Sammlung Göschen

Gruppentheorie

Von

Dr. Ludwig Baumgartner

Mit 6 Figuren

Sammlung Göschen

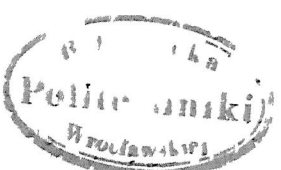
Gruppentheorie

Von

Dr. Ludwig Baumgartner
in München

Mit 6 Figuren

Berlin und Leipzig
Vereinigung wissenschaftlicher Verleger
Walter de Gruyter & Co.
vormals G. J. Göschen'sche Verlagshandlung — J. Guttentag, Verlagsbuchhandlung — Georg Reimer — Karl J. Trübner — Veit & Comp.
1921



Druck von
C. G. Roder G. m. b H., Leipzig
843020.

Inhaltsübersicht.

Folgende Bändchen der Sammlung Göschen sind im Text der Kürze halber nur mit Nummern zitiert:

B. Sporer, Niedere Analysis, Nr. 53.
M. Simon, Analytische Geometrie der Ebene, Nr. 65.
K. Doehlemann, Projektive Geometrie in synthetischer Behandlung, Nr. 72.
K. Knopp, Funktionentheorie I (Grundlagen der allgemeinen Theorie der analytischen Funktionen), Nr. 668.

Bemerkung über das Studium des vorliegenden Bändchens: Die folgende Darstellung der Gruppentheorie setzt lediglich die Grundbegriffe der Analysis (z. B. der reellen, rationalen, komplexen Zahl) und Geometrie (z. B. der Koordinaten und ihrer Transformation), keinerlei spezielle mathematische Kenntnisse voraus. Einzelne Beispiele aus anderen Gebieten können eventuell überschlagen werden. Dagegen ist — vielleicht in etwas höherem Grade als bei anderen Gebieten — Übung im exakten Denken, eine gewisse mathematische Reife Voraussetzung für ein erfolgreiches Studium.

Literatur.

Endliche und unendliche Gruppen:

H. Weber, Lehrbuch der Algebra, Bd. 1 und 2. Braunschweig 1898 bzw. 1899. (2. Aufl.)

J. A. de Séguier, Éléments de la théorie des groupes abstraits. Paris 1904.

Endliche Gruppen:

E. Netto, Gruppen- und Substitutionentheorie. Sammlung Schubert Nr. 55. Leipzig 1908.

W. Burnside, Theory of groups of finite order. Cambridge 1897.

L. Bianchi, Lezioni sulla teoria dei gruppi di sostituzioni. Pisa 1900.

F. Klein, Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade. Leipzig 1884.

Transformationsgruppen:

S. Lie, Theorie der Transformationsgruppen. 3 Bde. Leipzig 1888—93.

S. Lie, Vorlesungen über kontinuierliche Gruppen. Leipzig 1893.

S. Lie, Vorlesungen über Differentialgleichungen mit bekannten infinitesimalen Transformationen. Leipzig 1891.

I. Abschnitt.

Einführung in den Gruppenbegriff.

§ 1. Erste Abgrenzung des zu behandelnden Stoffes.

Gegenstand mathematischer Betrachtung sind häufig Systeme (Mengen, Komplexe) gleichartiger Dinge oder Elemente, von denen je zwei in bestimmter Reihenfolge nach einer gewissen Vorschrift wieder ein Element bestimmen oder, wie wir sagen wollen, sich zu einem solchen verknüpfen lassen. Ein Beispiel bietet das System der natürlichen Zahlen 1, 2, 3, ... mit der Addition als Verknüpfungsvorschrift, die Elemente 3 und 8 liefern das Element 11; oder das System der natürlichen Zahlen mit der Subtraktion als Verknüpfungsvorschrift, die Elemente 2 und 5 liefern die Zahl -3.

Das erste der beiden Beispiele ist insofern vollkommener als das zweite, als das Ergebnis der Verknüpfung stets wieder dem System angehört, 11 ist wieder eine natürliche Zahl, -3 dagegen nicht. Im ersteren Falle läßt sich das durch die Verknüpfung entstandene Element vermöge derselben Vorschrift wieder mit jedem Element des Systems verknüpfen, es hat also auch die sukzessive Verknüpfung von 3 oder mehr Elementen ohne weiteres einen Sinn; z. B. $(3 + 8) + 6 = 11 + 6 = 17$.

Wir stellen zunächst mehrere Beispiele solcher besonderer Systeme zusammen. Der Leser mag ein einzelnes Beispiel, dessen Gegenstand ihm nicht geläufig ist, vorerst überschlagen.

§ 2. Beispiele aus der Zahlenlehre.

1. Das System sei das der natürlichen Zahlen, die Elemente seien also 1, 2, 3, ... in inf. Die Verknüpfungsvorschrift sei die Addition. Z. B. $7 + 2 = 9$, $10 + 10 = 20$ (die beiden zu verknüpfenden Elemente können stets auch identisch sein).

2. Das System sei dasselbe, die Verknüpfungsvorschrift aber die Multiplikation. Auch sie liefert immer wieder eine natürliche Zahl, z. B. $4 \cdot 6 = 24$.

3. Das System sei das aller ganzen Zahlen $\ldots, -2, -1, 0, 1, 2, \ldots$, die Verknüpfungsvorschrift die Subtraktion. Z. B. $-6 - 2 = -8$, $1 - 1 = 0$.

4. Alle natürlichen Zahlen einschließlich Null, welche bei Division etwa mit 7 denselben Rest ergeben, nennt man „kongruent nach dem Modul 7", z. B. 6 und 13, geschrieben $6 \equiv 13 \pmod 7$. Nimmt man die nach dem Modul 7 kongruenten Zahlen je in eine Klasse, so erhält man 7 Klassen: $0, 7, 14, \ldots$; $1, 8, 15 \ldots$; ... schließlich 6, 13, 20, ... Wählt man aus jeder Klasse eine beliebige Zahl als Vertreterin der Klasse, so heißt man jedes System solcher 7 Zahlen ein „vollständiges Restsystem nach dem Modul 7". Das einfachste ist 0, 1, 2, 3, 4, 5, 6.

Wir wählen es als unser System von Elementen. Verknüpfen soll hier bedeuten: Addieren und die entstehende Zahl durch die kongruente Vertreterin ihrer Klasse ersetzen. Z. B. 6 und 4 liefert 3 ($6 + 4 = 10 \equiv 3$ [mod. 7]), 8 und 8 liefert 2.

§ 3. Beispiele aus der Funktionenlehre.

5. Das System bestehe aus den 4 Elementen

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

Die Verknüpfung zweier dieser Funktionen, etwa $f_i(x)$ und $f_k(x)$, sei die Bildung einer Funktion von einer Funktion, $f_k(f_i[x])$. Diese Reihenfolge, bei der die erste Funktion f_i die innere wird, ist willkürlich, muß aber von vornherein bestimmt festgelegt sein. In dem gegenwärtigen Beispiel ergibt zwar auch die umgekehrte Reihenfolge nichts anderes, vgl. jedoch Beispiel 6.

Man überzeugt sich leicht, daß die Verknüpfung von irgend zweien der vier Funktionen immer wieder auf eine Funktion des Systems führt, z. B. die Verknüpfung von f_3 und f_4 auf $f_2\left(\frac{-1}{-x} = \frac{1}{x}\right)$, von f_2 und f_2 auf f_1.

6. Das System bestehe aus allen ganzen Funktionen $g(x)$ einer komplexen Veränderlichen x, d. h. denjenigen Funktionen, deren Potenzreihenentwicklung in der ganzen Ebene konvergiert (s. Samml. Göschen 668, § 29). Die Funktionen x, $a_0 + a_1 x + \ldots + a_n x^n$, e^x, $\sin x$ finden sich unter den Elementen dieses Systems. Die Verknüpfung von $g_1(x)$ und $g_2(x)$ sei wie in Beispiel 5 die Bildung von $g_2(g_1[x])$. Eine ganze Funktion von einer ganzen Funktion ist wieder eine ganze Funktion.

§ 4. Beispiele aus der Algebra und Transformationslehre.

7. Die Gleichung

$$x^7 = 1 \quad \text{oder} \quad x^7 - 1 = 0$$

besitzt 7 Wurzeln, die sog. siebenten Einheitswurzeln, nämlich 1 und sechs komplexe Zahlen. Sie läßt sich in der Form schreiben:

$$(x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) = 0.$$

Die Wurzeln der Gleichung

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0$$

sind also die von 1 verschiedenen siebenten Einheitswurzeln. Nennen wir eine beliebige unter ihnen ε, so daß also gilt

$$\varepsilon^7 = 1 \text{ und } \varepsilon^6 + \varepsilon^5 + \varepsilon^4 + \varepsilon^3 + \varepsilon^2 + \varepsilon + 1 = 0,$$

so ist eine weitere ε^2, da

$$(\varepsilon^2)^6 + (\varepsilon^2)^5 + (\varepsilon^2)^4 + (\varepsilon^2)^3 + (\varepsilon^2)^2 + (\varepsilon^2) + 1 = 0$$

ist, wie Ausrechnung und Reduktion mittels $\varepsilon^7 = 1$ zeigt. Das Gleiche gilt für ε^3, ε^4, usw. Sämtliche von 1 verschiedenen siebenten Einheitswurzeln stellen sich somit dar durch $\varepsilon, \varepsilon^2, \varepsilon^3, \varepsilon^4, \varepsilon^5, \varepsilon^6$.

Dies sei unser System. Wir verknüpfen hier z. B. ε^3 und ε^6 durch die Bildung $(\varepsilon^3)^6$ und Reduktion mittels der Beziehung $\varepsilon^7 = 1$, erhalten also ε^4. In gleicher Weise liefert die Verknüpfung irgend zweier Elemente des Systems immer wieder ein solches.

8. Das folgende Beispiel wird eines der wichtigsten für uns sein und rechtfertigt daher eine etwas längere Vorbereitung.

Unter einer „Permutation" von n Dingen $a, b, c, \ldots$ versteht man das Ersetzen jedes dieser n Dinge durch eines von ihnen, derart, daß wieder alle n Dinge erhalten werden[1]). Man schreibt die ersetzenden Dinge unter die ursprünglichen und fügt das Ganze in Klammern, so daß z. B. die Permutation von 5 Dingen a, b, c, d, e, welche a durch c, b durch d, c durch a, d durch b, e durch e ersetzt, folgendermaßen geschrieben wird:

$$\begin{pmatrix} a & b & c & d & e \\ c & d & a & b & e \end{pmatrix}.$$

[1]) Man versteht unter einer Permutation z. B. von 3 Dingen a, b, c auch eine fertige Anordnung der 3 Dinge, z. B. c, a, b. Vgl. Samml. Göschen Nr. 53, § 15. Hier bedienen wir uns dieser Auffassung nicht, sondern verstehen unter einer Permutation stets das Ersetzen, den Übergang von jedem Ding zu einem neuen.

Natürlich bedeutet jeder Ausdruck mit anderer Anordnung der ersten Zeile, z. B.

$$\begin{pmatrix} c & e & d & b & a \\ a & e & b & d & c \end{pmatrix},$$

dasselbe, solange nur dieselben Dinge untereinander stehen, also c unter a, d unter b usw. Auch

$$\begin{pmatrix} a & b & c & d & e \\ a & b & c & d & e \end{pmatrix}$$

zählt als eine Permutation, die sog. „identische Permutation".

Im folgenden handelt es sich fast ausschließlich um Permutationen von Ziffern 1, 2, 3, ..., wir sprechen daher weiterhin von Ziffern, für irgendwelche Dinge würde wörtlich dasselbe gelten.

Zwei Permutationen der nämlichen Ziffern können wir verknüpfen, indem wir sie nacheinander ausführen, z. B.

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

Die erste ersetzt 1 durch 3, die zweite 3 durch 2, die beiden nacheinander ausgeführt also 1 durch 2, ebenso 2 durch 1, 3 durch 3. Das Ergebnis der Verknüpfung ist wieder eine Permutation, nämlich

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

Wir drücken die Verknüpfung durch Nebeneinanderschreiben aus. Ferner machen wir bei der Ausrechnung zweckmäßig von der erwähnten Willkürlichkeit der Anordnung der ersten Zeile Gebrauch. Wir wählen die erste Zeile der zweiten Permutation gleich der zweiten Zeile der ersten Permutation. Dann können wir das Ergebnis der Verknüpfung unmittelbar ablesen:

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

Die Reihenfolge der Verknüpfung ist hier durchaus wesentlich, ihre Umkehrung liefert im allgemeinen nicht dasselbe:

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

Wir wollen jetzt noch eine zweite, kürzere und übersichtlichere Schreibweise der Permutationen kennen lernen. Die Permutation

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

ersetzt 1 durch 3, 3 durch 4, 4 durch 2, 2 durch 5, 5 durch 1. Ordnen wir die Ziffern auf einem Kreise an, so daß auf jede Ziffer diejenige folgt, durch welche sie ersetzt wird, so charakterisiert uns dieses Schema die Permutation vollständig. Es genügt auch, wenn wir die Ziffern in derselben Anordnung der Bequemlichkeit halber wieder in einer Zeile schreiben, wobei wir mit irgendeiner Ziffer beginnen können; die Ziffernreihe wird dabei in Klammern geschlossen:

(1 3 4 2 5) oder (3 4 2 5 1) oder ....

bedeutet die Permutation, welche 3 durch die darauffolgende Ziffer 4, 4 durch 2, ..., die letzte Ziffer durch die erste ersetzt. Man nennt eine Permutation, welche sich in dieser Weise darstellen läßt, welche also bei passender Anordnung der Ziffern jede in die folgende, die letzte in die erste verwandelt, „zyklisch“ oder einen „Zyklus“.

Natürlich ist nicht jede Permutation zyklisch.

$$\begin{pmatrix}1&2&3&4&5&6&7\\4&3&1&2&6&5&7\end{pmatrix}$$

führt, wenn wir etwa mit 1 beginnen, zuerst auf einen Zyklus (1 4 2 3), wenn wir mit 5 beginnen, auf einen Zyklus (5 6), wenn wir mit 7 beginnen, auf einen „eingliedrigen" Zyklus (7). Diese drei Zyklen in beliebiger Reihenfolge nebeneinander gesetzt, stellen unsere Permutation eindeutig dar:

$$\begin{pmatrix}1&2&3&4&5&6&7\\4&3&1&2&6&5&7\end{pmatrix} = (1\,4\,2\,3)\,(5\,6)\,(7) = (7)\,(2\,3\,1\,4)\,(6\,5) = \text{usw.}$$

Sehen wir von den verschiedenen Möglichkeiten der Schreibweise ab, also von der Reihenfolge der Zyklen und von der zulässigen Verschiebung der Ziffern innerhalb jedes Zyklus, so können wir sagen:

Jede Permutation kann auf eine und nur eine Art in Zyklen (auch eingliedrige) mit lauter verschiedenen Ziffern zerlegt werden.

Die Verknüpfung solcher durch Zyklen dargestellten Permutationen, z. B. (1 3 2 4) (5) und (3) (4 1 5) (2), die natürlich durch die oben festgesetzte Verknüpfung der Permutationen definiert ist, geschieht nach folgendem Verfahren:

Die erste Permutation führt 1 in 3 über, die zweite 3 in 3, beide nacheinander also 1 in 3; wir schreiben auf (1 3) ... und fahren fort: die erste Permutation führt 3 in 2 über, die zweite 2 in 2, beide nacheinander also 3 in 2; wir schreiben auf (1 3 2)... und fahren fort: „2 in 4". „4 in 1", also „2 in 1"; wir sind bei der Ausgangsziffer angelangt, brauchen diese nicht mehr zu schreiben, sondern nur die Klammer zu schließen. (1 3 2) ist ein Zyklus des Resultates. Wir fahren fort mit einer noch nicht aufgeschriebenen Ziffer, z. B. 5: „5 in 5", „5 in 4", also „5 in 4"; wir schreiben auf (1 3 2) (5 4... und fahren fort: „4 in 1", „1 in 5", also „4 in 5". Dieser letzte Schritt

war eigentlich nur noch eine Probe, unsere 5 Ziffern waren ja bereits verbraucht. (1 3 2) (5 4) ist das Resultat, in Zyklen geschrieben.

Nach diesen Vorbereitungen betrachten wir das System aller möglichen Permutationen der 3 Ziffern 1, 2, 3. Wir finden 6 solche, die wir in Zyklen so schreiben können:

(1) (2) (3), (1 2) (3), (1 3) (2), (2 3) (1), (1 2 3), (1 3 2).

Verknüpfen bedeutet nacheinander ausführen. Wir sehen leicht, daß irgend zwei der Permutationen wieder eine im System vorkommende Permutation liefern, z. B. (1 2) (3) (1 2 3) = (1 3) (2).

9. Das System bestehe aus allen Transformationen (Substitutionen) der Form

$$\begin{aligned} x' &= a\,x + b\,y \\ y' &= c\,x + d\,y\,, \end{aligned}$$

wo a, b, c, d irgendwelche reelle Zahlen sind, für welche — damit die später (S. 21) notwendige Auflösung der Gleichungen nach x, y möglich ist — $a : b \neq c : d$.

Zwei Elemente des Systems sind also z. B.

$$(1)\quad \begin{aligned} x' &= 3\,x - \sqrt{2}\,y \\ y' &= x + y \end{aligned} \quad \text{und} \quad (2)\quad \begin{aligned} x' &= 5\,x + \tfrac{1}{2}\,y \\ y' &= x - 4\,y \end{aligned}.$$

Unter der Verknüpfung von (1) und (2) — in dieser Reihenfolge — verstehen wir das Nacheinander-Ausführen der beiden Transformationen, nämlich, wenn wir die zweite mit anderen Veränderlichen schreiben,

$$\begin{aligned} x'' &= 5\,x' + \tfrac{1}{2}\,y' \\ y'' &= x' - 4\,y'\,, \end{aligned}$$

die Bildung von

$$x'' = 5\,(3\,x - \sqrt{2}\,y) + \tfrac{1}{2}(x + y)$$
$$y'' = \quad (3\,x - \sqrt{2}\,y) - 4\,(x + y)$$

Jetzt führen wir wieder x', y' ein und erhalten als Ergebnis der Verknüpfung

$$x' = 15\tfrac{1}{2}\,x + (\tfrac{1}{2} - 5\sqrt{2})\,y$$
$$y' = -\,x - (\sqrt{2} + 4\quad)\,y$$

Dies ist wieder eine Transformation des Systems[1]).

§ 5. Beispiele aus der Geometrie.

10. Das System bestehe aus allen denjenigen Drehungen eines regulären n—ecks in seiner Ebene um seinen Mittelpunkt, die es wieder mit seiner Ausgangslage zur Deckung bringen. Drehungen, die sich um Vielfache von 2π unterscheiden, z. B. Linksdrehung um $\frac{2k\pi}{n}$ und Rechtsdrehung um $\frac{2(n-k)\pi}{n}$, gelten als identisch. In-Ruhe-lassen oder Drehung um $2k\pi$ zählt auch als Element. Sämtliche verschiedenen Elemente des Systems sind also: In-Ruhelassen, Rechtsdrehung um $\frac{2\pi}{n}$, Rechtsdrehung um $\frac{4\pi}{n}$, ..., Rechtsdrehung um $\frac{(2n-2)\pi}{n}$.

Wir verknüpfen 2 Drehungen, z. B. um $\frac{2k\pi}{n}$ und um $\frac{2l\pi}{n}$, indem wir sie nacheinander ausführen. Die Gesamt-

[1]) Geometrisch stellen die Gleichungspaare unseres Systems sämtliche affinen Beziehungen zweier Ebenen dar, bei welchen sich die Nullpunkte entsprechen. Vgl. z. B. K. Doehlemann, Geometrische Transformationen, Samml. Schubert Nr. 27, S. 139 ff.

bewegung der Figur ist dabei immer wieder eine im System vorkommende Drehung $\left(\text{um } \frac{2(k+l)\pi}{n}\right)$.

11. Das System bestehe aus den Elementen des eben betrachteten Systems und aus allen Umklappungen des regulären n—ecks aus der Ebene heraus um Symmetriegerade. Da es deren n gibt, ist die Anzahl der Umklappungen ebenfalls n, die Gesamtzahl der Elemente des Systems also $2n$. Verknüpfen bedeutet wieder nacheinander ausführen. Dabei erhalten wir immer wieder ein Element des Systems.

Z. B. sei für $n = 4$ ein erstes Element der Übergang von Fig. I zu II (Linksdrehung um $\frac{\pi}{2}$), ein zweites der Übergang von II zu III (Umklappung um die Symmetriegerade $D\,B$). Die Verknüpfung der beiden, d. h. der Übergang von I zu III ist wieder ein Element des Systems, nämlich die Umklappung um die Symmetriegerade S.

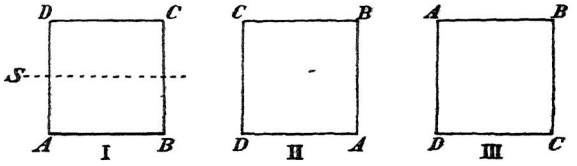


Fig. I.

Wie das Beispiel zeigt, legen wir die Elemente des Systems durch Einführung einer Bezeichnung der Eckpunkte fest. Wir können uns auch ein Koordinatensystem starr mit der Figur verbunden und mitbewegt denken. Bei der Verknüpfung wird die zweite Bewegung von der Endstellung der ersten aus ausgeführt.

Wir müssen hier auf eine zweite Auffassung aufmerksam machen, die wir uns nicht aneignen wollen. Ohne Einführung einer Bezeichnung oder eines Koordinatensystems könnten wir unser erstes Element als Linksdrehung um $\frac{\pi}{2}$, unser zweites als Umklappung um die von der linken oberen zur rechten unteren Ecke führende Symmetriegerade definieren. Auch nach der Ausführung des ersten Elements, also an der Stellung II würden wir dann um die von links oben nach rechts unten führende Symmetriegerade, nämlich um die Gerade $C\,A$ der Fig. II umklappen und kämen zu einer Stellung III'. Das Resultat der Verknüpfung wäre also ein anderes.

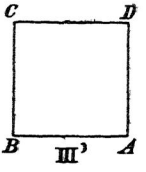


Fig. II.

Im Beispiel 10 decken sich die beiden Auffassungen, nicht aber in 12; in 13 und 14 ist nur die von uns gewählte Auffassung möglich.

12. Das System bestehe aus allen Drehungen eines regulären Tetraeders, die es wieder mit seiner Ausgangsstellung zur Deckung bringen. Auch hier rechnen wir das In-Ruhelassen als Element des Systems. Die weiteren Elemente sind, wenn wir die Ecken des Tetraeders mit A, B, C, D bezeichnen: die 8 Drehungen um $\frac{2\pi}{3}$ und $\frac{4\pi}{3}$ um die Senkrechten von D auf die Ebene $A\,B\,C$, von C auf die Ebene $A\,B\,D$, von B auf die Ebene $A\,C\,D$ und von A auf die Ebene $B\,C\,D$, ferner die 3 Drehungen um π um die Verbindungsgeraden der Mitte von $A\,B$ mit der Mitte von $C\,D$, der Mitte von $A\,C$ mit der Mitte von $B\,D$ und der Mitte von $B\,C$ mit der Mitte von $A\,D$.

Die Verknüpfung zweier Elemente, d. h. das Nacheinander-Ausführen, liefert stets wieder ein Element des Systems. Z. B. ergibt die Verknüpfung der vorletzten und letzten der eben angeführten 11 Drehungen die drittletzte.

13. Die Elemente des Systems seien alle möglichen Bewegungen[1]) einer bestimmten ebenen Figur in der Ebene, das In-Ruhe-lassen wieder eingeschlossen. Für die Verknüpfung gilt dasselbe wie in den letzten 3 Beispielen. Irgend 2 Bewegungen nacheinander ausgeführt, ergeben eine Lageveränderung der Figur, welche sich auch durch eine einzige Bewegung erreichen läßt.

4. Statt der Bewegungen einer ebenen Figur in der Ebene wählen wir die Bewegungen eines Körpers im dreidimensionalen Raum, sonst gilt dasselbe.

Diese Beispiele werden im folgenden kurz als Beispiel 1—14 zitiert.

§ 6. Die verschiedene Natur der einzelnen Beispiele.

Die angeführten Beispiele sind nicht ganz gleicher Art. Sofort bemerken wir, daß die Systeme teils endlich, teils unendlich viele Elemente enthalten. Wir nennen sie darnach „endlich“ oder „unendlich“.

Weitere Unterschiede finden wir bei genauerer Betrachtung der Verknüpfung. Dazu müssen wir eine Bezeichnung einführen, welche die Ausdrucksweise vereinfacht.

Systeme oder Teile von Systemen (auch „Komplexe“ genannt) werden mit großen deutschen Buchstaben be-

[1]) „Bewegung“ ist als Lagenveranderung aufzufassen, auf den Weg kommt es dabei nicht an.

zeichnet, z. B. $\mathfrak{S}$, $\mathfrak{R}$, $\mathfrak{G}$; die einzelnen Elemente der Systeme mit großen lateinischen Buchstaben, z. B. A, B, G. Die Verknüpfung wird symbolisch durch Multiplikation ausgedrückt, das Ergebnis auch „Produkt" genannt.

Aus 2 Elementen A und B können wir zwei Produkte $A\,B$ und $B\,A$ bilden. Manche unserer Beispiele liefern, wie wir auch A und B aus dem System wählen, durchweg zwei gleiche Produkte, $A\,B = B\,A$; so ist in Beispiel 1 etwa $7 + 2 = 2 + 7$ und ebenso für jedes Paar von natürlichen Zahlen. Das Gleiche gilt für die Beispiele 2, 4, 5, 7..... Dagegen liefern die Systeme 3, 6, 8, ... wenigstens für einen Teil der Elemente zwei verschiedene Produkte. So ist im System 3 etwa $3 - 5 \neq 5 - 3$. Wir nennen die Systeme der ersten Art „kommutativ", die der zweiten Art „nichtkommutativ".

Sind A, B, C drei Elemente eines Systems, so können wir einerseits $(A\,B)\,C$ bilden, d. h. zuerst A mit B verknüpfen, dann das Erhaltene mit C, anderseits $A\,(B\,C)$, d. h. zuerst $B\,C$ bilden, dann A mit diesem verknüpfen. Z. B. für $A = 2$, $B = 7$, $C = 4$ liefert die Verknüpfung des Beispiels 1 $(2 + 7) + 4$ bzw. $2 + (7 + 4)$, die Verknüpfung des Beispiels 3 $(2 - 7) - 4$ bzw. $2 - (7 - 4)$.

Ein System, das, welche Elemente A, B, C wir auch herausgreifen, stets zwei gleiche Produkte $(A\,B)\,C = A\,(B\,C)$ ergibt, heißt „assoziativ", ein System, das wenigstens zum Teil Verschiedenes liefert, „nichtassoziativ". Beispiel 3 ist nichtassoziativ, es ist ja $(2 - 7) - 4 \neq 2 - (7 - 4)$, alle übrigen Beispiele sind assoziativ.

Machen wir uns noch die Assoziativität des Beispiels 8 völlig klar! P_1, P_2, P_3 seien 3 der Permutationen, P_1 ersetze etwa die Ziffer 2 durch 1, P_2 1 durch 3, P_3 3 durch 1. Dann ersetzt das Produkt $P_1\,P_2\,P_3$ die Ziffer 2 durch 1,

gleichgültig ob zunächst $P_1\ P_2$ in eine 2 durch 3 ersetzende Permutation zusammengefaßt und dann mit P_3 verknüpft, also 3 durch 1 ersetzt wird, oder ob zuerst $P_2\ P_3$ in eine 1 durch 1 ersetzende Permutation zusammengefaßt und dann P_1 mit dieser verknüpft wird. Dasselbe gilt für jede andere Ziffer, deren Verwandlung wir verfolgen. Wir erkennen: Permutationen derselben n Ziffern sind immer assoziativ.

Bei einigen unserer Beispiele beachteten wir bereits das Vorhandensein eines Elements, das jedes andre Element, mit dem es verknüpft wird, ungeändert läßt. Von dieser Art war die identische Permutation und das In-Ruhelassen bei unseren geometrischen Beispielen. Man nennt ein solches Element „Einheitselement" und bezeichnet es mit E. Es ist charakterisiert durch die Gleichungen

$$A\,E = A \quad \text{und} \quad E\,A = A,$$

wo A alle Elemente des Systems durchläuft.

Beispiel 1 enthält kein Einheitselement, alle übrigen enthalten solche. In Beispiel 2 ist es die Zahl 1, in 3 und 4 die Zahl 0, in 5 und 6 die Funktion x, in 7 die Wurzel ε, in 9 der Fall $a = d = 1$, $b = c = 0$ (sog. „identische Transformation").

Bei unseren geometrischen Beispielen gibt es zu jeder Bewegung eine zweite, welche gerade wieder zur Ausgangsstellung zurückführt, so in Beispiel 10 zur Drehung um $\frac{2k\pi}{n}$ die Drehung um $\frac{-2k\pi}{n} = \frac{2(n-k)\pi}{n}$. Die Verknüpfung der beiden liefert das Einheitselement. Man nennt das zweite Element „invers" oder „reziprok" zum ersten und schreibt, wenn dieses A heißt, A^{-1} in Fort-

führung der an die Multiplikation angelehnten Bezeichnungsweise. Das inverse Element zu A ist charakterisiert durch die Gleichung

$$A\,A^{-1} = E\,.$$

Bei den Beispielen 1, 2. 6 finden wir innerhalb des Systems solche inverse Elemente nicht oder doch nicht zu allen Elementen. Dagegen bei den übrigen Beispielen. In Beispiel 3 und 5 ist jedes Element zu sich selbst invers, in Beispiel 4 ist etwa zu 5 invers 2, in Beispiel 7 zu ε^2 invers ε^4; in Beispiel 8 ist zu $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ invers die Permutation mit vertauschten Zeilen, nämlich $\begin{pmatrix}3&1&2\\1&2&3\end{pmatrix}$; in Beispiel 9 ist zu jeder Transformation diejenige invers, welche sich ergibt, wenn man die beiden Gleichungen nach x, y auflöst und nachträglich x', y' statt x, y und x, y statt x', y' schreibt

§ 7. Definition der Gruppe.

Wir wollen nun mittels der gefundenen Eigenschaften den strengen Begriff eines Systems festlegen, das wir „Gruppe“ nennen. Welche Eigenschaften wollen wir dabei aufnehmen? Würden wir die Endlichkeit verlangen, so würden wir zu viele Fälle ausschalten, würden wir die Kommutativität fordern, so gingen uns gerade die interessanteren Fälle verloren. Wir erhalten einen hinreichend umfassenden und der Untersuchung werten Begriff durch die

Definition: Ein System $\mathfrak{S}$ von Elementen $A, B, C, \ldots$ heißt eine „Gruppe“, wenn (für sämtliche Elemente) folgendes gilt:

I. Es liegt eine Vorschrift vor, welche ein erstes Element S und ein zweites Element T des Systems eindeutig ver-

knüpft, d. h. ein $S\,T$ definiert; dabei können S und T auch identisch sein.

