der Ruhe). Diese Kongruenzen sind nichts anderes als die Drehungen des Dieders um seine Achse um die Winkel 0, $\frac{2\pi}{n}$, ..., $(n-1)\frac{2\pi}{n}$.

Es sei eine beliebige, aber feste Kongruenz zweiter Art vorgegeben, also eine solche Kongruenz des Dieders, bei der die Eckpunkte S und S' ihre Plätze wechseln.
Führen wir nach dieser Kongruenz zweiter Art eine beliebige, aber feste Umklappung des Dieders aus, also eine Bewegung, die in einer Drehung des Dieders um den Winkel π um irgendeine beliebig gewählte Symmetrieachse besteht, so erhalten wir eine Kongruenz erster Art[27], also eine Drehung des Dieders um seine Achse.

Somit führt jede Kongruenz zweiter Art durch Zusammensetzen mit einer festen Umklappung zu einer gewissen Kongruenz erster Art. Daraus folgt:
Jede Kongruenz zweiter Art entsteht aus einer passenden Kongruenz erster Art durch voraufgehende oder nachfolgende Zusammensetzung mit einer willkürlich, aber fest gewählten Umklappung. Daraus folgt ferner, dass die Anzahl der Kongruenzen erster Art gleich der Anzahl der Kongruenzen zweiter Art, also ebenfalls gleich n ist.

Andererseits ist klar, dass alle Umklappungen Kongruenzen zweiter Art sind. Da es genau n solche Umklappungen gibt, erschöpfen sie offensichtlich auch die Gesamtheit der Kongruenzen zweiter Art.
Somit haben wir für $n \neq 4$ folgendes bewiesen: Die Kongruenzgruppe des n-eckigen Dieders ist eine nichtkommutative Gruppe der Ordnung $2n$, die aus n Drehungen um die Diederachse SS' und aus n Umklappungen, also Drehungen vom Winkeln π um die n Symmetrieachsen der Grundfläche des Dieders besteht. Man erhält alle n Umklappungen durch Addition einer einzigen zu den n Drehungen des Dieders um seine Achse SS'.

Da man ferner alle Drehungen des Dieders um seine Achse durch wiederholte Addition einer einzigen Drehung zu sich selbst erhält, und zwar der Drehung um den Winkel $\frac{2\pi}{n}$, so besitzt die Gruppe aller Kongruenzen ein Erzeugendensystem, das aus zwei Elementen besteht: aus der Drehung um den Winkel $\frac{2\pi}{n}$ und einer beliebigen Umklappung.

Der Fall $n = 4$ bildet dadurch eine Ausnahme, dass das viereckige Dieder im Spezialfall ein Oktaeder werden kann und dieses, wie wir unten sehen werden, nicht 8, sondern 24 Kongruenzen besitzt.
Dies erklärt sich daraus, dass man bei den regelmäßigen Oktaedern die Spitze S nicht nur mit der Spitze S', sondern auch mit jeder der Ecken der Grundfläche vertauschen kann. Eine der dafür notwendigen Bedingungen, dass nämlich zu jedem Eckpunkt die gleiche Anzahl Flächen und Kanten gehört, ist offensichtlich schon im Falle eines beliebigen viereckigen Dieders erfüllt. Bei einem regelmäßigen Oktaeder sind überdies für je zwei beliebige Ecken sowohl die entsprechenden Winkel auf den Seitenflächen als auch die Winkel zwischen den Seitenflächen einander

[27] Zwar ist jede einzelne dieser Drehungen eine Kongruenz zweiter Art, aber die Summe zweier Kongruenzen zweiter Art ist eine Kongruenz erster Art.

gleich und sogar die anstoßenden Flächen und Kanten kongruent.

3. Ausartungen: Die Drehungsgruppen eines Sektors und eines Rhombus

Die kleinste Eckenanzahl, die ein Vieleck haben kann, ist drei. Jedoch kann man bekanntlich eine Strecke als "ausgeartetes" Vieleck oder auch als "Vieleck mit zwei Ecken" auffassen.
Das wird auch insbesondere dadurch gerechtfertigt, dass die Kongruenzgruppe einer Strecke in irgendeiner sie enthaltenden Ebene eine zyklische Gruppe der Ordnung 2 ist. Sie besteht offensichtlich aus der identischen Kongruenz und aus der Drehung der Strecke um ihren Mittelpunkt um 180°.

Ähnlich kann ein gleichschenkliges Dreieck als Ausartungsfall einer regelmäßigen Pyramide aufgefasst werden: Die Kongruenzgruppe eines gleichschenkligen Dreiecks im Raume ist eine Gruppe der Ordnung 2.

Ferner ist ein ausgeartetes Dieder oder eine ausgeartete Doppelpyramide offensichtlich ein Rhombus. Die Gruppe der Kongruenzen oder Drehungen eines Rhombus im Raume besteht aus vier Elementen: Aus der identischen Abbildung a_0, aus den Klappungen a_1 und a_2 um jede der Diagonalen und aus der Drehung a_3 von 180° in seiner Ebene um den Rhombusmittelpunkt; diese ist die Summe der zwei vorgenannten Klappungen[28]. Die Additionstabelle unserer, Gruppe hat folgende Gestalt:

	a_0	a_1	a_2	a_3
a_0	a_0	a_1	a_2	a_3
a_1	a_1	a_0	a_3	a_2
a_2	a_2	a_3	a_0	a_1
a_3	a_3	a_2	a_1	a_0

sie fällt also mit der Additionstafel der Kleinschen Vierergruppe zusammen, die wir in Kap. I, § 1, Artikel 3 als zweites Beispiel eingeführt haben. Davon überzeugt man sich leicht direkt oder indem man einfach an Stelle der Drehungsgruppe des Rhombus die zu ihr isomorphe Gruppe der Permutation seiner vier Ecken A, B, C, D betrachtet:
Offensichtlich entsprechen den Drehungen a_0, a_1, a_2, a_3 folgende Permutationen der Eckpunkte[29]:

$$\begin{pmatrix} A & B & C & D \\ A & B & C & D \end{pmatrix}, \quad \begin{pmatrix} A & B & C & D \\ B & A & C & D \end{pmatrix}, \quad \begin{pmatrix} A & B & C & D \\ A & B & D & C \end{pmatrix}, \quad \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}$$

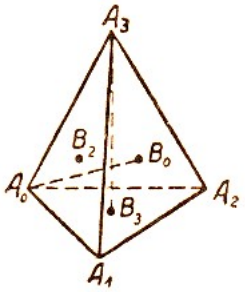
5.4 Die Drehungsgruppe des Tetraeders

Zur Bestimmung aller Kongruenzen des Tetraeders[30] $A_0A_1A_2A3$ (Abb. 7) betrachten wir zunächst diejenigen von ihnen, die eine bestimmte Ecke, beispielsweise A_0 festlassen.
Diese Kongruenzen führen denn das Dreieck $A_1A_2A_3$ in sich über, indem sie es um seinen Mittelpunkt B_0 um einen der Winkel 0, $\frac{2\pi}{3}$, $\frac{4\pi}{3}$ drehen. Daraus folgt, dass es genau drei Kongruenzen des Tetraeders $A_0A_1A_2A3$ gibt, die die Ecke A_0 festlassen:

[28] Wir betrachten eine der Diagonalen des Rhombus als "Grundlinie", die andere als Achse des entsprechenden ausgearteten Dieders und erhalten dann diese vier Bewegungen aus der Drehung um die "Achse" vom Winkel π und der Umlegung um die Grundlinie.

[29] Wir bezeichnen mit a_1 die Klappung um die Diagonale CD, mit a_2 die um die Diagonale AB.

[30] Unter einem Tetraeder verstehen wir hier und im folgenden stets ein regelmäßiges Tetraeder.



Die identische Kongruenz a_0, welche sämtliche Elemente des Tetraeders festlässt, und die zwei Drehungen a_1 und a_2 um die Winkel $\frac{2\pi}{3}$ bzw. $\frac{4\pi}{3}$ um die Achse A_0B_0.
Wir bezeichnen jetzt mit x_i irgendeine bestimmte Kongruenz des Tetraeders, die die Ecke A_0 in die Ecke A_1 überführt $(i = l, 2, 3)$. Mit x_0, bezeichnen wir wieder die identische Kongruenz.

Wir beweisen, dass jede Kongruenz b des Tetraeders[31] in der Form

$$b = a_i + x_k \tag{1}$$

geschrieben werden kann, wobei $i = 0, 1, 2$ und $k = 0, 1, 2, 3$ eindeutig bestimmt sind.
Die letzte Behauptung bedeutet folgendes: Ist $b = a_i + x_k$, $b' = a_{i'} + x_{k'}$ und gilt wenigstens eine der Ungleichungen $i \neq i'$, $k \neq k'$, so ist sicher $b \neq b'$.

Es sei also irgendeine Kongruenz b vorgegeben. Sie führt die Ecke A_0 in eine gewisse wohlbestimmte Ecke A_k über, wobei $k = 0, 1, 2, 3$ ist. Dann lässt aber die Kongruenz $b - x_k$ die Ecke A_0 fest, ist also offensichtlich ein eindeutig bestimmtes a_i, so dass $b - x_k = a_i$ und $b = a_i + x_k$ ist; hierbei sind i und k eindeutig bestimmt.
Da auch umgekehrt jedem Paar (i, k) nach (1) eine bestimmte Kongruenz des Tetraeders entspricht, gibt es eine eineindeutige Zuordnung zwischen sämtlichen Kongruenzen des Tetraeders und allen Paaren (i, k), wobei i die Werte 0, 1, 2 und k die Werte 0, 1, 2, 3 annimmt.

Daraus folgt, dass es genau 12 Kongruenzen des Tetraeders gibt. Jede Kongruenz des Tetraeders bedeutet nun eine bestimmte Permutation der Eckpunkte, also eine bestimmte Permutation der zugehörigen Nummern 0, 1, 2, 3.
Bei vier Elementen gibt es nun aber 24 Permutationen, von ihnen lassen sich jedoch, wie wir soeben gesehen haben, nur 12 als Bewegungen des Tetraeders im Raum verwirklichen. Wir wollen untersuchen, welche dieser Bewegungen welchen Permutationen entsprechen.

Wir bezeichnen zur Abkürzung als Flächenmittellinie des Tetraeders jede Gerade, die von einer Ecke A_i des Tetraeders zum Mittelpunkt B_i der dem Eckpunkt gegenüberliegenden Fläche führt. Kantenmittellinie nennen wir jede Gerade, die durch die Mitten zweier beliebiger einander gegenüberliegender Kanten des Tetraeders geht.

Jeder Flächenmittellinie entsprechen zwei nicht identische Kongruenzen des Tetraeders, und zwar Drehungen um sie vom Winkel $\frac{2\pi}{3}$ bzw. $\frac{4\pi}{3}$. Insgesamt erhalten wir daher acht Drehungen, die man als Permutationen der Nummern der Ecken folgendermaßen darstellen kann:

$$\begin{aligned}
a_1 &= \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 2 & 3 & 1 \end{pmatrix}, \quad & a_2 &= \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 3 & 1 & 2 \end{pmatrix}, \quad & a_3 &= \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 1 & 3 & 0 \end{pmatrix}, \\
a_4 &= \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 1 & 0 & 2 \end{pmatrix}, \quad & a_5 &= \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 3 & 2 & 0 \end{pmatrix}, \quad & a_6 &= \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 0 & 2 & 1 \end{pmatrix}, \\
a_7 &= \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 0 & 3 \end{pmatrix}, \quad & a_8 &= \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \end{pmatrix}
\end{aligned} \tag{2}$$

[31] Die Ecke A_0 lässt sich in A_1 und A_3 beispielsweise durch Drehungen um die Achse A_2B_2 (die die Ecke A_2 mit dem Mittelpunkt der gegenüberliegenden Fläche verbindet) überführen. A_0 geht in A_2 beispielsweise durch eine Drehung um die Achse A_3B_3 über.

Um jede Kantenmittellinie gibt es eine nicht identische Drehung vom Winkeln, das ergibt drei weitere Drehungen, da es drei Kantenmittellinien gibt; als Permutationen kann man sie folgendermaßen schreiben:

$$a_9 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \end{pmatrix}, \qquad a_{10} = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \end{pmatrix}, \qquad a_{11} = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \end{pmatrix} \tag{3}$$

Diese elf Drehungen ergeben zusammen mit der identischen Kongruenz ("identischen Drehung") a_0 genau die 12 Kongruenzen des Tetraeders. Jede von ihnen ist eine Drehung um eine der sieben Symmetrieachsen[32] des Tetraeders. Daher heißt die Gruppe dieser Kongruenzen auch Drehungsgruppe des Tetraeders.

Man prüft leicht nach, dass alle Permutationen (2) und (3) gerade sind. Da es aber insgesamt 12 gerade Permutationen von vier Elementen, in diesem Falle den Ecken des Tetraeders, gibt, ist dies offensichtlich eine eineindeutige und sogar isomorphe Zuordnung zwischen der Drehungsgruppe des Tetraeders und der alternierenden Permutationsgruppe von vier Elementen.

Wir wollen jetzt untersuchen, welche Untergruppen die Drehungsgruppe des Tetraeders besitzt.

In ihr gibt es, wie in jeder Gruppe, die zwei uneigentlichen Untergruppen: Erstens die gesamte betrachtete Gruppe und zweitens die Untergruppe, die nur aus dem neutralen Element besteht. Uns interessieren die übrigen, die eigentlichen Untergruppen der Drehungsgruppe des Tetraeders. Davon gibt es genau acht.

Zunächst bemerken wir, dass die Summe der Drehungen um den Winkel π um zwei verschiedene Kantenmittellinien eine Drehung ebenfalls um π um die dritte Kantenmittellinie ergibt; dies kann man sich geometrisch, aber auch durch Addition zweier beliebiger der Permutationen (3) klarmachen.
Daraus folgt, dass die Drehungen vom Winkeln um jede der drei Kantenmittellinien zusammen mit der identischen Drehung eine Gruppe der Ordnung vier bilden. Sie ist zur Kleinschen Vierergruppe, also auch zur Gruppe aller Drehungen des Rhombus, isomorph. Diese Gruppe bezeichnen wir mit H.
Unter allen Untergruppen der Drehungsgruppe des Tetraeders hat sie die höchste Ordnung.

In ihr sind drei Untergruppen zweiter Ordnung enthalten, deren jede aus den Drehungen vom Winkel 0 bzw. π um jeweils eine der gegebenen Kantenmittellinien besteht. Diese Untergruppen bezeichnen wir mit H_{01}, H_{02}, H_{03}. Außer den genannten gibt es noch vier Untergruppen der Ordnung drei, nämlich die Gruppen

$$H_i \qquad (i = 0, 1, 2, 3)$$

von denen jede aus drei Drehungen vom Winkel 0 bzw. $\frac{2\pi}{3}$ bzw. $\frac{4\pi}{3}$ um die entsprechenden Flächenmittellinien besteht.

Um zu beweisen, dass es in der Drehungsgruppe des Tetraeders keine anderen Untergruppen

[32] Diese sieben Symmetrieachsen sind die vier Flächen- und drei Kantenmittellinien des Tetraeders. Im weiteren Sinne des Wortes nennt man Symmetrieachse einer geometrischen Figur jede Gerade, um die die Figur um einen von Null verschiedenen Winkel so gedreht werden kann, dass sie mit sich selbst zur Deckung kommt. In diesem Zusammenhang weisen wir darauf hin, dass jede Bewegung eines festen Körpers im Raume, die irgendeinen Punkt O festlässt, eine Drehung dieses Körpers um eine gewisse durch diesen Punkt O verlaufende Achse ist.

gibt, genügt es zu zeigen, dass zwei beliebige von Null verschiedene Elemente, die entweder zwei verschiedenen Gruppen H_i oder deren eines einer Gruppe H_i und deren anderes einer Gruppe H_{0k} entnommen sind, bereits ein Erzeugendensystem der gesamten Drehungsgruppe des Tetraeders bilden.
Dazu genügt es wiederum, zwei beliebige aus der Reihe der Elemente a_1, a_3, a_5, a_7 etwa a_1 und a_3 zu betrachten oder eines der Elemente a_1, a_3, a_5, a_7 und eines aus der Reihe a_9, a_{10}, a_{11}.
Wir überlassen es dem Leser, den geometrischen Beweis durchzuführen, und zwar zu beweisen, dass jede Drehung des Tetraeders durch Addition aus einem beliebigen der angegebenen Drehungspaare erzeugt werden kann.

Man kann dasselbe Resultat auch rechnerisch herleiten. Folgende Identitäten zeigen, dass zum Beispiel die Elemente a_1 und a_3 ein Erzeugendensystem der Drehungsgruppe des Tetraeders bilden:

$$\begin{aligned} a_0 = a_1 - a_1 \quad &; \quad a_7 = a_1 + a_3 - a_1 \\ a_2 = 2a_1 \quad &; \quad a_8 = 2a_1 + a_3 \\ a_4 = 2a_3 \quad &; \quad a_9 = -a_3 + a_1 + 2a_3 \\ a_5 = -a_3 + a_1 + a_3 \quad &; \quad a_{10} = a_1 + a_3 \\ a_6 = -a_3 + 2a_1 + a_3 \quad &; \quad a_{11} = a_3 + a_1 \end{aligned}$$

Man darf aber nicht denken, dass jedes Element in eindeutiger Weise durch die Erzeugenden darstellbar wäre. So gilt etwa $a_7 = a_1 + a_3 - a_1$ und gleichzeitig $a_7 = -a_3 - a_1 + a_3 + a_1 + a_3$.
Die Drehungsgruppe des Tetraeders ist nicht kommutativ: Es ist nämlich $a_1 + a_3 = a_{10}$, hingegen $a_3 + a_1 = a_{11}$.

Übung.
Wir überlassen es dem Leser, folgenden allgemeinen Satz zu beweisen: Eine Menge E von Elementen einer Gruppe G ist dann und nur dann ein Erzeugendensystem dieser Gruppe, wenn keine eigentliche Untergruppe der Gruppe G existiert, die sämtliche Elemente der Menge E enthält.

