DIE GRUNDLEHREN DER MATHEMATISCHEN WISSENSCHAFTEN IN EINZELDARSTELLUNGEN
BAND V

A. SPEISER
THEORIE DER GRUPPEN VON ENDLICHER ORDNUNG

SPRINGER-VERLAG BERLIN HEIDELBERG GMBH

DIE GRUNDLEHREN DER

MATHEMATISCHEN WISSENSCHAFTEN

IN EINZELDARSTELLUNGEN MIT BESONDERER BERÜCKSICHTIGUNG DER ANWENDUNGSGEBIETE

GEMEINSAM MIT

W. BLASCHKE
HAMBURG

M. BORN
GÖTTINGEN

C. RUNGE
GÖTTINGEN

HERAUSGEGEBEN VON

R. COURANT
GÖTTINGEN

BAND V

GRUPPENTHEORIE

VON

ANDREAS SPEISER

Springer-Verlag Berlin Heidelberg GmbH

1923

DIE
THEORIE DER GRUPPEN
VON ENDLICHER ORDNUNG

MIT ANWENDUNGEN
AUF ALGEBRAISCHE ZAHLEN UND GLEICHUNGEN
SOWIE AUF DIE KRISTALLOGRAPHIE

VON

ANDREAS SPEISER
ORD. PROFESSOR DER MATHEMATIK
AN DER UNIVERSITÄT ZÜRICH

Springer-Verlag Berlin Heidelberg GmbH
1923

ISBN 978-3-662-41973-1 ISBN 978-3-662-42031-7 (eBook)
DOI 10.1007/978-3-662-42031-7

Ursprünglich erschienen bei Julius Springer in Berlin 1923.

Softcover reprint of the hardcover 1st edition 1923

Vorwort.

In ihren elementareren Teilen besteht die Gruppentheorie aus einer Reihe vielleicht nicht immer völlig organisch zusammenhängender Methoden und Begriffe, und die Gliederung des Stoffes ist hier schon in hohem Maße festgelegt. Wem unsere Darstellung etwas knapp erscheint, den verweisen wir zur Ergänzung auf die ausgezeichneten und ausführlichen Darstellungen von *Weber* (Algebra, Bd. 2) und von *Netto* (Gruppen- und Substitutionentheorie, Leipzig 1908). Beim Studium dieser Anfangsteile braucht man sich keineswegs streng an die Reihenfolge der Paragraphen zu halten, sondern im allgemeinen werden die ersten Paragraphen der einzelnen Kapitel leicht verständlich sein, die späteren dagegen wesentlich schwerer.

Erst mit der Theorie der Substitutionsgruppen setzt eine weittragende und systematische Theorie ein, die, wie wir am Schluß zu zeigen versuchen, noch lange nicht ausgeschöpft ist. Sie kommt im Grunde auf eine zahlentheoretische Behandlungsweise heraus, deren Terminologie (Produkt, Multiplizieren usw.) ja bereits von Anfang an erscheint.

Entsprechend dem Plane dieser Sammlung von Einzeldarstellungen wurde den Anwendungen besondere Aufmerksamkeit gewidmet. Neben mannigfaltigen algebraischen und zahlentheoretischen Sätzen kommt hier in erster Linie die Kristallographie in Betracht. Diese besitzt ja gegenüber allen anderen Fällen des Gelingens mathematischer Naturbeschreibung den Vorzug größter begrifflicher Einfachheit und strengster arithmetischer Präzision.

Bei der Durchsicht der Korrekturen haben mich die Herren Prof. Dr. *R. Courant,* Prof. Dr. *R. Fueter* und Prof. Dr. *G. Polya* unterstützt und auf manche Verbesserungen hingewiesen, wofür ihnen hier aufs beste gedankt sei.

Mein Dank gilt ferner meiner Frau, die mir bei der Herstellung des Manuskriptes geholfen hat.

Zürich, im Dezember 1922.

A. Speiser.

Inhaltsverzeichnis.

1. Kapitel.

Die Grundlagen.

2. Kapitel.

Normalteiler und Faktorgruppen.

3. Kapitel.

Abelsche Gruppen.

4. Kapitel.

Konjugierte Untergruppen.

5. Kapitel.

Sylowgruppen und p-Gruppen.

6. Kapitel.

Kristallographische Gruppen.

7. Kapitel.

Permutationsgruppen.

8. Kapitel.

Automorphismen.

9. Kapitel.

Monomiale Gruppen.

10. Kapitel.

Darstellung der Gruppen durch lineare homogene Substitutionen.

11. Kapitel.

Gruppencharaktere.

12. Kapitel.

Anwendungen der Theorie der Gruppencharaktere.

13. Kapitel.

Aritmethische Untersuchungen über Substitutionsgruppen.

14. Kapitel.

Gruppen von gegebenem Grade.

15. Kapitel.

Gleichungstheorie.

1. Kapitel.

Die Grundlagen.

§ 1. Die Postulate des Gruppenbegriffs.

Ein System von Elementen bildet eine ***Gruppe,*** wenn folgende vier Postulate erfüllt sind:

I. Das Gruppengesetz: Jedem geordneten Paar von gleichen oder verschiedenen Elementen des Systems ist eindeutig ein Element desselben Systems zugeordnet, das ***Produkt*** der beiden Elemente. Die Formel dafür ist: $AB = C$.

II. Das Assoziativgesetz: Für die Produktbildung gilt die Gleichung: $(AB)C = A(BC)$. Nicht verlangt wird jedoch das ***Kommutativgesetz*** $AB = BA$.

III. Das Einheitselement: Es gibt ein Element E, das für jedes Element A des Systems folgendem Gesetz gehorcht: $AE = EA = A$. E heißt das ***Einheitselement*** oder die ***Einheit*** der Gruppe.

IV. Das inverse Element: Zu jedem Element A gibt es ein inverses Element A^{-1}, das der Gleichung genügt: $AX = E$.

Eine Gruppe, bei der alle Elemente mit einander vertauschbar sind, heißt eine ***kommutative*** oder ***Abelsche Gruppe.***

Ist die Anzahl der Elemente endlich, so heißt die Gruppe eine ***endliche Gruppe.*** Die Anzahl der Elemente heißt die ***Ordnung*** der Gruppe.

Die bekanntesten Gruppen sind *Abel*sche Gruppen mit unendlich vielen Elementen: Die ganzen positiven und negativen Zahlen bilden nach dem Gesetz der Addition eine Gruppe, ebenso die positiven rationalen Zahlen nach dem Gesetz der Multiplikation. Die „Einheit" ist im ersten Falle 0, im zweiten 1. Ferner bilden alle reellen Zahlen nach dem Gesetz der Addition und, nach Weglassung der Null, nach dem Gesetz der Multiplikation eine Gruppe.

Das Postulat II ist die knappste Fassung der allgemeinen Forderung, daß ein Produkt mehrerer Elemente eindeutig bestimmt ist,

wenn man die Reihenfolge der Elemente beibehält. Sein Inhalt ist eben diese Forderung für ein Produkt von drei Elementen. Durch einen einfachen Schluß von n auf $n+1$ läßt sich hieraus der allgemeine Satz beweisen. Man setze voraus, daß jedes Produkt von n oder weniger Elementen eindeutig bestimmt ist. Ist nun eine Reihe von $n+1$ Elementen vorgelegt, deren Produkt zu bilden ist, so führt jede Produktbildung bis zu einem Produkt von zwei Elementen, deren erstes das Produkt der i ersten ursprünglichen Elemente darstellt, während das zweite das Produkt der übrigen ist. Es muß nun bloß gezeigt werden, daß auch der letzte Schritt für jeden Wert von i dasselbe Resultat liefert. Ist I das Produkt der i ersten Elemente, A das $(i+1)$-te Element und K das Produkt der übrigbleibenden, so folgt aus dem zweiten Postulat:

$$I(AK) = (IA)K.$$

Indem man i der Reihe nach die Zahlen $1, 2, \ldots, n-2$ durchlaufen läßt, gewinnt man das gesuchte Resultat.

Läßt man noch das kommutative Gesetz zu, so ist ein Produkt durch die Elemente allein, unabhängig von der Reihenfolge, bestimmt. Es wird nämlich: $ABCD = A(BC)D = A(CB)D = ACBD$, woraus unmittelbar folgt, daß zwei aufeinanderfolgende Elemente miteinander vertauscht werden dürfen. Da man ferner durch derartige „Transpositionen" eine beliebige Reihenfolge herstellen kann, so ist die Behauptung bewiesen.

Das Postulat III fordert die Existenz eines Einheitselementes. *Allein* mit Hilfe des ersten Postulates läßt sich zeigen, daß nur *ein* Element vorkommen kann, das den dortigen Bedingungen genügt. Sei nämlich F ein weiteres Element, für das stets die Gleichungen $AF = FA = A$ erfüllt sind, so ergibt sich für EF gleichzeitig das Element E und F. Wegen I folgt $E = F$.

Das zu A^{-1} inverse Element ist A. Denn aus $A^{-1}B = E$ folgt durch linksseitige Multiplikation mit A: $AA^{-1}B = A$, also $B = A$. A ist mit A^{-1} vertauschbar.

Ist $ABC \ldots F$ ein beliebiges Produkt von Elementen, so ist $F^{-1} \ldots C^{-1}B^{-1}A^{-1}$ das inverse dazu.

Historische Notiz: Die *abstrakte* Gruppentheorie ist eine relativ späte Entwicklungsphase des mathematischen Gebildes, das unseren Gegenstand bildet. Noch *Jordans* Traité des substitutions (1870) behandelt *Permutationsgruppen*. Aber die Methoden, die *Gauß, Cauchy, Galois* und *Jordan* benutzen, sind großenteils unabhängig von dieser speziellen Bedeutung der Elemente. Das erste System abstrakter Gruppenpostulate soll das von *Kronecker* 1870 aufgestellte sein (Auseinandersetzung einiger Eigenschaften der Klassenzahl idealer komplexer Zahlen, Werke Bd. 2; p. 273). Neuerdings haben sich amerikanische Mathematiker mit der Aufstellung von Postulaten beschäftigt, z. B. *E. V. Huntington* (Note on the definition of abstract groups and fields by sets of independent postulates, Am. Transact. 6, p. 181.)

§ 2. Die Gruppentafel.

Eine Gruppe ist vollständig bestimmt, wenn das Produkt zweier beliebiger Elemente bekannt ist. Zur Tabellierung benutzt man, wenigstens in einfacheren Fällen, die ***Gruppentafel***, eine zuerst von *Cayley*[1]) angewandte Methode. Das Schema ist ein Quadrat mit ebensovielen Zeilen resp. Kolonnen, als die Ordnung der Gruppe beträgt. Man bringt die Elemente, mit E beginnend, in eine bestimmte Reihenfolge, und bezeichnet sowohl die Zeilen als die Spalten der Reihe nach damit. In die Parzelle, welche durch den Durchschnitt der mit A bezeichneten Zeile und der mit B bezeichneten Kolonne gebildet wird, schreibt man das Produkt AB. Wir geben als Beispiel die Gruppe niedrigster Ordnung, in welcher das kommutative Gesetz nicht gilt:

	E	A	B	C	D	F
E	E	A	B	C	D	F
A	A	B	E	D	F	C
B	B	E	A	F	C	D
C	C	F	D	E	B	A
D	D	C	F	A	E	B
F	F	D	C	B	A	E

Man erkennt sofort als charakteristisches Merkmal für Gruppen mit dem kommutativen Gesetz die Symmetrie der Tafel in bezug auf die Hauptdiagonale. In der angegebenen Gruppe gilt aber z. B.: $AC = CB \neq CA$.

Dem Assoziativgesetz entspricht keine in die Augen fallende Eigenschaft der Tafel, dagegen stellt die Tatsache, daß in jeder Zeile und in jeder Kolonne jedes Element der Gruppe genau einmal vorkommt, eine fundamentale Eigenschaft aller Gruppen dar, wie folgendermaßen bewiesen wird:

Die Elemente einer Zeile sind in dem Ausdruck AX enthalten, wobei A ein festes Element darstellt, während X die ganze Gruppe durchläuft. Die Gleichung $AX = B$ läßt bei beliebigem A und B die eine Auflösung zu: $X = A^{-1}B$. Hieraus folgt, daß in dem System von der Gestalt AX jedes Element der Gruppe enthalten ist. Andererseits aber auch nur einmal; für endliche Gruppen ergibt sich das durch bloße Abzählung der Elemente, für unendliche muß man verwerten, daß aus $AB = AC$ folgt: $B = C$. Denn „multipliziert" man die Gleichung auf beiden Seiten von links mit A^{-1}, so erhält man: $A^{-1}AB = A^{-1}AC$ und daraus wegen des Assoziativgesetzes: $B = C$.

Eine modifizierte Tafel, die für spätere Untersuchungen von Wichtigkeit ist, erhält man, indem man entsprechende Zeilen und

[1]) Phil. Mag. (4) 7 (1854), p. 40.

Kolonnen nicht mit denselben, sondern mit inversen Elementen bezeichnet, in folgender Weise:

	E	A	B	C	$\cdots$
E	E	A	B	C	$\cdots$
A^{-1}	A^{-1}	E	$A^{-1}B$	$A^{-1}C$	$\cdots$
B^{-1}	B^{-1}	$B^{-1}A$	E	$B^{-1}C$	$\cdots$
C^{-1}	C^{-1}	$C^{-1}A$	$C^{-1}B$	E	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$

Die oben angeführte Gruppe nimmt dann folgende Gestalt an:

	E	A	B	C	D	F
E	E	A	B	C	D	F
B	B	E	A	F	C	D
A	A	B	E	D	F	C
C	C	F	D	E	B	A
D	D	C	F	A	E	B
F	F	D	C	B	A	E

Man bemerkt, daß in der Hauptdiagonalen stets E steht.

Satz 1: *Für endliche Gruppen lassen sich die Postulate* III *und* IV *ersetzen durch das Postulat* III*, *das für gewisse Anwendungen bequemer ist:*

III*: *Aus* $AB = AC$ *folgt* $B = C$ *und aus* $BA = CA$ *folgt ebenfalls* $B = C$.

Beweis: Das Postulat besagt für endliche Gruppen, daß AX und XA mit X die sämtlichen Elemente der Gruppe durchlaufen. Denn ist g die Ordnung der Gruppe, so stellt AX g Elemente dar, die wegen des Postulates III* voneinander verschieden sind, und daher mit den Elementen der Gruppe übereinstimmen müssen. Insbesondere läßt die Gleichung $AX = A$ eine Lösung zu, die mit E bezeichnet werde. Aus $AE = A$ folgt: $XAE = XA$ wegen des Assoziativgesetzes; also gilt für jedes Element der Gruppe: $XE = X$ und insbesondere: $EE = E$. Aber auch EX durchläuft mit X sämtliche Elemente der Gruppe und aus $EEX = EX$ folgt ebenso wie vorher, daß für jedes Element X der Gruppe die Gleichung gilt: $EX = X$. Damit ist das Postulat III aus dem Postulat III* abgeleitet. Das Postulat IV folgt sofort aus der Tatsache, daß die Gleichung $AX = E$ eine Lösung besitzen muß, weil AX alle Elemente, also auch das soeben nachgewiesene Element E, durchlaufen muß.

Für unendliche Systeme folgt aus III* nicht die Existenz des Einheitselementes. Die positiven ganzen Zahlen bilden nach dem

Gesetz der Addition ein System, das I, II und III* genügt, aber keine Gruppe bildet.

Im folgenden soll stets, falls nichts anderes bemerkt ist, ausschließlich von endlichen Gruppen die Rede sein.

§ 3. Untergruppen.

Definition: Ein Teilsystem von Elementen der Gruppe, das für sich den Postulaten I bis IV genügt, und daher selbst eine Gruppe bildet, heißt eine ***Untergruppe*** der gegebenen Gruppe.

Zwei Untergruppen lassen sich von vornherein angeben, nämlich einerseits die gegebene Gruppe selbst, andererseits das Element E, das offenbar für sich eine Gruppe bildet. Diese beiden Untergruppen werden durch den Ausdruck ***uneigentliche Untergruppen*** von den übrigen, den ***eigentlichen Untergruppen*** unterschieden. Die Auffindung der eigentlichen Untergruppen ist eine der Hauptaufgaben der Theorie.

Teilsysteme werden erzeugt z. B. durch fortgesetzte Multiplikation eines Elementes mit sich selbst. Man schreibt: $AA = A^2$, $AAA = A^3$ usw. und bezeichnet diese neuen Elemente als die ***Potenzen*** von A. Sie bilden unter sich ein System, in dem das Postulat I erfüllt ist, denn das Produkt der n-ten Potenz von A mit der m-ten ist gleich der $(m+n)$-ten Potenz von A: $A^m A^n = A^{m+n}$. Ferner ist das *Assoziativgesetz* erfüllt, und hieraus folgt in diesem speziellen Falle noch das *Kommutativgesetz*: Sei $n > m$ und $n = m + l$, dann wird $A^n A^m = (A^m A^l) A^m = A^m (A^l A^m) = A^m A^n$.

Satz 2: *In endlichen Gruppen bildet ein Element A zusammen mit seinen Potenzen eine kommutative Untergruppe, die durch A* ***erzeugte*** *Untergruppe. Gauß* nennt sie die ***Periode*** *von A.* Die Ordnung dieser Untergruppe heißt auch die ***Ordnung des Elementes A.***

Beweis: Da nach Voraussetzung nur endlich viele Elemente in der Gruppe vorhanden sind, so können bei fortgesetzter Potenzierung nur endlich viele verschiedene Elemente entstehen. Sei die $(n+1)$-te Potenz von A die niedrigste, welche gleich einer früheren Potenz von A ist, dann gilt eine Gleichung von der Gestalt: $A^{n+1} = A^m$. Hier muß m gleich 1 sein, denn durch Multiplikation mit A^{-1} erhält man $A^n = A^{m-1}$. Wäre also $m > 1$, so wäre bereits die n-te Potenz von A gleich einer niedrigeren, gegen die Voraussetzung. Aus $A^{n+1} = A$ folgt $A^n = E$ und $A^{n+i} = A^i$. Diese Bezeichnungsweise läßt sich nun auch auf negative Potenzen von A ausdehnen. Bereits ist das inverse Element von A mit A^{-1} bezeichnet worden. Aus $A^n = E$ ergibt sich $A^{n-1} = A^{-1}$, eine Formel, die aus der vorhergehenden hervorgeht für $i = -1$. Hiermit ist bewiesen, daß unter den Potenzen von A das Einheitselement vorkommt (Postulat III), und daß

zu jedem der n-Elemente $A, A^2, A^3, \ldots, A^{n-1}, E$ auch das inverse eine Potenz von A ist: $A^m A^{n-m} = E$, d. h. A bildet zusammen mit seinen Potenzen eine Gruppe, w. z. b. w.

Eine Gruppe, die durch ein Element erzeugt werden kann, heißt eine ***zyklische*** Gruppe.

Satz 3[1]: *Die Ordnung einer Untergruppe ist ein Teiler der Ordnung der ganzen Gruppe.*

Beweis: Die Gruppe sei mit $\mathfrak{G}$, die Untergruppe mit $\mathfrak{H}$ bezeichnet, ihre Ordnungen seien g und h. A sei ein Element von $\mathfrak{G}$ außerhalb von $\mathfrak{H}$, und X durchlaufe die sämtlichen Elemente der Untergruppe $\mathfrak{H}$. Alsdann durchläuft XA h Elemente, die unter sich verschieden sind. Sie sind aber auch von den Elementen der Untergruppe verschieden. Denn gesetzt der Fall, XA sei gleich einem Element H aus $\mathfrak{H}$, dann folgt aus der Gleichung: $XA = H$ durch linksseitige Multiplikation mit X^{-1}:

$$A = X^{-1}H.$$

Da X und H in $\mathfrak{H}$ enthalten sind, so ergibt sich der Widerspruch, daß A selbst in $\mathfrak{H}$ enthalten ist.

Die Gesamtheit der Elemente, die durch XA geliefert werden, wenn X die Elemente von $\mathfrak{H}$ durchläuft, heißt eine ***Nebengruppe*** von $\mathfrak{H}$ und wird symbolisch mit $\mathfrak{H}A$ bezeichnet. Möglicherweise ist durch die Elemente von $\mathfrak{H}$ und $\mathfrak{H}A$ zusammen bereits die ganze Gruppe erschöpft; sie ist alsdann von der Ordnung $2h$. Andernfalls gibt es noch ein weiteres Element außerhalb von $\mathfrak{H}$ und $\mathfrak{H}A$, etwa B. Mit diesem bildet man die Nebengruppe $\mathfrak{H}B$. Sie besteht wie $\mathfrak{H}A$ aus h verschiedenen Elementen, die von denen in $\mathfrak{H}$ verschieden sind. Aber auch $\mathfrak{H}A$ und $\mathfrak{H}B$ besitzen keine gemeinsamen Elemente, denn wäre $XA = YB$, (X und Y in $\mathfrak{H}$), so würde folgen: $Y^{-1}XA = B$. Da $Y^{-1}X$ in $\mathfrak{H}$ liegt, so folgt gegen die Voraussetzung, daß B bereits in der Nebengruppe $\mathfrak{H}A$ vorkommt. Ist durch die Elemente von $\mathfrak{H}$, $\mathfrak{H}A$ und $\mathfrak{H}B$ die Gruppe noch nicht erschöpft, so erhält man in gleicher Weise, wie bisher, eine neue Nebengruppe, die mit keiner der früheren ein Element gemeinsam hat. Das Verfahren muß nach einer endlichen Anzahl von Schritten ein Ende nehmen, so daß jedes Element der Gruppe $\mathfrak{G}$ genau in einer Nebengruppe untergebracht ist. Wir schreiben symbolisch: $\mathfrak{G} = \mathfrak{H} + \mathfrak{H}A + \mathfrak{H}B + \mathfrak{H}C + \ldots$. Aus dieser Verteilung der Elemente von $\mathfrak{G}$ in $\mathfrak{H}$ und seine Nebengruppen folgt der Satz ohne weiteres.

Als besonders wichtiger Spezialfall ist hervorzuheben, daß die

---

[1]) *J. L. Lagrange*: Réflexions sur la résolution algébrique des équations (Œuvres t. **3**, p. 205 bis 421). Der Algorithmus des Beweises geht auf *Euler* zurück (opera omnia I 2, S. 504).

Ordnung jedes Elementes ein Teiler der Ordnung der Gruppe ist. Denn die Ordnung eines Elementes ist gleichzeitig die Ordnung einer Untergruppe.

Kriterium für Untergruppen. *Ein Teilsystem von Elementen einer Gruppe bildet stets eine Untergruppe, wenn das Produkt zweier beliebiger Elemente desselben wieder im System liegt.*

Dieses Kriterium besagt, daß für Untergruppen von Gruppen endlicher Ordnung der Nachweis der Gültigkeit des ersten Gruppenpostulates genügt. Aus diesem folgt nämlich, daß mit dem Element A auch dessen Quadrat, also auch dessen dritte usw. Potenz, daher auch E und A^{-1} im System enthalten sind, womit für das System die Gültigkeit aller vier Gruppenpostulate nachgewiesen ist.

Unter dem ***Index*** einer Untergruppe versteht man die Anzahl der Nebengruppen, also bei endlichen Gruppen den Quotienten aus der Ordnung der Gruppe und derjenigen der Untergruppe.

Untergruppen einer Untergruppe sind selbst Untergruppen der ursprünglichen Gruppe. Diejenigen Elemente, die zwei Untergruppen einer Gruppe gemeinsam sind, bilden eine *Untergruppe*, welche der ***Durchschnitt*** der beiden Untergruppen genannt wird. Denn mit A und B ist auch das Produkt AB beiden Untergruppen gemeinsam.

§ 4. Beispiele von Gruppen.

Die „Elemente" einer Gruppe sind wie die Elemente einer Menge an keine Deutung gebunden und können in mannigfaltiger Weise auftreten. Wenn an einem Beispiel eine Gruppe aufgewiesen wird, so spricht man von einer ***Darstellung der Gruppe.*** Die abstrakte Gruppe, die dargestellt wird, erhält man aus ihrer Darstellung, indem man von der speziellen Bedeutung der Elemente abstrahiert. Daß bei dieser Abstraktion das Wesentliche bestehen bleibt, wird sich im Verlauf der Theorie immer mehr herausstellen.

In diesem Paragraphen soll zunächst ein Musterexemplar einer Gruppe in verschiedenen Darstellungen gegeben und in Augenschein genommen werden, die sogenannte ***Ikosaedergruppe***[1]).

Eine Kugel, deren Mittelpunkt festliegt, kann bekanntlich von jeder Lage in jede andere durch Drehung um eine Achse durch ihren Mittelpunkt übergeführt werden. Zwei Drehungen um dieselbe Achse, deren Drehwinkel sich bloß um Vielfache von 2π unterscheiden, ergeben dieselbe Endlage und sollen im folgenden als identisch gelten. Zwei Drehungen, von denen das nicht gilt, ergeben stets verschiedene Endlagen und gelten als verschieden. Führt man zwei Drehungen nacheinander aus, so läßt sich eine einzige Drehung an-

[1]) Vgl. *F. Klein*, Vorlesungen über das Ikosaeder (Leipzig 1884).

geben, welche die Anfangslage der Kugel in die Endlage überführt. Man hat damit jedem Paar von Drehungen eine neue Drehung zugeordnet. Nach diesem Gesetz der Zusammensetzung bilden die Drehungen der Kugel in sich selbst eine Gruppe. Das Einheitselement ist die Drehung um den Winkel 0 oder die Überführung der Kugel in dieselbe Lage. Die inverse Drehung ist eine Drehung um dieselbe Achse, aber um den entgegengesetzten Winkel. Außerdem gilt das Assoziativgesetz. Diese Gruppe ist von unendlicher Ordnung; man nennt sie eine *kontinuierliche Gruppe* weil ihre Elemente durch stetig veränderliche Parameter (Richtung der Drehachse und Sinus und Kosinus des Drehwinkels) charakterisiert werden können.

Aus dieser Gruppe lassen sich durch die Forderung der *Invarianz gewisser Figuren* endliche Gruppen ausscheiden. Diejenigen Drehungen, welche einen der Kugel einbeschriebenen regulären Körper mit sich selbst in Deckung bringen, bilden eine Gruppe. Wir bestimmen ihre *Ordnung* durch Abzählung der verschiedenen *Deckungslagen*. Beispiel: das *Oktaeder*. Hält man zwei gegenüberliegende Ecken und die sie verbindende Achse fest, so gibt es noch die vier Drehungen um die Winkel $0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$. An die Stelle der einen Ecke kann man jede der fünf übrigen Ecken bringen und für jede Ecke hat man vier Lagen des Oktaeders in Rechnung zu setzen, so daß im ganzen 24 Lagen entstehen. Der *Würfel* bietet nichts Neues, denn die Mittelpunkte der Seiten eines Oktaeders bilden die Ecken eines Würfels, der bei denselben Drehungen und bei keinen weiteren mit sich selbst zur Deckung kommt. Dagegen liefert das *Tetraeder* eine wesentlich neue Gruppe, deren Ordnung sofort auf 12 berechnet wird, endlich ergibt das *Ikosaeder* eine Gruppe von der Ordnung 60. Das *Pentagondodekaeder* liefert dieselbe Gruppe, da seine Eckpunkte wiederum mit den Mittelpunkten der 20 Seitenflächen des Ikosaeders in Beziehung stehen.

Außer diesen Polyedern müssen noch die sogenannten *Dieder* in Betracht gezogen werden, da sie besonders übersichtliche und für den Aufbau komplizierterer Gruppen wichtige Gruppen liefern. Ein Dieder besteht aus der doppelt zu zählenden Fläche eines regelmäßigen ebenen n-Ecks. Sein Mittelpunkt sei in den Kugelmittelpunkt gebracht. Alsdann gibt es genau $2n$ Drehungen der Kugel, welche das Dieder mit sich selbst zur Deckung bringen. Eine Drehung vom Winkel $\frac{2\pi}{n}$ um eine Achse senkrecht zur Fläche sowie die $n-1$ daraus durch Wiederholung entstehenden Drehungen mit den Winkeln $2\cdot\frac{2\pi}{n}, \ldots, n\cdot\frac{2\pi}{n}$ bilden die eine Hälfte. Dazu kommen noch n Drehungen vom Winkel π um die n Achsen auf der Diederfläche, die durch die

Eckpunkte resp. Kantenmittelpunkte gehen. Die ersten n seien mit $A, A^2, \ldots, A^n = E$ bezeichet; die übrigen n bilden die Nebengruppe dieser zyklischen Untergruppe. Sei C eines dieser letzteren Elemente, so gilt die geometrisch sofort ersichtliche Beziehung: $AC = CA^{-1}$. Daraus folgt weiter: $AAC = ACA^{-1} = CA^{-1}A^{-1}$ und schließlich: $A^iC = CA^{-i}$. Hieraus folgt weiter die geometrisch erkannte Tatsache, daß alle Elemente der Nebengruppe die Ordnung 2 haben: $A^iCA^iC = A^iCCA^{-i} = E$. Einen speziellen Fall der Diedergruppen bildet die in § 2 durch die Gruppentafel gegebene Gruppe. Hier ist $n = 3$.

Nun sollen die *Elemente* der Ikosaedergruppe angegeben werden. Die Drehung von $\frac{2\pi}{5}$ um eine Achse durch zwei gegenüberliegende Ecken des Ikosaeders erzeugt eine Untergruppe von der Ordnung 5, deren 4 von E verschiedene Elemente die Ordnung 5 haben. Im ganzen gibt es 6 solche Achsen, die zusammen 24 verschiedene Elemente von der Ordnung 5 ergeben. Drehungen um eine Achse durch die Mittelpunkte zweier gegenüberliegenden Seitenflächen ergeben Untergruppen von der Ordnung 3, die je 2 Elemente von der Ordnung 3 enthalten. Da es 10 solche Achsen gibt, so folgen hieraus 20 Elemente von der Ordnung 3. Die Drehungen von π um die 15 Achsen, welche je zwei gegenüberliegende Kantenmittelpunkte verbinden, liefen noch 15 Elemente von der Ordnung 2. Nimmt man das Einheitselement dazu, so sind damit alle 60 Elemente erschöpft, denn $1 + 24 + 20 + 15 = 60$.

Nach den Elementen müssen die *Untergruppen* aufgewiesen werden. Bereits sind 15 von der Ordnung 2, 10 von der Ordnung 3 und 6 von der Ordnung 5 aufgefunden, die übrigen entsprechen wieder geometrischen Invarianten.

Außer den 5 Drehungen um eine Achse durch Eckpunkte gibt es noch 5 Drehungen von π, welche diese Achse in sich selbst überführen, nämlich solche um gewisse Achsen senkrecht dazu. Damit erhält man eine Diedergruppe von der Ordnung 10, deren es entsprechend den 6 Achsen 6 gibt. Die 10 Achsen durch Seitenmittelpunkte ergeben ebensoviele Diedergruppen von der Ordnung 6, und die 15 Achsen durch die Kantenmittelpunkte liefern schließlich 5 Diedergruppen von der Ordnung 4. Hierzu kommen als die merkwürdigsten noch 5 Untergruppen von der Ordnung 12, die der folgenden geometrischen Tatsache entsprechen: Zu jeder Kante gibt es eine ihr gegenüberliegende parallele. Man denke sich ein solches Kantenpaar in der XZ-Ebene parallel der X-Achse eines rechtwinkligen räumlichen Koordinatensystems. Man erkennt nun sofort, daß es ein weiteres Kantenpaar parallel der Y-Achse, und ein drittes parallel der Z-Achse gibt. Die 15 Kantenpaare zerfallen so in fünf Systeme, von

denen jedes 3 Paare enthält, die unter sich ein orthogonales System bilden und je eine der 5 oben erwähnten Diedergruppen von der Ordnung 4 liefern. Die Mittelpunkte der Kanten eines Systems bilden die Eckpunkte eines *Oktaeders*. Man kann sonach dem Ikosaeder 5 Oktaeder einbeschreiben, die bei den Drehungen sich untereinander vertauschen. Diejenigen Drehungen der Ikosaedergruppe, bei denen ein Oktaeder mit sich selbst zur Deckung gebracht wird, bilden eine Untergruppe, deren Index 5, deren Ordnung also 12 ist (vgl. auch § 8). Hierdurch ist gleichzeitig bewiesen, daß die Oktaedergruppe, deren Ordnung 24 ist, eine Untergruppe vom Index 2 enthält.

Hiermit ist folgende große Zahl von Untergruppen der Ikosaedergruppe gefunden worden: 15 Gruppen von der Ordnung 2, 10 von der Ordnung 3, 6 von der Ordnung 5. Diese 31 Untergruppen sind sämtlich zyklisch. Dazu kommen folgende Diedergruppen: 5 von der Ordnung 4, 10 von der Ordnung 6, 6 von der Ordnung 10. Schließlich gibt es noch 5 Untergruppen von der Ordnung 12, die gleichzeitig Untergruppen der Oktaedergruppe sind. Insgesamt sind 57 eigentliche Untergruppen aufgewiesen worden. Daß damit alle Untergruppen aufgezählt sind, ist ein Satz, der mit den Hilfsmitteln der vorigen Paragraphen nicht bewiesen werden kann.

Die Gruppentheorie hat ihren Ausgang genommen von den *Permutationsgruppen*, und es soll daher schon an dieser Stelle einiges darüber angemerkt werden. Bringt man eine Anzahl verschiedener Dinge, etwa die Zahlen 1 bis n, in eine bestimmte Reihenfolge, so pflegt man sie eine ***Permutation*** dieser n Dinge zu nennen, und man beweist leicht, daß es $n!$ verschiedene Anordnungen oder Permutationen von n verschiedenen Dingen gibt. In der Gruppentheorie versteht man unter einer Permutation die *Operation der Vertauschung*, und zwar ist eine solche Permutation vollständig bestimmt, wenn angegeben ist für jedes Ding, wodurch es ersetzt wird. Eine Permutation der Zahlen 1 bis n wird bezeichnet, indem man in einer ersten Zeile diese Zahlen in irgendeiner Reihenfolge, am besten in der natürlichen, aufschreibt und in eine zweite Zeile unter jede Zahl diejenige schreibt, durch die sie bei Vertauschung ersetzt wird. Die sämtlichen Permutationen der Zahlen 1, 2, 3 sind sonach:

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

Führt man zwei Permutationen hintereinander aus, so ist das Resultat wieder eine Permutation, die aus diesen beiden ***zusammengesetzte Permutation.*** Damit ist das Gesetz zur Gruppenbildung gegeben. Das Einheitselement ist die identische Permutation, die keine Vertauschung ausübt; das inverse Element besteht darin, daß die

Vertauschung wieder rückgängig gemacht wird. Die 6 oben hingeschriebenen Permutationen bilden eine Gruppe, deren Gruppentafel durch diejenige des § 2 gegeben ist, wenn man die Permutationen in der angegebenen Reihenfolge mit E, A, B, C, D, F bezeichnet. So ist z. B.

$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\quad \text{d. h.}\quad AC=D.$$

Denn A ersetzt 1 durch 2, C führt 2 in 3 über, durch AC wird daher 1 in 3 übergeführt, usw.

Die sämtlichen Permutationen von n Dingen bilden eine Gruppe von der Ordnung $n!$. Die 5 Oktaeder, die einem Ikosaeder einbeschrieben werden konnten, erfahren bei jeder Drehung eine Vertauschung. Daher läßt sich die Ikosaedergruppe als Permutationsgruppe von 5 Dingen darstellen, wodurch die zentrale Stellung des Ikosaeders in der Theorie der Gleichungen 5. Grades bedingt ist.

***Cayleys* Satz 4** [1]: *Jede Gruppe* $\mathfrak{G}$ *läßt sich als Permutationsgruppe ihrer Elemente darstellen.*

Beweis: Die Elemente von $\mathfrak{G}$ seien $E, A, B, \ldots$ und X sei ein beliebiges unter ihnen, dann stellt

$$\begin{pmatrix}E&A&B&C&\ldots\\EX&AX&BX&CX&\ldots\end{pmatrix}$$

eine Permutation derselben dar. Ist S ein Element von $\mathfrak{G}$, so ist die obige Permutation identisch mit der folgenden:

$$\begin{pmatrix}S&AS&BS&CS&\ldots\\SX&ASX&BSX&CSX&\ldots\end{pmatrix},$$

denn auch diese ersetzt jedes Element durch das rechts mit X multiplizierte, bloß die Reihenfolge in der Schreibweise ist geändert. Ferner entspricht den Elementen

$$Y\colon \begin{pmatrix}E,&A,&B,&\ldots\\Y,&AY,&BY,&\ldots\end{pmatrix}\quad\text{und}\quad XY\colon \begin{pmatrix}E,&A,&B,&\ldots\\XY,&AXY,&BXY,&\ldots\end{pmatrix}.$$

Nun ist

$$\begin{pmatrix}E&A&B&\ldots\\Y&AY&BY&\ldots\end{pmatrix}=\begin{pmatrix}X&AX&BX&\ldots\\XY&AXY&BXY&\ldots\end{pmatrix},$$

also

$$\begin{pmatrix}E&A&B&\ldots\\X&AX&BX&\ldots\end{pmatrix}\begin{pmatrix}E&A&B&\ldots\\Y&AY&BY&\ldots\end{pmatrix}=\begin{pmatrix}E&A&B&\ldots\\XY&AXY&BXY&\ldots\end{pmatrix},$$

d. h. die Zusammensetzung der zu X und Y gehörigen Permutationen liefert die zu XY gehörige, womit der Satz bewiesen ist.

[1] Vgl. Anm. auf S. 3.

Scholion.

Um die Wichtigkeit der vier Postulate nachzuweisen, sei folgendes Beispiel angegeben, bei dem bloß IV nicht erfüllt ist, das aber ersichtlich gar nichts mehr mit einer Gruppe zu tun hat: Die Elemente seien die Zahlen von 0 bis 100; zwei Zahlen sei als „Produkt" ihr größter gemeinschaftlicher Teiler zugeordnet. Dieses Gesetz genügt dem Postulat I sowie dem Assoziativ- und dem Kommutativgesetz. Die Zahl 0 bildet das Einheitselement, wenn 0 als größter gemeinschaftlicher Teiler von 0 mit sich selbst definiert wird, dagegen gibt es für die Zahlen von 0 bis 100 keine inversen Zahlen. Bildet man das „Produkt" der Zahlen von 0 bis 100 mit 5, so erhält man nur 1 oder 5, von einer Permutation der Zahlen ist also keine Rede mehr.

§ 5. Elementenkomplexe.

Ein System von Elementen aus einer Gruppe heißt ein ***Komplex.*** Wir bezeichnen einen solchen nach dem Vorgang von *Frobenius*[1]) stets mit deutschen Buchstaben, außer wenn er aus einem einzigen Element besteht, wo im allgemeinen lateinische Buchstaben angewendet werden. Besteht der Komplex $\mathfrak{C}$ aus den Elementen $A, B, C, \ldots$, so wird das nach *Galois* in Formeln ausgedrückt unter Benutzung des Pluszeichens: $\mathfrak{C} = A + B + C + \ldots$ Als weitere Regeln stellen wir folgende auf: $\mathfrak{A} + \mathfrak{B}$ bedeutet die Gesamtheit der in $\mathfrak{A}$ und $\mathfrak{B}$ enthaltenen Elemente, $\mathfrak{A}\mathfrak{B}$ die Gesamtheit der Produkte je eines Elementes aus $\mathfrak{A}$ mit einem Element aus $\mathfrak{B}$; jedes Element wird nur einmal gezählt. Einen speziellen Fall dieser Bezeichnung stellt diejenige der Nebengruppen $\mathfrak{H}A$ dar. Die notwendige und hinreichende Bedingung dafür, daß der Komplex $\mathfrak{C}$ eine Untergruppe ist, besteht in der Gleichung $\mathfrak{C}\mathfrak{C} = \mathfrak{C}$ (vgl. das Kriterium auf S. 7).

Stets gilt das Distributivgesetz:

$$(\mathfrak{A} + \mathfrak{B})(\mathfrak{C} + \mathfrak{D}) = \mathfrak{A}\mathfrak{C} + \mathfrak{A}\mathfrak{D} + \mathfrak{B}\mathfrak{C} + \mathfrak{B}\mathfrak{D}.$$

Zunächst muß nun die Einteilung der Elemente einer Gruppe nach einer Untergruppe und deren Nebengruppen näher untersucht werden. Bereits in § 3 wurde gezeigt, daß die Elemente einer Gruppe $\mathfrak{G}$ durch eine Untergruppe $\mathfrak{H}$ in Systeme zerfallen: $\mathfrak{G} = \mathfrak{H} + \mathfrak{H}A + \ldots$, deren Anzahl gleich ist dem Index von $\mathfrak{H}$ unter $\mathfrak{G}$. Diese Zerlegung ist unabhängig von der speziellen Wahl der die Nebengruppen erzeugenden Elemente $A \ldots$, denn zwei Elemente X und Y aus $\mathfrak{G}$ gehören dann und nur dann zur selben Nebengruppe, wenn XY^{-1} in $\mathfrak{H}$ liegt. Ist nämlich $XY^{-1} = H$, so wird

$$\mathfrak{H}X = \mathfrak{H}(HY) = (\mathfrak{H}H)Y = \mathfrak{H}Y.$$

[1]) Über endliche Gruppen (Berl. Sitzungsber. 1895, S. 163).

Ein Komplex von der Gestalt $\mathfrak{H} A$ heißt eine ***rechtsseitige Nebengruppe*** und die Zerlegung $\mathfrak{G} = \mathfrak{H} + \mathfrak{H} A + \ldots$ die ***rechtsseitige Zerlegung*** von $\mathfrak{G}$ nach $\mathfrak{H}$.

Ein Komplex von der Gestalt $A \mathfrak{H}$ heißt eine ***linksseitige Nebengruppe*** von $\mathfrak{H}$. Von diesen gelten entsprechende Sätze, wie von den rechtsseitigen. Hier sei nur der folgende bewiesen: Zwei Elemente B und C gehören dann und nur dann zu derselben linksseitigen Nebengruppe, wenn $B^{-1}C$ in $\mathfrak{H}$ liegt. Ist nämlich $B^{-1}C = H$, so wird: $C = BH$ und $B = CH^{-1}$, und umgekehrt folgt aus $B = AH_1$ und $C = AH_2$:

$$B^{-1}C = H_1^{-1}H_2.$$

Wir fassen dies zusammen in folgendem

Satz 5: *Eine Gruppe $\mathfrak{G}$ zerfällt durch eine Untergruppe $\mathfrak{H}$ von der Ordnung h und dem Index k in k Komplexe von je h Elementen, die Untergruppe und ihre rechtsseitigen Nebengruppen. Eine zweite Zerlegung mit entsprechenden Eigenschaften wird durch die Untergruppe und ihre linksseitigen Nebengruppen geliefert. Zwei Elemente X und Y gehören derselben rechts- resp. linksseitigen Nebengruppe an, wenn XY^{-1} resp. $X^{-1}Y$ in $\mathfrak{H}$ liegt.*

Die beiden Zerlegungen sind im allgemeinen voneinander verschieden und stimmen nur für Normalteiler (§ 6) überein.

Man beweist leicht folgende Tatsache:

Ist $$\mathfrak{G} = \mathfrak{H} + \mathfrak{H} A_2 + \ldots + \mathfrak{H} A_k$$

eine rechtsseitige Zerlegung, so ist

$$\mathfrak{G} = \mathfrak{H} + A_2^{-1}\mathfrak{H} + \ldots + A_k^{-1}\mathfrak{H}$$

eine linksseitige.

Unter $\{\mathfrak{A}\}$ versteht man die Gesamtheit der Elemente, die sich als Produkt von beliebig vielen Elementen aus $\mathfrak{A}$ darstellen lassen. Jedes Element aus $\mathfrak{A}$ darf im Produkt beliebig oft vorkommen. Selbstverständlich ist $\{\mathfrak{A}\}\{\mathfrak{A}\} = \{\mathfrak{A}\}$, daher ist $\{\mathfrak{A}\}$ eine Untergruppe, und zwar die kleinste, welche den Komplex $\mathfrak{A}$ enthält. Jede Untergruppe, die $\mathfrak{A}$ enthält, enthält auch $\{\mathfrak{A}\}$. $\{\mathfrak{A}\}$ heißt die durch den Komplex $\mathfrak{A}$ ***erzeugte*** Untergruppe. $\{A\}$ ist die durch das Element A erzeugte zyklische Gruppe: $A, A^2, A^3, \ldots, A^n = E$.

Eine Gruppe kann gegeben sein durch erzeugende Elemente und gewisse zwischen ihnen bestehende Relationen. Die Diedergruppe von der Ordnung $2n$ ist vollständig bestimmt durch zwei Elemente A und C mit den Relationen:

$$1)\quad A^n = E, \qquad 2)\quad C^2 = E, \qquad 3)\quad CA = A^{-1}C.$$

Alle Elemente sind enthalten in der Gestalt $A^x C^y (x = 0, 1, \ldots, n-1;$ $y = 0,1)$. Alle weiteren Produkte lassen sich mit Hilfe der Relation 3)

auf diese zurückführen, und als Produkt zweier beliebiger Elemente $A^x C^y$ und $A^z C^t$ findet sich leicht:

$$A^x C^y A^z C^t = A^{x+(-1)^y z} C^{y+t}.$$

Man verifiziere die Geltung des assoziativen Gesetzes!

Zwei Komplexe $\mathfrak{A}$ und $\mathfrak{B}$, für die $\mathfrak{A}\mathfrak{B} = \mathfrak{B}\mathfrak{A}$ ist, heißen untereinander *vertauschbar*. Bei der Diedergruppe ist z. B. $\{A\}C = C\{A\}$. Die Tatsache, daß ein Komplex $\mathfrak{A}$ mit einem Element B vertauschbar ist: $\mathfrak{A}B = B\mathfrak{A}$, kann auch so geschrieben werden: $B^{-1}\mathfrak{A}B = \mathfrak{A}$.

2. Kapitel.

Normalteiler und Faktorgruppen.

§ 6. Normalteiler.

Definition: Besteht zwischen zwei Elementen A und B einer Gruppe $\mathfrak{G}$ eine Beziehung von der Gestalt $B = X^{-1}AX$, wobei X ebenfalls in $\mathfrak{G}$ liegt, so heißen A und B ***konjugierte Elemente*** und man sagt: *B entsteht durch **Transformation** von A mit X.*

Für diese Beziehung gelten die Grundgesetze der Äquivalenz:

1. Ist A mit B konjugiert, so ist auch B mit A konjugiert. Aus $B = X^{-1}AX$ folgt nämlich $A = XBX^{-1} = (X^{-1})^{-1}B(X^{-1})$.

2. Ist A mit C und B mit C konjugiert, so ist auch A mit B konjugiert. Aus $C = X^{-1}AX$ und $C = Y^{-1}BY$ folgt:

$$B = YX^{-1}AXY^{-1} = (XY^{-1})^{-1}A(XY^{-1}).$$

Satz 6: *Bezeichnet man die mit einem Element konjugierten Elemente als eine **Klasse** von Elementen, so zerfällt die Gruppe in eine Anzahl von Klassen, die untereinander keine gemeinsamen Elemente besitzen. Elemente derselben Klasse besitzen dieselbe Ordnung.*

Beweis: Es gilt: $X^{-1}AX \cdot X^{-1}AX = X^{-1}A^2X$ und allgemein $(X^{-1}AX)^n = X^{-1}A^nX$. Ist daher $A^n = E$, so wird $(X^{-1}AX)^n = X^{-1}EX = E$ und ist umgekehrt $(X^{-1}AX)^n = E$, so wird $X^{-1}A^nX = E$ und daraus folgt $A^n = E$.

Allgemeiner gilt die Formel

$$X^{-1}AX \cdot X^{-1}BX = X^{-1}ABX,$$

die wir folgendermaßen interpretieren: *Aus einer Gleichung $AB = C$ geht durch Transformation der drei Elemente mit demselben Element X eine richtige Gleichung hervor.*

Bilden also die Elemente $E, A, B, \ldots$ eine Untergruppe $\mathfrak{H}$, so bilden auch $E, X^{-1}AX, X^{-1}BX, \ldots$ eine Untergruppe, die wir nach dem vorigen Paragraphen mit $X^{-1}\mathfrak{H}X$ bezeichnen.

Definition: $\mathfrak{H}$ *und* $X^{-1}\mathfrak{H}X$ *heißen* ***konjugierte*** *Untergruppen.*

Konjugierte Gruppen besitzen dieselbe Ordnung und als abstrakte Gruppen sind sie einander gleich. Kennt man die Gruppentafel von $\mathfrak{H}$, so ergibt sich diejenige von $X^{-1}\mathfrak{H}X$ dadurch, daß man die Elemente von $\mathfrak{H}$ durch die mit X transformierten Elemente ersetzt. Indem wir die eingehende Betrachtung dieses allgemeinen Falles auf das 4. Kapitel verschieben, gehen wir zu der Behandlung eines besonders wichtigen von *Galois* entdeckten Spezialfalles über.

Definition: Eine Untergruppe, die mit ihren konjugierten identisch ist, heißt ein ***Normalteiler*** (eine ***invariante*** oder ***ausgezeichnete Untergruppe***) der Gruppe.

Ist also die Untergruppe $\mathfrak{N}$ ein Normalteiler, so gilt für jedes Element X der ganzen Gruppe die Gleichung $X^{-1}\mathfrak{N}X = \mathfrak{N}$ oder $\mathfrak{N}X = X\mathfrak{N}$. Mit jedem Element A liegt auch jedes konjugierte Element $X^{-1}AX$ in $\mathfrak{N}$, d. h. *ein Normalteiler enthält mit jedem Element die ganze zugehörige Klasse von Elementen.* Diese Bedingung ist zugleich hinreichend dafür, daß eine Untergruppe einen Normalteiler bildet.

Beispiele:

1. *Die Abelschen Gruppen.* Hier bildet jedes Element für sich eine Klasse, jede Untergruppe ist Normalteiler.

2. *Die Diedergruppen.* Hier bildet die zyklische Untergruppe vom Index 2 einen solchen. Denn die ganze Gruppe zerfällt unter Anwendung der Bezeichnung auf S. 13 in die Nebengruppen $\{A\} + \{A\}C$. Wegen $C^{-1}AC = A^{-1}$ wird $C\{A\} = \{A\}C$.

Satz 7: *Der Durchschnitt zweier Normalteiler ist wieder ein Normalteiler.*

Beweis: Mit jedem Element ist die ganze zugehörige Klasse den beiden Normalteilern gemeinsam. Daher besteht auch der Durchschnitt aus einer Summe von Klassen und ist ein Normalteiler.

Dagegen ist ein Normalteiler eines Normalteilers nicht notwendig ein Normalteiler der ganzen Gruppe.

Satz 8: *Die mit allen Elementen einer Gruppe vertauschbaren Elemente bilden einen Abelschen Normalteiler, der das* ***Zentrum*** *der Gruppe genannt wird.*

Beweis: Aus $AX = XA$ und $BX = XB$ folgt $ABX = AXB = XAB$, d. h. mit zwei Elementen gehört auch deren Produkt dem Zentrum an. Das Zentrum bildet daher eine Untergruppe und zwar offenbar einen *Abel*schen Normalteiler. Ferner ist jede Untergruppe des Zentrums Normalteiler der ganzen Gruppe.