II. Das Ergebnis dieser Verknüpfung ist wieder ein Element des Systems.

III. Die Verknüpfung ist assoziativ $(S\,T)\,U = S\,(T\,U)$; es kann also eindeutig $S\,T\,U$ geschrieben werden.

IV. *Es ist ein Einheitselement im System vorhanden*, d. h. ein Element E von der Art, daß für jedes Element S des Systems gilt

$$S\,E = E\,S = S.$$

V. Zu jedem Element S des Systems ist ein inverses Element im System vorhanden, d. h. ein Element S^{-1}, so daß

$$S\,S^{-1} = E.$$

Diese 5 definierenden Eigenschaften werden im folgenden kurz Eig. I—V genannt.

Gruppen werden meist mit dem Buchstaben $\mathfrak{G}$ bezeichnet.

§ 8. Einige unmittelbare Folgerungen.

Bei Eigenschaft IV müssen wir noch den Zweifel beheben, ob es nicht neben E ein zweites Einheitselement E' in der Gruppe geben kann. Da E Einheitselement ist, müßte dann, wenn wir das obige S gleich E' wählen,

$$E\,E' = E'$$

sein; ebenso müßte, da E' Einheitselement ist, für $S = E$

$$E\,E' = E$$

sein; daraus folgt

$$E' = E.$$

Satz 1. In jeder Gruppe gibt es nur ein Einheitselement.

Bei Eigenschaft V drängt sich uns die Frage auf, welches wieder das inverse Element zu S^{-1} ist. Nennen wir es X, so soll sein

$$S^{-1} X = E.$$

Ein vielverwandtes Mittel zur Umformung solcher gruppentheoretischer Gleichungen ist, wie bei gewöhnlichen Gleichungen, die nach Eig. I und II mögliche Multiplikation (d. h. Verknüpfung) beider Seiten mit einem passenden Element der Gruppe. Doch dürfen wir im allgemeinen nur beiderseits vorn oder beiderseits hinten einen Faktor ansetzen.

Im Hinblick auf die Gleichung $S S^{-1} = E$ multiplizieren wir hier vorne mit S:

$$S (S^{-1} X) = S E$$

oder nach Eig. III $\quad (S S^{-1}) X = S E$

oder nach Eig. V $\quad E X = S E$

oder nach Eig. IV $\quad X = S.$

Wir haben den

Satz 2. Das inverse Element zu S^{-1} ist S.

Beispiel: Wählen wir in Beispiel 8 das Element $S = (1\ 2\ 3)$, so ist dazu invers $S^{-1} = (1\ 3\ 2)$, weil $(1\ 2\ 3)\ (1\ 3\ 2) = E$. Zu S^{-1} ist nun tatsächlich wieder S invers, es ist $(1\ 3\ 2)\ (1\ 2\ 3) = E$.

Hinsichtlich der Anzahl der inversen Elemente zu einem gegebenen vermuten wir bei Betrachtung der Beispiele den

Satz 3. Es gibt zu jedem Element nur ein inverses in der Gruppe.

Wäre nämlich X ein zweites inverses Element zu S, also

$$S X = E \text{ neben } S S^{-1} = E,$$

so wäre $$S X = S S^{-1}$$
oder $$S^{-1} S X = S^{-1} S S^{-1}$$
oder $$E X = E S^{-1}$$
oder $$X = S^{-1}.$$

Ganz in derselben Weise läßt sich der allgemeinere Satz beweisen:

Satz 4. Sind A, B, C Elemente einer Gruppe, so folgt aus der Gleichung $A B = A C$ die Gleichung $B = C$, aus der Gleichung $B A = C A$ die Gleichung $B = C$.

Es folgt nämlich etwa aus $A B = A C$ durch linksseitige Multiplikation mit A^{-1}

$$A^{-1} A B = A^{-1} A C \text{ oder } E B = E C \text{ oder } B = C.$$

Aufgabe 1. Welche von den Beispielen 1—14 sind Gruppen?

§ 9. Über die Bedeutung und die historische Entwicklung der Gruppentheorie.

Daß der Gruppenbegriff einer der Grundbegriffe des exakten Denkens ist, ähnlich wie der Begriff der Menge, der Größe, der Funktion, werden wir schon aus der Verschiedenartigkeit der bisherigen Beispiele vermuten; im Laufe der Untersuchungen wird es immer deutlicher werden. Für die meisten mathematischen Disziplinen hat sich die gruppentheoretische Auffassung nicht nur als möglich, sondern als außerordentlich fruchtbar erwiesen. Nur mit Hilfe endlicher Gruppen läßt sich ein klarer Einblick in das Wesen der algebraischen Gleichungen und die Gesetze ihrer Auflösbarkeit gewinnen. Die Differentialgleichungen hängen aufs engste mit unendlichen Gruppen zusammen. Auch in gewissen Teilen der

Funktionenlehre treten gruppentheoretische Betrachtungen immer mehr in den Vordergrund. Freilich erfordern diese Zusammenhänge ein eingehendes Studium, wir können sie daher bei dem beschränkten Raum dieser Einführung nicht verfolgen. Dagegen läßt sich ohne größere Vorbereitungen eine wichtige Stellung des Gruppenbegriffs in der Geometrie erkennen. Der nächste Abschnitt soll uns zeigen, wie dieser Begriff hier geradezu als Einteilungsprinzip dienen kann.

Historisch hat sich der Gruppenbegriff zuerst bei der Untersuchung der algebraischen Gleichungen deutlich entwickelt. Die erste systematische Behandlung stammt von Augustin Louis Cauchy (1789—1857). Die Hauptstufen der weiteren Entwicklung bilden die Arbeiten von Niels Henrik Abel (1802—29) und Evariste Galois (1811—32) über die algebraischen Gleichungen, von Camille Jordan über Permutationsgruppen, von Sophus Lie (1842—99) über Transformationsgruppen und von Felix Klein über geometrische und funktionentheoretische Anwendungen der Gruppentheorie.

II. Abschnitt.

Der Gruppenbegriff in der Geometrie.

§ 10. Die äquiforme Gruppe.

Ehe wir unsere Hauptaufgabe in Angriff nehmen, den Bau einer Gruppe zu erforschen, soll uns eine allgemeine, auf A. Cayley und F. Klein zurückgehende Auffassung verschiedener geometrischer Gebäude die grundlegende Wichtigkeit des Gruppenbegriffes deutlich machen. Es handelt sich dabei nur um einen Überblick, nicht um eine

genaue Ausführung[1]). Für das Verständnis der folgenden Abschnitte bildet die Kenntnis dieses Abschnitts keine Voraussetzung.

Wir beschränken uns auf die Ebene, bemerken aber, daß für den dreidimensionalen Raum Analoges gilt.

Man kann die Eigenschaften der aus den Elementen Punkt und Gerade aufgebauten ebenen Gebilde auf folgende fundamentale Eigenschaften zurückführen: 1. Lage in der Ebene, 2. absolute Größe, 3. Senkrechtstehen oder Orthogonalität von zwei Geraden, 4. Parallelismus von zwei Geraden, 5. vereinigte Lage oder Inzidenz von Punkt und Gerade, d. h. die Tatsache, daß ein Punkt auf einer Geraden liegt, die Gerade durch den Punkt geht.

Die ersten beiden Eigenschaften sind nicht Gegenstand geometrischen Interesses. Wo z. B. ein Dreieck liegt, und wie groß es angenommen wird, ist ohne Belang für die ihm innewohnenden geometrischen Eigenschaften. In der elementaren Geometrie handelt es sich um die drei übrigen Eigenschaften.

Nun gibt es solche Verwandlungen oder Transformationen der ebenen Gebilde, welche gerade die drei letzten Eigenschaften unverändert lassen, während sie die ersten beiden im allgemeinen zerstören. Suchen wir diese Transformationen! Die Lage wird durch Bewegung oder Spiegelung[2]) geändert, die Größe durch Vergrößerung oder Verkleinerung. Jede Transformation, die entweder von einer dieser Arten ist oder sich aus ihnen zusammensetzt, heißt eine „Ähnlichkeitstransformation" oder „äquiforme Transformation". Sie erhält die Form und damit die

[1]) Eine eingehende Darstellung findet man in L. Heffter und C. Kohler, Lehrbuch der analytischen Geometrie, I. Bd., Leipzig 1905.

[2]) Spiegelung an einer Geraden, d. h. Ersetzen des Gebildes durch sein Spiegelbild, sein in bezug auf die Gerade symmetrisches Gebilde.

Eigenschaften 3, 4, 5. Das System aller Ähnlichkeitstransformationen ist das von uns gesuchte. Wir können nun auch sagen: In der elementaren Geometrie handelt es sich um diejenigen Eigenschaften, welche durch das System der Ähnlichkeitstransformationen nicht geändert werden.

Das Teilsystem der Bewegungen haben wir oben (Beispiel 13) als Gruppe erkannt, wobei wir als Verknüpfung das Nacheinander-Ausführen der Verwandlungen festsetzten. Dies führt uns dazu, auch das aus allen Ähnlichkeitstransformationen bestehende System bei gleicher Verknüpfungsvorschrift auf Gruppeneigenschaft zu prüfen. Daß zwei Ähnlichkeitstransformationen nacheinander ausgeführt einer Transformation derselben Art gleichkommen, erkennen wir ohne weiteres, wenn wir die Transformationen als diejenigen auffassen, welche die Form erhalten. Wenn T_1 die Form ungeändert läßt und ebenso T_2, so gilt das Gleiche von T_1 T_2. Die Transformationen sind ferner assoziativ; z. B. führt Vergrößerung mit Drehung (etwa in bezug auf den Koordinatenanfang) und darauffolgende Spiegelung (etwa an der X-Achse) zum gleichen Ergebnis wie Vergrößerung und darauffolgende Drehung mit Spiegelung. Es ist ein Einheitselement vorhanden, das In-Ruhe-lassen, und ein inverses Element zu jedem, nämlich dasjenige, welches wieder zur Ausgangsfigur zurückführt, z. B. zur Vergrößerung die entsprechende Verkleinerung, zur Spiegelung wieder die Spiegelung.

Das System der Ähnlichkeitstransformationen bildet also eine Gruppe, die sog. „Hauptgruppe“ oder „äquiforme Gruppe“. Die elementare Geometrie, auch „äquiforme Geometrie“ genannt, untersucht die Eigenschaften der Gebilde, welche ungeändert bleiben bei den Transformationen der äquiformen Gruppe. Man kann

dieses Ergebnis auch so ausdrücken: Die äquiforme Geometrie betrachtet alle Gebilde als identisch, welche durch die Transformationen der äquiformen Gruppe ineinander übergehen.

§ 11. Die affine Gruppe.

Wir erhalten eine enger beschränkte, an Begriffen und Sätzen ärmere Geometrie, die „affine Geometrie", wenn wir außer von der ersten und zweiten Eigenschaft auch noch von der dritten Eigenschaft, der Orthogonalität, absehen, z. B. uns nur noch für die Parallelogrammeigenschaften eines Rechtecks interessieren, etwa daß die Diagonalen sich halbieren.

Die Transformationen, welche die Eigenschaften 4 und 5 erhalten, aber 1, 2, 3 im allgemeinen zerstören, nennt man „affine Transformationen"[1]). Das System aller affinen Transformationen bildet wieder eine Gruppe, die „affine Gruppe". Es leuchtet nämlich unmittelbar ein, daß zwei affine Transformationen nacheinander ausgeführt wieder eine affine Transformation ergeben, indem wir sie als die Transformationen auffassen, welche jedes Paar paralleler Geraden wieder in ein Paar paralleler Geraden, jeden Punkt mit hindurchgehender Geraden wieder in einen Punkt mit hindurchgehender Geraden verwandeln.

---

[1]) Hierher gehört z. B. die Verwandlung, welche eine Figur in der Richtung der X-Achse in gleichem Maße verkürzt, in der Richtung der Y-Achse verlängert, wie etwa die auf diese Weise vor sich gehende Verwandlung eines Kreises in eine Ellipse. Parallele Sehnen gehen dabei wieder in parallele über, senkrechte im allgemeinen nicht in senkrechte. Betreffs weiterer affiner Transformationen vgl. Beispiel 9, Seite 15, Fußnote 1, ferner § 44. Dabei ist noch folgendes zu beachten. Für die analytische Darstellung ist es zweckmäßig, die Transformationen in der Weise ausgeführt zu denken, daß man nicht das einzelne Gebilde transformiert (dreht, streckt usw.), sondern die ganze Ebene samt ihren Gebilden. Dies erreicht man einfach durch Transformation der Koordinaten.

Auch über Assoziativität, Einheitselement und reziproke Elemente gilt dasselbe wie oben bei der äquiformen Gruppe.

Die affine Gruppe enthält naturgemäß auch sämtliche Transformationen der äquiformen Gruppe, weil auch diese Eigenschaft 4 und 5 ungeändert lassen; sie umfaßt also die äquiforme Gruppe. Anderseits gibt es natürlich weniger Eigenschaften, welche die (größere) Menge von Transformationen der umfassenderen Gruppe vertragen, die Sätze der affinen Geometrie sind ein Teil der Sätze der äquiformen.

§ 12. Die projektive Gruppe.

Gehen wir noch einen Schritt weiter und verzichten auch noch auf den Parallelismus, achten also nur noch auf die Inzidenz, z. B. nur auf die Viereckseigenschaften eines Parallelogramms, so kommen wir wiederum zu einer engeren Geometrie, der „projektiven Geometrie".

Die Transformationen, welche Eigenschaft 5 erhalten, dagegen 1, 2, 3, 4 im allgemeinen zerstören[1]), heißen „projektive Transformationen". Genau wie oben ergibt sich, daß sie wieder eine Gruppe bilden, die „projektive Gruppe"[2]). Diese umfaßt die affine und umsomehr die äquiforme Gruppe.

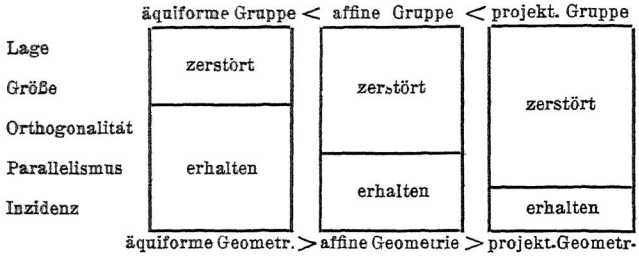
§ 13. Zusammenfassung und Überblick.

Der Inhalt der §§ 10, 11, 12 hat uns gezeigt, daß der Gruppenbegriff in die geometrische Betrachtungsweise Ordnung und Übersicht bringt. Jedem geometrischen Gebäude entspricht eine Gruppe, es werden nur diejenigen

[1]) Natürlich handelt es sich immer noch um Transformationen, welche jeden Punkt wieder in einen Punkt, jede Gerade wieder in eine Gerade verwandeln.

[2]) Die analytische Form sämtlicher projektiven Transformationen findet man in § 44.

Eigenschaften der Gebilde ins Auge gefaßt, welche gegenüber den Transformationen dieser Gruppe unveränderlich sind, die übrigen Eigenschaften außer acht gelassen, Gebilde, welche sich nur durch solche unterscheiden, als identisch betrachtet. Zur umfassenderen Gruppe gehört ein engeres geometrisches Gebäude. Die folgende schematische Zusammenstellung soll diese Verhältnisse nochmals vorführen:



Zuletzt soll noch ein Vergleich zur Klärung beitragen. Wir denken uns jede der betrachteten Transformationen als ein Sieb besonderer Art, in das wir die Eigenschaften der Gebilde legen. Durch die Siebe der äquiformen Gruppe gehen alle auf Orthogonalität, Parallelismus und Inzidenz beruhenden Eigenschaften hindurch. Werfen wir diese in die größere Zahl von Sieben der affinen Gruppe, so bleibt alles, was die Orthogonalität enthält, zurück, was noch durchfällt, ist auf Parallelismus und Inzidenz zurückführbar. Die größte Zahl von Sieben endlich, die der projektiven Gruppe, passieren nur die auf Indizenz allein beruhenden Eigenschaften.

Verfolgen wir denselben Prozeß nochmals umgekehrt! Verwenden wir zuerst die Siebe der projektiven Gruppe, so werden nur die Inzidenzeigenschaften durchgelassen,

wir erhalten die projektive Geometrie. Was zurückblieb, schütten wir in die Siebe der affinen Gruppe; so kommen zu den projektiven Eigenschaften noch alle auf dem Parallelismus beruhenden, zur projektiven Geometrie die sog. „Parallelmetrik" hinzu, beide zusammen bilden die affine Geometrie. Jetzt wird der Rest noch in die Siebe der äquiformen Gruppe gebracht; damit sondern wir noch die auf Orthogonalität beruhenden Eigenschaften ab, die affine Geometrie wird durch die „Orthogonalmetrik" zur äquiformen Geometrie ergänzt:

Äquiforme Geometrie		Orthogonalmetrik	z. B. Rechteckseigenschaften eines Rechtecks (gleiche Länge der Diagonalen)
	Affine Geometrie	Parallelmetrik	z. B. Parallelogrammeigenschaften eines Rechtecks (gegenseitiges Halbieren der Diagonalen)
		Projektive Geometrie	z. B. Viereckseigenschaften eines Rechtecks (Vorhandensein der Diagonalen).

III. Abschnitt.

Die endlichen Gruppen.

§ 14. Ordnung einer Gruppe; Isomorphismus; abstrakte Gruppe.

Wir gehen nun daran, die Eigenschaften der Gruppen zu erforschen und beschränken uns dabei zunächst auf den übersichtlicheren Fall der „endlichen Gruppe", d. h. der Gruppe mit einer endlichen Anzahl von Elementen. Diese Anzahl heißt „Ordnung" der Gruppe. Sie wird mit kleinen lateinischen Buchstaben bezeichnet, und zwar werden wir stets den der Gruppenbezeichnung entsprechenden Buchstaben wählen: Gruppe $\mathfrak{G}$ hat die Ordnung g.

Vergleichen wir unser Beispiel 4 mit Beispiel 10 für $n = 7$, so zeigt sich eine Verwandtschaft, die nicht nur darin liegt, daß gleich viele Elemente vorhanden sind, also die Ordnung übereinstimmt, sondern auch darin, daß sich die Elemente in gleicher Weise verknüpfen. Ordnen wir nämlich die Elemente folgendermaßen:

Beispiel 4:

$$0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6$$

Beispiel 10:

$$\text{Drehung um } 0,\ \frac{2\pi}{7},\ \frac{4\pi}{7},\ \frac{6\pi}{7},\ \frac{8\pi}{7},\ \frac{10\pi}{7},\ \frac{12\pi}{7},$$

so liefert z. B. die Verknüpfung des zweiten und fünften Elements der ersten Zeile das sechste, die Verknüpfung des zweiten und fünften Elements der zweiten Zeile ebenfalls das sechste, und dies gilt durchweg.

Man kann die Elemente zweier solcher Gruppen $\mathfrak{A}$, $\mathfrak{B}$ so anordnen, etwa $A_1, A_2, \ldots, A_g$ bzw. $B_1, B_2, \ldots, B_g$, daß, wenn

$$A_i A_k = A_l$$

ist, stets auch

$$B_i B_k = B_l$$

wird. Solche Gruppen zeigen nur eine Verschiedenheit in der Natur ihrer Elemente, nicht aber in ihren Verknüpfungsgesetzen, in ihrer Form. Sie heißen „isomorph". Wir schreiben $\mathfrak{A} \simeq \mathfrak{B}$.

Zwei Gruppen gleicher Ordnung brauchen durchaus nicht immer isomorph zu sein, wie der Vergleich des Beispiels 10 für $n = 4$ und des Beispiels 5 zeigt. Wie wir auch die Zuordnung versuchen, etwa

$$\text{Drehung um } 0,\ \frac{\pi}{2},\ \pi,\ \frac{3\pi}{2}$$

$$\text{Funktion} \qquad x, \frac{1}{x}, -x, -\frac{1}{x},$$

es liefern zwei entsprechende Produktbildungen hier wohl teilweise, aber niemals durchweg Entsprechendes. Z. B. liefert das zweite und vierte Element der ersten Zeile das erste Element, das zweite und vierte Element der zweiten Zeile aber das dritte Element.

Dagegen sind natürlich zwei Gruppen, welche derselben dritten isomorph sind, unter sich isomorph.

Da es uns bei allgemeinen mathematischen Untersuchungen gerade auf die Form ankommt, betrachten wir isomorphe Gruppen hierbei als nicht verschieden. Wir denken uns für alle isomorphen Gruppen einen Typ, bei dem wir die Elemente nur durch Zeichen darstellen, von ihrer Natur abstrahieren. Solche Gruppen heißen „abstrakte Gruppen". Es wird sich im folgenden um abstrakte Gruppen handeln, selbstverständlich werden wir aber immer wieder auf konkrete Beispiele zurückgreifen.

Aufgabe 2. Gibt es zu jeder Zahl g $(= 1, 2, 3, \ldots)$ eine Gruppe der Ordnung g?

Aufgabe 3. Man suche Beispiele isomorpher Gruppen.

Aufgabe 4. Kann eine Gruppe mit sich selbst isomorph sein, d. h. kann man ihre Elemente in zweierlei Reihenfolgen anordnen, so daß die Beziehung des Isomorphismus besteht („Automorphismus")?

§ 15. Erste Untersuchung über den Bau der Gruppen; Ordnung der Elemente; Untergruppe.

Um einen Einblick in den Bau einer Gruppe zu bekommen, liegt es nahe, zuerst besondere Fälle der Ver-

knüpfung zu betrachten. Ist A ein beliebiges Element der Gruppe $\mathfrak{G}$, so bilden wir — zur Veranschaulichung wird Beispiel 7 für $A = \varepsilon^3$ in Klammern beigesetzt[1]) —

$$\begin{array}{llllll} A, & AA, & AAA, & AAAA, & \ldots \\ [\varepsilon^3, & \varepsilon^2, & \varepsilon^6, & \varepsilon^4, & \ldots] \text{ und schreiben} \\ A, & A^2, & A^3, & A^4, & \ldots . \end{array}$$

Da wir auch schon dem Zeichen A^{-1} (durch die Definition $AA^{-1} = E$, § 7) eine Bedeutung beigelegt haben [ε^5], werden wir dazu geführt, diese Reihe nach links fortzusetzen. Wir verstehen zweckmäßig unter A^0 das Element $AA^{-1} = E$ [ε], unter A^{-s} das Element $A^{-1}A^{-1}A^{-1}\ldots$ (s mal) $= (A^{-1})^s$. Wir erhalten also

$$\begin{array}{l} \ldots, A^{-4}, A^{-3}, A^{-2}, A^{-1}, A^0, A, A^2, A^3, A^4, A^5, \ldots \\ [\ldots, \varepsilon^2, \varepsilon^6, \varepsilon^4, \varepsilon^5, \varepsilon, \varepsilon^3, \varepsilon^2, \varepsilon^6, \varepsilon^4, \varepsilon^5, \ldots]. \end{array}$$

Für diese „Potenzen" soll jetzt die Gültigkeit zweier gewöhnlicher Potenzregeln abgeleitet werden[2]). Es ist z. B.

$$A^4A^{-3} = AAAAA^{-1}A^{-1}A^{-1} = (\text{da } AA^{-1} = E)$$
$$AAAEA^{-1}A^{-1} = AAAA^{-1}A^{-1} = \text{usw., schließlich}$$
$$= A = A^{4-3} \quad [(\varepsilon^4)^6 = \varepsilon^3].$$

Ebenso erkennt man durch Betrachtung aller möglichen Fälle ($r, s \gtreqless 0$) die Gültigkeit der Gleichung

$$A^r A^s = A^{r+s} \text{ für alle } r, s \gtreqless 0.$$

Ähnlich läßt sich eine zweite Potenzregel beweisen.

---

[1]) Man beachte, daß dort die Produktbildung, etwa von ε^3 und ε^4, nicht als gewöhnliche Multiplikation, sondern als $(\varepsilon^3)^4$ definiert ist.

[2]) Der Leser hute sich davor, gelaufige Potenzregeln ohne weiteres anzuwenden; sie müssen alle erst aus den hier gegebenen Definitionen bewiesen werden.

Es ist

$$(A^5)^2 = A^5 A^5 = A^{5.2} \quad [\varepsilon^4].$$

Allgemein

(1) $\qquad (A^r)^s = A^{rs}$ für alle $r, s < 0.$

Das inverse Element zu A^3, bezeichnet als $(A^3)^{-1}$, ist definiert durch

$A^3(A^3)^{-1} = E$; da aber $AAAA^{-1}A^{-1}A^{-1} = E$ ist, oder $A^3(A^{-1})^3 = E$, so folgt

$$(A^3)^{-1} = (A^{-1})^3 \quad [\varepsilon^6];$$

ebenso ist allgemein

(2) $\qquad (A^r)^{-1} = (A^{-1})^r = A^{-r}$ für $r > 0.$

Mittels der Gleichungen (1) und (2) ergibt sich nun z. B.

$$(A^5)^{-2} \overset{1)}{=} [(A^5)^{-1}]^2 = [(A^{-1})^5]^2 = [A^{-1}]^{5.2} = A^{-5.2} \quad [\varepsilon^2]$$

$$(A^{-5})^2 = [(A^{-1})^5]^2 = [A^{-1}]^{5.2} = A^{-5.2} \quad [\varepsilon^2]$$

$$(A^{-5})^{-2} = \{[(A^{-1})^5]^{-1}\}^2 = \{[(A^{-1})^{-1}]^5\}^2 = \{A^5\}^2 = A^{5.2} \quad [\varepsilon^4].$$

Endlich ist z. B.

$$(A^0)^3 = A^0 A^0 A^0 = E = A^0 = A^{0.3} \quad [\varepsilon]$$

$$(A^3)^0 = A^3(A^3)^{-1} = E = A^{3.0} \quad [\varepsilon].$$

Damit erkennt man die allgemeine Gültigkeit der Gleichung

$$(A^r)^s = A^{rs} \text{ für } r, s \gtreqless 0.$$

Alle Elemente

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

[1]) Nach der Definition: $A^{-s} = (A^{-1})^s$ für jedes A (hier auf A^5 angewandt).

sind wieder Gruppenelemente. Da die Gruppe nur endlich viele Elemente hat, müssen gleiche darunter vorkommen, etwa $A^r = A^s$. Ist $r > s$, so folgt $A^r A^{-s} = A^s A^{-s}$ oder

$A^{r-s} = E$. [Für $A = \varepsilon^3$ ist $A^{15} = A^3$ oder $A^{15-3} = \varepsilon$]. Ist $r - s$ noch nicht die kleinste Zahl, für welche eine solche Gleichung gilt, so gibt es doch eine kleinste [für $A = \varepsilon^3$ die Zahl 6].

Satz 5. Zu jedem Element A einer endlichen Gruppe gibt es eine kleinste Zahl a, so daß $A^a = E$ ist. a heißt „Ordnung des Elements A".

Das Einheitselement E selbst und nur dieses hat die Ordnung 1.

Es sei nun a die Ordnung des Elements A, also $A^a = E$; dann ist auch

$$A^{na} = (A^a)^n = E^n = E \text{ für jede ganze Zahl } n.$$

Ist also $r - s$ durch a teilbar, so ist $A^{r-s} = E$. Wir können dies auch so ausdrücken: Ist A von der Ordnung a, so ist $A^r = A^s$, wenn $r \equiv s \pmod{a}$.

Nun sei umgekehrt $A^r = A^s$ oder $A^{r-s} = E$ und a wieder die Ordnung von A. Wäre dann nicht $r \equiv s \pmod{a}$, sondern etwa $r - s = na + q$, wobei $0 < q < a$, so wäre

$$E = A^{r-s} = A^{na+q} = A^{na} A^q = E A^q = A^q;$$

es gäbe also eine Zahl $q < a$, so daß $A^q = E$ wäre, a wäre im Widerspruch mit der Voraussetzung nicht die Ordnung von A.

Damit haben wir folgenden Satz bewiesen, der über die Beziehungen zwischen den Potenzen eines Elements vollen Aufschluß gibt:

Satz 6. Ist a die Ordnung des Elements A, so ist $A^r = A^s$ dann und nur dann, wenn $r \equiv s \pmod{a}$.

Danach stellen die sämtlichen Potenzen des Elements A nur a verschiedene Elemente vor. Betrachten wir den Komplex derselben und untersuchen ihn auf die Gültigkeit der Eigenschaften einer Gruppe![1]) Das Produkt zweier Potenzen von A ist wieder eine Potenz von A, also gleich einem im Komplex vorhandenen Element, E spielt wieder die Rolle des Einheitselements, und zu jeder Potenz A^r ist A^{-r} invers. Wir finden somit

Satz 7. Die a verschiedenen Potenzen eines einer Gruppe $\mathfrak{G}$ angehörigen Elements von der Ordnung a bilden eine Gruppe $\mathfrak{A}$.

Eine derartige, nur aus den Potenzen eines ihrer Elemente bestehende Gruppe heißt „zyklisch".

Satz 7 führt uns noch auf einen anderen wichtigen Begriff:

Eine Gruppe $\mathfrak{H}$, deren sämtliche Elemente unter den Elementen einer Gruppe $\mathfrak{G}$ vorkommen, heißt eine „Untergruppe" von $\mathfrak{G}$. Wir schreiben $\mathfrak{H} < \mathfrak{G}$ oder $\mathfrak{G} > \mathfrak{H}$[2]).

Die Gruppe $\mathfrak{A}$ des Satzes 7 gibt uns ein Beispiel einer Untergruppe. Die Gruppe des Beispiels 10 ist Untergruppe

[1]) In Fallen wie dem gegenwärtigen, wo das auf Gruppeneigenschaft zu untersuchende System bereits einer großeren Gruppe angehört, braucht Eig. I und III nicht mehr geprüft zu werden.

[2]) Ein einheitliches Zeichen für das Enthaltensein bzw. Enthalten hat sich bisher in der Literatur nicht eingebürgert. Wir verwenden die Zeichen des Großenvergleichs $<, =, >$ auch fur diesen „Mengenvergleich", wobei man sie etwa „enthalten in" oder „teilt", „gleich", „enthält" lese. Und zwar setzen wir die Zeichen nicht nur im Falle einer Untergruppe, sondern für jedes Enthalten oder Enthaltensein; z. B. $G < \mathfrak{G}$, wenn G Element von $\mathfrak{G}$ ist, $\mathfrak{C} \geqq \mathfrak{D}$, wenn $\mathfrak{D}$ Teilkomplex von $\mathfrak{C}$ ist, ihn vielleicht erschöpft. Wo es die Deutlichkeit verlangt, werden wir die Gruppeneigenschaft durch Beifügen eines kleinen g zum Zeichen hervorheben: $\mathfrak{H} \leqq_g \mathfrak{G}$.

derjenigen des Beispiels 11. Im Beispiel 12 bilden das In-Ruhe-lassen und die drei möglichen Drehungen um Verbindungsgerade von Mitten gegenüberliegender Seiten eine Untergruppe[1]).