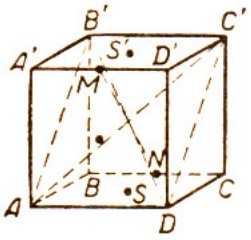
Unter Benutzung dieses Satzes sollen sämtliche Erzeugendensysteme der Drehungsgruppe des Tetraeders gefunden werden, die aus höchstens drei Elementen bestehen.
Bereits an diesem Beispiel sieht man, wie viele verschiedene Erzeugendensysteme eine endliche Gruppe haben kann.

5.5 Die Drehungsgruppe des Würfels und des Oktaeders

1. Um alle Kongruenzen eines Würfels[33] anzugeben, verfahren wir ebenso wie vorhin beim Tetraeder:

Wir betrachten zuerst nur die Kongruenzen des Würfels $ABCDA'B'C'D'$ (Abb. 8), die eine der Ecken, zum Beispiel A, in sich überführen.
Bei jeder Kongruenz eines Würfels gehen Ecken in Ecken, Kanten in Kanten, Flächen in Flächen über; auch die Diagonalen des Würfels gehen ineinander über. Eine gegebene Kongruenz lässt mit der Ecke A auch die, Diagonale AC' fest, da nur eine von A ausgehende Würfeldiagonale existiert.

[33] Ebenso wie beim Tetraeder verstehen wir unter einem Oktaeder stets ein regelmäßiges Oktaeder.



Also ist diese Kongruenz eine Drehung des Würfels um die Diagonale AC'. Von diesen Drehungen gibt es außer der identischen noch die beiden vom Winkel $\frac{2\pi}{3}$ und vom Winkel $\frac{4\pi}{3}$.

Es gibt also insgesamt drei Kongruenzen des Würfels, die den Eckpunkt A in sich überführen. Ebenso wie für den Eckpunkt A kann man die entsprechenden Drehungen für alle acht Ecken des Würfels finden.

Führt man entsprechende Überlegungen wie beim Tetraeder durch, so leitet man leicht ab, dass es insgesamt $3 \cdot 8 = 24$ Kongruenzen des Würfels gibt.

Wir wollen uns mit einer genaueren Festlegung dieser Kongruenzen befassen. Zunächst bemerken wir, dass ein Würfel 13 Symmetrieachsen hat: die vier Körperdiagonalen, die drei Geraden, welche je zwei gegenüberliegende Flächenmitten, sowie die sechs Geraden, die je zwei Mittelpunkte gegenüberliegender Kanten des Würfels verbinden.
Um jede der vier Diagonalen gibt es zwei nichtidentische Drehungen des Würfels, die den Würfel in sich überführen. Insgesamt gibt es also acht Drehungen um die Diagonalen.

Um jede der Geraden, welche die Mittelpunkte gegenüberliegender Flächen verbinden, gibt es drei nichtidentische Drehungen, und deren insgesamt folglich neun.

Schließlich haben wir eine nichtidentische Drehung vom Winkel π um jede Gerade, die die Mittelpunkte zweier gegenüberliegender Kanten verbindet, also insgesamt sechs dieser Art.
Somit gibt es $8 + 9 + 6 = 23$ nichtidentische Drehungen, die den Würfel in sich überführen. Wenn wir zu diesen noch die identische Drehung hinzufügen, erhalten wir 24 Kongruenzen, also alle überhaupt möglichen Kongruenzen des Würfels.

Somit erschöpfen die Drehungen des Würfels um seine Symmetrieachsen alle seine Kongruenzen.
Daher bezeichnet man ebenso wie beim Tetraeder die Gruppe der Kongruenzen des Würfels gewöhnlich als Drehungsgruppe des Würfels.
Ehe wir die Strukturuntersuchung der Drehungsgruppe fortsetzen, beweisen wir folgenden Hilfssatz:

Hilfssatz. Die einzige Drehung des Würfels, die jede der vier Diagonalen in sich überführt, ist die identische Drehung[34].

Wir bemerken zunächst, dass jede Drehung, die je zwei Diagonalen des Würfels, etwa. AC' und DB', in sich überführt, auch die Diagonalebene $ADC'B'$ (Abb. 8) in sich übergehen lässt. Jede nichtidentische Drehung, die eine gewisse Ebene in sich überführt, hat als Drehungsachse entweder eine in dieser Ebene liegende Gerade - in diesem Falle ist der Drehungswinkel gleich π - oder eine zu dieser Ebene senkrechte Gerade.
Nun führt aber eine Drehung der Ebene vom Winkeln um eine in ihr liegende Achse außer der Drehachse nur die zu dieser senkrechten Geraden der Ebene in sich über. Da das Rechteck $ADC'B'$ kein Quadrat ist, können seine Diagonalen, da sie nicht senkrecht aufeinander stehen, bei der Drehung um eine beliebige in der Ebene des Rechtecks liegende Achse nicht alle in sich selbst übergehen.

[34] Man darf folgendes nicht außer acht lassen: Geht bei einer vorgegebenen Drehung eine gegebene Diagonale, beispielsweise AC', in sich selbst über, so bedeutet das nicht, dass die Eckpunkte, die diese Diagonale festlegen (in unserem Falle die Ecken A und C'), wirklich in Ruhe bleiben. Sie können ihre Plätze vertauschen, d.h. A kann in C' und C' in A übergehen.

Also können AC' und DB' nur bei einer Drehung des Würfels um eine zur Ebene $ADC'B'$ senkrechte Achse in sich selbst übergehen. Diese Achse ist die Gerade MN, die die Mitten der Seiten $A'D'$ und BC verbindet. Die einzige nichtidentische Drehung des Würfels um die Gerade MN ist die Drehung um den Winkel π. Somit geht lediglich bei dieser Drehung jede der Diagonalen AC' und. DB' in sich über. Nun vertauschen aber bei dieser Drehung die beiden anderen Diagonalen BD' und CA' ihre Plätze, so dass es eine nichtidentische Drehung, die alle vier Diagonalen in sich überführt, überhaupt nicht gibt.

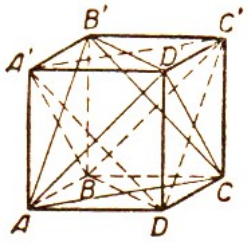
Also erfahren bei jeder nichtidentischen Drehung des Würfels seine vier Diagonalen eine nichtidentische Permutation. Daraus folgt:
Bei zwei verschiedenen Drehungen a und b erleiden auch die Diagonalen verschiedene Permutationen. Käme nämlich für zwei Drehungen a und b dieselbe Permutation der Diagonalen zustande, so blieben bei der Drehung $a - b$ alle Diagonalen fest, also wäre $a - b$ die identische Drehung, und die Drehungen a und b würden zusammenfallen.

Es entsprechen also den 24 verschiedenen Drehungen des Würfels die verschiedenen Permutationen der Diagonalen, die durch diese Drehungen hervorgebracht werden. Bekanntlich gibt es aber bei vier Elementen $1 \cdot 2 \cdot 3 \cdot 4 = 24$ Permutationen.
Daraus ergibt sich: Zwischen der Gruppe aller Würfeldrehungen und der Gruppe aller Permutationen der vier Diagonalen des Würfels besteht eine eineindeutige Zuordnung. Da bei unserer Zuordnung der Addition von Drehungen gerade die Addition der Permutationen[35]entspricht, so gilt folgender Satz:

1. Die Drehungsgruppe eines Würfels ist zur Gruppe aller Permutationen von vier Elementen isomorph.

Von den Untergruppen der Drehungsgruppe des Würfels erwähnen wir zunächst diejenigen zyklischen Untergruppen der Ordnung zwei, drei und vier, die aus Drehungen um die entsprechenden der 13 Symmetrieachsen des Würfels bestehen.
Es gibt sechs zyklische Untergruppen der Ordnung zwei, entsprechend der Anzahl der Achsen, die die Mittelpunkte je zweier gegenüberliegender Kanten verbinden; vier zyklische Untergruppen der Ordnung drei, gemäß der Anzahl der Diagonalen; drei zyklische Untergruppen der Ordnung vier, entsprechend der Anzahl der Geraden, die die Mittelpunkte gegenüberliegender Seitenflächen verbinden.

Viel interessanter sind folgende weitere Untergruppen.



a) Die Untergruppe der Ordnung zwölf, welche aus den Drehungen besteht, die gleichzeitig jedes der zwei dem Würfel einbeschriebenen Tetraeder $ACB'D'$ und $BDA'C'$ (Abb. 9) in sich überführen.
Diese Untergruppe besteht aus den $2 \cdot 4$ nichtidentischen Drehungen um die Diagonalen, aus den drei Drehungen vom Winkel π um die Achsen, welche die Mittelpunkte gegenüberliegender Seitenflächen verbinden, und aus der identischen Drehung.

b) Drei Untergruppen der Ordnung acht, die zur Gruppe der quadratischen Doppelpyramide (des Dieders) isomorph sind. Jede dieser Untergruppen besteht aus denjenigen Drehungen des

[35]Damit ist gemeint: Der Summe zweier Drehungen ist die Summe der diesen beiden Drehungen entsprechenden Permutationen zugeordnet, wobei sich die einander entsprechenden Summanden jeweils in der gleichen Reihenfolge befinden. Eine bloße eineindeutige Zuordnung zwischen den Drehungen und den Permutationen der Diagonalen hingegen würde lediglich eine im übrigen ganz willkürliche Zuordnung der Drehungen zu den Permutationen beinhalten.

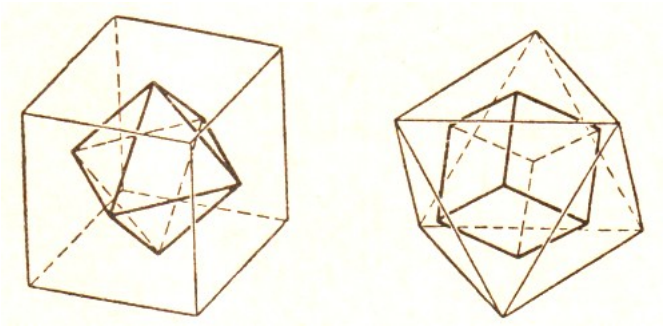
Würfels, die eine der Geraden in sich überführen, welche die Mittelpunkte zweier gegenüberliegender Flächen verbinden, beispielsweise die Punkte S und S' (Abb. 8).
Das dem Würfel einbeschriebene Oktaeder ist ein Spezialfall des quadratischen Dieders. Die Gruppe seiner Drehungen, die zwei seiner Ecken S und S' festlässt oder beide vertauscht, ist offensichtlich gerade die Gruppe des quadratischen Dieders.

Eine solche Untergruppe der Ordnung acht besteht aus folgenden acht Drehungen:
Vier Drehungen um die Achse SS' (einschließlich der identischen), zwei Drehungen vom Winkel π um die Achsen, die die Mittelpunkte der Kanten AA' und CC' bzw. BB' und DD' verbinden, und zwei Drehungen vom Winkel π um die Achsen, die die Mittelpunkte der Seitenflächen $ABB'A'$ und $CDD'C'$ bzw. $ADD'A'$ und $BCC'B'$ verbinden.

c) Eine Untergruppe der Ordnung vier, die aus der identischen Abbildung und drei Drehungen vom Winkel π um jede der Achsen besteht, welche die Mittelpunkte zweier gegenüberliegender Flächen verbinden. Diese Gruppe besteht aus denjenigen Drehungen, die in jeder der im vorigen Punkte erwähnten drei Untergruppen der Ordnung acht vorkommen. Sie ist kommutativ und zur Drehungsgruppe des Rhombus, also zur Kleinschen Vierergruppe, isomorph.
Außer dieser gibt es noch drei weitere Untergruppen der Ordnung vier, die ebenfalls der Drehungsgruppe des Rhombus isomorph sind.

2. Die Gruppe der Kongruenzen oder Drehungen eines regelmäßigen Oktaeders ist isomorph zur Drehungsgruppe des Würfels.

Um sich davon zu überzeugen, genügt es, um das regelmäßige Oktaeder einen Würfel zu beschreiben (Abb. 10) oder dem regelmäßigen Oktaeder einen Würfel einzubeschreiben (Abb. 11). Jeder Kongruenz des Oktaeders entspricht eine bestimmte Kongruenz des Würfels und umgekehrt.



Hierin kommt eine der dualen Beziehungen, die zwischen Würfel und Oktaeder bestehen, zum Ausdruck; wir werden sogleich näher auf sie eingehen.
Zunächst nennen wir zwei Elemente (Eckpunkte, Kanten, Flächen) irgendeines Vielflachs zusammengehörig, wenn eines dieser zwei Elemente dem anderen als konstituierendes Element angehört.
Demnach sind ein Eckpunkt und eine diesen Eckpunkt als Eckpunkt enthaltende Fläche, eine Fläche und eine Kante dieser Fläche, ein Eckpunkt und eine ihn als Endpunkt besitzende Kante Paare zusammengehöriger Elemente.

Zwei Vielflache heißen dual, wenn die Elemente des einen Vielflachs den Elementen des anderen eineindeutig zugeordnet werden können derart, dass dabei Paare zusammengehöriger Elemente des einen Vielflachs Paaren zusammengehöriger Elemente des anderen entsprechen und dass ferner den Eckpunkten des ersten Vielflachs die Flächen des zweiten, den Kanten des ersten Vielflachs die Kanten des zweiten, den Flächen des ersten Vielflachs die Ecken des

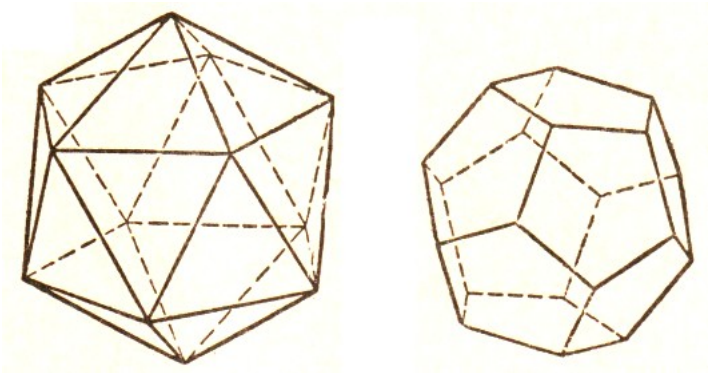
zweiten entsprechen.

Man sieht leicht, dass Würfel und Oktaeder in diesem Sinne zueinander dual sind. Das Tetraeder ist zu sich selbst dual.

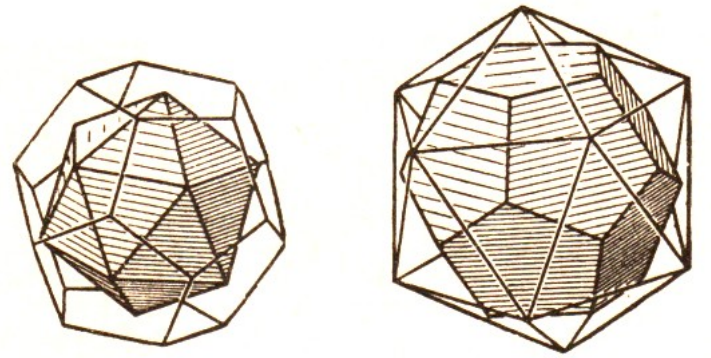
5.6 Die Drehungsgruppe des Ikosaeders und Dodekaeders

Allgemeine Bemerkungen über Drehungsgruppen regelmäßiger Vielflache

1. Von den fünf regelmäßigen Vielflachen bleiben noch zwei zu untersuchen: Ikosaeder[36] und Dodekaeder (Abb. 12 und 13).



Diese Vielflache sind zueinander dual, und die Gruppen ihrer Kongruenzen sind isomorph.
Um sich davon zu überzeugen, genügt es, das Ikosaeder in das Dodekaeder (Abb. 14) oder das Dodekaeder in das Ikosaeder (Abb. 15) einzubeschreiben.



Daher brauchen wir uns lediglich mit der Kongruenzgruppe des Ikosaeders vertraut zu machen. Um die Anzahl ihrer Elemente zu bestimmen, verfahren wir ebenso wie beim Tetraeder und beim Würfel. Wir betrachten nämlich zuerst diejenigen Kongruenzen des Ikosaeders, die einen bestimmten seiner Eckpunkte festlassen.

Es gibt fünf solcher Kongruenzen (a_i, $i = 0, 1, ..., 4$), nämlich fünf Drehungen um die Achse, die diese Ecke mit der gegenüberliegenden verbindet. Da es zwölf Ecken gibt (also $k = 0, 1, ..., 11$), beträgt die Anzahl der Kongruenzen des Ikosaeders $5 \cdot 12 = 60$.

Alle diese Kongruenzen sind Drehungen des Ikosaeders um seine Symmetrieachsen. Im einzelnen gibt es folgende Symmetrieachsen des Ikosaeders:

[36] Wir meinen wiederum ein regelmäßiges Ikosaeder und ein regelmäßiges Dodekaeder.

Sechs Achsen, die gegenüberliegende Eckpunkte verbinden; um jede von ihnen gibt es 4 nichtidentische Drehungen (mit den Winkeln $\frac{2\pi}{5}$, $\frac{4\pi}{5}$, $\frac{6\pi}{5}$, $\frac{8\pi}{5}$), die das Ikosaeder mit sich selbst zur Deckung bringen ; insgesamt erhalten wir also $4 \cdot 6 = 24$ Drehungen.
Zehn Achsen, die die Mittelpunkte gegenüberliegender Flächen verbinden; um jede dieser Achsen gibt es zwei nichtidentische Drehungen (mit den Winkeln $\frac{2\pi}{3}$ und $\frac{4\pi}{3}$), also insgesamt 20 Drehungen;

Fünfzehn Achsen, die die Mittelpunkte gegenüberliegender Kanten verbinden und von denen jede eine einzige nichtidentische Drehung um 180° liefert.
Also gibt es $24 + 20 + 15$, d.h. bei Hinzunahme der identischen insgesamt 60 Drehungen.

Durch ähnliche Überlegungen wie früher folgt hieraus, dass das Ikosaeder genau 31 Symmetrieachsen besitzt.
Da die Drehungsgruppe des Ikosaeders reichlich kompliziert ist, werden wir sie hier nicht weiter untersuchen. Wir erwähnen nur, dass sie der alternierenden Permutationsgruppe von fünf Elementen isomorph ist.