Als weitere Normalteiler erwähnen wir die durch die Elemente einer Klasse erzeugte Untergruppe. Denn ist $AB\ldots F$ ein Pro-

dukt von Elementen einer Klasse, so ist auch $X^{-1} A B \ldots F X = X^{-1} A X \cdot X^{-1} B X \ldots X^{-1} F X$ ein solches für jedes X. Daher enthält die Untergruppe die ganze durch $A B \ldots F$ repräsentierte Klasse und ist also Normalteiler.

Jede Gruppe $\mathfrak{G}$ besitzt zwei uneigentliche Normalteiler, nämlich ihre beiden uneigentlichen Untergruppen $\mathfrak{G}$ und E.

Wir definieren nun:

Definition: Eine Gruppe, die außer ihren beiden uneigentlichen Untergruppen keinen Normalteiler besitzt, heißt eine ***einfache*** Gruppe.

Offenbar sind alle Gruppen, deren Ordnung eine Primzahl ist, einfach. Sie sind zyklisch. Es gibt aber auch nicht-*Abel*sche einfache Gruppen.

Um hierfür ein Beispiel zu geben, wollen wir die Einfachheit der Ikosaedergruppe nachweisen, indem wir nur den Klassenbegriff benutzen. Schon jetzt sei aber bemerkt, daß die wirksamsten bisher bekannten Methoden zur Herstellung von einfachen Gruppen von der Theorie der Permutationsgruppen und der Kongruenzgruppen geliefert werden.

Die Elemente der Ikosaedergruppe lassen sich in folgender Weise in Klassen einteilen: Eine Drehung A von $\frac{2\pi}{5}$ um eine Achse durch eine Ecke besitzt die Ordnung 5. Sei X eine Drehung, welche irgendeine andere Ecke des Ikosaeders an ihre Stelle bringt; führt man dann die Drehung A aus und bringt die Ecke durch X^{-1} wieder an ihren alten Platz, so ist das Resultat $X A X^{-1}$ eine Drehung von $\frac{2\pi}{5}$ um diese Ecke. Hiermit ist nachgewiesen, daß 12 Operationen von der Ordnung 5 in eine Klasse gehören. Mit A gehört auch A^{-1} dazu, als Drehung um die gegenüberliegende Ecke. In gleicher Weise bilden die übrigen Elemente der Ordnung 5, nämlich die Drehungen um die Winkel $\frac{4\pi}{5}$, $\frac{6\pi}{5}$, eine Klasse. Daß diese beiden Klassen voneinander verschieden sind, folgt leicht aus dem eben Bewiesenen, braucht aber für das folgende nicht vorausgesetzt zu werden. Man beweist in gleicher Weise, daß alle 20 Elemente von der Ordnung 3 und alle 15 von der Ordnung 2 je eine Klasse bilden. Daher besitzt die Ikosaedergruppe folgende 5 Klassen: Das Einheitselement E bildet eine Klasse für sich, die 4 übrigen setzen sich aus 15, 20, 12 und 12 Elementen zusammen. Eine einfache Abzählung ergibt, daß kein Normalteiler vorhanden ist. Ein solcher müßte sich nämlich aus diesen Komplexen zusammensetzen, das Einheitselement enthalten und außerdem noch als Ordnung einen Teiler von 60 besitzen, was nicht möglich ist.

Definition: $C = B^{-1}A^{-1}BA$ heißt der ***Kommutator*** von A und B.

Offenbar gilt $BA = ABC$ und A und B sind dann und nur dann vertauschbar, wenn $C = E$ ist.

Satz 9: *Wenn zwei Normalteiler $\mathfrak{M}$ und $\mathfrak{N}$ einer Gruppe außer E kein gemeinsames Element besitzen, so ist jedes Element von $\mathfrak{M}$ mit jedem Element von $\mathfrak{N}$ vertauschbar.*

Beweis: Sei A in $\mathfrak{M}$ und B in $\mathfrak{N}$, dann liegt $B^{-1}AB$ in $\mathfrak{M}$, folglich auch $B^{-1}A^{-1}B$, denn dieses ist das inverse Element zum vorigen, daher schließlich auch der Kommutator $C = (B^{-1}A^{-1}B)A$. Andererseits liegt $C = B^{-1}(A^{-1}BA)$ auch in $\mathfrak{N}$, folglich ist C gleich dem einzigen $\mathfrak{M}$ und $\mathfrak{N}$ gemeinsamen Element E.

Historische Notiz. Der Begriff des Normalteilers wurde von *E. Galois* 1830 entdeckt (Lettre à *Auguste Chevalier*, Oeuvres publ. par *C. Picard*, p. 25, Paris 1897). Eine Publikation der Beweise erfolgte jedoch erst 1846 durch *Liouville* in seinem Journal. *Jordan* bezeichnete später seinen Traité des substitutions als einen Kommentar zu den Arbeiten von *Galois*.

§ 7. Faktorgruppen.

Ein Normalteiler $\mathfrak{N}$ und seine Nebengruppen können selbst als Elemente einer Gruppe aufgefaßt werden. Es gilt nämlich: $\mathfrak{N}A\,\mathfrak{N}B = \mathfrak{N}\,\mathfrak{N}A\,B = \mathfrak{N}AB$. Das Produkt zweier Nebengruppen des Normalteilers ist wieder eine Nebengruppe. Der Normalteiler selbst ist das Einheitselement und die zu $\mathfrak{N}A$ inverse Nebengruppe ist $\mathfrak{N}A^{-1}$.

Definition: Die Gruppe, deren Elemente durch einen Normalteiler $\mathfrak{N}$ von $\mathfrak{G}$ und seine Nebengruppen gebildet werden, heißt die ***Faktorgruppe*** oder ***Quotientengruppe*** des Normalteilers und wird mit $\mathfrak{G}/\mathfrak{N}$ bezeichnet. Ihre Ordnung ist gleich dem Index des Normalteilers.

Eine Gruppe ist nicht vollständig bestimmt durch einen Normalteiler und seine Faktorgruppe, aber ihre Ordnung ist das Produkt der Ordnungen des Normalteilers und der Faktorgruppe und die Analogie mit den Teilbarkeitseigenschaften der ganzen Zahlen kann weit fortgeführt werden.

Satz 10: *Eine Untergruppe der Faktorgruppe vom Index r besteht aus Nebengruppen, deren Elemente eine Untergruppe der ganzen Gruppe vom selben Index r bilden.*

Beweis: Die Untergruppe der Faktorgruppe bestehe aus den Nebengruppen $\mathfrak{H}$, $\mathfrak{H}A_2, \ldots, \mathfrak{H}A_s$. Nach Voraussetzung ist das Produkt zweier beliebiger von diesen Nebengruppen wieder eine solche. Daher liegt das Produkt zweier beliebiger Elemente des Komplexes $\mathfrak{H} + \mathfrak{H}A_2 + \ldots + \mathfrak{H}A_s$ in demselben Komplex und dieser bildet eine Untergruppe vom Index r.

Satz 11: *Jede Untergruppe $\mathfrak{H}$ von $\mathfrak{G}$, die einen Normalteiler $\mathfrak{N}$ von $\mathfrak{G}$ enthält, gehört zu einer Untergruppe der Faktorgruppe $\mathfrak{G}/\mathfrak{N}$.*

Beweis: $\mathfrak{N}$ ist Normalteiler von $\mathfrak{H}$, und es sei $\mathfrak{H} = \mathfrak{N} + \mathfrak{N}A_2 + \mathfrak{N}A_3 + \ldots + \mathfrak{N}A_s$. Diese Nebengruppen bilden die Elemente der Faktorgruppe $\mathfrak{H}/\mathfrak{N}$ und infolgedessen eine Untergruppe von $\mathfrak{G}/\mathfrak{N}$.

Durch diese beiden Sätze ist das Problem, diejenigen Untergruppen von $\mathfrak{G}$ zu finden, die einen Normalteiler $\mathfrak{N}$ enthalten, zurückgeführt auf das Problem, die sämtlichen Untergruppen von $\mathfrak{G}/\mathfrak{N}$ zu finden, da eine eindeutige Zuordnung zwischen ihnen hergestellt ist. Es gilt nun die weitere wichtige Tatsache, daß Normalteilern des einen Problems Normalteiler des anderen entsprechen:

Satz 12: *Jeder Normalteiler einer Faktorgruppe $\mathfrak{G}/\mathfrak{N}$ liefert einen Normalteiler von $\mathfrak{G}$; jeder Normalteiler, der $\mathfrak{N}$ enthält, entspricht einem Normalteiler der Faktorgruppe.*

Beweis: Die Nebengruppen $\mathfrak{N}, \mathfrak{N}A_2, \ldots, \mathfrak{N}A_s$ mögen einen Normalteiler von $\mathfrak{G}/\mathfrak{N}$ bilden. Dann gilt für jede beliebige Nebengruppe von $\mathfrak{N}$, etwa für $\mathfrak{N}X$, die Beziehung: $\mathfrak{N}X^{-1}\mathfrak{N}A_i\mathfrak{N}X = \mathfrak{N}A_i$. Hieraus folgt speziell, daß $X^{-1}\mathfrak{N}A_iX$ nur Elemente aus $\mathfrak{N}A_i$ enthält und daher damit identisch ist. Daher ist der Komplex $\mathfrak{N} + \mathfrak{N}A_2 + \ldots + \mathfrak{N}A_s$ mit allen Elementen von $\mathfrak{G}$ vertauschbar und bildet einen Normalteiler. Um auch den zweiten Teil der Behauptung zu beweisen, sei $\mathfrak{K} = \mathfrak{N} + \mathfrak{N}A_2 + \ldots + \mathfrak{N}A_s$ ein Normalteiler von $\mathfrak{G}$, der $\mathfrak{N}$ enthält. Dann gilt für jedes Element X von $\mathfrak{G}$ die Beziehung: $X^{-1}\mathfrak{K}X = \mathfrak{K}$ und insbesondere liegen die Elemente $X^{-1}\mathfrak{N}A_iX$ wieder in $\mathfrak{K}$. Es muß nun gezeigt werden, daß die Untergruppe $\mathfrak{K}/\mathfrak{N}$ von $\mathfrak{G}/\mathfrak{N}$ einen Normalteiler bildet, d. h. daß für beliebige X die Nebengruppe $\mathfrak{N}X^{-1}\mathfrak{N}A_i\mathfrak{N}X$ wieder in $\mathfrak{K}$ liegt. Diese Nebengruppe enthält aber speziell $X^{-1}\mathfrak{N}A_iX$ und liegt daher in $\mathfrak{K}$. In Formeln verläuft dieser Beweis folgendermaßen: Wegen $\mathfrak{N}X = X\mathfrak{N}$ ist $\mathfrak{N}X^{-1}\mathfrak{N}A_i\mathfrak{N}X = \mathfrak{N}\mathfrak{N}\mathfrak{N}X^{-1}A_iX = \mathfrak{N}X^{-1}A_iX$. Da mit A_i auch $X^{-1}A_iX$ zu $\mathfrak{K}$ gehört, so ist $\mathfrak{N}X^{-1}A_iX$ eine in $\mathfrak{K}$ liegende Nebengruppe.

Die Faktorgruppe kann nur für Normalteiler definiert werden, denn es gilt der

Satz 13: *Wenn das Produkt zweier beliebiger Nebengruppen einer Untergruppe $\mathfrak{H}$ stets wieder eine Nebengruppe von $\mathfrak{H}$ ist, so ist $\mathfrak{H}$ Normalteiler.*

Beweis: Sei h die Ordnung von $\mathfrak{H}$, dann enthält nach Voraussetzung bei beliebigem A und B der Komplex $\mathfrak{H}A\mathfrak{H}B$ h Elemente. Da E in $\mathfrak{H}$ vorkommt, so sind darunter die beiden Komplexe $\mathfrak{H}AB$ und $A\mathfrak{H}B$ enthalten und diese müssen identisch sein, da sie beide h Elemente besitzen. Daher gilt $\mathfrak{H}AB = A\mathfrak{H}B$ und, nach rechtsseitiger Multiplikation mit B^{-1}, $\mathfrak{H}A = A\mathfrak{H}$, womit der Satz bewiesen ist.

§ 8. Isomorphe und homomorphe Gruppen.

Zum Nachweis eines Normalteilers ist besonders wichtig der mit der Faktorgruppe aufs engste zusammenhängende Begriff der isomorphen Gruppen.

Definition: Ist jedem Element einer Gruppe $\mathfrak{G}$ ein und nur ein Element einer zweiten Gruppe $\mathfrak{G}'$ und jedem Element von $\mathfrak{G}'$ mindestens eines von $\mathfrak{G}$ zugeordnet dergestalt, daß auch dem Produkt zweier Elemente von $\mathfrak{G}$ das Produkt der zugeordneten Elemente von $\mathfrak{G}'$ entspricht, so heißt die Gruppe $\mathfrak{G}'$ ***isomorph*** mit $\mathfrak{G}$. Die Zuordnung heißt ein ***Isomorphismus*** von $\mathfrak{G}'$ mit $\mathfrak{G}$.

Aus der Definition folgt, daß die Ordnung von $\mathfrak{G}'$ höchstens gleich der Ordnung von $\mathfrak{G}$ ist. Sind die Ordnungen von $\mathfrak{G}$ und $\mathfrak{G}'$ identisch, so ist die Zuordnung der Elemente von $\mathfrak{G}$ und $\mathfrak{G}'$ eindeutig und die Gruppen sind als abstrakte Gruppen miteinander identisch. Sie heißen in diesem Fall ***homomorphe*** Gruppen.

Ist die Ordnung von $\mathfrak{G}'$ niedriger als diejenige von $\mathfrak{G}$, so muß es in $\mathfrak{G}$ mindestens zwei Elemente A und B geben, denen dasselbe Element A' von $\mathfrak{G}'$ entspricht. Das von E verschiedene Element AB^{-1} entspricht dann dem Einheitselement E' von $\mathfrak{G}'$. *Die Gesamtheit der Elemente von $\mathfrak{G}$, die E' entsprechen, bilden eine Untergruppe,* denn mit A und B entspricht auch AB dem Element $E'E' = E'$. *Diese Untergruppe ist Normalteiler,* denn dem Element $X^{-1}AX$ entspricht das Element $X'^{-1}E'X' = E'$ bei beliebigem X. Zwei Elementen X und Y von $\mathfrak{G}$ entspricht dann und nur dann dasselbe Element A' von $\mathfrak{G}'$, wenn XY^{-1} dem Einheitselement $A'A'^{-1} = E'$ entspricht, d. h. wenn sie in dieselbe Nebengruppe des Normalteilers $\mathfrak{N}$ gehören. Dem Produkt zweier Nebengruppen von $\mathfrak{N}$ entspricht das Produkt der zugeordneten Elemente von $\mathfrak{G}'$. Damit ist der Satz bewiesen:

Satz 14: *Ist $\mathfrak{G}'$ mit $\mathfrak{G}$ isomorph, so entspricht dem Einheitselement von $\mathfrak{G}'$ ein Normalteiler $\mathfrak{N}$ von $\mathfrak{G}$, und $\mathfrak{G}'$ ist homomorph mit der Faktorgruppe $\mathfrak{G}/\mathfrak{N}$.*

Ist eine einfache Gruppe mit einer anderen einfachen Gruppe isomorph, die aus mehr als einem Element besteht, so ist der Isomorphismus ein Homomorphismus. Die Vertauschungen der 5 Oktaeder beim Ikosaeder sind daher verschieden für zwei verschiedene Drehungen, denn die Gruppe der Vertauschungen der Oktaeder ist offenbar isomorph mit der Gruppe der Ikosaederdrehungen.

Mit Hilfe der bisherigen Entwicklungen ist es möglich, einen vollständigen Einblick in die Oktaedergruppe, auf der die Theorie der Gleichungen 4. Grades ruht, zu bekommen. Sie bildet ein außerordentlich lehrreiches Beispiel für die vorhergehenden Sätze.

Die drei Hauptachsen des Oktaeders, welche je zwei gegenüberliegende Ecken verbinden, mögen als die X-, Y- und Z-Achse bezeichnet werden. Jeder Oktaederdrehung entspricht eine Vertauschung dieser drei Achsen, und man sieht leicht, daß jede der sechs möglichen Vertauschungen dieser drei Achsen hervorgerufen wird. Damit ist ein Isomorphismus der Permutationsgruppe von drei Dingen mit der Gruppe der Oktaederdrehungen aufgedeckt, und infolgedessen besitzt die Oktaedergruppe, deren Ordnung 24 ist, einen Normalteiler $\mathfrak{N}$ von der Ordnung 4, bestehend aus denjenigen Drehungen, welche die drei Achsen in sich überführen. Diese vier Drehungen sind die identische sowie die drei Drehungen vom Winkel π um die drei Achsen. Ihre Faktorgruppe ist eine Diedergruppe von der Ordnung 6, welche einen Normalteiler vom Index 2 besitzt. Diesem entspricht ein Normalteiler der Oktaedergruppe von der Ordnung 12, bestehend aus $\mathfrak{N}$ und den 8 Drehungen von der Ordnung 3 um die Achsen durch zwei gegenüberliegende Seitenmittelpunkte. Auch dieser Normalteiler besitzt seine geometrische Deutung, die am besten am Würfel gezeigt werden kann, dessen Gruppe mit der Oktaedergruppe übereinstimmt. Der Würfel sei so aufgestellt, daß seine Kanten mit den Koordinatenachsen parallel sind. Der Normalteiler besteht wieder aus den drei Drehungen von π um die drei Koordinatenachsen und den Drehungen um Achsen durch die Eckpunkte. Aus den Eckpunkten kann man vier auswählen, welche gleichzeitig Eckpunkte eines einbeschriebenen Tetraeders sind. Auf der oberen Seite parallel der XY-Ebene seien es die beiden Ecken auf einer Diagonale von links vorne nach rechts hinten, auf der unteren diejenigen auf der Diagonale von rechts vorne nach links hinten. Die anderen vier Ecken bilden gleichfalls die Ecken eines einbeschriebenen Tetraeders. Bei jeder Drehung des Oktaeders erfahren diese zwei Tetraeder eine Vertauschung, und man überzeugt sich sofort, daß der Normalteiler aus denjenigen Drehungen besteht, bei denen jedes Tetraeder in sich übergeführt wird, während die übrigen Drehungen eine Vertauschung bewirken. Der Normalteiler von der Ordnung 12 ist homomorph mit der Gruppe der zwölf Tetraederdrehungen, er tritt auch als Untergruppe der Ikosaedergruppe auf.

Mit einer Gruppe ist die Faktorgruppe eines jeden ihrer Normalteiler isomorph. Häufig werden zwei Gruppen, die mit derselben Gruppe isomorph sind, unter sich als isomorph bezeichnet, doch soll diese Erweiterung des Begriffs hier nicht angewandt werden. Dagegen besteht das Gesetz, daß, wenn $\mathfrak{G}$ mit $\mathfrak{G}'$ und $\mathfrak{G}'$ mit $\mathfrak{G}''$ isomorph ist, dann auch $\mathfrak{G}$ mit $\mathfrak{G}''$ isomorph ist.

Ist eine mit $\mathfrak{G}$ isomorphe Gruppe gegeben, so kann der Isomorphismus oft auf mehrere Arten hergestellt werden, indem $\mathfrak{G}$ ver-

schiedene Normalteiler besitzen kann, deren Faktorgruppen homomorph sind. Beispiele dafür bieten sich schon unter den *Abel*schen Gruppen.

Ein Isomorphismus einer Gruppe mit sich selbst heißt ***Automorphismus.*** (8. Kapitel.)

§ 9. Der Hauptsatz über Normalteiler.

Unter einem ***größten Normalteiler*** einer Gruppe $\mathfrak{G}$ versteht man einen solchen, der in keinem anderen Normalteiler außer $\mathfrak{G}$ selbst enthalten ist. Eine Gruppe kann mehrere größte Normalteiler enthalten, und es gilt der folgende

Hauptsatz 15: *Sind* $\mathfrak{N}_1$ *und* $\mathfrak{N}_2$ *zwei größte Normalteiler von* $\mathfrak{G}$ *und ist* $\mathfrak{D}$ *ihr Durchschnitt, so bestehen zwischen den Faktorgruppen die Beziehungen:*

$$\mathfrak{G}/\mathfrak{N}_1 = \mathfrak{N}_2/\mathfrak{D} \qquad \mathfrak{G}/\mathfrak{N}_2 = \mathfrak{N}_1/\mathfrak{D}.$$

Beweis: Die durch $\mathfrak{N}_1$ und $\mathfrak{N}_2$ erzeugte Untergruppe $\mathfrak{N}_1\mathfrak{N}_2$ [1]) ist ein Normalteiler von $\mathfrak{G}$, der $\mathfrak{N}_1$ und $\mathfrak{N}_2$ enthält, und ist daher mit $\mathfrak{G}$ identisch. $\mathfrak{N}_1$ sei nach Nebengruppen von $\mathfrak{D}$ zerlegt: $\mathfrak{N}_1 = \mathfrak{D} + \mathfrak{D}A_2 + \mathfrak{D}A_3 + \ldots + \mathfrak{D}A_r$. Alsdann bilde man $\mathfrak{L} = \mathfrak{N}_2 + \mathfrak{N}_2A_2 + \mathfrak{N}_2A_3 + \ldots + \mathfrak{N}_2A_r$. Dieser Komplex enthält $\mathfrak{N}_2$ und $\mathfrak{N}_1$ und wir wollen zeigen, daß er mit $\mathfrak{N}_1\mathfrak{N}_2 = \mathfrak{G}$ identisch ist. Es ist nämlich:

$$\begin{aligned}\mathfrak{N}_1\mathfrak{N}_2 = \mathfrak{N}_2\mathfrak{N}_1 &= \mathfrak{N}_2(\mathfrak{D} + \mathfrak{D}A_2 + \ldots + \mathfrak{D}A_r)\\ &= \mathfrak{N}_2 + \mathfrak{N}_2A_2 + \ldots + \mathfrak{N}_2A_r = \mathfrak{L}\end{aligned}$$

wegen $\mathfrak{N}_2\mathfrak{D} = \mathfrak{N}_2$. Die Faktorgruppen $\mathfrak{G}/\mathfrak{N}_2$ und $\mathfrak{N}_1/\mathfrak{D}$ sind homomorph, denn aus $\mathfrak{N}_2A_i = \mathfrak{N}_2A_k$ folgt, daß $A_iA_k^{-1}$ in $\mathfrak{N}_2$ und daher in $\mathfrak{D}$ liegt, d. h. daß $i = k$ ist. Und ferner folgt aus $\mathfrak{N}_2A_i\mathfrak{N}_2A_k = \mathfrak{N}_2A_l$ sofort $\mathfrak{D}A_i\mathfrak{D}A_k = \mathfrak{D}A_l$, und umgekehrt. Damit ist die zweite Gleichung bewiesen. Die erste folgt durch Vertauschung der beiden Normalteiler.

Allgemeinere Fassung des Hauptsatzes: *Sind* $\mathfrak{H}$ *und* $\mathfrak{K}$ *zwei Untergruppen von* $\mathfrak{G}$ *und ist jedes Element von* $\mathfrak{K}$ *mit* $\mathfrak{H}$ *vertauschbar, bezeichnet ferner* $\mathfrak{L}$ *die Gruppe* $\mathfrak{H}\mathfrak{K}$ *und* $\mathfrak{D}$ *den Durchschnitt von* $\mathfrak{H}$ *und* $\mathfrak{K}$*, so ist* $\mathfrak{H}$ *Normalteiler von* $\mathfrak{L}$ *und* $\mathfrak{D}$ *Normalteiler von* $\mathfrak{K}$ *und* $\mathfrak{L}/\mathfrak{H} = \mathfrak{K}/\mathfrak{D}$.

Beweis: Ist K irgendein Element von $\mathfrak{K}$, so gilt: $K^{-1}\mathfrak{H}K = \mathfrak{H}$ und $K^{-1}\mathfrak{K}K = \mathfrak{K}$. Wenn D in $\mathfrak{D}$ liegt, so liegt daher auch $K^{-1}DK$ sowohl in $\mathfrak{H}$ als in $\mathfrak{K}$, also in $\mathfrak{D}$. Damit ist bewiesen, daß $\mathfrak{D}$ Normalteiler von $\mathfrak{K}$ ist. Nun sei $\mathfrak{K} = \mathfrak{D} + \mathfrak{D}K_2 + \ldots + \mathfrak{D}K_r$. Der Komplex $\mathfrak{L} = \mathfrak{H} + \mathfrak{H}K_2 + \ldots + \mathfrak{H}K_r$ bildet wieder eine Gruppe und $\mathfrak{H}$ ist Normalteiler von $\mathfrak{L}$. Denn stellt H irgendein Element aus $\mathfrak{H}$ vor, so

---

[1]) $\{\mathfrak{N}_1\mathfrak{N}_2\} = \mathfrak{N}_1\mathfrak{N}_2$; denn $\mathfrak{N}_1$ und $\mathfrak{N}_2$ sind vertauschbar, woraus folgt: $\mathfrak{N}_1\mathfrak{N}_2 \cdot \mathfrak{N}_1\mathfrak{N}_2 = \mathfrak{N}_1\mathfrak{N}_2$.

ist $(HK_i)^{-1}\mathfrak{H}(HK_i)=\mathfrak{H}$. Zwei Nebengruppen $\mathfrak{H}K_i$ und $\mathfrak{H}K_k$ sind stets verschieden, wenn i und k verschieden sind, denn sonst wäre $K_iK_k^{-1}$ in $\mathfrak{H}$ und also in $\mathfrak{D}$ gegen die Voraussetzung. Der Beweis verläuft von hier an wie oben.

Satz 16: *Ist $\mathfrak{N}$ ein Normalteiler von $\mathfrak{G}$, und $\mathfrak{H}$ irgendeine Untergruppe von $\mathfrak{G}$, ferner $\mathfrak{D}$ der Durchschnitt von $\mathfrak{N}$ und $\mathfrak{H}$, dann ist $\mathfrak{D}$ Normalteiler von $\mathfrak{H}$, und $\mathfrak{H}/\mathfrak{D}$ ist homomorph mit einer Untergruppe von $\mathfrak{G}/\mathfrak{N}$.*

Beweis: $\mathfrak{N}$ ist als Normalteiler von $\mathfrak{G}$ insbesondere mit jedem Element von $\mathfrak{H}$ vertauschbar. Eine Anwendung des vorhergehenden Satzes ergibt, daß $\mathfrak{D}$ Normalteiler von $\mathfrak{H}$ ist. Bezeichnet man wieder mit $\mathfrak{L}$ die durch $\mathfrak{H}$ und $\mathfrak{N}$ erzeugte Untergruppe von $\mathfrak{G}$, so wird $\mathfrak{H}/\mathfrak{D}=\mathfrak{L}/\mathfrak{N}$ und $\mathfrak{L}/\mathfrak{N}$ ist eine Untergruppe von $\mathfrak{G}/\mathfrak{N}$.

Ist s die niedrigste Potenz des Elementes A aus $\mathfrak{G}$, die in einem Normalteiler $\mathfrak{N}$ von $\mathfrak{G}$ liegt, so ist s ein Teiler des Indexes von $\mathfrak{N}$ unter $\mathfrak{G}$. Denn $\mathfrak{N}+\mathfrak{N}A+\ldots+\mathfrak{N}A^{s-1}$ bildet eine Untergruppe von $\mathfrak{G}$.

§ 10. Kompositionsreihen.

Definition: Ist $\mathfrak{N}_1$ ein größter Normalteiler von $\mathfrak{G}$, $\mathfrak{N}_2$ ein größter Normalteiler von $\mathfrak{N}_1$ (der nicht notwendig Normalteiler von $\mathfrak{G}$ zu sein braucht), $\mathfrak{N}_3$ ein größter Normalteiler von $\mathfrak{N}_2$ usw., so erhält man eine Reihe von Untergruppen, deren jede in der vorhergehenden enthalten ist und die mit $\mathfrak{E}$ schließt: $\mathfrak{G}, \mathfrak{N}_1, \mathfrak{N}_2, \ldots, \mathfrak{N}_r=E$. Diese Reihe heißt eine ***Kompositionsreihe*** von $\mathfrak{G}$.

Die Faktorgruppen zweier aufeinanderfolgenden Gruppen der Reihe: $\mathfrak{G}/\mathfrak{N}_1, \mathfrak{N}_1/\mathfrak{N}_2, \ldots, \mathfrak{N}_{r-1}/\mathfrak{N}_r$ sind lauter einfache Gruppen, denn wenn $\mathfrak{N}_i/\mathfrak{N}_{i+1}$ einen Normalteiler besäße, so gäbe es einen Normalteiler von $\mathfrak{N}_i$, der $\mathfrak{N}_{i+1}$ als eigentlichen Normalteiler enthielte gegen die Voraussetzung. Diese einfachen Gruppen sollen als die ***Primfaktorgruppen*** oder einfacher als die Primfaktoren der Kompositionsreihe bezeichnet werden.

Fundamentalsatz 17 *von Jordan-Hölder*[1]*: Für zwei beliebige Kompositionsreihen stimmen die Primfaktorgruppen in ihrer Gesamtheit, aber nicht notwendig in ihrer Reihenfolge, überein.*

Dieser Satz bildet ein gewisses Analogon zu dem Satz über die eindeutige Zerlegbarkeit einer ganzen Zahl in Primfaktoren. Immerhin ist zu bemerken, daß eine Gruppe durch die Primfaktorgruppen der Kompositionsreihen nur in speziellen Fällen, z. B. wenn sie einfach ist, vollständig bestimmt ist, und daß bei gegebener Reihenfolge der Primfaktorgruppen nicht notwendig eine Kompositionsreihe existiert, welche gerade diese Reihenfolge liefert.

---

[1]) *C. Jordan* bewies die Gleichheit der *Ordnungen* der Faktorgruppen; *O. Hölder*: Math. Ann. **34** (1897), S. 37, die Gleichheit der Faktorgruppen.

Beweis: Der Satz ist selbstverständlich für einfache Gruppen und daher für alle Gruppen, deren Ordnung eine Primzahl ist. Zum Beweis des allgemeinen Satzes wendet man vollständige Induktion an. Der Satz sei bewiesen für alle Gruppen, deren Ordnung ein Produkt von weniger als n Primzahlen sind, und die Ordnung von $\mathfrak{G}$ sei ein Produkt von n Primzahlen. Man darf ferner voraussetzen, daß $\mathfrak{G}$ einen eigentlichen Normalteiler besitzt, da der Satz für den anderen Fall selbstverständlich ist. Wenn $\mathfrak{G}$ nur *einen* größten Normalteiler besitzt, so folgt der Satz sofort aus der Voraussetzung. Es seien daher zwei Kompositionsreihen von $\mathfrak{G}$ gegeben mit verschiedenem erstem Normalteiler: $\mathfrak{G}, \mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_r = E$ und $\mathfrak{G}, \mathfrak{N}_1, \mathfrak{N}_2, \ldots, \mathfrak{N}_s = E$. Läßt man in den beiden Reihen $\mathfrak{G}$ weg, so erhält man Kompositionsreihen für $\mathfrak{M}_1$ und $\mathfrak{N}_1$, und für diese beiden Gruppen gilt der Satz nach Voraussetzung. Der Durchschnitt von $\mathfrak{M}_1$ und $\mathfrak{N}_1$ sei $\mathfrak{D}_1$, dann gilt wegen Satz 15 $\mathfrak{G}/\mathfrak{M}_1 = \mathfrak{N}_1/\mathfrak{D}_1$ und $\mathfrak{G}/\mathfrak{N}_1 = \mathfrak{M}_1/\mathfrak{D}_1$. Weil $\mathfrak{G}/\mathfrak{M}_1$ und $\mathfrak{G}/\mathfrak{N}_1$ einfache Gruppen sind, so ist $\mathfrak{D}_1$ größter Normalteiler sowohl von $\mathfrak{M}_1$ als von $\mathfrak{N}_1$, und man kann daher für diese beiden Untergruppen Kompositionsreihen bilden, die mit $\mathfrak{D}_1$ beginnen und von da an übereinstimmen: $\mathfrak{M}_1, \mathfrak{D}_1, \mathfrak{D}_2, \ldots, \mathfrak{D}_u = E$ und $\mathfrak{N}_1, \mathfrak{D}_1, \mathfrak{D}_2, \ldots, \mathfrak{D}_u = E$. Die beiden Kompositionsreihen von $\mathfrak{G}$: $\mathfrak{G}, \mathfrak{M}_1, \mathfrak{D}_1, \ldots, E$ und $\mathfrak{G}, \mathfrak{N}_1, \mathfrak{D}_1, \ldots, E$ besitzen wegen $\mathfrak{G}/\mathfrak{M}_1 = \mathfrak{N}_1/\mathfrak{D}_1$ und $\mathfrak{G}/\mathfrak{N}_1 = \mathfrak{M}_1/\mathfrak{D}_1$ dieselben Primfaktorgruppen, dasselbe gilt von den beiden Reihen: $\mathfrak{G}, \mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_r = E$ und $\mathfrak{G}, \mathfrak{M}_1, \mathfrak{D}_1, \ldots, E$, sowie von den beiden Reihen: $\mathfrak{G}, \mathfrak{N}_1, \mathfrak{N}_2, \ldots, \mathfrak{N}_r = E$ und $\mathfrak{G}, \mathfrak{N}_1, \mathfrak{D}_1, \ldots, E$, womit der Satz bewiesen ist.

Definition: Eine Gruppe, deren Primfaktorgruppen sämtlich einfache Gruppen von Primzahlordnung, also zyklische Gruppen sind, heißt eine ***auflösbare Gruppe.***

Die Oktaedergruppe ist auflösbar, denn sie besitzt einen Normalteiler vom Index 2, dieser einen solchen vom Index 3, nämlich eine Diedergruppe von der Ordnung 4. Diese letztere ist *Abel*sch und besitzt einen Normalteiler vom Index 2, dessen Ordnung 2 ist. Die Kompositionsreihe liefert daher 3 zyklische Primfaktorgruppen von der Ordnung 2 und einen von der Ordnung 3. Man beweist leicht, daß nur die eine Anordnung 2, 3, 2, 2 möglich ist.

Ist $\mathfrak{M}$ ein Normalteiler von $\mathfrak{G}$, so gibt es stets eine Kompositionsreihe von $\mathfrak{G}$, die $\mathfrak{M}$ enthält. Entweder ist $\mathfrak{M}$ ein größter Normalteiler von $\mathfrak{G}$, dann ist die Behauptung selbstverständlich. Im anderen Falle sei $\mathfrak{N}_1$ ein eigentlicher Normalteiler von $\mathfrak{G}$, der $\mathfrak{M}$ enthält, und zwar ein größter von dieser Beschaffenheit. Er ist größter Normalteiler von $\mathfrak{G}$. Wenn $\mathfrak{M}$ noch nicht größter Normalteiler von $\mathfrak{N}_1$ ist, so suche man wie vorher einen solchen, der $\mathfrak{M}$ enthält. Man erhält so eine Kompositionsreihe von $\mathfrak{G}$, die zunächst bis $\mathfrak{M}$ läuft, und von hier aus fährt man in der üblichen Weise fort. Ist diese Reihe $\mathfrak{G}, \mathfrak{N}_1, \mathfrak{N}_2, \ldots, \mathfrak{M}, \ldots$, so bildet $\mathfrak{G}/\mathfrak{M}, \mathfrak{N}_1/\mathfrak{M}, \mathfrak{N}_2/\mathfrak{M}, \mathfrak{M}/\mathfrak{M} = E$ eine

Kompositionsreihe von $\mathfrak{G}/\mathfrak{M}$ und man erhält alle Kompositionsreihen von $\mathfrak{G}$, die $\mathfrak{M}$ enthalten, bis zu dieser Untergruppe $\mathfrak{M}$, indem man alle Kompositionsreihen von $\mathfrak{G}/\mathfrak{M}$ bildet.

Satz 18: *Jede Untergruppe einer auflösbaren Gruppe ist auflösbar und ihre Primfaktorgruppen bestehen aus einem Teil derjenigen der ganzen Gruppe.*

Beweis: Sei $\mathfrak{H}$ eine Untergruppe der auflösbaren Gruppe $\mathfrak{G}$ und sei $\mathfrak{G}, \mathfrak{N}_1, \ldots, \mathfrak{N}_r = E$ eine Kompositionsreihe von $\mathfrak{G}$. Die letzte Gruppe dieser Reihe, die $\mathfrak{H}$ enthält, sei $\mathfrak{N}_{i-1}$, dann ist $\mathfrak{N}_i$ als Normalteiler von $\mathfrak{N}_{i-1}$ mit jedem Element von $\mathfrak{H}$ vertauschbar und $\{\mathfrak{N}_i \mathfrak{H}\} = \mathfrak{N}_{i-1}$, weil dies eine Gruppe sein muß, die $\mathfrak{N}_i$ als eigentlichen Normalteiler enthält, während sie selbst in $\mathfrak{N}_{i-1}$ enthalten ist; zwischen $\mathfrak{N}_i$ und $\mathfrak{N}_{i-1}$ gibt es aber keine Gruppe, da $\mathfrak{N}_{i-1}/\mathfrak{N}_i$ eine Gruppe von Primzahlordnung ist. Der Durchschnitt $\mathfrak{H}_1$ von $\mathfrak{H}$ und $\mathfrak{N}_i$ ist Normalteiler von $\mathfrak{H}$, und $\mathfrak{H}/\mathfrak{H}_1 = \mathfrak{N}_{i-1}/\mathfrak{N}_i$. Daher ist $\mathfrak{H}_1$ ein größter Normalteiler von $\mathfrak{H}$ und ist ganz in $\mathfrak{N}_i$ enthalten. Eine Fortsetzung dieses Verfahrens ergibt den Beweis unseres Satzes.

Satz 18a: *Es sei $\mathfrak{H}_i$ der Durchschnitt einer Untergruppe $\mathfrak{H}$ mit $\mathfrak{N}_i$, der i-ten Gruppe in der Kompositionsreihe $\mathfrak{G}, \mathfrak{N}_1, \mathfrak{N}_2, \ldots, \mathfrak{N}_r = E$, für $i = 1, 2, \ldots, r$, dann ist $\mathfrak{H}_{i-1}/\mathfrak{H}_i$ homomorph mit $\mathfrak{N}_{i-1}/\mathfrak{N}_i$ oder mit einer Untergruppe von $\mathfrak{N}_{i-1}/\mathfrak{N}_i$.*

Beweis: Man zeigt wie beim vorigen Beweis, daß jedes Element von $\mathfrak{H}_{i-1}$ mit $\mathfrak{N}_i$ vertauschbar ist und daß $\{\mathfrak{H}_{i-1}\mathfrak{N}_i\} = \mathfrak{L}_i$ in $\mathfrak{N}_{i-1}$ enthalten ist. Daraus folgt, daß $\mathfrak{L}_i/\mathfrak{N}_i$ eine Untergruppe von $\mathfrak{N}_{i-1}/\mathfrak{N}_i$ ist. Ferner ist $\mathfrak{L}_i/\mathfrak{N}_i = \mathfrak{H}_{i-1}/\mathfrak{H}_i$.

Der Satz 18 ist ein spezieller Fall von diesem Satz. $\mathfrak{H}, \mathfrak{H}_1, \ldots, \mathfrak{H}_r = E$ bildet nicht notwendig eine Kompositionsreihe, aber man kann weitere Gruppen dazwischen schalten unter Benutzung der Kompositionsreihen von $\mathfrak{H}_{i-1}/\mathfrak{H}_i$ und so zu einer Kompositionsreihe für $\mathfrak{H}$ gelangen. Natürlich brauchen die Gruppen $\mathfrak{H}_i$ nicht alle voneinander verschieden zu sein, $\mathfrak{H}_i$ kann ebensogut eigentlicher als uneigentlicher Normalteiler von $\mathfrak{H}_{i-1}$ sein.

§ 11. Hauptreihen.

Man kann ähnliche Reihen wie die Kompositionsreihen bilden, indem man nur Normalteiler von $\mathfrak{G}$ zuläßt.

Definition: Eine Reihe von Normalteilern von $\mathfrak{G}$: $\mathfrak{G}, \mathfrak{N}_1, \mathfrak{N}_2, \ldots, \mathfrak{N}_r = E$ heißt eine ***Hauptreihe*** von $\mathfrak{G}$, wenn jeder im vorhergehenden enthalten ist und wenn kein Normalteiler von $\mathfrak{G}$ dazwischengeschaltet werden kann, der in $\mathfrak{N}_{i-1}$ enthalten ist und $\mathfrak{N}_i$ enthält. Die Faktorgruppen $\mathfrak{G}/\mathfrak{N}_1, \mathfrak{N}_1/\mathfrak{N}_2, \ldots, \mathfrak{N}_{r-1}/E = \mathfrak{N}_{r-1}$ heißen die Primfaktorgruppen der Hauptreihe.

Satz 19: *Die Primfaktorgruppen zweier Hauptreihen derselben Gruppe stimmen in ihrer Gesamtheit untereinander überein.*

Beweis: Da $\mathfrak{N}_1, \mathfrak{N}_2, \ldots, \mathfrak{N}_{r-1}, E$ im allgemeinen nicht mehr Hauptreihe von $\mathfrak{N}_1$ sein wird, so muß die vollständige Induktion etwas anders angewandt werden als im vorigen Fall. Der letzte Normalteiler $\mathfrak{N}_{r-1}$ vor E ist ein solcher, der keinen eigentlichen Normalteiler von $\mathfrak{G}$ enthält außer sich selbst. Einen solchen Normalteiler heißt man einen ***kleinsten Normalteiler.*** Die Ordnung von $\mathfrak{G}$ sei ein Produkt von n Primfaktoren und die Gültigkeit des Satzes sei vorausgesetzt für alle Gruppen, deren Ordnung das Produkt von höchstens $n-1$ Primfaktoren ist. Die Reihe $\mathfrak{G}/\mathfrak{N}_{r-1}, \mathfrak{N}_1/\mathfrak{N}_{r-1}, \ldots, \mathfrak{N}_{r-2}/\mathfrak{N}_{r-1}, E$ bildet eine Hauptreihe für $\mathfrak{G}/\mathfrak{N}_{r-1}$. Wenn $\mathfrak{G}$ nur einen kleinsten Normalteiler besitzt, so folgt der Satz aus der Voraussetzung, da er für $\mathfrak{G}/\mathfrak{N}_{r-1}$ gilt. Ebenso folgt der Satz für zwei Hauptreihen, die denselben kleinsten Normalteiler enthalten. Nun seien $\mathfrak{M}$ und $\mathfrak{N}$ zwei kleinste Normalteiler und $\mathfrak{K} = \mathfrak{M}\mathfrak{N}$ (vgl. Satz 9) der durch sie erzeugte Normalteiler. Nach Satz 15 gilt $\mathfrak{K}/\mathfrak{N} = \mathfrak{M}$ und $\mathfrak{K}/\mathfrak{M} = \mathfrak{N}$. Zwischen $\mathfrak{K}$ und $\mathfrak{M}$ und ebenso zwischen $\mathfrak{K}$ und $\mathfrak{N}$ gibt es keinen Normalteiler von $\mathfrak{G}$, denn ein solcher müßte neben $\mathfrak{M}$ noch mindestens ein Element aus $\mathfrak{N}$, daher auch dessen ganze Klasse und den durch sie erzeugten Normalteiler enthalten. Dieser letztere ist aber identisch mit $\mathfrak{N}$, weil $\mathfrak{N}$ kleinster Normalteiler ist. Nun sei $\mathfrak{G}, \mathfrak{K}_1, \ldots, \mathfrak{K}, \mathfrak{M}, E$ eine Hauptreihe, die $\mathfrak{K}$ enthält. Dann ist auch $\mathfrak{G}, \mathfrak{K}_1, \ldots, \mathfrak{K}, \mathfrak{N}, E$ eine solche. Die Primfaktorgruppen dieser beiden Reihen stimmen überein, also auch diejenigen aller Hauptreihen, die $\mathfrak{M}$ oder $\mathfrak{N}$ enthalten, w. z. b. w.

Definition: Wenn jedes Element der Gruppe $\mathfrak{H}$ mit jedem Element der Gruppe $\mathfrak{K}$ vertauschbar ist und $\mathfrak{H}$ und $\mathfrak{K}$ außer E kein gemeinsames Element besitzen, so heißt $\mathfrak{H}\mathfrak{K}$ das ***direkte Produkt*** von $\mathfrak{H}$ und $\mathfrak{K}$.

Satz 20: *Ein kleinster Normalteiler ist entweder eine einfache Gruppe oder das direkte Produkt homomorpher einfacher Gruppen.*

Beweis: Der kleinste Normalteiler $\mathfrak{N}$ besitzt, wenn er nicht einfach ist, selber einen solchen, $\mathfrak{J}$. Mit $\mathfrak{J}$ ist auch $X^{-1}\mathfrak{J}X$ in $\mathfrak{N}$, wobei X ein beliebiges Element von $\mathfrak{G}$ bedeutet. $\mathfrak{J}$ und $X^{-1}\mathfrak{J}X$ sind homomorphe Gruppen und $X^{-1}\mathfrak{J}X$ ist kleinster Normalteiler von $X^{-1}\mathfrak{N}X = \mathfrak{N}$. Die verschiedenen Gruppen, die man erhält, wenn X alle Elemente von $\mathfrak{G}$ durchläuft, seien $\mathfrak{J}, \mathfrak{K}, \mathfrak{L} \ldots$. Die durch sie erzeugte Gruppe ist ein Normalteiler von $\mathfrak{G}$, der in $\mathfrak{N}$ enthalten ist und daher mit $\mathfrak{N}$ übereinstimmt. $\mathfrak{J}$ und $\mathfrak{K}$ besitzen außer E kein Element gemeinsam, da der Durchschnitt von $\mathfrak{J}$ und $\mathfrak{K}$ ein Normalteiler von $\mathfrak{N}$ sein muß. Die Gruppe $\{\mathfrak{J}\mathfrak{K}\}$ ist daher wegen Satz 9 das direkte Produkt von $\mathfrak{J}$ und $\mathfrak{K}$, und außerdem Normalteiler von $\mathfrak{N}$. Sie kann noch weitere Gruppen aus der Reihe $\mathfrak{J}, \mathfrak{K}, \mathfrak{L} \ldots$ enthalten. Wenn sie aber $\mathfrak{L}$ nicht enthält, so ist wieder jedes Element von $\mathfrak{L}$ mit jedem

Element von $\{\mathfrak{J}\mathfrak{K}\}$ vertauschbar und man hat das direkte Produkt $\mathfrak{J}\mathfrak{K}\mathfrak{L}$ zu bilden. Indem man so fortfährt, erhält man schließlich $\mathfrak{N}$ dargestellt als das direkte Produkt gewisser Gruppen aus der Reihe $\mathfrak{J}, \mathfrak{K}, \mathfrak{L}, \ldots$, womit der Satz bewiesen ist.

Satz 21: *Die Primfaktorgruppen einer Hauptreihe sind einfache Gruppen oder das direkte Produkt homomorpher einfacher Gruppen.*

Beweis: Ist $\mathfrak{G}, \mathfrak{N}_1, \mathfrak{N}_2, \ldots, E$ eine Hauptreihe von $\mathfrak{G}$, dann bildet, wie schon bemerkt, $\mathfrak{G}/\mathfrak{N}_i, \mathfrak{N}_1/\mathfrak{N}_i, \ldots, \mathfrak{N}_{i-1}/\mathfrak{N}_i, E$ eine Hauptreihe für $\mathfrak{G}/\mathfrak{N}_i$. Daher ist $\mathfrak{N}_{i-1}/\mathfrak{N}_i$ ein kleinster Normalteiler von $\mathfrak{G}/\mathfrak{N}_i$ und hat also die verlangte Beschaffenheit.

Aus einer Hauptreihe kann leicht eine Kompositionsreihe gebildet werden, indem man gewisse Gruppen einschaltet. Ist $\mathfrak{N}_{i-1}/\mathfrak{N}_i$ eine einfache Gruppe, so ist das offenbar nicht möglich, ist dagegen diese Faktorgruppe das direkte Produkt von n homomorphen Gruppen $\mathfrak{J}$, so kann man zwischen $\mathfrak{N}_{i-1}$ und $\mathfrak{N}_i$ genau $n-1$ Gruppen $\mathfrak{K}_1, \mathfrak{K}_2, \ldots, \mathfrak{K}_{n-1}$ hineinfügen und es wird: $\mathfrak{N}_{i-1}/\mathfrak{K}_1 = \mathfrak{K}_1/\mathfrak{K}_2 = \ldots = \mathfrak{K}_{n-1}/\mathfrak{N}_i = \mathfrak{J}$. Macht man das für alle Primfaktorgruppen der Hauptreihe, so erhält man eine Kompositionsreihe.

Für auflösbare Gruppen bestehen die Primfaktorgruppen der Hauptreihen aus lauter Abelschen Gruppen, deren Ordnung eine Primzahlpotenz und deren Typus $(p, p, ..)$ ist (vgl. § 14).

§ 12. Kommutatorgruppen.

Ist C der Kommutator von A und B, so ist $X^{-1}CX$ derjenige von $X^{-1}AX$ und $X^{-1}BX$. Daher bildet die Gesamtheit der Kommutatoren einer Gruppe eine Summe von Klassen, die im allgemeinen keine Untergruppe ist. Der von diesem Komplex erzeugte Normalteiler heißt die ***Kommutatorgruppe*** von $\mathfrak{G}$.

Satz 22: *Die Faktorgruppe der Kommutatorgruppe ist Abelsch und die Kommutatorgruppe ist in jedem Normalteiler enthalten, dessen Faktorgruppe Abelsch ist.*

Beweis: Sei $\mathfrak{C}$ die Kommutatorgruppe und C der Kommutator der beiden Elemente A und B von $\mathfrak{G}$. Dann wird $(B\mathfrak{C})(A\mathfrak{C}) = BA\mathfrak{C} = ABC\mathfrak{C} = AB\mathfrak{C} = (A\mathfrak{C})(B\mathfrak{C})$. Ist umgekehrt für den Normalteiler $\mathfrak{N}$ stets $A\mathfrak{N}B\mathfrak{N} = B\mathfrak{N}A\mathfrak{N}$, so wird $AB\mathfrak{N} = BA\mathfrak{N}$ und daher insbesondere $BA = ABN$, wobei N in $\mathfrak{N}$ liegt. Daher enthält $\mathfrak{N}$ jeden Kommutator und damit die ganze Kommutatorgruppe.

Die Kommutatorgruppe ist Durchschnitt aller Normalteiler mit Abelscher Faktorgruppe und insbesondere gilt der Satz, daß der Durchschnitt zweier Normalteiler mit *Abel*scher Faktorgruppe selbst eine *Abel*sche Faktorgruppe besitzt. Jede Untergruppe von $\mathfrak{G}$, die $\mathfrak{C}$ enthält, ist Normalteiler von $\mathfrak{G}$, weil $\mathfrak{G}/\mathfrak{C}$ *Abel*sch ist.

Die Kommutatorgruppe heißt auch erste abgeleitete Gruppe oder ***erste Ableitung*** von $\mathfrak{G}$. Sie besitzt selbst eine Kommutatorgruppe, die zweite Ableitung von $\mathfrak{G}$. Auch die zweite Ableitung ist Normalteiler von $\mathfrak{G}$, und der Beweis dieser Tatsache verläuft genau so wie derjenige für die erste Ableitung. Indem man die Kommutatorgruppe der zweiten Ableitung bildet, erhält man die dritte Ableitung, und eine Fortsetzung dieses Verfahrens liefert die Reihe der abgeleiteten Gruppen. Diese Reihe hat ein Ende, sobald eine Gruppe auftritt, die mit ihrer Kommutatorgruppe übereinstimmt, was z. B. stets eintritt, wenn sie einfach und nicht *Abel*sch ist.