Prüfen wir das Einheitselement E als System aufgefaßt auf Gültigkeit der Eig. I—V, so erkennen wir, daß es stets für sich eine Gruppe bildet. Als solche wird es mit $\mathfrak{E}$ bezeichnet. $\mathfrak{E}$ ist Untergruppe jeder Gruppe $\mathfrak{G}$.

Oft ist es zweckmäßig, auch $\mathfrak{G}$ selbst als Untergruppe von $\mathfrak{G}$ zu betrachten. Eine von $\mathfrak{E}$ und $\mathfrak{G}$ verschiedene Untergruppe von $\mathfrak{G}$ nennen wir auch „eigentliche“ oder „echte“ Untergruppe.

Aufgabe 5. Man bestimme die Ordnung jedes Elements des Beispiels 7.

Aufgabe 6. Gibt es zu jeder Zahl a ($= 1, 2, 3, \ldots$) eine zyklische Gruppe der Ordnung a?

Aufgabe 7. Die Gruppe Beispiel 8 hat mit Einschluß der uneigentlichen 6 Untergruppen; man suche sie.

§ 16. Fortsetzung.

Kehren wir wieder zu den Potenzen von Gruppenelementen zurück und betrachten nun 2 Elemente einer Gruppe, A mit Ordnung a und B mit Ordnung b, so können wir das Produkt $A\,B$ bilden und nach dessen Potenzen $(A\,B)^r$ fragen ($r \gtreqless 0$).

Im allgemeinen Falle läßt sich $(A\,B)^2 = A\,B\,A\,B$, $(A\,B)^3 = A\,B\,A\,B\,A\,B$, usw. nicht anders darstellen, es gilt also hier nicht dieselbe Regel wie für gewöhnliche Po-

[1]) Der II. Abschnitt bot uns in der affinen und aquiformen Gruppe Untergruppen der projektiven Gruppe, in der äquiformen eine Untergruppe der affinen, allerdings nicht von endlicher Ordnung.

tenzen. Wenn speziell $AB = BA$ ist, erhält man $A^2 B^2$, $A^3 B^3$, usw.

Für $(AB)^{-1}$ finden wir stets einen anderen Ausdruck. Es ist nach Definition das Element, das mit AB verknüpft das Einheitselement liefert. Dies leistet aber auch das Element $B^{-1}A^{-1}$, es ist ja $ABB^{-1}A^{-1} = AEA^{-1} = AA^{-1} = E$. Wir haben also zu setzen

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

wobei die Vertauschung der Reihenfolge zu beachten ist. Ähnlich ist

$$(AB)^{-n} = (B^{-1}A^{-1})^n.$$

Aufgabe 8. Man drücke $(ABC)^{-1}$ durch die inversen Elemente zu A, B, C aus.

Aufgabe 9. Man beweise: A und A^{-1} haben stets dieselbe Ordnung.

Aufgabe 10. Aus den Ordnungen a, b zweier Elemente A, B einer Gruppe läßt sich im allgemeinen kein Schluß ziehen auf die Ordnung c des Produktes AB. Im Falle $AB = BA$ aber beweise man, daß c ein Teiler von ab sein muß.

Aufgabe 11. Man beweise: AB und BA haben stets dieselbe Ordnung. Mit ABC hat BCA und CAB gleiche Ordnung, dagegen nicht notwendig ACB, BAC, CBA.

§ 17. Darstellung einer Gruppe durch ein quadratisches Schema.

Bei den bisherigen Überlegungen macht uns schon in einfachen Fällen der Umstand Schwierigkeit, daß wir bei den Beispielen das Produkt zweier Elemente erst errechnen oder durch mühsame Vorstellung finden müssen. Da kom-

men wir auf den Gedanken, uns für jede Gruppe von vornherein eine Tabelle anzulegen, welche zu irgend zwei Elementen ihr Produkt ohne weiteres angibt. Wir werden etwa zu der folgenden Anordnung geführt, die an der Kreuzungsstelle der mit A_i beginnenden Spalte und der mit A_k beginnenden Zeile das Produkt $A_i A_k$ enthält[1]):

$$\begin{array}{llll} E & A_2 & A_3 & \dots\, A_i \quad \dots\, \\ A_2 & A_2^2 & A_3 A_2 & \dots\, A_i A_2 \dots\, \\ A_3 & A_2 A_3 & A_3^2 & \dots\, A_i A_3 \dots\, \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ A_k & A_2 A_k & A_3 A_k & \dots\, A_i A_k \dots\, \\ \dots & \dots & \dots & \dots \end{array}$$

Der Leser stelle sich etwa zu den Beispielen 5 und 8 solche Quadrate her. Dabei genügt es, die Indizes statt der Elemente anzuschreiben.

Die Eigenschaften dieser Quadrate müssen die Gruppeneigenschaften widerspiegeln. Wir bemerken: In jeder Zeile und in jeder Spalte stehen genau alle Elemente der Gruppe. An die Entstehung einer Zeile oder Spalte denkend vermuten wir den

Satz 8. Sind $A_1, A_2, \dots, A_g$ sämtliche verschiedenen Elemente einer Gruppe $\mathfrak{G}$ und A_i ein beliebiges unter ihnen, so sind auch

$$A_1 A_i, A_2 A_i, \dots, A_g A_i \text{ oder}$$
$$A_i A_1, A_i A_2, \dots, A_i A_g$$

wieder gerade die sämtlichen Elemente von $\mathfrak{G}$.

Der Beweis ist einfach: Wäre etwa $A_r A_i = A_s A_i$, so wäre nach Satz 4 $A_r = A_s$.

[1]) Daß wir $A_i A_k$ und nicht $A_k A_i$ schreiben, ist willkürlich; doch merke man sich die einmal getroffene Wahl. Warum beginnen wir zweckmäßig mit E? Auch weiterhin können wir eine gewisse Ordnung einhalten, etwa ein Element mit seinen Potenzen folgen lassen.

Umgekehrt kann es sehr wohl möglich sein, g Elemente $A_1, A_2, \ldots, A_g$ in ein Quadrat von g^2 Feldern so einzuordnen, daß in jeder Zeile und jeder Spalte gerade diese g Elemente stehen, ohne daß diese eine Gruppe bilden. Es ist nämlich möglich, daß die Bedingung der Assoziativität nicht erfüllt ist. Beispiel:

1	2	3	4	5
2	4	1	5	3
3	5	4	1	2
4	3	5	2	1
5	1	2	3	4

Hier ist $(2\ 4)\ 5 = 2$, dagegen $2\ (4\ 5) = 5$.

Aufgabe 12. Wie müßte man das quadratische Schema einrichten, damit in der von links oben nach rechts unten laufenden Diagonale beständig E stünde?

§ 18. Zusammenhang der abstrakten Gruppen mit den Permutationsgruppen.

Wir kehren wieder zu einem quadratischen Schema zurück, das wir von einer Gruppe ausgehend gewinnen. In jeder Zeile stehen genau alle g Elemente der Gruppe. Der Übergang von der ersten Zeile zu jeder Zeile stellt eine Permutation der g Elemente vor. Wir erhalten so einschließlich der identischen g Permutationen. So liefert Beispiel 5, indem wir nur die Indizes schreiben:

$$P_1 = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\ P_2 = \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},\ P_3 = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\ P_4 = \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}.$$

Der Vergleich mit der ursprünglichen Gruppe führt uns auf den

Satz 9. Bilden $A_1, A_2, \ldots, A_g$ eine Gruppe $\mathfrak{G}$, so bilden die Permutationen

$$P_i = \begin{pmatrix} A_1 & A_2 & \dots & A_r & \dots & A_g \\ A_1 A_i & A_2 A_i & \dots & A_r A_i & \dots & A_g A_i \end{pmatrix} \text{ für } i = 1, 2, \dots g$$

ebenfalls eine Gruppe $\mathfrak{P}$, wenn wir unter Verknüpfen das Nacheinander-Ausführen verstehen, und es ist $\mathfrak{P} \cong \mathfrak{G}$.

Es ist nämlich Eig. I erfüllt, Permutationen derselben Dinge verknüpfen wir stets, indem wir sie nacheinander ausführen. Daß diese Verknüpfung immer assoziativ ist, haben wir uns schon in § 6 klar gemacht. Die Bedingungen des Einheitselements erfüllt die identische Permutation. Wir beweisen Eig. II und zugleich den Isomorphismus, indem wir zeigen: Ist $A_i A_k = A_l$, so ist $P_i P_k = P_l$ $(i, k = 1, 2, \dots g)$.

Schreiben wir uns auch P_k an:

$$P_k = \begin{pmatrix} A_1 & A_2 & \dots & A_s & \dots & A_g \\ A_1 A_k & A_2 A_k & \dots & A_s A_k & \dots & A_g A_k \end{pmatrix}.$$

P_i führt ein Element A_r in $A_r A_i$ über, P_k ein Element A_s in $A_s A_k$, also $A_r A_i$ in $A_r A_i A_k = A_r A_l$; $P_i P_k$ führt also A_r in $A_r A_l$ über, d. h. es ist gleich P_l.

Nun ist auch Eig. V unschwer zu bestätigen, indem man sich A_i^{-1} statt A_k denkt.

Es genügt, wenn wir in den Permutationen stets nur die Indizes anschreiben. Dann erhalten wir zu jeder Gruppe der Ordnung g eine isomorphe Permutationsgruppe von g Ziffern. Dies ist insofern ein sehr wichtiges Ergebnis, als es sagt, daß die Permutationsgruppen alle Formen der endlichen Gruppen überhaupt erschöpfen. Die Untersuchung der Permutationsgruppen wird also lohnend sein, zumal die Permutationen leicht so darstellbar sind, daß sie ihre Eigenschaften erkennen lassen (z. B. die Produktbildung bequem ausführbar ist).

Aufgabe 13. Man bilde zu Beispiel 8 die isomorphe Permutationsgruppe im Sinne des Satzes 9. Die Tatsache, daß wir dabei zwei isomorphe Permutationsgruppen von verschiedener Ziffernzahl erhalten, stellt uns vor neue Fragen: Durch welche Permutationsgruppen kann man überhaupt eine abstrakte Gruppe darstellen? Welches ist jene mit kleinster Ziffernzahl? Die allgemeine Lösung dieser Fragen ist noch nicht gelungen.

§ 19. Permutationen.

Ehe wir Permutationsgruppen untersuchen, müssen wir die einzelnen Permutationen näher betrachten.

In § 4 haben wir bereits folgenden Satz abgeleitet:

Satz 10. Jede Permutation kann (abgesehen von der Reihenfolge) auf eine und nur eine Art in Zyklen (auch eingliedrige) mit lauter verschiedenen Ziffern zerlegt werden.

Ganz anders verhält es sich bei der Zerlegung einer Permutation in ein Produkt von zyklischen Permutationen, bei denen wir auch gemeinsame Ziffern in den Faktoren zulassen; sie ist durchaus nicht mehr eindeutig. Schon ein einzelner Zyklus gestattet bei dieser Zulassung gemeinsamer Ziffern in den Faktoren eine weitere Zerlegung und zwar wieder in mehrfacher Weise, z. B.

$$(1\ 2\ 3) = (1\ 2)\,(1\ 3)^{1}) \quad \text{(Ziffer 1 gemeinsam)}$$
$$(1\ 2\ 3) = (2\ 3)\,(1\ 2) \quad (\ \text{„}\ 2\ \text{„}\ );$$

(1 2 3) ist also in zweifacher Weise zerlegt und zwar in zweigliedrige Zyklen, die man „Transpositionen“ nennt.

---

[1]) Ein derartiges Produkt ist als Produkt von 2 Permutationen derselben Ziffern (1, 2, 3) aufzufassen, nämlich [(1 2) (3)] [(1 3) (2)], die Multiplikation erfolgt also nach dem in § 4 angegebenen Verfahren. Eingliedrige Zyklen werden häufig nicht geschrieben; bei der Multiplikation sind sie hinzuzudenken.

Versuchen wir diese einfachste Zerlegung bei einem Zyklus von n Ziffern! Wir finden sukzessive durch Probieren

$$(1\ 2) = (1\ 2)$$
$$(1\ 2\ 3) = (1\ 2)(1\ 3)$$
$$(1\ 2\ 3\ 4) = (1\ 2)(1\ 3)(1\ 4)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

und bestätigen die Richtigkeit durch Ausmultiplizieren der rechten Seiten, können also den Satz aussprechen:

Satz 11. Jeder n-gliedrige Zyklus läßt sich als Produkt von $n-1$ Transpositionen darstellen.

Daß die gefundene Darstellung eines Zyklus durch Transpositionen nicht die einzige sein kann, sehen wir ohne weiteres daraus, daß wir jeder Darstellung noch das der Einheit gleiche Produkt (1 2) (1 2) anfügen können. Auf die Anzahl der Faktoren achtend werden wir aber nach einigen Proben folgende Gesetzmäßigkeit bemerken:

Satz 12. Jeder Zyklus von gerader Ziffernzahl läßt sich nur in eine ungerade Anzahl von Transpositionen zerlegen, jeder Zyklus von ungerader Ziffernzahl nur in eine gerade Anzahl.

Zum Beweis müssen wir uns überlegen, wie überhaupt eine Permutation P von n Ziffern durch Anfügen einer Transposition T aus 2 der n Ziffern geändert wird. Wir wollen die Untersuchung an einem Beispiel führen, sie ist danach leicht allgemein zu gestalten. Es sei

$$P = (1\ 2\ 3)(4\ 5)(6);$$

für T sind 2 Fälle möglich:

$T_1 = (2\ 3)$ (*die beiden Ziffern kommen in demselben* Zyklus von P vor),

$T_2 = (2\ 4)$ (die beiden Ziffern kommen in verschiedenen Zyklen von P vor).

$P\,T_1 = (4\ 5)\,(6)\,(1\ 2\ 3)\,(2\ 3)$ oder in Zyklen mit lauter verschiedenen Ziffern umgerechnet[1]),

$P\,T_1 = (4\ 5)\,(6)\,(1\ 3)\,(2)$, d. h. die Zyklenzahl hat sich (gegenüber P) um 1 vermehrt.

$P\,T_2 = (6)\,(1\ 2\ 3)\,(4\ 5)\,(2\ 4) = (6)\,(1\ 4\ 5\ 2\ 3)$, d. h. die Zyklenzahl hat sich um 1 vermindert.

Wir sprechen das Ergebnis aus in dem

Satz 13. Multipliziert man irgendeine Permutation von n Ziffern, die in r Zyklen mit lauter verschiedenen Ziffern zerfällt (Satz 10), mit einer Transposition aus 2 der n Ziffern, so erhält das Produkt (im Sinne des Satzes 10) $r+1$ oder $r-1$ Zyklen.

Damit gelingt uns nun nicht nur der Beweis des Satzes 12, sondern sogleich der Beweis der folgenden Verallgemeinerung dieses Satzes, die sich auf eine beliebige Permutation, nicht nur auf einen einzelnen Zyklus bezieht:

Satz 14. Jede beliebige Permutation P von n Ziffern und r Zyklen mit lauter verschiedenen Ziffern läßt sich auf unendlich viele Weisen in Transpositionen zerlegen (anders ausgedrückt: Zu jeder Permutation kann man durch eine willkürlich beginnende Reihe von Transpositionen gelangen), aber die Gesamtzahl der Transpositionen ist von der Form $n - r + 2\sigma$ ($\sigma = 0, 1, 2, \ldots$), also entweder stets gerade, wenn nämlich die (für eine gegebene Permutation unveränderlich festliegende) Zahl $n - r$ gerade ist, oder stets ungerade, wenn $n - r$ ungerade ist[2]).

Zerlegen wir nämlich nach Satz 11 jeden der r Zyklen von P in Transpositionen, so erhalten wir, wenn die

[1]) Man halte die Darstellungen durch Zyklen mit lauter verschiedenen Ziffern und durch Zyklen mit gemeinsamen Ziffern scharf auseinander!

[2]) Satz 12 ergibt sich durch die Spezialisierung $r = 1$; dann ist $n - r = n - 1$ ungerade oder gerade, je nachdem n gerade oder ungerade ist.

r Zyklen bzw. $\nu_1, \nu_2, \ldots, \nu_r$ Ziffern haben (wobei natürlich $\nu_1 + \nu_2 + \ldots + \nu_r = n$), eine Zerlegung von P in $(\nu_1 - 1) + (\nu_2 - 1) + \ldots + (\nu_r - 1) = n - r$ Transpositionen. Fügen wir ein Produkt von 2 gleichen Transpositionen an ($T\,T = E$, z. B. $(1\ 2)\,(1\ 2) = E$, vgl. Aufg. 18), so erhalten wir eine Zerlegung von P in $n - r + 2$ Transpositionen, durch Wiederholung Zerlegungen in $n - r + 2\sigma$ Transpositionen.

Wir müssen noch zeigen, daß umgekehrt jede mögliche Zerlegung von P in Transpositionen $n - r + 2\,\sigma$ Transpositionen enthält. Es sei also irgendeine Zerlegung von P in s Transpositionen $T_1, T_2, \ldots T_s$ vorgelegt. Dann können wir für s folgendermaßen mittels Satz 13 eine einschränkende Gleichung gewinnen:

$$P = T_1 T_2 \ldots T_{s-2} T_{s-1} T_s \text{ hat } r \text{ Zyklen}^{1})$$
$$P\,T_s = T_1 T_2 \ldots T_{s-2} T_{s-1} \text{ hat } r \pm 1 \text{ Zyklen}$$
$$P\,T_s T_{s-1} = T_1 T_2 \ldots T_{s-2} \text{ hat } r \pm 1 \pm 1 \text{ Zyklen}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$P\,T_s T_{s-1} \ldots T_2 T_1 = E \qquad \text{hat } r \pm 1 \pm 1 \ldots \pm 1 \text{ Zyklen.}$$

Von den s Gliedern ± 1 mögen σ den Wert -1, also $s - \sigma$ den Wert $+1$ haben; dann hat der letzte Ausdruck $r - \sigma + s - \sigma$ Zyklen. Anderseits ist er gleich der Einheitspermutation, $E = (1)\,(2) \ldots (n)$ hat aber gerade n Zyklen. Es ist daher

$$r - \sigma + s - \sigma = n \text{ oder } s = n - r + 2\,\sigma.$$

Beispiel:

$(1)\,(2\ 3\ 4) = (1\ 3)\,(2\ 4)\,(3\ 2)\,(1\ 2)\,(4\ 3)\,(2\ 4)$ hat 2 Zyklen

[1]) D. h. jede der beiden Seiten liefert r Zyklen mit lauter verschiedenen Ziffern, wenn wir nach Satz 10 die einzig mögliche Darstellung durch solche Zyklen bilden.

$(1)(2\ 3\ 4)(2\ 4) = (1\ 3)(2\ 4)(3\ 2)(1\ 2)(4\ 3)$
$=^{1})\ (1)(2\cdot 3)(4)$ hat $2+1$ Zyklen
$(1)(2\ 3\ 4)(2\ 4)(4\ 3) = (1\ 3)(2\ 4)(3\ 2)(1\ 2)$
$= (1)(2\ 4\ 3)$ hat $2+1-1$ Zyklen
$(1)(2\ 3\ 4)(2\ 4)(4\ 3)(1\ 2) = (1\ 3)(2\ 4)(3\ 2)$
$= (1\ 2\ 4\ 3)$ hat $2+1-1-1$ Zyklen
$(1)(2\ 3\ 4)(2\ 4)(4\ 3)(1\ 2)(3\ 2) = (1\ 3)(2\ 4)$
hat $2+1-1-1+1$ Zyklen
$(1)(2\ 3\ 4)(2\ 4)(4\ 3)(1\ 2)(3\ 2)(2\ 4) = (1\ 3)$
$= (1\ 3)(2)(4)$ hat $2+1-1-1+1+1$ Zyklen
$(1)(2\ 3\ 4)(2\ 4)(4\ 3)(1\ 2)(3\ 2)(2\ 4)(1\ 3)$
$= \mathrm{E} = (1)(2)(3)(4)$ hat $2+1-1-1+1+1+1$ Zyklen.

Es ist hier $n = 4$, $r = 2$, $\sigma = 2$, $s = 6$.

Die Permutationen mit gerader Transpositionenzahl nennt man „gerade“, die anderen „ungerade“ Permutationen.

Aufgabe 14. Man zerlege die Permutationen

$$A = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 4\,6\,3\,5\,1\,2\,7 \end{pmatrix}, \qquad B = \begin{pmatrix} 1\,2\ 3\,4\,5\,6\,7\,8\,9\,10 \\ 8\,5\,10\,9\,7\,2\,6\,4\,3\ 1 \end{pmatrix}$$

a) in Zyklen mit lauter verschiedenen Ziffern, b) in Transpositionen.

Aufgabe 15. Man bilde die Produkte $A\,B$ und $B\,A$ der beiden Permutationen in Aufgabe 14.

Aufgabe 16. Man berechne die sämtlichen Potenzen des Zyklus (1 2 3 4 5 6); welche Regel ergibt sich über die Anzahl der Potenzen und über ihre Bildung?

Aufgabe 17. Man berechne die Potenzen der Permu-

[1]) Durch Ausführung der Multiplikation in einem der beiden Ausdrücke nach der in § 4 angegebenen Methode.

tationen in Aufgabe 14. Wie viele verschiedene gibt es (welches ist die Ordnung dieser Permutationen)?

Aufgabe 18. Welches ist die inverse Permutation zum Zyklus $(1\ 2 \ldots n)$; was erhält man speziell für $n = 2$?

Aufgabe 19. Z_1 und Z_2 seien 2 Zyklen a) mit lauter verschiedenen, b) mit gemeinsamen Ziffern. Stimmen $Z_1 Z_2$ und $Z_2 Z_1$ überein? Man untersuche beide Fälle an Beispielen.

§ 20. Permutationsgruppen.

Über eine einzelne Permutation haben wir uns damit hinreichende Klarheit verschafft. Wir betrachten jetzt Systeme von Permutationen und verknüpfen die einzelnen Permutationen — wie schon bisher mehrmals geschehen — durch Nacheinander-Ausführen. Dabei ist es keine Einschränkung, wenn wir in ein System immer nur Permutationen von einer festen Anzahl n von Ziffern aufnehmen, denn jede Permutation von weniger Ziffern könnten wir durch Hinzufügen der fehlenden Ziffern als eingliedrige Zyklen zu einer solchen von n Ziffern ergänzen. Z. B. würden wir in dem System der beiden Permutationen (1 2 3) und (2 4) die erste durch (1 2 3) (4), die zweite durch (1) (3) (2 4) ersetzen.

Permutationen von n Ziffern und Systeme von solchen nennt man auch „vom Grade n“[1]).

Die erste Frage wird sein: Wie viele verschiedene Permutationen von n Ziffern (oder vom Grade n) gibt es überhaupt? Es gibt deren $1 \cdot 2 \cdot 3 \ldots n = n!$ (Samml. Göschen 53 § 15).

Eine Probe auf unsere Fig. I—V ergibt

[1]) Man verwechsle die Begriffe Grad und Ordnung nicht! Den ersten gibt es nur bei Permutationsgruppen, den zweiten bei jeder endlichen Gruppe.

Satz 15. Die $n!$ Permutationen von n Ziffern bilden eine Gruppe, die sog. „symmetrische Gruppe“ n^{ten} Grades $\mathfrak{S}_n$.

Satz 14 legt uns die weitere Frage vor: Wie viele gerade und wie viele ungerade Permutationen enthält die symmetrische Gruppe $\mathfrak{S}_n$? Aus Symmetriegründen vermuten wir

Satz 16. Die symmetrische Gruppe $\mathfrak{S}_n$ enthält $\frac{n!}{2}$ gerade und $\frac{n!}{2}$ ungerade Permutationen.

Einen einfachen Beweis liefert Satz 8. Wir multiplizieren jede Permutation unserer Gruppe mit einer und derselben Transposition, z. B. (1 2) — die in der Form (1 2)(3)(4)... selbst als Gruppenelement vorkommt —; dadurch erhalten wir wieder genau alle Permutationen der Gruppe, aus den geraden sind aber ungerade, aus den ungeraden gerade geworden. Also können diese nur gleich viele gewesen sein.

Bilden die beiden Teilsysteme, das System der $\frac{n!}{2}$ geraden und das System der $\frac{n!}{2}$ ungeraden Permutationen von n Ziffern ebenfalls je eine Gruppe? Schon allein Satz 1 und Eig. IV entscheiden nur zugunsten des ersten Systems:

Satz 17. Die $\frac{n!}{2}$ geraden Permutationen von n Ziffern bilden eine Gruppe, die sog. „alternierende Gruppe“ n^{ten} Grades.

Wir haben damit zur symmetrischen Gruppe $\mathfrak{S}_n$ eine Untergruppe von der Ordnung $\frac{n!}{2}$ gefunden. Die Aufsuchung aller sonstigen Untergruppen der symmetrischen Gruppe n^{ten} Grades ist ein sehr schwieriges Problem, von

dessen allgemeiner Lösung man noch weit entfernt ist. Allerdings läßt sich noch eine Reihe von Untergruppen mühelos gewinnen. (Siehe z. B. Aufgabe 21!)

Aufgabe 20. Man stelle die alternierende Gruppe der 4 Ziffern 1. 2, 3, 4 auf und vergleiche sie mit der Gruppe der Drehungen eines regulären Tetraeders (Beispiel 12), dessen Ecken man mit 1, 2, 3, 4 bezeichnet.

Aufgabe 21. Man bilde Untergruppen der symmetrischen Gruppe $\mathfrak{S}_5$, indem man diejenigen Elemente heraussucht, welche eine bestimmte Ziffer ungeändert lassen. Sodann sollen allgemeiner statt einer r Ziffern ungeändert bleiben. Endlich suche man das Verfahren noch weiter zu verallgemeinern.

§ 21. Kennzeichen für Gruppeneigenschaft.

Bevor wir weitere Untersuchungen über den Bau der Gruppen anstellen, wollen wir (in § 21 und 22) zwei allgemeine und für das folgende wichtige Fragen behandeln.

Die häufig auftretende Notwendigkeit, ein System auf Gruppeneigenschaft zu prüfen, legt uns die Frage nahe, ob wir nicht unsere Eig. I—V, wenigstens bei endlichen Gruppen, durch gleichwertige ersetzen können, deren Vorhandensein leichter zu entscheiden ist.

Wir haben schon bemerkt (§ 15), daß Eig. I u. III stets von selbst erfüllt sind, wenn das zu untersuchende System Teilkomplex einer größeren Gruppe ist. Da dies in den meisten Fällen zutrifft, brauchen wir für diese beiden Eigenschaften keinen Ersatz zu suchen. Eig. II, die wesentliche Gruppeneigenschaft, werden wir kaum umgehen können. So werden wir für Eig. IV u. V gleichwertige uchen.

Dazu betrachten wir die notwendigen Folgen aus diesen Eigenschaften und sehen zu, ob sie nicht vielleicht hinreichend sind. Eine solche Folge war in Satz 4 ausgesprochen. Denken wir uns also ein System $A_1, A_2, \ldots, A_n$, das die Eig. I, II, III und ferner die Eigenschaft hat, die wir IV′ nennen wollen, daß für alle Elemente

$$\text{IV}' \quad \begin{cases} \text{aus } A_i A_k = A_j A_l \text{ die Gleichung } A_k = A_l \text{ und} \\ \text{,, } A_k A_i = A_l A_j \text{ ,, ,, } A_k = A_l \text{ folgt.} \end{cases}$$

Folgt daraus vielleicht die Existenz eines Einheitselements und eines inversen Elements zu jedem? Für ein endliches n ist dies der Fall, wie wir beweisen wollen.

Bilden wir nach Eig. I

$$(1) \qquad A_i A_1,\ A_i A_2, \ldots, A_i A_n,$$

so sind dies wieder lauter Elemente des Systems nach Eig. II und zwar lauter verschiedene nach Eig. IV′ (vgl. den Beweis des Satzes 8), es sind also genau alle Elemente des Systems. Unter ihnen ist A_i, etwa

$$(2) \qquad A_i A_k = A_i; \text{ daraus folgt}$$

$$A_i A_k A_i = A_i A_i \text{ oder nach Eig. IV′}$$

$$(3) \qquad A_k A_i = A_i.$$

Nach Gleichung (2) und (3) hat A_k die Eigenschaft eines Einheitselements, wenigstens A_i gegenüber.

Wir zeigen, daß es sich auch jedem anderen Element A_j gegenüber so verhält, d. h. daß

$$A_j A_k = A_k A_j = A_j \text{ ist.}$$

A_j ist nämlich in der Reihe (1) enthalten, etwa

$$A_j = A_i A_l.$$

Multiplizieren wir nun Gleichung (3) hinten mit A_l, so wird sie

$A_k A_j = A_j$ und daraus folgt wie oben
$A_j A_k = A_j$.

A_k ist damit Einheitselement E unseres Systems.

Es muß in der Reihe (1) vorkommen, etwa

$$A_i A_m = E;$$

dann ist aber A_m das inverse Element zu dem (beliebigen) Element A_i. Wir haben somit bewiesen

Satz 18. Jedes endliche System, das die Eig. I, II, III, IV′ hat, ist eine Gruppe.

Der Satz ist insofern besonders wertvoll, als auch Eig. IV′ von selbst erfüllt ist, wenn das System Teilkomplex einer größeren Gruppe ist. Wir sprechen diese Tatsache aus als

Satz 19. Jeder Teilkomplex einer endlichen Gruppe, der die Eig. II hat, ist eine Gruppe.

Aufgabe 22 Man beweise: Ein Komplex von Permutationen, der die Eig. II hat, ist eine Gruppe.

§ 22. Darstellung der Komplexe und Gruppen bei allgemeinen Untersuchungen.

Die abstrakten Gruppen nach Satz 9 durch isomorphe Permutationsgruppen zu ersetzen, hat bei speziellen Untersuchungen über Gruppen niedriger Ordnung den Vorteil bequemer Einsicht in alle Beziehungen; bei Gruppen höherer Ordnung und bei allgemeinen Untersuchungen versagt die Methode gänzlich infolge ihrer außerordentlichen Weitläufigkeit. Wir werden auch keine andere einfache Darstellung finden, welche das innere Wesen der einzelnen Elemente direkt erkennen läßt, da eben die Kompliziertheit der Gruppen höherer Ordnung nicht zu beseitigen ist.