2. Die Drehungsgruppen der regulären Vielecke und Vielflache wurden als Gruppen ihrer Kongruenzen definiert.
Wir betrachten nun gleichsam zwei Exemplare des Raumes, von denen einer im anderen eingebettet ist. Den einen Raum denken wir uns als einen nach allen Seiten unendlich ausgedehnten starren Körper und bezeichnen ihn als starren Raum, während wir den anderen als leeren Raum auffassen.

Den starren Raum denken wir uns in den leeren verschiebbar eingebettet. Unser Vielflach erscheint als unbeweglicher Teil des starren Raumes, ist also nur zusammen mit ihm einer Bewegung fähig.[37]
Dann kann man sämtliche Drehungen des "starren" Raumes im "leeren" um irgendeine Achse betrachten, die das vorgegebene Vielflach mit sich zur Deckung bringen, es also in sich überführen.

Da sich jede Kongruenz der betrachteten Vielflache als Drehung um eine passende Achse erwies und jede Drehung des Vielflachs um eine Achse als Ursache für eine Drehung des Gesamtraumes um diese Achse angesehen werden kann, ist die Gruppe der Kongruenzen eines vorgegebenen Vielflachs isomorph zur Gruppe der Drehungen des Raumes, welche dieses Vielflach in sich überführen.
Eben diese Gruppe meint man gewöhnlich, wenn man von der Drehungsgruppe eines vorgegebenen regelmäßigen Vielflachs spricht. Oft bezeichnet man sie einfach als "Gruppe des regelmäßigen Vielflachs".

Die Gruppe einer regelmäßigen Pyramide (also eine endliche zyklische Gruppe), die Diedergruppen und die eben betrachteten Gruppen der regelmäßigen Vielflache sind die einzigen endlichen Untergruppen der Gruppe aller Bewegungen des Raumes.

[37] Dieser "feste", im ruhenden "leeren" bewegliche Raum gleicht einer auf einer Tischebene beweglichen Glasplatte (siehe § 2, drittes Beispiel).

6 Invariante Untergruppen

6.1 Konjugierte Elemente und Untergruppen

1. Transformation eines Gruppenelements mit Hilfe eines anderen

Wir betrachten in der Gruppe G zwei beliebige Elemente a und b. Das Element $-b+a+b$ heißt Transformierte des Elementes a mittels b.
Wir wollen untersuchen, unter welcher Bedingung die Gleichung

$$-b+a+b=a \tag{1}$$

gilt. Ist die Gleichung (1) erfüllt, so erhalten wir, wenn wir auf ihren beiden Seiten von links b hinzufügen,

$$a+b=b+a \tag{1'}$$

Ist also (1) erfüllt, so auch (1'), d.h., die Elemente a und b sind vertauschbar. Gilt umgekehrt (1'), so auch

$$-b+a+b=-b+b+a=a$$

und damit die Gleichung (1). Somit gilt:

Ein Element a' ist genau dann gleich seiner Transformierten mittels b, wenn die Elemente a und b vertauschbar sind, d.h. wenn die Gleichung (1') gilt.

Insbesondere gilt Gleichung (1) in kommutativen Gruppen für beliebige Elemente a und b.
Zur Veranschaulichung des Begriffes der Transformierten betrachten wir die Gruppe G aller Permutationen von n Elementen. Es sei

$$a=\begin{pmatrix} 1 & 2 & 3 & ... & n \\ a_1 & a_2 & a_3 & ... & a_n \end{pmatrix} \quad , \quad b=\begin{pmatrix} 1 & 2 & 3 & ... & n \\ b_1 & b_2 & b_3 & ... & b_n \end{pmatrix}$$

Dann gilt offensichtlich

$$-b=\begin{pmatrix} b_1 & b_2 & b_3 & ... & b_n \\ 1 & 2 & 3 & ... & n \end{pmatrix}, \quad -b+a=\begin{pmatrix} b_1 & b_2 & b_3 & ... & b_n \\ a_1 & a_2 & a_3 & ... & a_n \end{pmatrix},$$
$$-b+a+b=\begin{pmatrix} b_1 & b_2 & b_3 & ... & b_n \\ b_{a_1} & b_{a_2} & b_{a_3} & ... & b_{a_n} \end{pmatrix} \tag{2}$$

Die Formel (2) kann in Form folgender Regel aufgeschrieben werden:
Es sei

$$a=\begin{pmatrix} 1 & 2 & 3 & ... & n \\ a_1 & a_2 & a_3 & ... & a_n \end{pmatrix} \quad , \quad b=\begin{pmatrix} 1 & 2 & 3 & ... & n \\ b_1 & b_2 & b_3 & ... & b_n \end{pmatrix}$$

Um die Transformierte der Permutation a mittels der Permutation b zu erhalten, muss man in beiden Zeilen der wie üblich aufgeschriebenen Permutation a die Permutation b vornehmen.

Wir wollen diese Regel noch an einem Beispiel erläutern. Es sei zum Beispiel $n=3$ und

$$a=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad , \quad b=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Wir erhalten

$$-b+a+b=\begin{pmatrix} 3 & 2 & 1 \\ 2 & 3 & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \neq a$$

Man versteht die eben eingeführte Regel viel besser, wenn man den Begriff der Abbildung oder der Funktion[38] benutzt.
Die Permutation a kennzeichnet eine Funktion $y = f(x)$,

$$(x = 1, 2, 3, ...n; \quad y = 1, 2, 3, ..., n)$$

bei der zwei verschiedenen x-Werten immer zwei verschiedene y-Werte entsprechen. Die Permutation b ist eine Funktion $y = \phi(x)$ derselben Art wie $f(x)$. Die Permutation $-b + a + b$ ist dann eine Funktion $y = F(x)$, die durch folgende Formel definiert ist:

$$F(x) = \phi\{f[\phi^{-1}(x)]\} \tag{3}$$

Man erhält sie, indem man dem Element $\phi(x)$ das Element $\phi[f(x)]$ zuordnet. Dies ist unmittelbar zu sehen, wenn man in Formel (3) an Stelle von x das Element $\phi(x)$ einsetzt und beachtet, dass gilt

$$\phi^{-1}[\phi(x)] = x$$

Mit x durchläuft auch $\phi(x)$ alle Zahlen $1, 2, 3, ..., n$, nur in anderer Reihenfolge. Durch die Formel

$$F[\phi(x)] = \phi[f(x)] \tag{4}$$

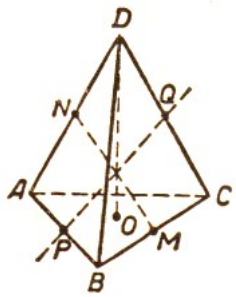
ist die Funktion $F(x)$, also die Permutation $-b + a + b$, eindeutig definiert.

Die Formel (4) stellt nur eine andere Schreibweise von (2) dar. Bezeichnet man schließlich $f(x)$ mit y, so kann man das erhaltene Resultat auch noch folgendermaßen formulieren:
Die Permutation F besteht darin, dass das Element $\phi(x)$ durch das Element $\phi(y)$ ersetzt wird.

Da jede endliche Gruppe einer gewissen Permutationsgruppe isomorph ist, erläutert Formel (2) den Begriff "Transformierte" wenigstens für alle endlichen Gruppen.

2. Transformation von Elementen der Tetraedergruppe

Wir betrachten als weiteres Beispiel die Drehungsgruppe des Tetraeders $ABCD$ (Abb. 16).



Es sei a die Drehung des Tetraeders vom Winkel π um die Achse MN, die die Mitten der Kanten BC und AD verbindet; es sei b die Drehung um die Achse DO, die A in C, B in A, C in B überführt. Dann ist $-b+a+b$ die Drehung vom Winkel π um die Achse PQ, die die Mittelpunkte der Kanten AB und CD verbindet.

Man kann sich davon sowohl unmittelbar als auch dadurch überzeugen, dass man die Drehung a als Permutation $\begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}$ und die Drehung b als Permutation $\begin{pmatrix} A & B & C & D \\ C & A & B & D \end{pmatrix}$ der Eckpunkte auffasst.

Führt man nun in jeder Zeile des Ausdruckes $\begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}$ die Permutation $\begin{pmatrix} A & B & C & D \\ C & A & B & D \end{pmatrix}$ aus,so erhält man $\begin{pmatrix} C & A & B & D \\ D & B & A & C \end{pmatrix}$, also $\begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}$, was der

[38] siehe Anhang § 4

Drehung um die Achse PQ um 180° entspricht.

Auf dieselbe Weise überzeugt man sich davon, dass $-a+b+a$ die Drehung um diejenige Achse ist, welche die Ecke A mit dem Mittelpunkt der Fläche BCD verbindet; sie führt B in C, C in D, D in B über.
Dieser Drehung entspricht die Permutation $\begin{pmatrix} A & B & C & D \\ A & C & D & B \end{pmatrix}$.

3. Konjugierte Elemente

Es sei G irgendeine Gruppe.
Satz I'. Ist das Element b die Transformierte des Elementes a mittels des Elementes c, so ist das Element a die Transformierte von b mittels $-c$.

Tatsächlich folgt aus

$$b = -c + a + c$$

wenn auf beiden Seiten von links c und von rechts $(-c)$ hinzugefügt wird,

$$c + b + (-c) = a \qquad \text{also} \qquad a = -(-c) + b + (-c)$$

Definition. Zwei Gruppenelemente heißen konjugiert, wenn eines von ihnen die Transformierte des anderen ist.

Satz I". Ist a zu b und b zu c konjugiert, so auch a zu c:

Da a zu b konjugiert ist, existiert ein Element d, so dass

$$b = -d + a + d \tag{5}$$

gilt; da b zu c konjugiert ist, existiert ein Element e derart, dass

$$b = -e + c + e \tag{5'}$$

gilt, folglich ist

$$-d + a + d = -e + c + e$$

Fügt man auf beiden Seiten der letzten Gleichung von links d und von rechts $-d$ hinzu, so erhält man:

$$a = (d - e) + c + (e - d) = -(e - d) + c + (e - d)$$

d.h., a ist die Transformierte von c mittels $e - d$, womit a als zu c konjugiert nachgewiesen ist.

Satz I"'. Jedes Element ist zu sich selbst konjugiert.

Es gilt nämlich

$$a = -0 + a + 0$$

Die Sätze I', I", I"' besagen, dass die Konjugiertheit zweier Gruppenelemente die Eigenschaften der Symmetrie[39], Transitivität und Reflexivität besitzt. Daraus folgt wegen Satz III des Anhangs

Satz 1. Jede Gruppe G zerfällt in Klassen paarweise zueinander konjungierter Elemente.

Dabei besteht die Klasse irgendeines Elementes a der Gruppe G aus allen zu a konjugierten

[39] Siehe Anhang § 5, insbesondere Artikel 8.

Elementen der Gruppe G, also aus den Transformierten des Elementes a mittels aller möglichen Elemente der Gruppe G.
Wir stellen fest, dass die Klasse des neutralen Elementes jeder Gruppe G nur aus diesem Element besteht (denn für beliebiges a gilt $-a+0+a=0$).

Aufgabe. Man beweise, dass die Drehungsgruppe des Tetraeders in folgende Klassen konjugierter Elemente zerfällt:

1. die Klasse, die allein aus dem neutralen Element besteht;

2. die Klasse, die aus den Drehungen vom Winkel $\frac{2}{3}\pi$ um jede der vier Achsen besteht, die jeweils die Ecken des Tetraeders mit den Mittelpunkten der gegenüberliegenden Seitenflächen verbinden;

3. die Klasse, die aus den vier Drehungen vom Winkel $\frac{4}{3}\pi$ um dieselben Achsen besteht (dabei werden die Drohungen von einer festen Ecke aus entweder im oder entgegen dem Uhrzeigersinn gerechnet);

4. die Klasse, die aus den Drehungen vom Winkel π um jede der drei Achsen besteht, die die Mittelpunkte zweier gegenüberliegender Kanten des Tetraeders verbinden.

Wir überlassen es dem Leser, auch Klassen konjugierter Elemente in anderen Drehungsgruppen zu untersuchen.

4. Transformation einer Untergruppe

Die Klasse konjugierter Elemente, zu der das Element a der Gruppe G gehört, besteht aus den Transformierten des Elementes a mittels aller möglichen Elemente b der Gruppe G.
Jetzt wählen wir irgendeine Untergruppe H der Gruppe G und wollen die Transformierten aller möglichen Elemente x dieser Untergruppe mittels eines willkürlich, aber fest gewählten Elementes b der Gruppe G betrachten. Die sich ergebende Menge von Elementen, also die Gesamtheit aller Elemente der Form

$$-b+x+b$$

wobei b ein von uns fest gewähltes Element der Gruppe G ist und x alle Elemente der Untergruppe H durchläuft, nennen wir Transformierte der Untergruppe H mittels b; wir bezeichnen sie mit

$$-b+H+b$$

Behauptung: $-b+H+b$ ist eine Gruppe.

Beweis:. 1. Es seien c_1 und c_2 zwei Elemente, die zu $-b+H+b$ gehören. Wir zeigen: c_1+c_2 gehört zu $-b+H+b$.
Es gilt

$$c_1=-b+x_1+b \qquad ; \qquad c_2=-b+x_2+b \tag{6}$$

wobei x_1 und x_2 Elemente der Gruppe H sind.
Aus (6) folgt unmittelbar:

$$c_1+c_2=-b+x_1+x_2+b \tag{7}$$

also ist c_1+c_2 die Transformierte des Elementen x_1+x_2 mittels b; daher gehört c_1+c_2 zu $-b+H+b$.

2. Wir zeigen: das neutrale Element 0 der Gruppe G gehört zu $-b+H+b$. Da 0 ein Element von H ist und $-b+0+b=0$ gilt, gehört 0 auch zu $-b+H+b$.

3. Gehört schließlich a zu $-b+H+b$, so ist auch $-a$ Element von $-b+H+b$: Gehört nämlich a zu $-b+H+b$, so ist $a=-b+x+b$, wobei x ein gewisses Element von H ist.
Dann ist aber $-a=-(-b+x+b)=-b+(-x)+b$, also ist $-a$ die Transformierte des Elementes $-x$ der Gruppe H mittels b, und folglich ist $-a$ ein Element der Menge $-b+H+b$.
Somit ist $-b+H+b$ eine Gruppe.

Jedem Element x der Gruppe H entspricht ein eindeutig bestimmtes Element der Gruppe $-b+H+b$, nämlich das Element $-b+x+b$.
Dabei entsprechen zwei verschiedenen Elementen x_1 und x_2 verschiedene Elemente $-b+x_1+b$ und $-b+x_2+b$; denn für $x_1 \neq x_2$ sind wegen der Eindeutigkeit der Subtraktion auch die Elemente x_1+b und x_2+b[40] verschieden und damit auch die Elemente $-b+x_1+b$ und $-b+x_2+b$[41]

Lässt man also dem Element x der Gruppe H das Element $-b+x+b$ der Gruppe $-b+H+b$ entsprechen, so erhält man eine eineindeutige Zuordnung zwischen H und $-b+H+b$. Wegen der Gleichungen (6) und (7) entspricht der Summe zweier Elemente x_1 und x_2 dabei die Summe der Elemente $(-b+x_1+b)$ und $(-b+x_2+b)$. Also ist diese Zuordnung ein Isomorphismus zwischen den Gruppen H und $-b+H+b$.
Damit haben wir folgenden Satz bewiesen:

Satz II. Die Transformierte der Untergruppe H der Gruppe G mittels b aus G ist eine zu H isomorphe Untergruppe von G.

Bemerkung. Aus der Definition der transformierten Untergruppe folgert man unmittelbar die nachstehenden Sätze:

1. Ist G eine kommutative Gruppe und H eine Untergruppe, so ist die Transformierte von H mittels eines beliebigen Elementes b der Gruppe G die Gruppe H selbst, da in diesem Falle die Transformierte eines beliebigen Elementes x mittels b dieses Element selbst ist, $-b+x+b=x$.

2. Ist G eine beliebige Gruppe, H eine Untergruppe und b ein Element von H, so ist

$$-b+H+b=H$$

da für jedes Element x der Gruppe H für zu H gehöriges b auch das Element $-b+x+b$ zu H gehört.

Ist die Untergruppe H_2 die Transformierte der Untergruppe H_1 mittels des Elementes b, so ist H_1 die Transformierte der Untergruppe H_2, mittels des Elementes $-b$.
Der Beweis folgt aus Satz I' der Nummer 3.

Definition. Zwei Untergruppen einer Gruppe G, deren eine eine Transformierte der anderen ist, heißen konjugierte Untergruppen.

Wegen $-0+H+0=H$ ist jede Gruppe zu sich selbst konjugiert.
Aus Satz I'' folgt, dass zwei Untergruppen, die zu einer dritten konjugiert sind, auch untereinander konjugiert sind, so dass die Menge aller Untergruppen einer Gruppe G in Klassen untereinander konjugierter Untergruppen zerfällt.
Wir wissen bereits (Satz II dieses Abschnitts), dass alle zueinander konjugierten Untergruppen zueinander isomorph sind.

[40] Aus $x_1+b=x_2+b=c$ folgt nämlich $x_1=c-b$ und $x_2=c-b$.
[41] Für $-b+x_1+b=-b+x_2+b=c$ gilt nämlich $x_1+b=b+c$ und $x_2+b=b+c$.

5. Beispiele

In der Drehungsgruppe des regelmäßigen Tetraeders gibt es, wie wir gesehen haben, folgende Untergruppen:

1. Zwei uneigentliche Untergruppen: Erstens die aus dem neutralen Element bestehende und zweitens die aus allen zwölf Drehungen des Tetraeders bestehende Untergruppe. Jede dieser Untergruppen ist offensichtlich zu sich selbst konjugiert.

2. Drei Untergruppen der Ordnung zwei: H_{01}, H_{02}, H_{03} deren jede aus Drehungen um die Winkel 0 und π um gewisse Kantenmittellinien besteht. Alle diese Gruppen bilden eine Klasse konjugierter Untergruppen.