Satz 23: *Eine Gruppe, für welche die Reihe der Ableitungen mit E schließt, ist auflösbar und alle auflösbaren Gruppen besitzen diese Eigenschaft.*

Beweis: Sei $\mathfrak{G}, \mathfrak{A}_1, \mathfrak{A}_2, \ldots, E$ die Reihe der Ableitungen von $\mathfrak{G}$; dann ist $\mathfrak{A}_{i-1}/\mathfrak{A}_i$ *Abel*sch und daher auflösbar; man kann also zwischen die einzelnen Gruppen dieser Reihe, wenn nötig, weitere einschalten, so daß man eine Kompositionsreihe von $\mathfrak{G}$ erhält, deren Primfaktorgruppen sämtlich Primzahlen als Ordnungen haben. Daher ist $\mathfrak{G}$ auflösbar. Ist umgekehrt $\mathfrak{G}$ auflösbar, so ist die Faktorgruppe jedes ihrer größten Normalteiler *Abel*sch, und der Kommutator von $\mathfrak{G}$ ist daher von $\mathfrak{G}$ verschieden. Dasselbe gilt von allen abgeleiteten Gruppen, denn jede Untergruppe einer auflösbaren Gruppe ist auflösbar.

Satz 24: *Ist $\mathfrak{G}'$ isomorph mit $\mathfrak{G}$, so ist auch die i-te Ableitung von $\mathfrak{G}'$ isomorph mit der i-ten Ableitung von $\mathfrak{G}$. $\mathfrak{G}'$ besitzt höchstens soviel verschiedene Ableitungen wie $\mathfrak{G}$.*

Beweis: Jedem Kommutator $B^{-1}A^{-1}BA$ von $\mathfrak{G}$ entspricht beim Isomorphismus der Kommutator $B'^{-1}A'^{-1}B'A'$, und jeder Kommutator von $\mathfrak{G}'$ entspricht einem solchen von $\mathfrak{G}$. Daher wird durch den Isomorphismus die erste Ableitung $\mathfrak{A}_1$ von $\mathfrak{G}$ der ersten Ableitung $\mathfrak{A}_1'$ von $\mathfrak{G}'$ zugeordnet und $\mathfrak{A}_1'$ ist isomorph mit $\mathfrak{A}_1$. Da die i-te Ableitung von $\mathfrak{G}$ die erste Ableitung von $\mathfrak{A}_{i-1}$ ist, so ist auch $\mathfrak{A}_i'$ isomorph mit $\mathfrak{A}_i$.

Satz 24a: *Ist $\mathfrak{N}$ ein Normalteiler von $\mathfrak{G}$ und ist die i-te Ableitung von $\mathfrak{G}/\mathfrak{N}$, aber keine frühere, gleich E, so enthält $\mathfrak{N}$ die i-te Ableitung $\mathfrak{A}_i$ von $\mathfrak{G}$, aber nicht die $(i-1)$-te $\mathfrak{A}_{i-1}$.*

Beweis: Es sei $\mathfrak{A}_k$ in $\mathfrak{N}$ enthalten. Dann ist $\mathfrak{G}/\mathfrak{N}$ isomorph mit $\mathfrak{G}/\mathfrak{A}_k$, weil $\mathfrak{N}/\mathfrak{A}_k$ ein Normalteiler von $\mathfrak{G}/\mathfrak{A}_k$ ist. Nach Satz 24 ist daher $k \geqq i$. Damit ist der zweite Teil des Satzes bewiesen. Nun sei $\mathfrak{G}/\mathfrak{N}, \mathfrak{A}_1/\mathfrak{N}, \ldots, \mathfrak{A}_{i-1}/\mathfrak{N}, E$ die Reihe der Ableitungen von $\mathfrak{G}/\mathfrak{N}$. Wir betrachten die Untergruppen $\mathfrak{G}, \mathfrak{N}_1, \mathfrak{N}_2, \ldots, \mathfrak{N}$. Ihre Faktorgruppen $\mathfrak{G}/\mathfrak{N}_1, \mathfrak{N}_1/\mathfrak{N}_2, \ldots$ sind sämtlich *Abel*sch, daher enthält $\mathfrak{N}_1$ jedenfalls $\mathfrak{A}_1$. $\mathfrak{A}_2$ ist als Kommutatorgruppe von $\mathfrak{A}_1$ a fortiori in der Kommutatorgruppe von $\mathfrak{N}_1$ enthalten, also auch in $\mathfrak{N}_2$, weil $\mathfrak{N}_2$ diese

letztere enthält. Da $\mathfrak{A}_2$ in $\mathfrak{N}_2$ enthalten ist, folgt genau so, daß $\mathfrak{A}_3$ in $\mathfrak{N}_3, \ldots,$ $\mathfrak{A}_i$ in $\mathfrak{N}_i = \mathfrak{N}$ enthalten ist, womit die Behauptung bewiesen ist.

Satz 25: *Sind $\mathfrak{N}_1$ und $\mathfrak{N}_2$ zwei Normalteiler von $\mathfrak{G}$ ohne gemeinsame Elemente außer E, und ist die i-te Ableitung von $\mathfrak{G}/\mathfrak{N}_1$ und $\mathfrak{G}/\mathfrak{N}_2$ das Einheitselement der betreffenden Gruppen, so ist auch die i-te Ableitung von $\mathfrak{G}$ gleich E.*

Beweis: Nach dem vorigen Satz ist die i-te Ableitung $\mathfrak{A}_i$ von $\mathfrak{G}$ sowohl in $\mathfrak{N}_1$ als in $\mathfrak{N}_2$ enthalten und daher gleich E.

§ 13. Ein Theorem von *Frobenius*.

Durch die bisher gewonnenen Ergebnisse sind wir in den Stand gesetzt, ein allgemeines Theorem zu beweisen für beliebige Gruppen. Vorher leiten wir folgenden Satz ab:

Satz 26: *Ein Element A von der Ordnung $n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$ läßt sich auf eine und nur eine Weise als Produkt darstellen von r untereinander vertauschbaren Elementen, deren Ordnungen die Primzahlpotenzen $p_1^{a_1}, p_2^{a_2}, \ldots, p_r^{a_r}$ sind.*

Beweis: Es sei $n = lm$, wobei l prim ist zu m, und man setze $A^l = B$ und $A^m = C$. B und C sind vertauschbar und von den Ordnungen m und l. Bestimmt man nun x und y aus der Kongruenz $lx + my \equiv 1 \pmod{n}$, so wird $A = B^x C^y$. Nun sei eine zweite Zerlegung gegeben $A = B_1 C_1$, für welche wiederum B_1 und C_1 vertauschbar sind und von den Ordnungen m und l. Es wird $A^l = B_1^l$, weil $C_1^l = E$, daher ist $B_1^l = B$ und $B_1^{lx} = B_1 = B^x$. Ebenso wird $C_1 = C^y$, womit die Eindeutigkeit der Zerlegung bewiesen ist. Setzt man nun $l = p_1^{a_1}$, $m = p_2^{a_2} \ldots p_r^{a_r}$, so erkennt man, daß der Faktor von der Ordnung $p_1^{a_1}$ durch A vollständig bestimmt ist. Dasselbe beweist man für die übrigen Primzahlpotenzen, womit der Satz vollständig bewiesen ist.

Wir beweisen jetzt folgenden Fundamentalsatz von *Frobenius*[1]).

Satz 27: *Ist g die Ordnung der Gruppe $\mathfrak{G}$ und ist n ein Teiler von g, so ist die Anzahl der Elemente aus $\mathfrak{G}$, die der Gleichung $X^n = E$ genügen, durch n teilbar.*

Beweis: *E. Netto*[2]) hat den ursprünglichen Beweisgang wesentlich vereinfacht und wir geben hier dessen Fassung wieder.

Der Satz gilt offenbar für Gruppen, deren Ordnung eine Primzahl ist und wir können daher die Methode der vollständigen Induktion anwenden. Wir setzen ihn also als bewiesen voraus für alle Gruppen

---

[1]) *G. Frobenius:* Über einen Fundamentalsatz der Gruppentheorie. Berl. Sitzungsber. **1903**, S. 987 und **1907**, S. 428.

[2]) *Netto*: Gruppen- und Substitutionentheorie, Leipzig 1908, S. 105.

deren Ordnung ein Teiler von g ist. In der Gruppe $\mathfrak{G}$ selbst gilt der Satz für $n = g$, denn die g Elemente von $\mathfrak{G}$ genügen der Gleichung $X^g = E$. Indem wir noch einmal vollständige Induktion anwenden, nehmen wir an, daß der Satz gilt für $n = mp$, wobei p eine Primzahl ist und beweisen, daß der Satz auch für m gilt.

Die Anzahl der Elemente, deren Ordnung ein Teiler von n ist, wollen wir mit n_n bezeichnen. Dann besagt also unsere Voraussetzung, daß n_{mp} durch mp teilbar ist. Diejenigen Elemente, deren Ordnung ein Teiler von m ist, sind enthalten unter den n_{mp} Elementen, deren Ordnung ein Teiler von mp ist. Daher wird

$$n_{mp} = n_m + \bar{n}_m,$$

wobei $\bar{n}_m$ die Anzahl derjenigen Elemente bezeichnet, deren Ordnung ein Teiler von mp, aber nicht von m ist. Wenn wir zeigen können, daß $\bar{n}_m$ durch m teilbar ist, so folgt dasselbe auch für n_m.

Wir setzen nun $m = p^{a-1}s$, wobei s prim ist zu p. Der Komplex $\mathfrak{A}$ der durch $\bar{n}_m$ abgezählten Elemente besteht aus lauter Elementen, deren Ordnung durch p^a, aber nicht durch p^{a+1} teilbar ist. Jedes dieser Elemente läßt sich auf eine und nur eine Weise als Produkt darstellen PQ, wobei die Ordnung von P gleich p^a, diejenige von Q zu p prim ist und P und Q vertauschbar sind. Zu jedem Element von $\mathfrak{A}$ gehört also eindeutig ein „Konstituent" P von der Ordnung p^a. Daß $\bar{n}_m$ durch p^{a-1} teilbar ist, läßt sich folgendermaßen einsehen. Ist $p^a r$ die Ordnung des Elementes A aus $\mathfrak{A}$, so gibt es unter den Potenzen von A (§ 15) $\varphi(p^a r) = p^{a-1}(p-1)\varphi(r)$ Elemente, deren Ordnung $p^a r$ ist, und diese Zahl ist durch p^{a-1} teilbar. Die Elemente von $\mathfrak{A}$ lassen sich so in Systeme ohne gemeinsame Elemente einteilen, und die Anzahl der Elemente in jedem System ist durch p^{a-1} teilbar. Das Gleiche gilt also auch für $\bar{n}_m$.

Nun muß gezeigt werden, daß diese Zahl auch durch s teilbar ist, und zu dem Zweck betrachten wir diejenigen Elemente aus $\mathfrak{A}$, deren Konstituent dasselbe Element P ist. Die Gesamtheit der Elemente aus $\mathfrak{G}$, die mit P vertauschbar sind, bilden eine Untergruppe $\mathfrak{H}$, deren Ordnung mit $p^a t$ bezeichnet sei. Der Index, der durch P erzeugten zyklischen Gruppe $\mathfrak{P}$ unter $\mathfrak{H}$ ist alsdann t. Wir betrachten nun die Faktorgruppe $\mathfrak{H}/\mathfrak{P}$. Da ihre Ordnung ein Teiler von g ist, so gilt für sie der zu beweisende Satz. Ist also s' der größte gemeinsame Teiler von s und t, so ist die Anzahl der Elemente der Faktorgruppe $\mathfrak{H}/\mathfrak{P}$, deren Ordnung ein Teiler von s' ist, durch s' teilbar. Die Anzahl der Elemente, deren Konstituent P ist, ist also durch s' teilbar, denn jede Nebengruppe von $\mathfrak{P}$, deren Ordnung Teiler von s' ist, liefert genau ein solches Element aus $\mathfrak{A}$. Wir betrachten nun die Klasse von P. Sie enthält genau $g/p^a t$ Elemente. Jedes dieser

Elemente ist Konstituent von gleich vielen Elementen aus $\mathfrak{A}$ und die Anzahl der durch sie gelieferten Elemente von $\mathfrak{A}$ ist daher teilbar durch $g\,s'/p^a\,t$.

Daß diese Zahl durch s teilbar ist, folgt nun ohne weiteres: s' ist größter gemeinschaftlicher Teiler von s und t, daher ist $g\,s'$ durch $s\,t$ teilbar, denn s und t sind Teiler von g; und da s und t zu p prim sind, so ist die Behauptung bewiesen. Hieraus folgt nun, daß sich die Elemente von $\mathfrak{A}$ in Systeme einteilen lassen, deren jedes eine durch s teilbare Anzahl von Elementen besitzt und von denen je zwei keine gemeinsamen Elemente enthalten. Die Elemente desselben Systems sind dadurch verbunden, daß ihre Konstituenten zur selben Klasse gehören. Hieraus folgt, daß $\bar{n}_m$ auch durch s teilbar ist, womit der Satz bewiesen ist.

3. Kapitel.

Abelsche Gruppen.

§ 14. Basis einer *Abel*schen Gruppe.

Bereits in Satz 26 wurde gezeigt, daß jedes Element A sich als Produkt vertauschbarer Elemente darstellen läßt, deren Ordnung Primzahlpotenzen sind, und zwar sind diese Elemente Potenzen von A. Das Problem erfordert die Lösung der folgenden zahlentheoretischen Aufgabe: Sei $n = p_1^{a_1} \dots p_r^{a_r}$ die Ordnung von A und $n_i = \frac{n}{p_i^{a_i}}$. Man löse die Kongruenz:

$$n_1 x_1 + n_2 x_2 + \dots + n_r x_r \equiv 1 \pmod{n}.$$

Dann wird, wenn man $A^{n_i} = A_i$ setzt, A_i von der Ordnung $p_i^{a_i}$ und $A = A_1^{x_1} A_2^{x_2} \dots A_r^{x_r}$, womit die Aufgabe gelöst ist.

Satz 28: *Eine Abelsche Gruppe $\mathfrak{G}$ von der Ordnung $g = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ ist das direkte Produkt von Abelschen Gruppen der Ordnungen $p_1^{a_1}, p_2^{a_2}, \dots, p_r^{a_r}$.*

Beweis: Diejenigen Elemente, deren Ordnung eine Potenz von p_i ist, bilden eine Untergruppe $\mathfrak{P}_i$. Die Ordnung von $\mathfrak{P}_i$ ist wieder eine Potenz von p_i Schlußbemerkung von § 9 oder Satz 27). Das direkte Produkt aller Untergruppen $\mathfrak{P}_i$ enthält wegen Satz 26 alle Elemente von $\mathfrak{G}$, aber auch jedes nur einmal, denn aus $P_1 P_2 \dots P_r = P_1' P_2' \dots P_r'$ folgt $P_1 P_1'^{-1} P_2 P_2'^{-1} \dots P_r P_r'^{-1} = E$, also $P_i = P_i'$. Die Ordnung von $\mathfrak{P}_i$ ist daher genau $p_i^{r_i}$.

Nun muß noch die Beschaffenheit von Gruppen untersucht werden, deren Ordnung die Potenz einer Primzahl ist.

Satz 29: *Jede Abelsche Gruppe $\mathfrak{G}$ ist das direkte Produkt zyklischer Gruppen.*

Beweis: Zunächst sei die Ordnung eine Potenz der Primzahl p. A_1 sei ein Element von möglichst hoher Ordnung $n = p^a$. Alsdann sei B ein solches Element, daß seine niedrigste Potenz, die gleich einer Potenz von A_1 ist, eine möglichst große Zahl ist. Ist p^k diese Zahl (vgl. § 9), so setze man $B^{p^k} = A_1^{q p^l}$ (q prim zu p). Alsdann ist $k \leqq l$, weil die Ordnung von $B \leqq$ der Ordnung von A_1 sein muß. Daher gibt es eine Potenz A' von A_1, welche der Gleichung genügt: $B^{p^k} = A'^{p^k}$. Nun wird $B A'^{-1} = A_2$ ein Element, dessen Ordnung p^k ist und von dem erst die p^k-te Potenz, d. h. E, in $\{A_1\}$ liegt. Das direkte Produkt von $\{A_1\}$ und $\{A_2\}$ ist in $\mathfrak{G}$ enthalten. Ferner sei C ein weiteres Element, für welches die niedrigste Potenz, die in $\{A_1\}\{A_2\}$ liegt, ein Maximum ist p^m. Man beweist genau wie bisher, daß es ein Element von der Ordnung p^m gibt, dessen sämtliche Potenzen, außer E, außerhalb von $\{A_1\}\{A_2\}$ liegen. Indem man so fortfährt, bis alle Elemente erschöpft sind, erhält man das im Satz ausgesprochene Resultat für Gruppen, deren Ordnung eine Primzahlpotenz ist. Da eine beliebige *Abel*sche Gruppe aber das direkte Produkt von solchen ist, so folgt auch der allgemeine Satz unmittelbar daraus.

Definition: Die Elemente $A_1, A_2, \ldots, A_r$ heißen eine ***Basis** einer Abelschen Gruppe,* wenn ihre Ordnungen $n_1, n_2, \ldots, n_r$ sämtlich Primzahlpotenzen sind und wenn sich jedes Element der Gruppe auf eine und nur eine Weise in der Gestalt darstellen läßt:

$$A = A_1^{x_1} A_2^{x_2} \ldots A_r^{x_r} \qquad \begin{matrix} x_1 = 0, 1, \ldots, n_1 - 1 \\ \cdot \quad \cdots\cdots\cdots\cdots \\ x_r = 0, 1, \ldots, n_r - 1 \end{matrix}$$

Fundamentalsatz 30: *Jede Abelsche Gruppe besitzt eine Basis.*

Die Zahlen $n_1, n_2, \ldots, n_r$, also die Ordnungen der Basiselemente, heißen die ***Invarianten** der Abelschen Gruppe.*

Satz 31: *Zwei verschiedene Abelsche Gruppen besitzen verschiedene Invarianten. Zu jedem System von Primzahlpotenzen $n_1, n_2, \ldots, n_r$ gibt es genau eine Abelsche Gruppe, welche sie zu Invarianten hat.*

Beweis: Der Satz braucht nur für Gruppen bewiesen zu werden, deren Ordnung eine Primzahlpotenz ist, denn die Invarianten einer beliebigen Gruppe setzen sich aus solchen für diese speziellen Gruppen zusammen. Es seien $A_1, A_2, \ldots, A_r$ und $B_1, B_2, \ldots, B_s$ zwei Basen derselben Gruppe und $m_1, m_2, \ldots, m_r$ resp. $n_1, n_2, \ldots, n_s$, die zu-

gehörigen Ordnungen. Ferner seien die Basiselemente so numeriert, daß $n_1 \geqq n_2 \geqq \ldots \geqq n_s$ und $m_1 \geqq m_2 \geqq \ldots \geqq m_r$. Alle Zahlen n und m sind Potenzen von p. Nun sei n_i die erste unter den Zahlen, die von ihrer entsprechenden Zahl m_i verschieden ist, so daß etwa gilt: $n_1 = m_1, \ldots, n_{i-1} = m_{i-1}$, $n_i > m_i$.

Die m_i-ten Potenzen aller Elemente von $\mathfrak{G}$ bilden eine Gruppe, deren Basiselemente die m_i-ten Potenzen der Basiselemente von $\mathfrak{G}$ sind. Diese Untergruppe ist unabhängig von der speziellen Wahl der Basis von $\mathfrak{G}$. Einerseits bilden so die Elemente $B_1^{m_i}, B_2^{m_i}, \ldots, B_s^{m_i}$ eine Basis und hieraus berechnet sich die Ordnung der Untergruppe als $\geqq p^{(n_1-m_i)+\ldots+(n_i-m_i)}$.

Andererseits bilden auch die Elemente $A_1^{m_i}, A_2^{m_i}, \ldots, A_r^{m_i}$ eine solche und man findet als Ordnung: $p^{m_1-m_i+\cdots+(m_i-m_i)}$, was einen Widerspruch ergibt.

Daß es für jedes System von Primzahlpotenzen eine *Abel*sche Gruppe gibt, die sie als Invarianten besitzt, wird dadurch bewiesen, daß man die Gruppe darstellt mit Hilfe des arithmetischen Kongruenzbegriffs. Seien $n_1, n_2, n_3, \ldots, n_s$ diese Invarianten, so bilde man die sämtlichen Zahlensysteme $(x_1, x_2, \ldots, x_s)$, wobei x_i nach dem Modul n_i zu reduzieren ist. Es gibt $n_1 n_2 \ldots n_s$ solche. Als Gruppengesetz nehme man die Vektoraddition $(x_1, x_2, \ldots, x_3) + (y_1, y_2, \ldots, y_s) = (x_1 + y_1, x_2 + y_2, \ldots, x_s + y_s)$. Als Basiselemente benutze man die s folgenden: $(1, 0, \ldots, 0)$, $(0, 1, 0, \ldots, 0)$, $\ldots$, $(0, 0, \ldots, 0, 1)$. Der Satz folgt dann unmittelbar.

Hierdurch ist das Problem vollständig gelöst, bei gegebener Ordnung alle möglichen *Abel*schen Gruppen anzugeben, ein Problem, von dessen Lösung man für nicht *Abel*sche Gruppen noch weit entfernt ist. Das wesentlich Neue der Gruppentheorie gegenüber der älteren Algebra besteht eben darin, daß das Kommutativgesetz nicht gilt.

Sind $n_1, n_2, \ldots, n_s$ die Invarianten von $\mathfrak{G}$, so bezeichnet man $\mathfrak{G}$ mit $(n_1, n_2, \ldots, n_s)$ und wenn die Gruppe eine Potenz von p als Ordnung besitzt, so genügt es, den Exponenten von p für die einzelnen Invarianten hinzuschreiben, wo keine Verwechslung möglich ist. So ist $(1, 1, 1)$ eine *Abel*sche Gruppe, die das direkte Produkt von drei zyklischen Gruppen der Ordnung p ist. Man nennt in beiden Fällen $\mathfrak{G}$ eine Gruppe vom ***Typus*** $(n_1, n_2, \ldots, n_s)$.

Historische Notiz: Zyklische und *Abel*sche Gruppen treten bei den zahlentheoretischen Untersuchungen von *Euler* häufig auf. Den Satz 30 hat *Gauß* 1801 sicher gekannt (Werke **2**, S. 266) und auf die Kompositionstheorie der quadratischen Formen angewendet. Vgl. auch den Anfang von § 61. Den ersten vollständigen Beweis gaben *Frobenius* und *Stickelberger* (Über Gruppen vertauschbarer Elemente, Crelles Journ. **86**, S. 217).

§ 15. Untergruppen und Faktorgruppen einer *Abel*schen Gruppe.

Satz 32: *Die Invarianten einer Untergruppe sind bei geeigneter Zuordnung Teiler der Invarianten der ganzen Gruppe.*

Beweis: Wegen Satz 28 können wir uns auf Gruppen $\mathfrak{G}$ beschränken, deren Ordnung eine Potenz der Primzahl p ist. In absteigender Anordnung seien die Invarianten von $\mathfrak{G}$ gegeben durch $(p^{a_1}, p^{a_2}, \ldots, p^{a_s})$, diejenigen von $\mathfrak{H}$ durch $(p^{b_1}, p^{b_2}, \ldots, p^{b_r})$. Die Elemente von der Ordnung p in $\mathfrak{G}$ bilden eine Untergruppe, deren Basiselemente von den p^{a_i-1}-ten Potenzen derjenigen von $\mathfrak{G}$ dargestellt werden. Ihre Ordnung ist daher p^s. Für die entsprechende Untergruppe von $\mathfrak{H}$ ist die Ordnung p^r. Daraus folgt $r \leqq s$. Nun sei b_i die erste Zahl in der Reihe der b, welche größer ist als die entsprechende Zahl a_i. Bildet man die p^{a_i}-ten Potenzen aller Elemente von $\mathfrak{G}$ und von $\mathfrak{H}$, so findet man im letzteren Falle mindestens i Basiselemente, im ersteren weniger als i. Das widerspricht der Tatsache, daß $\mathfrak{H}$ Untergruppe von $\mathfrak{G}$ ist.

Aus diesem Satz folgt im besonderen, daß die Untergruppen einer zyklischen Gruppe zyklisch sind. Ist g ihre Ordnung und A ein erzeugendes Element, ist ferner $g = hk$, so erzeugt A^k eine zyklische Untergruppe von der Ordnung h, und zwar die *einzige* von dieser Ordnung. Denn aus $(A^x)^h = E$ folgt, daß x durch k teilbar ist. Die Anzahl der Elemente von der Ordnung h ist gleich der Anzahl der zu h primen Zahlen in der Reihe $1, 2, \ldots, h$, also gleich der zahlentheoretischen Funktion $\varphi(h)$.

Satz 33: *Ist $\mathfrak{G}$ eine Abelsche Gruppe vom Typus $(n_1, n_2, \ldots, n_s)$ und ist irgendein anderer Typus gegeben $(m_1, m_2, \ldots, m_r)$ dergestalt, daß $r \leqq s$ und daß n_i/m_i ganze Zahlen sind, so besitzt $\mathfrak{G}$ mindestens eine Untergruppe vom Typus $(m_1, m_2, \ldots, m_r)$.*

Beweis: Sind $A_1, A_2, \ldots, A_s$ die Basiselemente von $\mathfrak{G}$, so sind $A_1^{\frac{n_1}{m_1}}, A_2^{\frac{n_2}{m_2}}, \ldots, A_s^{\frac{n_s}{m_s}}$ solche einer Untergruppe vom gewünschten Typus. Hierbei ist $m_{r+1} = \ldots = m_s = 1$ zu setzen.

Im allgemeinen gibt es mehrere Untergruppen von gegebenem Typus. Eine Gruppe von der Ordnung p^r und vom Typus $(1, 1, \ldots, 1)$ besitzt $\frac{p^r-1}{p-1}$ Untergruppen von der Ordnung p, denn jedes Element außer E gehört genau zu einer solchen und erzeugt sie. Ferner gehören außer E noch je $p-1$ Elemente von der Ordnung p zur Bildung einer Untergruppe. Da es im ganzen $p^r - 1$ Elemente von der

Ordnung p gibt, so verteilen sie sich in $\frac{p^r-1}{p-1}$ Systeme von je $p-1$ Elementen, die zusammen mit E jeweils eine Untergruppe bilden.

Die nähere Betrachtung der Gruppen vom Typus $(1, 1, \ldots, 1)$ ist deshalb von Wichtigkeit, weil die Primfaktorgruppen der Hauptreihen bei auflösbaren Gruppen zu ihnen gehören. Ist p^r die Ordnung einer solchen Gruppe, so besitzt eine Untergruppe von der Ordnung p^s den Typus $(1, 1, \ldots, s\text{-mal})$ und es soll nun die Anzahl N_{rs} der Untergruppen von dieser Ordnung p^s berechnet werden.

Es ist bereits bekannt, daß $N_{r1} = \frac{p^r-1}{p-1}$ ist. Nun soll $N_{r,s+1}$ aus $N_{r,s}$ berechnet werden. Ist $\mathfrak{H}$ eine Untergruppe von der Ordnung p^s, so erhält man alle Untergruppen von der Ordnung p^{s+1}, die $\mathfrak{H}$ enthalten, indem man die Untergruppen von der Ordnung p in $\mathfrak{G}/\mathfrak{H}$ benutzt. Die Anzahl dieser letzteren ist aber $\frac{p^{r-s}-1}{p-1} = N_{r-s,1}$. Benutzt man der Reihe nach die N_{rs} Untergruppen von der Ordnung p^s, so erhält man $N_{rs}N_{r-s,1}$ Untergruppen von der Ordnung p^{s+1}. Eine solche enthält aber $N_{s+1,s}$ Untergruppen vom Index p, daher sind schließlich je $N_{s+1,s}$ miteinander identisch, und es wird:

$$N_{r,s+1} = \frac{N_{rs} \cdot N_{r-s,1}}{N_{s+1,s}}.$$

Setzt man in dieser Formel $r-1$ an Stelle von r und dividiert sie durch die so entstehende, so erhält man:

$$\frac{N_{r,s+1}}{N_{r-1,s+1}} = \frac{N_{r-s,1}}{N_{r-s-1,1}} \cdot \frac{N_{r,s}}{N_{r-1,s}}.$$

Wenn man alsdann s die Zahlen 1 bis $t-1$ durchlaufen läßt und die so entstehenden Gleichungen miteinander multipliziert, so ergibt sich die einfache Gleichung:

$$\frac{N_{r,t}}{N_{r-1,t}} = \frac{N_{r,1}}{N_{r-t,1}} = \frac{p^r-1}{p^{r-t}-1},$$

und hieraus findet man schließlich, indem man r der Reihe nach durch $t+1, t+2, \ldots, r$ ersetzt und multipliziert:

$$N_{rt} = \frac{(p^r-1)(p^{r-1}-1)\ldots(p^{r-t+1}-1)}{(p-1)(p^2-1)\ldots(p^t-1)} \quad \text{wegen} \quad N_{tt} = 1.$$

Es wird insbesondere

$$N_{r,t} = N_{r,r-t}.$$

Satz 34: *Eine Abelsche Gruppe von der Ordnung p^r und vom Typus $(1, 1, \ldots, 1)$ besitzt $\frac{(p^r-1)(p^{r-1}-1)\ldots(p^{r-t+1}-1)}{(p-1)(p^2-1)\ldots(p^t-1)}$ Untergruppen von der Ordnung p^t.*

§ 16. Die *Galois*schen Imaginären und Reste nach Primzahlpotenzen.

Ein besonders instruktives und wichtiges Beispiel für *Abel*sche Gruppen wird durch die in der Zahlentheorie auftretenden Restklassen nach Primzahlen resp. Primidealen geliefert. Sie lassen sich überaus einfach und unabhängig von zahlentheoretischen Sätzen folgendermaßen definieren:

Definition: Ein System von Elementen bildet einen ***endlichen Körper*** oder ein System von ***Galoisschen Imaginären,*** wenn es folgenden Bedingungen genügt:

1. Die Elemente bilden eine kommutative Gruppe nach einem ersten Gesetz $A+B$, genannt *Addition*. Das Einheitselement wird mit 0 bezeichnet.

2. Die Elemente mit Ausnahme von 0 bilden unter sich eine kommutative Gruppe nach einem zweiten Gesetz AB genannt *Multiplikation*. Das Einheitselement wird mit 1 bezeichnet.

3. Für beliebige vier Elemente gilt das distributive Gesetz $(A+B)(C+D) = AC + AD + BC + BD$.

Es soll die Konstitution aller so entstehenden Körper hergeleitet werden. Das Produkt von 0 mit irgendeinem Element ist 0, wie sich aus dem Distributivgesetz ergibt: aus $A+0=A$ folgt $(A+0)B = AB + 0B = AB$, also $0B = 0$ und in derselben Weise $B0 = 0$.

Satz 35: *Die Anzahl der Elemente ist eine Primzahlpotenz und der Typus der ersten Gruppe ist* $(1, 1, \ldots, 1)$.

Beweis: Sei m die Ordnung der Multiplikationseinheit 1 nach dem Additionsgesetz. Man bezeichne ferner $1+1$ mit 2 usw. und $1+1+\ldots+1$ ($i$mal) mit i. Die so entstehenden Elemente verhalten sich wie die Restklassen mod m nach dem Gesetz der Addition. Wegen des Distributivgesetzes gilt für das zweite Gruppengesetz dasselbe wie für die gewöhnliche Multiplikation, es wird ik gleich derjenigen der Zahlen $0, 1, \ldots, m-1$, welche Rest mod m des gewöhnlichen Produktes der beiden Zahlen i und k ist. Angenommen, m sei keine Primzahl, sondern etwa $= rs$. Dann bilde man den Komplex r, $2r, \ldots (s-1)r$. Das Produkt zweier dieser Zahlen gehört wieder zu diesem Komplex, denn 0 kommt wegen 2. nicht darunter vor, er bildet daher eine Untergruppe. Dies ist aber für $r > 1$ nicht der Fall, da das Einheitselement 1 darin fehlt. Daher wird m eine Primzahl p. Nun sei a ein Element, das von $0, 1, \ldots, p-1$ verschieden ist. Es wird $a + a = 2a, \ldots, a + a + \ldots + a$ (p-mal) $= pa = 0$. Jedes Element außer 0 besitzt die Ordnung p nach dem ersten Gesetz, und der Typus dieser Gruppe ist $(1, 1, \ldots, 1)$.

Satz 36: *Die zweite Gruppe ist eine zyklische Gruppe von der Ordnung* $p^r - 1$.

Beweis: Ein Produkt von Elementen nach der zweiten Operation ist dann und nur dann $= 0$, wenn einer der Faktoren verschwindet. Man kann Gleichungen von der Gestalt $ax^n + bx^{n-1} + \ldots + f = 0$ bilden, wobei $a, b, \ldots, f$ gegebene Elemente des Körpers und x ein zu bestimmendes Element, eine Wurzel der Gleichung, bedeutet. Die bekannten Überlegungen der Algebra können hier wörtlich wiederholt werden. Es gilt identisch $(x-a)(x^{s-1} + x^{s-2}a + \ldots + a^{s-1}) = x^s - a^s$. Ist a eine Wurzel von $f(x) = 0$, so wird $f(x) - f(a) = f(x)$, und es läßt sich der Faktor $x - a$ aus $f(x)$ herausheben: $f(x) = (x-a) f_1(x)$. Man beweist sofort, daß eine weitere Wurzel von $f(x) = 0$ auch der Gleichung $f_1(x) = 0$ genügen muß, und schließlich folgt insbesondere, daß eine Gleichung vom Grade n höchstens n Wurzeln haben kann. Nun sei g die höchste vorkommende Ordnung eines Elementes in der zweiten Gruppe. Dann genügt jedes der $p^r - 1 = s$ Elemente nach Satz 30 der Gleichung $x^g = 1$. Also wird g nicht kleiner als s sein, und es muß (Satz 30) Elemente von der Ordnung s geben, d. h. die Gruppe ist zyklisch.

Beispiele: Die Restklassen nach einer Primzahl als Modul. Als erste Operation nimmt man die gewöhnliche Addition und ersetzt die Summe zweier Zahlen durch ihren Rest mod p. Die inverse Zahl wird die durch $-a$ repräsentierte Klasse und 0 ist das Einheitselement. Als zweites Gruppengesetz wird die gewöhnliche Multiplikation genommen. Daß die Zahlen $1, 2, \ldots, p-1$ eine Gruppe bilden, folgt aus der Geltung von III*, denn aus $ab \equiv ac$ folgt, da a zu p prim ist, $b \equiv c$. Es gibt daher eine Zahl, die mit ihren $p-1$ ersten Potenzen alle Restklassen außer 0 liefert.

Ebenso bilden die Restklassen in einem algebraischen Zahlkörper nach einem Primideal als Modul einen Körper. Ist die Norm des Primideals eine Primzahl*potenz*, so treten die allgemeinen *Galois*schen Imaginären auf.

Von besonderem Interesse sind die *Automorphismen eines Körpers*, d. h. Permutationen der Elemente, welche für beide Gruppen 1. und 2. Automorphismen liefern.

Satz 37: *Ein Körper mit* p^r *Elementen besitzt genau* r *Automorphismen. Man erhält sie, indem man jedes Element durch seine* p^i*-te Potenz ersetzt,* $i = 0, 1, 2, \ldots, r-1$.

Beweis: Der durch die Zahlen $0, 1, \ldots, p-1$ gebildete Körper besitzt keinen Automorphismus außer dem identischen. Denn sowohl das Einheitselement 0 der additiven Gruppe als das Einheitselement 1 der multiplikativen bleiben bei jedem Automorphismus ungeändert. Daher gilt dasselbe auch von $1+1=2$, $1+1+1=3$ usw. bis $p-1$.

Nun sei ein allgemeiner Körper mit p^r Elementen vorgelegt. Ersetzt man jedes Element durch seine p-te Potenz, so erhält man für die zyklische Gruppe einen Automorphismus, da p zu ihrer Ordnung $p^r - 1$ prim ist. Aber es wird auch $(a+b)^p = a^p + b^p$, wie aus der Tatsache folgt, daß die Binomialkoeffizienten $\binom{p}{i}$ außer $\binom{p}{0}$ und $\binom{p}{p}$ durch p teilbar sind. Bei diesem Automorphismus gehen die Zahlen $0, 1, \ldots, p-1$ in sich selbst über. Nachdem man diesen ersten Automorphismus ausgeführt hat, kann man weiterfahren und wiederum jedes Element durch seine p-te Potenz ersetzen usw. In dieser Weise erhält man gerade r verschiedene, denn es gilt für jedes Element $a^{p^r} = a$.

Man bilde nun die Gleichung $(x-a)(x-a^p)(x-a^{p^2})\ldots(x-a^{p^{r-1}}) = 0$. Die linke Seite besitzt als Koeffizienten die elementarsymmetrischen Funktionen von $a, a^p, a^{p^2}, \ldots, a^{p^{r-1}}$. Sei $f(a, \ldots, a^{p^{r-1}})$ eine solche. Dann wird nach Anwendung des Automorphismus $f(a, \ldots, a^{p^{r-1}})^p = f(a^p, \ldots, a^{p^r}) = f(a, \ldots, a^{p^{r-1}})$. Die p-te Potenz dieses Koeffizienten ist gleich der ersten, und sie sind daher Zahlen $0, 1, \ldots, p-1$. Die obige Gleichung besitzt r Wurzeln und ist vom Grade r. Geht bei einem weiteren Automorphismus a über in a^q, so muß auch a^q dieser Gleichung genügen, denn diese geht beim Automorphismus in sich selber über. q ist daher eine der Zahlen $p, p^2, \ldots, p^r$, denn die Gleichung kann nicht mehr als r Wurzeln haben.

Die Gruppe der Automorphismen ist eine zyklische von der Ordnung r.

Zum Schlusse sollen noch die zu p primen Reste $(\mathrm{mod}\ p^n)$ betrachtet werden. Sie bilden offenbar nach der Multiplikation eine Gruppe.

Es sei zunächst $p > 2$. Die Reste $\equiv 1\ (\mathrm{mod}\ p)$ bilden eine Untergruppe vom Index $p-1$, und ist $a \equiv 1\ (p^i)$ aber $\not\equiv 1\ (p^{i+1})$, so wird $a^p \equiv (1 + rp^i)^p = 1 + rp \cdot p^i + r^2 \frac{p(p-1)}{2} p^{2i} + \ldots \equiv 1\ (\mathrm{mod}\ p^{i+1})$ aber $\not\equiv 1 \cdot (\mathrm{mod}\ p^{i+2})$. Hieraus folgt: Diejenigen Reste, die $\equiv 1\ (\mathrm{mod}\ p)$, bilden eine zyklische Untergruppe von der Ordnung p^{n-1}, die erzeugt wird durch einen beliebigen Rest $\equiv 1\ (\mathrm{mod}\ p)$ aber $\not\equiv 1\ (\mathrm{mod}\ p^2)$, also etwa durch $1+p$. Die Faktorgruppe dieser Gruppe ist zyklisch und von der Ordnung $p-1$, denn sie ist homomorph mit der Gruppe der Reste mod p. Weil $p-1$ zu p prim ist, so ist die ganze Gruppe zyklisch und von der Ordnung $p^{n-1}(p-1)$.

Nun sei 2^n als Modul betrachtet. Hier bilden die 2^{n-2}-Reste $\equiv 1\ (\mathrm{mod}\ 4)$ eine zyklische Untergruppe, was genau so wie oben bewiesen wird. Dazu kommt noch die durch -1 und $+1$ gebildete Untergruppe von der Ordnung 2, daher ist hier der Typus der Gruppe $(2^{n-2}, 2)$.

Satz 38: *Die zu p primen Reste mod p^n bilden nach der Multiplikation für $p > 2$ eine zyklische Gruppe von der Ordnung $p^{n-1}(p-1)$, für $p = 2$ eine Abelsche vom Typus $(2^{n-2}, 2)$. Ist $a \equiv 1$ $\begin{cases} \text{mod } p \text{ für } p > 2 \\ \text{„ } 4 \text{ „ } p = 2, \end{cases}$ so ist $\frac{a^{p^r+s}-1}{a^{p^r}-1}$ eine genau durch die s-te und durch keine höhere Potenz von p teilbare ganze Zahl.*

Es ist nur eine andere Fassung dieses Satzes, wenn wir folgende Aussage machen:

Satz 38a: *Die Automorphismen einer zyklischen Gruppe von der Ordnung p^n bilden eine zyklische Gruppe von der Ordnung $p^{n-1}(p-1)$ für ungerade p und im Falle $p = 2$ eine Abelsche Gruppe vom Typus $(2^{n-2}, 2)$.*

Beweis: Ist P das erzeugende Element der Gruppe, so erhält man jeden Automorphismus, indem man P durch P^r ersetzt, wobei r alle zu p primen Reste mod p^n durchläuft. Sind $P \to P^r$ und $P \to P^s$ zwei Automorphismen, so ist der zusammengesetzte $P \to P^{rs}$, ihre Gruppe ist also die Gruppe des Satzes 38.

Historische Notiz: *Galois* hat die von ihm entdeckten Imaginären in der Arbeit: Sur la théorie des nombres (Oeuvres S. 15) behandelt, welche 1830 im Journal de Férussac t. **13**, S. 428 erschienen ist. Über ihre Bedeutung für die Zahlentheorie vgl. § 62. Eine ausführliche Theorie findet sich in der schönen Monographie von *L. C. Dickson*, Linear groups with an exposition of the Galois field theory, Leipzig 1901.

4. Kapitel.

Konjugierte Untergruppen.

§ 17. Normalisatoren.

Definition: Die Gesamtheit der Elemente einer Gruppe, die mit einem Komplex vertauschbar sind, bilden eine Untergruppe, die der ***Normalisator*** des Komplexes genannt wird. Falls der Komplex eine Untergruppe ist, oder falls er aus einem einzigen Element besteht, so ist er in seinem Normalisator enthalten.

Satz 39: *Die Gesamtheit der Elemente einer Gruppe, die mit einem Element vertauschbar sind, bildet eine Untergruppe, deren Index gleich ist der Anzahl der Elemente in der Klasse dieses Elementes.*

Beweis: Sei $\mathfrak{N}$ der Normalisator von A und B ein mit A konjugiertes Element, so bilden diejenigen Elemente S, für welche

$S^{-1}AS = B$ ist, eine Nebengruppe von $\mathfrak{N}$, denn sind S und T zwei solche, so wird ST^{-1} mit A vertauschbar. Daher gibt es so viele Nebengruppen von $\mathfrak{N}$, als es mit A konjugierte Elemente gibt.

Korollar: Die Anzahl der Elemente in einer Klasse ist ein Teiler der Ordnung der Gruppe. Denn sie ist Index einer Untergruppe.

Sind A und $S^{-1}AS$ zwei konjugierte Elemente, und ist $\mathfrak{N}$ der Normalisator von A, so ist $S^{-1}\mathfrak{N}S$ derjenige von $S^{-1}AS$. Daher bilden die Normalisatoren der Elemente einer Klasse ein System konjugierter Untergruppen. Die Normalisatoren zweier konjugierter Elemente können miteinander übereinstimmen, aber nur dann, wenn die beiden Elemente vertauschbar sind. Diese Bedingung ist jedoch nicht hinreichend.

Satz 40: *Der Index des Normalisators einer Untergruppe $\mathfrak{H}$ ist gleich der Anzahl der mit $\mathfrak{H}$ konjugierten Untergruppen.*

Der Beweis verläuft wie der vorhergehende.

Ein System konjugierter Untergruppen enthält niemals alle Elemente der Gruppe. Denn ist h die Ordnung, r der Index von $\mathfrak{H}$, so enthält das System nach Satz 40 höchstens $h \cdot r = g$ Elemente, darunter tritt E aber r-mal auf.

§ 18. Zerlegung einer Gruppe nach zwei Untergruppen.

Sind $\mathfrak{H}$ und $\mathfrak{K}$ zwei Untergruppen, so enthält der Komplex $\mathfrak{H}\mathfrak{K}$ eine Anzahl rechtsseitiger Nebengruppen von $\mathfrak{H}$ und eine Anzahl linksseitiger Nebengruppen von $\mathfrak{K}$. Sei $\mathfrak{D}$ der Durchschnitt von $\mathfrak{H}$ und $\mathfrak{K}$, h der Index von $\mathfrak{D}$ unter $\mathfrak{H}$ und k derjenige von $\mathfrak{D}$ unter $\mathfrak{K}$. Sind K_1 und K_2 zwei Elemente von $\mathfrak{K}$, so sind die beiden Nebengruppen $\mathfrak{H}K_1$ und $\mathfrak{H}K_2$ von $\mathfrak{H}$ dann und nur dann identisch, wenn $K_1K_2^{-1}$ in $\mathfrak{H}$ und also in $\mathfrak{D}$ liegt. Hieraus folgt sofort, daß $\mathfrak{H}\mathfrak{K}$ genau k rechtsseitige Nebengruppen von $\mathfrak{H}$ enthält, denn jede der k rechtsseitigen Nebengruppen von $\mathfrak{D}$ in $\mathfrak{K}$ ergibt eine Nebengruppe von $\mathfrak{H}$ in $\mathfrak{H}\mathfrak{K}$. Genau so beweist man, daß h linksseitige Nebengruppen von $\mathfrak{K}$ in $\mathfrak{H}\mathfrak{K}$ vorkommen.

Nun sei A irgendein Element von $\mathfrak{G}$, und man bilde den Komplex $\mathfrak{H}A\mathfrak{K}$. Ist A nicht in $\mathfrak{H}\mathfrak{K}$ enthalten, so enthält $\mathfrak{H}A\mathfrak{K}$ kein Element gemeinsam mit $\mathfrak{H}\mathfrak{K}$. Denn sei etwa $H_1AK_1 = H_2K_2$, so wäre $A = H_1^{-1}H_2K_2K_1^{-1}$, also wäre A ein Element in $\mathfrak{H}\mathfrak{K}$, gegen die Voraussetzung. Genau so beweist man, daß zwei Komplexe $\mathfrak{H}A\mathfrak{K}$ und $\mathfrak{H}B\mathfrak{K}$ entweder identisch sind oder kein Element gemeinsam haben. Diese Überlegungen sind im wesentlichen Wiederholungen der entsprechenden für eine Untergruppe und ihre Nebengruppen: für $\mathfrak{K} = E$ erhält man die rechtsseitigen Nebengruppen von $\mathfrak{H}$ und für $\mathfrak{H} = E$ die linksseitigen von $\mathfrak{K}$. Es muß nun untersucht werden, aus

wie vielen rechtsseitigen Nebengruppen von $\mathfrak{H}$ der Komplex $\mathfrak{H} A \mathfrak{K}$ besteht. Ist S irgendeines seiner Elemente, so liegt die ganze Nebengruppe $\mathfrak{H} S$ in $\mathfrak{H} A \mathfrak{K}$, denn es gilt die Gleichung $\mathfrak{H} H A K = \mathfrak{H} A K$. Damit $\mathfrak{H} A K_1 = \mathfrak{H} A K_2$ ist, muß $A K_1 K_2^{-1} A^{-1}$ in $\mathfrak{H}$ liegen, oder, was damit gleichbedeutend ist, es muß $K_1 K_2^{-1}$ in $A^{-1} \mathfrak{H} A$ enthalten sein und also auch im Durchschnitt $\overline{\mathfrak{D}}$ von $\mathfrak{K}$ und $A^{-1} \mathfrak{H} A$. Umgekehrt wenn K in diesem Durchschnitt liegt, so kann man setzen $K = A^{-1} H A$ und es wird $\mathfrak{H} A K = \mathfrak{H} A A^{-1} H A = \mathfrak{H} A$. Ist $\mathfrak{K} = \overline{\mathfrak{D}} + \overline{\mathfrak{D}} K_2 + \overline{\mathfrak{D}} K_3 + \ldots + \overline{\mathfrak{D}} K_k$, so ergeben zwei Elemente aus derselben Nebengruppe dieselbe Nebengruppe von $\mathfrak{H}$ und zwei aus verschiedenen Nebengruppen auch zwei verschiedene Nebengruppen von $\mathfrak{H}$. Es sind also ebenso viele Nebengruppen von $\mathfrak{H}$ in $\mathfrak{H} A \mathfrak{K}$ enthalten, als der Index des Durchschnittes von $\mathfrak{K}$ mit $A^{-1} \mathfrak{H} A$ unter $\mathfrak{K}$ beträgt. In analoger Weise folgt, daß die Anzahl der linksseitigen Nebengruppen von $\mathfrak{K}$ in $\mathfrak{H} A \mathfrak{K}$ gleich ist dem Index desselben Durchschnittes unter $A^{-1} \mathfrak{H} A$.

Satz 41: *Sind $\mathfrak{H}$ und $\mathfrak{K}$ zwei Untergruppen von $\mathfrak{G}$, so zerfällt $\mathfrak{G}$ in eindeutiger Weise in Komplexe von folgender Art:* $\mathfrak{G} = \mathfrak{H} \mathfrak{K} + \mathfrak{H} A \mathfrak{K} + \mathfrak{H} B \mathfrak{K} + \ldots$. *Man nennt dies die Zerlegung von $\mathfrak{G}$ nach dem* ***Doppelmodul*** $(\mathfrak{H}, \mathfrak{K})$. *Jedes Element von $\mathfrak{G}$ ist in einem und nur in einem Komplex enthalten und jeder Komplex von der Gestalt $\mathfrak{H} S \mathfrak{K}$ ist mit einem unter ihnen identisch.*

Die Anzahl der rechtsseitigen Nebengruppen von $\mathfrak{H}$ in $\mathfrak{H} A \mathfrak{K}$ ist gleich dem Index des Durchschnittes von $A^{-1} \mathfrak{H} A$ mit $\mathfrak{K}$ unter $\mathfrak{K}$, die Anzahl der linksseitigen Nebengruppen von $\mathfrak{K}$ in $\mathfrak{H} A \mathfrak{K}$ ist gleich dem Index desselben Durchschnittes unter $A^{-1} \mathfrak{H} A$.

Hiermit ist auch die Aufgabe gelöst, diejenigen Komplexe zu bestimmen, die gleichzeitig aus rechtsseitigen Nebengruppen von $\mathfrak{H}$ und linksseitigen Nebengruppen von $\mathfrak{K}$ bestehen. Ist nämlich A ein Element eines solchen Komplexes, so muß auch der Komplex $\mathfrak{H} A \mathfrak{K}$ darunter vorkommen. Wenn der Komplex damit noch nicht erschöpft ist, so muß er einen weiteren der in Satz 41 genannten Komplexe enthalten und eine Weiterführung dieses Verfahrens zeigt, daß der Komplex eine Summe von Komplexen von der Gestalt $\mathfrak{H} A \mathfrak{K}$ ist.

Der Satz 41 ist besonders wichtig wegen der Möglichkeit, gewisse einfache zahlentheoretische Sätze anzuwenden.