So müssen wir wieder zur Darstellung durch allgemeine Symbole zurückkehren. Verzichten wir hierbei schon darauf, in die Natur der Symbole hineinzusehen, so wollen wir doch den Vorteil einer recht knappen und übersichtlichen Ausdrucksweise. Wir werden die bereits in § 6 eingeführte Bezeichnungsweise weiter ausbauen und dabei auf die prägnante Schreibweise in Gleichungsform Wert legen, die sich schon wiederholt bei einzelnen Elementen bewährt hat.

Daß ein Komplex $\mathfrak{C}$ aus den Elementen $A_1, A_2, \ldots, A_n$ besteht, schreibt man

$$\mathfrak{C} = A_1 + A_2 + \ldots + A_n,$$

$$\text{speziell } \mathfrak{G} = A_1 + A_2 + \ldots + A_g,$$

$$\text{auch } \mathfrak{G} = \sum_{i=1}^{g} A_i.$$

Auf die Reihenfolge achtet man dabei nicht, z. B. auch $A_n + \ldots + A_2 + A_1$ bezeichnet man mit demselben $\mathfrak{C}$.

Daß ein Komplex $\mathfrak{C}$ aus den Teilkomplexen $\mathfrak{A}_1, \mathfrak{A}_2, \ldots \mathfrak{A}_m$ besteht, schreibt man

$$\mathfrak{C} = \mathfrak{A}_1 + \mathfrak{A}_2 + \ldots + \mathfrak{A}_m.$$

Dabei achtet man wieder nicht auf die Reihenfolge und auch nicht darauf, daß vielleicht die Komplexe rechts gemeinsame Elemente enthalten, so daß rechts dasselbe Element eigentlich öfter vorkommt. Nur verschiedene Elemente sollen wesentlich sein. Auf das Rechnen mit Komplexen hat dies einen Einfluß, den wir beim Rechnen mit Zahlen nicht gewöhnt sind; ist z. B.

$$\mathfrak{C} < \mathfrak{G}, \text{ so ist } \mathfrak{G} + \mathfrak{C} = \mathfrak{G},$$

$$\text{speziell } \mathfrak{G} + \mathfrak{G} = \mathfrak{G}.$$

Schon wiederholt (z. B. in Satz 8, Satz 16) waren wir veranlaßt, jedes Element eines Komplexes $\mathfrak{C}$ mit einem und demselben Element A zu multiplizieren. Den Komplex aller dabei entstehenden Elemente werden wir jetzt folgerichtig mit $\mathfrak{C}\,A$ bzw. $A\,\mathfrak{C}$ bezeichnen.

Z. B. schreibt sich nun Satz 8 in der einfachen Weise:

$$\mathfrak{G}\,A = A\,\mathfrak{G} = \mathfrak{G}\,, \text{ wenn } A < \mathfrak{G}$$

Endlich soll das Produkt $\mathfrak{C}\,\mathfrak{D}$ zweier Komplexe die Gesamtheit aller Elemente bedeuten, welche durch Multiplikation jedes Elements von $\mathfrak{C}$ mit jedem Element von $\mathfrak{D}$ — in dieser Reihenfolge — entsteht. Daß dabei vielleicht gleiche Elemente auftreten, lassen wir außer acht.

So ist z. B. $\mathfrak{C}\,\mathfrak{G} = \mathfrak{G}$, wenn $\mathfrak{C} < \mathfrak{G}$,
speziell $\mathfrak{G}\,\mathfrak{G} = \mathfrak{G}$.

Diese Beziehungen lassen sich beim gruppentheoretischen Rechnen in doppelter Weise verwenden. Einmal dazu, um aus einer Gruppe nach Bedarf einen Teilkomplex als Summanden oder Faktor herauszuheben (z. B. $\mathfrak{G}\,G$ statt $\mathfrak{G}$ zu schreiben), zweitens dazu, um gewisse Summanden oder Faktoren, die sozusagen von der Gruppe aufgesogen werden, wegzulassen (z. B. $\mathfrak{G}$ statt $\mathfrak{A}\,\mathfrak{G}$ zu schreiben).

Auch für die Addition von Komplexen gilt, wie bei der Addition von Zahlen. das assoziative und kommutative Gesetz; $\mathfrak{A} + \mathfrak{B}$ und $\mathfrak{B} + \mathfrak{A}$ oder $(\mathfrak{A} + \mathfrak{B}) + \mathfrak{C}$ und $\mathfrak{A} + (\mathfrak{B} + \mathfrak{C})$ enthalten die gleichen Elemente, auf die Reihenfolge achten wir ja nicht. Für die Multiplikation gilt wie bei einzelnen Elementen nur das assoziative Gesetz: $(\mathfrak{A}\,\mathfrak{B})\,\mathfrak{C} = \mathfrak{A}\,(\mathfrak{B}\,\mathfrak{C})$; jedes Element der linken Seite findet sich auch rechts und umgekehrt. Dagegen ist im allgemeinen $\mathfrak{A}\,\mathfrak{B} \neq \mathfrak{B}\,\mathfrak{A}$.

Aufgabe 23. Was bedeuten die Ausdrücke $X\mathfrak{A}Y$, $Y^{-1}\mathfrak{A}Z$, wenn $\mathfrak{A} = \sum_{i=1}^{a} A_i$? Wie läßt sich das Produkt der beiden Komplexe schreiben?

Aufgabe 24. Man gebe der Eig. II mittels der neuen Schreibweise eine andere Form.

Aufgabe 25 Man beweise: Ist $\mathfrak{C}$ Teilkomplex einer Gruppe, so ist $\mathfrak{C}\mathfrak{C} = \mathfrak{C}$ notwendige und hinreichende Bedingung dafür, daß $\mathfrak{C}$ selbst eine Gruppe ist.

§ 23. Weitere Erforschung des Baues der Gruppen; Zerlegung der Gruppen.

Wir setzen unseren in § 15 begonnenen Versuch fort, den geheimnisvollen Bau der Gruppen weiter zu entschleiern.

Zu jeder Gruppe kennen wir bereits Untergruppen. Die Gruppe

$$\mathfrak{A} = A_1 + A_2 + \ldots + A_a$$

sei nun eine Untergruppe der Gruppe $\mathfrak{G}$. Versuchen wir nach dem im vorigen Paragraphen Gelernten diese Gruppe $\mathfrak{A}$ wieder mit den Elementen von $\mathfrak{G}$ zu verknüpfen! Die Verknüpfung mit Elementen von $\mathfrak{A}$ liefert nichts Neues, $\mathfrak{A}A_i = \mathfrak{A}$.

Was aber enthält $\mathfrak{A}B$ für Elemente, wenn B ein Element von $\mathfrak{G}$ ist, welches nicht zu $\mathfrak{A}$ gehört? Der neue Komplex $\mathfrak{A}B$ deckt sich jedenfalls nicht mit $\mathfrak{A}$, weil er $EB = B$ enthält. Aber noch mehr. Wäre überhaupt eines seiner Elemente gleich einem Element von $\mathfrak{A}$, etwa

$$A_i B = A_k, \text{ so wäre } B = A_i^{-1} A_k,$$

was wegen der Gruppeneigenschaft von $\mathfrak{A}$ ein Element von $\mathfrak{A}$ vorstellt, gegen unsere Annahme. $\mathfrak{A}B$ enthält also

lauter neue Elemente (natürlich aus $\mathfrak{G}$) und zwar wieder a verschiedene, denn aus

$$A_i B = A_k B \text{ würde folgen } A_i = A_k.$$

Hätten wir statt B irgendein anderes Element aus $\mathfrak{A} B$, z. B. $A_i B$ gewählt, so wäre derselbe Komplex entstanden; es ist ja (§ 22)

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

Nun sei C ein Element von $\mathfrak{G}$, das weder $\mathfrak{A}$ noch $\mathfrak{A} B$ angehört. Wir bilden den Komplex $\mathfrak{A} C$ und finden auf dieselbe Weise wie eben, daß er wieder a verschiedene neue Elemente enthält. Wieder hätte uns jedes Element von $\mathfrak{A} C$ denselben Dienst getan.

So fahren wir fort, bis die ganze Gruppe $\mathfrak{G}$ erschöpft ist. Es können keine Elemente übrigbleiben, wir könnten ja mit ihnen durch Multiplikation mit $\mathfrak{A}$ noch Komplexe bilden.

Satz 20. Ist $\mathfrak{A}$ eine Untergruppe von $\mathfrak{G}$, so gibt es r Elemente $A, B, C, \ldots, S$, so daß

$$(1) \qquad \mathfrak{G} = \mathfrak{A} A + \mathfrak{A} B + \mathfrak{A} C + \ldots + \mathfrak{A} S.$$

Jeder Komplex der rechten Seite enthält a verschiedene Elemente, keine 2 Komplexe enthalten gemeinsame Elemente. Dieselbe Zerlegung entsteht, wenn statt A irgendein Element von $\mathfrak{A}$, statt B irgendein Element von $\mathfrak{A} B$ usw. gewählt wird.

Die Komplexe $\mathfrak{A} B, \mathfrak{A} C, \ldots$ nennen wir „Nebenkomplexe[1]) zur Untergruppe $\mathfrak{A}$", die Zerlegung heißt „Zerlegung nach dem Modul $\mathfrak{A}$", jedes mögliche

[1]) Man nennt sie auch „Nebengruppen", sie sind aber keine Gruppen.

System $A, B, \ldots, S$ ein „vollständiges Restsystem nach dem Modul $\mathfrak{A}$".

Jedes Element von $\mathfrak{G}$ kann als Element eines vollständigen Restsystems verwendet werden, weil jedes in einem der obigen Nebenkomplexe vorkommt.

Analog gibt es auch immer Zerlegungen

$$(2) \qquad \mathfrak{G} = A'\mathfrak{A} + B'\mathfrak{A} + C'\mathfrak{A} + \ldots + S'\mathfrak{A}.$$

Aufgabe 26. Man zerlege die symmetrische Gruppe von 3 Ziffern nach einem Modul a) der Ordnung 2, b) der Ordnung 3.

Aufgabe 27. Man beweise: Ist $A, B, C, \ldots$ ein vollständiges Restsystem für eine Zerlegung (1) nach Satz 20, so ist $A^{-1}, B^{-1}, C^{-1}, \ldots$ ein vollständiges Restsystem für eine Zerlegung (2).

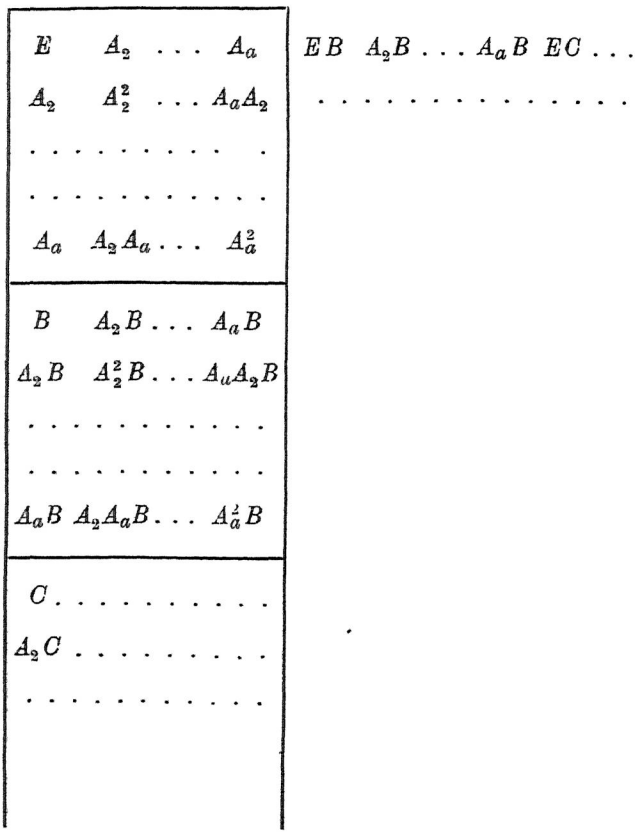
§ 24. Die Ordnung der Untergruppen und der Elemente.

Eine wichtige Folgerung aus dem vorigen erhalten wir, wenn wir in (1) oder (2) links und rechts die Elemente abzählen:

Satz 21 (Lagrange). $g = ar$ oder die Ordnung jeder Untergruppe von $\mathfrak{G}$ ist Teiler der Ordnung von $\mathfrak{G}$.

$\frac{g}{a} = r$ heißt „Index" der Untergruppe $\mathfrak{A}$ (in bezug auf $\mathfrak{G}$).

Einen guten Einblick in diese Zusammenhänge bekommen wir, wenn wir in unserer früheren Quadrat-Darstellung (§ 17) die durch Gleichung (1) gegebene Ordnung einhalten:



Jedes umrahmte Teilquadrat enthält die Elemente eines Teilkomplexes der Zerlegung (1), jedes a-mal; die einzelnen Zeilen eines solchen Teilquadrates enthalten dieselben Ele-

mente in verschiedenen Reihenfolgen, sowie sie sich bei den verschiedenen Restsystemen ergeben.

Denken wir daran, daß jedes Element einer Gruppe mit seinen verschiedenen Potenzen eine Untergruppe bildet (Satz 7), die Anzahl dieser Potenzen oder die Ordnung dieser Untergruppe aber Ordnung des Elements heißt, so erhalten wir mittels Satz 21 den

Satz 22. Die Ordnung jedes Elements einer Gruppe ist Teiler der Ordnung der Gruppe.

Damit ist die Natur der möglichen Elemente einer Gruppe von vorgegebener Ordnung g schon wesentlich beschränkt. Betrachten wir den besonderen Fall, daß $g = p$ eine Primzahl ist, so kann es außer E nur Elemente der Ordnung p geben und jedes erschöpft mit seinen p Potenzen bereits die ganze Gruppe.

Satz 23. Es gibt nur eine Gruppe von Primzahlordnung p, die zyklische Gruppe der Ordnung p.

Ist g keine Primzahl, so gibt es natürlich auch stets eine zyklische Gruppe der Ordnung g, die zyklische Permutation $(1\ 2\ 3 \ldots g)$ mit ihren Potenzen stellt ja eine solche vor; in den weitaus meisten Fällen gibt es aber noch andere Gruppen der Ordnung g.

§ 25. Aufbau der Gruppen.

Die gewonnenen Sätze geben uns ein Mittel an die Hand, um die Gruppen niedriger Ordnung synthetisch aus Elementen mit gewissen Verknüpfungseigenschaften herzustellen. Es folgt hierfür ein Beispiel, der Aufbau der Gruppen vierter Ordnung.

Wir bezeichnen die Elemente der gesuchten Gruppen mit G_1, G_2, G_3, G_4, und zwar seien sie nach wachsenden

Ordnungen geordnet, also $G_1 = E$, G_4 Element höchster Ordnung. Nach Satz 22 gibt es die Möglichkeiten:

I. G_4 hat die Ordnung 4,
II. G_4 „ „ „ 2.

I. G_4 mit seinen Potenzen liefert die zyklische Gruppe der Ordnung 4 ($G_4^2 = G_2, G_4^3 = G_3\ G_4^4 = E$).

II. $G_4^2 = E$; nach unserer Bezeichnung können dann auch G_3 und G_2 nur die Ordnung 2 haben: $G_3^2 = G_2^2 = E$.
$G_4 G_3$ ist unmöglich E (weil $G_4 G_4 = E$),
unmöglich G_4 (weil aus $G_4 G_3 = G_4$ folgte $G_3 = E$),
unmöglich G_3; also
$G_4 G_3 = G_2$; ebenso ergibt sich
$G_3 G_4 = G_2$; aus den letzten beiden Gleichungen erhält man durch Multiplikation mit G_4 bzw. G_3;

$$G_4 G_2 = G_3, \quad G_3 G_2 = G_4,$$
$$G_2 G_4 = G_3, \quad G_2 G_3 = G_4.$$

Nach § 17 ergibt sich das quadratische Schema:

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

Dabei ist vom assoziativen Gesetz bereits Gebrauch gemacht; daß es durchweg gilt, muß bestätigt werden, eine leichte, wenn auch etwas langwierige Arbeit. Wir erhalten eine Gruppe, die sog. „Vierergruppe“. Man stelle sie durch Permutationen dar!

Damit sind alle Möglichkeiten für eine Gruppe vierter Ordnung erschöpft.

Jedes System von Elementen einer Gruppe, durch deren (entsprechend oftmalige) Verknüpfung sich sämtliche Elemente der Gruppe darstellen lassen, heißt ein „System

erzeugender Elemente" der Gruppe. Man nennt die erzeugenden Elemente „unabhängig", wenn keines von ihnen entbehrlich, also bei Weglassung eines einzigen die Darstellung sämtlicher Gruppenelemente nicht mehr möglich ist.

Für die obige Gruppe I ist das Element G_4 (oder G_3) allein System unabhängiger erzeugender Elemente, für die Gruppe II das Paar G_4, G_3 (oder G_4, G_2 oder G_3, G_2).

Dem Leser ist sehr zu empfehlen, analog weitere Gruppen aufzubauen. An der folgenden Zusammenstellung mag er seine Resultate prüfen.

Ordnung g	1	2	3	4	5	6	7	8	9	10	11	12
Anzahl d. Gruppen der Ordnung g	1	1	1	2	1	2	1	5	2	2	1	5
Darunter Abelsche Gruppen[1])	1	1	1	2	1	1	1	3	2	1	1	2

§ 26. Vertauschbarkeit von Elementen; Transformation.

Wir haben bisher, um in den Bau einer Gruppe einzudringen, ein Element mit sich selbst oder ein Element mit einer Untergruppe verknüpft. Verbinden wir nun einmal zwei beliebige Elemente A, B einer Gruppe $\mathfrak{G}$! Wir erhalten die beiden Produkte $A\,B$ und $B\,A$.

Es gibt zwei Fälle:

$$1.\ A\,B = B\,A, \qquad 2.\ A\,B \neq B\,A.$$

Im Falle 1 heißen die Elemente A, B „vertauschbar" oder „kommutativ". Gilt diese Beziehung für alle möglichen Elementepaare der Gruppe, so heißt die Gruppe

[1]) Siehe den folgenden §

eine „vertauschbare", „kommutative" oder „Abelsche Gruppe". Wir denken uns im folgenden eine „nicht-Abelsche Gruppe" zugrunde gelegt, für eine Abelsche gelten die Ergebnisse zwar ebenfalls, werden aber trivial.

Die Beziehungen 1 und 2 können wir auch schreiben:

$$1'.\ B^{-1}AB = A, \qquad 2'.\ B^{-1}AB \neq A.$$

Die Bildung von $B^{-1}AB$ heißt man „Transformation von A mittels B", den Ausdruck $B^{-1}AB$ das „transformierte Element von A mittels B".

Wir wollen nun in unseren Beziehungen A festhalten, B dagegen die ganze Gruppe $\mathfrak{G}$ durchlaufen lassen und daher mit X bezeichnen. Wollen wir dabei die erste oder die zweite Form bevorzugen? Die zweite hat den Vorteil, daß X nur auf der linken Seite vorkommt. Wir entscheiden uns für sie und werden sehen, daß wir damit einen glücklichen Schritt tun, der uns gleich tief in das Wesen einer Gruppe hineinführt. Wir können unsere Aufgabe auch so auffassen: Es sollen alle möglichen transformierten Elemente von A mittels der Elemente von $\mathfrak{G}$ gebildet werden; welche Elemente entstehen dabei?

Beispiele: $\mathfrak{G}$ sei die symmetrische Gruppe von drei Ziffern; ihre Permutationen sind, durch Zyklen dargestellt:

$$A_1 = E,\ A_2 = (1\,2\,3),\ A_3 = (1\,3\,2),\ A_4 = (1\,2).$$
$$A_5 = (1\,3),\ A_6 = (2\,3).$$

Wählen wir $A = A_3$, so finden wir durch Ausrechnen

$$X^{-1}A_3X = A_3 \text{ für } X = A_1, A_2, A_3$$
$$X^{-1}A_3X = A_4 \text{ für } X = A_4, A_5, A_6.$$

Wählen wir $A = A_6$, so ergibt sich

$$X^{-1} A_6 X = A_6 \text{ für } X = A_1, A_6$$
$$X^{-1} A_6 X = A_5 \text{ für } X = A_2, A_4$$
$$X^{-1} A_6 X = A_4 \text{ für } X = A_3, A_5.$$

Wir vermuten aus den zwei Beispielen, wenn wir auf die Komplexe von Elementen X achten, die dieselben transformierten Elemente liefern:

1. Diejenigen Elemente X, welche A wieder in A transformieren. d. h. die mit A vertauschbaren Elemente der Gruppe $\mathfrak{G}$, bilden eine Gruppe $\mathfrak{B}_A$;

2. Diejenigen Elemente X, welche A in ein und dasselbe von A verschiedene Element transformieren, bilden einen Nebenkomplex zur Untergruppe $\mathfrak{B}_A$.

Suchen wir unsere Vermutungen allgemein zu beweisen!

Die erste Vermutung ist nach Satz 19 als richtig erwiesen, wenn Eig. II bestätigt ist. Sind also X_1, X_2 zwei beliebige Elemente von $\mathfrak{G}$, welche A wieder in A transformieren, d. h. für welche

(1) $X_1^{-1} A X_1 = A$ und (2) $X_2^{-1} A X_2 = A$,

so haben wir zu zeigen, daß auch für $X_1 X_2$ dasselbe gilt, also daß

$$(X_1 X_2)^{-1} A (X_1 X_2) = A \text{ oder } X_2^{-1} X_1^{-1} A X_1 X_2 = A.$$

Diese Gleichung ergibt sich aber tatsächlich, wenn wir das Element A in der linken Seite von (2) durch die linke Seite von (1) ersetzen.

Satz 24. Die mit irgendeinem festen Element A einer Gruppe vertauschbaren Gruppenelemente bilden eine Gruppe $\mathfrak{B}_A$.

Gehört A selbst zu $\mathfrak{B}_A$, welche sonstigen Elemente werden wir stets in $\mathfrak{B}_A$ vorfinden? Offenbar A mit seinen Potenzen, $\mathfrak{B}_A$ ist also zum mindesten die daraus bestehende Gruppe (vgl. die Beispiele). Das andere Extrem erhalten wir fur ein A, daß mit allen Elementen von $\mathfrak{G}$ vertauschbar ist, z. B. E; $\mathfrak{B}_E = \mathfrak{G}$.

Es kann in einer nicht-Abelschen Gruppe $\mathfrak{G}$ noch weitere mit allen Elementen von $\mathfrak{G}$ vertauschbare, also bei jeder Transformation unveränderliche Elemente geben[1]); man nennt sie „invariante" oder „isolierte Elemente".

Aufgabe 28. Man beweise: Sind die Elemente A, B einer Gruppe vertauschbar, so sind auch die Elemente A^r, B^s vertauschbar $(r, s \gtreqless 0)$

Aufgabe 29. Man transformiere eine Permutation mit einer anderen, etwa $(1\,2\,3)\,(4\,5)$ mit $\begin{pmatrix}1&2&3&4&5\\4&1&5&3&2\end{pmatrix}$; man vergleiche die Zyklen der ursprünglichen und der transformierten Permutation. Welche einfache Regel für die Transformation ergibt sich? Man beweise sie allgemein.

Aufgabe 30. Wie definiert man zweckmäßig gemäß § 22 die Vertauschbarkeit eines Elements mit einem Komplex oder die Vertauschbarkeit von zwei Komplexen? Man beweise: Die mit einem festen Komplex einer Gruppe vertauschbaren Gruppenelemente bilden eine Gruppe.

Aufgabe 31. Die invarianten Elemente einer Gruppe bilden eine Untergruppe, die sog. „Zentrale" der Gruppe.

§ 27. Fortsetzung, konjugierte Elemente.

Gehen wir nun zur zweiten Vermutung über! Nach der Definition von $\mathfrak{B}_A$ ist

[1]) Beispiel: $\mathfrak{G} = E + (1\,2\,3\,4) + (1\,3)\,(2\,4) + (1\,4\,3\,2) + (1\,3) + (1\,2)\,(3\,4) + (2\,4) + (1\,4)\,(2\,3)$, $A = (1\,3)\,(2\,4)$ ist invariant.

(1) $X^{-1} A X = A$ dann und nur dann, wenn $X < \mathfrak{B}_A$. Ist X' ein Element von $\mathfrak{G}$, das nicht $\mathfrak{B}_A$ angehört, so ist

(2) $$X'^{-1} A X' = A' (\neq A).$$

Wir wollen zeigen, daß ebenso wie X' alle Elemente des Nebenkomplexes $\mathfrak{B}_A X'$ das Element A' liefern und nur sie, d. h. daß

(3) $(X X')^{-1} A (X X') = A'$ dann und nur dann, wenn $X X' < \mathfrak{B}_A X'$.

In der Tat ergibt sich (3), wenn man in die linke Seite von (2) für A die linke Seite von (1) einträgt. Daß (3) auch nur für $X X' < \mathfrak{B}_A X'$ gilt, erkennen wir so: Ist

$$(X X')^{-1} A (X X') = A', \text{ so ist}$$
$$X'^{-1} (X^{-1} A X) X' = A' \text{ oder durch Vergleich mit (2)}$$
$$X^{-1} A X = A, \text{ d. h. } X < \mathfrak{B}_A \text{ oder}$$
$$X X' < \mathfrak{B}_A X'.$$

Es sei nun

$$X''^{-1} A X'' = A'' (\neq A, A');$$

dann ist analog

(4) $(X X'')^{-1} A X X'' = A''$ dann und nur dann, wenn $X X'' < \mathfrak{B}_A X''$.

So fahren wir fort, bis wir zu den Elementen des letzten Nebenkomplexes $\mathfrak{B}_A X^{\left(\frac{g}{v}-1\right)}$ kommen, die ein Element $A^{\left(\frac{g}{v}-1\right)}$ liefern (wo g, v die Ordnungen von $\mathfrak{G}$ bzw. $\mathfrak{B}_A$ sind). Fassen wir das Ergebnis nochmals zusammen:

Satz 25. Ist A ein festes Element der Gruppe $\mathfrak{G}$, und läßt man in $G^{-1} A G$ das Element G die ganze Gruppe $\mathfrak{G}$ durchlaufen, so entsteht:

solange G einer gewissen Untergruppe $\mathfrak{B}_A$ von $\mathfrak{G}$ angehört, wieder A,

solange G einem und demselben Nebenkomplex der Zerlegung von $\mathfrak{G}$ nach dieser Untergruppe,

$$\mathfrak{G} = \mathfrak{B}_A + \mathfrak{B}_A X' + \ldots + \mathfrak{B}_A X^{\left(\frac{g}{v}-1\right)},$$

angehört, ein und dasselbe Element und zwar für jeden Nebenkomplex ein anderes.

Im ganzen entstehen so $\frac{g}{v}$ *verschiedene Elemente* A, $A', \ldots, A^{\left(\frac{g}{v}-1\right)}$ durch Transformation aus A. Sie heißen die mit A in bezug auf die Gruppe $\mathfrak{G}$ „konjugierten Elemente".

§ 28. Fortsetzung, konjugierte Gruppen.

Hier erhebt sich die Frage: Was hätten wir erhalten, wenn wir statt von A von einem mit A konjugierten Elemente, etwa von A', ausgegangen wären? Anders ausgedrückt: Was ist $G^{-1}A'G$, wenn G die Gruppe $\mathfrak{G}$ durchläuft, wann ist es wieder A', welche Werte nimmt es sonst noch an?

Zur Beantwortung dieser Fragen gehen wir von Gleichung (3) aus, die wir auch so fassen können:

(3′) $Y^{-1}AY = A'$ dann und nur dann, wenn Y die Form $V_i X'$ hat, wo V_i ein beliebiges Element von $\mathfrak{B}_A$ ist. Um auf ein transformiertes Element von A' zu kommen, multiplizieren wir vorne mit Y, hinten mit Y^{-1} und erhalten, wenn wir noch die beiden Gleichungsseiten vertauschen,

$YA'Y^{-1} = A$ dann und nur dann, wenn $Y = V_i X'$, oder durch Einführung von Z^{-1} statt Y, um genau auf die Form eines transformierten Elements zu kommen,

(5) $Z^{-1}A'Z = A$ dann und nur dann, wenn $Z = (V_i X')^{-1}$

$= X'^{-1} V_i^{-1} = X'^{-1} V_k$, wo V_k wegen der Gruppeneigenschaft von $\mathfrak{B}_A$ wieder irgendein Element von $\mathfrak{B}_A$ ist.

Wir wollen aber rechts nicht A, sondern A' erhalten; dazu verhilft uns wieder Gleichung (3'); wir multiplizieren in (5) vorne mit Y^{-1}, hinten mit Y:

$Y^{-1}Z^{-1}A'ZY = Y^{-1}AY = A'$ dann und nur dann, wenn $Z = X'^{-1} V_k$, $Y = V_i X'$, wo V_k, V_i beliebige Elemente aus $\mathfrak{B}_A$.

$ZY = U$ gesetzt liefert

$U^{-1}A'U = A'$ dann und nur dann, wenn $U = X'^{-1}V_k V_i X'$ oder $U < X'^{-1}\mathfrak{B}_A X'$ (vgl. § 22, Aufgabe 23).

Die rechte Seite von (5) hätten wir, statt sie mittels der Gleichung (3') in A' zu verwandeln, mittels (4) in A'' verwandeln können; wir hätten erhalten

$W^{-1}A'W = A''$ dann und nur dann, wenn $W < X'^{-1}\mathfrak{B}_A X''$.

Man überzeugt sich so sukzessive, daß man bei Transformation von A' wieder alle $\frac{g}{v}$ Elemente $A', A'', \ldots, A$ erhält und zwar durch Transformation mit Elementen der Komplexe

(6) $\quad X'^{-1}\mathfrak{B}_A X',\ X'^{-1}\mathfrak{B}_A X'',\ \ldots,\ X'^{-1}\mathfrak{B}_A X.$

Betrachten wir zunächst den ersten dieser Komplexe näher! Zwei beliebige seiner Elemente sind $X'^{-1}V_i X'$ und $X'^{-1}V_k X'$, ihr Produkt ist

$X'^{-1}V_i X' X'^{-1} V_k X' = X'^{-1} V_i V_k X' = X'^{-1} V_l X'$.

Dies ist wieder ein Element aus $X'^{-1}\mathfrak{B}_A X'$, d. h. dieser

Komplex ist eine Gruppe. Sie heißt eine zu $\mathfrak{B}_A$ in bezug auf $\mathfrak{G}$ „konjugierte Gruppe".