3. Die Gruppe H der Ordnung vier (die Kleinsche Vierergruppe), welche die mengentheoretisehe Vereinigung der drei Gruppen H_{01}, H_{02}, H_{03} ist, also aus der identischen Drehung und aus Drehungen vom Winkeln um jede der drei Kantenmittellinien besteht.
Aus der Definition der Gruppe H als Vereinigung der Gruppen H_{01}, H_{02}, H_{03} und daraus, dass die Gruppen H_{01}, H_{02}, H_{03} eine Klasse konjugierter Untergruppen bilden, folgt, dass die Gruppe H lediglich zu sich selbst konjugiert ist.

4. Vier Untergruppen der Ordnung drei: H_0, H_1, H_2, H_3. Jede von ihnen besteht aus Drehungen um die Winkel 0, $\frac{2\pi}{3}$, $\frac{4\pi}{3}$ um gewisse Flächenmittellinien. Alle diese Gruppen bilden ebenfalls eine Klasse konjugierter Untergruppen.

Demnach zerfallen alle 10 Untergruppen der Drehungsgruppe eines regelmäßigen Tetraeders folgendermaßen in Klassen konjugierter Untergruppen:

1. drei jeweils aus einem Element bestehende Klassen, nämlich die jeweils eine einzige der uneigentlichen Untergruppen enthaltenden und die aus der einen Untergruppe der Ordnung vier bestehenden Klassen,

2. die Klasse aus den drei Untergruppen der Ordnung zwei;

3. die Klasse, die aus den vier Untergruppen der Ordnung drei besteht.

6.2 Invariante Untergruppen (Normalteiler)

1. Definition

Wenn eine Untergruppe H einer vorgelegten Gruppe G keine von sich verschiedene konjugierte Untergruppe besitzt (wenn also die Klasse aller Untergruppen, die in der Gruppe G zur Untergruppe H konjugiert sind, lediglich aus der einen Gruppe H besteht), so nennen wir die Untergruppe H invariante[42] Untergruppe (oder Normalteiler) der Gruppe G.

Offensichtlich kann die Definition der invarianten Untergruppe auch so formuliert werden:
Wir nennen eine Untergruppe H einer Gruppe G invariant, wenn die Transformierte eines beliebigen Elementes der Gruppe H mittels eines Elementes der Gruppe G ein Element der Gruppe H ist.

Der Begriff der invarianten Untergruppe ist einer der wichtigsten Begriffe der gesamten Algebra. Wenn es auch unmöglich ist, in diesen kurzen Darlegungen dem Leser die volle Bedeutung

[42] Invariant (lateinisch) bedeutet sich nicht ändernd bei einer Transformation der Untergruppe.

dieses Begriffes klarzumachen, der in der Algebra speziell in der sogenannten Galoisschen Theorie auftritt, so möchten wir doch hoffen, dass aus den Untersuchungen dieses und des nächsten Kapitels dem Leser deutlich wird, welch große Bedeutung die invarianten Untergruppen im logischen Aufbau der Gruppentheorie selbst besitzen.

2. Beispiele

Triviale Beispiele invarianter Untergruppen sind die beiden uneigentlichen Untergruppen jeder beliebigen Gruppe. Außerdem ist offensichtlich jede Untergruppe einer kommutativen Gruppe eine invariante Untergruppe.
Wir geben einige weniger triviale Beispiele an.

1. Die Gruppe der Verschiebungen einer Geraden in sich ist eine invariante Untergruppe aller Kongruenzen einer Geraden (Kap. V, § 2).

2. Die zyklische Gruppe A der Ordnung n, die aus allen Kongruenzen erster Art eines n-eckigen Dieders besteht, ist eine invariante Untergruppe der Gruppe aller Drehungen eines n-eckigen Dieders.[43]

3. Die alternierende Permutationsgruppe A_n von n Ziffern ist eine invariante Untergruppe der Gruppe S_n aller Permutationen von n Ziffern. Ist nämlich b ein beliebiges Element der Gruppe A_n, also eine beliebige gerade Permutation, und a ein beliebiges Element der Gruppe S_n also eine beliebige gerade oder ungerade Permutation, so ist das Signum der Permutation $-a+b+a$ gleich dem Produkt dreier Zahlen, die gleich $+1$ oder -1 sind:

$$(\operatorname{sgn} -a) \cdot (\operatorname{sgn} b) \cdot (\operatorname{sgn} a)$$

Da $(\operatorname{sgn} -a) = (\operatorname{sgn} a)$ ist, so ist $(\operatorname{sgn} -a) \cdot (\operatorname{sgn} a)$ in jedem Falle, d.h. für beliebiges a, gleich $+1$. Folglich gilt

$$(\operatorname{sgn}(-a+b+a)) = (\operatorname{sgn} b) = +1$$

dies bedeutet, dass $-a+b+a$ eine gerade Permutation, also Element der Gruppe A_n ist.
Somit ist die Transformierte eines beliebigen Elementes b der Gruppe A_n ein (im allgemeinen von b verschiedenes) Element der Gruppe A_n, d.h., A_n ist eine invariante Untergruppe der Gruppe S_n.

Wir kehren zu den Beispielen invarianter und nicht invarianter Untergruppen zurück.

Wir haben bereits gesehen, dass es in der Gruppe aller Drehungen des Tetraeders eine eigentliche invariante Untergruppe der Ordnung vier gibt. Da die Gruppe aller Drehungen des Tetraeders isomorph zur alternierenden Gruppe A_4 der Permutationen von vier Elementen ist (also zur Gruppe aller geraden Permutationen von vier Elementen), so kann man das erhaltene Resultat auch so formulieren:
Die alternierende Permutationsgruppe von vier Elementen besitzt eine invariante Untergruppe der Ordnung vier.

Dies Ergebnis ist sehr wichtig:
Es zeigt sich, dass für $n > 4$ die alternierende Permutationsgruppe A_n von n Ziffern außer den zwei uneigentlichen Untergruppen keine invariante Untergruppe enthält.

[43] Ist nämlich a eine Kongruenz aus erster und b eine Kongruenz zweiter Art, so gilt (wie in Kap. V, § 3 gezeigt wurde): $a+b=b-a$ und daher $-b+a+b=-a$. Da dies für jedes Element der Untergruppe A gilt, ist $-b+A+b=A$.

Diese Tatsache, deren Beweis der Leser beispielsweise in dem bereits zitierten Buche "Gruppentheorie" von A.G. Kurosch finden kann, hat große Bedeutung in der Algebra:
Sie hängt eng damit zusammen, dass im allgemeinen eine Gleichung des Grades $n > 4$ nicht durch Radikale (Wurzelausdrücke) gelöst werden kann.

Die Drehungsgruppe des Würfels ist, wie wir wissen, zur Gruppe S_4 isomorph. Also gibt es in ihr sicher eine zur Gruppe A_4 isomorphe invariante Untergruppe. Diese Untergruppe ist uns bereits aus Kap. V, § 5 bekannt: Sie besteht aus den Drehungen, die jedes der beiden dem Würfel einbeschriebenen Tetraeder in sich überführen.

Wir haben auch bereits die drei Untergruppen der Ordnung acht erwähnt, die in der Drehungsgruppe des Würfels enthalten sind. Diese drei Gruppen bilden eine Klasse untereinander konjugierter Gruppen, folglich ist keine davon invariant. Dafür ist der Durchschnitt dieser drei Gruppen eine invariante Untergruppe, die, wie wir wissen, aus dem neutralen Element und aus drei Drohungen des Würfels von 180° um jede der drei Geraden besteht, die die Mittelpunkte zweier gegenüberliegender Seiten verbinden.[44]
Andere eigentliche invariante Untergruppen außer den angegebenen Gruppen der Ordnung zwölf und vier gibt es in der Drehungsgruppe des Würfels nicht.

Wir erwähnen noch folgende Klassen konjugierter Gruppen:

1. Die Klasse, die aus drei zyklischen Gruppen der Ordnung vier besteht; jede dieser Gruppen besteht aus Drehungen um eine der Achsen, die die Mittelpunkte zweier gegenüberliegender Flächen des Würfels verbinden.

2. Die Klasse, die aus vier zyklischen Gruppen der Ordnung drei besteht; jede dieser Gruppen besteht aus Drehungen um eine der Diagonalen.

3. Die Klasse, die aus sechs zyklischen Gruppen der Ordnung zwei besteht; jede dieser Gruppen besteht aus Drehungen um eine der Achsen, die die Mittelpunkte zweier gegenüberliegender Kanten verbinden.

Schließlich betrachten wir die uns bereits bekannte Bewegungsgruppe der Ebene in sich genauer (Kap. V, § 2).
Wir stellen folgende Bemerkung voran. Jede Bewegung einer Ebene in sich ordnet jedem Punkt x der Ebene einen gewissen eindeutig bestimmten Punkt $f(x)$ der Ebene zu, nämlich denjenigen, in den der Punkt x durch die vorgegebene Bewegung übergeht.

Wir können also jede Bewegung als eine gewisse Abbildung der Ebene auf sich auffassen. Diese Abbildung ist eine kongruente Abbildung, der Abstand zwischen den Punkten bleibt also ungeändert.
Werden zwei Punkte x und y in $f(x)$ und $f(y)$ übergeführt, so ist der Abstand zwischen den Punkten $f(x)$ und $f(y)$ gleich dem Abstand zwischen den Punkten x und y. Daraus folgt insbesondere, dass niemals zwei verschiedene Punkte der Ebene bei der Bewegung gleichzeitig in ein und denselben Punkt übergeben können.
Sind die zwei Punkte x und y verschieden, so ist ihr Abstand ungleich Null. Dann muss aber auch der Abstand zwischen den Punkten $f(x)$ und $f(y)$ von Null verschieden sein; also können die Punkte $f(x)$ und $f(y)$ nicht zusammenfallen. Somit ist jede Bewegung eine eineindeutige Abbildung der Ebene auf sich.

[44] Dem Leser sei empfohlen, folgenden allgemeinen Sets zu beweisen: Der Durchschnitt aller Gruppen, die in einer gewissen Klasse untereinander konjugierter Untergruppen vorkommen, ist eine invariante Untergruppe.

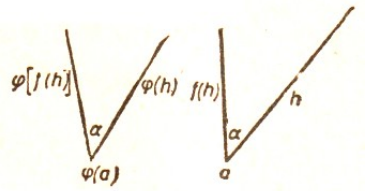
Eine als eineindeutige Abbildung der Ebene auf sich aufgefasste Bewegung wollen wir mit dem Symbol $f(x)$ bezeichnen, wobei x natürlich ein willkürlicher Punkt der Ebene ist.
Es seien zwei Bewegungen $f(x)$ und $\phi(x)$ vorgegeben. Wir wollen die Transformierte der Bewegung $f(x)$ mittels der Bewegung $\phi(x)$ aufstellen. Nach Definition ist dies die Bewegung

$$F(x) = \phi\{f[\phi^{-1}(x)]\} \tag{1}$$

Da $\phi(x)$ eine eineindeutige Abbildung der Ebene ist, so ist die Bewegung $F(x)$ vollständig beschrieben, wenn bekannt ist, wohin bei dieser Bewegung der Punkt $\phi(x)$ für beliebiges x übergeht.
Mit anderen Worten: die Abbildung $F(x)$ ist für beliebiges x definiert, wenn wir wissen, wohin sie (ebenfalls für beliebiges x) den Punkt $\phi(x)$ überführt. Ersetzt man nun in Formel (1) x durch $\phi(x)$ und beachtet, dass $\phi^{-1}[\phi(x)] = x$ ist, so erhält man

$$F[\phi(x)] = \phi[f(x)] \tag{2}$$

Durch diese Formel ist die Bewegung $F(x)$ vollständig bestimmt.



Setzt man $f(x) = y$, so bedeutet die Formel (2) folgendes: Die Bewegung F führt den Punkt $\phi(x)$ für beliebiges x in den Punkt $\phi(y)$ über.
Wir beweisen jetzt folgende Aussage:

Ist f eine Drehung um den Punkt a vom Winkel α, so ist F eine Drehung um den Punkt $\phi(a)$ vom gleichen Winkel α (Abb. 17).
Da f eine Drehung um a ist, so ist $f(a) = a$. woraus sich nach Formel (2) ergibt:

$$F[\phi(a)] = \phi(a)$$

F ist also eine Drehung um $\phi(a)$. Die Bewegung f dreht eine von a ausgehende willkürliche Halbgerade h um den Winkel α und führt diese dabei in die Halbgerede $f(h)$ über.
Die Bewegung ϕ, die eine kongruente Abbildung ist, führt die Figur, die aus den beiden von a unter dem Winkel α ausgehenden Halbgeraden h und $f(h)$ besteht, in eine kongruente Figur über, die aus den beiden Halbgeraden $\phi(h)$ und $\phi[f(h)] = F[\phi(h)]$ besteht, die von $\phi(a)$ ausgehen.
Somit erhält man die Halbgerade $F[\phi(h)]$ aus der Halbgeraden $\phi(h)$ ebenfalls durch eine Drehung vom Winkel α, d.h., da die Bewegung F die Halbgerade $\phi(h)$ um den Winkel α dreht, ist also F eine Drehung um den Winkel α.

Aus dem eben Bewiesenen folgt:
Die Transformierte der Gruppe der Drehungen der Ebene um den Punkt a mittels einer beliebigen Bewegung ϕ ist die Gruppe der Drehungen der Ebene um den Punkt $\phi(a)$.

Es sei f eine Translation der Ebene längs der Geraden g und ϕ eine beliebige Bewegung der Ebene in sich.
Dann gilt zunächst die Identität

$$f(g) = g$$

d.h., die Gerade g geht bei der Bewegung f in sich über.
Die Bewegung ϕ führt die Gerade G in die Gerade $\phi(g)$ über. Aus Formel (2) folgt bei Anwendung auf einen beliebigen Punkt x der Geraden g:

$$F[\phi(g)] = \phi(g)$$

Die Bewegung F führt also die Gerade $\phi(g)$ in sich über und ist folglich eine Translation längs dieser Geraden. Da ϕ eine kongruente Abbildung ist, so ist der Abstand zwischen x und $y = f(x)$ gleich dem Abstand zwischen $\phi(x)$ und $\phi[f(x)]$, also zwischen $\phi(x)$ und $F[\phi(x)]$. Dies bedeutet: Die Translation F verrückt die Punkte der Ebene um die gleiche Strecke wie die Translation f.

Aus dem Bewiesenen folgt:
Die Gruppe der Parallelverschiebungen der Ebene längs einer vorgegebenen Geraden g wird durch eine willkürlich vorgegebene Bewegung ϕ in die Gruppe der Parallelverschiebungen der Ebene längs der Geraden $\phi(g)$ transformiert.

Da jede Bewegung ϕ jede Parallelverschiebung der Ebene in eine Parallelverschiebung transformiert, so erhalten wir folgendes wichtige Resultat:
Die Gruppe aller Parallelverschiebungen der Ebene (längs aller möglichen Geraden) ist eine invariante Untergruppe der Gruppe aller Bewegungen der Ebene in sich.

7 Homomorphe Abbildungen

7.1 Definition der homomorphen Abbildung und ihres Kernes

Definition und einfache Eigenschaften

Es sei jedem Element a einer Gruppe A ein Element

$$b = f(a)$$

einer Gruppe B zugeordnet. Die Gesamtheit aller so erhaltenen Elemente $b = f(a)$ der Gruppe B bezeichnen wir mit $f(A)$. Wir sagen, es liege eine Abbildung f der Gruppe A in die Gruppe B vor: mengenmäßig gilt nämlich $f(A) \subseteq B$.
Wir führen jetzt folgende grundlegende Definition ein:

Eine Abbildung f einer Gruppe A in eine Gruppe B heißt homomorph, wenn für je zwei beliebige Elemente a_1 und a_2 der Gruppe A die Bedingung

$$f(a_1 + a_2) = f(a_1) + f(a_2) \tag{1}$$

erfüllt ist, wobei das Zeichen $+$ auf der linken Seite der Gleichung (1) natürlich als Zeichen der Addition in der Gruppe A, hingegen auf der rechten Seite der Gleichung (1) als Zeichen der Addition in der Gruppe B aufgefasst werden muss.

Satz. Ist f eine homomorphe Abbildung einer Gruppe A in eine Gruppe B, so ist die Menge $f(A) \subseteq B$ eine Untergruppe der Gruppe B.

Beweis. Es genügt zu beweisen:
1. Sind B_1 und b_2 Elemente der Menge $f(A)$, so ist $b_1 + b_2$, ebenfalls ein Element der Menge $f(A)$.
2. Das neutrale Element der Gruppe B ist Element der Menge $f(A)$.
3. Ist b ein Element der Menge $f(A)$, so ist $-b$ ebenfalls Element der Menge $f(A)$.

Wir beweisen diese Punkte 1, 2, 3 nacheinander.
1. Es seien b_1 und b_2 zwei Elemente der Menge $f(A)$. Dies bedeutet, dass Elemente a_1 und a_2 der Gruppe A mit $f(a_1) = b_1$ und $f(a_2) = b_2$ existieren.
Da aber die Abbildung f homomorph ist, gilt:

$$f(a_1 + a_2) = b_1 + b_2$$

Danach ist also das dem Element $a_1 + a_2$ der Gruppe A durch die Abbildung f zugeordnete Element $b_1 + b_2$ Element der Menge $f(A)$. Der erste Punkt ist damit bewiesen.

2. Es sei 0 das neutrale und a ein beliebiges Element der Gruppe A. In der Gruppe A gilt $a + 0 = a$, woraus für die Gruppe B folgt:

$$f(a + 0) = f(a)$$

Da die Abbildung f homomorph ist, gilt

$$f(a) + f(0) = f(a)$$

d.h., $f(0)$ ist das neutrale Element der Gruppe B. Das erledigt den zweiten Punkt.

3. Es sei b ein beliebiges Element der Menge $f(A) \subseteq B$. Es existiert ein Element a der Gruppe A mit $f(a) = b$. Wir bezeichnen mit b' das Element $f(-a)$ der Menge $f(A)$ und beweisen, dass $b' = -b$ gilt. Es gilt nämlich

$$a + (-a) = 0 \qquad \text{also gilt} \qquad f(a) + f(-a) = 0'$$

(0' bezeichnet das neutrale Element der Gruppe B), also

$$b + b' = 0' \qquad \text{d.h.} \qquad b' = -b$$

was zu beweisen war.