Zunächst sei $\mathfrak{H} = \mathfrak{K}$. Der erste Komplex wird dann $\mathfrak{H} \mathfrak{H} = \mathfrak{H}$. Ein zweiter möge m_2 rechtsseitige Nebengruppen enthalten, ein i-ter m_i. Bezeichnet man den Index von $\mathfrak{H}$ unter $\mathfrak{G}$ mit m, so wird

$$m = m_1 + m_2 + \ldots + m_r,$$

wobei $m_1 = 1$ ist. Hieraus folgt insbesondere $m_i < m$. Nach dem

Satz 41 ist m_i der Index des Durchschnittes von $\mathfrak{H}$ mit einer konjugierten Gruppe unter $\mathfrak{H}$ und es ergibt sich der

Satz 42: *Sind $\mathfrak{H}$ und $S^{-1}\mathfrak{H}S$ zwei konjugierte Untergruppen von $\mathfrak{G}$, so ist der Index ihres Durchschnittes unter $\mathfrak{H}$ kleiner als der Index von $\mathfrak{H}$ unter $\mathfrak{G}$.*

Allgemein gilt der Satz, daß *der Index des Durchschnittes zweier beliebiger Untergruppen $\mathfrak{H}$ und $\mathfrak{K}$ unter $\mathfrak{K}$ höchstens gleich dem Index von $\mathfrak{H}$ unter $\mathfrak{G}$ ist.* Der Beweis wird genau wie für den Satz 42 geführt.

Historische Notiz: Doppelmoduln wurden zuerst von *Cauchy* betrachtet. Die Abhandlungen 300—327 seiner Werke (1. Serie Bd. 9 und 10) enthalten an manchen Stellen derartige Untersuchungen, z. B. Bd. 10, S. 66. Die heutige Gestalt der Theorie stammt von *G. Frobenius* (Über endliche Gruppen, Berl. Berichte 1895, S. 163).

5. Kapitel.

Sylowgruppen und p-Gruppen.

§ 19. Sylowgruppen.

Ist p ein Primteiler der Ordnung einer Gruppe $\mathfrak{G}$, so enthält $\mathfrak{G}$ ein Element von der Ordnung p. Dies ist ein Spezialfall des Satzes 27, der zum erstenmal (1845) von *Cauchy*[1]) bewiesen worden ist. Ein überaus einfacher Beweis ist der folgende:

Der Satz gilt für Gruppen von der Ordnung p und allgemein auch für alle *Abel*schen Gruppen. Man setze voraus, daß er für alle Gruppen gilt, deren Ordnung das Produkt von höchstens $n-1$ Primzahlen ist und beweist dann folgendermaßen seine Gültigkeit für Gruppen, deren Ordnung das Produkt von n Primzahlen ist. Wenn $\mathfrak{G}$ eine Untergruppe besitzt, deren Index zu p prim ist, so ist die Ordnung derselben durch p teilbar und sie enthält daher nach Voraussetzung Elemente von der Ordnung p. Es braucht also bloß der Fall betrachtet zu werden, wo der Index jeder Untergruppe durch p teilbar ist. Nun ist speziell die Anzahl der Elemente in einer Klasse nach Satz 39 ein solcher Index. Angenommen, diese Anzahlen seien stets entweder gleich 1 oder durch p teilbare Zahlen, so folgt, daß es außer E noch weitere Klassen geben muß, die nur ein Element enthalten. Diese letzteren bilden das Zentrum der Gruppe $\mathfrak{G}$ und seine Ordnung unterscheidet sich von derjenigen von $\mathfrak{G}$ um ein Vielfaches von p; sie ist daher selbst durch p teilbar und enthält als *Abel*sche Gruppe ein Element von der Ordnung p.

[1]) Oeuvres. 1. Serie Bd. 9, S. 358.

Satz 43[1]: *Ist p^r die höchste in der Ordnung von $\mathfrak{G}$ aufgehende Potenz von p, so gibt es in $\mathfrak{G}$ Untergruppen von der Ordnung p^r und zwei beliebige derselben sind konjugiert. Sie heißen die* ***Sylowgruppen*** *von $\mathfrak{G}$. Jede Untergruppe, deren Ordnung eine Potenz von p ist, ist in einer von ihnen als Untergruppe enthalten.*

Beweis: Die Tatsache, daß es eine Untergruppe von der Ordnung p^r gibt, läßt sich mit den Hilfsmitteln des vorherigen Beweises erhärten. Man wende dieselbe vollständige Induktion an und nehme den Satz als bewiesen an für Gruppen von niedrigerer Ordnung. Im Falle, daß eine Untergruppe existiert, deren Index zu p prim ist, besitzt diese und also auch $\mathfrak{G}$ eine Untergruppe von der Ordnung p^r nach Voraussetzung. Im anderen Falle sei $\mathfrak{P}$ eine Untergruppe von der Ordnung p, die im Zentrum enthalten ist. Ihre Existenz ist nachgewiesen worden. $\mathfrak{P}$ ist Normalteiler von $\mathfrak{G}$, und $\mathfrak{G}/\mathfrak{P}$ ist eine Gruppe, deren Ordnung kleiner ist als diejenige von $\mathfrak{G}$. Sie besitzt daher eine Sylowgruppe von der Ordnung p^{r-1} und zu ihr gehört eine Untergruppe von $\mathfrak{G}$ mit der Ordnung p^r.

Um den Satz in allen seinen Teilen zu beweisen, zieht man die Resultate des vorherigen Paragraphen heran. Sei $\mathfrak{P}$ irgendeine Untergruppe, deren Ordnung eine Potenz von p ist, und sei $\mathfrak{G} = \mathfrak{P} + \mathfrak{P} A_2 \mathfrak{P} + \mathfrak{P} A_3 \mathfrak{P} + \ldots + \mathfrak{P} A_s \mathfrak{P}$ die Zerlegung von $\mathfrak{G}$ nach $(\mathfrak{P}, \mathfrak{P})$. Die Anzahl der Nebengruppen von $\mathfrak{P}$ in $\mathfrak{P} A_i \mathfrak{P}$ sei m_i und der Index von $\mathfrak{P}$ unter $\mathfrak{G}$ sei m. Dann wird $m = m_1 + m_2 + \ldots + m_s$. Die Zahlen m_i sind als Teiler der Ordnung von $\mathfrak{P}$ Potenzen von p oder 1. Ist nun m durch p teilbar, so muß wegen $m_1 = 1$ eine durch p teilbare Anzahl von Größen m_i gleich 1 sein. Wenn aber $\mathfrak{P} A \mathfrak{P}$ nur eine rechtsseitige Nebengruppe von $\mathfrak{P}$ enthält, so wird $\mathfrak{P} A = A \mathfrak{P}$ oder $A^{-1} \mathfrak{P} A = \mathfrak{P}$, wie eine einfache Abzählung der Elemente ergibt. Sind $\mathfrak{P} A \mathfrak{P}$ und $\mathfrak{P} B \mathfrak{P}$ zwei solche Komplexe, so wird $(\mathfrak{P} A \mathfrak{P})(\mathfrak{P} B \mathfrak{P}) = \mathfrak{P} A \mathfrak{P} B \mathfrak{P} = \mathfrak{P} A B \mathfrak{P} = \mathfrak{P} A B$ und daraus folgt, daß auch $\mathfrak{P} A B \mathfrak{P}$ ein solcher Komplex ist, und daß diese Komplexe eine Gruppe bilden. Ihnen entspricht der Normalisator von $\mathfrak{P}$. Denn ist A ein Element daraus, so wird $A \mathfrak{P} = \mathfrak{P} A$ und also $\mathfrak{P} A \mathfrak{P} = \mathfrak{P} A$. Hiermit ist bewiesen, daß der Index von $\mathfrak{P}$ unter dem Normalisator von $\mathfrak{P}$ durch p teilbar ist. Sei $\mathfrak{N}$ dieser Normalisator, so besitzt $\mathfrak{N}/\mathfrak{P}$ eine Untergruppe von der Ordnung p und daher ist $\mathfrak{P}$ als Normalteiler in einer Gruppe enthalten, deren Ordnung eine Potenz von p ist. Das Verfahren nimmt erst ein Ende, wenn man zu einer Untergruppe gelangt ist, deren Ordnung die höchste in der Ordnung von $\mathfrak{G}$ aufgehende Potenz von p ist. Damit ist die erste und dritte Aussage des Satzes bewiesen.

---

[1]) *L. Sylow:* Théorèmes sur les groupes de substitutions. Math. Ann. 5, S. 584.

Nun seien $\mathfrak{P}$ und $\mathfrak{Q}$ zwei Sylowgruppen von derselben Ordnung, und man zerlege $\mathfrak{G}$ nach $(\mathfrak{P}, \mathfrak{Q})$:

$$\mathfrak{G} = \mathfrak{P}\mathfrak{Q} + \mathfrak{P}A_2\mathfrak{Q} + \mathfrak{P}A_3\mathfrak{Q} + \ldots + \mathfrak{P}A_s\mathfrak{Q}.$$

Wiederum ist die Anzahl der Nebengruppen von $\mathfrak{P}$ in jedem der Komplexe 1 oder eine Potenz von p. Die Gesamtzahl der Nebengruppen ist aber gleich dem Index von $\mathfrak{P}$ unter $\mathfrak{G}$ und daher zu p prim. Daher muß mindestens einer der Komplexe, etwa $\mathfrak{P}A\mathfrak{Q}$, aus bloß einer Nebengruppe von $\mathfrak{P}$ bestehen. Daraus folgt aber, daß der Index des Durchschnittes von $A^{-1}\mathfrak{P}A$ und $\mathfrak{Q}$ unter $\mathfrak{Q}$ gleich 1 ist und so wird $\mathfrak{Q} = A^{-1}\mathfrak{P}A$, womit der Satz bewiesen ist.

Satz 44: *Ist $\mathfrak{H}$ eine Untergruppe von $\mathfrak{G}$ und sind $\mathfrak{P}_1$ und $\mathfrak{P}_2$ zwei Sylowgruppen von $\mathfrak{H}$, so sind sie nicht beide in derselben Sylowgruppe von $\mathfrak{G}$ enthalten.*

Beweis: Wären $\mathfrak{P}_1$ und $\mathfrak{P}_2$ in derselben Sylowgruppe von $\mathfrak{G}$ enthalten, so wäre die durch $\mathfrak{P}_1$ und $\mathfrak{P}_2$ erzeugte Gruppe eine Untergruppe dieser Sylowgruppe und sie besäße daher ebenfalls eine Potenz von p als Ordnung. Da sie außerdem in $\mathfrak{H}$ enthalten wäre, so müßte sie dieselbe Ordnung wie $\mathfrak{P}_1$ besitzen, was nur möglich ist, wenn $\mathfrak{P}_1 = \mathfrak{P}_2$.

§ 20. Normalisatoren der Sylowgruppen[1]).

Satz 45: *Der Normalisator einer Sylowgruppe ist sein eigener Normalisator.*

Beweis: Sei $\mathfrak{P}$ eine Sylowgruppe von $\mathfrak{G}$ und $\mathfrak{J}$ ihr Normalisator. Wenn nun Q ein Element außerhalb von $\mathfrak{J}$ ist, dergestalt, daß $Q^{-1}\mathfrak{J}Q = \mathfrak{J}$, so ist $Q^{-1}\mathfrak{P}Q \neq \mathfrak{P}$ und $\mathfrak{J}$ müßte neben $\mathfrak{P}$ auch $Q^{-1}\mathfrak{P}Q = \mathfrak{P}'$ enthalten. Beide Untergruppen $\mathfrak{P}$ und $\mathfrak{P}'$ wären *Sylowgruppen* von $\mathfrak{J}$ und als solche innerhalb $\mathfrak{J}$ konjugiert. Das widerspricht der Tatsache, daß $\mathfrak{P}$ Normalteiler von $\mathfrak{J}$ ist.

Der Satz läßt sich verallgemeinern in folgender Weise: *Ist die Ordnung einer Untergruppe prim zu ihrem Index, so ist der Normalisator der Untergruppe sein eigener Normalisator, d. h. es gibt außer seinen eigenen Elementen keines in $\mathfrak{G}$, das mit ihm vertauschbar ist.* Der Beweis verläuft genau so wie für den speziellen Fall.

Ist weiter $\mathfrak{P}_1$ eine Untergruppe der Sylowgruppe $\mathfrak{P}$, die in keiner anderen Sylowgruppe enthalten ist, so ist jedes Element, das mit $\mathfrak{P}_1$ vertauschbar ist, auch mit $\mathfrak{P}$ vertauschbar. Der Normalisator von $\mathfrak{P}_1$ ist im Normalisator von $\mathfrak{P}$ enthalten. Denn wenn $S^{-1}\mathfrak{P}_1 S = \mathfrak{P}_1$, so ist $\mathfrak{P}_1$ auch in $S^{-1}\mathfrak{P}S$ enthalten und nach Voraussetzung folgt,

[1]) Die Sätze dieses Paragraphen stammen von *Frobenius* und *Burnside*.

daß alsdann $S^{-1}\mathfrak{P}S = \mathfrak{P}$ ist. Eine Änderung tritt sofort ein, wenn die Untergruppe $\mathfrak{P}_1$ noch in anderen Sylowgruppen vorkommt.

Satz 46: *Besitzt der Durchschnitt $\mathfrak{P}_1$ zweier Sylowgruppen die Eigenschaft, daß keine Untergruppe von $\mathfrak{G}$, die $\mathfrak{P}_1$ enthält (außer $\mathfrak{P}_1$ selbst), in mehr als einer Sylowgruppe enthalten ist, so sind die Normalisatoren von $\mathfrak{P}_1$ in denjenigen Sylowgruppen, die $\mathfrak{P}_1$ enthalten, homomorph. Der Normalisator von $\mathfrak{P}_1$ in $\mathfrak{G}$ enthält Elemente, die nicht in den Normalisatoren dieser Sylowgruppen vorkommen.*

Beweis: Die Normalisatoren $\mathfrak{N}_1, \mathfrak{N}_2, \ldots, \mathfrak{N}_s$ von $\mathfrak{P}_1$ in den Sylowgruppen, die $\mathfrak{P}_1$ enthalten, besitzen $\mathfrak{P}_1$ als echte Untergruppe. Sie sind die Sylowgruppen des Normalisators $\mathfrak{N}$ von $\mathfrak{P}_1$ in $\mathfrak{G}$, denn sie sind in $\mathfrak{N}$ enthalten und umgekehrt kann eine Sylowgruppe von $\mathfrak{N}$ nur in *einer* der Sylowgruppen von $\mathfrak{G}$ enthalten sein, weil sie $\mathfrak{P}_1$ als *eigentliche* Untergruppe enthält. Hiernach ist also jeder Sylowgruppe von $\mathfrak{G}$, die $\mathfrak{P}_1$ enthält, eine und nur eine Sylowgruppe des Normalisators von $\mathfrak{P}_1$ zugeordnet. Irgendein Element von $\mathfrak{N}$, das nicht mit einer Sylowgruppe von $\mathfrak{N}$ vertauschbar ist, ist auch nicht mit einer der Sylowgruppen von $\mathfrak{G}$ vertauschbar, womit die letzte Behauptung des Satzes erwiesen ist.

Die Anzahl der konjugierten Normalisatoren einer Sylowgruppe ist nach Satz 40 und 45 gleich dem Index des Normalisators. Der Durchschnitt zweier verschiedener konjugierter Normalisatoren besitzt einen durch p teilbaren Index. Man zerlege nun $\mathfrak{G}$ nach $(\mathfrak{N}, \mathfrak{N})$:

$$\mathfrak{G} = \mathfrak{N}\mathfrak{N} + \mathfrak{N}A\mathfrak{N} + \ldots.$$

Ist n der Index von $\mathfrak{N}$, so wird $n \equiv 1 \pmod{p}$. Denn $\mathfrak{N}\mathfrak{N} = \mathfrak{N}$ enthält bloß eine Nebengruppe von $\mathfrak{N}$, die übrigen Komplexe dagegen stets eine durch p teilbare Zahl.

Satz 47: *Der Index des Normalisators einer Sylowgruppe von der Ordnung p^r ist stets kongruent 1 (mod p).*

Die Anzahl der verschiedenen Sylowgruppen von der Ordnung p^r ist $\equiv 1$ (mod p), denn sie ist gleich der Anzahl der Normalisatoren.

Satz 48: *Wenn P und Q zwei Elemente des Zentrums einer Sylowgruppe sind, die im Normalisator derselben nicht konjugiert sind, so gehören sie in $\mathfrak{G}$ zu verschiedenen Klassen. Zwei Normalteiler einer Sylowgruppe sind entweder im Normalisator konjugiert oder sie sind in der ganzen Gruppe nicht konjugiert.*

Beweis: Sei $\mathfrak{P}$ die Sylowgruppe und sei

$$S^{-1}PS = Q \qquad S^{-1}\mathfrak{P}S = \mathfrak{P}' \neq \mathfrak{P}.$$

Man betrachte die Untergruppe $\mathfrak{R}$ bestehend aus den mit Q vertauschbaren Elementen. Sie enthält $\mathfrak{P}$ und $\mathfrak{P}'$, denn Q ist im Zentrum von $\mathfrak{P}$, ebenso auch P, daher ist $S^{-1}PS = Q$ im Zentrum von $S^{-1}\mathfrak{P}S = \mathfrak{P}'$. $\mathfrak{P}$ und $\mathfrak{P}'$ sind Sylowgruppen von $\mathfrak{R}$ und daher in $\mathfrak{R}$

konjugiert. Sei T in $\mathfrak{K}$ und $T^{-1}\mathfrak{P}T = \mathfrak{P}'$, dann ist nach Definition $T^{-1}QT = Q$. Also:

$$T^{-1}S^{-1}PST = Q \qquad T^{-1}S^{-1}\mathfrak{P}ST = \mathfrak{P}.$$

ST gehört also zum Normalisator von $\mathfrak{P}$ und transformiert P in Q. Die zweite Aussage des Satzes beweist man wörtlich wie die erste, indem man nur statt P und Q die beiden Normalteiler einsetzt.

Satz 49: *Ist eine Sylowgruppe von $\mathfrak{G}$ im Zentrum ihres Normalisators enthalten, so gehören alle ihre Elemente zu verschiedenen Klassen von $\mathfrak{G}$.*

Beweis: Zwei Elemente der Sylowgruppe sind im Normalisator nicht konjugiert, daher nach dem vorigen Satz auch nicht in $\mathfrak{G}$.

§ 21. Gruppen, deren Ordnung eine Primzahlpotenz ist.

Eine Gruppe, deren Ordnung die Potenz p^s einer Primzahl ist, sei kurz als ***p*-Gruppe** bezeichnet.

Satz 50: *Jede p-Gruppe besitzt ein von E verschiedenes Zentrum.*

Beweis: Bezeichnet man mit $h_1, h_2, \ldots, h_r$ die Anzahlen der Elemente in den r Klassen, so wird $h_1 + h_2 + \ldots + h_r = p^s$. Die Zahlen h sind entweder $= 1$ oder Potenzen von p und, da $h_1 = 1$ ist, muß es außer E noch weitere Elemente geben, die für sich allein eine Klasse bilden. Diese bilden das Zentrum.

Satz 51: *Jede p-Gruppe ist auflösbar.*

Beweis: Sei $\mathfrak{Z}_1$ das Zentrum der Gruppe $\mathfrak{G}$, dann ist auch $\mathfrak{G}/\mathfrak{Z}_1$ eine p-Gruppe und besitzt ein Zentrum. Diesem entspricht ein Normalteiler $\mathfrak{Z}_2$ von $\mathfrak{G}$, der $\mathfrak{Z}_1$ als eigentlichen Normalteiler enthält. Indem man so fortfährt, erhält man eine Reihe von Normalteilern $\mathfrak{E}, \mathfrak{Z}_1, \mathfrak{Z}_2, \ldots$, die notwendig mit $\mathfrak{G}$ endet, und bei der stets $\mathfrak{Z}_i/\mathfrak{Z}_{i-1}$ eine *Abel*sche Gruppe ist. Die Ableitung von $\mathfrak{G}$ ist jedenfalls im letzten $\mathfrak{Z}$ enthalten und daher von $\mathfrak{G}$ verschieden, womit der Satz bewiesen ist.

Satz 52: *Jede eigentliche Untergruppe einer p-Gruppe ist von ihrem Normalisator verschieden und kommt in einer Kompositionsreihe vor.*

Beweis: Man zerlege $\mathfrak{G}$ nach $(\mathfrak{H}, \mathfrak{H})$, wobei $\mathfrak{H}$ die gegebene Untergruppe bezeichnet. Ein Komplex $\mathfrak{H}A\mathfrak{H}$ enthält entweder nur eine, oder p^i Nebengruppen $(i = 1, 2, \ldots)$. Nun ist

$$\mathfrak{G} = \mathfrak{H}\mathfrak{H} + \mathfrak{H}A\mathfrak{H} + \mathfrak{H}B\mathfrak{H} + \ldots$$

und $\mathfrak{H}\mathfrak{H} = \mathfrak{H}$. Daher muß es außer $\mathfrak{H}$ noch weitere Komplexe geben, die bloß eine Nebengruppe enthalten und diese bilden zusammen mit $\mathfrak{H}$ den Normalisator. Um eine Kompositionsreihe zu erhalten, die $\mathfrak{H}$ enthält, suche man eine Untergruppe von $\mathfrak{G}$, die $\mathfrak{H}$

als Normalteiler vom Index p enthält. Eine solche muß nach dem eben Bewiesenen existieren. Von dieser steige man in derselben Weise zu einer Gruppe mit höherer Ordnung auf, bis man zu $\mathfrak{G}$ gelangt. Die so erhaltenen Untergruppen bilden zusammen mit einer Kompositionsreihe von $\mathfrak{H}$ eine Kompositionsreihe von $\mathfrak{G}$, die $\mathfrak{H}$ enthält.

Satz 53: *Die Primfaktorgruppen der Hauptreihen sind Gruppen von der Ordnung p.*

Beweis: Man kann die Reihe $E, \mathfrak{Z}_1, \mathfrak{Z}_2, \ldots, \mathfrak{G}$ zu einer Hauptreihe ergänzen, indem man zwischen $\mathfrak{Z}_{i-1}$ und $\mathfrak{Z}_i$ Normalteiler von $\mathfrak{G}$ einschaltet. Nun ist $\mathfrak{Z}_i/\mathfrak{Z}_{i-1}$ das Zentrum von $\mathfrak{G}/\mathfrak{Z}_{i-1}$. Jede Untergruppe von $\mathfrak{Z}_i/\mathfrak{Z}_{i-1}$ ist Normalteiler von $\mathfrak{G}/\mathfrak{Z}_{i-1}$ und daher ist jede Untergruppe von $\mathfrak{G}$, die $\mathfrak{Z}_{i-1}$ enthält und die in $\mathfrak{Z}_i$ enthalten ist, Normalteiler von $\mathfrak{G}$. Infolgedessen ist eine Kompositionsreihe, die man durch Ergänzung der Reihe $E, \mathfrak{Z}_1, \mathfrak{Z}_2, \ldots, \mathfrak{G}$ erhält, eine Hauptreihe, womit der Satz bewiesen ist.

Hieraus folgt, daß es für jede Ordnung $p^s (s < r)$ mindestens einen Normalteiler gibt.

Satz 54: *Die Anzahl der Normalteiler von gegebener Ordnung in einer p-Gruppe ist $\equiv 1 \pmod{p}$.*

Beweis: Ein Normalteiler von der Ordnung p gehört dem Zentrum an. Denn ist A ein erzeugendes Element dieses Normalteilers und S ein beliebiges anderes, so wird $S^{-1}AS = A^x$. Daraus folgt weiter $S^{-2}AS^2 = A^{x^2}$ und $S^{-i}AS^i = A^{x^i}$. Nun ist, wenn x zu p prim ist, $x^{p-1} \equiv 1 \pmod{p}$ und daher wird S^{p-1} mit A vertauschbar. Da $p - 1$ prim ist zur Ordnung von S, so wird auch S mit A vertauschbar. Die sämtlichen Normalteiler von der Ordnung p erzeugen eine *Abel*sche Gruppe vom Typus $(1, 1, \ldots, 1)$, die zum Zentrum gehört und jede ihrer Untergruppen von der Ordnung p ist ein solcher Normalteiler. Die Anzahl dieser Untergruppen ist $\equiv 1 \pmod{p}$ nach Satz 34. Wenn das Zentrum $a + 1$ Basiselemente besitzt, so besitzt es $p^a + p^{a-1} + \ldots + 1$ Untergruppen von der Ordnung p, die mit den Normalteilern von derselben Ordnung identisch sind. Man nehme nun den Satz als bewiesen an für die Gruppen von der Ordnung p^{r-1}. Dann folgt der Satz für Gruppen von der Ordnung p^r leicht aus dem soeben bewiesenen. Jeder Normalteiler von der Ordnung p^{r-1} ist in einer Hauptreihe enthalten und enthält daher insbesondere einen Normalteiler $\mathfrak{P}$ von $\mathfrak{G}$ von der Ordnung p. Die Ordnung von $\mathfrak{G}/\mathfrak{P}$ ist p^{r-1} und die Anzahl ihrer Normalteiler von der Ordnung p^{s-1} ist daher $\equiv 1 \pmod{p}$. Also ist die Anzahl der Normalteiler von $\mathfrak{G}$ mit der Ordnung p^s, die $\mathfrak{P}$ enthalten, $\equiv 1 \pmod{p}$. Jeder Normalteiler von der Ordnung p liefert ein solches System, und da die Anzahl dieser Normalteiler $\equiv 1$ ist, so ist auch die Gesamtzahl der Untergruppen in diesen Systemen

$\equiv 1 \pmod{p}$. Eine Untergruppe kann hierbei mehrfach auftreten, u. zw. tritt sie offenbar genau so oft auf, als die Zahl der in ihr enthaltenen Normalteiler von $\mathfrak{G}$ mit der Ordnung p beträgt. Diese letzteren erzeugen wieder eine im Zentrum enthaltene *Abel*sche Gruppe vom Typus $(1, \ldots, 1)$ und ihre Anzahl ist ebenfalls $\equiv 1 \pmod{p}$. Wenn man jede Untergruppe nur einmal zählt, so läßt man eine durch p teilbare Zahl von Gruppen weg und die Anzahl der verschiedenen Normalteiler von der Ordnung p^s bleibt $\equiv 1 \pmod{p}$.

Satz 55: *Die Anzahl der Untergruppen von gegebener Ordnung in einer p-Gruppe ist $\equiv 1 \pmod{p}$.*

Beweis: Für die Normalteiler ist der Satz soeben bewiesen. Die übrigen ordnen sich in Systeme konjugierter, deren jedes eine durch p teilbare Zahl von Gruppen enthält.

Jede Untergruppe vom Index p ist Normalteiler, denn sie muß von ihrem Normalisator verschieden sein.

Satz 56: *Wenn eine p-Gruppe bloß einen Normalteiler vom Index p besitzt, so ist sie zyklisch.*

Beweis: Der Satz gilt für *Abel*sche Gruppen. Es genügt daher zu seinem Beweis zu zeigen, daß eine solche Gruppe *Abel*sch ist. Der Satz gelte für Gruppen von der Ordnung p^{r-1}. Ist $\mathfrak{G}$ eine Gruppe von der Ordnung p^r und $\mathfrak{P}$ einer ihrer Normalteiler von der Ordnung p, so ist $\mathfrak{G}/\mathfrak{P}$ nach Voraussetzung zyklisch, da diese Faktorgruppe nur einen Normalteiler vom Index p enthält. Sei Q irgendein Element aus einer diese zyklische Gruppe $\mathfrak{G}/\mathfrak{P}$ erzeugenden Nebengruppe, dann ist $Q^{p^{r-1}}$ in $\mathfrak{P}$, aber keine frühere Potenz. Wenn $\mathfrak{G}$ nicht zyklisch ist, so ist $Q^{p^{r-1}} = E$ und Q erzeugt zusammen mit $\mathfrak{P}$ eine *Abel*sche Gruppe, da $\mathfrak{P}$ zum Zentrum von $\mathfrak{G}$ gehört, womit der Satz bewiesen ist.

§ 22. Spezielle p-Gruppen.

Zunächst sollen Gruppen von der ungeraden Ordnung p^t untersucht werden mit zyklischem Normalteiler, dessen Faktorgruppe zyklisch ist. Sei P ein erzeugendes Element des Normalteilers, seine Ordnung p^r und Q ein Element aus einer die Faktorgruppe erzeugenden Nebengruppe. Es wird $Q^{-1}PQ = P^a$ und daraus $Q^{-i}PQ^i = P^{a^i}$. Q^i ist dann und nur dann mit P vertauschbar, wenn $a^i \equiv 1 \pmod{p^r}$. Sei die p^s-te Potenz von Q die erste mit P vertauschbare; dann erzeugt a mit seinen Potenzen eine Untergruppe von der Ordnung p^s in der multiplikativen Gruppe der zu p primen Reste mod p^r. Diese wird nach Satz 38 gebildet durch diejenigen Reste mod p^r, die $\equiv 1 \pmod{p^{r-s}}$ sind. Insbesondere ist $1 + p^{r-s}$ ein erzeugender Rest. Man setze, um übersichtliche Formeln zu erhalten, $P = P_r$, $P_r^p = P_{r-1}, \ldots,$

$P_1^p = P_0 = E$. Dann ist P_i ein Element von der Ordnung p^i und es wird $Q^{-1}PQ = PP_s$. Die spezielle Wahl von $1 + p^{r-s}$ als erzeugenden Rest bedeutet keine wesentliche Einschränkung. Ist nämlich $1 + l\,p^{r-s}$ ein anderer, so gibt es eine Potenz von $1 + l\,p^{r-s}$, etwa die m-te, die kongruent $1 + p^{r-s}$ ist $(\mathrm{mod}\, p^r)$. Es wird dann $Q^{-m}PQ^m = PP_s$, was bloß auf eine andere Auswahl des die Faktorgruppe erzeugenden Elementes herauskommt, indem Q^m statt Q gewählt ist.

Satz 57: *Ist Q mit der durch P erzeugten Gruppe $\{P\}$ vertauschbar und ist Q^{p^s} die niedrigste Potenz von Q, die mit P vertauschbar ist, so ist P^{p^s} die niedrigste Potenz von P, die mit Q vertauschbar ist.*

Beweis: Aus der Voraussetzung folgt, daß $Q^{-1}PQ = PP'$ ist, wo P' eine Potenz von P ist und die Ordnung p^s besitzt. Es wird daher $Q^{-1}P^{p^s}Q = P^{p^s}P'^{p^s} = P^{p^s}$ und hieraus folgt, daß p^s die niedrigste Zahl ist, für die gilt $Q^{-1}P^{p^s}Q = P^{p^s}$.

Satz 58: *Ist die durch P erzeugte Gruppe ein Normalteiler mit zyklischer Faktorgruppe von $\mathfrak{G}$ und gibt es in $\mathfrak{G}$ kein Element von höherer Ordnung als diejenige von P, so enthält $\mathfrak{G}$ eine zu $\{P\}$ prime zyklische Untergruppe, deren Ordnung gleich der Ordnung der Faktorgruppe von $\{P\}$ ist.*

Beweis: Nach Satz 38 ist $\frac{a^{p^{t+1}}-1}{a-1}$ genau durch p^t und durch keine höhere Potenz von p teilbar, wenn $a \equiv 1 \,(\mathrm{mod}\, p)$ ist. Nun sei Q ein Element aus einer die Faktorgruppe erzeugenden Nebengruppe von $\{P\}$. Der Index von $\{P\}$ sei $p^u = s$. Alsdann ist Q^s in $\{P\}$ enthalten und jedenfalls auch in $\{P^s\}$, weil sonst die Ordnung von Q größer wäre als die von P. Irgendein anderes Element in derselben Nebengruppe, wie Q ist von der Gestalt P^iQ. Um $(P^xQ)^s$ allgemein zu berechnen, benutzt man die folgende Formel:

$$(P^xQ)^s = P^x(QP^xQ^{-1})(Q^2P^xQ^{-2})\ldots(Q^{s-1}P^xQ^{-(s-1)})Q^s.$$

Setzt man nun $QPQ^{-1} \equiv P^a$, wo $a \equiv 1 \,(\mathrm{mod}\, p)$ ist, so wird $Q^iPQ^{-i} = P^{a^i}$ und $Q^iP^xQ^{-i} = P^{xa^i}$. Die Formel wird nun zu

$(P^xQ)^s = P^cQ^s$, wobei $c = x(1 + a + a^2 + \ldots + a^{s-1}) = x\frac{a^s-1}{a-1}$ ist.

P^c ist daher ein die Untergruppe $\left\{P^{\frac{s}{p}}\right\}$ erzeugendes Element und durchläuft diese ganze Gruppe, wenn man x die Zahlen $0, 1, \ldots$ durchlaufen läßt. Insbesondere kommt darunter auch das Element Q^{-s} vor, womit der Satz bewiesen ist.

Eine große Menge von Sätzen folgt aus dem eben bewiesenen.

Satz 59: *Eine p-Gruppe mit ungeradem p, die nur eine eigentliche Untergruppe von einer gegebenen Ordnung besitzt, ist zyklisch.*

Beweis: Zunächst sei der Satz bewiesen für den Fall, daß die Gruppe nur eine Untergruppe von der Ordnung p besitzt. Sei P ein Element von möglichst hoher Ordnung und $\mathfrak{H}$ eine Untergruppe, die $\{P\}$ als Normalteiler vom Index p enthält, dann fällt $\mathfrak{H}$ unter die Voraussetzungen des vorherigen Satzes und es gibt außerhalb von $\{P\}$ eine Untergruppe von der Ordnung p. Daher muß die Ordnung von $\{P\}$ gleich der Ordnung der Gruppe sein und sie ist zyklisch. Wenn ferner $\mathfrak{G}$ bloß eine Untergruppe $\mathfrak{P}$ von der Ordnung p^i besitzt, so nehme man einen Normalteiler $\mathfrak{N}$ von der Ordnung p^{i-1}. $\mathfrak{G}/\mathfrak{N}$ besitzt nur eine Untergruppe von der Ordnung p und ist daher zyklisch. Also ist auch $\mathfrak{G}/\mathfrak{P}$ zyklisch. Da jeder Normalteiler von $\mathfrak{G}$ mit dem Index p die Untergruppe $\mathfrak{P}$ enthalten muß und da $\mathfrak{G}/\mathfrak{P}$ zyklisch ist, so enthält $\mathfrak{G}$ bloß einen Normalteiler vom Index p und ist daher selber zyklisch nach Satz 56.

Satz 60: *Eine p-Gruppe (p ungerade), deren eigentliche Untergruppen zyklisch sind und deren Ordnung $p^r > p^2$ ist, ist zyklisch.*

Beweis: Zwei Untergruppen vom Index p besitzen als Durchschnitt eine Untergruppe von der Ordnung p^{r-2}. Da sie zyklisch sind, so besitzen sie nur eine solche Untergruppe und infolgedessen gibt es nur eine Untergruppe von der Ordnung p^{r-2}, denn eine solche ist in einer Untergruppe von der Ordnung p^{r-1} enthalten; $\mathfrak{G}$ ist also nach dem vorigen Satz zyklisch.

Ist $\{P\}$ ein zyklischer Normalteiler von $\mathfrak{G}$, dessen Faktorgruppe *Abel*sch ist, so bilden die mit P vertauschbaren Elemente einen Normalteiler von $\mathfrak{G}$, dessen Faktorgruppe zyklisch ist, da sie homomorph mit einem Automorphismus von $\{P\}$ ist. Ist der Typus von $\mathfrak{G}/\{P\}$ $(n_1, n_2, \ldots, n_r)$, und sind $Q_1, Q_2, \ldots, Q_r$ Elemente aus r-Nebengruppen, von $\{P\}$, die $\mathfrak{G}/\{P\}$ erzeugen, so folgt leicht aus den Sätzen über *Abel*sche Gruppen, daß man alle diese Elemente außer *einem* mit P vertauschbar annehmen kann, während das ausgezeichnete den Automorphismus liefert. Ist außerdem P ein Element von höchster Ordnung in $\mathfrak{G}$, so kann man die Ordnung von Q_i gleich p^{n_i} annehmen nach dem vorhergehenden Satz, denn die durch P und Q_i erzeugte Gruppe ist von dem dortigen Typus. Damit ist noch nicht gesagt, daß die Elemente $Q_1, Q_2, \ldots, Q_r$ unter sich vertauschbar sind und eine *Abel*sche Gruppe vom Typus $(n_1, n_2, \ldots, n_r)$ bilden, sondern ihre Kommutatoren können durch gewisse Potenzen von P geliefert werden. Die Kommutatorgruppe ist gewiß in $\{P\}$ enthalten, da $\mathfrak{G}/\{P\}$ *Abel*sch ist.

Es sei speziell $\mathfrak{G}$ eine Gruppe, deren Zentrum zyklisch ist. Die Faktorgruppe des Zentrums sei *Abel*sch und vom Typus $(1, 1, \ldots,)$,

ferner sei das Element P, welches das Zentrum erzeugt, ein Element von höchster Ordnung. Die Aufgabe ist, alle Gruppen von dieser Beschaffenheit anzugeben.

Nach Satz 58 kann man in jeder Nebengruppe des Zentrums ein Element von der Ordnung p finden und außerdem ist jede Untergruppe von $\mathfrak{G}$, die das Zentrum enthält, Normalteiler von $\mathfrak{G}$. Nun seien $Q_1, Q_2, \ldots, Q_r$ Elemente von der Ordnung p in den die Faktor gruppe erzeugenden Nebengruppen. Ist eines dieser Elemente mit allen übrigen vertauschbar, so ist das Zentrum nicht zyklisch. Man wird daher voraussetzen, daß jedes Element Q mit irgendeinem anderen nicht vertauschbar ist. Sei etwa $Q_1 Q_2 Q_1^{-1} Q_2^{-1} = R$, so ist R eine Potenz von P, weil die Kommutatorgruppe der kleinste Normalteiler mit *Abel*scher Faktorgruppe ist. Ferner ist p die Ordnung von R, denn Q_2 ist mit R vertauschbar, und $Q_1 Q_2 Q_1^{-1} = R Q_2$. Erhebt man in die p-te Potenz, so folgt: $R^p Q_2^{\,p} = E$ oder $R^p = E$. Ist P_1 irgendein Element von der Ordnung p in $\{P\}$, so kann man setzen $Q_1^{-1} Q_2 Q_1 = Q_2 P_1$, indem man eventuell Q_2 durch eine seiner Potenzen ersetzt, was bloß auf eine andere Wahl des Basiselementes kerauskommt. Wäre auch Q_3 nicht mit Q_1 vertauschbar und etwa wiederum $Q_3^{-1} Q_1 Q_3 = Q_1 P_1$, so kann man Q_3 durch $Q_2^{-1} Q_3$ ersetzen und erhält so ein mit Q_1 vertauschbares Basiselement, dessen Ordnung man durch Multiplikation mit einer Potenz von P als p annehmen kann, und das wieder mit Q_3 bezeichnet werden mag. In dieser Weise fortfahrend, kann man $Q_3, Q_4, \ldots$ als mit Q_1 vertauschbar annehmen. Indem man für Q_2 gleich verfährt, kann man $Q_3, Q_4, \ldots$ als mit Q_2 vertauschbar annehmen, denn es wird

$$Q_2^{-1} Q_1 Q_2 = Q_1 P_1^{-1}.$$

Da Q_3 mit Q_1 und Q_2 vertauschbar ist, so muß es ein weiteres Basiselement, etwa Q_4 geben, das mit Q_3 nicht vertauschbar ist und für das man die Gleichung annehmen kann $Q_3^{-1} Q_4 Q_3 = Q_3 P_1$. So gelangt man schließlich zu Paaren von Basiselementen Q_1, Q_2; Q_3, Q_4; $Q_5, Q_6 \ldots$. Es gilt $Q_1^{-1} Q_2 Q_1 = Q_2 P_1$ und $Q_2^{-1} Q_1 Q_2 = Q_1 P_1^{-1}$, während Q_1 und Q_2 mit allen übrigen Basiselementen vertauschbar sind. Die Elemente $Q_1, Q_3, Q_5, \ldots$, die mit $R_1, R_2, \ldots$ bezeichnet werden mögen, bilden eine *Abel*sche Gruppe vom Typus $(1, 1, \ldots, 1)$ und ebenso die Elemente $Q_2, Q_4, \ldots$, die mit $S_1, S_2, \ldots$ bezeichnet werden mögen. Alle Elemente von $\mathfrak{G}$ sind in der Gestalt $P^a R_1^{b_1} R_2^{b_2} \ldots S_1^{c_1} S_2^{c_2} \ldots$ darstellbar und für das Produkt zweier beliebiger Elemente gilt das Gesetz:

$$P^a R_1^{b_1} R_2^{b_2} \ldots S_1^{c_1} S_2^{c_2} \ldots P^d R_1^{e_1} R_2^{e_2} \ldots S_1^{f_1} S_2^{f_2} \ldots$$
$$= P^{a+d} P_1^{c_1 e_1 + \cdots} R_1^{b_1 + e_1} R_2^{b_2 + e_2} \ldots S_1^{c_1 + f_1} S_2^{c_2 + f_2} \ldots$$

Man erhält alle Gruppen, für die $\mathfrak{G}/\{P\}$ *Abel*sch und vom Typus

$(1, 1, \ldots, 1)$ ist, für die $\{P\}$ zum Zentrum gehört und in welchen P ein Element höchster Ordnung ist, indem man eine beliebige der soeben definierten Gruppen mit einer beliebigen *Abel*schen Gruppe vom Typus $(1, 1, \ldots, 1)$ multipliziert.

Nun sei $\mathfrak{P}$ ein zyklischer Normalteiler von $\mathfrak{G}$ mit einer Faktorgruppe vom Typus $(1, 1, \ldots, 1)$, aber $\mathfrak{P}$ liege nicht mehr im Zentrum von $\mathfrak{G}$. Dann gibt es ein Element Q, das der Gleichung genügt $Q^{-1}PQ = PP_1$ und die übrigen Basiselemente der Faktorgruppe kann man als mit P vertauschbare annehmen. Diese letzteren erzeugen mit P zusammen eine Gruppe von dem vorhin angegebenen Typus. Wenn sie ein direktes Produkt ist, so ist auch die ganze Gruppe ein solches, denn sei etwa R mit P und mit den sämtlichen Basiselementen außer Q vertauschbar, so kann man setzen $Q^{-1}RQ = RP_1$, daher wird PR^{-1} ein Element von derselben Ordnung wie P, das zum Zentrum der Gruppe gehört. Man käme zu einer Gruppe vom vorhergehenden Typus, folglich wird R auch mit Q vertauschbar.

Es ist nun leicht, sämtliche p-Gruppen mit zyklischen Normalteilern $\mathfrak{P}$ vom Index p und p^2 zu bestimmen. Ist der Index gleich p, so gibt es außer der zyklischen Gruppe noch eine *Abel*sche vom Typus $(r, 1)$. Ferner gibt es eine nicht *Abel*sche von der Gestalt $P^{p^r} = E, Q^p = E,\ Q^{-1}PQ = PP_1$.

Ist der Index von $\mathfrak{P}$ gleich p^2, so unterscheide man die Fälle, wo $\mathfrak{G}/\mathfrak{P}$ vom Typus (2) resp. vom Typus $(1, 1)$ ist. Im ersteren Fall gibt es drei Möglichkeiten: $P^{p^r} = E,\ Q^{p^2} = E,\ Q^{-1}PQ = PP^a$, wobei $a = 0,\ p^{r-1},\ p^{r-2}$ ist. Der erste Exponent ergibt eine *Abel*sche Gruppe vom Typus $(r, 2)$. Ist die Faktorgruppe nicht zyklisch, so gibt es eine *Abel*sche Gruppe vom Typus $(r, 1, 1)$ ferner, wenn P zum Zentrum gehört, die Gruppe

$$P^{p^r} = E,\ Q^p = E, R^p = E,\ Q^{-1}PQ = P,\ R^{-1}PR = P,\ Q^{-1}RQ = RP_1.$$

Ist P nicht im Zentrum, so ist die Gruppe das direkte Produkt einer zyklischen Gruppe von der Ordnung p und der Gruppe $P^{p^r} = E$, $Q^p = E,\ Q^{-1}PQ = PP^{p^{r-1}}$. Weitere Fälle sind nicht möglich.

Für Gruppen, deren Ordnung eine Potenz von 2 ist, treten modifizierte Betrachtungen ein, und dieser Fall ist komplizierter als der mit ungeradem p. Es soll der Fall behandelt werden, wo ein zyklischer Normalteiler von der Ordnung 2^s vorhanden ist, dessen Faktorgruppe zyklisch ist und von der Ordnung 2^r. Ist $x \equiv 1 \pmod 4$, so wird $\frac{x^{2^{r+1}} - 1}{x - 1}$ genau durch r-te und durch keine höhere Potenz von 2 teilbar. Nun sei P ein den Normalteiler erzeugendes Element und Q ein Element aus einer die Faktorgruppe erzeugenden Nebengruppe. Man setze $Q^{-1}PQ = P^x$, ist Q mit P vertauschbar, so wird $x \equiv 1$

$(\mathrm{mod}\ 2^r)$ und daher $x \equiv 1\ (\mathrm{mod}\ 4)$. Ist P ein Element von höchster Ordnung in $\mathfrak{G}$, so beweist man genau wie für ungerade Primzahlen, daß es in derselben Nebengruppe, wie Q, ein Element von der Ordnung 2^s gibt. Es gibt daher nur die folgenden Typen:

$$P^{2^r} = E,\ Q^{2^s} = E.\quad Q^{-1}PQ = PP_s (r = 2, 3, 4, \ldots)$$

Um auch den Fall $x \equiv -1\ (\mathrm{mod}\ 4)$ zu untersuchen, seien die Gruppen von der Ordnung 8 betrachtet mit einem Normalteiler von der Ordnung 4, der durch ein Element P erzeugt werden kann. Wenn die Gruppe nicht *Abel*sch ist, so muß für ein Element Q außerhalb von P die Relation bestehen: $Q^{-1}PQ = P^3$. Ist Q von der Ordnung 2, so erhält man die Diedergruppe

$$P^4 = E,\ Q^2 = E,\ Q^{-1}PQ = P^{-1}.$$

Die 4 Elemente P^iQ $(i = 0, 1, 2, 3)$ sind sämtlich von der Ordnung 2. Es gibt aber noch eine weitere Gruppe, die ***Quaternionengruppe.*** Hier ist Q von der Ordnung 4 und es gilt $P^2 = Q^2$. Dieses letztere Element ist das einzige von der Ordnung 2, denn PQ ist von der Ordnung 4 und ebenso P, P^3, Q, Q^3 und PQ^3. Setzt man $P^2 = -1$, und bezeichnet man PQ mit R, so gelten die Gesetze der *Quaternionen*: $PQ = R$, $QR = P$, $RP = Q$, $PQ = -QP$, $QR = -RQ$, $RP = -PR$, $P^2 = Q^2 = R^2 = -1$.

6. Kapitel.

Kristallographische Gruppen.

§ 23. Die ebenen Gitter[1]).

Eine geradlinige Reihe äquidistanter Punkte nennen wir eine ***Punktreihe.*** Der Abstand zweier benachbarter Punkte heißt die ***Elementardistanz*** der Reihe. Man erhält eine Punktreihe, indem man von einem beliebigen Punkt einen Vektor $\mathfrak{p}$ beliebig oft abträgt und die Endpunkte markiert und dasselbe mit dem Vektor $-\mathfrak{p}$ macht. Man erhält in dieser Weise die Gesamtheit der Vektoren $x\mathfrak{p}$ $(x = 0, \pm 1, \pm 2, \ldots)$ von dem gewählten Anfangspunkt aus abgetragen.

Entsprechend der letzten Erzeugungsweise definieren wir das ***ebene Punktgitter.*** Gegeben seien zwei beliebige Vektoren $\mathfrak{p}_1$ und $\mathfrak{p}_2$, die nicht derselben Geraden angehören. Von dem beliebig gewählten Punkt O aus trage man die Gesamtheit der Vektoren

$$x_1\mathfrak{p}_1 + x_2\mathfrak{p}_2$$

ab und markiere deren Endpunkte. Diese bilden ein ebenes Gitter. Man kann die Gitterpunkte als die Punkte mit ganzzahligen Koor-

[1]) Literatur zur Kristallographie siehe S. 171.

dinaten in einem beliebigen geradlinigen Koordinatensystem definieren, und umgekehrt kann man zu einem gegebenen Punktgitter ein solches Koordinatensystem konstruieren, indem man als Anfangspunkt O wählt und als Einheitsvektoren der x- und y-Achse $\mathfrak{p}_1$ und $\mathfrak{p}_2$ nimmt.

Ein Gitter gestattet eine unendliche Gruppe von Translationen in sich selbst, nämlich die durch die Vektoren $x_1\mathfrak{p}_1 + x_2\mathfrak{p}_2$ definierten. Diese Gruppe ist *Abel*sch und besitzt zwei Erzeugende $\mathfrak{p}_1$ und $\mathfrak{p}_2$. Es besteht nun die Frage, ob ein Gitter noch weitere Bewegungen in sich selbst besitzen kann. Hierzu genügt es, die Bewegungen, welche O ungeändert lassen, zu untersuchen, denn geht bei der Bewegung B der Punkt O in P über und bezeichnet T die Translation, welche O in P überführt, so ist auch BT^{-1} eine Bewegung des Gitters in sich, und diese läßt O ungeändert, d. h. sie ist eine *Drehung* des Gitters um O. Hierdurch bekommen wir völlige Übersicht über die Gruppe aller Bewegungen des Gitters: sie wird erzeugt durch die Gruppe der Translationen $\mathfrak{T}$ und die dazu teilerfremde der Drehungen, welche O ungeändert lassen. $\mathfrak{T}$ ist Normalteiler der ganzen Gruppe, $B^{-1}TB$ ist diejenige Translation, deren Vektor aus dem Vektor T durch die Drehung B hervorgeht.

Jedes ebene Gitter gestattet um seine Gitterpunkte eine Drehung von 180^0. Daher brauchen wir nur Drehungsgruppen von gerader Ordnung zu betrachten. Um zu untersuchen, welche Ordnungen für weitere Symmetrien noch in Frage kommen, nehmen wir einen Gitterpunkt P_1, dessen Distanz von O ein Minimum ist. Der Vektor von O nach P_1 ist dann ein kürzester Gittervektor. Beginnen wir mit einer Drehung von der Ordnung 4, so entstehen aus P_1 die weiteren Punkte P_2, P_3 und P_4. OP_1 und OP_2 erzeugen ein quadratisches Gitter, dem auch P_3 und P_4 angehören. Weitere Gitterpunkte können nicht vorhanden sein, denn ein solcher läge in einem Fundamentalquadrat und hätte daher mindestens von einer Ecke desselben eine kleinere Entfernung als OP_1. Es gibt daher, abgesehen von der Lage und der Größe, nur ein Gitter, das Drehungen von der Ordnung 4 gestattet, nämlich das quadratische. Genau so beweist man, daß es nur ein Gitter gibt, das Drehungen von 60^0, also von der Ordnung 6, gestattet, nämlich das durch Aneinanderreihen von gleichseitigen Dreiecken erzeugte.

Kein Gitter gestattet Drehungen von weniger als 60^0. Wir beweisen diesen Satz für die Ordnung 8. Es sei wieder P_1 ein nächster Gitterpunkt bei O. Alsdann entstehen aus ihm durch die Drehungen 7 weitere Gitterpunkte $P_2, P_3, \ldots, P_8$. Den Gittervektor $\overline{P_2P_3}$ setzen wir in P_1 an und erhalten einen von O verschiedenen Gitterpunkt im Inneren des Achteckes, der entgegen der Voraussetzung näher bei O liegt als P_1.