Die übrigen Komplexe von (6) erweisen sich leicht als die Nebenkomplexe bei der Zerlegung von $\mathfrak{G}$ nach der Gruppe $X'^{-1}\,\mathfrak{B}_A\,X'$. Es ist nämlich etwa

$$X'^{-1}\,\mathfrak{B}_A\,X'' = X'^{-1}\,\mathfrak{B}_A\,X'\,(X'^{-1}\,X'');$$

hat also die Form eines Nebenkomplexes zu $X'^{-1}\,\mathfrak{B}_A\,X'$. Wäre ferner ein Element des Nebenkomplexes gleich einem Element der Gruppe, etwa

$$X'^{-1}\,V_i\,X'' = X'^{-1}\,V_k\,X', \text{ so wäre}$$
$$V_i\,X'' = V_k\,X',$$

während dies doch gerade Elemente aus verschiedenen Nebenkomplexen zu $\mathfrak{B}_A$ sind.

Wir haben also gefunden:

Wie man von A ausgehend durch Transformation mit je einem Element aus $\mathfrak{B}_A$ und dessen Nebenkomplexen die zu A konjugierten Elemente $A, A', \ldots, A^{\left(\frac{g}{v}-1\right)}$ erhält, erhält man von irgendeinem dieser Elemente, etwa A', aus durch Transformation mit je einem Element aus einer zu $\mathfrak{B}_A$ konjugierten Gruppe und ihren Nebenkomplexen wieder dieselben Elemente $A, A', \ldots. A^{\left(\frac{g}{v}-1\right)}$ (wenn auch in anderer Reihenfolge). Es ist also auch A zu A' konjugiert, A spielt keine besondere Rolle, alle Elemente A, $A', \ldots, A^{\left(\frac{g}{v}-1\right)}$ sind untereinander konjugiert. Man nennt sie eine „Klasse konjugierter Elemente".

Hinsichtlich der konjugierten Gruppen führen wir noch zwei Tatsachen an, deren leichte Beweise wir dem Leser überlassen:

1. Die Elemente der konjugierten Gruppe $X'^{-1}\,\mathfrak{B}_A\,X'$ entstehen aus den Elementen von $\mathfrak{B}_A$ nicht nur durch Transformation mit X', sondern mit jedem Element des Komplexes $\mathfrak{B}_A\,X'$; Transformation von $\mathfrak{B}_A$ mit je einem Element aus den Komplexen der Zerlegung von $\mathfrak{G}$ nach $\mathfrak{B}_A$ liefert alle konjugierten Gruppen zu $\mathfrak{B}_A$ (aber nicht notwendig lauter verschiedene).

2. Transformation von $X'^{-1}\,\mathfrak{B}_A\,X'$ mit je einem Element aus den Komplexen der Zerlegung von $\mathfrak{G}$ nach $X'^{-1}\mathfrak{B}_A\,X'$ liefert ebenfalls alle konjugierten Gruppen, darunter auch $\mathfrak{B}_A$. $\mathfrak{B}_A$ ist nicht bevorzugt, alle konjugierten Gruppen sind untereinander konjugiert.

Aufgabe 32. Man beweise: Die mit $\mathfrak{B}_A$ konjugierten Gruppen sind isomorph.

§ 29. Zusammenfassung der letzten Untersuchungen.

Wir stellen die Ergebnisse dieser Untersuchungen nochmals zusammen:

Satz 26. Durch Transformation irgendeines Elements einer Gruppe $\mathfrak{G}$ mit allen Elementen von $\mathfrak{G}$ erhält man eine Klasse konjugierter Elemente

$$A, A', \ldots, A^{(i)}, \ldots .$$

Alle diese Elemente sind untereinander konjugiert (entstehen durch Transformation auseinander).

Jedem Elemente $A^{(i)}$ dieser Klasse entspricht eine Gruppe $\mathfrak{B}_{A^{(i)}}$ der damit vertauschbaren Elemente von $\mathfrak{G}$. Alle diese Gruppen sind untereinander konjugiert (entstehen durch Transformation auseinander), und zwar:

Zerlegt man $\mathfrak{G}$ in Nebenkomplexe nach einer dieser Gruppen, etwa $\mathfrak{B}_{A^{(i)}}$, und wählt aus jedem Nebenkomplex je ein Element, so liefern diese Elemente

von $A^{(i)}$ aus durch Transformation die konjugierten Elemente,
von $\mathfrak{B}_{A^{(i)}}$ aus durch Transformation die konjugierten Gruppen
(diese letzteren brauchen aber nicht alle verschieden auszufallen).

Geht man bei der ganzen Betrachtung der §§ 26—28 von einem Element B aus, das nicht zur Klasse $A, A', \ldots$ gehört, so findet man eine neue Klasse konjugierter Elemente. Man kann so die ganze Gruppe $\mathfrak{G}$ in Klassen konjugierter Elemente einteilen. Jedes invariante Element bildet dabei eine Klasse für sich.

Die nebenstehende Tabelle gibt eine Übersicht der gefundenen Beziehungen für unser Beispiel der symmetrischen Permutationsgruppe von drei Ziffern.

Aufgabe 33. Man überlege sich die Ergebnisse der §§ 26—29 für den Fall, daß $\mathfrak{G}$ eine Abelsche Gruppe ist.

Aufgabe 34. Man stelle die nebenstehende Tabelle für eine andere Gruppe, etwa die Seite 64, Fußnote, angegebene Gruppe achter Ordnung auf.

§ 30. Invariante Untergruppe.

Die letzte Spalte in der nebenstehenden Tabelle zeigt uns, wenn wir $A_1 + A_2 + A_3$ kurz mit $\mathfrak{B}$ bezeichnen, daß z. B.

$$A_4^{-1}\,\mathfrak{B}\,A_4 = \mathfrak{B} \text{ ist, während}$$
$$A_4^{-1}\,A_2\,A_4 = A_3 \text{ ist, d. h.}$$

die Transformation mit A_4 reproduziert die Gruppe $\mathfrak{B}$ in ihrer Gesamtheit, ohne daß sie jedes einzelne Element reproduziert.

Elemente A der Gruppe $\mathfrak{G}$	Gruppe $\mathfrak{B}_A$ der mit A vertauschbaren Elemente	Komplexe der Zerlegung von $\mathfrak{G}$ nach $\mathfrak{B}_A$	Durch Transformation mit je einem Element aus jedem Komplex	
			aus A hervorgehend. Klasse konjugierter Elemente	aus $\mathfrak{B}_A$ hervorgehende konjugierte Gruppen
$A_1 = E$	$\mathfrak{G}$	$\mathfrak{G}$	E	$\mathfrak{G}$
$A_2 = (123)$	$A_1 + A_2 + A_3$	$(A_1 + A_2 + A_3) + (A_4 + A_5 + A_6)$	$A_2,\ A_3$	$A_1 + A_2 + A_3,\ A_1 + A_3 + A_2$
$A_3 = (132)$	$A_1 + A_2 + A_3$	$(A_1 + A_2 + A_3) + (A_4 + A_5 + A_6)$	$A_3,\ A_2$	$A_1 + A_2 + A_3,\ A_1 + A_3 + A_2$
$A_4 = (12)$	$A_1 + A_4$	$(A_1 + A_4) + (A_2 + A_5) + (A_3 + A_6)$	$A_4,\ A_6,\ A_5$	$A_1 + A_4,\ A_1 + A_6,\ A_1 + A_5$
$A_5 = (13)$	$A_1 + A_5$	$(A_1 + A_5) + (A_2 + A_6) + (A_3 + A_4)$	$A_5,\ A_4,\ A_6$	$A_1 + A_5,\ A_1 + A_4\ A_1 + A_6$
$A_6 = (23)$	$A_1 + A_6$	$(A_1 + A_6) + (A_2 + A_4) + (A_3 + A_5)$	$A_6,\ A_5,\ A_4$	$A_1 + A_6,\ A_1 + A_5,\ A_1 + A_4$

Verstehen wir unter der „Vertauschbarkeit einer Gruppe $\mathfrak{B}$ mit einem Element A“ die Beziehung $\mathfrak{B}A = A\mathfrak{B}$ (ohne Rücksicht auf die Reihenfolge der Elemente auf der linken und rechten Seite), so können wir auch sagen:

Eine Gruppe und ein Element können sehr wohl vertauschbar sein, ohne daß jedes einzelne Element der Gruppe mit dem Element vertauschbar ist.

Ist $\mathfrak{H}$ eine beliebige Untergruppe von $\mathfrak{G}$, so suchen wir jetzt in Analogie mit der Betrachtung des § 26 die mit $\mathfrak{H}$ vertauschbaren Elemente von $\mathfrak{G}$, d. h. die Elemente X, für welche gilt

$$\mathfrak{H}X = X\mathfrak{H} \text{ oder } X^{-1}\mathfrak{H}X = \mathfrak{H}.$$

Unser Beispiel bietet uns hier zwei extreme Fälle: Mit $\mathfrak{H} = A_1 + A_4$ ist nur $X = A_1$ oder A_4 vertauschbar, mit $\mathfrak{H} = A_1 + A_2 + A_3$ ist jedes Element von $\mathfrak{G}$ vertauschbar, $\mathfrak{H}$ ist gegenüber der Transformation mit jedem Element von $\mathfrak{G}$ invariant.

Diese Eigenschaft

$$\mathfrak{H}X = X\mathfrak{H} \text{ oder } X^{-1}\mathfrak{H}X = \mathfrak{H} \text{ für alle } X \text{ von } \mathfrak{G}$$

zeichnet die Untergruppe $\mathfrak{H}$ besonders aus, man nennt $\mathfrak{H}$ eine „ausgezeichnete“ oder „invariante Untergruppe“ von $\mathfrak{G}$, auch „Normalteiler“ von $\mathfrak{G}$. Wir schreiben in Fortführung unserer § 15 eingeführten Bezeichnungsweise $\mathfrak{H} \prec \mathfrak{G}$.

Während wir in den vorhergehenden Paragraphen den transformierenden Elementen X besondere Beachtung schenkten, wollen wir hier unser Augenmerk mehr auf die zu transformierende Gruppe $\mathfrak{H}$ richten. Wir haben eben in der invarianten Untergruppe einen sehr wichtigen Begriff entdeckt, den wir noch von einer anderen Seite beleuchten wollen.

Ist $\mathfrak{H}$ eine beliebige Untergruppe von $\mathfrak{G}$ und lassen wir in $X^{-1}\mathfrak{H}X$ das Element X die Elemente von $\mathfrak{G}$ durchlaufen, so wird im allgemeinen bald $\mathfrak{H}$, bald nicht $\mathfrak{H}$ entstehen. Unter allen Umständen aber ist der entstehende Komplex, wie uns der spezielle Fall des § 28 $\mathfrak{H} = \mathfrak{B}_A$ vermuten läßt, wieder eine Gruppe. Der Beweis hierfur verläuft wie im erwahnten speziellen Fall. Sind nämlich $X^{-1}H_1X$ und $X^{-1}H_2X$ zwei beliebige Elemente des Komplexes $X^{-1}\mathfrak{H}X$, so ist ihr Produkt

$$X^{-1}H_1X \cdot X^{-1}H_2X = X^{-1}H_1H_2X = X^{-1}H_3X,$$

also wieder ein Element desselben Komplexes, da $H_1H_2 = H_3$ wieder ein Element von $\mathfrak{H}$ ist.

Man nennt die aus $\mathfrak{H}$ auf diese Weise (durch Transformation mit je einem Element von $\mathfrak{G}$) entstehenden Gruppen allgemein „die konjugierten Gruppen zu $\mathfrak{H}$ in bezug auf $\mathfrak{G}$".

Wodurch ist nun der Fall der invarianten Untergruppe ausgezeichnet? $\mathfrak{H}$ ist invariante Untergruppe von $\mathfrak{G}$ dann und nur dann, wenn alle in bezug auf $\mathfrak{G}$ mit $\mathfrak{H}$ konjugierten Gruppen identisch sind mit $\mathfrak{H}$ selbst.

Aufgabe 35. Man beweise: Konjugierte Gruppen sind isomorph

§ 31. Beispiele invarianter Untergruppen.

Zur symmetrischen Permutationsgruppe $\mathfrak{G}$ von drei Ziffern sind außer $A_1 + A_2 + A_3$ in weiterem Sinne auch $\mathfrak{E}$ und $\mathfrak{G}$ invariante Untergruppen, dagegen nicht die übrigen Untergruppen wie $A_1 + A_4$.

Ist $\mathfrak{G}$ eine Abelsche Gruppe, so ist natürlich jede Untergruppe invariant. Z. B. wird man in der zyklischen Per-

mutationsgruppe von zwölf Ziffern leicht invariante Untergruppen der Ordnungen 2, 3, 4, 6 finden.

Die Gruppe $\mathfrak{G}$ der Tetraederdrehungen (Beispiel 12) enthält eine zur Vierergruppe isomorphe invariante Untergruppe. Diese besteht aus den drei letzten der in Beispiel 12, S. 17 angeführten Drehungen und dem In-Ruhelassen. Bezeichnet man wie in Aufgabe 20 die Ecken des Tetraeders mit 1, 2, 3, 4 und drückt die Drehungen durch die entsprechenden Eckenvertauschungen aus, so erhält die fragliche Untergruppe die Form einer Permutationsgruppe. Sie stellt sich in Zyklen geschrieben durch

$$(1)(2)(3)(4),\ (1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3)$$

dar, geht also tatsächlich in die in § 25 angegebene Vierergruppe über. Wir können nun leicht auch die Invarianz dieser Untergruppe bestätigen. Die Transformation mit jedem Element der Tetraedergruppe führt immer wieder auf die Untergruppe zurück; z. B. ergibt sich für das Element $(1\,2\,3)(4)$, dessen inverses Element $(1\,3\,2)(4)$ ist:

$$\begin{array}{llll}
(1\,3\,2)(4) & (1)(2)(3)(4) & (1\,2\,3)(4) = & (1)(2)(3)(4) \\
(1\,3\,2)(4) & (1\,2)(3\,4) & (1\,2\,3)(4) = & (1\,4)(2\,3) \\
(1\,3\,2)(4) & (1\,3)(2\,4) & (1\,2\,3)(4) = & (1\,2)(3\,4) \\
(1\,3\,2)(4) & (1\,4)(2\,3) & (1\,2\,3)(4) = & (1\,3)(2\,4).
\end{array}$$

Aufgabe 31 liefert eine allgemeine invariante Untergruppe, die Zentrale. Diese hat sogar die für den Begriff nicht notwendige Eigenschaft, daß sich beim Transformationsprozeß alle einzelnen Elemente reproduzieren. Z. B. hat die S. 64, Fußnote 1, angegebene Gruppe die invarianten Elemente E und $(1\,3)(2\,4)$; daß diese tatsächlich eine invariante Untergruppe bilden, läßt sich genau so bestätigen wie im letzten Beispiel.

Es gibt auch Gruppen, welche keine „eigentliche

(echte) invariante Untergruppe" besitzen, d. h. keine außer $\mathfrak{E}$ und sich selbst; man nennt solche Gruppen „einfach". Ein trivialer Fall einfacher Gruppen sind die Gruppen, welche überhaupt keine eigentliche Untergruppe besitzen (die Gruppen von Primzahlordnung). Interessant aber und selten sind die Fälle einfacher Gruppen, die wohl eigentliche Untergruppen, aber eben keine invarianten besitzen. Die alternierende Gruppe von fünf Ziffern (Ordnung 60) ist die Gruppe niedrigster Ordnung dieser Art.

Man beachte, daß sich die Invarianz einer Untergruppe $\mathfrak{H}$ immer auf eine bestimmte Gruppe $\mathfrak{G}$ bezieht. Wenn $\mathfrak{H}$ in $\mathfrak{G}$ invariant ist, braucht es in einer größeren Gruppe $\mathfrak{G}'$, die ihrerseits $\mathfrak{G}$ umfaßt, nicht invariant zu sein, aus $\mathfrak{H} \trianglelefteq \mathfrak{G}$ und $\mathfrak{G} < \mathfrak{G}'$ folgt nicht notwendig $\mathfrak{H} \trianglelefteq \mathfrak{G}'$, auch nicht, wenn $\mathfrak{G} \trianglelefteq \mathfrak{G}'$. Das folgende Beispiel beweist diese negative Behauptung:

$\mathfrak{G}'$ = alternierende Permutationsgruppe von vier Ziffern
$= E + (1\,2\,3)\,(4) + \ldots$
$\mathfrak{G}$ = Vierergruppe $= E + (1\,2)\,(3\,4) + (1\,3)\,(2\,4) + (1\,4)\,(2\,3)$
$\mathfrak{H}$ = Untergruppe der Ordnung $2 = E + (1\,2)\,(3\,4)$;
$\mathfrak{H}$ geht durch Transformation mit $(1\,2\,3)\,(4)$ nicht in sich, sondern in $E + (1\,4)\,(2\,3)$ über.

Dagegen gilt umgekehrt:

Satz 27. Bestehen zwischen den drei Gruppen $\mathfrak{H}, \mathfrak{G}, \mathfrak{G}'$ die Beziehungen

$$\mathfrak{H} < \mathfrak{G} < \mathfrak{G}' \text{ und } \mathfrak{H} \trianglelefteq \mathfrak{G}', \text{ so ist } \mathfrak{H} \trianglelefteq \mathfrak{G}.$$

Wenn nämlich $\mathfrak{H}$ mit allen Elementen von $\mathfrak{G}'$ vertauschbar ist, so ist es auch mit allen Elementen von $\mathfrak{G}$ vertauschbar, die ja einen Teil der Elemente von $\mathfrak{G}'$ ausmachen.

Aufgabe 36. Man beweise: Enthält eine Gruppe eine Untergruppe $\mathfrak{H}$ der Ordnung h und sonst keine Untergruppe dieser Ordnung, so ist $\mathfrak{H}$ invariante Untergruppe.

Aufgabe 37. Man beweise: Eine Untergruppe vom Index 2 ist immer invariant.

Aufgabe 38 Man beweise: Eine invariante Untergruppe der Ordnung 2 besteht immer aus zwei invarianten Elementen.

Aufgabe 39. Man beweise: Eine Untergruppe $\mathfrak{H} = H_1 + H_2 + \ldots + H_h$ der Gruppe $\mathfrak{G}$ ist dann und nur dann invariante Untergruppe von $\mathfrak{G}$, wenn für jedes Element G von $\mathfrak{G}$ und jedes Element H_i von $\mathfrak{H}$ eine Gleichung gilt

$$H_i G = G H_k \text{, wo } H_k < \mathfrak{H}.$$

§ 32. Fortsetzung der Untersuchung über die invariante Untergruppe; Faktorgruppe.

Daß die invariante Untergruppe ein grundlegender Begriff ist, zeigt sich bei Betrachtungen, welche sich bisher auf die allgemeinen Untergruppen bezogen.

Zerlegen wir nach Satz 20 $\mathfrak{G}$ nach dem Model $\mathfrak{H}$ unter der Voraussetzung $\mathfrak{H} < \mathfrak{G}$!

$$\mathfrak{G} = \mathfrak{H} + \mathfrak{H}G_2 + \mathfrak{H}G_3 + \ldots + \mathfrak{H}G_{\frac{g}{h}}.$$

Wegen der Invarianz der Untergruppe $\mathfrak{H}$ können wir dafür auch schreiben

$$\mathfrak{G} = \mathfrak{H} + G_2\mathfrak{H} + G_3\mathfrak{H} + \ldots + G_{\frac{g}{h}}\mathfrak{H};$$

jedes vollständige Restsystem rechts ist hier zugleich vollständiges Restsystem links und umgekehrt.

Bilden wir jetzt wie in § 24 die quadratische Darstellung der Gruppe $\mathfrak{G}$, wie sie uns die durch die obige Zerlegung

gegebene Ordnung vorschreibt, die Elemente von $\mathfrak{H}$ bezeichnen wir dabei mit $E, H_2, \ldots, H_h$. Was für Elemente stehen in jedem der Teilquadrate? Schreiben wir der besseren Übersicht halber die Zeilen der Teilquadrate mittels der Gruppenbezeichnung $\mathfrak{H}$, so erhalten wir:

$\mathfrak{H}$ $\mathfrak{H}H_2$ . . . $\mathfrak{H}H_h$	$\mathfrak{H}G_2$ $\mathfrak{H}G_2H_2$ . . . $\mathfrak{H}G_2H_h$	$\mathfrak{H}G_3$ $\mathfrak{H}G_3H_2$ . . . $\mathfrak{H}G_3H_h$	
$\mathfrak{H}G_2$ $\mathfrak{H}H_2G_2$ . . . $\mathfrak{H}H_hG_2$	$\mathfrak{H}G_2G_2$ $\mathfrak{H}G_2H_2G_2$ . . . $\mathfrak{H}G_2H_hG_2$		
$\mathfrak{H}G_3$ $\mathfrak{H}H_2G_3$ . . . $\mathfrak{H}H_hG_3$	$\mathfrak{H}G_2G_3$ $\mathfrak{H}G_2H_2G_3$ . . . $\mathfrak{H}G_2H_hG_3$		

Beachten wir die Invarianz der Untergruppe $\mathfrak{H}$, also die Beziehung $\mathfrak{H}G_i = G_i\mathfrak{H}$, und die spezielle Beziehung $\mathfrak{H}H_i = H_i\mathfrak{H} = \mathfrak{H}$, so erkennen wir die interessante Tatsache, daß hier alle h Zeilen jedes einzelnen Teilquadrates untereinander gleich sind (z. B.: $\mathfrak{H}G_2H_2G_2 = G_2\mathfrak{H}H_2G_2$

$= G_2 \mathfrak{H} G_2 = \mathfrak{H} G_2 G_2$). Schreiben wir diese nur noch einmal in jedes Teilquadrat, so wird unsere Darstellung:

$\mathfrak{H}$	$\mathfrak{H}G_2$	$\mathfrak{H}G_3$
$\mathfrak{H}G_2$	$\mathfrak{H}G_2G_2$	$\mathfrak{H}G_3G_2$
$\mathfrak{H}G_3$	$\mathfrak{H}G_2G_3$	

Was ist z. B. $\mathfrak{H} G_2 G_3$? $G_2 G_3$ ist wieder ein Element von $\mathfrak{G}$, also nach § 23 wieder ein Element aus einem Restsystem, d. h. $\mathfrak{H} G_2 G_3$ ist wieder einer der Komplexe der Zerlegung von $\mathfrak{G}$ nach dem Modul $\mathfrak{H}$. Ferner ist nach § 22

$$\mathfrak{H}G_2G_3 = \mathfrak{H}\mathfrak{H}G_2G_3 = \mathfrak{H}G_2\mathfrak{H}G_3 .$$

Fassen wir also jeden in einem Teilquadrat stehenden Komplex nur noch als ein Ganzes auf, so ist unsere letzte Darstellung wieder eine quadratische Darstellung nach Art der Darstellung einer Gruppe. Wir vermuten den

Satz 28. Ist $\mathfrak{H} \lessdot \mathfrak{G}$ und

$$(1) \qquad \mathfrak{G} = \mathfrak{H} + \mathfrak{H}G_2 + \ldots + \mathfrak{H}G_{\substack{g \\ h}}$$

eine Zerlegung von $\mathfrak{G}$ nach dem Modul $\mathfrak{H}$, so bilden die Komplexe dieser Zerlegung, jeder als ein einziges Element aufgefaßt, eine Gruppe. Die Verknüpfungsvorschrift ist dabei die Multiplikation von Komplexen nach § 22.

Nachweis der Eig. II:

$$\mathfrak{H}G_i \cdot \mathfrak{H}G_k = \mathfrak{H}\mathfrak{H}G_iG_k = \mathfrak{H}G_iG_k = \mathfrak{H}G_l.$$

Dies ist wieder ein Komplex unserer Zerlegung, G_l braucht nicht eines der Elemente $E, G_2, \ldots, G_{\frac{g}{h}}$ zu sein, es genügt, daß es irgendeinem der Komplexe. also überhaupt $\mathfrak{G}$ angehört (Satz 20).

Eig. III ist erfüllt, da, wie schon in § 22 betont, auch die Komplexmultiplikation assoziativ ist.

Nachweis der Eig. IV: Einheitselement ist $\mathfrak{H}$, da $\mathfrak{H} G_i \cdot \mathfrak{H} = \mathfrak{H} \cdot \mathfrak{H} G_i = \mathfrak{H} G_i$ für jedes G_i von $\mathfrak{G}$.

Nachweis der Eig. V: Zum Komplex $\mathfrak{H} G_i$ ist $\mathfrak{H} G_i^{-1}$ invers; denn

$$\mathfrak{H} G_i \mathfrak{H} G_i^{-1} = \mathfrak{H} \mathfrak{H} G_i G_i^{-1} = \mathfrak{H}.$$

Damit ist die Auffassung der Gruppe $\mathfrak{G}$ gewissermaßen in zwei Stufen zerlegt: Wir denken uns zunächst eine Gruppe der Ordnung $\frac{g}{h}$, deren Elemente ganze Komplexe sind; das Einheitselement ist dabei die Untergruppe $\mathfrak{H}$. Dann erst denken wir jeden Komplex in seine einzelnen Elemente aufgelöst.

Unsere doppelte Quadrateinteilung bringt die Verhältnisse übersichtlich zum Ausdruck. In der Schreibweise deutet man sie an, indem man die Gruppe der Komplexe in der Form $\frac{\mathfrak{G}}{\mathfrak{H}}$ schreibt; dann gilt symbolisch[1]) für die Gruppen

$$\mathfrak{G} = \frac{\mathfrak{G}}{\mathfrak{H}} \cdot \mathfrak{H}$$

analog der gewöhnlichen Beziehung zwischen ihren Ordnungen

[1]) Die Multiplikation ist dabei nicht im Sinne des § 22 gemeint, sondern mit $\mathfrak{H}$ Multiplizieren bedeutet hier Auflösen der vorher als Ganzes aufgefaßten Komplexe in ihre einzelnen Elemente.

$$g = \frac{g}{h} \cdot h .$$

$\frac{\mathfrak{G}}{\mathfrak{H}}$ heißt „Faktorgruppe", „Quotientengruppe" oder „komplementäre Gruppe" zu $\mathfrak{H}$ (in bezug auf $\mathfrak{G}$). Der früher (§ 24) schon eingeführte Index $\frac{g}{h}$ hat jetzt eine besondere Bedeutung erhalten.

Die rechte Seite der Gleichung (1) bedeutet die neue Gruppe oder die Gruppe $\mathfrak{G}$, je nachdem man die Komplexe als Ganzes auffaßt oder nicht. Wir wollen jedoch den ersteren Fall durch Einschließen der Komplexe in Klammern zum Ausdruck bringen:

$$\frac{\mathfrak{G}}{\mathfrak{H}} = (\mathfrak{H}) + (\mathfrak{H} G_2) + \ldots + (\mathfrak{H} G_{\frac{g}{h}}).$$

Man überlege sich nochmals, daß all dies nur für eine invariante Untergruppe $\mathfrak{H}$ einen Sinn hat!

§ 33. Maximale invariante Untergruppe; Kompositionsreihe.

Ist $\mathfrak{K}$ eine invariante Untergruppe von $\mathfrak{H}$[1]), so können wir $\mathfrak{H}$ die bisherige Rolle von $\mathfrak{G}$ spielen lassen und erhalten eine Faktorgruppe $\frac{\mathfrak{H}}{\mathfrak{K}}$ und die symbolische Gleichung

$$\mathfrak{H} = \frac{\mathfrak{H}}{\mathfrak{K}} \cdot \mathfrak{K}, \text{ also}$$

$$\mathfrak{G} = \frac{\mathfrak{G}}{\mathfrak{H}} \cdot \frac{\mathfrak{H}}{\mathfrak{K}} \cdot \mathfrak{K}.$$

So fahren wir fort. Wenn sich keine eigentliche in-

[1]) Man beachte, daß wir nicht $\mathfrak{K} \neq \mathfrak{G}$ verlangen

variante Untergruppe mehr findet, so ist doch immer noch die uneigentliche $\mathfrak{E}$ vorhanden, die Zerspaltung endet also immer mit $\mathfrak{E}$:

$$\mathfrak{G} = \frac{\mathfrak{G}}{\mathfrak{H}} \cdot \frac{\mathfrak{H}}{\mathfrak{K}} \cdot \frac{\mathfrak{K}}{\mathfrak{L}} \cdot \ldots \cdot \frac{\mathfrak{T}}{\mathfrak{E}} \cdot \mathfrak{E}.$$

Unser Verfahren ist aber noch sehr unvollkommen. Wir haben die invariante Untergruppe immer ganz willkürlich gewählt; vielleicht hätte es z. B. zwischen $\mathfrak{G}$ und $\mathfrak{H}$ noch eine invariante Untergruppe $\mathfrak{H}'$ gegeben, die ihrerseits $\mathfrak{H}$ als invariante Untergruppe enthalten hätte.

Wir definieren: Eine invariante Untergruppe $\mathfrak{H}$ der Gruppe $\mathfrak{G}$ heißt „größte oder maximale invariante Untergruppe“ von $\mathfrak{G}$ — wir schreiben $\mathfrak{H} \text{ m}\!<\!\mathfrak{G}$ —, wenn es keine invariante Untergruppe $\mathfrak{H}'$ von $\mathfrak{G}$ gibt, welche $\mathfrak{H}$ enthält. Solche maximale invariante Untergruppen kann es natürlich mehrere, auch von verschiedener Ordnung geben. Z. B. hat die zyklische Gruppe der Ordnung 6 größte invariante Untergruppen von den Ordnungen 2 und 3.

Verwendet man bei der obigen Zerspaltung der Gruppe $\mathfrak{G}$ durchweg nur maximale invariante Untergruppen, ist also $\mathfrak{H} \text{ m}\!<\!\mathfrak{G}$, $\mathfrak{K} \text{ m}\!<\!\mathfrak{H}$ usw., so nennt man die Reihe von Gruppen

$$\mathfrak{G}, \mathfrak{H}, \mathfrak{K}, \ldots, \mathfrak{T}, \mathfrak{E}$$

eine „Kompositionsreihe“ der Gruppe $\mathfrak{G}$. Auch solcher kann es mehrere geben, es wird aber ein interessanter Satz einen gewissen einheitlichen Charakter aller dieser aufdecken.

Aufgabe 40. $\mathfrak{G}$ sei 1. die zyklische Permutationsgruppe der Ordnung 12, 2. die alternierende Gruppe von

vier Ziffern, 3. die symmetrische Gruppe von drei Ziffern. Man suche a) die sämtlichen invarianten Untergruppen, b) die Kompositionsreihen von $\mathfrak{G}$, c) die aus je zwei aufeinander folgenden Gruppen der Kompositionsreihen gebildeten Faktorgruppen.

§ 34. Durchschnitt zweier Untergruppen.

Wir werden die im letzten Paragraphen gewonnene Zerspaltung einer Gruppe weiter untersuchen (§ 39), müssen uns aber vorher (§ 34—38) noch eine genauere Kenntnis der Beziehungen zwischen den Untergruppen einer Gruppe erwerben und dabei besonders auf die invarianten Untergruppen achten.