Somit ist jede homomorphe Abbildung einer Gruppe A in eine Gruppe B eine homomorphe Abbildung der Gruppe A auf eine gewisse Untergruppe der Gruppe B.

Bemerkung I. In den eben durchgeführten Überlegungen ist der Beweis zweier wichtiger Aussagen enthalten, die für jede homomorphe Abbildung einer Gruppe A in eine Gruppe B gelten:

$$f(0) = 0' \qquad \text{und} \qquad f(-a) = -f(a) \tag{2,3}$$

Bemerkung II. Im Hinblick auf die grundlegende Bemerkung in Kap.III, § 2 können wir sagen: Eine eineindeutige homomorphe Abbildung einer Gruppe A auf eine Gruppe B ist eine isomorphe Abbildung.

Definition. Sei f eine homomorphe Abbildung einer Gruppe A in eine Gruppe B. Die Menge aller Elemente x der Gruppe A, die durch f auf das neutrale Element der Gruppe B abgebildet werden, heißt Kern der homomorphen Abbildung f und wird mit $f^{-1}(0')$ bezeichnet.

Satz. Der Kern einer homomorphen Abbildung f der Gruppe A in eine Gruppe B ist eine invariante Untergruppe der Gruppe A.

Beweis. Aus der Definition der homomorphen Abbildung ergibt sich: Aus

$$f(a_1) = 0', \quad f(a_2) = 0' \qquad \text{folgt} \qquad f(a_1 + a_2) = 0'$$

Sind also a_1 und a_2 Elemente von $f^{-1}(0')$, so ist auch $a_1 + a_2$ Element von $f^{-1}(0')$.

Weiter haben wir beim Beweis des vorigen Satzes gesehen, dass $f(0)$ das neutrale Element der Gruppe B ist; also 0 ist Element von $f^{-1}(0')$.
Ist schließlich $f(a) = 0'$, so ist $f(-a) = -f(a) = 0'$; mit a ist auch $-a$ Element von $f^{-1}(0')$. Daraus folgt bereits, dass $f^{-1}(0')$ eine Untergruppe der Gruppe A ist.

Um zu beweisen, dass $f^{-1}(0')$ eine invariante Untergruppe der Gruppe A ist, müssen wir uns davon überzeugen, dass die Transformierte $-a+x+a$ eines beliebigen Elementes x der Gruppe $f^{-1}(0')$ mittels eines beliebigen Elementen a der Gruppe A wieder Element der Gruppe $f^{-1}(0')$ ist. Mit anderen Worten, man muss sich davon überzeugen, dass

$$f(-a + x + a) = 0'$$

gilt, sobald $f(x) = 0'$ ist. Dies ist aber sofort einzusehen, denn für $f(x) = 0'$ gilt:

$$f(-a + x + a) = -f(a) + f(x) + f(a) = -f(a) + 0' + f(a) = -f(a) + f(a) = 0'$$

Damit ist dieser Satz vollständig bewiesen.
Wir werden später sehen, dass auch umgekehrt jede invariante Untergruppe einer Gruppe A Kern einer gewissen homomorphen Abbildung der Gruppe A ist.

7.2 Beispiele homomorpher Abbildungen

I. Wir betrachten die Gruppe G aller ganzen Zahlen

$$..., -n, -(n-1), ..., -2, -1, 0, 1, 2, ..., (n-1, n, ...$$

und eine Gruppe G_2 der Ordnung zwei, deren Elemente b_0 und b_1 seien, und deren Additionstabelle lauten möge:

$$b_0 + b_0 = b0, \quad b_0 + b_1 = b1 + b_0 = b_1, \quad b_1 + b_1 = b0,$$

Offensichtlich ist b_0 das neutrale Element der Gruppe G_2.
Wir konstruieren jetzt folgende Abbildung f der Gruppe G auf die Gruppe G_2:

Jeder geraden Zahl ordnen wir das Element b_0 der Gruppe G_2, und jeder ungeraden Zahl das Element b_1 der Gruppe G_2 zu. Diese Abbildung ist homomorph.
Seien nämlich a und a' zwei ganze Zahlen. Sind a und a' beide gerade Zahlen, so ist $a + a'$ ebenfalls gerade, und es gilt

$$f(a + a') = f(a) = f(a') = b_0 = f(a) + f(a')$$

Ist eine der beiden Zahlen a und a', etwa a, gerade, hingegen die andere ungerade, so ist $a+a'$ ungerade, so dass

$$f(a) = b_0, \quad f(a') = b_1 \qquad , \qquad f(a + a') = b_1 = b_0 + b_1 = f(a) + f(a')$$

gilt.
Sind schließlich a und a' ungerade Zahlen, so ist $a + a'$ eine gerade Zahl, und es gilt

$$f(a) = f(a') = b_1, \qquad f(a + a') = b_0 = b_1 + b_1 = f(a) + f(a')$$

Der Kern unseres Homomorphismus ist offensichtlich die Gruppe aller geraden Zahlen.
Wir verallgemeinern dieses Beispiel. Es sei eine beliebige natürliche Zahl $m \geq 2$ gegeben. Wir betrachten die zyklische Gruppe G_m der Ordnung m mit den Elementen b_0, b_1, b_2, ..., b_{m-1} und der Additionstafel

	b_0	b_1	b_2	...	b_{m-2}	b_{m-1}
b_0	b_0	b_1	b_2	...	b_{m-2}	b_{m-1}
b_1	b_1	b_2	b_3	...	b_{m-1}	b_0
b_2	b_2	b_3	b_4	...	b_0	b_1
...	...	...	...	...	...	...
b_{m-2}	b_{m-2}	b_{m-1}	b_0	...	b_{m-4}	b_{m-3}
b_{m-1}	b_{m-1}	b_0	b_1	...	b_{m-3}	b_{m-2}

(das neutrale Element ist mit b_0 bezeichnet).

Wir konstruieren jetzt eine homomorphe Abbildung] der Gruppe G aller ganzen Zahlen auf die Gruppe G_M.
Dazu erinnern wir vorher an folgenden arithmetischen Satz:
Jede ganze Zahl a liefert bei Division durch eine natürliche Zahl m als Rest eine der Zahlen $0, 1, ..., m-1$. Dabei in der Rest der Zahl a als die eindeutig bestimmte nichtnegative Zahl r definiert, die den Bedingungen

$$a = mq + r, \qquad 0 \leq r \leq m - 1 \tag{1}$$

genügt, wobei q ganz ist (q heißt Quotient bei Division von a durch m). Dieser Satz ist natürlich allgemein für positives a bekannt.
Für $a = 0$ gilt offensichtlich $0 = m \cdot 0 + 0$ bei der Division von Null durch eine beliebige natürliche Zahl erhält man sowohl für den Quotienten als auch für den Rest Null.
Der Fall eines negativen a erfordert vielleicht doch einige Erläuterungen. Ist a negativ, so ist $-a$ positiv.

Wir dividieren die natürliche Zahl $-a$ durch die natürliche Zahl m, bezeichnen den Quotienten mit q' und den Rest mit r'. Wir können annehmen, r' sei positiv (wäre $r' = 0$, so wäre $-a$ und folglich auch a ohne Rest durch m teilbar). Also gilt

$$-a = mq' + r', \qquad 0 < r' \leq m - 1 \qquad \text{und somit}$$

$$a = -mq' - r' = -m - mq' + m - r' = m(-1 - q') + (m - r')$$

Aus $0 < r' \leq m - 1$ folgt offensichtlich $0 < m - r' \leq m - 1$.
Setzt man $q = -1 - q'$, $r = m - r'$, so gilt für die ganzen Zahlen 0, q, r die Beziehung

$$a = mq + r, \qquad 0 \leq r' \leq m - 1 \tag{2}$$

Man überzeugt sich leicht davon, dass die Darstellung der ganzen Zahlen a nach Gleichung (2) für vorgegebenes natürliches m und ganze q und r mit $0 \leq r \leq m - 1$ eindeutig ist, also die ganzen Zahlen q und r durch die Bedingungen (2) vollständig definiert sind.

Es sei nämlich auch

$$a = mq_1 + r_1, \qquad 0 \leq r_1 \leq m - 1 \tag{2'}$$

Dann subtrahieren wir die Gleichung (2') gliedweise von der Gleichung (2) und erhalten:

$$0 = m(q - q_1) + (r - r_1) \qquad \text{d.h.} \qquad r - r_1 = m(q_1 - q)$$

Daraus folgt, dass die ganze Zahl $r - r_1$ ohne Rest durch m teilbar ist. Es ist aber $r - r_1$ die Differenz zweier nichtnegativer Zahlen, die nicht größer als $m-1$ sind; folglich ist der absolute Betrag dieser Differenz ebenfalls nicht größer als $m - 1$. Daher kann die Zahl $r - r_1$ nur dann ohne Rest durch m teilbar sein, wenn sie gleich Null ist. Also gilt

$$r - r_1 = 0, \quad r = r_1 \qquad \text{und} \qquad a = mq_1 + r \tag{3}$$

Aus den Gleichungen (3) und (2) erhalten wir:

$$q_1 = \frac{a - r}{m}, \qquad q = \frac{a - r}{m}, \qquad q = q_1$$

was zu beweisen war.

Wegen der Ungleichung $0 \leq r \leq m - 1$ entspricht der ganzen Zahl r das Element b_r der Untergruppe G_m. Also entspricht jeder ganzen Zahl a für eine festgewählte natürliche Zahl in $m \geq 2$ ein eindeutig bestimmtes Element der zyklischen Gruppe G_m der Ordnung m, nämlich das Element b_r, wobei r der Rest bei der Division von a durch m ist. Dieses Element b_r nennen wir Rest der Zahl a modulo m.

Durch die eben angegebene Relation ist auch eine Abbildung f der Gruppe G auf die Gruppe G_m hergestellt. Wir beweisen, dass diese Abbildung f homomorph ist.

Es seien a und a' zwei ganze Zahlen und es sei

$$a = mq + r, \quad 0 \leq r \leq m-1 \qquad , \qquad a' = mq' + r', \quad 0 \leq r' \leq m-1 \tag{4}$$

Dann gilt

$$a + a' = m(q + q') + r + r'$$

Nun braucht aber $r + r'$, das natürlich der Ungleichung $0 \leq r + r'$ genügt, die Ungleichung $r + r' \leq m - 1$ nicht zu erfüllen. Sicher aber gilt

$$r + r' = mq'' + \rho$$

wobei q'' der Quotient bei Division von $r + r'$ durch m (er ist, wie man leicht sieht, gleich 0 oder 1) und ρ der Rest bei dieser Division ist; daher gilt

$$a + a' = m(q + q' + q'') + \rho, \qquad 0 \leq \rho \leq m - 1$$

Also entspricht dem Element $a + a'$ bei unserer Abbildung f das Element b_ρ der Gruppe G_m: Betrachtet man die Additionstafel der zyklischen Gruppe der Ordnung m, so sieht man, dass

$$b_r + b_{r'} = b_\rho$$

gilt (wobei ρ wie früher der Rest bei der Division von $r + r'$ durch m ist).
Also gilt

$$f(a + a') = b_\rho = b_r + b_{r'} = f(a) + f(a')$$

womit auch bewiesen ist, dass die Abbildung f homomorph ist.

Die soeben durchgeführte Konstruktion der homomorphen Abbildung f der Gruppe aller ganzen Zahlen auf die zyklische Gruppe der Ordnung m ist von grundlegender Bedeutung in der elementaren Zahlentheorie. Wir wollen diese homomorphe Abbildung mit f_M bezeichnen.
Der Kern des Homomorphismus f_m ist die Gruppe aller ganzen Zahlen, die ohne Rest durch m teilbar sind.

II. Es sei A' die Gruppe aller Bewegungen der Ebene in sich. Wir wählen in der Ebene einen bestimmten Punkt O und einen bestimmten von O ausgehenden Strahl h.
Jede Bewegung f der Ebene in sich führt den Strahl h in einen Strahl $f(h)$ über. Der Strahl $f(h)$ schließt mit dem Strahl h einen gewissen Winkel ein[45], den wir mit ω bezeichnen.
Dieser Winkel ist dann und nur dann gleich Null, wenn die Strahlen $f(h)$ und h parallel und gleichgerichtet sind, wenn also die Bewegung f eine Parallelverschiebung ist.

Wir ordnen jetzt einer Bewegung f eine Drehung der Ebene um den Winkel ω_f zu. Auf diese Weise erhält man eine Abbildung der Gruppe aller Bewegungen der Ebene auf die Gruppe aller Drehungen der Ebene um den Punkt O und auf die zu ihr isomorphe Gruppe κ (siehe Kap. V, § 2). Diese Abbildung ist homomorph, wovon sich der Leser leicht überzeugt. Der Kern dieser Abbildung ist die Gruppe aller Parallelverschiebungen der Ebene.

III. In Kap. V, § 2 wurde im zweiten Beispiel gezeigt, dass jeder reellen Zahl ein gewisses Element der Gruppe κ entspricht.
Durch diese Zuordnung wird eine homomorphe Abbildung der Gruppe aller reellen Zahlen auf die Gruppe κ hergestellt, wobei der Kern dieser Abbildung die unendliche zyklische Gruppe ist, welche aus allen reellen Zahlen besteht, die ganzzahlige Vielfache von 2π sind.

[45] Diesen Winkel zwischen dem Strahl h und dem Strahl $f(h)$ erhält man, indem man durch den Punkt O den zu $f(h)$ parallelen und mit ihm gleichgerichteten Strahl zieht.

8 Klasseneinteilung von Gruppen nach einer gegebenen Untergruppe, Restklassengruppen

8.1 Linke und rechte Nebenklassen

Linke Nebenklassen

Es sei eine Gruppe G und darin eine Untergruppe U vorgegeben. Wir stellen uns jetzt die Aufgabe, folgendes zu beweisen:
Die vorgegebene Untergruppe U definiert (und zwar im allgemeinen auf zwei verschiedene Weisen) eine Einteilung der Gruppe G in ein gewisses System paarweise durchschnittsfremder Untermengen, deren eine die Untergruppe U selbst ist, während die übrigen durch ein gewisses höchst einfaches Gesetz eineindeutig auf U abgebildet werden können.

Um diese Einteilung zu erhalten, verfahren wir folgendermaßen:
Wir nennen zwei Elemente a und b der Gruppe G äquivalent bezüglich der Untergruppe U, wenn die linke Differenz der Elemente b und a, also das Element $-a+b$, ein Element der Untergruppe U ist.

Diese Äquivalenz (wir nennen sie linksseitige Äquivalenz) ist symmetrisch. Ist nämlich

$$-a+b=u$$

wobei u ein Element der Gruppe U ist, so ist

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

ebenfalls Element der Untergruppe U.
Diese Äquivalenz ist transitiv. Gilt nämlich

$$-a+b=u_1 \qquad , \qquad -b+c=u_2$$

wobei u_1 und u_2 Elemente der Untergruppe U sind, so ist

$$-a+c=(-a+b)+(-b+c)=u_1+u_2$$

ebenfalls Element der Untergruppe U.
Schließlich ist diese Äquivalenz reflexiv, da

$$-a+a=0$$

ein Element der Untergruppe U ist.

Also zerfällt die Gruppe G auf Grund des Satzes III aus § 5 des Anhangs in Klassen von Elementen, die bezüglich der Untergruppe U untereinander äquivalent sind. Diese Klassen heißen linke Nebenklassen der Gruppe G nach der Untergruppe U.
Wir weisen darauf hin, dass die linke Nebenklasse $'K_a$ des Elementes a einer Gruppe G aus allen den Elementen x besteht, die der Bedingung $-a+x=u$ genügen, wobei u Element der Untergruppe U ist, d.h. aus allen Elementen der Form $x=a+u$, wobei u Element der Untergruppe U ist.

Wir bemerken noch: Ist a Element von U (insbesondere $a=0$), so ist $'K_a=U$, da in diesem Falle $a+u$ für beliebiges u aus U Element der Gruppe U ist; und jedes Element u der Gruppe

U kann in der Form $a + u_1$ dargestellt werden, wobei wieder $u_1 = -a + u$ ein Element der Gruppe U bedeutet.
Da jedes Element der Menge $'K_a$ in der Form $a+u$ dargestellt werden kann und für verschiedene Elemente u_1 und u_2 der Gruppe U die Elemente $a+u_1$ und $a+u_2$, der Menge $'K_a$ verschieden sind, so erhalten wir eine eineindeutige Zuordnung zwischen U und einem beliebigen $'K_a$, wenn wir jedem Element u der Gruppe U das Element $a + u$ der Klasse $'K_a$ zuordnen.

Schließlich bemerken wir, dass es unter allen Klassen $'K_a$ nur eine Klasse gibt, die Untergruppe der Gruppe G ist, nämlich U.
Wenn also $'K_a$ Untergruppe ist, so muss das neutrale Element der Gruppe G in $'K_a$ vorkommen. Es ist folglich das gemeinsame Element der Klassen $'K_a$ und U, und daher fällt $'K_a$ mit U zusammen.

2. Der Fall einer endlichen Gruppe G

Wegen der eineindeutigen Zuordnung, die zwischen jedem der $'K_a$ und der Untergruppe U existiert, bestehen bei einer endlichen Gruppe G alle $'K_a$ aus der gleichen Anzahl m von Elementen, wobei m die Ordnung der Gruppe U ist. Ist die Anzahl aller verschiedenen Klassen gleich j und ist n die Ordnung der Gruppe G, so gilt offensichtlich $n = mj$.
Daraus folgt insbesondere die schon früher erwähnte Tatsache (Kap. II, § l), nämlich:

Satz von Lagrange. Die Ordnung jeder Untergruppe einer endlichen Gruppe G ist ein Teiler der Gruppenordnung von G.

Die Zahl j, also die Anzahl der linken Nebenklassen[46] der Gruppe G nach der Untergruppe U, heißt Index der Untergruppe U in der Gruppe G.