Außer den Drehungen müssen wir noch die Existenz von Symmetriegeraden behandeln, und auch hier können wir uns auf den Fall beschränken, wo die Gerade durch O geht. Diese ist alsdann immer eine Gittergerade, denn ist P ein Gitterpunkt außerhalb der Geraden und $\overline{P}$ sein symmetrischer Punkt, so tragen wir den Gittervektor OP von $\overline{P}$ aus ab und gelangen in einen Punkt auf der Symmetriegeraden. Da wir annehmen dürfen, daß OP nicht senkrecht steht zu dieser Geraden, so ist der neugefundene Punkt von O verschieden. Man findet so zwei verschiedene Gitter: das allgemeine rechteckige und das zentrierte rechteckige, welches durch Hinzufügung der Mittelpunkte der Rechtecke aus dem vorigen entsteht. Dieses letztere kann nach der Gestalt eines Fundamentalparallelogramms auch das rhombische Gitter genannt werden. Im Fall des quadratischen Gitters ist auch das zentrierte quadratisch. Das hexagonale Gitter ist ein spezielles rhombisches Gitter.

Die Bewegungen und Symmetrien, welche O festlassen, bilden eine endliche Gruppe, die ***Symmetriegruppe.*** Sie charakterisiert die makroskopischen Eigenschaften der Kristalle. Unsere 5 Gitter liefern 4 Symmetriegruppen, wenn wir von den Untergruppen absehen, denn das rechtwinklige und das rhombische Gitter besitzen dieselben Symmetrien.

§ 24. Die Raumgitter.

Raumgitter werden erzeugt durch drei Vektoren $\mathfrak{p}_1$, $\mathfrak{p}_2$ und $\mathfrak{p}_3$, deren Richtungen nicht derselben Ebene angehören, indem man sie von einem beliebigen Punkt aus positiv und negativ beliebig oft abträgt. Eine Ebene, die drei nicht in einer Geraden liegende Gitterpunkte enthält, heißt eine ***Gitterebene.*** Die in ihr liegenden Gitterpunkte des Gitters bilden ein ebenes Gitter. Wählt man die drei Vektoren $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$ als Einheitsstrecken von drei Koordinatenachsen mit dem Ursprung in O, so bilden die Gitterpunkte die Gesamtheit der Punkte mit ganzzahligen Koordinaten. Gitterebenen können dargestellt werden durch lineare Gleichungen mit ganzzahligen Koeffizienten, und umgekehrt liefert jede derartige Gleichung eine Gitterebene, sobald der größte gemeinschaftliche Teiler der Koeffizienten der drei Variablen gleich 1 ist. Dies sei im folgenden stets angenommen; diese Koeffizienten heißen alsdann die ***Indizes*** der Ebene.

Kennt man eine Gitterebene, so läßt sich das ganze Raumgitter durch Translation derselben erzeugen. Jede parallele Ebene durch einen Gitterpunkt ist wiederum Gitterebene und das darin enthaltene Gitter ist kongruent mit dem ursprünglichen. Wir betrachten die parallele Ebene durch O; ihre Gitterpunkte seien gegeben durch $x_1 \mathfrak{q}_1 + x_2 \mathfrak{q}_2$. Ferner sei P ein Gitterpunkt auf einer der beiden nächsten parallelen Gitterebenen, und $\mathfrak{q}_3$ bedeute den Vektor OP.

Alsdann bekommt man das ganze nächste Parallelgitter in der Gestalt $x_1 \mathfrak{q}_1 + x_2 \mathfrak{q}_2 + \mathfrak{q}_3$. Das darauf folgende parallele Gitter wird durch $x_1 \mathfrak{q}_1 + x_2 \mathfrak{q}_2 + 2\,\mathfrak{q}_3$ gegeben sein; denn gäbe es zwischen diesen beiden Ebenen noch einen weiteren Gitterpunkt, so hätten wir schon zu Beginn nicht die nächste parallele Gitterebene gewählt.

Jedes Raumgitter besitzt O als Symmetriezentrum, d. h. trägt man einen Gittervektor von O aus in umgekehrter Richtung ab, so gelangt man wieder in einen Gitterpunkt. Diese Operation der ***Spiegelung am Anfangspunkt*** ist im dreidimensionalen Raum keine Bewegung, sie kann erzeugt werden durch eine Drehung von 180^0 um eine beliebige durch O gehende Gerade und eine nachfolgende Spiegelung an der dazu senkrechten Ebene durch O. Nun sind alle Symmetrien von Gittern, die wir aufsuchen wollen, Bewegungen, oder Bewegungen verbunden mit Spiegelungen, und wir können uns daher beschränken auf die verschiedenen Bewegungsgruppen, da die Operationen zweiter Art von selbst mitfolgen durch das Symmetriezentrum.

Bekanntlich sind alle Bewegungen des Raumes, bei denen O festbleibt, Drehungen um eine Achse durch O. Wir beweisen nun den

Satz 61: *Die Ebene durch O senkrecht zu einer Drehachse ist eine Gitterebene.*

Beweis: Wenn die Drehung von der Ordnung 3 oder mehr ist, so ist der Satz ohne weiteres klar. Man nehme irgendeinen Gitterpunkt außerhalb der Drehachse und übe die Drehungen aus. Alsdann erhält man mindestens 3 Gitterpunkte, die nicht in einer Geraden liegen, dagegen in einer Ebene senkrecht zur Achse. Aber auch für eine Achse von der Ordnung 2 gilt der Satz. Es sei P ein beliebiger Gitterpunkt außerhalb der Achse und P_1 der Punkt, in den er durch die Drehung um 180^0 übergeht. Heftet man den Vektor $P_1 O$ an im Punkte P, so gelangt man in einen Gitterpunkt, der in der zur Achse senkrechten Ebene durch O liegt.

Durch diesen Satz ist es leicht, die Gitter mit besonderen Symmetrien zu konstruieren. Eine Drehachse durch O muß das ganze zu ihr senkrechte ebene Gitter in sich transformieren. Ihre Ordnung kann daher nur 2, 3, 4, 6 sein. Wir nennen solche Achsen ***Zweierachsen, Dreierachsen*** usw.; in der Bezeichnung der Kristallographie heißen sie ***Digyren, Trigyren, Tetragyren*** und ***Hexagyren.*** Eine solche Achse darf alle zu ihr senkrechten Ebenen nur in solchen Punkten durchstechen, welche die betreffende Drehung des ebenen Gitters zulassen.

Ein Gitter ohne besondere Symmetrien heißt ***triklin.*** Seine Gruppe besteht aus einem Symmetriezentrum und der Identität.

Ein Gitter mit einer Zweierachse heißt ***monoklin.*** Das zur Achse senkrechte ebene Gitter ist beliebig und die Achse kann in einen Gitterpunkt oder in den Mittelpunkt der Verbindungsstrecke zweier

Gitterpunkte einstechen. Danach erhalten wir *zwei Typen monokliner Gitter.* Man kann das ebene Gitter in der Richtung der Zweierachse parallel zu sich verschieben und in äquidistanten Punkten fixieren. Alsdann erhält man ein Gitter mit aufrechten Fundamentalparallelepipeden. Oder die Zweierachse trifft die Gitterebene abwechselnd in Gitterpunkten und in den oben erwähnten Mittelpunkten. Man erhält ein Gitter, das man sich aufgebaut denken kann aus aufrechten Parallelepipeden, die in ihrem Mittelpunkt einen weiteren Gitterpunkt enthalten.

Ein Gitter mit einer Viererachse heißt ***tetragonal.*** Die zur Achse senkrechte Ebene trägt ein quadratisches Gitter und kann daher von der Achse nur in Gitterpunkten oder in den Mittelpunkten der Quadrate durchstochen werden. Man erhält auch hier *zwei Gitter*, bestehend aus aufrechten Parallelepipeden mit quadratischem Querschnitt, die zentriert sind oder nicht.

Ein Gitter mit einer Sechserachse heißt ***hexagonal.*** Das zur Achse senkrechte Gitter ist hexagonal und kann von der Achse nur in einem Gitterpunkt durchstoßen werden. Es gibt daher nur einen Typus hexagonaler Gitter.

Eine Sechserachse ist gleichzeitig Dreierachse und das eben erwähnte Gitter gehört daher auch zu einer solchen. Daneben gibt es aber ein weiteres Gitter, das ***rhomboedrische***, das eine Dreierachse besitzt. Die zur Achse senkrechte Gitterebene muß ein hexagonales Gitter tragen, aber die Achse darf außer durch Gitterpunkte noch durch die Mittelpunkte der gleichseitigen Dreiecke gehen, aus denen das Gitter aufgebaut werden kann. Die Achse trifft nur jede dritte Gitterebene in einem Gitterpunkt, die beiden jeweils dazwischenliegenden Ebenen werden in Mittelpunkten von Dreiecken getroffen, die um 60^0 gegeneinander gedreht erscheinen.

Das ***rhombische*** Raumgitter besitzt drei aufeinander senkrechte Zweierachsen, die wir als Koordinatenachsen wählen. Jede Gitterebene durch eine dieser Achsen besitzt sie als Symmetriegerade und kann daher nur ein rechtwinkliges oder rhombisches Gitter tragen. Wenn die Koordinatenebenen rechteckige Gitter enthalten, so erhalten wir *zwei Gitter:* ein aus rechtwinkligen Quadern aufgebautes, die im Innern zentriert sind oder nicht. Im andern Fall nehmen wir an, daß die horizontale Basisebene rhombisch ist, und wir erhalten wiederum *zwei Gitter*, die man am besten von Quadern ausgehend beschreibt: Es wird das eine Gitter aus basiszentrierten, das andere aus allseitig flächenzentrierten Quadern aufgebaut.

Das ***kubische*** Gitter ist ein Spezialfall des vorigen und hat die Symmetrie des Würfels. Da hier die Koordinatenebenen gleichwertig sind, so gibt es nur drei Gitter, die sich aus einfachen oder innenzentrierten oder allseitig flächenzentrierten Würfeln aufbauen.

Eine nähere Betrachtung der Gitter zeigt, daß eine Dreier-, Vierer- und Sechserachse 3, 4 resp. 6 zu ihr senkrechte Zweierachsen bedingt. Dieser Satz läßt sich umkehren: Zwei Zweierachsen durch O, welche den Winkel α unter sich bilden, bedingen eine dazu senkrechte Achse, deren Drehwinkel 2α beträgt. Führt man nämlich die Drehung von 180^0 um die beiden Achsen hintereinander aus, so ist das Resultat gleichbedeutend mit der angegebenen Drehung um die senkrechte Achse.

Wir zeigen nun, daß nur die 14 Gitter vorkommen. Wenn nur Zweierachsen auftreten, so müssen sie einen Winkel von 90^0 miteinander bilden, und es ist nur der monokline und der rhombische Fall möglich. Wenn eine Dreierachse vorhanden ist und nicht der rhomboedrische Fall vorliegt, so muß es eine Zweierachse geben, die nicht senkrecht zu ihr steht. Durch die Drehungen von der Ordnung 3 geht diese in 2 neue Lagen über, an denen sich gleiche Achsen befinden müssen. Diese bilden unter sich Winkel, die kleiner als 120^0 sind. Sind sie 90^0, so haben wir eine Konfiguration, die im kubischen Fall vorliegt, nämlich die rechtwinkligen Koordinatenachsen und die Dreierachse, welche sie gleichwertig macht und zyklisch vertauscht. Ist der Winkel 60^0, so haben wir wieder eine Konfiguration der Oktaedergruppe, nämlich die Achsen durch die Mitten einer Seitenfläche des Oktaeders und der sie begrenzenden Kanten. In den Fällen von 45^0 und 30^0 werden wir auf Vierer- und Sechserachsen geführt.

Bei einer Viererachse kommen wir auf Zweierachsen, die einen Winkel von weniger als 90^0 bilden. Ist er 60^0, so haben wir eine Konfiguration des Oktaeders, ist er 45^0, so ist der Winkel, den eine dieser Zweierachsen mit der Viererachse bildet, die ja auch eine Zweierachse ist, kleiner als 45^0 und wir kommen zu Sechserachsen.

Bei einer Sechserachse kommen nur die Winkel 45^0 und 30^0 in Betracht. 45^0 ist ausgeschlossen, denn wenn wir nur die geraden Drehungen der Sechserachse nehmen, so kommen wir auf eine Dreierachse mit einem Winkel, der größer ist als 45^0, d. h. auf den kubischen Fall. Aber auch 30^0 ist ausgeschlossen, denn bezeichnen wir die Zweierachsen in der Reihenfolge, wie sie durch die Drehung entstehen, mit 1 bis 6, so müßten folgendes die Winkel zwischen ihnen sein:

$$\sphericalangle(1,2) = 30^0,\ \sphericalangle(1,3) = 45^0,\ \sphericalangle(1,4) = 60^0,\ \sphericalangle(1,5) = 45^0,$$
$$\sphericalangle(1,6) = 30^0,$$

und dies ist offenbar nicht möglich.

Die 7 Axenkonfigurationen, die wir gefunden haben, bilden die 7 ***Kristallsysteme***. Unter ihren Gruppen kommen zwei *umfassenste* vor, die hexagonale und kubische. Nun müssen wir die Untergruppen aufsuchen (vgl. auch § 27).

§ 25. Die Kristallklassen.

Nicht jeder Kristall besitzt die volle Gruppe aller Symmetrien seines Systems, sondern bloß eine Untergruppe. Wir haben gesehen, daß die einzelnen Gitter bereits durch Untergruppen bestimmt sind, ja wir haben sie sogar durch solche hergeleitet und erst nachträglich gefunden, daß sie noch weitere Symmetrien aufweisen. Die volle Gruppe ist jeweils das direkte Produkt der zugehörigen Bewegungsgruppe und einer Gruppe von der Ordnung 2, deren Elemente die Identität und das Symmetriezentrum sind. Diese Gruppen heißen die *Holoedrie* des betreffenden Systems. Normalteiler vom Index 2, z. B. die Bewegungsgruppen, heißen im allgemeinen *Hemiedrien,* solche vom Index 4 *Tetartoedrien.*

Wir gehen nun an die Aufzählung der sämtlichen Untergruppen. Jede von ihnen definiert eine bestimmte ***Kristallklasse,*** hierbei werden aber zwei Gruppen, welche dieselben Symmetrieelemente in derselben Konfiguration, aber in verschiedener Lage zum Gitter aufweisen, nicht als verschieden angesehen.

1. *Triklines System:* Die *Hemiedrie* besteht aus der Identität allein, die *Holoedrie* enthält außerdem noch das Symmetriezentrum.

2. *Monoklines System:* Die *Holoedrie* besteht aus E, einer Zweier achse, dem Symmetriezentrum und einer zur Achse senkrechten Symmetrieebene und bildet eine *Abel*sche Gruppe vom Typus (2, 2). Jedes der drei zuletzt genannten Elemente bestimmt mit E zusammen eine Untergruppe vom Index 2, aber die mittlere gehört ins trikline System, daher bleiben zwei noch übrig: $E +$ Symmetrieebene bildet die *Hemiedrie,* $E +$ Zweierachse die *Hemimorphie.*

3. *Rhombisches System.* Die *Holoedrie* ist *Abel*sch von der Ordnung 8 und vom Typus (2, 2, 2). Sie besitzt 7 Gruppen von der Ordnung 2, die jeweils aus E und einer der 3 Zweierachsen oder der 3 Symmetrieebenen oder schließlich dem Symmetriezentrum bestehen. Alle diese gehören bereits zu einem der früheren Systeme. Ferner gibt es 7 Untergruppen von der Ordnung 4. Von diesen bilden 3 die monokline Holoedrie, bezogen auf je eine der drei Achsen; diese fallen weg. Außer diesen gibt es drei Untergruppen, die aus E, einer Zweierachse und zwei durch sie hindurchgehenden Symmetrieebenen bestehen. Diese bilden die *rhombische Hemimorphie* Schließlich bleibt die Drehungsgruppe, welche E und 3 Zweierachsen enthält und *rhombische Hemiedrie* heißt.

4. *Rhomboedrisches System.* Die Bewegungsgruppe ist die Diedergruppe von der Ordnung 6. Die *Holoedrie* besitzt die Ordnung 12. Sie enthält einen Normalteiler vom Index 4, die *Tetartoedrie*, deren Faktorgruppe *Abel*sch und vom Typus (2, 2) ist. Es gibt also noch *drei Hemiedrien:* die *Paramorphie*, welche außer der Dreierachse

noch das Symmetriezentrum und damit noch zwei Drehspiegelachsen enthält, die *Hemimorphie*, welche außer der Achse noch Symmetrieebenen durch dieselbe besitzt, und schließlich die *Enantiomorphie*, welche die sämtlichen 6 Drehungen enthält.

5. *Hexagonales System.* Hier bildet die Sechserachse die *Tetartoedrie* und ist Normalteiler der Holoedrie vom Index 4. Genau wie im vorherigen Fall treten *drei Hemiedrien* auf, sie werden gleich bezeichnet wie vorher. Freilich treten hier noch weitere Untergruppen auf, die nachher untersucht werden sollen.

6. *Tetragonales System.* Wie das vorige.

7. *Kubisches System.* Hier bildet die *Tetraedergruppe* die *Tetartoedrie*. Sie ist genau wie die drei vorigen in der Holoedrie enthalten. Die *Enantiomorphie* (reine Drehungsgruppe) ist hier offenbar die *Oktaedergruppe*.

Während wir in 1 bis 4 sämtliche Untergruppen kennen, müssen wir noch die übrigen Gruppen untersuchen. Wir beginnen mit dem hexagonalen System. Die Gruppe hat die Ordnung 24, ihre *Sylow*gruppe von der Ordnung 8 bildet das rhombische System, da die Sechserachse zugleich Zweierachse ist, sie liefert also keine neue Kristallklasse. Jede andere Untergruppe enthält die Untergruppe von der Ordnung 3, und diese ist stets Normalteiler, denn es gibt nur eine Dreierachse. Der Index dieses Normalteilers unter der Holoedrie ist 8, die Faktorgruppe ist *Abel*sch und vom Typus (2, 2, 2). Es gibt also 7 Untergruppen von der Ordnung 6 und ebensoviel von der Ordnung 12. Von der Ordnung 6 ist die Sechserachse, ferner die drei Hemiedrien des rhomboedrischen Systems. Von den letzteren zählen aber die Hemimorphie und die Enantiomorphie doppelt, da wir aus den 6 Zweierachsen des hexagonalen Systems auf zwei Arten drei auswählen können, um die Enantiomorphie zu erhalten. Ebenso können wir aus den 6 Symmetrieebenen durch die Sechserachse auf zwei Arten drei auswählen, welche die Hemimorphie ergeben. Die beiden Konfigurationen ergeben sich jeweils auseinander durch Drehung von 60^0 um die Dreierachse. Es bleibt also noch eine Untergruppe übrig und diese besteht aus der Dreierachse und einer horizontalen Symmetrieebene, die also zur Achse senkrecht steht. Diese Klasse heißt die *trigonale Paramorphie*. Sie gehört nicht zum rhomboedrischen Gitter, denn dieses besitzt keine horizontale Symmetrieebene, sondern nur zum hexagonalen, trotzdem wird sie meist dem rhomboedrischen System zugezählt. Unter den Untergruppen von der Ordnung 12 kommen 5 bereits unter den früher aufgezählten vor, und es bleiben zwei übrig, die aber nur als eine zählen. Es ist dies die Dreierachse mit drei dazu senkrechten Zweierachsen, also die rhomboedrische Enantiomorphie, der ferner noch eine horizontale Symmetrieebene hinzugefügt ist. Diese Klasse heißt die *trigonale Holoedrie*.

Ähnlich liegen die Verhältnisse im *tetragonalen System.* Nimmt man hier zu der Viererachse das Symmetriezentrum, so erhält man eine *Abel*sche Gruppe vom Typus (4, 2). Diese besitzt außer der Achse noch eine Operation von der Ordnung 4, nämlich die Drehspiegelachse. Die zugehörige Klasse heißt *tetragonale Tetartoedrie II. Art.* Auch diese Gruppe ist Normalteiler der Holoedrie und in drei Normalteilern von der Ordnung 8 enthalten, von denen wir erst einen haben, nämlich die tetragonale Paramorphie. Die beiden anderen sind gleich beschaffen und entstehen durch Hinzufügen zweier Zweierachsen und zweier Symmetrieebenen durch die Drehspiegelachse, welche die Winkel zwischen den Zweierachsen halbieren. Diese Klasse heißt die *tetragonale Hemiedrie II. Art.*

Das kubische System liefert keine weiteren Klassen mehr. Die Sylowgruppen von der Ordnung 16 sind tetragonale Holoedrien, die Untergruppen mit Dreierachsen gehören in das kubische oder das rhomboedrische System.

Es ist bemerkenswert, daß bereits so einfache Gruppen, wie die drei zuletzt behandelten, eine große Mannigfaltigkeit von Untergruppen und eine äußerst komplizierte Struktur aufweisen. Sie sind darum besonders lehrreich, und gerade ein Vergleich des hexagonalen Falles mit dem tetragonalen wird die tiefere Erkenntnis des Baues von Gruppen aufs nachhaltigste fördern.

7. Kapitel.

Permutationsgruppen.

§ 26. Zerlegung der Permutationen in Zyklen[1].

Die Aufgabe dieses Kapitels bildet ein eingehenderes Studium der durch Permutationen dargestellten Gruppen. Sie sind besonders wichtig, weil durch sie gewisse, für alle Anwendungen fundamentale Gruppen in einfachster Weise behandelt werden können. Aber ihre Bedeutung reicht noch viel weiter, denn wie bereits in § 4 gezeigt worden ist, besitzt jede Gruppe eine Darstellung durch Permutationen, und wir werden später sehen, daß sich jede Eigenschaft der Permutationsgruppen so aussprechen läßt, daß sie als Eigenschaft einer abstrakten Gruppe erscheint.

Wir behandeln zum Anfang eine neue Darstellung der Permutationen und beginnen mit einem Beispiel. In der Permutation

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

[1] Zur Geschichte der Permutationsgruppen vgl. § 60.

wird 1 ersetzt durch 2, 2 durch 5, 5 durch 4, 4 durch 3 und 3 durch 1. Dies kann durch folgendes Symbol bezeichnet werden (1, 2, 5, 4, 3), in dem wir darunter eine *zyklische Vertauschung* oder einen ***Zyklus*** der fünf Variablen in der Klammer verstehen dergestalt, daß jede Zahl durch die folgende, die letzte aber durch die erste ersetzt wird. Offenbar bewirkt die angegebene Permutation dieselbe Vertauschung wie das obige Klammersymbol, aber das letztere ist viel übersichtlicher als die bisher angewandte Bezeichnung.

So sind auch die Potenzen der Permutation leicht aus dem Klammersymbol abzulesen. Um z. B. das Quadrat zu bilden, hat man jeweils um 2 Stellen nach rechts zu gehen und allgemein für die n-te Potenz in zyklischer Weise um n Stellen nach rechts. Man sieht sofort, daß die fünfte Potenz unserer Permutation die identische ergibt.

Als ein weiteres Beispiel betrachten wir die Permutation

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

Hier geht 1 über in 5, 5 in 3 und 3 in 1, so daß hiermit bereits ein Zyklus geschlossen ist. 2 geht über in 4 und 4 in 2. In unserm Fall ist also die Permutation das Produkt der zwei Zyklen (1, 5, 3)(2, 4), von 3 resp. 2 Variabeln. Die Ordnung dieser Permutation muß sowohl durch 3 als durch 2 teilbar sein und ist, wie man sich leicht überzeugt, gleich 6.

Man sieht nun sofort, daß sich jede Permutation in der angegebenen Weise in ein Produkt von Zyklen zerlegen läßt, wobei jede Variable nur einmal vorkommt. Bleibt eine Variable ungeändert bei der Permutation, so gibt sie Anlaß zu einem Zyklus von einem einzigen Glied, und wir setzen fest, daß solche Zyklen weggelassen werden. So ist z. B.

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

Satz 62: *Die Ordnung einer Permutation ist gleich dem kleinsten gemeinsamen Vielfachen der Ordnungen der einzelnen Zyklen, und die Ordnung eines Zyklus ist gleich der Anzahl der Variablen, die darin auftreten.*

Sieht man von der Bedingung ab, daß 2 Zyklen keine gemeinsamen Variablen enthalten dürfen, so läßt sich selbstverständlich jede Permutation auf beliebig viele Weise als Produkt von Zyklen darstellen, insbesondere als Produkt von ***Transpositionen.*** Hierunter verstehen wir die Vertauschung zweier aufeinander folgenden Variablen. Der Zyklus $(1, 2, 3, \ldots, n)$ kann offenbar ersetzt werden durch die aufeinander folgenden Transpositionen $(1, 2)$, $(1, 3)$, $(1, 4)$, $\ldots$, $(1, n)$. Es ist also:

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

und in ähnlicher Weise lassen sich die übrigen Zyklen der Permutation behandeln. Wir merken noch an, daß die Anzahl der Transpositionen bei Zyklen gerader Ordnung eine ungerade, im andern Fall eine gerade ist.

Der zu einem Zyklus inverse Zyklus wird erhalten, indem man die Variablen in umgekehrter Reihenfolge aufschreibt; die zu einem Produkt von Zyklen inverse Operation erhält man, indem man die Folge der Zyklen umkehrt und außerdem jeden einzelnen Zyklus durch den inversen ersetzt. So ist z. B.

$$((1,\ 2,\ 3)(1,\ 2,\ 4))^{-1} = (4,\ 2,\ 1)(3,\ 2,\ 1).$$

Nun gilt der

Satz 63: *Die Anzahl der Transpositionen, aus denen eine Permutation gebildet werden kann, ist stets gerade oder stets ungerade.*

Beweis: Man bildet das Differenzenprodukt

$$\left.\begin{array}{r}(x_1 - x_2)(x_1 - x_3)\dots(x_1 - x_n)\\ (x_2 - x_3)\dots(x_2 - x_n)\\ \dots\dots\dots\dots\dots\dots\\ (x_{n-1} - x_n)\end{array}\right\} = D.$$

Vertauscht man hier 1 und 2, so ändert D das Vorzeichen, und allgemein überzeugt man sich leicht davon, daß jede Vertauschung zweier Indizes dasselbe bewirkt. Eine gerade Anzahl von Vertauschungen läßt daher D ungeändert, während eine ungerade Anzahl D in $-D$ überführt.

Eine Permutation wird stets entweder D unverändert lassen oder D in $-D$ überführen. Im ersten Fall kann sie sich nur aus einer geraden Anzahl, im zweiten Fall nur aus einer ungeraden Anzahl von Transpositionen zusammensetzen lassen.

Sind S und T zwei Permutationen, so ist es eine für das Folgende wichtige Aufgabe, die Permutation $T^{-1}ST$ zu bilden. Wir bezeichnen

$$S = \begin{pmatrix}1,\ 2,\ \dots,\ n\\ i_1,\ i_2,\ \dots,\ i_n\end{pmatrix} \qquad T = \begin{pmatrix}1,\ 2,\ \dots,\ n\\ k_1,\ k_2,\ \dots,\ k_n\end{pmatrix} = \begin{pmatrix}i_1,\ i_2,\ \dots,\ i_n\\ l_1,\ l_2,\ \dots,\ l_n\end{pmatrix} \text{ vgl. § 4}$$

und

$$ST = \begin{pmatrix}1,\ 2,\ \dots,\ n\\ l_1,\ l_2,\ \dots,\ l_n\end{pmatrix},$$

dann wird

$$T^{-1}ST = \begin{pmatrix}k_1,\ k_2,\ \dots,\ k_n\\ l_1,\ l_2,\ \dots,\ l_n\end{pmatrix}.$$

Hieraus folgt der

Satz 64: *Eine Permutation S wird transformiert durch die Permutation T, indem man in den beiden Zeilen der Permutation S die Permutation T ausführt.*

In der Bezeichnungsweise durch Zyklen wird das Resultat noch einfacher. Man überzeugt sich leicht, daß ein Zyklus durch die Permutation T transformiert wird, indem man die Variablen des Zyklus der Permutation unterwirft. So ergibt z. B. das Produkt der Zyklen $(1, 2, 3)(2, 3, 4)$ transformiert durch die Permutation $\begin{pmatrix}1, 2, 3, 4\\2, 1, 4, 3\end{pmatrix}$ das folgende Produkt $(2, 1, 4)(1, 4, 3)$, denn ein Produkt wird transformiert, indem man die einzelnen Faktoren transformiert.

Umgekehrt sind zwei Permutationen, deren Zerlegung in Zyklen mit verschiedenen Variablen eine gleichartige ist, d. h. jeweils aus gleichviel Zyklen derselben Ordnung besteht, durch Transformation ineinander überführbar. Z. B. $(1, 2, 3, 4, 5)$ und $(2, 4, 1, 5, 3)$ sind ineinander transformierbar durch die Permutation $\begin{pmatrix}1, 2, 3, 4, 5\\2, 4, 1, 5, 3\end{pmatrix}$ resp. die dazu Inverse.

Zum Schluß dieses Paragraphen seien noch ein paar spezielle Formeln angemerkt. *Zwei Zyklen mit einer einzigen gemeinsamen Variablen ergeben multipliziert wiederum einen Zyklus:*

$$(x_1, \ldots, x_n)(x_1, y_2, \ldots, y_m) = (x_1, \ldots, x_n, y_2, y_3, \ldots, y_m).$$

Die Ordnung des zusammengesetzten Zyklus ist gleich der um 1 verminderten Summe der Ordnungen der beiden Faktoren.

Das Produkt zweier Transpositionen läßt sich durch dreigliedrige Zyklen erzeugen. So ist

$$(ab)(cd) = (abd)(acd) \quad \text{und} \quad (ab)(ac) = (abc).$$

Infolgedessen lassen sich alle geraden Permutationen auch als Produkte dreigliedriger Zyklen darstellen, und umgekehrt ist ein solches Produkt stets eine gerade Permutation.

§ 27. Die symmetrische und alternierende Permutationsgruppe.

Die sämtlichen Permutationen von n Variablen bilden eine Gruppe von der Ordnung $n!$, welche die ***symmetrische Gruppe*** von n Variablen genannt wird. In dieser Gruppe sind 2 Permutationen mit gleichartiger Zerlegung in Zyklen von verschiedenen Variablen konjugiert.

Besteht die Permutation aus a Zyklen von der Ordnung 1, b Zyklen von der Ordnung 2, c von der Ordnung 3 usw., so daß $n = a + 2b + 3c + \ldots$, so gibt es im ganzen, wie eine leichte Rechnung zeigt,

$$\frac{n!}{1^a a!\, 2^b b!\, 3^c c! \ldots}$$

Permutationen von diesem Typus, wobei $0! = 1$ zu setzen ist. Diese Zahl stellt daher auch die Anzahl der Permutationen in der betreffen-

den Klasse dar. Die Anzahl der Klassen in der symmetrischen Gruppe ist gleich der Anzahl der Lösungen der Gleichung $n = a + 2b + 3c + \ldots$ in ganzen Zahlen $\geqq 0$. Für $n = 2$ erhält man die Gruppe von der Ordnung 2; $n = 3$ liefert die Diedergruppe von der Ordnung 6; $n = 4$ ergibt die Oktaedergruppe von der Ordnung 24, denn diese ist ja bestimmt durch die Vertauschungen der 4 Diagonalen, welche die Mittelpunkte gegenüberliegender Seiten des Oktaeders verbinden. Eine weitere Besprechung folgt unten und wir gehen über zur

Definition: Die *alternierende Gruppe* von n Variablen besteht aus den sämtlichen geraden Permutationen der n Variablen. Diese bilden eine Untergruppe vom Index 2 der symmetrischen Gruppe, denn ist $\mathfrak{A}$ die alternierende Gruppe und S irgendeine ungerade Permutation, so stellt $\mathfrak{A}S$ alle ungeraden Permutationen dar. $\mathfrak{A}$ ist ferner Normalteiler der symmetrischen Gruppe, denn mit T ist auch $S^{-1}TS$ eine gerade Permutation.

Die alternierende Gruppe von 3 Variablen ist zyklisch und von der Ordnung 3. Im Falle von 4 Variablen a, b, c, d besitzt sie die Ordnung 12. Wir behaupten nun, daß diese Gruppe einen Normalteiler von der Ordnung 4 besitzt. In der Tat bilden die 3 Permutationen, welche die 4 Variablen zu je zweien vertauschen, zusammen mit der identischen eine Untergruppe:

$$E,\ A = (a,b)(c,d),\ B = (a,c)(b,d),\ C = (a,d)(b,c)$$

mit den Relationen $AB = BA = C$; sie ist *Abel*sch und vom Typus (2, 2), also eine Vierergruppe. Daß sie Normalteiler ist, folgt daraus, daß sie die sämtlichen Permutationen von dem betreffenden Typus enthält. Die Kompositionsreihe der symmetrischen Gruppe von vier Variablen besteht daher aus den Gruppen $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, E, wobei $\mathfrak{A}$ die alternierende Gruppe ist, $\mathfrak{B}$ die eben aufgestellte *Abel*sche Gruppe von der Ordnung 4 und $\mathfrak{C}$ eine ihrer drei Untergruppen von der Ordnung 2. $\mathfrak{A}$ und $\mathfrak{B}$ sind Normalteiler der symmetrischen Gruppe, $\mathfrak{C}$ dagegen nicht. Weiterhin gilt nun der wichtige

Satz 65[1]**:** *Die alternierende Gruppe von n Variablen ist einfach, sobald n größer als 4 ist.*

Beweis: Ein Normalteiler der alternierenden Gruppe, der einen dreigliedrigen Zyklus (a, b, c) enthält, enthält alle weiteren dreigliedrigen Zyklen und stimmt infolgedessen mit der alternierenden Gruppe überein. Denn da mindestens 5 Variable zur Verfügung stehen, so kann man stets eine *gerade* Permutation angeben, welche die 3 Variablen (a, b, c) in drei beliebig gegebene Variable (a_1, b_1, c_1) überführt. Durch diese Permutation wird aber der Zyklus (a, b, c) in den Zyklus (a_1, b_1, c_1) transformiert. Nun sei eine beliebige Permutation

[1]) *Galois, E.:* Oeuvres, S. 26.

des Normalteilers in folgender Weise durch Zyklen dargestellt: $S = (a_1, \ldots, a_r) \ldots (c_1, \ldots, c_s)$ und wir machen die Voraussetzung, daß $s \geqq 3$ sei, dann gehört auch

$$T = (a_1, \ldots, a_r) \ldots (c_1, \ldots, c_{s-3}, c_{s-1}, c_s, c_{s-2})$$

zum Normalteiler, denn S geht in T über, indem man die Variablen (c_{s-2}, c_{s-1}, c_s) zyklisch vertauscht, was eine gerade Permutation ist. Der Normalteiler enthält also auch ST^{-1}, und man findet leicht, daß dies der dreigliedrige Zyklus (c_{s-3}, c_s, c_{s-2}) ist, womit nach dem Vorhergehenden der Satz für alle Untergruppen bewiesen ist, die Permutationen von höherer als zweiter Ordnung enthalten.

Wenn der Normalteiler die Permutation $(a, b)(c, d)$ enthält, so muß er auch $(b, e)(c, d)$ enthalten, wobei e irgendeine fünfte Variable, die ja vorhanden ist, darstellt, und das Produkt dieser beiden ist wiederum ein dreigliedriger Zyklus, nämlich (a, e, b). Falls die Permutation nicht bloß aus 2 Vertauschungen besteht, so müssen es mindestens 4 sein, z. B. $(a_1, a_2)(b_1, b_2)(c_1, c_2)(d_1, d_2)$, alsdann ist auch die folgende Permutation im Normalteiler enthalten $(a_1, a_2)(b_1, c_1)(b_2, d_1)(c_2, d_2)$. Das Produkt dieser beiden ergibt eine Permutation von der Ordnung 3, nämlich $(b_1, d_1, c_2)(b_2, c_1, d_2)$, womit wir auf den früheren Fall zurückgeführt sind. Wir haben hierbei die übrigen Vertauschungen, welche allenfalls zur Permutation gehören, weggelassen, da sie in beiden Permutationen gleich bleiben sollen und sich daher bei der Multiplikation aufheben.

§ 28. Transitive und intransitive Permutationsgruppen.

Von jetzt an sollen die Variablen einer Permutationsgruppe auch als solche bezeichnet werden, indem wir statt $1, 2, \ldots, n$ schreiben: $x_1, x_2, \ldots, x_n$. n heißt der ***Grad*** der Gruppe.

Indem wir nun von einer Variablen, etwa x_1 ausgehen, untersuchen wir, in welche Variablen x_1 durch die verschiedenen Permutationen übergeführt wird. Da die identische Permutation in jeder Permutationsgruppe enthalten ist, so kommt darunter x_1 selber vor. Durch Einführung einer geeigneten Bezeichnungsweise dürfen wir annehmen, daß die übrigen Variablen $x_2, \ldots, x_r$ sind. Wir behaupten nun, daß diese r Variablen bei allen Permutationen der Gruppe nur unter sich vertauscht werden. Es möge nämlich bei der Permutation S die Variable x_i in x_k übergeführt werden, wobei i eine Zahl zwischen 1 und r bedeutet. Ist dann T eine Permutation, die x_1 in x_i überführt, so wird TS einerseits zur Permutationsgruppe gehören, andererseits aber auch x_1 in x_k überführen. Nach der Voraussetzung folgt nun, daß k ebenfalls ein Index zwischen 1 und r ist. Sind ferner i und k zwei Indizes zwischen 1 und r und führen S resp. T die Variable x_1 in x_i resp. x_k

über, so führt $S^{-1}T$ die Variable x_i in x_k über. Man sieht sonach, daß durch irgend eine Variable x_i die zugehörigen Variablen x_1 bis x_r eindeutig bestimmt sind und man nennt x_1 bis x_r *durch die Permutationsgruppe* ***transitiv verbundene Variable.*** Eine Variable außerhalb von $x_1, \ldots, x_r$ wird wiederum einem transitiven System angehören, das durch eine beliebige unter seinen Variablen vollständig bestimmt ist, und das System der n Variablen zerfällt somit in eine Anzahl transitiver Teilsysteme. Eine Permutationsgruppe, bei der mehr als ein transitives System vorkommt, heißt eine ***intransitive Permutationsgruppe.*** Betrachtet man nur die Variablen eines transitiven Teilsystems, so bilden ihre durch die Gruppe hervorgerufenen Permutationen eine mit der Gesamtgruppe isomorphe Gruppe. Diejenigen Permutationen, welche diese Variablen ungeändert lassen, bilden also einen Normalteiler der ganzen Gruppe.

Als Beispiel geben wir die zyklische Gruppe von der Ordnung 6 in fünf Variablen:

$$(x_1, x_2, x_3)\,(x_4, x_5).$$

Diese Gruppe ist intransitiv, der Normalteiler, der die drei ersten Variablen ungeändert läßt, ist von der Ordnung 2, derjenige, der x_4 und x_5 nicht ändert, von der Ordnung 3.

Es genügt, die transitiven Permutationsgruppen zu untersuchen, da sich die übrigen aus jenen zusammensetzen lassen.

Satz 66: *In einer transitiven Permutationsgruppe von n Variablen bilden diejenigen Permutationen, die x_1 resp. x_2 usw. ungeändert lassen, ein System von n konjugierten Untergruppen vom Index n unter der ganzen Gruppe.*

Beweis: Daß die Permutationen, die etwa x_1 ungeändert lassen, eine Untergruppe $\mathfrak{H}$ bilden, ist klar; sind ferner T und S zwei Permutationen, die beide x_1 in x_i überführen, so gehört ersichtlich ST^{-1} zu $\mathfrak{H}$, d. h. S und T gehören derselben Nebengruppe von $\mathfrak{H}$ an. Hiernach zerfällt die ganze Gruppe genau in n Nebengruppen von $\mathfrak{H}$. Ist nun $\mathfrak{H}'$ diejenige Gruppe, die x_i ungeändert läßt und T eine Permutation, die x_1 in x_i überführt, so wird $T^{-1}\mathfrak{H}T$ eine Untergruppe sein, die x_i ungeändert läßt; und da ihre Ordnung dieselbe ist wie diejenige von $\mathfrak{H}'$, so wird $\mathfrak{H}' = T^{-1}\mathfrak{H}T$.

Nach der Definition ist $\mathfrak{H}$ eine intransitive Permutationsgruppe, indem ja x_1 für sich ein transitives System bildet. Wir müssen nun untersuchen, was eintritt, wenn $\mathfrak{H}$ in den übrigen Variablen transitiv ist.

Definition: Eine Permutationsgruppe $\mathfrak{G}$ heißt ***r-fach transitiv,*** wenn sie Permutationen enthält, die $x_1, \ldots, x_r$ in jedes System von r Variablen aus $x_1, \ldots, x_n$ überführen.

Aus dieser Definition folgt ohne weiteres, wie oben, daß in der Gruppe $\mathfrak{G}$ Permutationen auftreten, welche ein beliebiges System

von r aus den n Variablen in ein beliebiges derartiges System überführen. Diejenigen Permutationen, welche $x_1, \ldots, x_r$ in sich selbst überführen, bilden eine Untergruppe $\mathfrak{H}$, und diejenigen, welche diese Variablen in ein und dasselbe System überführen, bilden eine Nebengruppe von $\mathfrak{H}$. Der Index von $\mathfrak{H}$ ist also gleich der Anzahl der möglichen Systeme von r Variablen, in die $x_1, \ldots, x_r$ übergeführt werden kann, und diese Anzahl ist gleich: $n(n-1)\ldots(n-r+1)$. Hieraus folgt der

Satz 67: *Die Ordnung einer r-fach transitiven Gruppe vom Grade n ist gleich $n(n-1)\ldots(n-r+1)d$, wobei d ein Teiler von $(n-r)!$ ist.*

Denn d ist die Ordnung der Untergruppe $\mathfrak{H}$, und $\mathfrak{H}$ vertauscht $n-r$ Variable.

Wir betrachten nun speziell die zweifach transitiven Gruppen. Eine solche kann auch als transitive Gruppe charakterisiert werden, bei welcher die Untergruppe, die x_1 ungeändert läßt, in den übrigen Variablen transitiv ist. Denn sie muß Permutationen enthalten, die x_1, x_2 in ein beliebiges Paar x_1, x_i $(i = 2, \ldots, n)$ überführt; daraus folgt nun leicht, daß auch ein beliebiges Paar von Variablen x_i, x_k in x_i, x_l übergeführt werden kann, wobei $l \neq i$. Da die Gruppe transitiv ist, so gibt es jedenfalls eine Permutation, die x_1 in x_i überführt und x_2 möge dabei in x_k übergehen; durch Zusammensetzung mit einer geeigneten aus den vorhin angegebenen Permutationen kann man nun erreichen, daß k sowie i einem beliebigen Index gleich wird, womit bewiesen ist, daß die Gruppe zweifach transitiv ist.

§ 29. Darstellung von Gruppen durch Permutationen.

Bereits in § 4 haben wir den Begriff der *Darstellung* einer abstrakten Gruppe eingeführt. Es ist vorteilhaft, ihn etwas zu erweitern.

Eine Permutationsgruppe stellt die abstrakte Gruppe $\mathfrak{G}$ dar, wenn jedem Element der letzteren eine und nur eine Permutation zugeordnet ist und umgekehrt jeder Permutation mindestens ein Element, dergestalt, daß dem Produkt zweier Elemente auch das Produkt der zugeordneten Permutationen zugeordnet ist. Die Permutationsgruppe ist also *isomorph* mit der abstrakten Gruppe. Im folgenden wird die Aufgabe gelöst werden, alle Darstellungen einer abstrakten Gruppe durch transitive Permutationsgruppen zu finden.

Ist $\mathfrak{H}$ irgendeine Untergruppe der abstrakten Gruppe $\mathfrak{G}$ vom Index n und ist, in rechtsseitige Nebengruppen zerlegt

$$\mathfrak{G} = \mathfrak{H} + \mathfrak{H}T_2 + \ldots + \mathfrak{H}T_n,$$

so läßt sich in folgender Weise eine Permutationsgruppe von n Variablen definieren, welche mit $\mathfrak{G}$ isomorph ist: Man multipliziere die n Nebengruppen $\mathfrak{H}, \mathfrak{H}T_2, \ldots, \mathfrak{H}T_n$ rechts mit dem beliebigen Element S

aus $\mathfrak{G}$. Hierdurch erfahren sie eine Permutation und diese bezeichnen wir als die Darstellung des abstrakten Elementes S. Man sieht sofort, daß man auf diese Weise eine Darstellung von $\mathfrak{G}$ erhält, wenn man die n Nebengruppen als zu permutierende Variable betrachtet. Es ist nun von Wichtigkeit zu untersuchen, welche der Nebengruppen durch S in sich selbst übergeführt werden. Wenn das z. B. für $\mathfrak{H}$ der Fall ist, so muß die Beziehung gelten $\mathfrak{H} S = \mathfrak{H}$, d. h. S muß in der Untergruppe $\mathfrak{H}$ liegen und umgekehrt, wenn dies der Fall ist, so wird $\mathfrak{H}$ ungeändert bleiben. $\mathfrak{H} T$ bleibt ungeändert, wenn $\mathfrak{H} T S = \mathfrak{H} T$ oder $T^{-1}\mathfrak{H} T \cdot S = T^{-1}\mathfrak{H} T$, d. h. wenn S in der zu $\mathfrak{H}$ konjugierten Untergruppe $T^{-1}\mathfrak{H} T$ liegt.

Hiernach läßt die zu S gehörige Permutation genau so viele „Variable", nämlich Nebengruppen, ungeändert, als die Anzahl der mit $\mathfrak{H}$ konjugierten Untergruppen beträgt, die S enthalten. Die identische Permutation wird von allen denjenigen Elementen S erzeugt, die in allen mit $\mathfrak{H}$ konjugierten Untergruppen enthalten sind. Die Gesamtheit dieser Elemente bildet einen Normalteiler der ganzen Gruppe $\mathfrak{G}$ und umgekehrt ist jeder Normalteiler von $\mathfrak{G}$, der in $\mathfrak{H}$ enthalten ist, auch in den mit $\mathfrak{H}$ konjugierten Untergruppen enthalten. Bezeichnet $\mathfrak{N}$ den größten Normalteiler von $\mathfrak{G}$, der in $\mathfrak{H}$ enthalten ist, so entspricht seinen Elementen und nur diesen die identische Permutation, und die durch $\mathfrak{H}$ erzeugte Permutationsgruppe ist also homomorph mit der Faktorgruppe $\mathfrak{G}/\mathfrak{N}$. Nachdem das festgestellt ist, können wir leicht die wichtige Tatsache erweisen, daß wir auf diesem Weg alle transitiven Darstellungen der Gruppe erhalten, so daß also jede transitive Permutationsgruppe durch eine Untergruppe der durch sie dargestellten abstrakten Gruppe ***erzeugt*** werden kann.

Es sei nämlich $\mathfrak{G}$ die Permutationsgruppe und $\mathfrak{H}$ diejenige Untergruppe, die x_1 ungeändert läßt, ferner sei

$$\mathfrak{G} = \mathfrak{H} + \mathfrak{H} T_2 + \ldots + \mathfrak{H} T_n,$$

wobei $\mathfrak{H} T_i$ diejenige Nebengruppe bedeutet, deren Permutationen x_1 in x_i überführen. Nun möge die beliebige Permutation S unter anderem die Variable x_k in die Variable x_l überführen. Wir behaupten, daß die Beziehung gilt:

$$\mathfrak{H} T_k S = \mathfrak{H} T_l.$$

Zum Beweis bedenken wir, daß $T_k S$ die Variable x_1 in x_l überführt und somit eine Permutation aus $\mathfrak{H} T_l$ ist, etwa $H T_l$. Nun wird $\mathfrak{H} T_k S = \mathfrak{H} H T_l = \mathfrak{H} T_l$, womit die Behauptung erwiesen ist. Damit ist bewiesen, daß die mit S bezeichnete Permutation der Variablen $x_1, \ldots, x_n$ identisch ist mit der Permutation der Nebengruppen von $\mathfrak{H}$, die durch rechtsseitige Multiplikation mit S entsteht. Wir sprechen die gefundenen Resultate in folgendem Satz aus:

Satz 68: *Man erhält jede Darstellung einer Gruppe durch transitive Permutationsgruppen, indem man irgendeine Untergruppe $\mathfrak{H}$ und ihre Nebengruppen rechtsseitig mit den Elementen der Gruppe multipliziert; ist irgendeine Permutationsgruppe gegeben und $\mathfrak{H}$ diejenige Untergruppe, die eine der Variablen ungeändert läßt, so ist die durch $\mathfrak{H}$ erzeugte Permutationsgruppe identisch mit der gegebenen Permutationsgruppe, bei geeigneter Zuordnung der Nebengruppen zu den Variablen der Permutationsgruppe.*

Die schon früher angegebene Darstellung einer Gruppe von der Ordnung g durch g Variable, welche aus der Gruppentafel entspringt, ist offenbar in unserer allgemeinen Aufstellung enthalten, wenn man für $\mathfrak{H}$ die Einheitsgruppe E wählt. Einige scheinbar andere Methoden, aus abstrakten Gruppen Permutationsgruppen zu bilden, seien hier noch besprochen. Wählt man statt rechtsseitiger Nebengruppen linksseitige, $\mathfrak{G} = \mathfrak{H} + U_2\mathfrak{H} + \ldots + U_n\mathfrak{H}$, so erhält man eine Darstellung, indem man dem Element S die durch linksseitige Multiplikation mit S^{-1} hervorgerufene Permutation dieser Nebengruppen zuordnet. In der Tat entspricht

$$S \text{ die Permutation: } \begin{pmatrix} \mathfrak{H}, & U_2\mathfrak{H}, \ldots, & U_n\mathfrak{H} \\ S^{-1}\mathfrak{H}, & S^{-1}U_2\mathfrak{H}, \ldots, & S^{-1}U_n\mathfrak{H} \end{pmatrix}$$

$$T: \begin{pmatrix} \mathfrak{H}, & U_2\mathfrak{H}, \ldots, & U_n\mathfrak{H} \\ T^{-1}\mathfrak{H}, & T^{-1}U_2\mathfrak{H}, \ldots, & T^{-1}U_n\mathfrak{H} \end{pmatrix}$$

und

$$ST: \begin{pmatrix} \mathfrak{H}, & U_2\mathfrak{H}, \ldots, & U_n\mathfrak{H} \\ T^{-1}S^{-1}\mathfrak{H}, & T^{-1}S^{-1}U_2\mathfrak{H}, \ldots, & T^{-1}S^{-1}U_n\mathfrak{H} \end{pmatrix}.$$

Da sich nun aber die durch T hervorgerufene Permutation auch so schreiben läßt:

$$T: \begin{pmatrix} S^{-1}\mathfrak{H}, & S^{-1}U_2\mathfrak{H}, \ldots, & S^{-1}U_n\mathfrak{H} \\ T^{-1}S^{-1}\mathfrak{H}, & T^{-1}S^{-1}U_2\mathfrak{H}, \ldots, & T^{-1}S^{-1}U_n\mathfrak{H} \end{pmatrix},$$

so sieht man, daß die Zusammensetzung der beiden zu S und T gehörigen Permutationen die zu ST gehörige Permutation ergibt.

Um nun zu beweisen, daß diese Permutationsgruppe bei geeigneter Anordnung der Nebengruppen mit einer früheren identisch ist, schreiben wir die rechts- und linksseitigen Nebengruppen in besonderer Weise auf. Ist

$$\mathfrak{G} = \mathfrak{H} + \mathfrak{H}T_2 + \ldots + \mathfrak{H}T_n$$

eine Zerlegung von $\mathfrak{G}$ nach rechtsseitigen Nebengruppen, so ist nach § 5

$$\mathfrak{G} = \mathfrak{H} + T_2^{-1}\mathfrak{H} + \ldots + T_n^{-1}\mathfrak{H}$$

eine solche nach linksseitigen Nebengruppen. Multipliziert man der Reihe nach $\mathfrak{H}, \mathfrak{H}T_2, \ldots, \mathfrak{H}T_n$ rechts mit S, so erhält man genau die-

selbe Permutation der Nebengruppen, wie wenn man die linksseitigen Nebengruppen $\mathfrak{H}, T_2^{-1}\mathfrak{H}, \ldots, T_n^{-1}\mathfrak{H}$ links mit S^{-1} multipliziert, so daß in der Tat die durch linksseitige Multiplikation hervorgerufene Permutationsgruppe mit einer rechtsseitigen identisch ist.