$\mathfrak{A}$ und $\mathfrak{B}$ seien zwei Untergruppen einer Gruppe $\mathfrak{G}$; wir fragen nach weiteren Untergruppen von $\mathfrak{G}$, etwa:

1. Gibt es eine Untergruppe von $\mathfrak{G}$, welche sowohl in $\mathfrak{A}$ als $\mathfrak{B}$ enthalten ist?

2. Gibt es eine Untergruppe von $\mathfrak{G}$, welche sowohl $\mathfrak{A}$ als $\mathfrak{B}$ enthält?

1. Ist D_1 ein Element, das in $\mathfrak{A}$ und in $\mathfrak{B}$ enthalten ist, D_2 ein ebensolches, so ist auch $D_1 D_2$ in $\mathfrak{A}$ und in $\mathfrak{B}$ enthalten wegen der Gruppeneigenschaft von $\mathfrak{A}$ und $\mathfrak{B}$, wir haben (nach Satz 19) den

Satz 29. Die gemeinsamen Elemente zweier Untergruppen $\mathfrak{A}$, $\mathfrak{B}$ einer Gruppe $\mathfrak{G}$ bilden eine Gruppe $\mathfrak{D}$; man nennt sie den „Durchschnitt“ von $\mathfrak{A}$ und $\mathfrak{B}$, geschrieben $\mathfrak{D} = (\mathfrak{A}, \mathfrak{B})$.

$\mathfrak{D}$ existiert immer, zum mindesten ist ja $\mathfrak{E}$ zwei Gruppen gemeinsam.

Das Analoge gilt für jede endliche Anzahl von Unterruppen einer Gruppe.

Beispiel: $\mathfrak{G}$ sei die zyklische Permutationsgruppe der Ordnung 12

$$\mathfrak{G} = E + G + G^2 + G^3 + \ldots\ldots\ldots\ldots + G^{11},$$
$$\mathfrak{A} = E + G^2 + G^4 + G^6 + G^8 + G^{10},$$
$$\mathfrak{B} = E + G^3 + G^6 + G^9,$$
$$\mathfrak{D} = E + G^6.$$

Aufgabe 41. Man beweise: Der Durchschnitt $\mathfrak{D}$ aller mit einer Untergruppe $\mathfrak{H}$ einer Gruppe $\mathfrak{G}$ konjugierten Gruppen ist eine invariante Untergruppe von $\mathfrak{G}$.

Man überlege sich den besonderen Fall $\mathfrak{H} \prec \mathfrak{G}$.

§ 35. Produkt zweier Untergruppen.

Zur Beantwortung der Frage 2 des vorigen Paragraphen liegt es nahe, die Komplexe $\mathfrak{A}\,\mathfrak{B}$ oder $\mathfrak{B}\,\mathfrak{A}$ zu bilden. Aber wir wissen noch nicht, wie viele verschiedene Elemente jeder dieser Komplexe enthält und ob er eine Gruppe bildet.

Die Multiplikation jedes Elements A von $\mathfrak{A}$ mit jedem Element B von $\mathfrak{B}$ ergibt $a\,b$ Elemente des Komplexes $\mathfrak{A}\,\mathfrak{B}$, darunter können aber gleiche sein. Es seien mit einem beliebigen Produkt $A_1 B_1$ genau $r-1$ weitere Produkte gleich, etwa (bei geeigneter Bezeichnung)

$$(1) \qquad A_1 B_1 = A_2 B_2 = \ldots\ldots = A_r B_r;$$

bilden wir nun, um auf andere gleiche Produkte zu kommen,

$$(2) \qquad A A_1 B_1 B = A A_2 B_2 B = \ldots\ldots = A A_r B_r B$$

und lassen A die Gruppe $\mathfrak{A}$, B die Gruppe $\mathfrak{B}$ durchlaufen, so durchläuft nach Satz 8 auch $A A_1$ und $B_1 B$ diese Gruppen, $(A A_1)(B_1 B)$ stellt also sukzessive jedes mögliche Produkt aus einem Element von $\mathfrak{A}$ mit einem Element von $\mathfrak{B}$ vor, und Beziehung (2) liefert zu jedem sol-

chen Produkt $r-1$ weitere gleiche. Es kann auch zu keinem Produkt mehr als $r-1$ gleiche geben, da wir sonst, statt von (1) von einer solchen Gleichheit von mehr als r Produkten ausgehend, auch zu $A_1 B_1$ mehr als $r-1$ gleiche fänden. Die Anzahl der verschiedenen Elemente von $\mathfrak{A}\,\mathfrak{B}$ ist also $\frac{a\,b}{r}$.

Ein einfaches Mittel führt uns nun zu den Elementen von $\mathfrak{B}\,\mathfrak{A}$. Wir denken an die Eig. V von $\mathfrak{G}$, $\mathfrak{A}$, $\mathfrak{B}$ und an Satz 3 und bilden zu jedem Glied der Beziehung (1) das inverse:

$$(A_1 B_1)^{-1} = (A_2 B_2)^{-1} = \ldots = (A_r B_r)^{-1} \text{ oder}$$
$$B_1^{-1} A_1^{-1} = B_2^{-1} A_2^{-1} = \ldots = B_r^{-1} A_r^{-1}.$$

$B_1^{-1} A_1^{-1}$ ist irgendein Element von $\mathfrak{B}\,\mathfrak{A}$, und wir haben $r-1$ weitere gleiche und auch nicht mehr; sonst kämen wir, nochmals durch Inversion, in Widerspruch mit (1).

Nun schließen wir weiter wie oben und kommen zu

Satz 30. Sind $\mathfrak{A}$. $\mathfrak{B}$ Untergruppen einer Gruppe $\mathfrak{G}$, so haben die Komplexe $\mathfrak{A}\,\mathfrak{B}$ und $\mathfrak{B}\,\mathfrak{A}$ die gleiche Anzahl von verschiedenen Elementen, und zwar ist diese ein Teiler von $a\ b$.

Wir fragen uns: Wann ist $\mathfrak{B}\,\mathfrak{A} = \mathfrak{A}\,\mathfrak{B}$? Dazu muß jedes beliebige Element $B_i A_k$ mit einem Element $A_r B_s$ übereinstimmen, also
$B_i A_k = A_r B_s$, wo B_i Gruppe $\mathfrak{B}$, A_k Gruppe $\mathfrak{A}$ durchläuft.
Dann muß sein, indem wir wie oben verfahren,
$A\,B_i A_k\,B = A\,A_r B_s\,B$, wo A Gruppe $\mathfrak{A}$, B Gruppe $\mathfrak{B}$ durchläuft.
Oder

$$(A\,B_i)(A_k\,B) = (A\,A_r)(B_s\,B).$$

Jeder der beiden Faktoren der linken Seite durchläuft nun alle *möglichen Produkte von* $\mathfrak{A}\,\mathfrak{B}$, die rechte Seite aber hat wieder die Form eines solchen Produktes, etwa $A_n B_m$; d. h. nach Satz 19 $\mathfrak{A}\,\mathfrak{B}$ ist eine Gruppe.

Ist umgekehrt $\mathfrak{A}\,\mathfrak{B}$ eine Gruppe, so enthält es (für $B = E$) die Gruppe $\mathfrak{A}$ und ebenso $\mathfrak{B}$ und damit auch $\mathfrak{B}\,\mathfrak{A}$; wegen der im letzten Satz nachgewiesenen gleichen Elementezahl ist dann $\mathfrak{A}\,\mathfrak{B} = \mathfrak{B}\,\mathfrak{A}$.

Wie haben damit einen neuen Satz gefunden, der uns zugleich die aufgeworfene zweite Frage soweit beantwortet, als es für das folgende nötig ist.

Satz 31. Sind $\mathfrak{A}, \mathfrak{B}$ Untergruppen einer Gruppe $\mathfrak{G}$, so ist $\mathfrak{A}\,\mathfrak{B}$ (und $\mathfrak{B}\,\mathfrak{A}$) dann und nur dann eine Gruppe, wenn $\mathfrak{A}\,\mathfrak{B} = \mathfrak{B}\,\mathfrak{A}$ ist.

Beispiel: $\mathfrak{G}$ sei die symmetrische Gruppe von vier Ziffern $\mathfrak{S}_4$, $\mathfrak{A}$ die Gruppe $E + (1\,2)\,(3)\,(4)$, $\mathfrak{B}_1$ die Gruppe $E + (1\,2\,3)\,(4) + (1\,3\,2)\,(4)$, $\mathfrak{B}_2$ die zyklische Gruppe von vier Ziffern. Dann ist $\mathfrak{A}\,\mathfrak{B}_1 = \mathfrak{B}_1\,\mathfrak{A}$ und tatsächlich eine Gruppe ($\simeq \mathfrak{S}_3$); dagegen ist $\mathfrak{A}\,\mathfrak{B}_2 \neq \mathfrak{B}_2\,\mathfrak{A}$ und weder $\mathfrak{A}\,\mathfrak{B}_2$ noch $\mathfrak{B}_2\,\mathfrak{A}$ eine Gruppe.

Aufgabe 42. Wie weit existiert ein gruppentheoretisches Analogon zu dem zahlentheoretischen Satz: Die kleinste Zahl, in der zwei Zahlen a, b ohne Rest aufgehen, ist $\frac{a\,b}{d}$, wo d der größte gemeinsame Teiler von a und b ist?

§ 36. Durchschnitt und Produkt zweier invarianter Untergruppen.

Lassen wir nun $\mathfrak{A}$ und $\mathfrak{B}$ invariante Untergruppen von $\mathfrak{G}$ sein, so liefern unsere Betrachtungen eine Reihe von Sätzen, die wieder die Wichtigkeit des Begriffes der invarianten Untergruppe dartun.

1. Nach Voraussetzung ist

$$G^{-1}\mathfrak{A}G = \mathfrak{A} \text{ und } G^{-1}\mathfrak{B}G = \mathfrak{B} \text{ für jedes } G \text{ von } \mathfrak{G}.$$

Es sei nun D ein beliebiges Element des Durchschnittes $\mathfrak{D}$ von $\mathfrak{A}$ und $\mathfrak{B}$, also D in $\mathfrak{A}$ und in $\mathfrak{B}$ enthalten. Dann ist $G^{-1}DG$ in $G^{-1}\mathfrak{A}G$ und $G^{-1}\mathfrak{B}G$, d. h. in $\mathfrak{A}$ und $\mathfrak{B}$ enthalten und damit in $\mathfrak{D}$. Da dies für jedes Element D von $\mathfrak{D}$ gilt, können wir auch sagen: $G^{-1}\mathfrak{D}G$ ist in $\mathfrak{D}$ enthalten. Wegen der gleichen Ordnung kann aber dann nur $G^{-1}\mathfrak{D}G = \mathfrak{D}$ sein, und dies bedeutet $\mathfrak{D} \text{ }_1\!\!<\!\!\cdot\, \mathfrak{G}$.

Um so mehr ist dann $\mathfrak{D} \text{ }_1\!\!<\!\!\cdot\, \mathfrak{A}$ und $\mathfrak{D} \text{ }_1\!\!<\!\!\cdot\, \mathfrak{B}$ (Satz 27).

Wir können das Gefundene mit unseren Bezeichnungen kurz so ausdrücken:

Satz 32. Ist $\mathfrak{A} \text{ }_1\!\!<\!\!\cdot\, \mathfrak{G}$, $\mathfrak{B} \text{ }_1\!\!<\!\!\cdot\, \mathfrak{G}$, $\mathfrak{D} = (\mathfrak{A}, \mathfrak{B})$, so ist $\mathfrak{D} \text{ }_1\!\!<\!\!\cdot\, \mathfrak{A}$, $\mathfrak{D} \text{ }_1\!\!<\!\!\cdot\, \mathfrak{B}$, $\mathfrak{D} \text{ }_1\!\!<\!\!\cdot\, \mathfrak{G}$.

2. Hier benützen wir die Voraussetzung der Invarianz in der Form

$$\mathfrak{A}G = G\mathfrak{A} \text{ und } \mathfrak{B}G = G\mathfrak{B} \text{ für jedes } G \text{ von } \mathfrak{G}.$$

A fortiori ist dann $\mathfrak{A}B = B\mathfrak{A}$ für jedes B von $\mathfrak{B}$ oder $\mathfrak{A}\mathfrak{B} = \mathfrak{B}\mathfrak{A}$, also nach Satz 31 $\mathfrak{A}\mathfrak{B}$ eine Gruppe. Weiterhin folgt aus der Voraussetzung $\mathfrak{A}\mathfrak{B}G = \mathfrak{A}G\mathfrak{B} = G\mathfrak{A}\mathfrak{B}$ für jedes G von $\mathfrak{G}$, d. h. $\mathfrak{A}\mathfrak{B} \text{ }_1\!\!\leqq\!\!\cdot\, \mathfrak{G}$.

Endlich ist nach Voraussetzung und Satz 27

$$\mathfrak{A} \text{ }_1\!\!<\!\!\cdot\, \mathfrak{A}\mathfrak{B} \text{ und } \mathfrak{B} \text{ }_1\!\!<\!\!\cdot\, \mathfrak{A}\mathfrak{B}.$$

Fassen wir unsere Ergebnisse zusammen:

Satz 33. Ist $\mathfrak{A} \text{ }_1\!\!<\!\!\cdot\, \mathfrak{G}$, $\mathfrak{B} \text{ }_1\!\!<\!\!\cdot\, \mathfrak{G}$, so ist $\mathfrak{A}\mathfrak{B}\,(= \mathfrak{B}\mathfrak{A})$ eine Gruppe und zwar

$$\mathfrak{A}\mathfrak{B} \text{ }_1\!\!\leqq\!\!\cdot\, \mathfrak{G}\,, \quad \mathfrak{A} \text{ }_1\!\!<\!\!\cdot\, \mathfrak{A}\mathfrak{B}\,, \quad \mathfrak{B} \text{ }_1\!\!<\!\!\cdot\, \mathfrak{A}\mathfrak{B}\,.$$

Aufgabe 43. Man beweise: Sind $\mathfrak{A}$ und $\mathfrak{B}$ Untergruppen

einer Gruppe $\mathfrak{G}$, und ist eine der beiden invariante Untergruppe, so ist $\mathfrak{A}\,\mathfrak{B}$ eine Gruppe und gleich $\mathfrak{B}\,\mathfrak{A}$.

§ 37. Beziehungen zwischen zwei Faktorgruppen.

Die Gruppe $\mathfrak{A}$ (und ebenso $\mathfrak{B}$) des vorigen Paragraphen stellt eine Gruppe vor, welche invariante Untergruppe von zwei Gruppen $\mathfrak{A}\,\mathfrak{B}$ und $\mathfrak{G}$ ist, von denen die erste wieder invariante Untergruppe der zweiten ist.

Wir schalten hier eine für später wichtige Untersuchung ein, indem wir allgemeiner annehmen, daß die mittlere Gruppe nicht notwendig die Produktform $\mathfrak{A}\,\mathfrak{B}$ hat, sondern daß

$$\mathfrak{A} \subset \mathfrak{G},\quad \mathfrak{A} \subset \mathfrak{H},\quad \mathfrak{H} \subset \mathfrak{G}.$$

Es liegt nahe, nach der Beziehung zwischen den Faktorgruppen $\frac{\mathfrak{H}}{\mathfrak{A}}$ und $\frac{\mathfrak{G}}{\mathfrak{A}}$ zu fragen, die sich — beide aus Nebenkomplexen zu $\mathfrak{A}$ bestehend — wohl unschwer vergleichen lassen. Es ist bei entsprechender Bezeichnung

$$(1)\qquad \frac{\mathfrak{H}}{\mathfrak{A}} = (\mathfrak{A}) + (\mathfrak{A}\,H_2) + \ldots + (\mathfrak{A}\,\underset{a}{H_h})$$

$$(2)\qquad \frac{\mathfrak{G}}{\mathfrak{A}} = (\mathfrak{A}) + (\mathfrak{A}\,G_2) + \ldots\ldots\ldots + (\mathfrak{A}\,\underset{a}{G_g}).$$

Da jedes Element H_i in $\mathfrak{G}$ enthalten ist, so sind die Komplexe von (1) sämtlich unter den Komplexen von (2) enthalten, es ist also

$$\frac{\mathfrak{H}}{\mathfrak{A}} \subset \frac{\mathfrak{G}}{\mathfrak{A}}.$$

Aus Analogiegründen vermuten wir auch die Invarianz der Untergruppe $\frac{\mathfrak{H}}{\mathfrak{A}}$ in bezug auf $\frac{\mathfrak{G}}{\mathfrak{A}}$.

In der Tat gilt (vgl. Aufgabe 39) für das Produkt aus irgendeinem Element der ersten und irgendeinem Element der zweiten Gruppe

$$\mathfrak{A}H_i \cdot \mathfrak{A}G_k = \mathfrak{A}\mathfrak{A}H_iG_k = (\text{weil } \mathfrak{H} \trianglelefteq \mathfrak{G})$$
$$\mathfrak{A}\mathfrak{A}G_kH_l = \mathfrak{A}G_k \cdot \mathfrak{A}H_l;$$

dies bedeutet nach Aufgabe 39 die vermutete Invarianz.

Beachten wir noch, daß nach Satz 27 aus der Beziehung $\mathfrak{A} \trianglelefteq \mathfrak{G}$ die Beziehung $\mathfrak{A} \trianglelefteq \mathfrak{H}$ von selbst folgt, wenn nur $\mathfrak{A} < \mathfrak{H}$ ist, so haben wir insgesamt dieses Ergebnis:

Satz 34. Ist $\mathfrak{A} \trianglelefteq \mathfrak{G}$, $\mathfrak{A} < \mathfrak{H}$, $\mathfrak{H} \trianglelefteq \mathfrak{G}$, so ist $\frac{\mathfrak{H}}{\mathfrak{A}} \trianglelefteq \frac{\mathfrak{G}}{\mathfrak{A}}$.

Wir wollen auch die folgende Umkehrung beweisen:

Satz 35. Ist $\mathfrak{A} \trianglelefteq \mathfrak{G}$, $\mathfrak{A} \trianglelefteq \mathfrak{H}$, $\frac{\mathfrak{H}}{\mathfrak{A}} \trianglelefteq \frac{\mathfrak{G}}{\mathfrak{A}}$, so ist $\mathfrak{H} \trianglelefteq \mathfrak{G}$.

Die beiden Faktorgruppen seien wieder durch (1) und (2) vorgestellt. Nach Voraussetzung ist jeder Komplex von (1) als Ganzes aufgefaßt unter den Komplexen von (2) enthalten; dasselbe gilt natürlich noch, wenn wir jeden Komplex in seine einzelnen Elemente aufgelöst denken; es ist also $\mathfrak{H} < \mathfrak{G}$.

Da $\frac{\mathfrak{H}}{\mathfrak{A}}$ invariante Untergruppe von $\frac{\mathfrak{G}}{\mathfrak{A}}$ ist, gilt (vgl. Aufgabe 39)

$\mathfrak{A}G_k\mathfrak{A}H_i = \mathfrak{A}H_l\mathfrak{A}G_k$ für jedes $\mathfrak{A}G_k$ von (2) und jedes $\mathfrak{A}H_i$ von (1), d. h. bei entsprechender Wahl der vollständigen Restsysteme für jedes G_k von $\mathfrak{G}$ und jedes H_i von $\mathfrak{H}$; $\mathfrak{A}H_l$ ist wieder ein Komplex von (1).

Wir formen die Gleichung zwischen den Komplexen mittels der Voraussetzungen so um, daß wir eine entsprechende Gleichung zwischen den einzelnen Elementen von $\mathfrak{H}$ und $\mathfrak{G}$ daraus gewinnen können:

$$\mathfrak{A}\,\mathfrak{A}\,G_k\,H_i = \mathfrak{A}\,\mathfrak{A}\,H_l\,G_k\,,$$
$$\mathfrak{A}\,G_k\,H_i = \mathfrak{A}\,H_l\,G_k\,;$$

unter den Elementen der linken Seite ist $E\,G_k\,H_i$ enthalten, ihm ist ein Element der rechten Seite gleich, etwa

$$E\,G_k\,H_i = A\,H_l\,G_k\,.$$

$A\,H_l$ ist (da $\mathfrak{A} < \mathfrak{H}$) ein Element H von $\mathfrak{H}$, also

$$G_k\,H_i = H\,G_k\,.$$

Dies bedeutet, weil G_k jedes Element von $\mathfrak{G}$, H_i jedes Element von $\mathfrak{H}$ sein kann, daß $\mathfrak{H} \text{ }_1\!< \mathfrak{G}$.

§ 38. Durchschnitt und Produkt zweier maximaler invarianter Untergruppen; Isomorphismus von Faktorgruppen.

Wir kehren jetzt wieder zurück zur Betrachtung zweier Untergruppen $\mathfrak{A}$, $\mathfrak{B}$ einer Gruppe $\mathfrak{G}$, ihrem Durchschnitt $\mathfrak{D} = (\mathfrak{A}, \mathfrak{B})$ und ihrem Produkt $\mathfrak{A}\,\mathfrak{B}$. Die Fälle, daß $\mathfrak{A}$ und $\mathfrak{B}$ beliebige oder daß $\mathfrak{A}$ und $\mathfrak{B}$ invariante Untergruppen sind, sind schon erledigt.

Wir lassen jetzt $\mathfrak{A}$ und $\mathfrak{B}$ maximale invariante Untergruppen von $\mathfrak{G}$ sein. Unser Beispiel § 34 entspricht bereits diesen Voraussetzungen. Die tatsächliche Bildung von $\mathfrak{A}\,\mathfrak{B}$ ergibt hier $\mathfrak{A}\,\mathfrak{B} = \mathfrak{G}$. Es gilt allgemein:

Satz 36. Ist $\mathfrak{A} \text{ }_m\!< \mathfrak{G}$. $\mathfrak{B} \text{ }_m\!< \mathfrak{G}$, so ist $\mathfrak{A}\,\mathfrak{B} = \mathfrak{G}$.

Nach Satz 33 ist nämlich $\mathfrak{A}\,\mathfrak{B} \text{ }_1\!\leqq \mathfrak{G}$; anderseits ist aber $\mathfrak{A}$ maximale invariante Untergruppe von $\mathfrak{G}$, es kann also nur sein

$$\mathfrak{A}\,\mathfrak{B} = \mathfrak{A} \text{ oder } = \mathfrak{G};$$

ganz ebenso ergibt sich wegen $\mathfrak{B} \text{ }_m\!< \mathfrak{G}$

$$\mathfrak{A}\,\mathfrak{B} = \mathfrak{B} \text{ oder } = \mathfrak{G};$$

dies sagt zusammen aus: $\mathfrak{A}\,\mathfrak{B} = \mathfrak{G}$.

Wenden wir uns nun zur Untersuchung des Durch-

schnitts $\mathfrak{D} = (\mathfrak{A}, \mathfrak{B})$! Es gilt Satz 32 und damit existieren folgende Faktorgruppen, die wir zunächst an unserem Beispiel (§ 34) verfolgen wollen:

$$\frac{\mathfrak{G}}{\mathfrak{A}} = (\mathfrak{A}) + (\mathfrak{A}G) \qquad \frac{\mathfrak{G}}{\mathfrak{B}} = (\mathfrak{B}) + (\mathfrak{B}G) + (\mathfrak{B}G^2)$$
$$= (\mathfrak{A}) + (\mathfrak{A}G^3) \qquad = (\mathfrak{B}) + (\mathfrak{B}G^2) + (\mathfrak{B}G^4)$$
$$\frac{\mathfrak{A}}{\mathfrak{D}} = (\mathfrak{D}) + (\mathfrak{D}G^2) + (\mathfrak{D}G^4) \qquad \frac{\mathfrak{B}}{\mathfrak{D}} = (\mathfrak{D}) + (\mathfrak{D}G^3).$$

Wir bemerken eine große Ähnlichkeit zwischen den über Kreuz stehenden Gruppen. Sie sind von gleicher Ordnung und können mit denselben Restsystemen aufgebaut werden. Diese Eigenschaften führen uns zu der Vermutung:

Satz 37. Ist $\mathfrak{A} \text{ m}< \mathfrak{G}$, $\mathfrak{B} \text{ m}< \mathfrak{G}$, $\mathfrak{D} = (\mathfrak{A}, \mathfrak{B})$, so ist

$$\frac{\mathfrak{G}}{\mathfrak{A}} \cong \frac{\mathfrak{B}}{\mathfrak{D}} \text{ und } \frac{\mathfrak{G}}{\mathfrak{B}} \cong \frac{\mathfrak{A}}{\mathfrak{D}}; \; g\,d = a\,b\,.$$

Zum Beweis etwa der ersten der beiden analogen Behauptungen suchen wir wie im Beispiel für beide Gruppen Komplexzerlegungen mit gleichen Restsystemen zu gewinnen. Es sei die Zerlegung von $\mathfrak{B}$ nach dem Modul $\mathfrak{D}$

$$(1) \qquad \mathfrak{B} = \mathfrak{D} + \mathfrak{D}B_2 + \ldots + \mathfrak{D}B_{\frac{b}{d}}.$$

Um daraus $\mathfrak{G}$ herzustellen, multiplizieren wir nach Satz 36 mit $\mathfrak{A}$:

$$\mathfrak{A}\mathfrak{B} = \mathfrak{A}\mathfrak{D} + \mathfrak{A}\mathfrak{D}B_2 + \ldots + \mathfrak{A}\mathfrak{D}B_{\frac{b}{d}} \quad \text{oder}$$

$$(2) \qquad \mathfrak{G} = \mathfrak{A} + \mathfrak{A}B_2 + \ldots + \mathfrak{A}B_{\frac{b}{d}}.$$

Rechts stehen lauter Komplexe nach dem Modul $\mathfrak{A}$; wir haben die Zerlegung von $\mathfrak{G}$ nach dem Modul $\mathfrak{A}$ vor uns, wenn die Komplexe alle verschieden sind. Dies trifft zu; wäre in (2)

$$\mathfrak{A}\, B_i = \mathfrak{A}\, B_k\,, \text{ so wäre}$$

(3) $$B_i = A\, B_k \text{ oder}$$

$$A = B_i\, B_k^{-1} < \mathfrak{B}\,;$$

wegen $A < \mathfrak{A}$ hätten wir damit

$$A < \mathfrak{D}.$$

Aus (3) erhielten wir dann

$$\mathfrak{D}\, B_i = \mathfrak{D}\, A\, B_k = \mathfrak{D}\, B_k\,,$$

d. h. in (1) wären ebenfalls zwei Komplexe gleich.

Wir erkennen nun leicht den behaupteten Isomorphismus, indem wir in (1) und (2) entsprechende Komplexe einander zuordnen. Aus

(4) $$\mathfrak{D}\, B_i \cdot \mathfrak{D}\, B_k = \mathfrak{D}\, B_l$$

folgt durch Multiplikation mit $\mathfrak{A}$

$$\begin{aligned} \mathfrak{A}\,\mathfrak{D}\, B_i\,\mathfrak{D}\, B_k &= \mathfrak{A}\,\mathfrak{D}\, B_l \\ \mathfrak{A}\, B_i\,\mathfrak{D}\, B_k &= \mathfrak{A}\, B_l \\ B_i\,\mathfrak{A}\,\mathfrak{D}\, B_k &= \mathfrak{A}\, B_l \\ B_i\,\mathfrak{A}\, B_k &= \mathfrak{A}\, B_l\,, \end{aligned}$$

daraus durch nochmalige Multiplikation mit $\mathfrak{A}$

(5) $$\mathfrak{A}\, B_i \cdot \mathfrak{A}\, B_k = \mathfrak{A} \cdot B_l\,.$$

Fassen wir jetzt jeden Komplex als Ganzes auf, so stellen die rechten Seiten von (1) und (2) die Faktorgruppen $\frac{\mathfrak{B}}{\mathfrak{D}}$ und $\frac{\mathfrak{G}}{\mathfrak{A}}$, die Gleichungen (4) und (5) ihren Isomorphismus vor.

Der Isomorphismus von $\frac{\mathfrak{G}}{\mathfrak{A}}$ und $\frac{\mathfrak{B}}{\mathfrak{D}}$ bedeutet den völlig analogen Bau der beiden Gruppen. Nun ist nach Voraussetzung $\mathfrak{A}$ maximale invariante Untergruppe von $\mathfrak{G}$; es

scheint also sehr wahrscheinlich, daß dasselbe für die invariante Untergruppe $\mathfrak{D}$ der Gruppe $\mathfrak{B}$ gilt, nämlich daß $\mathfrak{D} \text{ m}< \mathfrak{B}$.

Um dies zu untersuchen, müssen wir uns fragen: Was bedeutet der besondere Fall $\mathfrak{A} \text{ m}< \mathfrak{G}$ für die Faktorgruppe $\frac{\mathfrak{G}}{\mathfrak{A}}$ für eine Besonderheit?

Ist $\mathfrak{A}$ nicht maximale invariante (wohl aber invariante) Untergruppe von $\mathfrak{G}$, sondern gibt es eine Gruppe $\mathfrak{H}$, so daß

$$\mathfrak{A} < \mathfrak{H} \text{ und } \mathfrak{H} \text{ i}< \mathfrak{G},$$

so ist nach Satz 34

$$\frac{\mathfrak{H}}{\mathfrak{A}} \text{ i}< \frac{\mathfrak{G}}{\mathfrak{A}};$$

wir haben damit eine invariante Untergruppe der Faktorgruppe $\frac{\mathfrak{G}}{\mathfrak{A}}$ gefunden, diese ist jedenfalls nicht einfach (§ 31).

Umgekehrt: Ist $\frac{\mathfrak{G}}{\mathfrak{A}}$ nicht einfach, existiert also eine Faktorgruppe $\frac{\mathfrak{H}}{\mathfrak{A}}$, so daß

$$\frac{\mathfrak{H}}{\mathfrak{A}} \text{ i}< \frac{\mathfrak{G}}{\mathfrak{A}},$$

so ist nach Satz 35

$$\mathfrak{H} \text{ i}< \mathfrak{G},$$

also $\mathfrak{A}$ nicht maximale invariante Untergruppe von $\mathfrak{G}$. Wir können demnach die letzte Frage beantworten durch den

Satz 38. Ist überhaupt $\mathfrak{A} \text{ i}< \mathfrak{G}$, so ist $\mathfrak{A} \text{ m}< \mathfrak{G}$ dann und nur dann, wenn $\frac{\mathfrak{G}}{\mathfrak{A}}$ einfach ist.

Hiermit ist die besondere Beziehung $\mathfrak{A} \text{ m}< \mathfrak{G}$ in eine

Besonderheit der Faktorgruppe $\frac{\mathfrak{G}}{\mathfrak{A}}$ übersetzt; diese überträgt sich natürlich infolge des Isomorphismus auf die Faktorgruppe $\frac{\mathfrak{B}}{\mathfrak{D}}$, d. h. $\frac{\mathfrak{B}}{\mathfrak{D}}$ ist einfach; und damit ist $\mathfrak{D} \text{ m}< \mathfrak{B}$, also unsere obige Vermutung bestätigt.