3. Rechte Nebenklassen

Wir nennen jetzt zwei Elemente a und b äquivalent (rechtsseitige Äquivalenz) bezüglich der Untergruppe U, wenn ihre rechte Differenz $b - a = b + (-a)$ Element der Untergruppe U ist. Man prüft leicht nach, dass diese Äquivalenz symmetrisch, transitiv und reflexiv ist. In der Tat folgt aus

$$b - a = u$$

wobei u Element der Gruppe U ist,

$$a - b = -(b - a) = -u$$

und aus

$$b - a = u_1 \qquad , \qquad c - b = u_2$$

wobei u_1 und u_2 in U liegen, folgt

$$c - a = (c - b) + (b - a) = u_2 + u_1$$

Schließlich gehört $a - a = 0$ zu U.
Die rechtsseitige Äquivalenz definiert eine Einteilung der Gruppe G in rechte Nebenklassen, wobei die rechte Nebenklasse K'_a des gegebenen Elementes a aus allen denjenigen Elementen x besteht, für die $x - a = u$ ein Element der Gruppe U ist, also aus allen Elementen der Form $x = u + a$, wobei u zu U gehört.

[46] Diese Zahl kam auch im Falle einer unendlichen Gruppe endlich sein. So zum Beispiel, wenn G die Gruppe aller ganzen Zahlen und U diejenige Untergruppe von G ist, welche aus allen Zahlen besteht, die ohne Rest durch die ganze Zahl $\mu \geq 2$ teilbar sind.

Gehört a zu U, so fällt die Klasse K'_a mit U zusammen.

Ordnet man jedem Element u der Untergruppe U das Element $u1 + a$ der Klasse K'_a zu, so erhält man eine eineindeutige Zuordnung zwischen U und der Klasse K'_a.
Im Fall einer endlichen Untergruppe U sind auch alle Klassen K'_a nach dieser Untergruppe endlich und bestehen aus der gleichen Anzahl von Elementen wie U selbst. Ist die Gruppe G endlich von der Ordnung n und hat die Untergruppe die Ordnung m, so gilt wie vorhin

$$n = mj$$

wobei j die Anzahl aller verschiedenen rechten Nebenklassen nach der Untergruppe U ist, die daher gleich der Anzahl aller verschiedenen linken Nebenklassen ist.

Also kann der Index einer Untergruppe U bezüglich einer Gruppe G sowohl als Anzahl der linken wie auch als Anzahl der rechten Nebenklassen der Gruppe G nach der Untergruppe U definiert werden:
Er ist gleich dem Quotienten der Gruppenordnung von G durch die Gruppenordnung von U.

4. Das Zusammenfallen der linken Nebenklassen mit den rechten bei einer invarianten Untergruppe

Ganz von selbst erhebt sich jetzt die Frage: In welchem Falle gilt für jedes Element a der Gruppe G

$$'K_a = K'_a$$

Dazu ist offensichtlich notwendig und hinreichend, dass jedes Element der Form $a + u$ gleich einem gewissen $u' + a$ und umgekehrt jedes Element $u + a$ gleich einem gewissen Element $a + u'$ ist (dabei bedeuten immer u, u' Elemente der Untergruppe U).
Beide Bedingungen sind äquivalent; denn die erste Bedingung besagt: Zu jedem a aus G und jedem u aus U kann man ein u' aus U finden, derart dass

$$a + u = u' + a$$

gilt, so dass also

$$a + u + (-a) = u' \qquad \text{d.h.} \qquad -(-a) + U + (-a) = U$$

gilt. Da ein jedes Element der Gruppe G bei passender Wahl des Elementes a in der Form $-a$ dargestellt werden kann, so bedeutet die erste Bedingung einfach:
Die Transformierte der Untergruppe U mittels eines beliebigen Elementes der Gruppe G fällt mit U zusammen, oder: U ist eine invariante Untergruppe der Gruppe G.

Die zweite Bedingung lautet: Zu jedem a aus G und jedem a aus U kann man ein u' aus U finden, derart dass

$$u + a = a + u', \quad \text{also} \quad -a + u + a = u', \quad \text{d.h.} \quad -a + U + a = U$$

gilt.
Somit drückt die zweite Bedingung ebenfalls die Forderung aus, dass U eine invariante Untergruppe der Gruppe G ist.
Somit haben wir bewiesen:

Satz. Es sei U eine Untergruppe einer Gruppe G. Für jedes Element a der Gruppe G fällt die

linke Nebenklasse dieses Elementes bezüglich der Untergruppe U genau dann mit der rechten Nebenklasse desselben Elementes zusammen, wenn U eine invariante Untergruppe der Gruppe G ist.

Da bei einer invarianten Untergruppe U für jedes Element a der Gruppe G

$$'K_a = K'_a$$

gilt, so kann man an Stelle von $'K_a$ und K'_a einfach $K_a =' K_a = K'_a$ schreiben, und diese Menge heißt einfach Nebenklasse des Elementes a bezüglich der invarianten Untergruppe U. Insbesondere stimmen die rechten Nebenklassen mit den linken überein, wenn U eine Untergruppe einer kommutativen Gruppe G ist, da alle Untergruppen einer kommutativen Gruppe Normalteiler sind (Kap. III, § 2, Abschn. 2).

5. Beispiele

I. Es sei G die Gruppe aller ganzen Zahlen und $U \subseteq G$ die Gruppe aller der Zahlen, die ohne Rest durch m teilbar sind.
Ist a eine beliebige ganze Zahl, so besteht K_a aus allen Zahlen der Form $a + mq$ mit ganzem q: Das sind alle die Zahlen, die bei der Division durch m ein und denselben Rest liefern wie die Zahl a. Daher ist die Anzahl der verschiedenen Nebenklassen gleich der Anzahl der verschiedenen bei der Division durch m auftretenden Reste. Deren Anzahl aber ist m, da als Rest bei der Division durch m die Zahlen $0, 1, 2, ..., m-1$ und nur sie auftreten. Also gibt es folgende Nebenklassen:

0) die Klasse aller Zahlen, die bei der Division durch in den Rest 0 liefern. Sie fällt mit der Gruppe U zusammen und besteht aus den Zahlen

$$..., -qm, -(q-1)m, ..., -3m, -2m, -m, 0, m, 2m, 3m, ..., qm, ...$$

1) Die Klasse aller Zahlen, die bei der Division durch m den Rest 1 liefern. Diese sind

$$..., -qm+1, -(q-1)m+1, ..., -3m+1, -2m+1, -m+1, 1, m+1, 2m+1, 3m+1, ..., qm+1, ...$$

2) Die Klasse aller Zahlen, die bei der Division durch m den Rest 2 liefern. Dies sind die Zahlen

$$..., -qm+2, -(q-1)m+2, ..., -3m+2, -2m+2, -m+2, 2, m+2, ..., qm+2, ...$$

... ...
$m-1$) Die Klasse aller Zahlen, die bei der Division durch in den Rest $(m-1)$ liefern. Diese Klasse besteht aus den Zahlen

$$..., -qm+(m-1), -(q-1)m+(m-1), ..., -3m+(m-1), -2m+(m-1),$$
$$-m+(m-1), (m-1), m+(m-1), 2m+(m-1), ..., qm+(m-1), ...$$

oder, was dasselbe ist, aus den Zahlen

$$..., -2m-1, -m-1, -1, m-1, 2m-1, 3m-1, ...$$

II. Es sei G die Gruppe S_3 aller Permutationen von drei Elementen und U die Untergruppe der Ordnung 2 (und folglich vom Index 3), die aus den folgenden Permutationen besteht:

$$P_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \text{und} \quad P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Die Einteilung der Gruppe G in linke und rechte Nebenklassen ist aus folgender Tabelle ersichtlich:

Linke Nebenklassen	Rechte Nebenklassen
$U = (P_0, P_2)$	$U = (P_0, P_2)$
(P_1, P_3)	(P_1, P_4)
(P_4, P_5)	(P_3, P_5)

III. Die alternierende Permutationsgruppe A_n von n Elementen ist selbst eine invariante Untergruppe vom Index 2 der symmetrischen Gruppe S_n. Die zwei Klassen, die zu dieser Untergruppe gehören, sind die Gruppe A_n selbst und die Klasse aller ungeraden Permutationen.

IV. In der Drehungsgruppe des n-eckigen Dieders bilden die Kongruenzen erster Art eine invariante Untergruppe vom Index 2. Eine der beiden Klassen nach dieser Untergruppe ist sie selbst, die andere besteht aus allen Kongruenzen zweiter Art.

V. Die Gruppe U aller Verschiebungen einer Geraden in sich ist eine invariante Untergruppe vom Index 2 in der Gruppe G aller Kongruenzen der Geraden. Die beiden durch diese Untergruppe definierten Klassen sind die Gruppe U selbst und die Klasse aller Kongruenzen zweiter Art.

VI. Es sei G die Gruppe aller komplexen Zahlen mit der gewöhnlichen Addition als Gruppenoperation. Es sei U die Untergruppe aller reellen Zahlen. Die Klassen, nach denen die kommutative Gruppe G bezüglich ihrer Untergruppe U zerfällt, sind Mengen K_β deren jede aus allen komplexen Zahlen der Form

$$x + i\beta$$

besteht, wobei x und β reelle Zahlen sind, β vorgegeben ist und x alle reellen Zahlen durchläuft. Werden wie gewöhnlich die komplexen Zahlen als Punkte der Ebene dargestellt[47], so erscheint jede Klasse als eine zur reellen Achse (also zur Abszissenachse) parallele Gerade.

8.2 Die Restklassengruppe zu einer vorgegebenen invarianten Untergruppe

1. Definition

Es sei U eine invariante Untergruppe einer gewissen gegebenen Gruppe G. Wir betrachten die Menge aller Klassen, in die die Gruppe G bezüglich der Untergruppe U zerfällt.
Diese Menge bezeichnen wir mit V und beweisen, dass man in ihr eine Addition so definieren kann, dass V zu einer Gruppe wird, auf die die Gruppe G homomorph abgebildet werden kann.

Es seien v_1 und v_2 zwei willkürliche Elemente der Gruppe V. Dann bestimmen v_1 und v_2 zwei Klassen der Gruppe G nach der invarianten Untergruppe U.
Wir wählen in jeder dieser Klassen ein bestimmtes Element, etwa ein Element x_1 aus der Klasse v_1 und ein Element x_2 aus der Klasse v_2. Mit v_3 bezeichnen wir die Klasse, in der das Element $x_1 + x_2$ der Gruppe G liegt.

Wir beweisen, dass die Klasse v_3 nicht davon abhängt, welche Elemente x_1 und x_2 aus den Klassen v_1 und v_2 gewählt worden sind. Mit anderen Worten, wir beweisen:
Ist x_1' irgendein Element der Klasse v_1 das im allgemeinen von x_1 verschieden ist, und ist x_2' irgendein Element der Klasse v_2 das im allgemeinen von x_2 verschieden ist, so liegt das Element $x_1' + x_2'$ in der gleichen Klasse v_3 in der $x_1 + x_2$ liegt.

[47] Dabei gilt als Darstellung der komplexen Zahl $x + iy$ der Punkt der Ebene mit den Koordinaten x und y.

Tatsächlich gehören zwei Elemente a und b dann und nur dann zu ein und derselben Klasse bezüglich der invarianten Untergruppe U, wenn ihre Differenz zu U gehört.
Wir betrachten die Differenz

$$(x_1 + x_2) - (x_1' + x_2') = x_1 + x_2 - x_2' - x_1' = x_1 + (x_2 - x_2') - x_1'$$

Da x_2 und x_2' zu ein und derselben Klasse v_2 gehören, so ist

$$x_2 - x_2' = u_2$$

wobei u_2 ein gewisses Element von U ist; es gilt dann

$$(x_1 + x_2) - (x_1' + x_2') = x_1 + x_2 - x_2' - x_1' = x_1 + u_2 - x_1' \tag{1}$$

Nun ist U aber eine invariante Untergruppe, daher ist

$$x_1 + u_2 = u' + x_1$$

wobei u' ein geeignetes Element der Gruppe U ist. Setzt man dies in Formel (1) ein, so erhält man

$$(x_1 + x_2) - (x_1' + x_2') = u' + x_1 - x_1'$$

Nun gehören x_1 und x_1' ein und derselben Klasse v_1 an, daher ist $x_1 - x_1' = u_1$, wobei u_1 ein gewisses Element der Gruppe U ist. Folglich gilt

$$(x_1 + x_2) - (x_1' + x_2') = u' + u_1$$

d.h., $(x_1 + x_2) - (x_1' + x_2')$ ist ein Element $u = u' + u_1$ der Gruppe U, was zu beweisen war.

Da die so erhaltene Klasse v_3 definiert ist, sobald die Klassen v_1 und v_2 definiert sind, so erhalten wir:

$$v_1 + v_2 = v_3 \tag{2}$$

Dies ist die Definition der Summe $v_1 + v_2$ zweier Klassen v_1 und v_2.
Also:

Summe zweier Nebenklassen v_1 und v_2 heißt diejenige Nebenklasse v_3, die nach folgender Regel gebildet ist: In jeder der Klassen v_1 und v_2 wählen wir ein willkürliches Element, addieren diese beiden Elemente und nehmen die Klasse, zu der ihre Summe gehört. Diese ist dann die Klasse v_3.

Aus dieser Definition und daraus, dass die Addition der Elemente in der Gruppe G dem assoziativen Gesetz genügt, folgt unmittelbar, dass auch die Addition von Klassen dem assoziativen Gesetz genügt.
Wir beweisen, dass die Klasse U in bezug auf die eben definierte Addition die Rolle des neutralen Elementes spielt, dass also für jede Klasse 0 folgende Gleichung gilt:

$$v + U = U + v = v \tag{3}$$

Dazu wählen wir ein willkürliches Element x der Klasse v und als Element der Klasse U das neutrale Element 0. Dann ist nach Definition der Addition die Klasse $v + U$ die Klasse, die das Element $x + 0 = x$ enthält, also dieselbe Klasse v.
Ebenso ist die Klasse $U + v$ die Klasse, die das Element $0 + x = x$ enthält, also dieselbe Klasse v. Damit ist die Formel (3) bewiesen.

Endlich beweisen wir, dass es zu jeder Klasse K eine bestimmte entgegengesetzte Klasse gibt, die wir mit $-K$ bezeichnen und die die Bedingung

$$K + (-K) = (-K) + K = U$$

erfüllt.
Dazu wählen wir in der Klasse K irgendein Element a und definieren die Klasse $-K$ als die Klasse, die das Element $-a$ enthält.
Nach Definition der Addition von Klassen stellt jede der beiden Summen $K + (-K)$ und $(-K) + K$ die Klasse der, die das Element $a + (-a) = (-a) + a = 0$ enthält, und dies ist die Klasse U.

Also erfüllt die von uns definierte Addition alle Axiome des Gruppenbegriffs. Folglich ist bei unserer Definition der Addition die Menge der Klassen der Gruppe G nach einer ihrer invarianten Untergruppen U eine gewisse Gruppe V. Die Klasse U ist dabei das neutrale Element der Gruppe V.

Die Gruppe V heißt Restklassengruppe der Gruppe G bezüglich ihrer invarianten Untergruppe U (sie wird bei multiplikativer Schreibweise Faktorgruppe genannt und mit G/U bezeichnet).

2. Der Homomorphiesatz

Es sei wie früher eine Gruppe G und eine ihrer invarianten Untergruppen U gegeben. Jedem Element x der Gruppe G ordnen wir ein bestimmtes Element der Restklassengruppe V zu, nämlich die Klasse, die das Element x enthält.
Aus der so hergestellten Abbildung ϕ der Gruppe G auf die Gruppe V und aus der Definition der Addition in der Gruppe V folgt unmittelbar, dass diese Abbildung homomorph ist. 2. Der Homomorphiesatz Welche Elemente der Gruppe G werden auf das neutrale Element der Gruppe V abgebildet?
Da dieses neutrale Element U ist, so lautet die offensichtliche Antwort auf unsere Frage: Alle Elemente der invarianten Untergruppe U und nur sie werden durch die Abbildung ϕ auf das neutrale Element der Gruppe V abgebildet.

Aus den Überlegungen dieses und des vorhergehenden Artikels folgt: Jede invariante Untergruppe U der Gruppe G ist Kern einer gewissen homomorphen Abbildung der Gruppe G, nämlich der homomorphen Abbildung der Gruppe G auf ihre Restklassengruppe bezüglich U.

Es sei jetzt eine willkürliche homomorphe Abbildung f irgendeiner Gruppe A auf irgendeine Gruppe B vorgelegt. Es sei U der Kern dieser homomorphen Abbildung. Wir wissen, dass U eine invariante Untergruppe der Gruppe A ist. Die Restklassengruppe der Gruppe A in bezug auf U bezeichnen wir mit V.
Es sei b irgendein Element der Gruppe B. Dann existiert wenigstens ein Element a der Gruppe A, das durch die Abbildung f auf das Element b abgebildet wird:

$$b = f(a)$$

Wir wollen das volle Urbild des Elementes b bei der Abbildung f bestimmen, d.h. die Menge aller Elemente x der Gruppe A, die durch die Abbildung f auf b abgebildet werden. Dieses volle Urbild bezeichnen wir wie üblich mit $f^{-1}(b)$.
Also ist $f^{-1}(b)$ nach Definition die Menge aller Elemente x der Gruppe A, für die die Gleichung

$$f(x) = b$$

gilt.
Es sei, wie bereits gesagt, a ein beliebiges Element, das auf b abgebildet wird. Ist x ein anderes Element der Menge $f^{-1}(b)$, so gilt

$$f(a) = b, \quad f(x) = b, \quad f(-a) = -b, \quad f[x + (-a)] = b + (-b) = 0$$

(die Null rechts ist das neutrale Element der Gruppe B), und dies bedeutet, dass $x + (-a)$ ein gewisses Element u der Gruppe U, also $x = a + u$ Element derselben Klasse nach der invarianten Untergruppe U ist, zu der a gehört. Liegen umgekehrt a und x in einer Klasse, so gilt

$$x = a + u \qquad , \qquad f(x) = f(a) + f(u) = f(a) + 0 = f(a)$$

d.h., a und x werden auf ein und dasselbe Element b der Gruppe B abgebildet oder, mit anderen Worten: sie sind in demselben vollen Urbild $f^{-1}(b)$ enthalten.

Also sind die vollen Urbilder $f^{-1}(b)$ der Elemente der Gruppe B die Nebenklassen der Gruppe A nach der invarianten Untergruppe U.
Dadurch wird eine eineindeutige Zuordnung ψ zwischen der Gruppe B und der Gruppe V hergestellt.