Eine weitere Möglichkeit, die abstrakte Gruppe $\mathfrak{G}$ als Permutationsgruppe darzustellen, ist die folgende: $P_1, \ldots, P_r$ seien die Elemente einer *Klasse* von $\mathfrak{G}$. Dem beliebigen Element S von $\mathfrak{G}$ ordnen wir diejenige Permutation der Elemente P zu, welche durch Transformation mit S gebildet wird, also $S^{-1}P_1S, \ldots, S^{-1}P_rS$. Man sieht ohne weiteres ein, daß dies eine Darstellung von $\mathfrak{G}$ ergibt; aber auch sie ist identisch mit einer durch unsere allgemeine Methode erzeugten. Sei nämlich $\mathfrak{H}$ diejenige Untergruppe, welche aus den mit P_1 vertauschbaren Elementen der Gruppe besteht, dann ist r der Index von $\mathfrak{H}$ unter $\mathfrak{G}$ und die Nebengruppen von $\mathfrak{H}$ sind $\mathfrak{H}, \mathfrak{H}S_2, \ldots, \mathfrak{H}S_r$, wobei die S_i der Gleichung genügen: $S_i^{-1}P_1S_i = P_i$.

Rechtsseitige Multiplikation mit S ergibt die Permutation

$$\mathfrak{H}S,\ \mathfrak{H}S_2S, \ldots, \mathfrak{H}S_rS,$$

und wir behaupten, daß dies dieselbe Permutation ist, wie

$$S^{-1}P_1S, \ldots, S^{-1}P_rS.$$

In der Tat, wenn $\mathfrak{H}S_iS = \mathfrak{H}S_k$ ist, so wird S_iS das Element P_1 in P_k transformieren, und daher $S^{-1}P_iS = P_k$ sein. Gleich wie also die Nebengruppe $\mathfrak{H}P_i$ durch S in $\mathfrak{H}P_k$ übergeführt wird, so P_i in P_k, womit die Behauptung erwiesen ist.

Zum Schluß soll noch untersucht werden, wann zwei verschiedene Untergruppen $\mathfrak{H}$ und $\mathfrak{K}$ bei geeigneter Anordnung der Nebengruppen zu derselben Permutationsgruppe führen.

Die Nebengruppen von $\mathfrak{H}$ nehmen wir in der Reihenfolge:

$$\mathfrak{H}, \mathfrak{H}T_2, \ldots, \mathfrak{H}T_r.$$

Bei $\mathfrak{K}$ wollen wir die Untergruppe selbst nicht an die erste Stelle setzen, sondern wir bezeichnen die Nebengruppen allgemein mit

$$\mathfrak{K}U_1, \mathfrak{K}U_2, \ldots, \mathfrak{K}U_r.$$

Wenn nun die Vertauschung, die zu S gehört, in beiden Fällen dieselbe sein soll, so müssen insbesondere diejenigen Elemente, welche die erste Variable, nämlich $\mathfrak{H}$ resp. $\mathfrak{K}U_1$ ungeändert lassen, in beiden Fällen dieselben sein. Nun folgt aus $\mathfrak{H}S = \mathfrak{H}$, daß S in $\mathfrak{H}$ liegt und aus $\mathfrak{K}U_1S = \mathfrak{K}U_1$, daß S zu $U_1^{-1}\mathfrak{K}U_1$ gehört. Es muß also $\mathfrak{H} = U_1^{-1}\mathfrak{K}U_1$ sein, d. h. $\mathfrak{H}$ und $\mathfrak{K}$ müssen konjugierte Untergruppen sein. Umgekehrt, wenn $\mathfrak{H}$ und $\mathfrak{K}$ konjugierte Untergruppen sind, so erzeugen sie dieselbe Permutationsgruppe bei geeigneter Numerierung der Variablen.

§ 30. Primitive und imprimitive Permutationsgruppen.

Die transitiven Gruppen werden eingeteilt in primitive und imprimitive Gruppen.

Definition: Eine transitive Permutationsgruppe heißt ***imprimitiv,*** wenn sich ihre Variablen dergestalt in Systeme mit mehr als einer Variablen einteilen lassen, daß die Variablen eines jeden Systems entweder nur unter sich vertauscht werden, oder in die Variablen eines anderen Systems übergeführt werden.

Es ist klar, daß die Anzahl der Variablen in jedem System dieselbe sein muß. Diejenigen Permutationen, welche die Variablen eines jeden Systems nur unter sich vertauschen, bilden einen Normalteiler der Gruppe, denn wir erhalten eine mit der Gruppe isomorphe Permutationsgruppe, wenn wir bloß die Vertauschungen der Systeme untereinander betrachten, und die erwähnte Untergruppe gehört offenbar zu der Einheitspermutation dieser isomorphen Gruppe. Diejenigen Permutationen hingegen, welche die Variablen eines bestimmten Systems unter sich vertauschen, bilden eine Untergruppe $\mathfrak{K}$, welche diejenige Untergruppe $\mathfrak{H}$ enthält, die eine bestimmte Variable des Systems in sich selbst transformiert.

Die imprimitiven Gruppen haben sonach die besondere Eigenschaft, daß diejenige Untergruppe $\mathfrak{H}$, welche eine Variable, z. B. x_1, nicht ändert, in einer weiteren Untergruppe $\mathfrak{K}$ enthalten ist. Umgekehrt gibt eine solche Untergruppe $\mathfrak{K}$ stets Anlaß zu einer imprimitiven Gruppe. Denn sei $\mathfrak{K} = \mathfrak{H} + \mathfrak{H}S_2 + \ldots + \mathfrak{H}S_l$, und $\mathfrak{G} = \mathfrak{K} + \mathfrak{K}T_2 + \ldots + \mathfrak{K}T_m$, so werden zunächst bei Multiplikation mit einem beliebigen Element S die Nebengruppen von $\mathfrak{K}$ unter sich vertauscht. Eine Nebengruppe von $\mathfrak{K}$ besteht genau aus den Elementen von l Nebengruppen von $\mathfrak{H}$, denn es ist z. B.:

$$\mathfrak{K}T_2 = \mathfrak{H}T_2 + \mathfrak{H}S_2T_2 + \ldots + \mathfrak{H}S_lT_2.$$

Die sämtlichen Nebengruppen von $\mathfrak{H}$ zerfallen sonach in m Systeme von je l Nebengruppen, und jedes System enthält gerade diejenigen Nebengruppen von $\mathfrak{H}$, die zusammen eine Nebengruppe von $\mathfrak{K}$ bilden. Es ist nun klar, daß bei Multiplikation mit S die Nebengruppen eines solchen Systems entweder nur unter sich permutiert werden, oder aber in die Nebengruppen eines neuen Systems übergeführt werden, d. h. die durch $\mathfrak{H}$ erzeugte Permutationsgruppe ist imprimitiv. Daß eine Permutationsgruppe eventuell in mehrfacher Weise imprimitiv sein kann, ist nun auch fast selbstverständlich; dies ist der Fall, wenn es mehrere Untergruppen von $\mathfrak{G}$ gibt, die $\mathfrak{H}$ enthalten. Die Existenz einer jeden dieser besonderen Untergruppen macht sich durch eine besondere Art der Imprimitivität geltend.

Die imprimitiven Gruppen sind stets nur einfach transitiv, denn im entgegengesetzten Fall müßte z. B. das Variablenpaar x_1x_2 in

jedes der Paare $x_1 x_i$ übergeführt werden können, was der Tatsache widerspricht, daß dieses Paar nur in ein Paar desselben oder eines anderen Systems übergeführt werden kann.

Von besonderer Wichtigkeit sind die ***primitiven*** Gruppen. Sie werden erzeugt durch solche Untergruppen $\mathfrak{H}$ von $\mathfrak{G}$, die in keiner weiteren enthalten sind, d. h. von größten Untergruppen von $\mathfrak{G}$; und wir können über sie einige wichtige Sätze angeben.

Satz 69: *Der Grad einer primitiven Permutationsgruppe, die auflösbar ist, ist stets Potenz einer Primzahl p^n und die Gruppe enthält einen und nur einen kleinsten Normalteiler; seine Ordnung ist p^n.*

Beweis: Es sei $\mathfrak{H}$ die (größte) Untergruppe von $\mathfrak{G}$, welche die primitive Permutationsgruppe $\mathfrak{G}$ erzeugt, und $\mathfrak{N}$ ein kleinster Normalteiler von $\mathfrak{G}$, dann ist $\mathfrak{G} = \{\mathfrak{N}, \mathfrak{H}\}$. Weil $\mathfrak{G}$ auflösbar ist, so ist $\mathfrak{N}$ eine *Abel*sche Gruppe, deren Ordnung Potenz einer Primzahl, etwa p^n ist. Ist $\mathfrak{D}$ der Durchschnitt von $\mathfrak{H}$ und $\mathfrak{N}$, so ist $\mathfrak{D}$ Normalteiler von $\mathfrak{H}$ und es gilt die Beziehung $\mathfrak{H}/\mathfrak{D} = \mathfrak{G}/\mathfrak{N}$ (Satz 15^2). Hieraus folgt, daß der Index von $\mathfrak{H}$ unter $\mathfrak{G}$ gleich dem Index von $\mathfrak{D}$ unter $\mathfrak{N}$, d. h. eine Potenz von p ist. Wir behaupten ferner, daß $\mathfrak{D} = E$ ist, d. h. daß $\mathfrak{N}$ und $\mathfrak{H}$ zueinander teilerfremd sind. In der Tat sei P ein Element, das $\mathfrak{H}$ und $\mathfrak{N}$ gemeinsam ist, so ist P mit allen Elementen von $\mathfrak{N}$ vertauschbar, weil $\mathfrak{N}$ *Abel*sch ist. Setzt man: $\mathfrak{G} = \mathfrak{H} + \mathfrak{H}T_2 + \ldots + \mathfrak{H}T_l$, so darf man nach § 9 die Elemente $T_2, \ldots, T_l$ aus $\mathfrak{N}$ wählen. Die zu $\mathfrak{H}$ konjugierten Untergruppen sind alsdann $T_i^{-1}\mathfrak{H}T_i$. Da P mit allen T vertauschbar ist, so kommt P in allen zu $\mathfrak{H}$ konjugierten Untergruppen vor und gehört also zu einem Normalteiler von $\mathfrak{G}$, der in $\mathfrak{H}$ enthalten ist. Dies ist aber nicht möglich, da $\mathfrak{H}$ außer E keinen Normalteiler von $\mathfrak{G}$ enthält. Hiermit ist gezeigt, daß der Grad der Permutationsgruppe genau $= p^n$ ist. Es bleibt nun noch übrig zu zeigen, daß $\mathfrak{N}$ der *einzige* kleinste Normalteiler von $\mathfrak{G}$ ist. Angenommen nämlich, es gäbe noch einen zweiten $\mathfrak{N}'$, dann ist auch dieser *Abel*sch, und ferner ist jedes Element von $\mathfrak{N}$ mit jedem Element von $\mathfrak{N}'$ vertauschbar, denn $\mathfrak{N}$ und $\mathfrak{N}'$ haben außer E kein Element gemeinsam. Das direkte Produkt von $\mathfrak{N}$ und $\mathfrak{N}'$ ist selbst ein *Abel*scher Normalteiler von $\mathfrak{G}$ und wir bezeichnen ihn mit $\mathfrak{M}$. Nun läßt sich genau derselbe Beweis, den wir für $\mathfrak{N}$ geführt haben, auch für $\mathfrak{M}$ führen; also müßte der Index von $\mathfrak{H}$ unter $\mathfrak{G}$ auch gleich der Ordnung von $\mathfrak{M}$ sein, was einen Widerspruch ergibt. Wir können sonach den folgenden allgemeinen Satz aussprechen:

Satz 70: *Ist $\mathfrak{H}$ eine größte Untergruppe der **auflösbaren** Gruppe $\mathfrak{G}$ und $\mathfrak{N}$ der größte in $\mathfrak{H}$ enthaltene Normalteiler von $\mathfrak{G}$, dann besitzt die Faktorgruppe $\mathfrak{G}/\mathfrak{N}$ nur einen Abelschen Normalteiler und dessen Ordnung ist gleich dem Index von $\mathfrak{H}$ unter $\mathfrak{G}$.*

Da dieser *Abel*sche Normalteiler kleinster Normalteiler ist, so ist sein Typus durch die allgemeinen Regeln bestimmt.

Wir wollen noch einige einfache Folgerungen aus unserer Methode angeben:

Satz 71: *Ist $\mathfrak{H}$ eine Untergruppe von $\mathfrak{G}$ vom Index n, und ist ferner $\mathfrak{N}$ der größte in $\mathfrak{H}$ enthaltene Normalteiler von $\mathfrak{G}$, so ist die Ordnung von $\mathfrak{G}/\mathfrak{N}$ ein Teiler von $n!$*

Denn die Gruppe $\mathfrak{G}/\mathfrak{N}$ läßt sich homomorph darstellen als Permutationsgruppe von n Variablen. Ist p die größte in der Ordnung einer *einfachen Gruppe* enthaltene Primzahl, so besitzt diese Gruppe keine Untergruppe, deren Index kleiner als p ist. Allgemeiner läßt sich folgender Satz aussprechen:

Satz 72: *Ist die Ordnung der Untergruppe $\mathfrak{H}$ gleich ab, die von $\mathfrak{G}$ gleich abn, und ist jede in b aufgehende Primzahl $\geqq n$, jede in a aufgehende $< n$, so ist die Ordnung des größten in $\mathfrak{H}$ enthaltenen Normalteilers von $\mathfrak{G}$ durch b teilbar.*

Beweis: Es sei $\mathfrak{N}$ der größte in $\mathfrak{H}$ enthaltene Normalteiler von $\mathfrak{G}$, dann ist die Ordnung von $\mathfrak{G}/\mathfrak{N}$ ein Teiler von $n!$, diejenige von $\mathfrak{H}/\mathfrak{N}$ also ein Teiler von $(n-1)!$. Diese letztere Zahl ist aber sicherlich zu b prim, folglich muß b in der Ordnung von $\mathfrak{N}$ aufgehen.

Historische Notiz: Satz 69 ist von *Galois* entdeckt worden. Die Aufstellung sämtlicher auflösbarer primitiver Gruppen vom Grade p^n bildet den Inhalt der zweiten Hälfte von *Jordan*s Traité des substitutions. Der Verfasser hat seine Beweise später wesentlich vereinfacht und in zwei Abhandlungen niedergelegt: Recherches sur les groupes résolubles (Memorie della Pontificia Accademia Romana dei Nuovi Lincei **26** (1908), S. 7—39) und Mémoire sur les groupes résolubles (J. de math. 1917, S. 263—374). Die Fälle p^3 und p^4 behandelt *Gösta Bucht* (Die umfassendsten primitiven metazyklischen Kongruenzgruppen mit drei oder vier Variablen, Archiv för Mat., Astr. och Fys. Bd. **11**, 1916.)

§ 31. Die Charaktere einer Permutationsgruppe.

Wir betrachten eine transitive Permutationsgruppe $\mathfrak{G}$ und zählen bei jeder Permutation die Variablen, die ungeändert bleiben. Diese Zahl wird der ***Charakter*** der Permutation genannt, und wir wollen einige Eigenschaften dieser wichtigen Zahlen herleiten.

$\mathfrak{H}$ sei diejenige Untergruppe von $\mathfrak{G}$, deren Permutationen eine Variable ungeändert lassen, und es sei

$$\mathfrak{G} = \mathfrak{H} + \mathfrak{H}T_2 + \cdots + \mathfrak{H}T_n.$$

Die Anzahl der Permutationen, welche die erste Variable ungeändert lassen, ist gleich der Anzahl der Elemente in $\mathfrak{H}$; diejenige der Permutationen, welche die i-te Variable in sich selbst überführen, ist gleich der Anzahl der Elemente in $T_i^{-1}\mathfrak{H}T_i$. Auch ihre Anzahl ist gleich der Ordnung von $\mathfrak{H}$. Für jede Variable gibt es also genau

gleich viele Permutationen, welche sie ungeändert lassen. Die Summe der Charaktere aller Permutationen ist daher gleich der Ordnung von $\mathfrak{H}$ multipliziert mit n, also gleich der Ordnung von $\mathfrak{G}$. Ist die Gruppe intransitiv, so wird jeder transitive Bestandteil an die Summe der Charaktere denselben Bestandteil liefern. Hieraus folgt der

Satz 73: *Ist $\mathfrak{G}$ eine Permutationsgruppe von der Ordnung g, so ist die Summe der Charaktere der Permutationen gleich kg, wobei k die Anzahl der transitiven Systeme von $\mathfrak{G}$ bedeutet.*

Wir betrachten nunmehr die Elemente der Untergruppe $\mathfrak{H}$ und die zu ihnen gehörigen Permutationen. Die Summe ihrer Charaktere ist gleich der Ordnung von $\mathfrak{H}$ multipliziert mit der Anzahl der Komplexe, in die $\mathfrak{G} \bmod (\mathfrak{H}, \mathfrak{H})$ zerfällt (Satz 73), denn nur solche Nebengruppen von $\mathfrak{H}$, die zum selben Komplex gehören, sind bei der Untergruppe $\mathfrak{H}$ transitiv verbunden. Diese Anzahl der Komplexe bezeichnen wir mit l. Nehmen wir statt $\mathfrak{H}$ die konjugierte Untergruppe $T_i^{-1}\mathfrak{H}T_i$, so liefert sie dieselbe Zahl für die Summe der Charaktere. Bei der Gesamtheit dieser n konjugierten Untergruppen erhalten wir als Summe der Charaktere die Zahl lg. Hierbei sind nun die Elemente im allgemeinen mehrfach gezählt, und indem wir sie ordnen, erhalten wir eine neue Abzählung der Charaktere. Wenn nämlich der Charakter eines Elementes r ist, so tritt dieses Element genau in r von den zu $\mathfrak{H}$ konjugierten Untergruppen auf. Jedes Element liefert also als Beitrag zu der Summe das Quadrat seines Charakters. Nun kann man auch noch die Elemente außerhalb des Systems der zu $\mathfrak{H}$ konjugierten Untergruppen heranziehen. Ihr Charakter ist Null, und wenn wir sie zu unserer Summe hinzunehmen, so wird nichts geändert. Dies Resultat kann man in folgendem Satz zusammenfassen:

Satz 74: *Die Summe der Quadrate der Charaktere einer transitiven durch $\mathfrak{H}$ erzeugten Permutationsgruppe von der Ordnung g ist gleich lg, wobei l die Anzahl der Komplexe von Nebengruppen darstellt, in die $\mathfrak{G} \bmod (\mathfrak{H}, \mathfrak{H})$ zerfällt.*

8. Kapitel.

Automorphismen.

§ 32. Automorphismen einer Gruppe.

Ist $\mathfrak{G}$ irgendeine Gruppe und S eines ihrer Elemente, so erhält man durch Transformation aller Elemente von $\mathfrak{G}$ mit S einen Automorphismus (§ 8) von $\mathfrak{G}$. Ist nämlich $AB = C$, so folgt daraus $S^{-1}AS \cdot S^{-1}BS = S^{-1}CS$,

Die so entstehenden Automorphismen einer Gruppe nennt man ***innere Automorphismen.*** Ersetzt man jedes Element durch das

beim Automorphismus ihm entsprechende, so erhält man eine Permutation der Elemente, die man durch

$$\begin{Bmatrix} X \\ S^{-1}XS \end{Bmatrix}$$

bezeichnen kann, wobei X die Elemente von $\mathfrak{G}$ durchläuft. In vielen Fällen gibt es aber auch weitere Automorphismen der Gruppe und diese nennt man zum Unterschied von den früheren ***äußere*** Automorphismen. Wenn dabei dem Element X das Element X' zugeordnet ist, so bezeichnen wir diesen Automorphismus mit

$$\begin{Bmatrix} X \\ X' \end{Bmatrix}.$$

Als Beispiel für Gruppen mit äußeren Automorphismen erwähnen wir die zyklische Gruppe von der Ordnung 3, bestehend aus den Elementen A, A^2, $A^3 = E$. Sie besitzt keinen innern Automorphismus, außer dem identischen, dagegen den äußeren $E' = E$, $A' = A^2$, $(A^2)' = A$.

Die sämtlichen Automorphismen einer Gruppe bilden selbst eine Gruppe, denn, wenn man hintereinander die Permutation des ersten Automorphismus, dann diejenige des zweiten ausführt, so erhält man wiederum einen Automorphismus.

Diese Gruppe ist intransitiv, denn E wird stets sich selbst entsprechen.

Satz 75: *Die innern Automorphismen bilden einen Normalteiler der sämtlichen Automorphismen.*

Beweis: Transformiert man den Automorphismus

$$\begin{Bmatrix} X \\ S^{-1}XS \end{Bmatrix}$$

durch den allgemeinen Automorphismus

$$\begin{Bmatrix} X \\ X' \end{Bmatrix},$$

so hat man nach Satz 64 in beiden Zeilen der ersten Permutation die zweite Permutation auszuführen. Dies ergibt den neuen Automorphismus.

$$\begin{Bmatrix} X' \\ S'^{-1}X'S' \end{Bmatrix}.$$

Er ersetzt jedes Element X' durch das Element $S'^{-1}X'S'$. Wir dürfen hier das allgemeine Element X' selbstverständlich auch mit X bezeichnen und unser Automorphismus ist identisch mit dem innern Automorphismus

$$\begin{Bmatrix} X \\ S'^{-1}XS' \end{Bmatrix}.$$

Satz 76: *Die Gruppe der innern Automorphismen ist isomorph mit der gegebenen Gruppe und zwar entspricht der Einheit das Zentrum der Gruppe*, denn nur für diese Elemente wird der Automorphismus der identische.

Wir gehen wieder aus von einer Gruppe $\mathfrak{G}$ und wollen annehmen, sie sei als Normalteiler in einer umfassenderen Gruppe $\mathfrak{J}$ enthalten. Transformiert man $\mathfrak{G}$ durch irgend ein Element von $\mathfrak{J}$, so erhält man einen Automorphismus für $\mathfrak{G}$, der nicht notwendigerweise ein innerer ist. So ergeben z. B. die Diedergruppen einen äußern Automorphismus für ihren zyklischen Normalteiler vom Index 2. Es ist nun die Frage, ob sich zu einer beliebigen Gruppe $\mathfrak{G}$ eine umfassendere Gruppe $\mathfrak{J}$ definieren läßt, die in der angegebenen Weise alle Automorphismen von $\mathfrak{G}$ liefert. Die Permutationsgruppen geben uns in der Tat die Mittel zur Hand, diese Frage zu bejahen.

Wir gehen aus von der durch die Gruppentafel gelieferten Darstellung von $\mathfrak{G}$ durch Permutationsgruppen. Zu dem Element S gehört so die Permutation, welche wir in unserer Symbolik mit

$$\begin{Bmatrix} X \\ XS \end{Bmatrix}$$

bezeichnen. Ist nun ein Automorphismus von $\mathfrak{G}$ gegeben, wobei allgemein S' dem S entspricht, so ist die Permutation, welche S entspricht, offenbar die folgende

$$\begin{Bmatrix} X \\ XS' \end{Bmatrix}.$$

Diese letztere können wir aber auch so schreiben

$$\begin{Bmatrix} X' \\ X'S' \end{Bmatrix},$$

denn beide stellen dieselbe Permutation, bloß in anderer Reihenfolge der Variablen dar.

Nehmen wir zu unserer Darstellung von $\mathfrak{G}$ die Permutationsgruppe der Automorphismen von $\mathfrak{G}$ hinzu, so sind beides Untergruppen der Gruppe aller Permutationen der Elemente von $\mathfrak{G}$. Die beiden Gruppen erzeugen also eine Untergruppe der symmetrischen Gruppe aller Vertauschungen der Elemente von $\mathfrak{G}$. Sie haben überdies keine Permutation außer der identischen gemein, denn während die Gruppe der Automorphismen E ungeändert läßt, wird bei der Darstellung von $\mathfrak{G}$ jeweils E in ES übergeführt und ES ist nur für das Einheitselement $= E$. Die zusammengesetzte Gruppe bezeichnen wir nun mit $\mathfrak{R}$, die Darstellung von $\mathfrak{G}$ wiederum mit $\mathfrak{G}$ und behaupten den

Satz 77: *$\mathfrak{G}$ ist Normalteiler von $\mathfrak{K}$ und jeder Automorphismus von $\mathfrak{G}$ entsteht durch Transformation mit einer Permutation von $\mathfrak{K}$.*

Beweis: $\mathfrak{K}$ ist nach Definition erzeugt durch die Gruppe $\mathfrak{G}$, aus der wir die Permutation $\begin{Bmatrix} X \\ XS \end{Bmatrix}$ herausgreifen und durch die Gruppe der Automorphismen von $\mathfrak{G}$, deren Permutationen wir durch $\begin{Bmatrix} X \\ X' \end{Bmatrix}$ bezeichnen. Transformieren wir die erste der angegebenen Permutationen durch die zweite, so erhalten wir $\begin{Bmatrix} X' \\ X'S' \end{Bmatrix}$. Diese ist identisch mit $\begin{Bmatrix} X \\ XS' \end{Bmatrix}$, d. h, mit der zu S' gehörigen Permutation von $\mathfrak{G}$. Damit ist zunächst gezeigt, daß $\mathfrak{G}$ Normalteiler von $\mathfrak{K}$ ist, dessen Index gleich der Ordnung der Gruppe aller Automorphismen von $\mathfrak{G}$ ist. Weiter aber folgt auch, wenn wir beachten, daß S' dasjenige Element ist, das S zugeordnet ist durch den Automorphismus $\begin{Bmatrix} X \\ X' \end{Bmatrix}$, die Tatsache, daß die Transformation der Elemente von $\mathfrak{G}$ durch $\begin{Bmatrix} X \\ X' \end{Bmatrix}$ gerade den durch dieses Symbol repräsentierten Automorphismus für $\mathfrak{G}$ ergibt, womit unser Satz vollständig bewiesen ist.

Definition: Die Gruppe $\mathfrak{K}$ heißt das ***Holomorph*** von $\mathfrak{G}$.

$\mathfrak{K}$ hat offenbar die Eigenschaft, daß man die Nebengruppen des Normalteilers $\mathfrak{G}$ erhält, indem man $\mathfrak{G}$ der Reihe nach mit den Elementen einer zweiten Untergruppe von $\mathfrak{K}$, nämlich der Gruppe der Automorphismen, multipliziert. Diese zweite Untergruppe besitzt selbst einen Normalteiler, der isomorph ist mit $\mathfrak{G}$, nämlich die Gruppe der innern Automorphismen von $\mathfrak{G}$. Diese letztere ist aber gewiß nicht Normalteiler von $\mathfrak{K}$, denn sonst wäre jedes seiner Elemente mit jedem Element von $\mathfrak{G}$ vertauschbar.

Satz 78: *Das Holomorph einer Gruppe $\mathfrak{G}$ von der Ordnung g ist der Normalisator von $\mathfrak{G}$ in der symmetrischen Gruppe von g Variablen.*

Beweis: Unter den Permutationen von $\mathfrak{G}$ verstehen wir wie immer $\begin{Bmatrix} X \\ XS \end{Bmatrix}$, wobei S die Elemente von $\mathfrak{G}$ durchläuft. Nun sei irgendeine Permutation der g Elemente gegeben: $P = \begin{Bmatrix} X \\ X' \end{Bmatrix}$. Soll sie zum Normalisator von $\mathfrak{G}$ gehören, so muß sie mit $\mathfrak{G}$ vertauschbar sein, und wenn man die Permutationen von $\mathfrak{G}$ durch sie transformiert, so erhält man einen Automorphismus von $\mathfrak{G}$. Derselbe Automorphismus wird aber auch durch eine Permutation Q des Holomorphs ge-

liefert. Bildet man nun $PQ^{-1}=R$, so ist die Permutation R mit allen Permutationen von $\mathfrak{G}$ vertauschbar und es bleibt nun noch zu beweisen übrig, daß das Holomorph alle diese Permutationen enthält.

Es sei $R=\begin{Bmatrix} X \\ X' \end{Bmatrix}$ eine Permutation, die mit allen Permutationen von $\mathfrak{G}$ vertauschbar ist. Transformiert man $\begin{Bmatrix} X \\ X\,S \end{Bmatrix}$ mit dieser Permutation, so erhält man $\begin{Bmatrix} X' \\ (X\,S)' \end{Bmatrix}$. Da diese Permutation identisch sein soll mit der vorigen, so muß die Beziehung gelten $(X\,S)'=X'\,S$. Dies genügt, um die Beschaffenheit der Permutation R zu bestimmen. Es sei nämlich A dasjenige Element, in das E durch R übergeführt wird, d. h. es sei $E'=A$. Indem wir die obige Beziehung benutzen, folgt:

$$X'=(E\,X)'=E'\,X=A\,X,$$

so daß sich R in folgender Weise ausdrückt: $R=\begin{Bmatrix} X \\ A\,X \end{Bmatrix}$. Läßt man hierin A alle Elemente von $\mathfrak{G}$ durchlaufen, so erhält man n Permutationen, und es ist leicht zu zeigen, daß sie alle mit den Elementen von $\mathfrak{G}$ vertauschbar sind, denn führt man hintereinander die beiden Permutationen aus: $\begin{Bmatrix} X \\ X\,S \end{Bmatrix}$ und $\begin{Bmatrix} X \\ A\,X \end{Bmatrix}$, so erhält man die Permutation $\begin{Bmatrix} X \\ A\,X\,S \end{Bmatrix}$, gleichgültig welche Reihenfolge man gewählt hat. Es bleibt nun noch übrig zu zeigen, daß die Permutationen von der Gestalt $R=\begin{Bmatrix} X \\ A\,X \end{Bmatrix}$ sämtlich im Holomorph von $\mathfrak{G}$ enthalten sind. Nun gehört gewiß $\begin{Bmatrix} X \\ A\,X\,A^{-1} \end{Bmatrix}$ als innerer Automorphismus zum Holomorph und ebenso $\begin{Bmatrix} X \\ X\,A \end{Bmatrix}$, denn dies ist eine Permutation von $\mathfrak{G}$, also auch ihr Produkt. Dies ist aber die Permutation R.

Ein Automorphismus transformiert stets zwei Elemente, die zur selben Klasse gehören, in zwei neue Elemente von derselben Eigenschaft. Denn wenn $A=S^{-1}BS$ ist, so geht diese Gleichung beim Automorphismus über in die Gleichung $A'=S'^{-1}B'S'$, d. h. A' und B' sind wiederum konjugiert. Die innern Automorphismen führen jedes Element in ein Element derselben Klasse über. Bei äußern Automorphismen dagegen kann es vorkommen, daß die Elemente einer Klasse übergeführt werden in die Elemente einer andern Klasse, wofür die zyklischen Gruppen Beispiele liefern. Natürlich müssen sowohl die Ordnung als die Anzahl der Elemente für zwei ver-

schmolzene Klassen dieselben sein. Man kann zu der Gruppe der Automorphismen eine isomorphe Gruppe bilden, indem man bloß die Permutationen der Klassen unter sich berücksichtigt. Der identischen Permutation entsprechen dann diejenigen Automorphismen, welche die Elemente in ihren Klassen lassen.

Wir sprechen nun den Satz aus:

Satz 79: *Diejenigen Automorphismen, welche die Elemente in ihren Klassen lassen, bilden einen Normalteiler der Gruppe aller Automorphismen, dessen Ordnung nur Primteiler der Ordnung von $\mathfrak{G}$ enthält.*

Dieser eben betrachtete Normalteiler ist nicht immer identisch mit der Gruppe der innern Automorphismen.

Beweis: Sei J irgendein Automorphismus aus diesem Normalteiler, dessen Ordnung eine Primzahl p ist. Die Gruppe $\{\mathfrak{G}, J\}$ enthält $\mathfrak{G}$ als Normalteiler, dessen Index p gleich der Ordnung von J ist. J ist gewiß nicht mit allen Elementen von $\mathfrak{G}$ vertauschbar und wir betrachten nun die Klasse der mit J konjugierten Elemente. Es muß notwendigerweise Elemente geben, die mit keinem Element dieser Klasse vertauschbar sind (§ 17). Sei S ein solches Element, dann muß die Klasse, zu der S gehört, eine durch p teilbare Anzahl von Elementen besitzen. Denn J kann mit keinem Element der Klasse von S vertauschbar sein. Wäre nämlich J mit $T^{-1}ST$ vertauschbar, so wäre auch S mit TJT^{-1} vertauschbar, was gegen die Voraussetzung ist. Transformiert man nun S der Reihe nach mit den Potenzen von J, so erhält man p verschiedene Elemente der Klasse von S, und indem man so fortfährt, sieht man, daß die Anzahl der Elemente in der Klasse durch p teilbar ist. Ist p zur Ordnung von $\mathfrak{G}$ prim, so erhalten wir einen Widerspruch, denn diese Anzahl ist ein Teiler der Ordnung von $\mathfrak{G}$.

Ist J ein Automorphismus, dessen Ordnung die Potenz einer Primzahl p^n ist, die prim ist zur Ordnung von $\mathfrak{G}$, so bilde man die p^{n-1}-te Potenz von J. Es gibt nun ein Element S von $\mathfrak{G}$, das mit dieser Potenz und also auch mit jeder Potenz von J *nicht* vertauschbar ist, außer mit E. Die Anzahl der Elemente in der Klasse von S ist also ein Vielfaches von p^n, d. h. sie muß aus mindestens p^n verschiedenen Klassen von $\mathfrak{G}$ zusammengesetzt sein.

§ 33. Charakteristische Untergruppen einer Gruppe.

Definition: Ein Normalteiler der Gruppe $\mathfrak{G}$ heißt eine ***charakteristische Untergruppe,*** wenn er bei jedem Automorphismus von $\mathfrak{G}$ in sich selbst übergeführt wird.

Mit Hilfe des Holomorphs $\mathfrak{H}$ von $\mathfrak{G}$ lassen sich die sämtlichen charakteristischen Untergruppen von $\mathfrak{G}$ auffinden. Eine solche ist nämlich stets auch Normalteiler von $\mathfrak{H}$, und umgekehrt ist jeder

Normalteiler von $\mathfrak{R}$, der in $\mathfrak{G}$ enthalten ist, charakteristische Untergruppe von $\mathfrak{G}$.

Wir greifen nun eine beliebige Hauptreihe von $\mathfrak{R}$ heraus, die $\mathfrak{G}$ enthält:

$$\mathfrak{R}, \mathfrak{R}_1, \ldots, \mathfrak{G}, \mathfrak{G}_1, \ldots, \mathfrak{G}_r = E.$$

Die Reihe $\mathfrak{G}, \mathfrak{G}_1, \ldots, \mathfrak{G}_r$ besteht aus lauter charakteristischen Untergruppen von $\mathfrak{G}$, deren jede die folgende enthält, und zwar gibt es zwischen zwei aufeinander folgenden Gliedern keine charakteristische Untergruppe von $\mathfrak{G}$. Eine solche Reihe wird eine ***charakteristische Reihe*** von $\mathfrak{G}$ genannt. Jede charakteristische Reihe von $\mathfrak{G}$ kann zu einer Hauptreihe von $\mathfrak{R}$ ergänzt werden. Man braucht zu dem Zweck bloß die eben angeführte Reihe von $\mathfrak{R}$ bis $\mathfrak{G}$ anzuschließen. Indem wir nun einfach die bekannten Sätze über Hauptreihen anwenden, erhalten wir den folgenden

Satz 80: *Ist* $\mathfrak{G}, \mathfrak{G}_1, \ldots, \mathfrak{G}_r = E$ *eine charakteristische Reihe von* $\mathfrak{G}$, *so sind die Faktorgruppen* $\mathfrak{G}_i/\mathfrak{G}_{i+1}$ *einfache Gruppen oder das direkte Produkt von solchen. Jede charakteristische Reihe einer Gruppe besteht aus gleichvielen Gliedern und die darin auftretenden Faktorgruppen* $\mathfrak{G}_i/\mathfrak{G}_{i+1}$ *sind bei zwei Reihen in ihrer Gesamtheit dieselben.*

Bei auflösbaren Gruppen existiert also stets eine charakteristische Reihe und die Faktorgruppe zweier aufeinanderfolgender Untergruppen ist *Abel*sch, ihre Ordnung ist eine Primzahlpotenz p^l und ihr Typus $(p, p, \ldots)$.

Bei jedem Automorphismus geht der Kommutator zweier Elemente A und B, nämlich $B^{-1}A^{-1}BA$ wiederum in einen Kommutator, nämlich denjenigen von A' und B' über. *Daher ist die Kommutatorgruppe stets eine charakteristische Untergruppe.* Ferner ist die kleinste Untergruppe, welche alle Untergruppen von einer bestimmten Ordnung enthält, stets eine charakteristische Untergruppe. Denn bei jedem Automorphismus werden die Untergruppen von einer bestimmten Ordnung nur unter sich vertauscht, daher wird die von ihnen erzeugte Untergruppe in sich selbst übergeführt.

Eine weitere charakteristische Untergruppe ist das *Zentrum*. Ist eine *Sylowgruppe* Normalteiler, so ist sie charakteristische Untergruppe, denn sie ist dann die einzige Untergruppe von ihrer Ordnung.

§ 34. Vollständige Gruppen.

Der Begriff der charakteristischen Untergruppen einer Gruppe $\mathfrak{G}$ ist insbesondere dann von Wichtigkeit, wenn $\mathfrak{G}$ selbst Normalteiler einer umfassenderen Gruppe $\mathfrak{G}'$ ist. Jede charakteristische Untergruppe von $\mathfrak{G}$ ist dann auch Normalteiler von $\mathfrak{G}'$. Wir betrachten nun das Holomorph $\mathfrak{R}$ von $\mathfrak{G}$ und machen die Voraussetzung, daß $\mathfrak{G}$

eine charakteristische Untergruppe von $\mathfrak{K}$ ist. Ist $\mathfrak{K}$ selbst als Normalteiler in $\mathfrak{K}'$ enthalten, so ist $\mathfrak{G}$ Normalteiler von $\mathfrak{K}'$, und wir zeigen nun, daß es in jeder Nebengruppe von $\mathfrak{K}$ ein Element gibt, das mit jedem Element von $\mathfrak{G}$ vertauschbar ist. Es sei S irgendein Element aus $\mathfrak{K}'$, so liefert $S^{-1}\mathfrak{G}S$ einen Automorphismus von $\mathfrak{G}$, der auch durch ein Element K des Holomorphs $\mathfrak{K}$ hervorgerufen wird. SK^{-1} ist mit jedem Element von $\mathfrak{G}$ vertauschbar und gehört zu derselben Nebengruppe von $\mathfrak{K}$ wie K.

Definition: Eine Gruppe, deren sämtliche Automorphismen innere Automorphismen sind, und deren Zentrum nur aus E besteht, heißt eine ***vollständige*** Gruppe.

Satz 81: *Wenn eine vollständige Gruppe $\mathfrak{G}$ Normalteiler einer Gruppe $\mathfrak{G}'$ ist, so ist $\mathfrak{G}'$ das direkte Produkt von $\mathfrak{G}$ und einer anderen Untergruppe.*

Beweis: Nach dem eben Ausgeführten gibt es in jeder Nebengruppe von $\mathfrak{G}$ ein mit allen Elementen von $\mathfrak{G}$ vertauschbares Element. Die Gesamtheit der mit allen Elementen von $\mathfrak{G}$ vertauschbaren Elemente bildet einen Normalteiler von $\mathfrak{G}'$, dessen Ordnung mindestens gleich dem Index von $\mathfrak{G}'$ unter $\mathfrak{G}'$ ist. Dieser Normalteiler hat aber mit $\mathfrak{G}$ außer E kein Element gemein. Daher ist seine Ordnung gleich dem Index von $\mathfrak{G}$, und $\mathfrak{G}'$ ist das direkte Produkt von $\mathfrak{G}$ mit diesem Normalteiler.

Wir erweisen nun an einem einfachen Beispiel die Existenz von vollständigen Gruppen. Es sei P ein Element, dessen Ordnung eine ungerade Primzahl p ist. Man erhält die sämtlichen Automorphismen dieser zyklischen Gruppe, indem man P irgendeine zu p prime Potenz zuordnet.

Ist r eine Primitivzahl für p, so bilde man die durch folgende Elemente erzeugte Gruppe:

$$A^p = E, \qquad B^{p-1} = E, \qquad B^{-1}AB = A^r.$$

In dieser Gruppe ist offenbar $\{A\}$ charakteristische Untergruppe. *Wir behaupten, daß sie eine vollständige Gruppe ist.* Ist nämlich irgendein äußerer Automorphismus gegeben, so wird er einen Automorphismus von $\{A\}$ ergeben, der auch durch Transformation mit einer Potenz von B geliefert wird. Wenn daher die Gruppe einen äußeren Automorphismus zuläßt, so muß sie auch einen solchen besitzen, der A in sich selbst überführt. B muß alsdann in ein Element $BA^s (s = 1, 2, \ldots, p)$ übergehen, denn auch das zugeordnete Element B' muß A in A^r transformieren.

Der Automorphismus ist nun aber vollständig bestimmt, wenn feststeht, in welche Elemente die erzeugenden A und B übergehen. Wir behaupten jetzt, daß der Automorphismus $A' = A$, $B' = BA^s$ ein innerer ist und zwar, daß er durch Transformation mit einer Potenz

von A geliefert wird. In der Tat folgt aus $B^{-1}AB = A^r$ leicht: $ABA^{-1} = BA^{r-1}$. Da r von 1 verschieden ist, so ist A^{r-1} ein Element von der Ordnung p, das wir der Einfachheit halber mit $\bar{A}$ bezeichnen.

Indem man weiter transformiert, erhält man die Gleichung

$$A^i B A^{-i} = B\bar{A}^i$$

und unter diesen p inneren Automorphismen kommt sicher der zu untersuchende vor. Damit ist z. B. nachgewiesen, daß die Diedergruppe von der Ordnung 6, d. h. die symmetrische Gruppe von 3 Variablen, eine vollständige Gruppe ist.

Wir geben nun ein hinreichendes Kriterium einer vollständigen Gruppe, indem wir den Satz beweisen:

Satz 82: *Die Gruppe der Automorphismen einer Gruppe $\mathfrak{G}$ ohne Zentrum ist eine vollständige Gruppe, wenn ihre Untergruppe der inneren Automorphismen eine charakteristische ist.*

Beweis: Die Gruppe der inneren Automorphismen ist homomorph mit $\mathfrak{G}$, weil $\mathfrak{G}$ kein Zentrum besitzt. Wir bezeichnen sie infolgedessen mit $\bar{\mathfrak{G}}$ und die ganze Gruppe der Automorphismen mit $\mathfrak{A}$. Jeder Automorphismus von $\bar{\mathfrak{G}}$ wird durch Transformation mit einem Element von $\mathfrak{A}$ geliefert. Denn sei $\begin{Bmatrix} X \\ X' \end{Bmatrix}$ ein solches, so geht der innere Automorphismus $\begin{Bmatrix} X \\ S^{-1}XS \end{Bmatrix}$ über in $\begin{Bmatrix} X' \\ S'^{-1}X'S' \end{Bmatrix}$, d. h. das Element $\bar{S}$ von $\bar{\mathfrak{G}}$ wird in $\bar{S}'$ übergeführt und das ist gerade der betrachtete Automorphismus. Wir betrachten jetzt das Holomorph von $\mathfrak{A}$. $\bar{\mathfrak{G}}$ ist Normalteiler und infolgedessen gibt es in jeder Nebengruppe von $\mathfrak{A}$ ein mit allen Elementen von $\bar{\mathfrak{G}}$ vertauschbares Element. Die Gesamtheit dieser Elemente bildet einen Normalteiler $\mathfrak{N}$ des Holomorphs, dessen Ordnung mindestens gleich dem Index von $\mathfrak{A}$ ist. $\mathfrak{N}$ und $\mathfrak{A}$ sind nun teilerfremd, da es in $\mathfrak{A}$ außer E kein mit allen Elementen von $\bar{\mathfrak{G}}$ vertauschbares Element gibt. Das Holomorph von $\mathfrak{A}$ ist also das direkte Produkt von $\mathfrak{A}$ und $\mathfrak{N}$ und es liefert für $\mathfrak{A}$ keinen äußeren Automorphismus. Daher ist $\mathfrak{A}$ eine vollständige Gruppe.

§ 35. Automorphismen *Abel*scher Gruppen.

Ist $\mathfrak{G}$ eine *Abel*sche Gruppe von der Ordnung $n = p_1^{a_1} \dots p_r^{a_r}$, so ist sie das direkte Produkt von r *Abel*schen Gruppen mit den Ordnungen $p_1^{a_1}, \dots, p_r^{a_r}$. Jede dieser Untergruppen ist charakteristische Untergruppe und wird daher bei jedem Automorphismus in sich selbst transformiert. Die Automorphismengruppe von $\mathfrak{G}$ ist das direkte

Produkt der Automorphismengruppen dieser Untergruppen. Daher kommt es nur darauf an, die Automorphismengruppe solcher *Abel*schen Gruppen zu betrachten, deren Ordnung eine Primzahlpotenz p^r ist. Wir beginnen mit dem Typus $(p, p, \ldots)$. Ein Automorphismus ist festgelegt durch Angabe derjenigen Elemente, in welche die Basiselemente übergehen. Für das erste Element hat man freie Wahl unter den $p^r - 1$ von E verschiedenen Elementen, für das zweite noch unter den $p^r - p$ Elementen, die nicht Potenzen des ausgewählten sind, usw. Die Ordnung der Automorphismengruppe ist also

$$(p^r - 1)(p^r - p)\ldots(p^r - p^{r-1}).$$

Sie läßt sich in bemerkenswerter Weise durch Matrizen[1]) darstellen. Bei einem Automorphismus mögen die Basiselemente $A_1, A_2, \ldots, A_r$ übergehen in $A_1', A_2', \ldots, A_r'$ und es sei

$$A_k' = A_1^{a_{1k}} A_2^{a_{2k}} \ldots A_r^{a_{rk}} \qquad (k = 1, 2, \ldots, r).$$

Die Matrix (a_{ik}) besteht aus (mod p) reduzierten ganzen Zahlen. Ist (b_{ik}) die Matrix für einen anderen Automorphismus derselben Gruppe, so erhält man diejenige für den zusammengesetzten Automorphismus durch Zusammensetzung der Matrizen (a_{ik}) und (b_{ik}) Zeilen mit Kolonnen, wie man sich sofort durch Einsetzen überzeugt. Eine Matrix liefert dann und nur dann einen Automorphismus, wenn sie umkehrbar ist, d. h. wenn ihre Determinante $\not\equiv 0 \pmod{p}$ ist.

Satz 83: *Die Gruppe der Automorphismen einer Abelschen Gruppe von der Ordnung p^r und vom Typus $(p, p, \ldots)$ ist homomorph mit der Gruppe homogener ganzzahliger linearer Substitutionen von r Variablen (mod p) betrachtet, deren Determinante $\not\equiv 0$ (mod p) ist.*

Oft läßt sich ein Automorphismus durch Einführung neuer Basiselemente auf eine einfachere Gestalt bringen, wie folgendes Beispiel verdeutlicht: Es sei $r = p - 1$ und der Automorphismus bestehe in der zyklischen Vertauschung der $p - 1$ Basiselemente $A_1, \ldots, A_{p-1}$. Wir führen jetzt die neuen Basiselemente $B_1, \ldots, B_{p-1}$ ein durch die Gleichungen

$$B_s = A_1 A_2^s A_3^{s^2} \ldots A_{p-1}^{s^{p-2}} \qquad (s = 1, 2, \ldots, p - 1)$$

Da die Determinante der zugehörigen Matrix gleich dem Differenzenprodukt der Zahlen $1, 2, \ldots, p - 1$ ist, so ist sie zu p prim, die B bilden daher wiederum eine Basis der Gruppe. Bei dem Automorphismus geht B_s in B_s^t über, wobei t durch die Kongruenz $st \equiv 1 \pmod{p}$ bestimmt ist. Dieser Satz ist gleichbedeutend mit der Tatsache, daß die zyklische Permutation von $p - 1$ Variabeln (mod p) vollständig

[1]) Wir benutzen im folgenden einige Begriffe, die erst in § 40 auseinandergesetzt werden.

reduzierbar ist auf die Diagonalform und daß ihre charakteristischen Wurzeln aus den Resten $1, 2, \ldots, p-1 \pmod p$ bestehen (§ 58).

Genau nach denselben Prinzipien wie oben lassen sich auch die Gruppen vom Typus $(p^a, p^a, \ldots)$ behandeln. An die Stelle der Matrizen mod p treten diejenigen mod p^a. Wir wollen die eigentümliche Struktur dieser wichtigen Gruppen aufdecken. Die Gruppe der ganzzahligen Matrizen von r Zeilen und Kolonnen bestehend aus Resten mod p^a sei mit $\mathfrak{G}$ bezeichnet. Die Determinanten der Matrizen müssen $\not\equiv 0 \pmod p$ sein. Diejenigen Matrizen, die (mod p) der Einheitsmatrix kongruent sind, bilden einen Normalteiler $\mathfrak{N}$ von $\mathfrak{G}$, und allgemein bilden die Matrizen, die der Einheitsmatrix (mod p^i) kongruent sind, den Normalteiler $\mathfrak{N}_i$. Die Faktorgruppe $\mathfrak{G}/\mathfrak{N}$ ist offenbar homomorph mit der Gruppe der Matrizen (mod p), ihre Ordnung ist daher $(p^r-1)(p^r-p)(p^r-p^2)\ldots(p^r-p^{r-1})$. Um nun die Faktorgrupe $\mathfrak{N}_i/\mathfrak{N}_{i+1}$ zu bestimmen, müssen wir die Substitutionen von $\mathfrak{N}_i \pmod{p^{i+1}}$ betrachten. Sie haben unter Benützung der Addition von Matrizen (vgl. S. 101) folgende Gestalt: $E + p^i A$, wobei E die Einheitsmatrix und A eine ganz beliebige ganzzahlige Matrix mod p bedeutet. Die Gruppe $\mathfrak{N}_i/\mathfrak{N}_{i+1}$ hat also die Ordnung p^{r^2}. Sind $E + p^i A$ und $E + p^i B$ zwei Matrizen aus $\mathfrak{N}_i$, so ist die zusammengesetzte

$$(E + p^i A)(E + p^i B) \equiv E + p^i(A + B) \pmod{p^{i+1}},$$

d. h. die Gruppe N_i/N_{i+1} ist homomorph mit der additiven Gruppe der Matrizen $A \pmod p$. Diese ist ersichtlich vom Typus $(p, p, \ldots)$ und kann erzeugt werden durch die r^2 Matrizen, die je an einer Stelle 1 stehen haben und sonst überall 0. Wir sprechen das in folgendem Satz aus:

Satz 84: *Die Automorphismengruppe einer Abelschen Gruppe von der Ordnung p^{ar} und vom Typus $(p^a, p^a, \ldots)$ besitzt eine Reihe von a Normalteilen $\mathfrak{N}_1, \mathfrak{N}_2, \ldots, \mathfrak{N}_{a-1}, E$, von denen jeder im vorhergehenden enthalten ist. Die Faktorgruppe $\mathfrak{G}/\mathfrak{N}_1$ ist homomorph mit der Gruppe der Automorphismen der Abelschen Gruppe von der Ordnung p^r und vom Typus $(p, p, \ldots)$, die übrigen Faktorgruppen sind Abelsch von der Ordnung p^{r^2} und vom Typus $(p, p, \ldots)$.*

Ist $E + p^i A$ eine Matrix aus $\mathfrak{N}_i$, so ist ihre p-te Potenz gleich $E + p^{i+1} A + \frac{p(p-1)}{2} p^{2i} A^2 + \ldots$ und für $p > 2$ wird diese Matrix $\equiv E \pmod{p^{i+1}}$, aber nicht $\pmod{p^{i+2}}$, d. h. sie liegt in N_{i+1}, aber nicht mehr in N_{i+2}. Derselbe Schluß gilt noch für $p = 2$ und $i > 1$.