Wir können jetzt Satz 37 noch folgendermaßen ergänzen:

Satz 39. Ist $\mathfrak{A} \text{ m}< \mathfrak{G}$, $\mathfrak{B} \text{ m}< \mathfrak{G}$, $\mathfrak{D} = (\mathfrak{A}, \mathfrak{B})$, so ist $\mathfrak{D} \text{ m}< \mathfrak{A}$, $\mathfrak{D} \text{ m}< \mathfrak{B}$,

$$\frac{\mathfrak{G}}{\mathfrak{A}} \cong \frac{\mathfrak{B}}{\mathfrak{D}}, \quad \frac{\mathfrak{G}}{\mathfrak{B}} \cong \frac{\mathfrak{A}}{\mathfrak{D}}; \; g\,d = a\,b.$$

Aufgabe 44. Man verfolge den Satz 39 an folgendem Beispiel:

$\mathfrak{A}$ besteht aus der Permutation (1 2 3 4) (5 6 7 8) und ihren Potenzen,

$\mathfrak{B}$ besteht aus der Permutation (1 5 3 7) (2 8 4 6) und ihren Potenzen,

$\mathfrak{G}$ besteht aus den 8 verschiedenen Permutationen von $\mathfrak{A}$ $\mathfrak{B}$ (sog. „Quaternionengruppe").

§ 39. Der Satz von Jordan-Hölder über die Kompositionsreihen.

Nach den Vorbereitungen der letzten Paragraphen setzen wir die Untersuchung der Kompositionsreihen fort.

Betrachten wir zunächst die Kompositionsreihen der Gruppen niedrigster Ordnung!

Die Gruppe $\mathfrak{G}$ der Ordnung 2 hat natürlich nur die Kompositionsreihe $\mathfrak{G}$, $\mathfrak{E}$; ebenso

die Gruppe der Ordnung 3.

Von den beiden Gruppen der Ordnung 4 (§ 25) hat die zyklische Gruppe

$$\mathfrak{G} = E + (1\,2\,3\,4) + (1\,3)\,(2\,4) + (1\,4\,3\,2)$$

nur die Kompositionsreihe $\mathfrak{G}$, $E + (1\,3)\,(2\,4)$, $\mathfrak{E}$.

Die Vierergruppe

$$\mathfrak{G} = E + (1\,2)\,(3\,4) + (1\,3)\,(2\,4) + (1\,4)\,(2\,3)$$

hat, wenn $E + (1\,2)\,(3\,4) = \mathfrak{A}_1$, $E + (1\,3)\,(2\,4) = \mathfrak{A}_2$, $E + (1\,4)\,(2\,3) = \mathfrak{A}_3$ gesetzt wird, die drei Kompositionsreihen

$$\mathfrak{G},\ \mathfrak{A}_1,\ \mathfrak{E};\quad \mathfrak{G},\ \mathfrak{A}_2,\ \mathfrak{E};\quad \mathfrak{G},\ \mathfrak{A}_3,\ \mathfrak{E};$$

die zugehörigen Faktorgruppen bzw. Indizes sind:

$$\frac{\mathfrak{G}}{\mathfrak{A}_1},\ \frac{\mathfrak{A}_1}{\mathfrak{E}};\qquad \frac{\mathfrak{G}}{\mathfrak{A}_2},\ \frac{\mathfrak{A}_2}{\mathfrak{E}};\qquad \frac{\mathfrak{G}}{\mathfrak{A}_3},\ \frac{\mathfrak{A}_3}{\mathfrak{E}};$$

$$2,\ 2;\qquad 2,\ 2;\qquad 2,\ 2.$$

Die Gruppe $\mathfrak{G}$ der Ordnung 5 hat nur die Kompositionsreihe $\mathfrak{G}$, $\mathfrak{E}$.

Von den beiden Gruppen der Ordnung 6 hat die zyklische Gruppe

$$\mathfrak{G} = E + (1\,2\,3\,4\,5\,6) + (1\,3\,5)\,(2\,4\,6) + (1\,4)\,(2\,5)\,(3\,6) + (1\,5\,3)\,(2\,6\,4) + (1\,6\,5\,4\,3\,2),$$

wenn $E + (1\,3\,5)\,(2\,4\,6) + (1\,5\,3)\,(2\,6\,4) = \mathfrak{A}$, $E + (1\,4)\,(2\,5)\,(3\,6) = \mathfrak{B}$

gesetzt wird, die beiden Kompositionsreihen

$$\mathfrak{G},\ \mathfrak{A},\ \mathfrak{E};\quad \mathfrak{G},\ \mathfrak{B},\ \mathfrak{E}$$

mit den Faktorgruppen $\dfrac{\mathfrak{G}}{\mathfrak{A}},\ \dfrac{\mathfrak{A}}{\mathfrak{E}};\qquad \dfrac{\mathfrak{G}}{\mathfrak{B}},\ \dfrac{\mathfrak{B}}{\mathfrak{E}}.$

und den Indizes $2,\ 3;\qquad 3,\ 2.$

Bezüglich der zweiten Gruppe der Ordnung 6 (symmetrische Gruppe von drei Elementen) und weiterer Beispiele vergleiche man Aufgabe 40.

Diese Beispiele zeigen uns in allen Fällen, wo zwei oder mehr Kompositionsreihen vorhanden sind:

Sämtliche Kompositionsreihen einer Gruppe enthalten gleich viele Glieder. Und wenn wir die Faktorgruppen betrachten: Zu jeder Faktorgruppe einer Reihe finden wir eine solche gleicher Ordnung in jeder anderen Reihe, zu jedem Index also einen gleichen Index. Ja noch mehr: Wir können je zwei isomorphe Faktorgruppen zusammenordnen (natürlich mit Änderung der Reihenfolge). In dieser letzten Beziehung sind die vorher angeführten enthalten.

Wir versuchen den allgemeinen Beweis durch vollständige Induktion in bezug auf die Ordnung g.

Es sei also $\mathfrak{G}$ eine Gruppe der Ordnung g; zwei ihrer Kompositionsreihen seien

I. $\mathfrak{G}, \mathfrak{A}_1, \mathfrak{A}_2, \ldots\ldots, \mathfrak{A}_n = \mathfrak{E}$ mit den Faktorgruppen $\frac{\mathfrak{G}}{\mathfrak{A}_1}, \frac{\mathfrak{A}_1}{\mathfrak{A}_2}, \ldots, \frac{\mathfrak{A}_{n-1}}{\mathfrak{E}}$,

II. $\mathfrak{G}, \mathfrak{B}_1, \mathfrak{B}_2, \ldots\ldots, \mathfrak{B}_m = \mathfrak{E}$ mit den Faktorgruppen $\frac{\mathfrak{G}}{\mathfrak{B}_1}, \frac{\mathfrak{B}_1}{\mathfrak{B}_2}, \ldots, \frac{\mathfrak{B}_{m-1}}{\mathfrak{E}}$.

Wir nehmen an: Alle Gruppen, deren Ordnung kleiner als g ist, besitzen paarweise isomorphe Faktorgruppen. Dann haben wir für die Kompositionsreihen I und II unserer Gruppe $\mathfrak{G}$ mit Ordnung g dasselbe nachzuweisen.

1. Fall. $\mathfrak{B}_1 = \mathfrak{A}_1$. Weil die Ordnung von $\mathfrak{A}_1$ und $\mathfrak{B}_1$ kleiner als g ist, gilt unsere Behauptung nach Annahme für $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{E}$ und für $\mathfrak{B}_1 = \mathfrak{A}_1, \mathfrak{B}_2, \ldots, \mathfrak{E}$ und damit auch für I und II, weil hier noch $\frac{\mathfrak{G}}{\mathfrak{A}_1} \cong \frac{\mathfrak{G}}{\mathfrak{B}_1}$ ist.

2. Fall. $\mathfrak{B}_1 \neq \mathfrak{A}_1$. $\mathfrak{A}_1$ und $\mathfrak{B}_1$ sind also zwei verschiedene maximale invariante Untergruppen von $\mathfrak{G}$. Satz 39 gibt

uns dann eine maximale invariante Untergruppe von $\mathfrak{A}_1$ und $\mathfrak{B}_1$, nämlich $\mathfrak{D} = (\mathfrak{A}_1, \mathfrak{B}_1)$, so daß wir durch weitere Zerspaltung von $\mathfrak{D}$ noch die Kompositionsreihen erhalten:

III. $\mathfrak{G}, \mathfrak{A}_1, \mathfrak{D}, \mathfrak{D}_1, \ldots\ldots, \mathfrak{D}_l = \mathfrak{E}$ mit den Faktorgruppen $\frac{\mathfrak{G}}{\mathfrak{A}_1}, \frac{\mathfrak{A}_1}{\mathfrak{D}}, \frac{\mathfrak{D}}{\mathfrak{D}_1}, \ldots, \frac{\mathfrak{D}_{l-1}}{\mathfrak{E}}$,

IV. $\mathfrak{G}, \mathfrak{B}_1, \mathfrak{D}, \mathfrak{D}_1, \ldots\ldots, \mathfrak{D}_l = \mathfrak{E}$ mit den Faktorgruppen $\frac{\mathfrak{G}}{\mathfrak{B}_1}, \frac{\mathfrak{B}_1}{\mathfrak{D}}, \frac{\mathfrak{D}}{\mathfrak{D}_1}, \ldots \frac{\mathfrak{D}_{l-1}}{\mathfrak{E}}$.

Satz 39 sagt uns noch, daß die ersten beiden Faktorgruppen von III und IV bei Zuordnung über Kreuz isomorph sind. Da die folgenden Faktorgruppen übereinstimmen, haben wir:

Die Faktorgruppen III sind paarweise isomorph den Faktorgruppen IV.

Jetzt vergleichen wir I und III. Es gilt wegen der Übereinstimmung der ersten beiden Gruppen ($\mathfrak{G}$ u. $\mathfrak{A}_1$) nach unserer Annahme:

Die Faktorgruppen I sind paarweise isomorph den Faktorgruppen III.

Ebenso durch Vergleich von II und IV:

Die Faktorgruppen II sind paarweise isomorph den Faktorgruppen IV.

Mittels der Beziehung zwischen III und IV folgt aus den beiden letzten Beziehungen:

Die Faktorgruppen I sind paarweise isomorph den Faktorgruppen II.

Wir haben bewiesen:

Satz 40 (Jordan und Hölder): Sämtliche möglichen Kompositionsreihen einer Gruppe enthalten gleich viele Glieder, die Reihen der Indizes stimmen (abgesehen von

der Reihenfolge) überein, die Faktorgruppen sind (abgesehen von der Reihenfolge) paarweise isomorph.

Von besonderer Bedeutung sind diejenigen Gruppen, deren Indexreihe aus lauter Primzahlen besteht, deren Faktorgruppen also lauter Gruppen von Primzahlordnung sind. Man nennt solche Gruppen „auflösbar" (nach H. Weber „metazyklisch").

Beispielsweise ist die symmetrische Permutationsgruppe von drei oder vier Ziffern auflösbar, diejenige von fünf Ziffern nicht auflösbar. (Vgl. die am Ende des § 31 erwähnte einfache Gruppe.)

§ 40. Ausblick auf weitere Untersuchungen über endliche Gruppen.

Von den allgemeinen Fragen über endliche Gruppen wird sich uns die folgende in erster Linie aufdrängen:

Es liege eine endliche Zahl g vor; wie viele nichtisomorphe Gruppen der Ordnung g gibt es und welcher Art sind diese?

Daß es nur eine endliche Anzahl von Gruppen einer endlichen Ordnung g geben kann, folgt daraus, daß nach Satz 9 jede mit einer Untergruppe der symmetrischen Permutationsgruppe von g Ziffern isomorph sein muß. Im übrigen aber ist man in der Lösung der aufgeworfenen schwierigen Frage über bescheidene Anfänge noch nicht hinausgekommen.

Eine zweite wichtige Frage ist diese:

Es liege eine Gruppe der Ordnung g vor; wie viele und welche Untergruppen besitzt sie?

Von den ebenfalls noch spärlichen Resultaten in dieser Richtung führen wir eines ohne Beweis an:

Satz von Sylow: Ist die Ordnung g einer Gruppe durch eine Primzahlpotenz p^n teilbar, so besitzt die Gruppe (mindestens) eine Untergruppe der Ordnung p^n.

Die sonstigen Untersuchungen beziehen sich meist auf Gruppen besonderer Art; z. B. die Abelschen Gruppen, deren Theorie einen gewissen Abschluß erreicht hat. Sehr ausgedehnt sind die Untersuchungen über die speziellen Eigenschaften der Permutationsgruppen. Mit Rücksicht auf algebraische Anwendung sind die auflösbaren Gruppen besonders eingehend betrachtet, aber auch hier bei der großen Schwierigkeit der auftretenden Probleme erst verhältnismäßig spezielle Ergebnisse erzielt worden.

Weiteres über die hier angedeuteten Dinge findet man in E. Netto, Gruppen- und Substitutionentheorie, Samml. Schubert 55.

IV. Abschnitt.

Die unendlichen Gruppen.

§ 41. Beispiele unendlicher Gruppen aus der Zahlenlehre.

Wir wollen zunächst den uns bereits bekannten Beispielen von „unendlichen Gruppen", d. h. Gruppen mit unendlich vielen Elementen (Beispiel 9, 13, 14, sowie die Gruppen des II. Abschnitts) noch einige weitere anfügen.

Die Menge aller gemeinen komplexen Zahlen mit Ausschluß der Null bildet eine unendliche Gruppe, wenn die gewöhnliche Multiplikation als Verknüpfungsvorschrift bestimmt wird.

Sind nämlich $a + bi$ und $c + di$ irgend zwei komplexe Zahlen, so ist $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$ wieder eine solche Zahl. Eig. III ist hier nichts anderes als das assoziative Gesetz der Multiplikation komplexer Zahlen. Einheitselement ist die Zahl 1. Inverses Element zu $a + bi$ ist die Zahl $x + yi$, für welche $(a + bi)(x + yi) = 1$ ist; man findet hieraus $x = \frac{a}{a^2 + b^2}$, $y = \frac{-b}{a^2 + b^2}$ und damit eine Zahl $x + yi$ des Systems, solange $a + bi$ (also $a^2 + b^2$) von Null verschieden ist. Wir erkennen den Grund, warum die Null ausgeschlossen werden mußte.

Die Multiplikation komplexer Zahlen ist kommutativ, $(a + bi)(c + di) = (c + di)(a + bi)$, alle Elemente der Gruppe sind vertauschbar. Man nennt sie eine „unendliche kommutative oder Abelsche Gruppe".

Eine Untergruppe dieser Gruppe ist die Menge aller reellen Zahlen mit Ausschluß der Null. Das Produkt reeller Zahlen ist ja stets wieder reell, für Assoziativität und Einheitselement gilt dasselbe wie eben, zu jeder von Null verschiedenen reellen Zahl a ist die reelle Zahl $\frac{1}{a}$ invers.

Ganz analog ergibt sich als Untergruppe dieser Gruppe die Menge aller rationalen Zahlen mit Ausschluß der Null, endlich als Untergruppe dieser die Menge aller Potenzen einer natürlichen Zahl wie

$$\ldots, 2^{-3}, 2^{-2}, 2^{-1}, 2^0, 2^1, 2^2, 2^3, \ldots .$$

Damit isomorph ist die Menge aller ganzen Zahlen (einschließlich 0) mit der Addition als Verknüpfungsvorschrift, wie die Betrachtung der Exponenten des vorigen Beispiels zeigt.

Wir haben hier den Fall „unendlicher zyklischer Gruppen“ vor uns, d. h. Gruppen, die lediglich aus den ganzzahligen Potenzen — im gruppentheoretischen Sinn — eines ihrer Elemente (2 oder 2^{-1} bzw. für die isomorphe Gruppe 1 oder -1) bestehen.

Im Anschluß hieran wollen wir eine wieder mit diesen beiden Gruppen isomorphe geometrische Gruppe kennen lernen, die uns ein anschauliches Bild solcher Gruppen gibt und zudem einer wichtigen Verallgemeinerung fähig ist.

Aufgabe 45. Man suche noch weitere Untergruppen der angegebenen Gruppe der komplexen Zahlen.

§ 42. Beispiele unendlicher Gruppen aus der Geometrie.

Wir müssen hier zunächst an eine geometrische Verwandtschaft erinnern, die Kreisverwandtschaft oder Inversion oder Transformation durch reziproke Radien. Es liege ein Kreis K mit Radius r um den Punkt O vor. Wir ordnen nach folgenden Regeln jedem Punkt P der Ebene einen (im allgemeinen) anderen Punkt P' der Ebene zu:

1. P' liegt wieder auf dem Strahl, der von O aus durch P geht,
2. $O\,P' : r = r : O\,P$.

Diese Inversion nennen wir auch eine Spiegelung an K, P' das Spiegelbild von P. Jede Kurve ergibt durch Spiegelung ihrer einzelnen Punkte wieder eine Kurve, jede Fläche eine Fläche. Die Eigenschaften dieser Spiegelung sind, soweit sie im folgenden in Betracht kommen[1]):

Die Zuordnung ist eine gegenseitige, entspricht Punkt P' dem Punkt P, so entspricht Punkt P dem Punkt P'.

[1]) Die Beweise und weitere Eigenschaften findet man in Samml. Goschen Nr. 65, § 17.

Jeder Punkt des Kreises K entspricht sich selbst.

Jedem Kreis entspricht wieder ein Kreis (wenn die Gerade als Kreis mit unendlich großem Radius aufgefaßt wird), der Kreislinie eine Kreislinie, der Kreisfläche eine Kreisfläche.

Kreisen, die sich berühren, entsprechen Kreise, die sich berühren, speziell jedem Kreis, der den Kreis K von außen berührt, ein Kreis, der K von innen berührt und umgekehrt.

Zwei orthogonalen Kreisen entsprechen zwei orthogonale Kreise, speziell entspricht ein zu K orthogonaler Kreis sich selbst.

Wir zeichnen jetzt (Fig. III) zwei beliebige (etwa gleich große) sich berührende Kreise K_1 und K'_1. Aus diesen erzeugen wir durch fortgesetzte Spiegelung nach dem Prinzip der reziproken Radien an den beiden Kreisen unendlich viele Kreise; und zwar gehe über durch Spiegelung

an K_1	an K'_1
K'_1 in K_2	K_1 in K'_2
K'_2 in K_3	K_2 in K'_3
K'_3 in K_4	K_3 in K'_4
.....	.....

Die Gebiete zwischen den Kreisen färben wir abwechselnd weiß und schwarz und bezeichnen sie kurz durch die beiden begrenzenden Kreise in runden oder eckigen Klammern entsprechend der weißen oder schwarzen Farbe, also etwa $(K_1\,K'_1)$, $[K'_1\,K'_2]$, ... Nun sehen wir zu, wie diese Gebiete durch die Spiegelungen an K_1 und K'_1 ineinander übergehen, indem wir die Spiegelbilder der begrenzenden Kreise verfolgen. Es geht über durch Spiegelung:

an K_1	an K'_1
$(K_1\,K'_1)$ in $[K_1\,K_2]$	$[K_1\,K_2]$ in $(K'_2\,K'_3)$
$(K'_2\,K'_3)$ in $[K_3\,K_4]$	$[K_3\,K_4]$ in $(K'_4\,K'_5)$
.....	.....

Wir können diese Tabelle auch nach oben unbegrenzt fortsetzen; als nächste Zeile würde sich oben anschließen:

$(K_2\,K_3)$ in $[K'_1\,K'_2]$ $\quad$ $[K'_1\,K'_2]$ in $(K_1\,K'_1)$.

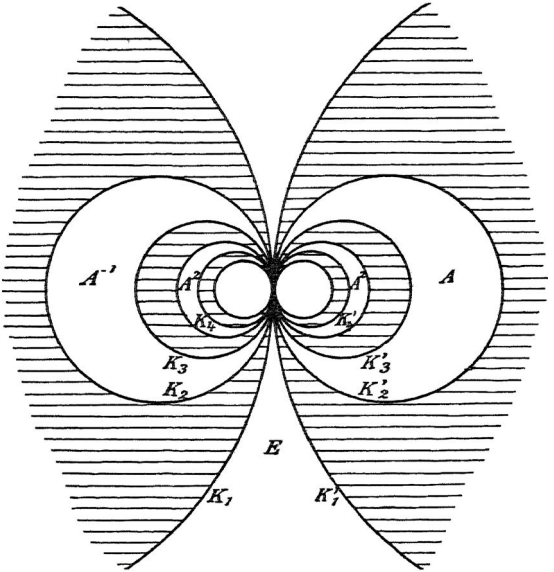


Fig. III.

Durch doppelten Spiegelungsprozeß — an K_1 und darauf an K'_1 — geht also uber

$$\begin{array}{l}\cdots\cdots\cdots\cdots\cdots\\ (K_2\,K_3) \text{ in } (K_1\,K'_1)\\ (K_1\,K'_1) \text{ in } (K'_2\,K'_3)\\ (K'_2\,K'_3) \text{ in } (K'_4\,K'_5)\\ \cdots\cdots\cdots\cdots\cdots\end{array}$$

d. h. jedes weiße Gebiet in das nächstfolgende weiße. Wir können uns den Übergang vorstellen als ein Ausdehnen bzw. Zusammenziehen jedes weißen Gebietes in sein weißes Nachbargebiet oder auch — weil ja zugleich die schwarzen Gebiete in schwarze übergehen — als ein entsprechendes Dehnen oder Zusammenziehen der ganzen Ebene.

Den doppelten Spiegelungsprozeß, der alle Gebiete gleichzeitig transformiert, bezeichnen wir als Element A. A^{-1} soll den umgekehrten Prozeß bedeuten, also die Überführung jedes weißen Gebietes in das auf der anderen Seite benachbarte weiße oder die Spiegelung an K'_1 und darauf an K_1. A^2, der zweimal nacheinander ausgeführte Prozeß A, bedeutet die Überführung jedes weißen Gebietes in ein übernächstes weißes, A^3 in ein drittnächstes usw. Das Unverändert-lassen der Figur nennen wir A^0 oder E. Alle Potenzen von A sind verschieden, da wir unendlich viele weiße Gebiete haben.

Das System aller dieser Potenzen

$$\ldots, A^{-3}, A^{-2}, A^{-1}, A^0, A, A^2, A^3, \ldots$$

bildet eine unendliche zyklische Gruppe, da irgend zwei Prozesse A^i, A^k nacheinander ausgeführt wieder einen solchen Prozeß (A^{i+k}) liefern, und auch die übrigen Gruppeneigenschaften sich ohne weiteres ergeben.

Eine gute Übersicht über diese Gruppe bekommen wir, wenn wir in jedes Gebiet dasjenige Element hineinschreiben, durch welches ein beliebiges Ausgangsgebiet in dieses Gebiet übergeführt wird. Als Ausgangsgebiet ist in der Figur ($K_1 K'_1$) gewählt.

§ 43. Fortsetzung.

Wir wollen jetzt unsere Betrachtung verallgemeinern. K, K', K'' seien drei (etwa gleich große) sich von außen

beruhrende Kreise (Fig. IV). Wir spiegeln wieder nach dem Prinzip der reziproken Radien jeden der drei Kreise an den beiden anderen. Da die beiden Kreise K, K' sich

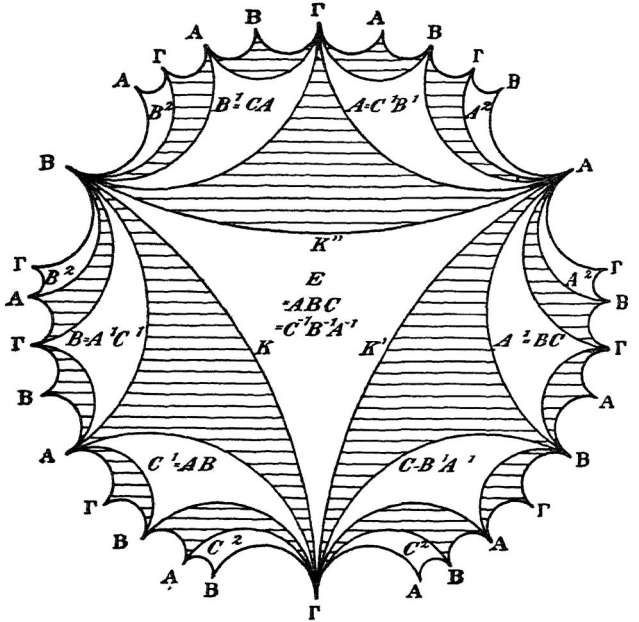


Fig. IV.

gegenseitig berühren und jeder den Kreis K'' von außen berührt, gehen sie durch Spiegelung an K'' in zwei Kreise über, welche sich wieder gegenseitig und zudem den Kreis K'' von innen berühren. Das Analoge gilt für die Spiegelung an K und an K'. Wir erhalten weitere sechs Kreise,

Diese spiegeln wir wieder an K, K', K'' und erhalten zwölf neue Kreise usw. Alle so entstehenden Kreise berühren sich und ihre Berührungspunkte liegen sämtliche auf einem Kreis[1]). In der Figur ist nur das Innere dieses Kreises gezeichnet. Die entstehenden Kreisbogendreiecke färben wir abwechselnd weiß und schwarz. Wir nennen sie alle $A\ B\ \Gamma$, achten aber darauf, daß alle Ecken, die durch Spiegelung auseinander hervorgehen, gleich bezeichnet sind.

Ein weißes Dreieck, etwa das zwischen K, K', K'' gelegene, geht durch Spiegelung an K' in ein schwarzes über, dieses durch Spiegelung an K'' wieder in ein weißes (in der Figur das mit A bezeichnete). Spiegeln wir nicht nur ein Dreieck, sondern die ganze Figur durch diesen doppelten Spiegelungsprozeß — an K' und darauf an K'' —, so geht die ganze Figur in sich über, jedes weiße Dreieck in ein anderes weißes.

Wir bezeichnen diesen Prozeß als Element A. Er führt z. B. die mit E, A, A^{-1}, A^{-2}, C bezeichneten Dreiecke beziehungsweise über in die mit $A, A^2, E, A^{-1}, B^{-1}$ bezeichneten. Den Prozeß, der den eben beschriebenen wieder aufhebt, nämlich Spiegelung an K'' und darauf an K', nennen wir A^{-1}. Analog soll der Prozeß der Spiegelung der ganzen Figur an K'' und darauf an K als Element B, seine Umkehrung als B^{-1}, der Prozeß der Spiegelung an K und darauf an K' als Element C, seine Umkehrung als C^{-1} bezeichnet werden. Unter E verstehen wir wieder das Unverändert-lassen der Figur. Unter A^2 den zweimal

[1]) Es ist dies der Kreis C durch die drei Berührungspunkte von K, K', K''. C geht, da es orthogonal ist zu K, K', K'', bei jeder Spiegelung in sich über, und damit die Berührungspunkte von K, K', K'' immer wieder in Punkte von C, d. h. die Berührungspunkte aller entstehenden Kreise liegen auf C. Ebenso stehen alle entstehenden Kreise senkrecht auf C, weil K, K', K'' auf C senkrecht stehen.

nacheinander ausgeführten Prozeß A, unter AB den Prozeß A mit darauffolgendem Prozeß B usw. BA ist hier verschieden von AB. Aber alle derartigen Prozesse sind jedenfalls enthalten in der Form $A^{\alpha} B^{\beta} C^{\gamma} A^{\alpha'} B^{\beta'} C^{\gamma'} \ldots$, wo $\alpha, \beta, \gamma, \alpha', \beta', \gamma', \ldots$ irgendwelche Werte aus der Reihe 0, 1, 2, ... haben.

Die Gesamtheit dieser Prozesse bildet eine unendliche Gruppe; denn die Verknüpfung irgend zweier ergibt wieder dieselbe Form, sie ist assoziativ, es ist ein Einheitselement vorhanden, und zu $A^{\alpha} B^{\beta} C^{\gamma} A^{\alpha'} B^{\beta'} C^{\gamma'} \ldots$ ist $\ldots C^{-\gamma'} B^{-\beta'} A^{-\alpha'} C^{-\gamma} B^{-\beta} A^{-\alpha}$ invers.

In der Figur trägt wieder jedes Dreieck den Namen desjenigen Elements, durch welches das Ausgangsdreieck zwischen K, K', K'' in dieses Dreieck übergeführt wird. Jedes Dreieck erhält so zwei Namen, bei Vermeidung negativer Potenzen einen einzigen (wenn wir Teilprodukte, welche gleich E sind, wegheben).

In analoger Weise können wir von n sich berührenden Kreisen ausgehen, entsprechend n Elemente $A, B, C, \ldots$ definieren und aus ihnen eine Gruppe aufbauen.

Wir erhalten so die umfassendste Gruppe, die sich aus endlich vielen Elementen erzeugen läßt (vgl. § 25), jede andere aus ebenso vielen Elementen erzeugte ist in ihr als Untergruppe enthalten. Nicht aber überhaupt jede unendliche Gruppe; denn es gibt deren auch solche, die sich nicht aus endlich vielen Elementen erzeugen lassen, wie z. B. die Menge der rationalen Zahlen außer Null, durch die Multiplikation verknüpft, da es ja unendlich viele Primzahlen gibt[1]).

[1]) Näheres über die hier betrachteten Gruppen findet der Leser in Math. Annalen 20 (1882), S. 1ff. oder in Burnside, Theory of groups, S. 255ff.

Aufgabe 46. Man zeichne einen weiteren Fall der angeführten Gruppendarstellungen, etwa für $n = 4$.

§ 44. Beispiele unendlicher Gruppen aus der Transformationslehre.

Beispiel 9 ist noch erheblicher Verallgemeinerungen fähig. Die Funktionen, welche die neuen Veränderlichen durch die alten ausdrücken, sind dort ganze lineare homogene Funktionen von zwei Veränderlichen. Man überzeugt sich in derselben Weise davon, daß man wieder eine Gruppe (die „affine Gruppe der Ebene") erhält, wenn ganze lineare inhomogene Funktionen von zwei Veränderlichen eingeführt werden, also

$$x' = a\,x + b\,y + e$$
$$y' = c\,x + d\,y + f,$$

wieder mit der Bedingung der Auflösbarkeit nach x, y: $a\,d - b\,c \neq 0$.