Jedem Element der Gruppe V, das eine gewisse Klasse der Gruppe A nach der invarianten Untergruppe U, also volles Urbild eines gewissen Elementes der Gruppe B ist, entspricht eben dieses Element b der Gruppe B. Dabei ist jedes Element b der Gruppe B einer einzigen Klasse, d.h. einem einzigen Element der Gruppe V zugeordnet, nämlich der Klasse, die volles Urbild des Elementes b ist. Die Abbildung ψ ist homomorph:

Es seien v_1 und v_2 zwei Elemente der Gruppe V und

$$v_1 + v_2 = v_3 \tag{1}$$

Es sei a_1 ein beliebiges Element der Klasse v_1, a_2 ein beliebiges Element der Klasse v_2 und $a_3 = a_1 + a_2$.
Wir wissen, dass dann a_3 zu v_3 gehört.
Wir setzen

$$f(a_1) = b_1, \qquad f(a_2) = b_2, \qquad f(a_3) = b_3$$

Da f ein Homomorphismus ist, gilt

$$b_1 + b_2 = b_3 \tag{2}$$

Da aber v_1, v_2, v_3 die entsprechenden vollen Urbilder der Elemente b_1, b_2, b_3 sind, so ist

$$\psi(v_1) = b_1, \qquad \psi(v_2) = b_2, \qquad \psi(v_3) = b_3$$

so dass die Gleichung (2) in folgender Form geschrieben werden kann :

$$\psi(v_1) + \psi(v_2) = \psi(v_3)$$

Damit haben wir bewiesen, dass die Abbildung ψ homomorph ist. Wegen der Eineindeutigkeit der homomorphen Abbildung der Gruppe V auf die Gruppe B ist die Abbildung ψ eine isomorphe Abbildung von V auf B.
Das Endergebnis aller Überlegungen ist der folgende Satz.

Homomorphiesatz. Jede homomorphe Abbildung einer Gruppe A auf eine andere Gruppe B hat als Kern eine gewisse invariante Untergruppe der Gruppe A.

Umgekehrt ist jede invariante Untergruppe U der Gruppe A Kern einer gewissen homomorphen Abbildung ϕ der Gruppe A auf die Restklassengruppe V der Gruppe A bezüglich U.
Die Abbildung ψ erhält man, wenn man jedem Element der Gruppe A seine Klasse bezüglich der invarianten Untergruppe U zuordnet.
Ist f eine beliebige homomorphe Abbildung der Gruppe A auf die Gruppe B, so sind die vollen Urbilder der Elemente der Gruppe B bei dieser Abbildung die Klassen der Gruppe A nach dem Kern U der Abbildung f und die Gruppe B ist isomorph der Restklassengruppe der Gruppe A bezüglich U.

Also fallen die invarianten Untergruppen einer vorgegebenen Gruppe A mit den Kernen aller möglichen homomorphen Abbildungen dieser Gruppe zusammen. Alle zur Gruppe Ahomomorphen Gruppen fallen mit den Gruppen zusammen, die den Restklassengruppen der Gruppe A bezüglich aller möglichen ihrer invarianten Untergruppen isomorph sind.[48]

Korrolar. Eine homomorphe Abbildung einer Gruppe A auf eine Gruppe B ist genau dann ein Isomorphismus, wenn der Kern dieser Abbildung nur aus dem neutralen Element der Gruppe A besteht.

[48] Dem Leser bleibt es überlassen, unter dem Gesichtspunkt den eben bewiesenen Homomorphiesatzes die früher behandelten Beispiele invarianter Untergruppen und homomorpher Abbildungen nochmals zu durchdenken und die Restklassengruppen nach ihnen zu bestimmen.

9 Anhang Elementare Begriffe der Mengenlehre

Die wichtigsten Begriffe der Mengenlehre, von denen in diesem Anhang die Rede ist und die man fortwährend in der Mathematik anwendet, sind in erster Linie die Begriffe Menge, Abbildung, Einteilung in Klassen sowie die elementaren Mengenoperationen, nämlich die Bildung von Vereinigung und Durchschnitt mehrerer (manchmal unendlich vieler) Mengen.

9.1 Der Begriff der Menge

Die Begriffe Menge und Abbildung gehören zu den mathematischen Begriffen, die sich nicht auf einfachere Begriffe zurückführen lassen und daher nicht logisch definiert werden können. Daher spricht man nur von einer Erklärung der Bedeutung dieser Begriffe.

Im alltäglichen Leben sowie auch in jeder wissenschaftlichen Überlegung benutzen wir fortwährend den Begriff Menge, oder wie man manchmal sagt, Gesamtheit:
Man kann von einer Menge oder einer Gesamtheit von Gegenständen sprechen, die sich in einem gegebenen Augenblick in einem gegebenen Zimmer befinden, von der Menge oder Gesamtheit der Personen, die im Hörsaal oder im Konzertsaal anwesend sind, von der Menge oder Gesamtheit der Bäume, die in einem bestimmten Garten wachsen, von der Menge der Bücher, aus denen eine bestimmte Bibliothek besteht, von der Menge der Sterne, die die Milchstraße bilden usw.

Man kann ferner von der Menge der Moleküle sprechen, die in einem Volumen eines gegebenen Stoffes enthalten sind, oder von der Menge der Zellen eines lebenden Organismus.
Wenn wir sagen: eine Schar Gänse, ein Sack Kartoffeln, ein Korb Äpfel, so sind dies vom mathematischen Gesichtspunkt aus Mengen:
Gänse, die die vorgegebene Schar bilden, Kartoffeln oder Äpfel, die sich in einem Sack oder Korb befinden.

Die angeführten Beispiele sind Beispiele endlicher Mengen: Alle angegebenen Mengen bestehen aus einer gewissen endlichen Anzahl von Elementen, die sehr groß sein kann (wie zum Beispiel im Falle der Wassermoleküle, die in einem vorgegebenen Volumen Wasser enthalten sind), die aber jedenfalls endlich ist.

Es treten aber auch unendliche Mengen auf. Solche sind zum Beispiel die Menge aller natürlichen (also aller ganzen, positiven) Zahlen, die Menge aller Geraden, die (in der Ebene oder im Raume) durch einen vorgegebenen Punkt hindurchgehen; die Menge aller Kreise, die durch zwei gegebene Punkte, die Menge aller Ebenen, die durch eine vorgegebene Gerade hindurchgehen, usw.

Die Mengenlehre widmet sich vor allem der Untersuchung der unendlichen Mengen.
Die Theorie der endlichen Mengen bezeichnet man oft auch als Kombinatorik.

Die einfachen Eigenschaften der Mengen, über die wir hier sprechen wollen, erstrecken sich fast immer gleichermaßen sowohl auf endliche als auch auf unendliche Mengen.

Wir weisen noch auf folgendes hin: In der Mathematik ist es durchaus gerechtfertigt, Mengen zu betrachten, deren Elementanzahl gleich Eins ist, sowie auch diejenige Menge, die überhaupt keine Elemente enthält (die "leere" Menge).
Nehmen wir einmal an, dass wir allgemein von einer Menge von Kreisen sprechen, die durch gewisse gegebene Punkte hindurchgehen.

Ist die Anzahl dieser Punkte gleich Zwei, so ist die Menge der durch sie hindurchgehenden Kreise unendlich. Sind es jedoch drei derartige Punkte, so gibt es (falls die drei Punkte nicht in einer Geraden liegen) nur einen durch sie hindurchgehenden Kreis.
Mit anderen Worten: die Menge der Kreise, die durch drei Punkte hindurchgehen, besteht aus einem Element. Die Menge der Kreise aber, die durch drei in einer Geraden liegende Punkte hindurchgehen, enthält kein einziges Element. Sie ist die leere Menge, da es solche Kreise überhaupt nicht gibt.

Wir erklären diese Dinge an einem Beispiel aus dem täglichen Leben. Wir nehmen an, dass wir von der Menge der Schüler sprechen, die in einer bestimmten Unterrichtsstunde anwesend sind und deren Alter zwischen 17 und 19 Jahren einschließlich liegt.
Diese Menge ist in dem Sinne vollständig bestimmt, dass wir von jedem der in dieser Unterrichtsstunde anwesenden Schüler auf dem Wege einer einfachen Umfrage erfahren können, ob er zu dieser Menge gehört oder nicht. Dabei wissen wir aber im voraus nicht, wie viele Schüler Elemente unserer Menge sind.
Es können 10, es können 5, es kann einer sein, und es kann in unserer Klasse keinen Schüler dieser Altersklasse geben, dann etwa, wenn alle jünger als 17 Jahre sind. In diesem Fall ist unsere Menge leer; in den vorigen besteht sie aus 10, aus 5 oder aus einem Element.

Mengen, die aus einem Element bestehen, werden in unserem Buche oft vorkommen. Die leere Menge brauchen wir hier nicht näher zu betrachten; ihre Benutzung erweist sich aber in der Mathematik oft als notwendig und vorteilhaft.

9.2 Teilmengen

Wir betrachten die Menge A aller Personen, die in einem bestimmten Hörsaal zugegen sind. Dann sind die Menge der anwesenden Frauen ebenso wie die Menge der im Hörsaal anwesenden Männer Beispiele von Teilmengen der Menge A.

Beispiele anderer Teilmengen der Menge A sind:
Die Teilmenge derjenigen Personen, die noch nicht 20 Jahre alt sind; die Teilmenge der Personen, die noch nicht 30 Jahre alt sind; die Teilmenge, die aus allen Personen besteht, deren Größe zwischen 160 und 170 cm liegt; die Teilmenge aller Personen, die größer als 165 cm sind; die Teilmenge aller in Berlin wohnenden Personen; die Teilmenge aller der Personen, die einen bestimmten Beruf oder eine bestimmte soziale Stellung haben, usw.

Es ist ohne weiteres verständlich, dass gewisse dieser Teilmengen aus einem Element bestehen können; von gewissen anderen kann es sich herausstellen, dass sie überhaupt keine Elemente enthalten.
Es kann aber auch sein, dass irgendeine der angegebenen Teilmengen mit der gesamten Menge A zusammenfällt, zum Beispiel wenn alle im Hörsaal anwesenden Personen Frauen sind oder wenn sie alle noch nicht 30 Jahre alt sind. Es kann außerdem eintreten, dass gewisse dieser Teilmengen zusammenfallen (wenn beispielsweise alle im Hörsaal anwesenden Personen Frauen und diese alle jünger als 30 Jahre sind) oder dass gewisse Teilmengen mit der gesamten Menge A zusammenfallen.

Die allgemeine Definition einer Teilmenge ist die:

Eine Menge B heißt Teilmenge einer Menge A, wenn jedes Element der Menge B gleichzeitig Element der Menge A ist.

Eine Teilmenge der Menge A heißt uneigentlich, wenn sie mit der Menge A zusammenfällt (mit anderen Worten: die Menge A selbst rechnet man zu ihren Teilmengen hinzu und bezeichnet sie als uneigentliche Teilmenge). Ist die Menge B eine Teilmenge der Menge A, so sagen wir auch: B ist in A enthalten oder A enthält B, und schreiben dafür: $B \subseteq A$ oder $A \supseteq B$. Das Zeichen $\subseteq$ nennen wir Inklusionszeichen. Die leere Menge ist Teilmenge jeder Menge.

Wir geben weitere Beispiele an.
Die Menge aller geraden Zahlen ist Teilmenge der Menge aller ganzen Zahlen. Die Menge aller ganzen Zahlen ist Teilmenge der Menge aller rationalen Zahlen.

9.3 Mengenoperationen

1. Die Vereinigung von Mengen

Wir kehren jetzt zu dem Beispiel zurück, das wir am Anfang des vorigen Paragraphen betrachtet haben.
Unter allen Personen, die in einem gegebenen Hörsaal anwesend sind, betrachten wir die Menge M aller der Personen, die wenigstens einer der folgenden Bedingungen genügen

1. Sie sind jünger als 20 Jahre;
2. sie sind größer als 165 cm.

Mit anderen Worten: in unsere Menge M gehen alle die Personen ein, die weniger als 20 Jahre alt sind (unabhängig von ihrer Größe) und auch alle die Personen, die größer als 165 cm sind (unabhängig von ihrem Alter). Die Menge M heißt die Vereinigung der beiden Mengen: Der Menge M_1 aller Anwesenden, die jünger als 20 Jahre, und der Menge M_2 aller Anwesenden, die größer als 165 cm sind.

Die allgemeine Definition der Vereinigung zweier Mengen A und B lautet:
Als Vereinigung der Mengen A und B bezeichnet man die Menge; die aus allen Elementen der Menge A und aus allen Elementen der Menge B besteht.

Bemerkung. Aus dem eben angeführten Beispiel erkennt man, dass man Mengen auch dann vereinigen kann, wenn sie gemeinsame Elemente haben. Es kommt natürlich vor, dass die Mengen M_1 und M_2 gemeinsame Elemente besitzen, dass es also in unserem Hörsaal Personen gibt, die jünger als 20 Jahre und gleichzeitig größer als 165 cm sind.
Wir bemerken insbesondere: Ist die Menge B Teilmenge der Menge A, so fällt die Vereinigung der Mengen B und A mit der Menge A zusammen. Besteht beispielsweise die Menge A aus allen im Hörsaal befindlichen Personen, die noch nicht 30 Jahre alt, und die Menge B aus allen den Anwesenden, die jünger als 20 Jahre sind, so fällt die Vereinigung der Mengen A und B offensichtlich mit der Menge A zusammen.

Ganz entsprechend definiert man die Vereinigung von drei, von vier usw. Mengen. Man kann auch die Vereinigung unendlich vieler Mengen definieren. Alles dies ist in folgender Definition zusammengefasst:

Es sei eine beliebige endliche oder unendliche Gesamtheit von Mengen gegeben. Als Vereinigung der Mengen der gegebenen Gesamtheit bezeichnet man die Menge aller Elemente, die in wenigstens einer der der Gesamtheit angehörenden Mengen liegen.

Es sei zum Beispiel A_k die Menge aller regelmäßigen k-Ecke der Ebene (mit $k = 3, 4, 5, ...$), also A_3 die Menge aller gleichseitigen Dreiecke, A_4 die Menge aller Quadrate usw.

Die Menge aller regelmäßigen Vielecke ist die Vereinigung der Mengen A_3, A_4, A_5, ..., A_k, ...

Wir bezeichnen mit B_k ($k = 3, 4, 5, ...$) die Menge aller regelmäßigen Vielecke, deren Seitenanzahl k nicht überschreitet. Dann ist B_k die Vereinigung der Mengen B_3, B_4 ..., B_{k-1}, B_k und die Menge aller regelmäßigen Vielecke ist die Vereinigung der Mengen B_k, $k = 3, 4, 5, ...$ Weiter ist offensichtlich $A_3 = B_3$ und

$$B_3 \subseteq B_4 \subseteq B_5 \subseteq ... \subseteq B_k \subseteq B_{k+1} \subseteq ...$$

Bemerkung. Die Vereinigung von Mengen wird auch manchmal ihre Summe genannt.

2. Der Durchschnitt von Mengen

Es sei M_1 die Menge der in einem Hörsaal anwesenden Personen, die jünger als 20 Jahre sind, und M_2 die Menge der im Hörsaal anwesenden Personen, die größer als 165 cm sind.
Unter dem Durchschnitt der Mengen M_1 und M_2 versteht man die Menge der Elemente, die sowohl zur Menge M_1 als auch zur Menge M_2 gehören, also in unserem Beispiel die Menge aller der Anwesenden, die jünger als 20 Jahre und gleichzeitig größer als 165 cm sind. Natürlich kann diese Menge auch leer sein.

Allgemein nennt man Durchschnitt der Mengen einer gegebenen (endlichen oder unendlichen) Gesamtheit die Menge, die aus den Elementen besteht, die allen Mengen der gegebenen Gesamtheit angehören.
Wir bemerken: Ist $B \subseteq A$, so ist der Durchschnitt der Mengen A und B die Menge B.

Aufgabe. Wir wollen unter Dreieck immer die Menge aller Punkte verstehen, die innerhalb dieses Dreiecks liegen.
Man beweise, dass die Vereinigung aller gleichseitigen Dreiecke, die dem Kreis um 0 mit dem Radius 1 einbeschrieben sind, die Menge aller innerhalb des Kreises liegenden Punkte und der Durchschnitt dieser Dreiecke die Menge aller der Punkte ist, die innerhalb des Kreises um 0 mit dem Radius $\frac{1}{2}$ liegen.
Man formuliere auch die Lösung der analogen Aufgabe für einbeschriebene Quadrate und andere regelmäßige Vielecke sowie für regelmäßige Vielecke, die dem Kreis umbeschrieben sind.

Bemerkung. Der Durchschnitt von Mengen wird auch manchmal ihr Produkt genannt.

9.4 Abbildungen oder Funktionen

Nehmen wir an, eine gewisse Anzahl von Personen ginge ins Theater. Beim Betreten des Theaters geben sie ihre Mäntel usw. ab und erhalten dafür eine Nummer, unter der die Sachen in der Garderobe aufbewahrt werden.

Was interessiert uns mathematisch an dieser allen bekannten Erscheinung?
Was uns interessiert, ist folgende Tatsache:
Jedem Zuschauer des Theaters entspricht (oder ist zugeordnet) ein gewisser Gegenstand, nämlich die Nummer, die dieser Zuschauer in der Garderobe erhalten hat.

Wenn wir in irgendeiner Weise jedem Element a einer gewissen Menge A ein bestimmtes Element b einer gewissen Menge B zuordnen, so sagen wir, die Menge A werde in die Menge B abgebildet oder es sei eine Funktion gegeben, deren Argument die Menge A durchläuft und deren Werte in der Menge B liegen.

Um anzudeuten, dass das gegebene Element b dem Element a zugeordnet ist, schreibt man $b = f(a)$ und sagt, b sei das Bild des Elementes a bei der vorgegebenen Abbildung f oder b sei der Wert der Funktion für den Argumentwert a.