Wir gehen nun über zum allgemeinsten Fall einer *Abel*schen Gruppe von der Ordnung p^n. Sie möge in ihrer Basis n_1 Elemente von der Ordnung p, n_2 von der Ordnung $p^2, \ldots, n_r$ von der Ord-

nung p^r enthalten, so daß $n = n_1 + 2n_2 + \ldots + r n_r$. Die p-ten Potenzen der Basiselemente erzeugen eine charakteristische Untergruppe $\mathfrak{N}$, bestehend aus allen Elementen, welche p-te Potenzen von Elementen sind. Diese Untergruppe wird daher bei allen Automorphismen von $\mathfrak{G}$ in sich selbst transformiert. Wir betrachten die Untergruppe der ganzen Automorphismengruppe $\mathfrak{A}$, bestehend aus denjenigen Automorphismen, die die Elemente von $\mathfrak{N}$ nicht verändern. Sie bildet einen Normalteiler $\mathfrak{A}_1$ von $\mathfrak{A}$ und wir wollen sie näher untersuchen. Bei den Automorphismen von $\mathfrak{A}_1$ werden die Elemente einfach mit Elementen der Ordnung p multipliziert, denn geht S über in S' und setzt man $S' = ST$, so muß nach Erhebung in die p-te Potenz für S und S' dasselbe Element hervorgehen, d. h. es wird $T^p = E$. Allgemein sei $\mathfrak{P}_i$ der Komplex der Basiselemente von der Ordnung p^i. Die Basiselemente aus $\mathfrak{P}_2, \ldots, \mathfrak{P}_r$ darf man mit ganz beliebigen Elementen der Ordnung p multiplizieren, immer erhält man Automorphismen aus $\mathfrak{A}_1$, und diese bilden eine Untergruppe von der Ordnung $p^{(n_1+n_2+\cdots+n_r)(n_2+\cdots+n_r)}$, und zwar ist sie ein Normalteiler von $\mathfrak{A}_1$, denn sie besteht aus allen Automorphismen aus $\mathfrak{A}_1$, welche die sämtlichen Elemente von der Ordnung p, insbesondere diejenigen aus $\mathfrak{P}_1$ ungeändert lassen. Der Typus ist $(p, p, \ldots)$.

Nun betrachten wir die Elemente aus $\mathfrak{P}_1$. Die durch sie erzeugte Gruppe besitzt eine Automorphismengruppe von der Ordnung

$$\psi(n_1) = (p^{n_1} - 1)(p^{n_1} - p)\ldots(p^{n_1} - p^{n_1-1}).$$

Außerdem darf noch jedes dieser Basiselemente mit einem beliebigen der durch $\mathfrak{P}_2, \mathfrak{P}_3, \ldots, \mathfrak{P}_r$ erzeugten Elemente von der Ordnung p multipliziert werden, deren Anzahl zusammen mit E gleich $p^{n_2+\cdots+n_r}$ ist.

Man findet so für die Ordnung von A_1:

$$\psi(n_1) \cdot p^{(2n_1+n_2+\cdots+n_r)(n_2+\cdots+n_r)}.$$

Diese Formel gilt auch für $n_1 = 0$, wenn man $\psi(0) = 1$ setzt.

Hierdurch gelangt man zu einer Rekursionsformel. Die Faktorgruppe $\mathfrak{A}/\mathfrak{A}_1$ ist nämlich homomorph mit der Automorphismengruppe der Gruppe aller p-ten Potenzen von $\mathfrak{G}$, wie leicht ersichtlich ist. Diese kann gleich behandelt werden. Man findet folgendes Resultat:

Satz 85: *$\mathfrak{G}$ sei eine Abelsche Gruppe mit n_i Basiselementen von der Ordnung p^i $(i = 1, 2, \ldots, r)$ und $\mathfrak{A}_i$ sei die Untergruppe der Automorphismengruppe von $\mathfrak{G}$, welche die Elemente, die p^i-te Potenzen von Elementen aus $\mathfrak{G}$ sind, ungeändert läßt, so besitzt die Automorphismengruppe $\mathfrak{A}$ von $\mathfrak{G}$ folgende Reihe von Normalteilern $\mathfrak{A}_r = \mathfrak{A}, \mathfrak{A}_{r-1}, \ldots, \mathfrak{A}_1, E$. Die Faktorgruppe $\mathfrak{A}_i/\mathfrak{A}_{i-1}$ besitzt einen Abelschen Normalteiler vom Typus $(p, p, \ldots)$ und von der Ordnung $p^{(n_i+\cdots+n_r)(n_{i+1}+\cdots+n_r)}$, dessen Index gegeben ist durch $\psi(n_i)\, p^{n_i(n_{i+1}+\cdots+n_r)}$.*

In der Ordnung der Automorphismengruppe gehen also nur solche Primzahlen auf, die eine der Zahlen

$$p,\ p-1,\ p^2-1,\ \ldots,\ p^m-1$$

teilen, wobei m die größte der Zahlen n_i ist.

Zum Schluß soll noch eine praktische Methode zur Herstellung aller Automorphismen *Abel*scher Gruppen angegeben werden. Sie besteht in folgendem Verfahren: Man greift eine Untergruppe $\mathfrak{H}$ heraus und sucht eine Untergruppe von $\mathfrak{G}$, etwa $\mathfrak{G}''$, die homomorph ist mit $\mathfrak{G}/\mathfrak{H}$. Alsdann multipliziert man jedes Element einer Nebengruppe von $\mathfrak{H}$ mit demjenigen Element von $\mathfrak{G}''$, das ihr beim Homomorphismus entspricht. Man beweist leicht, daß jeder Automorphismus auf diesem Weg erhalten wird, aber dieses Verfahren liefert nicht stets Automorphismen, wie sogleich an einem Beispiel gezeigt wird: Wählt man für $\mathfrak{H}$ die Untergruppe E, so wird $\mathfrak{G}''=\mathfrak{G}$. Daher wird jedem Element sein Quadrat zugeordnet. Es ist klar, daß dies dann und nur dann einen Automorphismus ergibt, wenn die Ordnung der Gruppe ungerade ist. Dagegen erhält man stets einen Automorphismus einer *Abel*schen Gruppe, wenn man die Elemente in die s-te Potenz erhebt, sobald s prim ist zur Ordnung der Gruppe.

§ 36. Zerlegbare Gruppen.

Bei unseren Untersuchungen über *Abel*sche Gruppen ergab sich als fundamentaler Satz, daß jede dieser Gruppen das direkte Produkt zyklischer Gruppen ist. Zyklische Gruppen, deren Ordnung eine Primzahlpotenz ist, lassen sich nicht mehr als direktes Produkt von zwei Gruppen, die beide von E verschieden sind, darstellen. Wir wollen eine Gruppe, die nicht das direkte Produkt zweier Gruppen ist, als eine ***unzerlegbare Gruppe*** bezeichnen. Zwei verschiedene Zerlegungen einer *Abel*schen Gruppe als Produkt unzerlegbarer Gruppen haben die Eigenschaft, daß jeder unzerlegbare Faktor der einen Zerlegung homomorph ist mit einem solchen der zweiten. Auf diese Eigenschaft gründeten sich ja die Invarianten der *Abel*schen Gruppen. Im allgemeinen gibt es mehrere Zerlegungen, so besitzt z. B. die *Abel*sche Gruppe vom Typus (p, p) im ganzen $\frac{p(p+1)}{2}$ verschiedene Zerlegungen als Produkt zweier zyklischer Gruppen, wenn man von der Reihenfolge der Faktoren absieht.

Es fragt sich nun, wie die Verhältnisse liegen, wenn es sich um nicht *Abel*sche Gruppen handelt, die direktes Produkt von Gruppen sind. Derartige Gruppen nennen wir ***zerlegbare*** Gruppen, sie lassen sich stets als direktes Produkt unzerlegbarer Gruppen darstellen.

Zunächst behandeln wir als Gegenstück zu den *Abel*schen Gruppen die Gruppen ohne Zentrum und beweisen von ihnen den folgenden

Satz 86: *Eine zerlegbare Gruppe ohne Zentrum läßt sich auf eine und nur eine Weise als Produkt unzerlegbarer Gruppen darstellen, von der Reihenfolge der Faktoren abgesehen.*

Um den Beweis dieses Satzes vorzubereiten, müssen wir zunächst einige einfache Bemerkungen über die direkten Produkte machen. Es sei $\mathfrak{G} = \mathfrak{H}_1 \cdot \mathfrak{H}_2 \dots \mathfrak{H}_n$ eine Zerlegung von $\mathfrak{G}$ in unzerlegbare Faktoren. Dann ist jedes Element von $\mathfrak{H}_i$ mit jedem Element von $\mathfrak{H}_k$ vertauschbar, sobald $i \neq k$, denn die Normalteiler $\mathfrak{H}$ haben außer E kein Element gemeinsam. Jedes Element von $\mathfrak{G}$ läßt sich auf eine und nur eine Weise als Produkt von Elementen aus $\mathfrak{H}_1, \mathfrak{H}_2, \dots, \mathfrak{H}_n$ darstellen. Ist also $H = H_1 \cdot H_2 \dots H_n$, wobei H_i in $\mathfrak{H}_i$ liegt, so sind diese Faktoren $H_1, H_2, \dots$ eindeutig bestimmt durch H. Man nennt H_i den *Konstituenten* von H in $\mathfrak{H}_i$. Selbstverständlich sind die Konstituenten eines Elementes H unter sich und mit dem Element H vertauschbar. Nun seien H und K zwei *vertauschbare* Elemente. Wir können leicht zeigen, daß alsdann auch die Konstituenten dieser Elemente untereinander vertauschbar sind. Es ist nämlich K_1 vertauschbar mit $H_2 \dots H_n$. Transformieren wir nun K mit H, so erhalten wir wiederum K, infolgedessen müssen auch die Konstituenten von K bei der Transformation mit H in sich selbst übergeführt werden. Daher muß K_1 mit H und also auch mit H_1 vertauschbar sein. Nunmehr sind wir in der Lage, unseren Satz zu beweisen.

Es seien 2 Zerlegungen von $\mathfrak{G}$ in unzerlegbare Faktoren gegeben:

$$\mathfrak{G} = \mathfrak{H}_1 \dots \mathfrak{H}_r = \mathfrak{K}_1 \dots \mathfrak{K}_s.$$

Die Konstituenten der Elemente von $\mathfrak{K}_i$ in $\mathfrak{H}_1$ bilden eine Untergruppe von $\mathfrak{H}_1$, denn ist H_1 der Konstituent von K in $\mathfrak{H}_1$ und H'_1 derjenige von K', wobei K und K' in $\mathfrak{K}_i$ liegen, so ist $H_1 H'_1$ derjenige von KK'. Allgemein bilden die Konstituenten der Elemente irgendeiner Untergruppe von $\mathfrak{G}$ in einem unzerlegbaren Faktor eine Untergruppe.

Man betrachte nun der Reihe nach die Konstituenten von $\mathfrak{K}_1, \mathfrak{K}_2, \dots, \mathfrak{K}_s$ in $\mathfrak{H}_1$. Jede ist eine Untergruppe von $\mathfrak{H}_1$ und wir behaupten, daß diese Untergruppen zueinander teilerfremd sind. Sei nämlich H Konstituent in $\mathfrak{H}_1$ eines Elementes K_1 aus $\mathfrak{K}_1$ und eines Elementes K_2 aus $\mathfrak{K}_2$. Da K_1 mit allen Elementen von $\mathfrak{K}_2, \mathfrak{K}_3, \dots, \mathfrak{K}_s$ vertauschbar ist, so gilt dasselbe von seinem Konstituenten H. Weil H aber auch Konstituent von K_2 ist, so ist es auch vertauschbar mit allen Elementen von $\mathfrak{K}_1, \mathfrak{K}_3, \dots$, d. h. H ist mit allen Elementen von $\mathfrak{K}_1, \dots, \mathfrak{K}_s$ und also auch mit allen Elementen von $\mathfrak{G}$ vertauschbar. Hieraus folgt, daß unter unserer Voraussetzung über $\mathfrak{G}$ für H nur E in Betracht kommen kann. Sind nun $\overline{\mathfrak{H}}_1, \dots, \overline{\mathfrak{H}}_s$ die Konstituenten von $\mathfrak{K}_1, \dots, \mathfrak{K}_s$ in $\mathfrak{H}_1$, so sind die Untergruppen $\overline{\mathfrak{H}}_i$ zu je zweien teilerfremd. Ferner ist jedes Element der einen mit jedem Element jeder anderen vertauschbar. $\mathfrak{H}$ muß nun identisch sein mit

dem direkten Produkt $\overline{\mathfrak{H}}_1 \cdot \ldots \cdot \overline{\mathfrak{H}}_s$, denn jedes Element H von $\mathfrak{H}$ ist Produkt seiner Konstituenten in $\mathfrak{K}_1, \ldots, \mathfrak{K}_s$, also Produkt von Elementen aus $\overline{\mathfrak{H}}_1, \ldots, \overline{\mathfrak{H}}_s$. Weil $\mathfrak{H}_1$ unzerlegbar ist, so muß $\mathfrak{H}$ mit einer der Untergruppen $\overline{\mathfrak{H}}_i$ übereinstimmen, während die übrigen nur aus dem Element E bestehen. Hieraus folgt, daß $\mathfrak{H}_1$ in einem der unzerlegbaren Faktoren $\mathfrak{K}_1, \ldots, \mathfrak{K}_s$ enthalten ist, etwa in $\mathfrak{K}_1$, während es mit den übrigen teilerfremd ist. Genau dasselbe kann man nun für $\mathfrak{K}_1$ zeigen: $\mathfrak{K}_1$ ist in einer der Gruppen $\mathfrak{H}_i$ enthalten, während die übrigen zu $\mathfrak{K}_1$ teilerfremd sind. Diese Gruppe muß also $\mathfrak{H}_1$ sein. Nimmt man die beiden Resultate zusammen, so folgt $\mathfrak{K}_1 = \mathfrak{H}_1$. Indem man den Satz weiter anwendet, erkennt man, daß jeder Faktor $\mathfrak{H}$ mit einem der Faktoren $\mathfrak{K}$ übereinstimmt, womit der Satz bewiesen ist.

Um den allgemeinen Fall zu behandeln, stellen wir folgende Definition auf.

Definition: Zwei homomorphe Untergruppen $\mathfrak{H}$ und $\mathfrak{H}'$ einer Gruppe heißen ***zentral homomorph***, wenn es eine homomorphe Zuordnung $X \rightarrow X'$ der Elemente von $\mathfrak{H}$ und $\mathfrak{H}'$ gibt, derart, daß XX'^{-1} zum Zentrum der Gruppe gehört.

Falls die Gruppen $\mathfrak{H}$ und $\mathfrak{H}'$ nicht *Abel*sch sind, so besitzen sie einen Normalteiler gemeinsam, dessen Faktorgruppe *Abel*sch ist, denn setzt man $X' = XA$, so gehört A zum Zentrum und die sämtlichen Multiplikatoren A, die auftreten, wenn X' alle Elemente von $\mathfrak{N}'$ durchläuft, bilden eine *Abel*sche Gruppe, die mit $\mathfrak{H}$ und $\mathfrak{H}'$ isomorph ist. Diejenigen Elemente, für die $X = X'$ ist, entsprechen dem Einheitselement derselben.

Der von *Maclagan-Wedderburn*[1]) aufgestellte und von *Remak*[2]) zuerst vollständig bewiesene Satz lautet nun:

Satz 87: *Sind zwei verschiedene Zerlegungen einer Gruppe in unzerlegbare Gruppen gegeben, so ist die Anzahl der Faktoren gleich und zu jedem Faktor der einen Zerlegung gibt es einen Faktor der anderen, der mit ihm zentral homomorph ist.*

Beweis[3]): Es sei

$$\mathfrak{G} = \mathfrak{H}_1 \cdot \mathfrak{H}_2 \ldots \mathfrak{H}_r = \mathfrak{K}_1 \cdot \mathfrak{K}_2 \ldots \mathfrak{K}_s .$$

Wenn wir zeigen können, daß zwei nicht *Abel*sche Faktoren, etwa $\mathfrak{H}_1$ und $\mathfrak{K}_1$ zentral homomorph sind, so ist der Satz sofort be-

[1]) *Maclagan-Wedderburn:* On the Direct Product in the theory of finite groups (Ann. of Math., 2nd ser., **10**, S. 173).

[2]) *Remak, R.;* Crelles Journ. 139, S. 293, und: Über die Zerlegung der endlichen Gruppen in direkte unzerlegbare Faktoren, Sitzungsber. der physikomath. Gesellschaft zu Kiew, 1913.

[3]) Dieser Beweis stammt von O. Schmidt (Sur les produits directes Bull. de la Soc. math. de France **41**, S. 161).

wiesen, unter Anwendung vollständiger Induktion. Denn seien $\mathfrak{H}_1^c$ und $\mathfrak{K}_1^c$ die Zentren von $\mathfrak{H}_1$ und $\mathfrak{K}_1$, so wird

$$\mathfrak{H}_1^c \cdot \mathfrak{H}_2 \dots \mathfrak{H}_r = \mathfrak{K}_1^c \cdot \mathfrak{K}_2 \dots \mathfrak{K}_s$$

und da diese Gruppe von niedrigerer Ordnung als $\mathfrak{G}$ ist, so kann man für sie das Theorem voraussetzen. Die Zentren sind in beiden Fällen dieselben.

Alles kommt also darauf an, zwei zentral homomorphe Faktoren aufzufinden, die nicht *Abel*sch sind. Es sei $\mathfrak{H}_1$ ein nicht *Abel*scher Faktor unserer Zerlegungen von *größter Ordnung*.

1. Fall: *Die erste Zerlegung enthält außer* $\mathfrak{H}_1$ *noch einen nicht Abelschen Faktor.* Die Konstituenten von $\mathfrak{H}_1$ in $\mathfrak{K}_i$ bilden eine Untergruppe $\mathfrak{K}_i'$ von $\mathfrak{K}_i$. Das direkte Produkt dieser Untergruppen enthält $\mathfrak{H}_1$ und enthält daher den Faktor $\mathfrak{H}_1$:

$$\mathfrak{K}_1' \cdot \mathfrak{K}_2' \dots \mathfrak{K}_s' = \mathfrak{H}_1 \cdot \mathfrak{H} = \mathfrak{G}'.$$

Alle Elemente von $\mathfrak{H}$ sind mit denjenigen von $\mathfrak{H}_1$ vertauschbar und daher auch mit deren Konstituenten, den Elementen von $\mathfrak{K}_1', \mathfrak{K}_2', \dots, \mathfrak{K}_s'$. Also gehört $\mathfrak{H}$ zum Zentrum von

$$\mathfrak{H}_1 \cdot \mathfrak{H} = \mathfrak{G}'$$

und diese Gruppe ist eigentliche Untergruppe von $\mathfrak{G}$, da sie nur *einen* nicht *Abel*schen Faktor $\mathfrak{H}_1$ enthält. $\mathfrak{H}_1$ ist daher zentral homomorph mit einem Faktor $\mathfrak{K}_i'$ von $\mathfrak{G}'$. Da aber $\mathfrak{H}_1$ von höchster Ordnung ist, so muß dieser Faktor mit einer der Gruppen $\mathfrak{K}_i$ selber übereinstimmen, womit der Satz im ersten Fall bewiesen ist.

2. Fall: $\mathfrak{H}_1$ *ist der einzige nicht Abelsche Faktor der ersten Zerlegung.* Es sei $\mathfrak{K}_1$ ein nicht *Abel*scher Faktor der zweiten Zerlegung und $\mathfrak{H}_1', \mathfrak{H}_2', \dots, \mathfrak{H}_r'$ seien die Untergruppen seiner Konstituenten in $\mathfrak{H}_1, \dots, \mathfrak{H}_r$. Wiederum wird

$$\mathfrak{H}_1' \cdot \mathfrak{H}_2' \dots \mathfrak{H}_r' = \mathfrak{K}_1 \cdot \mathfrak{K} = \mathfrak{G}'.$$

Wenn $\mathfrak{H}'_1 = \mathfrak{H}_1$, so ist $\mathfrak{H}_1$ zentral homomorph mit $\mathfrak{K}_1$, denn die übrigen $\mathfrak{H}_i$ $(i > 1)$ gehören zum Zentrum und $\mathfrak{H}_1$ ist von größter Ordnung.

Wenn $\mathfrak{H}_1'$ eigentliche Untergruppe von $\mathfrak{H}_1$ ist, so ist auch $\mathfrak{G}'$ nicht identisch mit $\mathfrak{G}$ und $\mathfrak{K}_1$ wird zentral homomorph mit einer Untergruppe $\mathfrak{H}_1''$ von $\mathfrak{H}_1'$ (Fall 1). Da aber die Ordnung von $\mathfrak{H}_1'$ höchstens gleich der Ordnung von $\mathfrak{K}_1$ ist, so wird $\mathfrak{H}_1'' = \mathfrak{H}_1'$. In gleicher Weise betrachten wir die Komponente von $\mathfrak{H}_1'$ in $\mathfrak{K}_1$ und finden, daß sie zentral homomorph mit $\mathfrak{H}_1'$ ist, also mit $\mathfrak{K}_1$ selber übereinstimmt. Daraus folgt nun weiter, daß in der zweiten Zerlegung $\mathfrak{K}_1 \cdot \mathfrak{K}_2 \dots \mathfrak{K}_s$ der erste Faktor $\mathfrak{K}_1$ durch $\mathfrak{H}_1'$ ersetzt werden kann, und wir erhalten

$$\mathfrak{K}_1 \cdot \mathfrak{K}_2 \dots \mathfrak{K}_s = \mathfrak{H}_1' \ \mathfrak{K}_2 \dots \mathfrak{K}_s = \mathfrak{H}_1 \cdot \mathfrak{H}_2 \dots \mathfrak{H}_r = \mathfrak{G}.$$

Da $\mathfrak{H}_1'$ Untergruppe von $\mathfrak{H}_1$ ist, so folgt aus der mittleren Zerlegung, daß

$$\mathfrak{H}_1 = \mathfrak{H}_1' \cdot \mathfrak{K}$$

wird, wo $\mathfrak{K}$ der gemeinsame Teiler von $\mathfrak{H}_1$ mit $\mathfrak{K}_2 \cdot \mathfrak{K}_3 \ldots \mathfrak{K}_s$ ist. Da $\mathfrak{H}_1$ unzerlegbar ist, so wird $\mathfrak{K} = E$ und $\mathfrak{H}_1 = \mathfrak{H}_1'$ zentral homomorph mit $\mathfrak{K}_1$.

Aus der Bemerkung auf S. 88 folgt, *daß die Kommutatorgruppe bei sämtlichen Zerlegungen die nämliche Zerlegung erfährt.* Wir machen hier auf einen eigentümlichen ***Dualismus*** zwischen dem Zentrum und der Faktorgruppe des Kommutators aufmerksam, den man am deutlichsten durch Herbeiziehung des Körperbegriffs klar machen kann:

Zwei Zerlegungen einer Gruppe in unzerlegbare teilerfremde Faktoren unterscheiden sich nur in der Verteilung des Zentrums.

Zwei verschiedene Arten, einen *Galois*schen Körper aus unzerlegbaren teilerfremden *Galois*schen Körpern zusammenzusetzen, unterscheiden sich nur in der Verteilung der Unterkörper mit *Abel*scher Gruppe.

Beide Sätze drücken im nicht *Abel*schen Fall zwei völlig verschiedene Eigenschaften aus.

Beispielsweise lautet der zu Satz 86 duale so:

Eine Gruppe, die mit ihrer Kommutatorgruppe identisch ist, läßt sich auf eine und nur eine Weise in unzerlegbare Faktoren zerlegen.

9. Kapitel.

Monomiale Gruppen.

§ 37. Monomiale Gruppen.

Eine wichtige Verallgemeinerung der Permutationsgruppen bilden die *monomialen Gruppen.* Sie mögen gleichzeitig hier als Übergang zu den allgemeinen linearen Substitutionsgruppen dienen.

Definition: Eine ***monomiale Substitution*** von n Variablen geht aus einer Permutation hervor, wenn die Variablen noch mit einem Faktor versehen werden.

Ist dieser Faktor in allen Fällen gleich 1, so ist die Substitution eine Permutation. Wir definieren nun die Zusammensetzung zweier solcher Substitutionen: Wenn bei der ersten, P, die Variable x_h übergeführt wird in $a\,x_i$, bei der zweiten, Q, x_i in $b\,x_k$, so wird die zusammengesetzte Substitution PQ die Variable x_h überführen in $a\,b\,x_k$. Als Beispiel geben wir die folgende Substitution an: $\begin{pmatrix} x_1 & x_2 \\ a\,x_2 & \frac{1}{a}\,x_1 \end{pmatrix}$. Übt man die Substitution zweimal aus, so erhält man die identische Substitution, welche x_1 und x_2 in sich selbst überführt. a kann hierbei als eine beliebige reelle oder komplexe von 0 verschiedene Zahl angenommen werden.

Definition: Unter einer ***monomialen Gruppe*** versteht man ein System von monomialen Substitutionen, die nach der angegebenen Zusammensetzung eine Gruppe bilden.

Zu jeder monomialen Substitution gehört eine bestimmte Permutation der n Variablen, die man dadurch erhält, daß man die Faktoren gleich 1 setzt. Ordnet man jeder Substitution die entsprechende Permutation zu, so bilden diese letzteren eine mit der monomialen Gruppe isomorphe Permutationsgruppe. Der identischen Permutation entsprechen hierbei diejenigen Substitutionen, welche die Variablen bloß mit einem Faktor versehen, sie aber nicht permutieren. Hieraus folgt der

Satz 88: *Diejenigen Substitutionen einer monomialen Gruppe, welche die Variablen nicht permutieren, bilden einen Abelschen Normalteiler.*

Daß nämlich zwei derartige Substitutionen miteinander vertauschbar sind, ist ohne weiteres ersichtlich, weil die Multiplikation von Zahlen dem kommutativen Gesetz gehorcht.

Wir haben oben gesagt, daß die Faktoren beliebige Zahlen sein können, aber wir müssen nun bedeutende Einschränkungen machen. Die Substitution P möge x_1 in $a\,x_1$ überführen. Ihre Ordnung sei n, dann bleibt x_1 bei P^n ungeändert. Andererseits sieht man, daß diese selbe Potenz x_1 in $a^n x_1$ überführt, und hieraus folgt, daß $1 = a^n$ also a eine n-te Einheitswurzel ist. Dieser Satz läßt sich noch weiter verallgemeinern. Man kann monomiale Substitutionen in Zyklen zerlegen, ähnlich wie die Permutationen. Man beginnt zu dem Zweck mit einer Variablen, z. B. x_1 und sucht, in welche neue Variable sie übergeht. Mit dieser neuen Variablen verfährt man gleich und kommt schließlich zu der alten mit einem Faktor versehenen Variablen zurück. Als Beispiel nehmen wir die folgende Substitution:

$$\begin{pmatrix} x_1 & x_2 & x_3 \\ a\,x_2 & b\,x_3 & c\,x_1 \end{pmatrix}.$$

Diese bildet einen dreigliedrigen Zyklus. Wir bilden nun ihre dritte Potenz. Man sieht, daß sie keine Permutation der Variablen bewirkt, sondern bloß eine Multiplikation der sämtlichen Variablen mit $a \cdot b \cdot c$. Ist nun die Ordnung der Substitution $3n$, so muß $a\,b\,c$ genau eine n-te Einheitswurzel sein. Hieraus folgt nun der

Satz 89: *Bilden die Variablen einer Substitution einen r-gliederigen Zyklus in der zugehörigen Permutation, so ist das Produkt der auftretenden Faktoren eine Einheitswurzel. Die Ordnung der Substitution ist rn, wobei n die Ordnung dieser Einheitswurzel bedeutet.*

Wir betrachten von jetzt an nur transitive Substitutionsgruppen d. h. solche, bei denen die Variable x_1 in eine beliebige andere mit einem Faktor versehene Variable überführt werden kann.

Diejenigen Substitutionen, welche eine bestimmte Variable x_1 nicht permutieren, sondern nur mit einem Faktor versehen, bilden eine Untergruppe $\mathfrak{K}$, deren Index gleich der Anzahl der Variablen ist.

Unter den Substitutionen von $\mathfrak{K}$ hinwiederum bilden diejenigen, welche x_1 in x_1 überführen (für welche der Faktor 1 ist), eine Untergruppe $\mathfrak{H}$. $\mathfrak{H}$ ist Normalteiler von $\mathfrak{K}$ und die Faktorgruppe $\mathfrak{K}/\mathfrak{H}$ ist zyklisch. Denn jede Substitution von $\mathfrak{K}$ wird x_1 mit einem Faktor versehen, und dieser Faktor ist nach Satz 89 eine Einheitswurzel. Man kann daher jeder Substitution von $\mathfrak{K}$ diese Substitution von x_1 zuordnen und erhält so eine mit $\mathfrak{K}$ isomorphe Gruppe von Substitutionen einer Variablen. Der identischen Substitution entsprechen hierbei die Substitutionen von $\mathfrak{H}$. Nun ist aber eine Substitutionsgruppe in einer Variablen stets zyklisch, denn ist n ein Teiler der Ordnung, so gibt es genau n Substitutionen, deren n-te Potenz die identische Substitution ist, nämlich $x' = \varepsilon^i x$ $(i = 0, 1, \ldots, n-1)$, wobei ε eine n-te Einheitswurzel ist. Es kann daher nicht zwei zyklische Untergruppen von derselben Ordnung geben, und hieraus folgt nach den Sätzen über *Abel*sche Gruppen unsere Behauptung.

Wir wollen nun zeigen, wie man zu einer gegebenen Gruppe monomiale Darstellungen findet. Sei P ein Element von der Ordnung n und $\mathfrak{P}$ die durch P erzeugte zyklische Gruppe. Ferner sei die Gruppe $\mathfrak{G}$ in Nebengruppen zerlegt:

$$\mathfrak{G} = \mathfrak{P} + \mathfrak{P}T_2 + \ldots + \mathfrak{P}T_m.$$

Wir bilden jetzt die folgenden Ausdrücke:

$$E + \varepsilon P + \varepsilon^2 P^2 + \ldots + \varepsilon^{n-1} P^{n-1},$$
$$E + \varepsilon P + \varepsilon^2 P^2 + \ldots + \varepsilon^{n-1} P^{n-1})T_2 = T_2 + \varepsilon P T^2 + \ldots + \varepsilon^{n-1} P^{n-1} T_2,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$(E + \varepsilon P + \ldots + \varepsilon^{n-1} P^{n-1})T_m,$$

wobei ε eine beliebige n-te Einheitswurzel bedeutet.

Multipliziert man den ersten Ausdruck rechts mit P^r, so reproduziert er sich mit dem Faktor ε^{-r} versehen. Um nun zu untersuchen, was bei der Multiplikation mit dem beliebigen Element T aus den Ausdrücken wird, betrachten wir das bestimmte Beispiel:

$$(E + \varepsilon P + \ldots + \varepsilon^{n-1} P^{n-1})T_i T.$$

Wir setzen $T = T_i^{-1} U$ und suchen diejenige Nebengruppe von $\mathfrak{P}$ aus, die U enthält. Sei $U = P^r T_k$, dann wird das Produkt zu:

$$\varepsilon^{-r}(E + \varepsilon P + \ldots + \varepsilon^{n-1} P^{n-1})T_k.$$

Die rechtsseitige Multiplikation mit T hat also zur Folge, daß die oben gebildeten Ausdrücke untereinander vertauscht und mit einem Faktor versehen werden, d. h. *sie erfahren eine monomiale Substitution.*

Man kann noch allgemeinere Darstellungen definieren. Sei $\mathfrak{K}$ irgendeine Untergruppe von $\mathfrak{G}$, die einen Normalteiler $\mathfrak{H}$ mit zyklischer Faktorgruppe besitzt. Ferner sei

$$\mathfrak{G} = \mathfrak{K} + \mathfrak{K}T_2 + \ldots + \mathfrak{K}T_m$$

und

$$\mathfrak{K} = \mathfrak{H} + \mathfrak{H}P + \ldots + \mathfrak{H}P^{n-1}.$$

Wir bilden die ähnlich wie früher gebauten Ausdrücke:

$$\begin{aligned}
&\mathfrak{H} + \varepsilon\mathfrak{H}P + \ldots + \varepsilon^{n-1}\mathfrak{H}P^{n-1}\\
&(\mathfrak{H} + \varepsilon\mathfrak{H}P + \ldots + \varepsilon^{n-1}\mathfrak{H}P^{n-1})\,T_2\\
&\cdots\cdots\cdots\cdots\\
&\cdots\cdots\cdots\cdots
\end{aligned}$$

Multipliziert man sie rechts mit T, so erfahren auch sie eine monomiale Substitution; denn sei wiederum $T = T_i^{-1}U$ und $U = KT_k$ schließlich $K = HP^r$, wobei H ein Element aus $\mathfrak{H}$ bedeutet, so wird:

$$\begin{aligned}
&(\mathfrak{H} + \varepsilon\mathfrak{H}P + \ldots + \varepsilon^{n-1}\mathfrak{H}P^{n-1})\,T_iT\\
&= \varepsilon^{-r}(\mathfrak{H} + \varepsilon\mathfrak{H}P + \ldots + \varepsilon^{n-1}\mathfrak{H}P^{n-1})\,T_k.
\end{aligned}$$

Rechtsseitige Multiplikation mit T wird also auch diese Ausdrücke mit einem Faktor versehen und untereinander vertauschen, da sie ja aus den Elementen je einer Nebengruppe von $\mathfrak{K}$ gebildet sind. Man erhält so wiederum eine monomiale Darstellung von $\mathfrak{G}$ und zeigt leicht, daß die identische Substitution von denjenigen Elementen geliefert wird, die $\mathfrak{H}$ und seinen konjugierten Gruppen gemeinsam sind. Ist also $\mathfrak{N}$ der größte in $\mathfrak{H}$ enthaltene Normalteiler von $\mathfrak{G}$, so ist die monomiale Darstellung homomorph mit $\mathfrak{G}/\mathfrak{N}$.

§ 38. Ein Satz von *Burnside*.

Die monomialen Gruppen lassen sich verwenden, um äußerst wichtige Sätze über die Existenz von Normalteilern von Gruppen zu beweisen. Bildet man nämlich das Produkt der n Variablen, so wird es durch jede monomiale Substitution in sich selbst übergeführt und mit einem Faktor versehen, d. h. dieses Produkt erfährt selbst eine monomiale Substitution von einer Variablen. Der auftretende Faktor ist das Produkt der in der ursprünglichen Substitution auftretenden Faktoren. Diejenigen Substitutionen, bei denen das Produkt gleich 1 ist, bilden einen Normalteiler der ganzen Gruppe, dessen Faktorgruppe zyklisch ist. Kann man daher von irgendeiner Gruppe $\mathfrak{G}$ eine monomiale Darstellung angeben mit einer Substitution, bei der das Produkt der Faktoren nicht gleich 1 ist, so ist die Kommutatorgruppe von $\mathfrak{G}$ eine eigentliche Untergruppe.

Satz 90[1]: *Ist eine Sylowgruppe von der Ordnung p^a im Zentrum ihres Normalisators enthalten, so enthält die Gruppe einen Normalteiler von Index p^a.*

Beweis: Sei $\mathfrak{P}$ die *Sylow*gruppe; sie ist *Abel*sch. Ihr Typus sei $(p^{a_1}, \ldots, p^{a_r})$ und eine Basis $P_1, \ldots, P_r$. Jedes Element der Gruppe, das mit $\mathfrak{P}$ vertauschbar ist, ist mit jedem Element von $\mathfrak{P}$ vertauschbar. Wir bilden nun die durch $P_2, \ldots, P_r$ erzeugte Untergruppe $\mathfrak{Q}$ von $\mathfrak{P}$. Sie ist Normalteiler mit zyklischer Faktorgruppe und vom Index p^{a_1}. Nunmehr bilden wir die durch diese beiden Gruppen erzeugte monomiale Gruppe und daher die Ausdrücke:

$$(\mathfrak{Q} + \varepsilon \mathfrak{Q} P_1 + \ldots + \varepsilon^{p^{a_1}-1} \mathfrak{Q} P_1^{p^{a_1}-1}) T_i \qquad \varepsilon^{p^{a_1}} = 1,$$

wobei T_i Repräsentanten der Nebengruppen der *Sylow*gruppe sind und $T_1 = E$ gesetzt sein mag.

Zunächst ist zu untersuchen, welche dieser Ausdrücke bei der Multiplikation mit P_1 bloß mit einem Faktor versehen werden. Dies ist gewiß mit dem ersten der Fall, der den Faktor ε^{-1} erhält. Wenn der i-te Ausdruck den Faktor α erhält, so muß P_1 in der Gruppe $T_i^{-1} \mathfrak{P} T_i$ enthalten sein; nach Satz 49 ist dann P_1 mit T_i vertauschbar, denn $T_i P_1 T_i^{-1}$ ist in $\mathfrak{P}$, wenn P_1 in $T_i^{-1} \mathfrak{P} T_i$ ist. Infolgedessen ist der Faktor ebenfalls ε^{-1}. Die Anzahl der Ausdrücke, die bloß einen Faktor erhalten, ist gleich dem Index von $\mathfrak{P}$ unter der Gruppe der mit P_1 vertauschbaren Elemente, also eine zu p prime Zahl q. Alle übrigen Ausdrücke erfahren eine Permutation. Das Produkt der bei diesen letzteren auftretenden Faktoren ist höchstens eine p^{a_1-1}te Einheitswurzel (Satz 89). Daher ist das Produkt sämtlicher Faktoren genau eine p^{a_1}-te Einheitswurzel. Hieraus folgt, daß $\mathfrak{G}$ einen Normalteiler enthält mit zyklischer Faktorgruppe von der Ordnung p^{a_1}. Die Gruppe $\{P_1\}$ ist teilerfremd zum Normalteiler. Genau denselben Satz kann man für jedes Basiselement P_i beweisen, und der Durchschnitt aller der so nachgewiesenen Normalteiler besitzt eine zu p prime Ordnung, und sein Index ist gleich der Ordnung der *Sylow*gruppe, womit der Satz bewiesen ist.

Eine Fülle von wichtigen Folgerungen lassen sich aus diesem Satz ableiten.

Satz 91: *Eine Gruppe, deren Ordnung Produkt von lauter verschiedenen Primfaktoren ist, ist auflösbar, und besitzt einen Normalteiler, dessen Index dem kleinsten Primfaktor gleich ist.*

Ist also die Ordnung von $\mathfrak{G}$ gegeben durch $g = p_1 p_2 \ldots p_r$ und $p_i > p_{i-1}$, so gibt es eine Hauptreihe für $\mathfrak{G}$ von der Gestalt $\mathfrak{G}, \mathfrak{G}_1, \ldots, \mathfrak{G}_r = E$. Der Index von $\mathfrak{G}_i$ unter $\mathfrak{G}_{i-1}$ ist p_i.

[1]) *Burnside*: Theory of groups, S. 327.

Beweis: Die *Sylow*gruppe von der Ordnung p_1 ist zyklisch und die Gruppe ihrer Automorphismen ebenfalls zyklisch und von der Ordnung $p_1 - 1$. Nun ist aber p_1 die kleinste Primzahl, die in g aufgeht, daher kann ein Automorphismus dieser *Sylow*gruppe, der durch Transformation mit einem Element von $\mathfrak{G}$ hervorgerufen wird, nur der identische sein. Die *Sylow*gruppe ist also im Zentrum ihres Normalisators enthalten und infolgedessen enthält $\mathfrak{G}$ einen Normalteiler vom Index p_1. Daß auch $\mathfrak{G}_i$ Normalteiler von $\mathfrak{G}$ ist, folgt daraus, daß $\mathfrak{G}_i$ charakteristische Untergruppe von $\mathfrak{G}_{i-1}$ ist.

Satz 92: *Bezeichnet $\mathfrak{P}$ eine Sylowgruppe von $\mathfrak{G}$, deren Ordnung p^a ist, und ist jedes Element von $\mathfrak{G}$, dessen Ordnung zu p prim ist, mit jedem Element von $\mathfrak{P}$ vertauschbar, so ist $\mathfrak{G}$ das direkte Produkt von $\mathfrak{P}$ und einer Untergruppe, deren Ordnung zu p prim ist.*

Beweis: $\mathfrak{P}$ ist jedenfalls Normalteiler von $\mathfrak{G}$. Wenn $\mathfrak{P}$ *Abel*sch ist, so ist $\mathfrak{P}$ im Zentrum von $\mathfrak{G}$ enthalten, und wir haben offenbar den Fall des Satzes von *Burnside*. Dann enthält $\mathfrak{G}$ einen Normalteiler vom Index p^a und ist daher das direkte Produkt dieses Normalteilers und $\mathfrak{P}$.

Wenn $\mathfrak{P}$ nicht *Abel*sch ist, so bezeichne $\mathfrak{P}_1$ die Kommutatorgruppe von $\mathfrak{P}$. Sie ist als charakteristische Untergruppe auch Normalteiler von $\mathfrak{G}$. Die Gruppe $\mathfrak{G}/\mathfrak{P}_1$ genügt der Bedingung für den vorhin behandelten Fall, nämlich $\mathfrak{P}/\mathfrak{P}_1$ ist in ihrem Zentrum enthalten. Daher enthält $\mathfrak{G}$ einen Normalteiler, dessen Index gleich der Ordnung von $\mathfrak{P}/\mathfrak{P}_1$ ist. In diesem Normalteiler ist $\mathfrak{P}_1$ als *Sylow*gruppe enthalten, und man kann nun auf ihn dasselbe Verfahren anwenden. Man erhält so schließlich einen Normalteiler vom Index p^a und $\mathfrak{G}$ ist infolgedessen das direkte Produkt dieses Normalteilers und $\mathfrak{P}$.

Satz 93: *Die Ordnung einer einfachen Gruppe ist stets durch das Quadrat ihres kleinsten Primfaktors teilbar,* denn sonst wäre die *Sylow*gruppe, die zu diesem kleinsten Primfaktor gehört, im Zentrum ihres Normalisators enthalten und die Gruppe wäre verschieden von ihrer Kommutatorgruppe.

Hieraus läßt sich leicht beweisen, daß *die Ordnung einer einfachen Gruppe, falls sie gerade ist, stets durch* 4 *teilbar sein muß und, falls sie durch* 4, *aber nicht durch* 8 *teilbar ist, stets den Teiler* 12 *hat.* Denn in diesem letzteren Fall ist die *Sylow*gruppe von der Ordnung 4 *Abel*sch. Sie muß vom Typus (2, 2) sein, da ihr Normalisator einen vom identischen verschiedenen Automorphismus von ungerader Ordnung liefern muß. Dies ist im zyklischen Falle nicht möglich, dagegen im andern Falle gibt es einen Automorphismus von der Ordnung 3. Die Ordnungen aller bisher bekannten einfachen Gruppen sind durch 12 teilbar.

Mit Hilfe des Satzes 93 kann man zeigen, daß es nur eine einfache Gruppe von der Ordnung 60 gibt, denn hier muß die *Sylow*-

gruppe von der Ordnung 4 als Normalisator eine Gruppe von der Ordnung 12 haben, deren Typus leicht bestimmt werden kann. Sind nämlich P und Q die Basiselemente der *Sylow*gruppe, so daß

$$P^2 = E,\ Q^2 = E,\ PQ = QP$$

und ist ferner R von der Ordnung 3, so gelten die Beziehungen:

$$R^{-1}PR = Q,\ R^{-1}QR = PQ.$$

Da die einfache Gruppe diese Untergruppe vom Index 5 besitzt, so kann sie als Permutationsgruppe von 5 Variablen dargestellt werden und ist daher mit der alternierenden Gruppe von 5 Variablen identisch.

§ 39. Herstellung sämtlicher monomialer Gruppen.

Aus jeder monomialen Gruppe kann man beliebig viele weitere bilden durch Einführung neuer Variabler in folgender Weise:

Man setze

$$y_1 = a_1 x_1, \ldots, y_n = a_n x_n.$$

Wird bei einer beliebigen Substitution x_i übergeführt in εx_i, so geht $a_i x_i$ über in $a_i \varepsilon x_i$, d. h. y_i wird ebenfalls in εy_i übergeführt. Geht dagegen x_i über in $a x_k$, so geht $a_i x_i$ über in $a_i a x_k$, d. h. y_i wird übergeführt in $a \cdot \frac{a_i}{a_k} y_k$. Auch die Variablen y erfahren also eine monomiale Substitution, man nennt sie eine mit der ursprünglichen ***äquivalente*** Gruppe.

Wir betrachten nur transitive Gruppen und wollen nun untersuchen, ob man durch eine geeignete Transformation eine besonders einfache Gestalt derselben erhalten kann. Wiederum sei $\mathfrak{H}$ die Untergruppe derjenigen Substitutionen, die x_1 ungeändert lassen, $\mathfrak{K}$ möge diejenigen Substitutionen bezeichnen, die x_1 bloß mit einem Faktor versehen. Dann ist $\mathfrak{H}$ Normalteiler von $\mathfrak{K}$ und die Faktorgruppe $\mathfrak{K}/\mathfrak{H}$ ist zyklisch. Ihre Ordnung sei n. Der auftretende Faktor ist dann stets eine n-te Einheitswurzel. Nun sei die Zerlegung von $\mathfrak{G}$ in Nebengruppen von $\mathfrak{K}$:

$$\mathfrak{G} = \mathfrak{K} + \mathfrak{K} T_2 + \ldots + \mathfrak{K} T_r,$$

diejenige von $\mathfrak{K}$ nach $\mathfrak{H}$:

$$\mathfrak{K} = \mathfrak{H} + \mathfrak{H} P + \ldots + \mathfrak{H} P^{n-1}.$$

In der Substitution T_i möge x_1 übergeführt werden in $a_i x_i$, dann führen wir als neue Variable ein $y_i = a_i x_i$ für jeden Wert von $i = 2, 3, \ldots, r$. Alsdann wird jede Substitution der Gruppe $x_1 = y_1$ überführen in $\varepsilon^j y_l$, wobei j einen der Indizes $1, \ldots, n$ und ε eine n-te Einheitswurzel bedeutet, während l von 1 bis r läuft.

Wir bilden nunmehr die Ausdrücke

$$(\mathfrak{H} + \varepsilon \mathfrak{H} P + \ldots + \varepsilon^{n-1} \mathfrak{H} P^{n-1}) T_i \quad (i = 1, 2, \ldots r)$$

und behaupten, daß unsere monomiale Gruppe identisch ist mit der durch rechtsseitige Multiplikation dieser Ausdrücke entstehenden monomialen Darstellung.

Zum Beweis betrachten wir eine beliebige Substitution U der Gruppe. Sie möge y_i überführen in $a\,y_k$. Dann wird $T_i U$ die Variable y_1 in $a\,y_k$ überführen. Hieraus folgt, daß a eine Potenz von ε, etwa ε^{-l} ist. $T_i U$ läßt sich infolgedessen in der Gestalt schreiben $H P^l T_k$, wobei H in $\mathfrak{H}$ ist. Es wird also

$$U = T_i^{-1} H P^l T_k.$$

Multiplizieren wir nun andererseits den i-ten unserer Ausdrücke, der der Variablen y_i zugeordnet ist, mit U, so erhalten wir

$$(\mathfrak{H} + \varepsilon\mathfrak{H}P + \ldots) T_i (T_i^{-1} H P^l T_k) = \varepsilon^{-l} (\mathfrak{H} + \varepsilon\mathfrak{H}P + \ldots) T_k.$$

Hiermit ist gezeigt, daß die rechtsseitige Multiplikation mit U gerade diejenige monomiale Substitution erzeugt, welche in der monomialen Gruppe mit U bezeichnet worden ist. Wir fassen das Resultat in den folgenden Satz zusammen:

Satz 94: *Jede transitive monomiale Gruppe läßt sich so transformieren, daß sie mit einer durch Untergruppen nach der Methode von § 37 erzeugten monomialen Gruppe identisch ist.*

Insbesondere ergibt sich hieraus, *daß es zu jeder monomialen Gruppe eine äquivalente gibt, deren Faktoren sämtlich Einheitswurzeln sind.*

10. Kapitel.

Darstellung der Gruppen durch lineare homogene Substitutionen.

Die folgende Theorie der Darstellungen von Gruppen durch Substitutionen ist bei weitem das wichtigste und am weitesten entwickelte Gebiet der Gruppentheorie. Sie ist von *G. Frobenius* geschaffen worden und hängt aufs engste zusammen mit der Theorie der hyperkomplexen Größen, in der namentlich *Molien* (Math. Ann. **41** und **42**) grundlegende Resultat erzielt hatte. Die Arbeiten von *Frobenius* aus diesem Gebiet sind sämtlich in den Berliner Berichten erschienen und wir geben hier ihre Titel:

Über vertauschbare Matrizen S. 601—614, 1896. — Über Gruppencharaktere S. 985—1021, 1896. — Über die Primfaktoren der Gruppendeterminante S. 1343 bis 1382, 1896; do. II S. 401—409, 1903. — Über die Darstellung der endlichen Gruppen durch lineare Substitutionen S. 994—1015, 1897; do. II, S. 482—500, 1899. — Über Relationen zwischen den Charakteren einer Gruppe und denen ihrer Untergruppen S. 501—515, 1898. — Über die Komposition der Charaktere einer Gruppe S. 330—339, 1899. — Über die Charaktere der symmetrischen

Gruppe S. 516—534, 1900. — Über die Charaktere der alternierenden Gruppe S. 303—315, 1901. — Über auflösbare Gruppen S. 337—345, 1893; do. II, S. 1027—1044, 1895; do. III, S. 849—857, 1901; do. IV, S. 1216—1230, 1901; do. V, S. 1324—1329, 1901. — Über Gruppen der Grade p oder $p+1$, S. 351—369, 1902. — Über primitive Gruppen des Grades n und der Klasse $n-1$ S. 455 bis 459, 1902. — Über die charakteristischen Einheiten der symmetrischen Gruppe S. 328—358, 1903. — Über die Charaktere der mehrfach transitiven Gruppen S. 558—571, 1904. — Über die reellen Darstellungen der endlichen Gruppen, gemeinsam mit *I. Schur*, S. 186—208, 1906. — Über die Äquivalenz der Gruppen linearer Substitutionen, gemeinsam mit *I. Schur*. S. 209—217, 1906. — Über die mit einer Matrix vertauschbaren Matrizen S. 3—15, 1910.

Die wichtigsten früheren Resultate von *Frobenius* wurden unabhängig von *Burnside* wiedergefunden. Letzterem verdankt man eine Reihe der wichtigsten Anwendungen der Theorie sowie deren klassische Darstellung in seiner Theory of groups of finite order, second edition, Cambridge 1911, auf die wir für die Zitate seiner Arbeiten verweisen.