Von hier aus erhalten wir eine wiederum umfassendere Gruppe (die „projektive Gruppe der Ebene"), wenn wir statt der ganzen Funktionen gebrochene, aber noch lineare Funktionen und zwar mit gleichem Nenner in einer und derselben Transformation[1]) benützen:

$$x' = \frac{a\,x + b\,y + e}{g\,x + h\,y + k}$$
$$y' = \frac{c\,x + d\,y + f}{g\,x + h\,y + k};$$

die Bedingung der Auflösbarkeit nach x, y wird hier[2])

[1]) Durch einen Versuch der Verknüpfung im Falle verschiedener Nenner erkennt man, daß Eig. II dabei zerstört würde

[2]) Bezeichnet man nämlich den Nenner mit N, so kann man die Gleichungen ersetzen durch

$$a\frac{x}{N} + b\frac{y}{N} + e\frac{1}{N} = x'$$

$$\begin{vmatrix} a & b & e \\ c & d & f \\ g & h & k \end{vmatrix} \neq 0.$$

Endlich können wir noch die Zahl der Veränderlichen auf n erhöhen. Wir erhalten die sog. „allgemeine projektive Gruppe". Z. B. für $n = 3$:

$$x' = \frac{a_{11}\,x + a_{12}\,y + a_{13}\,z + a_{14}}{a_{41}\,x + a_{42}\,y + a_{43}\,z + a_{44}}$$

$$y' = \frac{a_{21}\,x + a_{22}\,y + a_{23}\,z + a_{24}}{a_{41}\,x + a_{42}\,y + a_{43}\,z + a_{44}}$$

$$z' = \frac{a_{31}\,x + a_{32}\,y + a_{33}\,z + a_{34}}{a_{41}\,x + a_{42}\,y + a_{43}\,z + a_{44}}$$

mit der Bedingung, daß die der obigen analoge Determinante der Koeffizienten nicht verschwindet.

Für $n = 4$ wollen wir die folgenden zwei Untergruppen der allgemeinen projektiven Gruppe wegen ihrer großen Bedeutung für die Grundlagen der Physik erwähnen. Die Veränderlichen sind dabei x, y, z, t, die für die einzelnen Transformationen verschiedenen Konstanten sind v und das davon abhängige k; c ist eine absolute Konstante. Prüfung auf unsere Eig. II, IV, V ergibt die Gruppeneigenschaft.

$$c\frac{x}{N} + d\frac{y}{N} + f\frac{1}{N} = y'$$

$$g\frac{x}{N} + h\frac{y}{N} + k\frac{1}{N} = 1;$$

dann ergibt sich die obige Bedingung nach den Regeln der Auflösung der drei linearen Gleichungen mit den drei Unbekannten $\frac{x}{N}$, $\frac{y}{N}$, $\frac{1}{N}$ (Samml. Göschen Nr. 53, § 31).

1) $x' = x - v\,t\,, \quad y' = y\,, \quad z' = z\,, \quad t' = t\,;$

2) $x' = k\,(x - v\,t)\,, \; y' = y\,, \quad z' = z\,, \quad t' = k\,(t - \frac{v}{c^2}\,x)\,,$

$$\text{wobei } k = \frac{1}{\sqrt{1 - \frac{v^2}{c^2}}}\,^{1}).$$

Aufgabe 47. Man suche Untergruppen der angeführten projektiven Gruppen durch Spezialisierung der Konstanten.

§ 45. Vergleich der Eigenschaften endlicher und unendlicher Gruppen.

Nach den angeführten Beispielen zeigen sich die unendlichen Gruppen in vielen Punkten analog den endlichen. Auch unter ihnen finden wir zyklische, kommutative und nichtkommutative (Beispiel 9), stillschweigend konnten wir auch die Begriffe der Untergruppe, des Isomorphismus und der abstrakten Gruppe übertragen.

Wir wollen nun in Kürze verfolgen, wieweit die sonstigen für endliche Gruppen entwickelten Begriffe und Sätze bei unendlichen Gruppen ihre Geltung behalten.

Während § 14 und 16 sich ohne weiteres übertragen, gilt dies nur zum Teil von § 15. Wir begegnen bei unendlichen Gruppen Elementen endlicher Ordnung neben solchen unendlich hoher Ordnung. (Beispiel: die Transformation $x' = 3\,x \pm 4\,y$, $y = 2\,x \pm 3\,y$, für die unteren Zeichen ist die Ordnung 2, für die oberen ∞). Die zum Satz 5

[1]) Der mit den Elementen der Relativitätstheorie vertraute Leser wird in der ersten der beiden Gruppen diejenige der „Galilei-Transformationen" des vierdimensionalen Raum-Zeit-Kontinuums erkennen, in der zweiten die Gruppe der „Lorentz-Transformationen", welche die moderne Physik an die Stelle der ersten gesetzt hat.

führenden Betrachtungen und dieser Satz selbst werden hinfällig für unendliche Gruppen.

§ 17 und 18 beruhen wesentlich auf der Endlichkeit der Ordnung und gelten daher nicht mehr oder doch nicht ohne besondere Vorbereitung und Einführung von neuen Begriffen. Desgleichen § 19, 20 und 21.

Die in § 22 eingeführte Schreibweise läßt sich auch bei unendlichen Gruppen anwenden; z. B. drückt die Schreibweise $\mathfrak{G} = G_1 + G_2 + G_3 + \ldots$ wieder aus, daß $\mathfrak{G}$ aus den Elementen $G_1, G_2, G_3, \ldots$ besteht. Lassen sich die Elemente einer unendlichen Gruppe nicht abzählen, wie etwa im obigen Beispiel der komplexen Zahlen, so kann man diese symbolische Summe allerdings nur durch einige herausgegriffene Beispiele von Elementen andeuten.

Die Zerlegung einer Gruppe in Komplexe nach einer Untergruppe, wie sie § 23 für endliche Gruppen entwickelt, läßt sich auf unendliche ausdehnen. Dagegen gelten die Sätze 21, 22, 23 des § 24 naturgemäß nicht. Faßt man aber den Index einer Untergruppe als die Anzahl der Komplexe bei Zerlegung nach dieser Untergruppe auf, so bleibt dieser Begriff bestehen. Der Index einer Untergruppe einer unendlichen Gruppe kann endlich oder unendlich sein.

Es folgen hierfür zwei Beispiele.

1. $\mathfrak{G}$ sei die Gruppe der durch Addition zu verknüpfenden ganzen komplexen Zahlen $a + b\,i$; a und b durchlaufen also je sämtliche ganzen Zahlen. $\mathfrak{G}$ ist tatsächlich eine Gruppe, da

$$(a + b\,i) + (a' + b'\,i) = (a + a') + (b + b')\,i$$

und damit wieder eine Zahl derselben Art ist, ferner die Zahl 0 die Rolle des Einheitselementes spielt und zu $a + b\,i$ die Zahl $-a - b\,i$ invers ist.

Ziehen wir (Fig. V) in der komplexen Zahlenebene alle Parallelen zu den beiden Achsen in den Abständen ± 1, ± 2, $\pm 3, \ldots$, so geben die Eckpunkte des entstehenden Gitters ein Bild unserer Gruppe.

Nun sei $\mathfrak{H}$ die Untergruppe von $\mathfrak{G}$, welche aus den Zahlen $a + b\,i$ besteht, in welchen sowohl a als b gerade

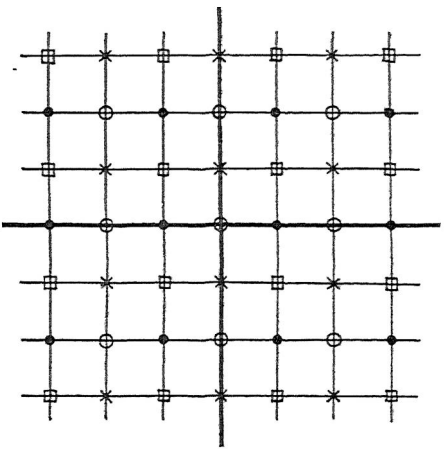


Fig. V.

sind. Wir schreiben die Elemente von $\mathfrak{H}$ in der Form $2\,\alpha + 2\,\beta\,i$, wo α, β wieder alle ganzen Zahlen durchlaufen. Daß $\mathfrak{H}$ eine Gruppe ist, ergibt sich genau wie bei $\mathfrak{G}$. In der Figur entsprechen ihr die durch Ringe bezeichneten Gitterpunkte.

Ein Element von $\mathfrak{G}$, das nicht zu $\mathfrak{H}$ gehört, ist $G_2 = 1$. Der Nebenkomplex $\mathfrak{H}\,G_2$ enthält die Elemente $2\,\alpha + 2\,\beta\,i + 1 = (2\,\alpha + 1) + 2\,\beta\,i$ (die Punkte der Figur). Ein weder zu $\mathfrak{H}$ noch zu $\mathfrak{H}\,G_2$ gehöriges Element von $\mathfrak{G}$ ist

$G_3 = i$. Der Nebenkomplex $\mathfrak{H} G_3$ enthält die Elemente $2\alpha + 2\beta i + i = 2\alpha + (2\beta + 1) i$ (die Kreuze der Figur). Ein noch nicht vorgekommenes Element von $\mathfrak{G}$ ist $G_4 = 1 + i$. Der Nebenkomplex $\mathfrak{H} G_4$ enthält die Elemente $2\alpha + 2\beta i + 1 + i = (2\alpha + 1) + (2\beta + 1) i$ (die Qua-

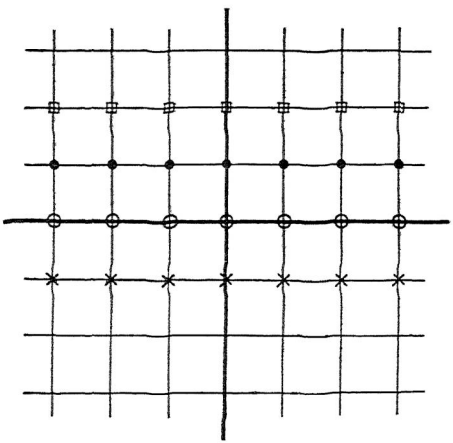


Fig. VI.

drate der Figur). Damit ist die Gruppe $\mathfrak{G}$ erschopft, ihre Zerlegung nach der Untergruppe $\mathfrak{H}$ ist

(1) $\mathfrak{G} = \mathfrak{H} + \mathfrak{H} G_2 + \mathfrak{H} G_3 + \mathfrak{H} G_4$; der Index ist 4[1]).

2. $\mathfrak{G}$ sei wieder dieselbe Gruppe, $\mathfrak{H}'$ die aus den reellen ganzen Zahlen a bestehende Untergruppe (Ringe der

[1]) Zugleich stellt $\mathfrak{H}$ das interessante Beispiel einer Untergruppe vor, die mit ihrer eigenen Gruppe isomorph ist. Die Zuordnung der Elemente $\alpha + \beta i$ von $\mathfrak{G}$ und $2\alpha + 2\beta i$ von $\mathfrak{H}$ erfüllt tatsächlich die Forderung des Isomorphismus. Wir erkennen dies auch unmittelbar, wenn wir das geometrische Bild von $\mathfrak{H}$ als das in doppeltem Maßstabe gezeichnete Bild von $\mathfrak{G}$ auffassen.

Fig. VI). $G_2 = i$ liefert den Nebenkomplex $\mathfrak{H}' G_2$ der Elemente $a + i$, $G_3 = -i$ den Nebenkomplex $\mathfrak{H}' G_3$ der Elemente $a - i$, $G_4 = 2i$ den Nebenkomplex $\mathfrak{H}' G_4$ der Elemente $a + 2i$ usw. in inf. $\mathfrak{G}$ wird durch keine endliche Zahl von Nebenkomplexen erschöpft. Die Zerlegung ist hier

(2) $\mathfrak{G} = \mathfrak{H}' + \mathfrak{H}' G_2 + \mathfrak{H}' G_3 + \mathfrak{H}' G_4 + \ldots$; der Index ist ∞.

Nicht immer läßt sich die Zerlegung einer unendlichen Gruppe nach einer Untergruppe in dieser Weise aufschreiben, das vollständige Restsystem läßt sich nicht immer in eine abzählbare Reihe $G_1 = E, G_2, G_3, \ldots$ anordnen. Als Beispiel betrachte man die obige Gruppe $\mathfrak{G}$ als Untergruppe der Gruppe aller (auch gebrochen-rationalen und irrationalen) wieder durch Addition zu verknüpfenden komplexen Zahlen. Immerhin kann man auch dann noch von einer Zerlegung und von einem (nicht abzählbar-unendlichen) Index sprechen.

Die in § 26—38 behandelten Begriffe der Vertauschbarkeit, der konjugierten Elemente und Gruppen, der invarianten und maximalen invarianten Untergruppe, der Faktorgruppe, des Durchschnitts und Produkts zweier Gruppen bleiben für unendliche Gruppen bestehen, desgleichen die hierüber gewonnenen Sätze, soweit sie nicht (wie in § 35) ausdrücklich die Endlichkeit der Gruppe benützen. Der Begriff der Kompositionsreihe und der Satz von Jordan-Hölder des § 39 verlieren ihre Bedeutung.

Verweilen wir noch kurz bei den wichtigsten dieser Begriffe! Die obigen Untergruppen $\mathfrak{H}$ und $\mathfrak{H}'$ der Gruppe $\mathfrak{G}$ geben uns, da $\mathfrak{G}$ eine Abelsche Gruppe ist, Beispiele von unendlichen invarianten Untergruppen, die aber nicht maximal sind. Es läßt sich zwischen diese Untergruppen

und $\mathfrak{G}$ die Untergruppe einschieben, die aus allen komplexen Zahlen $a + b\,i$ besteht, wo a alle ganzen, b nur die geraden Zahlen durchläuft (Ringe und Punkte der Fig. V).

Die beiden Zerlegungen (1) und (2) liefern auch Beispiele von Faktorgruppen. Die erste $\frac{\mathfrak{G}}{\mathfrak{H}}$ ist der Vierergruppe isomorph, die zweite $\frac{\mathfrak{G}}{\mathfrak{H}'}$ der Gruppe $\mathfrak{H}'$ (ein besonderer Fall, der auch bei endlichen Gruppen vorkommt).

Aufgabe 48. Man bilde Komplexzerlegungen von unendlichen Gruppen nach den dazu gewonnenen Untergruppen und bestimme die Indizes.

Aufgabe 49. $\mathfrak{B}$ sei die Gruppe aller Verschiebungen (ohne eigene Rotation) eines Kreises K in seiner Ebene derart, daß sein Mittelpunkt auf einem festen Kreise läuft. $\mathfrak{R}$ sei die Gruppe aller Rotationen des Kreises K um seinen Mittelpunkt. Dann ist $\mathfrak{R}\,\mathfrak{B} = \mathfrak{B}\,\mathfrak{R}$ eine Gruppe, welche $\mathfrak{B}$ und $\mathfrak{R}$ als Untergruppen hat. Man suche die konjugierten Untergruppen, überzeuge sich von der Invarianz der Untergruppen und bestimme die Faktorgruppen.

Nimmt man statt der stetigen Verschiebungen und Rotationen ruckweise Verschiebungen und Rotationen um $\frac{2k\pi}{m}$ bzw. $\frac{2l\pi}{n}$ vor, so erhält man analoge endliche Gruppen der Ordnungen $m\,n$.

Man verallgemeinere das Verfahren!

Lösung der Aufgaben.

1. Beispiel 4, 5, 7, 8, 9, 10, 11, 12, 13, 14.

2. Ja; dies zeigt schon Beispiel 4, das wir für jede Zahl g ebenso bilden können wie für die Zahl 7; ebenso Beispiel 10.

4. Ja; dies zeigt folgende Zuordnung der Elemente des Beispiels 4 oder 5:

$$\begin{matrix} 0\,1\,2\,3\,4\,5\,6 \\ 0\,2\,4\,6\,1\,3\,5 \end{matrix} \quad \text{bzw.} \quad \begin{matrix} f_1\,f_2\,f_3\,f_4 \\ f_1\,f_2\,f_4\,f_3 \end{matrix}$$

5. $\varepsilon, \varepsilon^2, \varepsilon^3, \varepsilon^4, \varepsilon^5, \varepsilon^6$ haben bzw. die Ordnungen 1, 7, 3, 3, 6, 2.

6. Ja; vgl. Beispiel 10.

7. $\mathfrak{G}$; $E, (12)(3)$; $E, (13)(2)$; $E, (23)(1)$; $E, (123), (132)$; die Gruppe selbst.

8. $(ABC)^{-1} = C^{-1}B^{-1}A^{-1}$.

9. a sei die Ordnung von A, a' von A^{-1}.

$$(A^{-1})^a = (A^a)^{-1} = E^{-1} = E, \quad \text{also} \quad (1)\ a' \leqq a,$$

$$A^{a'} = ((A^{-1})^{a'})^{-1} = E^{-1} = E, \quad \text{also} \quad (2)\ a \leqq a';$$

aus (1) und (2) folgt $a = a'$.

10. Wegen $AB = BA$ ist $(AB)^{ab} = A^{ab}B^{ab} = E$. Ist auch $(AB)^c = E$, so ist nach Satz 6 $c \equiv ab \pmod{c}$.

11. c sei die Ordnung von AB, c' von BA.

$$(BA)^c = B(AB)^{c-1}A = B(AB)^{c-1}ABB^{-1}$$
$$= B(AB)^cB^{-1} = BEB^{-1} = E;$$

also $c' \leqq c$. Analog findet man $c \leqq c'$, also ist $c = c'$.

12. Lautet die erste Zeile $E, A_2, A_3, \ldots$, so müßte die erste Spalte $E, A_2^{-1}, A_3^{-1}, \ldots$ sein.

13. $E, (12)(36)(45), (13)(25)(46), (14)(26)(35), (156)(234), (165)(243)$.

14. $A = (145)(26)(3)(7)$ u. a. $= (14)(15)(26)$
$B = (1849310)(2576)$ u. a. $= (84)(89)(83)(810)(81)(62)(65)(67)$.

15. $AB = (19310)(2)(47658)$, $BA = (18572)(31049)(6)$.

16. (123456), $(135)(246)$, $(14)(25)(36)$, $(153)(264)$, (165432), $(1)(2)(3)(4)(5)(6)$; die Anzahl der Potenzen ist gleich der Anzahl der Ziffern; man erhält die r^{te} Potenz, indem man von einer beliebigen Ziffer der zyklischen Anordnung ausgehend jede r^{te} Ziffer nimmt und daraus neue Zyklen bildet.

17. Unter Weglassung der eingliedrigen Zyklen ist $A^2 = (154)$, $A^3 = (26)$, $A^4 = (145)$, $A^5 = (154)(26)$, $A^6 = E$. Die Ordnung einer Permutation ist das kleinste gemeinsame Vielfache der Zahlen der Ziffern in den einzelnen Zyklen.

18. $(n\,n-1\ldots21)$; jede Transposition ist zu sich selbst invers.

19. a) $Z_1Z_2 = Z_2Z_1$, b) im allgemeinen $Z_1Z_2 + Z_2Z_1$.

20. Die beiden Gruppen sind isomorph.

21. Die Elemente, welche etwa 1 ungeändert lassen, bilden eine mit $\mathfrak{S}_4$ isomorphe Gruppe.

Die Elemente, welche etwa 1, 2, 3 ungeändert lassen, bilden die mit $\mathfrak{S}_3$ isomorphe Gruppe: (1) (2) (3) (4) (5), (1) (2) (3) (4 5).

Die Elemente, welche etwa 1, 2, 3 unter sich vertauschen, bilden eine Gruppe 12ter Ordnung (isomorph Beispiel 11 für $n = 6$); unter Weglassung der eingliedrigen Zyklen ist sie: E, (1 2), (1 3), (2 3), (1 2 3), (1 3 2), (4 5), (1 2) (4 5), (1 3) (4 5), (2 3) (4 5), (1 2 3) (4 5), (1 3 2) (4 5).

Die Elemente, bei welchen die Vertauschungen etwa von 1, 2, 3 für sich betrachtet eine Gruppe bilden, z. B. die zyklische Gruppe der drei Elemente, bilden eine Gruppe (isomorph der zyklischen Gruppe 6ter Ordnung): E, (1) (2) (3) (4 5), (1 2 3) (4) (5), (1 2 3) (4 5), (1 3 2) (4) (5), (1 3 2) (4 5).

22. Ein Komplex von Permutationen kann stets als Teilkomplex der symmetrischen Gruppe der betreffenden Ziffern aufgefaßt werden; weiter nach Satz 19.

23. $$X\mathfrak{A}Y = XA_1Y + XA_2Y + \ldots + XA_\alpha Y.$$

$$X\mathfrak{A}Y \,.\, Y^{-1}\mathfrak{A}Z = X\mathfrak{A}E\mathfrak{A}Z = X\mathfrak{A}\mathfrak{A}Z = X\mathfrak{A}Z.$$

24. $$\mathfrak{G}\mathfrak{G} \leqq \mathfrak{G}.$$

25. Ist $\mathfrak{C}$ eine Gruppe, so ist $\mathfrak{C}\mathfrak{C} = \mathfrak{C}$ nach Satz 8.
Ist $\mathfrak{C}\mathfrak{C} = \mathfrak{C}$, so besteht Eig. II, also ist $\mathfrak{C}$ nach Satz 19 eine Gruppe.

26. $$[E + (1\,2)] + [(1\,3) + (1\,2\,3)] + [(2\,3) + (1\,3\,2)];$$
$$[E + (1\,2\,3) + (1\,3\,2)] + [(1\,2) + (2\,3) + (1\,3)].$$

27. Wenn etwa $\mathfrak{A}B$ und $\mathfrak{A}C$ lauter verschiedene Elemente enthalten, enthalten auch $B^{-1}\mathfrak{A}$ und $C^{-1}\mathfrak{A}$ lauter verschiedene; wäre etwa $B^{-1}A_i = C^{-1}A_k$, so ware $(B^{-1}A_i)^{-1} = (C^{-1}A_k)^{-1}$ oder $A_i^{-1}B = A_k^{-1}C$, also hätten $\mathfrak{A}B$ und $\mathfrak{A}C$ ein Element gemeinsam.

28. Für positive Exponenten:
$$A^rB^s = A^{r-1}ABB^{s-1} = A^{r-1}BAB^{s-1} = \text{usw.}$$
Darauf führt man auch den Fall negativer Exponenten zurück; z. B. $A^{-\varrho} = A^{\alpha-\varrho}$, wo α die Ordnung von A ist.

29. Die transformierte Permutation ist
$$\begin{pmatrix}4&1&5&3&2\\1&2&3&4&5\end{pmatrix}(1\,2\,3)(4\,5)\begin{pmatrix}1&2&3&4&5\\4&1&5&3&2\end{pmatrix} = (4\,1\,5)(3\,2).$$
Die transformierte Permutation hat genau die alte Form (ebenso viele Zyklen von entsprechender Länge); man erhält die neuen Zyklen, indem man die transformierende Permutation auf die Ziffern der zu transformierenden (in Zyklusform) ausübt, gerade als ob keine Zyklusklammern dastünden. Beweis:

$$\text{Ist } P = \begin{pmatrix}1&2&\cdots\\ \alpha_1&\alpha_2&\cdots\end{pmatrix},\quad A = \begin{pmatrix}1&2&\cdots\\ \beta_1&\beta_2&\cdots\end{pmatrix}, \text{ so ist}$$

$$P^{-1}AP = \begin{pmatrix}\alpha_1&\alpha_2&\cdots\\1&2&\cdots\end{pmatrix}\begin{pmatrix}1&2&\cdots\\ \beta_1&\beta_2&\cdots\end{pmatrix}\begin{pmatrix}\beta_1&\beta_2&\cdots\\ \alpha_{\beta_1}&\alpha_{\beta_2}&\cdots\end{pmatrix} = \begin{pmatrix}\alpha_1&\alpha_2&\cdots\\ \alpha_{\beta_1}&\alpha_{\beta_2}&\cdots\end{pmatrix}.$$

Dies sowie A denke man nun in Zyklusform. α_i und α_{β_i} sind die Ziffern, in welche i und β_i durch P übergeführt werden.

30. Vertauschbarkeit des Elements A mit dem Komplex $\mathfrak{C}$: $A\mathfrak{C} = \mathfrak{C}A$; Vertauschbarkeit der Komplexe $\mathfrak{C}$ und $\mathfrak{D}$: $\mathfrak{C}\mathfrak{D} = \mathfrak{D}\mathfrak{C}$.
Ist $A\mathfrak{C} = \mathfrak{C}A$ und $B\mathfrak{C} = \mathfrak{C}B$, so ist $AB\mathfrak{C} = A\mathfrak{C}B = \mathfrak{C}AB$.

31. Ist $J_1 G = G J_1$ und $J_2 G = G J_2$ für alle G von $\mathfrak{G}$, so ist $J_1 J_2 G = J_1 G J_2 = G J_1 J_2$ für alle G von $\mathfrak{G}$.

32. Man ordne die Elemente A und $X^{-1}AX$ der Gruppe $\mathfrak{G}_A$ bzw. $X^{-1}\mathfrak{G}_A X$ einander zu. Ist $AB = C$, so ist $X^{-1}AXX^{-1}BX = X^{-1}CX$.

35. Wie 32.

36. Die mit $\mathfrak{H}$ konjugierten Gruppen haben ebenfalls die Ordnung h, müssen also hier mit $\mathfrak{H}$ identisch sein.

37. Ist $\mathfrak{H} \varepsilon< \mathfrak{G}$ vom Index 2, so ist $\mathfrak{G} = \mathfrak{H} + \mathfrak{H}G$ und $\mathfrak{G} = \mathfrak{H} + G'\mathfrak{H}$; $\mathfrak{H}G = G'\mathfrak{H}$. G kann jedes Element von $\mathfrak{G}$ sein, das nicht $\mathfrak{H}$ angehört (Satz 20), ebenso G'. Wir können also $G' = G$ wählen. Damit ist $\mathfrak{H}G = G\mathfrak{H}$.

38. Ist $\mathfrak{H} = E + H \mathrel{i<} \mathfrak{G}$, so ist für jedes G von $\mathfrak{G}$ $(E+H)G = G(E+H)$ oder $EG + HG = GE + GH$ oder $HG = GH$.

39. Läßt man in der Gleichung $H_i G = G H_k$ das Element H_i die Gruppe $\mathfrak{H}$ durchlaufen, so durchläuft H_k ebenfalls die ganze Gruppe $\mathfrak{H}$, so daß also $\mathfrak{H}G = G\mathfrak{H}$ ist. Gehörte nämlich zu zwei Elementen H_i, H_j dasselbe H_k, so wäre $H_i G = H_j G$ oder $H_i = H_j$.
Ist umgekehrt $\mathfrak{H}G = G\mathfrak{H}$, so ist $H_i G = G H_k$.

40. 2a) Eigentliche invariante Untergruppe ist nur $\mathfrak{H} = E + (12)(34) + (13)(24) + (14)(23)$; 2b) Kompositionsreihen gibt es 3: $\mathfrak{G}, \mathfrak{H}, \mathfrak{K}_i, \mathfrak{E}$, wo $\mathfrak{K}_1 = E + (12)(34)$, $\mathfrak{K}_2 = E + (13)(24)$, $\mathfrak{K}_3 = E + (14)(23)$; 2c) $\frac{\mathfrak{G}}{\mathfrak{H}}$, $\frac{\mathfrak{H}}{\mathfrak{K}_i}$, $\frac{\mathfrak{K}_i}{\mathfrak{E}}$; sie sind isomorph den zyklischen Gruppen von 3, 2, 2 Ziffern.

41. Aus $\mathfrak{D} \leqq G^{-1}\mathfrak{H}G$ für alle G von $\mathfrak{G}$ folgt
$G'^{-1}\mathfrak{D}G' \leqq G'^{-1}G^{-1}\mathfrak{H}GG'$ für alle G, G' von $\mathfrak{G}$
oder $G'^{-1}\mathfrak{D}G' \leqq G''^{-1}\mathfrak{H}G''$ für alle G', G'' von $\mathfrak{G}$.
D. h. $G'^{-1}\mathfrak{D}G' \leqq \mathfrak{D}$ oder wegen der gleichen Ordnung
$G'^{-1}\mathfrak{D}G' = \mathfrak{D}$ für alle G' von $\mathfrak{G}$.
Der Satz ist eine Verallgemeinerung der Tatsache, daß eine mit allen konjugierten übereinstimmende Untergruppe eine invariante ist.

42. $\mathfrak{A}\mathfrak{B}$ hat die Ordnung $\frac{ab}{d}$, wo d (in § 35 mit r bezeichnet) die Ordnung von $\mathfrak{D} = (\mathfrak{A}, \mathfrak{B})$ ist. Es ist nämlich $A_1 B_1 = (A_1 D)(D^{-1} B_1) = A_2 B_2$, wir erhalten so mittels jedes Elementes D von $\mathfrak{D}$ ein mit $A_1 B_1$ gleiches Produkt aus einem Element von $\mathfrak{A}$ und einem Element von $\mathfrak{B}$. Umgekehrt liefert jede Gleichung $A_1 B_1 = A_2 B_2$ oder $A_2^{-1} A_1 = B_2 B_1^{-1}$ zu einem Element von $\mathfrak{A}$ ein gleiches Element von $\mathfrak{B}$, also ein Element von $\mathfrak{D}$.

43. $\mathfrak{A}\mathfrak{B} = \mathfrak{B}\mathfrak{A}$ folgt schon aus einer der beiden Gleichungen $\mathfrak{A}G = G\mathfrak{A}$, $\mathfrak{B}G = G\mathfrak{B}$.

44. $\mathfrak{D} = E + (13)(24)(57)(68)$; die Faktorgruppen haben samtlich die Ordnung 2.

45. Z B. die Menge der Zahlen $a + b\sqrt{2}$ (mit Ausschluß der Null), wo a, b rationale Zahlen sind.

47. Z. B. $x' = x - a$, $y' = y - b$ („Translationen") oder $x' = x\cos\alpha + y\sin\alpha$, $y' = -x\sin\alpha + y\cos\alpha$ („Rotationen") oder

$$x' = \frac{x}{1 - ax}, \quad y' = \frac{y}{1 - ax}.$$

49 Ist $\mathfrak{S} = E + V_2 + V_3 + \ldots$, $\mathfrak{R} = E + R_2 + R_3 + \ldots$, so ist $\mathfrak{R}\mathfrak{S} = \mathfrak{R} + \mathfrak{R}V_2 + \mathfrak{R}V_3 + \ldots = \mathfrak{S} + R_2\mathfrak{S} + R_3\mathfrak{S} + \ldots$.

$V^{-1}\mathfrak{R}V = \mathfrak{R}$ fur alle V von $\mathfrak{S}$; $\frac{\mathfrak{R}\mathfrak{S}}{\mathfrak{R}} = (\mathfrak{R}) + (\mathfrak{R}V_2) + (\mathfrak{R}V_3) + \ldots \cong \mathfrak{S}$.

Man kann statt der zwei Bewegungen auch 3, 4, ..., n Bewegungen kombinieren, indem man auf K wieder einen Kreis laufen laßt usw. Anderseits kann man statt der Kreise auch etwa Kugeln wählen mit allen Drehungen in sich bzw. den nach Beispiel 12 gegebenen Drehungen, wenn man in die Kugeln regulare Polyeder einzeichnet.

Register.