Dabei können verschiedene Fälle eintreten, die wir nun behandeln wollen.
Es kann vorkommen, dass zu einer gegebenen Vorstellung alle Eintrittskarten ausverkauft sind. Dann gibt es gewöhnlich auch in der, Garderobe keinen freien Platz. Nicht nur jeder Zuschauer hat eine Nummer erhalten, sondern es sind auch alle Nummern unter die Zuschauer aufgeteilt. Dieser Fall nimmt in einer allgemeinen mathematischen Untersuchung folgende Gestalt an:

Jedem Element a der Menge A ist ein Element $b = f(a)$ der Menge B zugeordnet, und dabei ist auch jedes Element der Menge B wenigstens einem Element der Menge A zugeordnet.
In diesem Falle bezeichnet man f als Abbildung der Menge A auf die Menge B.

Weshalb betonen wir: Jedes Element der Menge B ist wenigstens einem Element der Menge A zugeordnet?
Weil es eintreten kann, dass verschiedenen Elementen der Menge A ein und dasselbe Element der Menge B zugeordnet sein kann. In unserem speziellen Beispiel bedeutet dies, dass mehrere Personen ihren Mantel unter ein und derselben Nummer zur Aufbewahrung gegeben haben.

Der wichtigste Fall einer Abbildung ist die Abbildung einer Menge auf eine andere. Zu ihm kommt man leicht, indem man vom allgemeinen Fall der Abbildung einer Menge in eine andere ausgeht.
Es sei nämlich eine beliebige Abbildung f der Menge A in die Menge B gegeben. Die Menge aller der Elemente der Menge B, die bei der Abbildung f wenigstens einem Element der Menge A zugeordnet sind, nennen wir Bildmenge von A bei der Abbildung f; wir bezeichnen sie mit $f(A)$.
Es ist offensichtlich, dass die Abbildung f eine Abbildung der Menge A auf die Menge $f(A)$ ist.

Diese Bemerkung gestattet, uns im folgenden auf die Betrachtung von Abbildungen einer Menge auf eine andere zu beschränken.
Im Beispiel der Theaterbesucher ist A die Menge der Zuschauer, die eine bestimmte Vorstellung besuchen, und $f(A)$ die Menge aller besetzten Nummern der Garderobe.

Definition. Es sei eine Abbildung f einer Menge A auf eine Menge B gegeben. Es sei b ein willkürliches Element der Menge B. Die Menge aller Elemente der Menge A, denen bei der Abbildung f das gegebene Element b zugeordnet ist, heißt volles Urbild des Elementes b bei der Abbildung f. Diese Menge bezeichnen wir mit $f^{-1}(b)$.

In unserem Beispiel ist b eine beliebige Nummer in der Garderobe des Theaters. Das volle Urbild eines Elementes b ist die Menge aller der Theaterbesucher, die ihren Mantel unter dieser Nummer b aufgehängt haben.

Wir betrachten jetzt den Fall, dass auf jeder Nummer lediglich ein Mantel aufgehängt ist, dass also das volle Urbild $f^{-1}(b)$ jedes Elementes b der Menge B lediglich aus einem Element der Menge A besteht. In diesem Falle heißt die Abbildung der Menge A auf die Menge B eineindeutig.

Wir geben noch ein Beispiel, das den Begriff der eineindeutigen Abbildung verdeutlicht.
Wir stellen uns eine Kavallerieabteilung vor. Auf jeden Reiter kommt ein Pferd, und auf jedem Pferd sitzt ein Reiter. Damit ist eine eineindeutige Abbildung der Menge aller Reiter auf die

Menge aller Pferde (einer bestimmten Abteilung) und auch die eineindeutige Abbildung der Menge aller Pferde auf die Menge aller Reiter hergestellt (wir sprechen immer von den Reitern und Pferden einer bestimmten Abteilung).

Dieses Beispiel zeigt, dass eine eineindeutige Abbildung einer Menge A auf eine Menge B automatisch eine ebenfalls eineindeutige Abbildung der Menge B auf die Menge A nach sich zieht:
Besteht jede Menge $f^{-1}(b)$, wobei b ein beliebiges Element von B ist, nur aus einem Element a, so erhalten wir die Abbildung f^{-1} der Menge B auf die Menge A, indem wir jedem Element b der Menge B das Element $a = f^{-1}(b)$ der Menge A zuordnen. Die Abbildung f^{-1} bezeichnet man als die zur Abbildung f inverse Abbildung.

Also führt eine eineindeutige Abbildung einer Menge A auf eine Menge B zu folgendem:
Jedes Element a der Menge A vereinigen wir mit einem gewissen eindeutig bestimmten Element $f(a)$ zu einem Paar. Dabei zeigt es sich, dass jedes Element b der Menge B genau einmal, und zwar mit dem zu b eindeutig bestimmten Element a der Menge A gepaart ist. Ordnet man jedem Element b der Menge B das mit ihm gepaarte Element a der Menge A zu, so erhält man eine eineindeutige Abbildung f^{-1} der Menge B auf die Menge A, die zur Abbildung f invers ist.

Somit ist bei einer, eineindeutigen Abbildung einer Menge auf eine andere keine der beiden Mengen bevorzugt, da jede der beiden Mengen eineindeutig auf die andere abgebildet wird. Um diese Gleichberechtigung der beiden Mengen hervorzuheben, spricht man oft von einer eineindeutigen Zuordnung zwischen zwei Mengen und versteht darunter die Gesamtheit der beiden eineindeutigen und zueinander inversen Abbildungen jeder Menge auf die andere.

9.5 Einteilung einer Menge in Teilmengen

1. Mengen von Mengen (Mengensysteme)

Wir können Mengen betrachten, die aus verschiedenen Elementen bestehen. Insbesondere können wir Mengen von Mengen betrachten, also Mengen, deren Elemente selbst Mengen sind.
Wir sind ihnen bereits begegnet, als wir die Definition der Vereinigung und des Durchschnitts von Mengen eingeführt haben: Dort war die Rede von der Vereinigung oder vom Durchschnitt mehrerer (endlich oder unendlich vieler) Gesamtheiten von Mengen, also eben von Mengen von Mengen.
Zu den damals angeführten Beispielen fügen wir noch einige hinzu, die dem täglichen Leben entnommen sind.

Eine Menge von Mengen ist zum Beispiel die Menge aller Berliner Sportvereine (jeder dieser Sportvereine wird von seinen Mitgliedern gebildet); die Menge aller wissenschaftlichen Kongresse eines bestimmten Jahres oder Landes, die Menge aller Gewerkschaftsorganisationen, die Menge aller militärischen Abteilungen (Divisionen, Regimenter, Bataillone, Kompanien, Züge usw.) einer gegebenen Armee sind ebenfalls Mengen von Mengen.

Diese Bei- spiele zeigen, dass sich Mengen, die Elemente einer gegebenen Menge von Mengen sind, in einigen Fällen überschneiden können, dagegen in anderen Fällen keine gemeinsamen Elemente zu haben brauchen.
So ist zum Beispiel die Menge aller Gewerkschaftsorganisationen eine Menge paarweise fremder Mengen, da ein Bürger nicht gleichzeitig Mitglied zweier verschiedener Gewerkschaften sein

kann. Andererseits ist die Menge aller militärischen Abteilungen irgendeiner Armee ein Beispiel einer Menge von Mengen, von denen einige Elemente Teilmengen der anderen Elemente sind : jeder Zug ist Teilmenge einer gewissen Kompanie, eine Kompanie ist Teilmenge einer Division usw.

Die Menge aller Sportvereine einer gegebenen Stadt besteht im allgemeinen aus sich überschneidenden Mengen, da ein und dieselbe Person in mehreren Sportvereinen aktiv sein kann (zum Beispiel in einem Schwimmklub und in einer Volleyballmannschaft oder einem Skiverein.)

Bemerkung. Zur Vereinfachung der Schreibweise werden wir manchmal anstatt des Ausdruckes "Menge von Mengen" den völlig gleichbedeutenden Ausdruck "Mengensystem" oder "Gesamtheit von Mengen" benutzen.

2. Einteilung in Klassen

Wir erhalten eine sehr wichtige Klasse von Mengensystemen, wenn wir alle möglichen Einteilungen irgendeiner Menge in paarweise durchschnittsfremde Mengen betrachten. Mit anderen Worten:
Es sei eine Menge M vorgegeben, die als Vereinigung paarweise durchschnittsfremder Teilmengen (in endlicher oder unendlicher Anzahl) dargestellt ist. Diese Teilmengen sind Summanden der Vereinigung und auch Elemente der gegebenen Einteilung der Menge M.

Beispiel I. Es sei M die Menge aller Schüler irgendeiner Schule. Die Schule ist in Klassen aufgeteilt, die offensichtlich auch durchschnittsfremde Teilmengen bilden und deren Vereinigung die gesamte Menge M ergibt.

Beispiel II. M sei die Menge aller Schüler der Oberschulen Berlins. Die Menge M kann beispielsweise auf folgende beiden Weisen in paarweise durchschnittsfremde Teilmengen zerlegt werden:

1. wir vereinigen in einem Summanden die Schüler ein und derselben Schule[49] (wir zerlegen also die Menge aller Schüler nach Schulen);

2. wir vereinigen in einem Summanden alle Schüler der gleichen Klasse (der verschiedenen Schulen).

Beispiel III. Es sei M die Menge aller Punkte der Ebene. Wir wählen in dieser Ebene irgendeine Gerade g und zerlegen die gesamte Ebene in zu g parallele Geraden. Die Mengen der Punkte jeder einzelnen Geraden sind ebenfalls derartige Mengen, in die wir die Menge M zerlegt haben.

Bemerkung I. Diejenigen Leser, die wissen, was ein Koordinatensystem ist, mögen sich die Gerade g als eine der Koordinatenachsen (der Bestimmtheit halber der Abszissenachse) dieses Koordinatensystems vorstellen.

Bemerkung II. Ist eine gegebene Menge M in paarweise durchschnittsfremde Teilmengen zerlegt, deren Vereinigung die Menge M ergibt, so spricht man zur Abkürzung einfach von einer Klasseneinteilung der Menge M.

Satz 1. Es sei eine Abbildung f der Menge A auf eine Menge B vorgegeben. Die vollen Urbilder $f^{-1}(b)$ aller möglichen Punkte b der Menge B bilden eine Klasseneinteilung der Menge A. Die Menge dieser Klassen ist der Menge B eineindeutig zugeordnet.

[49] Unter der Voraussetzung, dass jeder Schüler nur eine Schule besucht.

Dieser Satz ist eigentlich sofort klar: Jedem Element a der Menge A entspricht bei der Abbildung f ein und nur ein Element $b = f(a)$ der Menge B derart, dass a zum vollen Urbild $f^{-1}(b)$ gehört. Dies bedeutet aber auch, dass die vollen Urbilder der Punkte b erstens als Vereinigung die gesamte Menge A ergeben und zweitens paarweise durchschnittsfremd sind.

Die Menge der Klassen ist der Menge B eineindeutig zugeordnet:
Jedem Element b der Menge B entspricht die Klasse $f^{-1}(b)$, und jeder Klasse $f^{-1}(b)$ entspricht das Element b der Menge B.

Satz II. Es sei eine Klasseneinteilung einer Menge A vorgegeben. Diese Einteilung erzeugt eine Abbildung der Menge A auf eine gewisse Menge B, nämlich auf die Menge aller Klassen der gegebenen Einteilung. Diese Abbildung erhält man, wenn man jedem Element der Menge A die Klasse zuordnet, der es angehört.

Der Beweis des Satzes ist bereits in seiner Formulierung enthalten.

Beispiel. Bei der Einteilung der Berliner Schüler ist diese Abbildung der Menge A aller Schüler auf die Menge B aller Schulen bereits angegeben worden[50]. Jedem Schüler ist die Schule, die er besucht, zugeordnet.
Bei aller Selbstverständlichkeit der in unseren beiden Sätzen formulierten Tatsachen hat man sie in der Mathematik nicht sofort in ihrer mathematisch treffenden Formulierung gefunden. Nachdem man diese aber einmal gewonnen hatte, erlangte sie sofort im logischen Aufbau verschiedener mathematischer Disziplinen, vor allem der Algebra, sehr große Bedeutung.

3. Äquivalenzrelationen

Es sei eine Klasseneinteilung einer Menge M vorgegeben. Wir führen folgende Definition ein: Wir nennen zwei Elemente der Menge M äquivalent in bezug auf die gegebene Klasseneinteilung der Menge M, wenn sie zu ein und derselben Klasse gehören.
Teilen wir die Berliner Schüler nach Schulen ein, so sind also zwei Schüler "äquivalent", wenn sie die gleiche Schule besuchen (auch wenn sie verschiedenen Klassen angehören). Wenn wir die Schüler nach Klassen einteilen, so sind zwei Schüler "äquivalent", wenn sie ein und derselben Klasse (wenn auch verschiedenen Schulen) angehören.

Unsere eben definierte Äquivalenzrelation besitzt folgende Eigenschaften:
Die Eigenschaft der Symmetrie. Sind a und b äquivalent, so auch b und a.

Die Eigenschaft der Transitivität. Sind sowohl die Elemente a und b als auch b und c äquivalent, so sind a und c äquivalent ("zwei Elemente a und c, die einem dritten b äquivalent sind, sind auch untereinander äquivalent").

Schließlich fassen wir jedes Element als zu sich selbst äquivalent auf; diese Eigenschaft der Äquivalenzrelation heißt Reflexivität.
Somit definiert jede Klasseneinteilung einer vorgegebenen Menge zwischen den Elementen dieser Menge eine bestimmte Äquivalenzrelation, die die Eigenschaften der Symmetrie, Transitivität und Reflexivität besitzt.

Wir nehmen jetzt an, durch irgendein Verfahren stehe ein gewisses Kriterium zur Verfügung, das es uns ermöglicht, von gewissen Elementepaaren der Menge M als von äquivalenten Paaren zu sprechen. Dabei fordern wir von dieser Äquivalenz lediglich, dass sie die Eigenschaften der Symmetrie, Transitivität und Reflexivität besitzt.

[50] Unter der Voraussetzung, dass jeder Schüler nur eine Schule besucht

Wir beweisen, dass diese Äquivalenzrelation eine Klasseneinteilung der Menge M definiert.

Wir bezeichnen als Klasse K_a eines gegebenen Elementes a der Menge M die Menge aller Elemente, die zu a äquivalent sind.
Da unsere Äquivalenzrelation nach Voraussetzung reflexiv ist, so ist jedes Element a in seiner Klasse enthalten.
Wir beweisen: Wenn sich zwei Klassen überschneiden (also wenigstens ein gemeinsames, Element besitzen), so fallen sie sogar zusammen (d.h., jedes Element der einen Klasse ist gleichzeitig Element der anderen Klasse).

Die Klassen K_a und K_b mögen das Element c gemeinsam haben. Bezeichnet man die Äquivalenz irgend zweier Elemente x und y durch $x \sim y$, so gilt nach Definition der Klassen $a \sim c$, $b \sim c$, folglich wegen der Symmetrie $c \sim b$ und wegen der Transitivität

$$a \sim b \tag{1}$$

Es sei y irgendein Element der Klasse K_b. Dann gilt:

$$b \sim y$$

Wegen der Transitivität und (1) ist

$$a \sim y$$

d.h., y ist Element der Klasse K_a. Es sei jetzt x irgendein Element der Klasse K_a. Dann gilt:

$$a \sim x$$

und wegen der Symmetrie

$$x \sim a$$

sowie wegen (1) und der Transitivität

$$x \sim b$$

Infolge der Symmetrie ist

$$b \sim x$$

d.h., x gehört zur Klasse K_a.
Somit fallen zwei Klassen K_a und K_b die ein gemeinsames Element c besitzen, tatsächlich zusammen.

Wir haben bewiesen, dass die verschiedenen Klassen K_a ein System paarweise durchschnittsfremder Teilmengen der Menge M bilden. Ferner ergibt die Vereinigung der Klassen die gesamte Menge M, da jedes Element der Menge M seiner Klasse angehört.
Wir wiederholen die in diesem Artikel bewiesenen Resultate, indem wir sie in folgendem Satz zusammenfassen:

Satz III. Jede Klasseneinteilung einer Menge M definiert zwischen den Elementen der Menge M eine gewisse Äquivalenzrelation, die die Eigenschaften der Symmetrie, Transitivität und Reflexivität besitzt.
Umgekehrt definiert jede Äquivalenzrelation, die zwischen den Elementen der Menge M besteht und die Eigenschaften der Symmetrie, Transitivität und Reflexivität besitzt, eine Einteilung der Menge M in durchschnittsfremde Klassen paarweise zueinander äquivalenter Elemente.

Literatur

Baumgartner, L.: Gruppentheorie, 4. Aufl., W. de Gruyter, Berlin 1964.

Boruvka, O.: Grundlagen der Gruppoid- und Gruppentheorie, VEB Deutscher Verlag der Wissenschaften, Berlin 1960.

Kochendörffer, R.: Lehrbuch der Gruppentheorie unter besonderer Berücksichtigung der endlichen Gruppen, Akademische Verlagsgesellschaft, Leipzig 1966.

Kochendörffer, R.: Einführung in die Algebra, 3. Aufl., VEB Deutscher Verlag der Wissenschaften, Berlin 1966.

Kurosch, A. G.: Gruppentheorie I, II, 2. Aufl., Akademie-Verlag. Berlin 1970 bzw. 1971 (Übersetzung aus dem Russischen).

Ljubarski, G. J.: Anwendungen der Gruppentheorie in der Physik, VEB Deutscher Verlag der Wissenschaften, Berlin 1962.

Logowski, H., und H. J. Weinert: Grundzüge der Algebra, Teil 1: All. gemeine Gruppentheorie, 3. Aufl., B. G. Teubner, Leipzig 1966.

Smirnow, W. I.: Lehrgang der höheren Mathematik. Teil III , 5. Aufl., VEB Deutscher Verlag der Wissenschaften, Berlin 1967 (Übersetzung uns dem Russischen).

Specht, W.: Gruppentheorie, Springer-Verlag, Berlin-Göttingen-Heidelberg 1956.

Speiser, A.: Die Theorie der Gruppen von endlicher Ordnung, 4. Aufl., Birkhäuser, Basel 1966.

van der Waerden, B. L.: Algebra, Bd. I., 7. Aufl., Springer-Verlag, Berlin-Heidelberg-New York 1966.

Zassenhaus, H.: Jahrbuch der Gruppentheorie, Bd. I, B. G. Teubner, Leipzig-Berlin 1937.