Als dritter erfolgreicher Bearbeiter ist *I. Schur* zu erwähnen, dessen wichtigste Arbeiten aus diesem Gebiet die folgenden sind:

Neue Begründung der Theorie der Gruppencharaktere, Berl. Ber. S. 406 bis 432, 1905. — Arithmetische Untersuchungen über endliche Gruppen linearer Substitutionen, ib. S. 164—184, 1906. — Über Gruppen linearer Substitutionen mit Koeffizienten aus einem algebraischen Zahlkörper, Math. Ann. 71, S. 355 bis 367. — Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen, Crelles Journ. 127, S. 20—50 und 132, S. 85—137. — Über die Darstellung der symmetrischen und der alternierenden Gruppe durch gebrochene lineare Substitutionen, Crelles Journ. 139, S. 155—250.

§ 40. Substitutionen.

Definition: Eine ***lineare homogene Substitution vom Grade n*** besteht aus n Gleichungen von der Gestalt:

$$\left.\begin{aligned} x_1' &= a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ x_2' &= a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ x_n' &= a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n \end{aligned}\right\} \qquad (1)$$

Sie ist eindeutig bestimmt durch das quadratische Schema der Koeffizienten:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix},$$

das wir nach *Kronecker* mit (a_{ik}) bezeichnen. Die Determinante $D = |a_{ik}|$ heißt die ***Determinante der Substitution.*** Ist sie von 0 verschieden, so lassen sich die Gleichungen (1) folgendermaßen nach $x_1, \ldots, x_n$ auflösen:

$$\begin{aligned} Dx_1 &= A_{11}x_1' + A_{21}x_2' + \ldots + A_{n1}x_n' \\ Dx_2 &= A_{12}x_1' + A_{22}x_2' + \ldots + A_{n2}x_n' \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ Dx_n &= A_{1n}x_1' + A_{2n}x_2' + \ldots + A_{nn}x_n' \end{aligned}$$

Hierbei bedeutet allgemein A_{ik} die Unterdeterminante von a_{ik} in A. Diese neue Substitution heißt die *inverse* zu A und wird mit A^{-1} bezeichnet. Sie entsteht aus $\left(\frac{A_{ik}}{D}\right)$ durch Vertauschung der Zeilen mit den Kolonnen, d. h. durch ***Transposition***.

Um in einer Funktion der Variablen $x_1, \ldots, x_n$ die Substitution A auszuführen, hat man diese Variablen durch die rechten Seiten von (1) zu ersetzen, d. h. man hat aus $f(x_1, \ldots, x_n)$ zu bilden $f(x_1', \ldots, x_n')$ und $x_1', \ldots, x_n'$ mit Hilfe der Gleichungen (1) durch die linearen Funktionen der x auszudrücken. Dies ist die genaue Verallgemeinerung des Begriffs: Permutation der Variablen. Insbesondere erhält man die rechten Seiten von (1), indem man auf die Variablen $x_1, \ldots, x_n$ die Substitution A ausübt.

Ist eine zweite Substitution mit der Matrix $B = (b_{ik})$ gegeben, so kann man sie auf die n linearen Funktionen der rechten Seite von (1) ausüben. Diese gehen alsdann wiederum über in lineare Funktionen von $x_1, \ldots, x_n$ und wir erhalten eine neue Substitution, das *Produkt AB von A und B*. Bezeichnet man sie mit $C = (c_{ik})$, so wird

$$c_{ik} = \sum_{l=1}^{n} a_{il} b_{lk} \qquad (i, k = 1, 2, \ldots, n)$$

d. h. C entsteht aus A und B, indem man die Zeilen von A mit den Kolonnen von B komponiert. AA wird durch A^2 abgekürzt und entsprechend werden die höheren „Potenzen" von A mit A^i bezeichnet. Die Determinante von (c_{ik}) wird gleich dem Produkt der Determinanten von (a_{ik}) und (b_{ik}):

$$|c_{ik}| = |a_{ik}| \cdot |b_{ik}|.$$

Die Zusammensetzung von A mit A^{-1} ergibt die ***Einheitsmatrix***

$$E = (e_{ik}) \quad e_{ik} = \begin{cases} 0 & (i \neq k) \\ 1 & (i = k) \end{cases}.$$

Nunmehr seien n lineare Formen von $x_1, x_2, \ldots, x_n$ gegeben:

$$\begin{aligned} s_{11}x_1 + \ldots + s_{1n}x_n &= y_1 \\ &\cdots\cdots\cdots\cdots\cdots \\ s_{n1}x_1 + \ldots + s_{nn}x_n &= y_n. \end{aligned}$$

Die Matrix $S = (s_{ik})$ habe eine von 0 verschiedene Determinante. Übt man auf die Variablen $y_1, \ldots, y_n$ die Substitution A aus, so erfahren auch die $x_1, \ldots, x_n$ eine solche, und man findet sie in folgender Weise: Man hat die Variablenreihe $x_1, \ldots, x_n$ durch die Reihe $y_1, \ldots, y_n$

zu ersetzen, d. h. man hat auf $x_1, \ldots, x_n$ die Substitution S^{-1} auszuüben. Alsdann folgt die Ausführung von A und schließlich hat man von den y wiederum zu den x überzugehen, was durch S geschieht. So erhält man den für das Folgende fundamentalen

Satz 95: *Übt man auf die n linearen Ausdrücke*

$$\begin{array}{l} s_{11}x_1 + \ldots + s_{1n}x_n = y_1 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ s_{n1}x_1 + \ldots + s_{nn}x_n = y_n \end{array} \qquad S = (s_{ik}), \quad |s_{ik}| \neq 0$$

die Substitution A aus, so erfahren die n Variablen $x_1, \ldots, x_n$ *die Substitution* $S^{-1}AS$.

$S^{-1}AS$ heißt die durch S aus A ***transformierte*** Matrix.

Nunmehr sei A eine Matrix, von der eine bestimmte Potenz die Einheitsmatrix E ergibt. Der kleinste Exponent a, welcher der Gleichung genügt $A^a = E$, heißt die *Ordnung* von A. Offenbar bilden $A, A^2, \ldots, A^a = E$ eine zyklische Gruppe von der Ordnung a. Wir beweisen nunmehr den

Satz 96: *Jede Matrix von endlicher Ordnung läßt sich in eine* ***Diagonalmatrix*** *transformieren, d. h. in eine Matrix von der Gestalt:* (c_{ik}), $c_{ik} = 0$, $i \neq k$, *bei der alle Koeffizienten außerhalb der Hauptdiagonalen* 0 *sind. Ist a die Ordnung der Matrix, so genügen die Koeffizienten* c_{ii} *der Gleichung* $c_{ii}^a = 1$.

Beweis: Man übt auf x_1 der Reihe nach die Substitutionen $E, A, A^2, \ldots, A^{a-1}$ aus und erhält so a lineare Formen:

$$y_1 = x_1, \; y_2, \; \ldots, \; y_a.$$

Versteht man unter ε eine primitive a-te Einheitswurzel, so bildet man weiter die a Linearformen:

$$\begin{array}{l} y_1 + y_2 + y_3 + \ldots + y_a = z_0 \\ y_1 + \varepsilon^{-1}y_2 + \varepsilon^{-2}y_3 + \ldots + \varepsilon^{-(a-1)}y_a = z_1 \\ y_1 + \varepsilon^{-2}y_2 + \varepsilon^{-2\cdot 2}y_3 + \ldots + \varepsilon^{-2(a-1)}y_a = z_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ y_1 + \varepsilon^{-(a-1)}y_2 + \varepsilon^{-2(a-1)}y_3 + \ldots + \varepsilon^{-(a-1)(a-1)}y_a = z_{a-1}. \end{array}$$

Ihre Summe ist $= ay_1$.

$z_0, \ldots, z_{a-1}$ sind Linearformen von $x_1, \ldots, x_n$. Übt man nun auf die Variablen x die Substitution A aus, so erfahren $y_1, \ldots, y_a$ eine zyklische Vertauschung, indem allgemein y_i übergeht in y_{i+1} (y_a in y_1). Daher bleibt z_0 ungeändert und z_i geht über in $\varepsilon^i z_i$.

Die n Linearformen von x: $z_0, \ldots, z_{a-1}$ verschwinden sicher nicht sämtlich, denn ihre Summe ist $ay_1 = ax_1$. Aber es können zwischen ihnen Beziehungen bestehen. Wir wählen ein System von linear unabhängigen z aus, so daß alle übrigen sich linear durch sie ausdrücken lassen. Zu dem Zweck beginnen wir etwa mit z_0. Ist $z_1 = c \cdot z_0$

($c = \text{const.}$), so läßt man z_1 weg, sonst nimmt man z_1 zu z_0. Ist $z_2 = c_0 z_0 + c_1 z_1$, so läßt man z_2 weg, sonst nimmt man es zu den vorigen. In dieser Weise erhält man ein System von der Art, wie es gesucht ist. Wenn unter den a Formen z *nicht* n linear unabhängige vorkommen, so gibt es noch weitere Formen von $x_1, \ldots, x_n$, die sich nicht linear durch $z_0, \ldots, z_{a-1}$ ausdrücken lassen. Speziell kann man hierfür eine der Variablen x wählen, denn wenn sich alle x ausdrücken lassen, so gilt dasselbe von allen ihren linearen Formen Wir gehen von einer solchen neuen Form y_1' aus und wiederholen unser Verfahren. Man erhält so $z_0', \ldots, z_{a-1}'$, und darunter gibt es gewiß eine Form, die von den Formen $z_0, \ldots, z_{a-1}$ linear unabhängig ist, denn die Summe ist wiederum $a y_1'$, was nach Voraussetzung von $z_0, \ldots, z_{a-1}$ linear nicht abhängt. Nimmt man die unabhängigen zu den früher ausgewählten und setzt das Verfahren fort, so gelangt man schließlich zu n linear unabhängigen Formen $t_1, t_2, \ldots, t_n$ der Variablen $x_1, \ldots, x_n$, welche sämtlich die Eigenschaft haben, daß nach Ausführung der Substitution A die Variable t übergeht in $\varepsilon^k t$. Die Determinante der n Formen $t_1, \ldots, t_n$ ist gewiß von Null verschieden, weil sie linear unabhängig sind, und daraus folgt wegen Satz 95 unsere Behauptung.

Wir zeigen nun, daß die Koeffizienten der Diagonalmatrizen, abgesehen von der Reihenfolge, bestimmt sind durch die Matrix. Sie heißen die ***charakteristischen Wurzeln*** der Matrix. Sei

$$S^{-1} A S = \begin{pmatrix} \varepsilon_1 & 0 \ldots 0 \\ 0 & \varepsilon_2 \ldots 0 \\ \cdots\cdots\cdots \\ 0 & 0 \ldots \varepsilon_n \end{pmatrix},$$

so sind $\varepsilon_1, \ldots, \varepsilon_n$ offenbar die Wurzeln der Gleichung

$$\begin{vmatrix} \varepsilon_1 - t, & 0, & \ldots, & 0 \\ 0, & \varepsilon_1 - t, & \ldots, & 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ 0, & 0, & \ldots, & \varepsilon_n - t \end{vmatrix} = 0.$$

Wir beweisen nun, daß die Gleichung

$$\begin{vmatrix} a_{11} - t, & a_{12}, & \ldots, & a_{1n} \\ a_{21}, & a_{22} - t, & \ldots, & a_{2n} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{n1}, & a_{n2}, & \ldots, & a_{nn} - t \end{vmatrix} = 0$$

dieselben Wurzeln besitzt. Sie heißt die ***charakteristische Gleichung*** von A.

Zum Beweis verwenden wir eine neue Symbolik, die ***Addition von Matrizen***. Ist $A = (a_{ik})$ und $B = (b_{ik})$, so verstehen wir unter $A + B$

die Matrix $(a_{ik}+b_{ik})$, die man aus A und B erhält, indem man jeweils die Koeffizienten an derselben Stelle in A und B addiert. Kombiniert man Addition und Multiplikation, so gilt das *Distributivgesetz*:

$$(A+B)C = AC + BC, \qquad C(A+B) = CA + CB.$$

Bezeichnet man ferner mit tA die Matrix (ta_{ik}), so läßt sich die Matrix der charakteristischen Gleichung schreiben:

$$(A - tE).$$

Transformiert man sie durch S, so erhält man:

$$S^{-1}(A - tE)S = S^{-1}AS - S^{-1}(tE)S.$$

Nun ist tE mit S vertauschbar und man erhält:

$$S^{-1}(A - tE)S = S^{-1}AS - tE.$$

Geht man zu den Determinanten über, so folgt:

$$|A - tE| = |S^{-1}AS - tE|,$$

womit bewiesen ist der

Satz 97: *Zwei Matrizen, die durch Transformation auseinander hervorgehen, haben dieselbe charakteristische Gleichung.*

Wenn die sämtlichen Wurzeln der charakteristischen Gleichung untereinander übereinstimmen, so hat die Matrix A, falls sie von endlicher Ordnung ist, die Diagonalform; denn es gibt eine Substitution S, welche der Gleichung genügt:

$$S^{-1}AS = \varepsilon E,$$

wobei ε die Wurzel der charakteristischen Gleichung ist. Daraus folgt:

$$A = S(\varepsilon E)S^{-1} = \varepsilon E.$$

Hieraus kann man leicht zeigen, daß Satz 96 nicht für beliebige Matrizen gilt, z. B. nicht für

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

denn hier sind 1 und 1 die charakteristischen Wurzeln, aber aus $S^{-1}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}S = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ folgt $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, was ein Widerspruch ist. Die Ordnung dieser Matrix ist nicht endlich.

§ 41. Substitutionsgruppen.

Es seien g Matrizen vom Grade n mit nicht verschwindender Determinante gegeben mit der Eigenschaft, daß das Produkt von je zweien wiederum eine der g Matrizen ist; dann bilden sie eine Gruppe von der Ordnung g. Denn die Eigenschaften *I*, *II* und *III** sind erfüllt; aus $AB = AC$ folgt: $A^{-1}AB = A^{-1}AC$, also $B = C$.

Die Permutationsgruppen und die monomialen Gruppen lassen sich als Spezialfälle der Substitutionsgruppen auffassen. Z. B. ist die Permutation

$$\begin{pmatrix} x_1 & x_2 \\ x_2 & x_1 \end{pmatrix}$$

gleichbedeutend mit der Substitution

$$x_1' = x_2,$$
$$x_2' = x_1,$$

deren Matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ist.

Es entstehen nun zwei Fundamentalprobleme:

1. *Gegeben ist eine abstrakte Gruppe. Man soll alle Darstellungen derselben durch Matrizen angeben.*

2. *Gegeben ist der Grad der Matrizen. Man solle alle endlichen Gruppen, welche durch Matrizen dieses Grades dargestellt werden können, angeben.*

Das erste Problem wird den Gegenstand der folgenden Paragraphen bilden. Die Theorie ist von *Frobenius* entwickelt worden. Das zweite Problem ist noch weit von der Lösung entfernt, doch werden wir immerhin einige wichtige Sätze zu entwickeln haben.

Aus jeder Substitutionsgruppe E, A, B, ... kann man im allgemeinen unendlich viele neue ableiten, indem man die Matrizen durch eine feste Matrix transformiert. Die Matrizen

$$S^{-1}ES = E, \quad S^{-1}AS, \quad S^{-1}BS, \quad \ldots$$

bilden in der Tat eine mit E, A, B, ... homomorphe Gruppe, denn aus

$$AB = C \text{ folgt: } S^{-1}AS \cdot S^{-1}BS = S^{-1}ABS = S^{-1}CS.$$

Die Zuordnung $A \to S^{-1}AS$ liefert den Homomorphismus. Zwei solche Substitutionsgruppen heißen ***äquivalent.*** Es ist offenbar für die beiden Probleme nur nötig, aus jedem System äquivalenter Gruppen einen Repräsentanten zu betrachten. Diese einfachen Überlegungen gestatten bereits, für zyklische Gruppen das Problem 1 völlig zu lösen. Ist A, A^2, ..., $A^a = 1$ die Gruppe von der Ordnung a, so erhält man eine Darstellung durch Substitutionen vom Grade 1, indem man unter A die Substitution $x' = \varepsilon x$ versteht, wobei ε eine beliebige a-te Einheitswurzel bedeutet. Setzt man $\varepsilon = 1$, so erhält man die identische Darstellung $x' = x$, welche jedem Element die Matrix (1) zuordnet. Außer diesen gibt es noch $a - 1$ weitere, entsprechend den übrigen Wurzeln von $x^a = 1$. Ist ε eine primitive a-te Einheitswurzel, so kann man die a verschiedenen Darstellungen vom Grade 1 in folgendes Schema bringen:

	E	A	A^2	...	A^{a-1}
Γ_0	1	1	1	...	1
Γ_1	1	ε	ε^2	...	ε^{a-1}
Γ_2	1	ε^2	ε^4	...	$\varepsilon^{2(a-1)}$
...	...	...	...	...	...
Γ_{a-1}	1	ε^{a-1}	$\varepsilon^{2(a-1)}$	...	$\varepsilon^{(a-1)(a-1)}$

(1)

Die Einheitswurzeln einer Zeile bilden jeweils eine Darstellung der Gruppe, die wir mit Γ_0, ... bezeichnen. *In dieser Weise angeordnet, bilden die a Darstellungen eine quadratische Matrix,* eine Tatsache, die auch bei allgemeinen Gruppen wiederum zum Vorschein kommen wird.

Ist nunmehr eine Darstellung Γ von höherem Grade gegeben, so läßt sich die dem Element A entsprechende Matrix transformieren auf die Form:

$$A = \begin{vmatrix} \varepsilon^{i_1} & 0 & \dots & 0 \\ 0 & \varepsilon^{i_2} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \varepsilon^{i_n} \end{vmatrix}$$

A und seine sämtlichen Potenzen haben die Diagonalform und man wird füglich diese Darstellung als ***Summe der n Darstellungen*** (ε^{i_1}), (ε^{i_2}), ... bezeichnen können:

$$\Gamma = \Gamma_{i_1} + \Gamma_{i_2} + \dots + \Gamma_{i_n}.$$

Diese Definition der *Summe von Darstellungen* hat mit derjenigen der Summe von Matrizen nichts zu tun. Man erhält nun alle Darstellungen der zyklischen Gruppe, indem man die Summe bildet:

$$g_0 \Gamma_0 + g_1 \Gamma_1 + \dots + g_{a-1} \Gamma_{a-1} = \Gamma, \tag{2}$$

wobei g_i ganze positive Zahlen sind, und Γ durch eine beliebige Substitution vom Grade $g_0 + g_1 + \dots + g_{a-1}$ transformiert. $\Gamma_0, \dots, \Gamma_{a-1}$ heißen die ***irreduziblen Darstellungen*** der Gruppe und die Formel (2) besagt, daß Γ den ***irreduziblen Bestandteil*** Γ_i genau g_i-mal enthält.

Es ist nun die Frage, *ob man für* Γ *die irreduziblen Bestandteile angeben kann, ohne* Γ *auf die Diagonalform zu transformieren.* Stellt A eine beliebige Matrix von der Ordnung a dar, so ist die Summe der charakteristischen Wurzeln gegeben durch den Ausdruck

$$a_{11} + a_{22} + \dots + a_{nn},$$

denn die charakteristische Gleichung von A ist:

$$|A - tE| = (-1)^n t^n + (-1)^{n-1} t^{n-1}(a_{11} + a_{22} + \dots + a_{nn}) + \dots = 0.$$

Wenn nun die irreduziblen Bestandteile der Darstellung E, A, A^2, ... durch $g_0 \Gamma_0 + \dots + g_{a-1} \Gamma_{a-1}$ gegeben sind, wenn wir ferner

die Summe der Koeffizienten der Hauptdiagonale in E, A, A^2, ... mit $n_1 = n$, n_2, ..., n_a bezeichnen, so gelten die Gleichungen:

$$\begin{aligned} g_0 + g_1 + \quad &\dots + g_{a-1} = n_1, \\ g_0 + \varepsilon g_1 + \quad &\dots + \varepsilon^{a-1} g_{a-1} = n_2, \\ &\dots\dots\dots\dots \\ g_0 + \varepsilon^{a-1} g_1 + &\dots + \varepsilon^{(a-1)(a-1)} g_{a-1} = n_a. \end{aligned}$$

Hieraus berechnen sich die Zahlen in g_0, ..., g_{a-1} in folgender Weise:

$$\begin{aligned} a \cdot g_0 &= n_1 + n_2 + \quad \dots + n_a, \\ a \cdot g_1 &= n_1 + \varepsilon^{-1} n_2 + \quad \dots \varepsilon^{-(a-1)} n_a, \\ &\dots\dots\dots\dots \\ a \cdot g_{a-1} &= n_1 + \varepsilon^{-(a-1)} n_2 + \dots + \varepsilon^{-(a-1)(a-1)} n_a, \end{aligned}$$

womit die Aufgabe gelöst ist. Bereits durch die Summe der Diagonalkoeffizienten der Matrizen ist also die Darstellung bestimmt und zwei Darstellungen, für welche diese Zahlen übereinstimmen, sind äquivalent.

Definition: *Man nennt* $\sum_{i=1}^{n} a_{ii}$ *den* ***Charakter*** $\chi(A)$ *der Matrix* $A = (a_{ik})$, *und die Gesamtheit der Charaktere der Matrizen einer Gruppe heißt das* ***Charakterensystem*** *der Substitutionsgruppe.*

Wir haben also für zyklische Gruppen den Satz bewiesen:

Satz 98: *Zwei Darstellungen einer zyklischen Gruppe sind dann und nur dann äquivalent, wenn sie dasselbe Charakterensystem besitzen.*

Denn sie lassen sich auf dieselbe Diagonalform transformieren.

§ 42. Reduzible und irreduzible Substitutionsgruppen.

Definition: Eine Substitutionsgruppe heißt ***reduzibel***, wenn sie sich so transformieren läßt, daß ihre Matrizen sämtlich die Gestalt haben:

$$A = \left| \begin{array}{c|c} P & Q \\ \hline 0 & R \end{array} \right|,$$

wobei P eine quadratische Matrix vom Grade n_1, R eine ebensolche vom Grade n_2 ($n_1 + n_2 = n$), und Q eine rechteckige Matrix von n_1 Zeilen und n_2 Spalten darstellt, während 0 eine Matrix mit n_2 Zeilen und n_1 Spalten bedeutet, deren Koeffizienten sämtlich 0 sind. Übt man sie auf die Variablen x_1, ..., x_n aus, so werden die n_2 letzten nur unter sich substituiert. Daraus folgt, daß das Produkt zweier derartiger Matrizen (mit gleichem n_1 resp. n_2) wiederum eine solche Matrix ist.

Ist speziell A' die Matrix $\begin{pmatrix} P' & Q' \\ 0 & R' \end{pmatrix}$, wobei die zugehörigen Zahlen wieder n_1 und n_2 sein sollen, so wird $AA' = \begin{pmatrix} PP' & PQ' + QR' \\ 0 & RR' \end{pmatrix}$.

Nimmt man also aus jeder Matrix den Bestandteil P resp. R gesondert, so bilden auch sie eine Gruppe, die isomorph ist mit der ursprünglichen Gruppe. Ist Q nicht überall die Nullmatrix, so heißt die Gruppe ***halb reduziert***, sonst ***ganz reduziert***. Es gilt nun der

Fundamentalsatz 99[1]**:** *Jede halbreduzierte endliche Gruppe ist äquivalent mit einer ganz reduzierten.*

Beweis: Wir beginnen mit *reellen* Gruppen vom Grade n. Übt man ihre g Substitutionen E, A, B ... auf die quadratische Form

$$x_1^2 + x_2^2 + \ldots + x_n^2$$

aus und addiert die so erhaltenen Formen, so erhält man eine positive definite quadratische Form von $x_1, \ldots, x_n$, die sich nicht ändert, wenn man eine beliebige Substitution der Gruppe auf sie ausübt. Wir bezeichnen sie mit

$$f = \sum_{i,\,k=1}^{n} \alpha_{ik} x_i x_k \quad (\alpha_{ik} = \alpha_{ki}).$$

Der Koeffizient von x_i^2 ist α_{ii}, derjenige von $x_i x_k\,(i \neq k)$ ist $2\alpha_{ik}$. Bildet man nun

$$\frac{1}{\alpha_{11}}(\alpha_{11}x_1 + \alpha_{12}x_1 + \ldots + \alpha_{1n}x_n)^2,$$

so stimmen diejenigen Terme, die x_1 enthalten, überein mit den entsprechenden in f, daher wird:

$$f = \frac{1}{\alpha_{11}}(\alpha_{11}x_1 + \ldots + \alpha_{12}x_n)^2 + g(x_2, \ldots, x_n),$$

wobei g eine quadratische Form der Variablen $x_2, \ldots, x_n$ ist.

Setzt man

$$y_1 = \frac{1}{\sqrt{\alpha_{11}}}(\alpha_{11}x_1 + \ldots + \alpha_{1n}x_n),$$

so ist

$$f = y_1^2 + g(x_2, \ldots, x_n).$$

Auf g kann man dasselbe Verfahren ausüben und fortfahren, bis schließlich f übergeführt ist in $y_1^2 + y_2^2 + \ldots + y_n^2$. Die hierbei benutzte Substitution hat offenbar die Gestalt:

$$\begin{aligned}
y_1 &= s_{11}x_1 + s_{12}x_2 + \ldots + s_{1n}x_n,\\
y_2 &= \qquad\quad s_{22}x_2 + \ldots + s_{2n}x_n,\\
&\ldots\ldots\ldots\ldots\ldots\\
y_n &= \qquad\qquad\qquad\quad s_{nn}x_n.
\end{aligned}$$

Wir bezeichnen sie mit T^{-1}.

[1]) *H. Maschke:* Beweis des Satzes, daß diejenigen endlichen linearen Substitutionsgruppen, in welchen einige durchgehends verschwindende Koeffizienten auftreten, intransitiv sind. Math. Ann. **52**, S. 363. 1899.

Es ist also f die Summe der Quadrate von n Linearformen. Keine derselben kann verschwinden, denn sonst gäbe es außer $x_1 = x_2 = \ldots = x_n = 0$ noch weitere Wertesysteme der Variablen x, für welche $f = 0$ wäre, was ausgeschlossen ist, da dies für den Summanden $x_1^2 + \ldots + x_n^2$ nicht gilt und alle weiteren nur positive Werte annehmen können. Die Substitution T^{-1} gibt nach den x aufgelöst eine solche von gleicher Gestalt,

$$T \qquad \begin{aligned} x_1 &= t_{11}y_1 + t_{12}y_2 + \ldots + t_{1n}y_n, \\ x_2 &= \quad t_{22}y_2 + \ldots + t_{2n}y_n, \\ &\ldots\ldots\ldots\ldots\ldots \\ x_n &= \quad t_{nn}y_n. \end{aligned}$$

Die Substitutionsgruppe

$$E,\ T^{-1}AT,\ T^{-1}BT,\ \ldots$$

läßt nun $y_1^2 + \ldots + y_n^2$ ungeändert, man nennt sie eine ***orthogonale Gruppe***, und wir haben den Satz bewiesen:

Satz 100: *Jede endliche reelle Substitutionsgruppe ist äquivalent mit einer* ***orthogonalen Substitutionsgruppe.***

Ist $A = \begin{pmatrix} P & Q \\ 0 & R \end{pmatrix}$ halbreduziert, so gilt dasselbe auch von $T^{-1}AT$, denn T und T^{-1} sind halbreduziert, wir brauchen also den Satz 99 nur für orthogonale halbreduzierte Substitutionsgruppen zu beweisen, und *hier zeigt sich nun, daß solche stets ganz reduziert sind.* Wenn A orthogonal ist, so gelten die Beziehungen:

$$\sum_{k=1}^{n} a_{ik}^2 = 1, \qquad \sum_{k=1}^{n} a_{ik}a_{lk} = 0, \qquad i \neq l,$$

d. h. setzt man A Zeile mit Zeile mit sich selbst zusammen, so erhält man die Einheitsmatrix; oder anders ausgedrückt: die zu A inverse Matrix ist die *transponierte* Matrix A^0. Nun hat die inverse Matrix dieselbe halbreduzierte Form: $A^{-1} = \begin{pmatrix} P' & Q' \\ 0 & R' \end{pmatrix}$, die transponierte dagegen ist $\begin{pmatrix} P^0 & 0 \\ Q^0 & R^0 \end{pmatrix}$ und daraus folgt, daß Q' die Nullmatrix ist, w. z. b. w.

Um den Satz 99 auch für komplexe Gruppen zu beweisen, benutzt man das Hilfsmittel der *Hermite*schen Formen. Zugleich mit Γ bildet auch das aus den konjugiert imaginären Matrizen bestehende System eine Gruppe $\bar{\Gamma}$, denn aus $AB = C$ folgt $\bar{A}\,\bar{B} = \bar{C}$, wobei allgemein $\bar{A}$ die zu A konjugiert imaginäre Matrix bedeutet. Man benutzt nun zwei Reihen von je n Variablen: $x_1, \ldots, x_n$ und $\bar{x}_1, \ldots, \bar{x}_n$ und bildet den Ausdruck

$$x_1\bar{x}_1 + x_2\bar{x}_2 + \ldots + x_n\bar{x}_n.$$

Erteilt man $\bar{x}_i$ stets den konjugierten Wert zu x_i, so stellt diese Form nur positive reelle Zahlen dar und sie verschwindet bloß für

$$x_1 = x_2 = \ldots = x_n = 0.$$

Übt man nun auf die Variablen $x_1, \ldots, x_n$ die Substitution A, auf $\bar{x}_1, \ldots, \bar{x}_n$ gleichzeitig $\bar{A}$ aus, so geht die Form über in:

$$\sum_{i=1}^{n}(a_{i1}x_1 + \ldots + a_{in}x_n)(\bar{a}_{i1}\bar{x}_1 + \ldots + \bar{a}_{in}\bar{x}_n),$$

und diese Form hat die Gestalt:

$$\sum_{i,\,k=1}^{n} r_{ik}\, x_i \bar{x}_k,$$

wobei $r_{ik} = \bar{r}_{ki}$ ist. *Eine solche Form heißt eine* ***Hermitesche Form.***

Summiert man über alle Formen, die man erhält, wenn man A die Substitutionen von Γ durchlaufen läßt, so erhält man eine *Hermite*sche Form:

$$f = \sum_{i,\,k=1}^{n} \alpha_{ik} x_i \bar{x}_k, \qquad \alpha_{ik} = \bar{\alpha}_{ki}, \text{ also } \alpha_{ii} \text{ reell.}$$

Sie kann nur verschwinden, wenn alle Variablen 0 sind und nimmt sonst lauter positive Werte an. Entsprechend dem reellen Fall erkennt man, daß

$$(\alpha_{11}x_1 + \alpha_{21}x_2 + \ldots + \alpha_{n1}x_n)(\alpha_{11}\bar{x}_1 + \alpha_{12}\bar{x}_2 + \ldots + \alpha_{1n}\bar{x}_n)$$

in denjenigen Termen mit $\alpha_{11}f$ übereinstimmt, die x_1 oder $\bar{x}_1$ enthalten. Daher wird

$$f - \frac{1}{\alpha_{11}}(\alpha_{11}x_1 + \ldots + \alpha_{n1}x_n)(\alpha_{11}\bar{x}_1 + \ldots + \alpha_{1n}\bar{x}_n)$$

bloß noch von den Variablenreihen $x_2 \ldots x_n$, $\bar{x}_2 \ldots \bar{x}_n$ abhängen. Führt man daher die beiden konjugiert imaginären Substitutionen aus:

$$y_1 = \frac{1}{\sqrt{\alpha_{11}}}(\alpha_{11}x_1 + \ldots + \alpha_{n1}x_n)$$

und

$$\bar{y}_1 = \frac{1}{\sqrt{\alpha_{11}}}(\alpha_{11}\bar{x}_1 + \ldots + \alpha_{1n}\bar{x}_n),$$

so geht f über in $y_1\bar{y}_1 + g(x_2 \ldots x_n, \bar{x}_2 \ldots \bar{x}_n)$. Dabei ist g wiederum eine *Hermite*sche Form, und indem man fortfährt, wird f zu

$$y_1\bar{y}_1 + \ldots + y_n\bar{y}_n.$$

Eine Substitution, welche diese Form ungeändert läßt, heißt eine ***unitäre*** Substitution. Man kann sie auch durch die Eigenschaft definieren, daß die zu ihrer Matrix inverse Matrix die *transponierte* der *konjugiert imaginären Matrix* ist. Man gelangt nun genau wie im reellen Fall zum Ziel.

Eine ganz reduzierte Gruppe, deren Matrizen die Gestalt haben:

$$A = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$$

ist bereits bestimmt durch die beiden Bestandteile:

$$\Gamma_1 = E_1, \; A_1, \; B_1, \; \ldots \quad \text{und} \quad \Gamma_2 = E_2, \; A_2, \; B_2, \; \ldots$$

Wir bezeichnen sie mit $\Gamma = \Gamma_1 + \Gamma_2$.

Es ist möglich, daß Γ_1 sich weiter reduzieren läßt, aber wenn man fortfährt, gelangt man stets zu einem Ende, indem man Gruppen erhält, die sich nicht weiter reduzieren lassen. Solche Substitutionsgruppen heißen ***irreduzibel***, und wir können das Resultat zusammenfassen in den

Satz 101: *Jede endliche Substitutionsgruppe ist entweder irreduzibel oder vollständig reduzibel auf eine Summe irreduzibler Gruppen.*

Enthält Γ vollständig reduziert die irreduziblen Bestandteile Γ_i je n_i-mal $(i = 1, \ldots, r)$, so schreibt man

$$\Gamma = n_1 \Gamma_1 + n_2 \Gamma_2 + \ldots + n_r \Gamma_r.$$

Wir beweisen noch den

Satz 102: *Die irreduziblen Bestandteile einer Abelschen Substitutionsgruppe sind sämtlich vom Grade* 1. *Sie läßt sich transformieren in eine Gruppe, deren Matrizen sämtlich die Diagonalform haben.*

Beweis: Wir benutzen vollständige Induktion, indem wir den Satz als bewiesen annehmen für Gruppen, deren Grad kleiner als n ist.

Γ sei also eine *Abel*sche Gruppe, die nicht in reduzierter Form gegeben ist. Dann gibt es eine Matrix A in Γ, die mindestens zwei verschiedene charakteristische Wurzeln besitzt, und wir nehmen an, daß A in Diagonalform erscheint. Die Koeffizienten in der Hauptdiagonale von A seien der Reihe nach $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)$. Durch eine weitere Transformation, welche auf eine bloße Vertauschung der Variablen herauskommt, kann man erreichen, daß in der Hauptdiagonalen zuerst alle Wurzeln kommen, die gleich ε_1 sind, während die übrigen von ε_1 verschieden sind. Es sei also

$$\varepsilon_1 = \varepsilon_2 = \ldots = \varepsilon_m \qquad \varepsilon_i \neq \varepsilon_1 \qquad i > m.$$

Nunmehr sei B eine beliebige Matrix von Γ. Dann wird $AB = BA$, also:

$$(\varepsilon_k b_{ik}) = (\varepsilon_i b_{ik}),$$

d. h.

$$\varepsilon_k b_{ik} = \varepsilon_i b_{ik}.$$

Ist also $\varepsilon_i \neq \varepsilon_k$, so wird $b_{ik} = 0$, insbesondere ist $b_{ik} = 0$, sobald

$$i \leqq m \qquad k > m$$

oder

$$i > m \qquad k \leqq m,$$

d. h. aber, daß B ganz reduziert ist, nämlich Summe zweier quadratischer Matrizen vom Grade m und $n-m$. Da B eine beliebige Matrix von Γ ist, so ist auch Γ reduziert. Auf jeden der beiden Bestandteile kann man das Verfahren fortsetzen, bis völlige Reduktion auf die Diagonalform erreicht ist.

§ 43. Die Fundamentalrelationen der Koeffizienten irreduzibler Substitutionsgruppen.

Im vorigen Paragraphen wurde gezeigt, daß jede Substitutionsgruppe auf irreduzible Bestandteile reduziert werden kann. Unsere Aufgabe ist nun die Untersuchung dieser letzteren, und dabei zeigt sich die merkwürdige Tatsache, daß ihre Koeffizienten einer Reihe von Relationen genügen, die ganz verschieden sind von den Relationen, welche durch die Zusammensetzung der Matrizen und die Gruppeneigenschaft bedingt sind.

Jede Gruppe besitzt als irreduzible Darstellung die identische Gruppe Γ_1, deren Matrizen sämtlich aus (1) bestehen. Nunmehr sei $\Gamma = E, A, B, \ldots$ eine Darstellung der abstrakten Gruppe $\mathfrak{G}$.

Aus ihr leiten wir sofort eine neue Darstellung ab in folgender Weise: Transponiert man die Matrizen A und B (d. h. vertauscht man die Zeilen mit den Kolonnen), und bezeichnet man allgemein mit S^0 die zu S transponierte Matrix, so folgt aus $AB = C$ die andere Gleichung $B^0 A^0 = C^0$. Andrerseits gilt auch $B^{-1} A^{-1} = C^{-1}$. Bildet man daher zu jeder Matrix S die Matrix $S_t = S^{0-1}$, indem man nacheinander transponiert und zur inversen übergeht (diese beiden Operationen sind vertauschbar), so folgt aus $AB = C$ wiederum $A_t B_t = C_t$. Wir bezeichnen die Gruppe Γ_t, deren Matrizen aus $E, A_t, B_t, \ldots$ bestehen als *die zu Γ* ***adjungierte Substitutionsgruppe.***

Satz 103: *Das Charakterensystem vom Γ_t ist konjugiert imaginär zu demjenigen von Γ.*

Beweis: Wir zeigen, daß $\chi(A)$ konjugiert imaginär zu $\chi(A_t)$ ist in folgender Weise: Es gilt zunächst $\chi(A) = \chi(A^0)$, ferner ist $\chi(A^{-1})$ konjugiert imaginär zu $\chi(A)$, denn sei A auf Diagonalform reduziert $= \begin{pmatrix} \varepsilon_1 & 0 & \ldots & 0 \\ 0 & \varepsilon_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \varepsilon_n \end{pmatrix}$, so wird $A^{-1} = \begin{pmatrix} \varepsilon_1^{-1} & 0 & \ldots & 0 \\ 0 & \varepsilon_2^{-1} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & \ldots & \varepsilon_n^{-1} \end{pmatrix}$

und da die Zahlen ε Einheitswurzeln sind, so stimmt ε^{-1} mit der konjugiert imaginären Zahl zu ε überein.

Die Adjungierte der Adjungierten Gruppe stimmt mit der ursprünglichen Gruppe überein: $\Gamma_{tt} = \Gamma$, wie ohne weiteres aus der Definition

folgt, wenn wir berücksichtigen, daß Transposition und Inversion vertauschbare Operationen von der Ordnung 2 sind.

Sind Γ und Γ' zwei beliebige Darstellungen von $\mathfrak{G}$, so läßt sich aus ihnen in einfacher Weise eine neue Darstellung zusammensetzen.

Die Matrizen von Γ resp. Γ' seien $E, A, B, \ldots$ resp. $E', A', B', \ldots$ und E, E' resp. A, A' usw. seien jeweils Darstellungen desselben Elementes von $\mathfrak{G}$. Die Grade von Γ und Γ' seien n und n'. Wir bilden nun zwei Reihen von Variablen $x_1, \ldots, x_n$ und $y_1, \ldots, y_{n'}$. Auf die x_i werden nur Substitutionen von Γ und auf die y_i nur die entsprechenden von Γ' angewendet. Bildet man die sämtlichen Produkte $x_1 y_1, x_2 y_1, \ldots, x_n y_1, \quad x_1 y_2, \ldots, x_n y_2, \ldots, \quad x_1 y_{n'}, \ldots, x_n y_{n'}$ und übt man auf die Variablen A resp. A' aus, so erfahren die Produkte selbst eine lineare Substitution, und zwar gilt folgende Beziehung:

Ist A gegeben durch

$$x_i' = \sum_{j=1}^{n} a_{ij} x_j \qquad (i = 1, \ldots, n)$$

und A' gegeben durch

$$y_k' = \sum_{l=1}^{n'} a_{kl}' y_l \qquad (k = 1, \ldots, n')$$

so wird:

$$x_i' y_k' = \sum_{j=1}^{n} \sum_{l=1}^{n'} a_{ij} a_{kl}' x_j y_l.$$

Zu jedem Paar von entsprechenden Substitutionen aus Γ und Γ' gehört also eine bestimmte Substitution vom Grade $n\,n'$ und diese bilden eine mit $\mathfrak{G}$ isomorphe Gruppe. Wir bezeichnen diese Darstellung von $\mathfrak{G}$ als die durch ***Komposition*** *von* Γ *und* Γ' entstandene Darstellung $\Gamma\Gamma'$. Vertauscht man Γ und Γ', so erhält man eine äquivalente Substitutionsgruppe, denn das kommt darauf hinaus, daß man die Produkte in folgender Reihenfolge aufschreibt:

$$y_1 x_1, y_2 x_1, \ldots, y_n x_1, y_1 x_2, \ldots$$

Dies ist aber nur eine Vertauschung der Substitutionsvariablen.

Wir beweisen nunmehr den

Satz 104: *Sind* Γ *und* Γ' *zwei irreduzible Substitutionsgruppen, und ist* Γ' *nicht äquivalent mit* Γ_t, *so gibt es keine bilineare Form der Variablen* $x_1, \ldots, x_n$ *und* $y_1, \ldots, y_{n'}$, *die stets invariant bleibt, wenn auf die beiden Variablenreihen irgend zwei entsprechende Substitutionen von* Γ *und* Γ' *ausgeübt werden.*

Beweis: Jede Bilinearform $\sum_{i=1}^{n} \sum_{k=1}^{n'} r_{ik} x_i y_k = f$ läßt sich durch lineare Substitutionen auf eine Normalform transformieren. In der Tat, man bilde

$$(r_{11} x_1 + r_{21} x_2 + \ldots + r_{n1} x_n)(r_{11} y_1 + \ldots + r_{1n'} y_{n'}).$$

Dieses Produkt stimmt in denjenigen Termen, die x_1 oder y_1 enthalten, mit $r_{11} f$ überein. Hierbei darf man voraussetzen, daß $r_{11} \neq 0$ ist. Denn sonst sei $r_{ik} \neq 0$; vertauscht man nun x_1 mit x_i und y_1 mit y_k, so wird r_{ik} zum Koeffizienten von $x_1 y_1$. Dabei haben die beiden Variabelnreihen nur unter sich eine Substitution erfahren.

Setzt man

$$\frac{1}{\sqrt{r_{11}}}(r_{11} x_1 + \ldots + r_{n1} x_n) = u_1$$

$$\frac{1}{\sqrt{r_{11}}}(r_{11} y_1 + \ldots + r_{1n'} y_{n'}) = v_1,$$

so kann man f so schreiben:

$$u_1 v_1 + g(x_2, \ldots, x_n, y_2, \ldots, y_{n'}).$$

Indem man dieses Verfahren fortsetzt, erkennt man, daß sich die Bilinearform stets in der Gestalt annehmen läßt:

$$x_1 y_1 + \ldots + x_r y_r,$$

wobei natürlich $r \leqq n$, $r \leqq n'$ ist.

Nun sei (a_{ik}) eine Substitution von Γ und (a'_{ik}) die entsprechende von Γ'.

In der invarianten Form $x_1 y_1 + \ldots + x_r y_r$ üben wir zunächst bloß die Substitution (a_{ik}) auf die Variabeln x aus und erhalten:

$$y_1 \cdot \sum_1^n a_{1i} x_i + y_2 \cdot \sum_1^n a_{2i} x_i + \ldots + y_r \sum_1^n a_{ri} x_i.$$

Diese Form ordnen wir nach den x:

$$x_1 \sum_1^r a_{i1} y_i + x_2 \sum_1^r a_{i2} y_i + \ldots + x_n \sum_1^r a_{in} y_i.$$

Üben wir nun auf die Variabeln y die Substitution (a'_{ik}) aus, so muß die ursprüngliche Form $x_1 y_1 + \ldots + x_r y_r$ entstehen. Vergleicht man die Koeffizienten von $x_1, \ldots, x_r$, so findet man, daß (a'_{ik}) die r Linearformen

$$\sum_{i=1}^r a_{i1} y_i \quad \text{bis} \quad \sum_{i=1}^r a_{ir} y_i$$

überführt in y_1 bis y_r.

Ist $r < n'$, so ist also Γ' reduzibel. Dasselbe beweist man für Γ, falls $r < n$ ist. Es wird also $r = n = n'$ und $\Gamma' \simeq \Gamma_t$

Satz 105: *Sind Γ und Γ' zwei irreduzible Darstellungen von $\mathfrak{G}$, so enthält die komponierte Substitutionsgruppe $\Gamma\Gamma'$ nach vollständiger Reduktion die identische Darstellung genau einmal oder nicht, je nachdem Γ mit Γ' äquivalent ist oder nicht.*

Beweis: Wenn eine beliebige Substitutionsgruppe die identische Darstellung genau r-mal enthält, so gibt es nach Satz **101** genau r

unabhängige lineare Formen der Substitutionsvariablen, die invariant sind gegenüber den Substitutionen der Gruppe. In $\Gamma\Gamma'$ bestehen die Substitutionsvariablen aus den Produkten $x_i y_k$ und es müßte r unabhängige invariante Bilinearformen geben. Ist also Γ' nicht äquivalent mit Γ_t, so ist $r = 0$, womit ein Teil des Satzes bewiesen ist.

Nun möge für Γ und Γ_t außer $f = x_1 y_1 + \ldots + x_n y_n$ auch noch $g = \sum_{i,k=1}^{n} r_{ik} x_i y_k$ invariant sein; dann läßt sich g nach dem Beweis zu Satz 104 durch zwei Substitutionen auf die Variabelnreihen x und y in die Gestalt f transformieren. Sind d und d' die Substitutionsdeterminanten, so wird die „Determinante" von g: $|r_{ik}| = r$ nach der Substitution zu $d r d'$. Nun ist aber die Determinante von f gleich 1, daher ist $d r d' = 1$ und $r \neq 0$. *Es kann also keine invariante Bilinearform geben, deren Determinante* $= 0$ *ist.* Mit g und f ist auch $g - tf$ invariant, unter t eine beliebige Konstante verstanden. Die Determinante dieser Form ist

$$|r_{ik} - t e_{ik}| \qquad e_{ik} = \begin{cases} 0 \text{ für } i \neq k \\ 1 \text{ für } i = k \end{cases}$$

und man kann t so bestimmen, daß sie verschwindet, ohne daß die ganze Matrix zur Nullmatrix wird. Also gibt es bloß eine invariante Bilinearform und deren Multipla: $C f$.

Aus diesem Satze folgen die grundlegenden Relationen, denen die Koeffizienten irreduzibler Substitutionsgruppen genügen. Bezeichnen wir das System $(e_{ik}, a_{ik}, b_{ik}, \ldots)$ der Koeffizienten, die an der Stelle $(i\,k)$ in allen Matrizen von Γ auftreten, als eine ***Stellenzeile,*** so können wir sagen, daß alle Relationen bilineare Verbindungen (skalare Produkte) von Stellenzeilen enthalten.

Derartige Summen bezeichnen wir mit

$$\sum_S .$$

worunter also die Summe über alle Elemente $E, A, B, \ldots$ von $\mathfrak{G}$ verstanden ist.

Die grundlegenden Relationen sind enthalten in folgendem

Satz 106: *Ist Γ' nicht äquivalent mit Γ_t, so bestehen zwischen den Koeffizienten von Γ und Γ' die Gleichungen:*

$$\sum_S s_{ik} s'_{lm} = 0.$$

Zwischen Γ und Γ_t bestehen die Gleichungen

$$\sum_S s_{ik} s'_{ik} = \frac{g}{n} \qquad \text{und} \qquad \sum_S s_{ik} s'_{lm} = 0,$$

sobald $(l\,m)$ verschieden ist von $(i\,k)$. n bedeutet den Grad, g die Ordnung von Γ.

Beweis: Übt man auf $x_i y_l$ die Substitutionen von Γ und Γ' der Reihe nach aus und addiert die Bilinearformen, so muß im ersten Fall die Summe identisch verschwinden, im zweiten Fall kann auch die Form $C(x_1 y_1 + \ldots + x_n y_n)$ herauskommen. Die Form lautet nun, wenn man $\sum_S s_{ik} s'_{lm}$ mit s_{iklm} bezeichnet:

$$\sum_{k=1}^{n} \sum_{m=1}^{n'} s_{iklm} x_k y_m.$$

Daher muß im ersten Fall stets $s_{iklm} = 0$ sein, womit die 1. Aussage des Satzes bewiesen ist. Im zweiten Fall müssen jedenfalls die Koeffizienten von $x_k y_m (k \neq m)$ verschwinden, d. h.

$$s_{iklm} = 0 \qquad (k \neq m).$$

Ferner muß sein:

$$s_{i1l1} = s_{i2l2} = \ldots = s_{inln},$$

wobei noch offenbleibt, ob der Wert 0 ist oder nicht. Nun gelten aber für die Zahlen s_{iklm} die Beziehungen:

$$s_{iklm} = s_{mlki}.$$

In der Tat stimmt der Koeffizient s_{ik} in S nach Definition überein mit dem Koeffizienten an der Stelle (ki) in S_t^{-1}, ebenso derjenige von S^{-1} an der Stelle (lm) mit dem Koeffizienten von S_t an der Stelle (ml).

Man kann daher setzen:

$$\sum_S s_{ik} s'_{lm} = \sum_{S^{-1}} s'_{ki} s_{ml}$$

und, da die Summationsfolge keinen Einfluß hat auf die Summe, so wird:

$$s_{iklm} = s_{mlki}.$$

Hieraus folgt sofort, daß auch für $i \neq l$ stets $s_{iklm} = 0$ ist. Also sind gewiß nur die Zahlen $s_{ikik} \neq 0$, und zwar haben sie alle denselben Wert, denn aus

$$s_{i1i1} = s_{i2i2} = \ldots = s_{inin}$$

folgt:

$$s_{1i1i} = s_{2i2i} = \ldots = s_{nini},$$

woraus unsere Behauptung ersichtlich wird.

Um den gemeinsamen Wert dieser Größen zu bestimmen, ziehen wir eine Folgerung aus dem bewiesenen 1. Teil des Satzes.

Dieser besagt folgendes: Sind $E, A, B, \ldots$ die Matrizen von Γ und ist $e'_{ik}, a'_{ik}, b'_{ik}, \ldots$ eine Stellenzeile aus Γ', wobei Γ' nicht äquivalent ist mit Γ_t, so gilt die Beziehung:

$$e'_{ik} E + a'_{ik} A + b'_{ik} B + \ldots = 0.$$

Hieraus folgt

Satz 107: *Ist Γ verschieden von der identischen Darstellung, so verschwindet die Summe der Matrizen von Γ und also auch die Summe der Charaktere.*

In $\Gamma\Gamma_t$ ist die Summe der Charaktere offenbar $\sum_{i=1}^{n} s_{iiii}$. Andererseits enthält diese Darstellung die identische Darstellung genau einmal, daher ist diese Summe $= g$. Daraus folgt:

$$s_{1111} = \frac{g}{n},$$

womit auch der zweite Teil von Satz 106 bewiesen ist.

II. Kapitel.

Gruppencharaktere.

§ 44. Äquivalenz von Substitutionsgruppen.

Satz 108: *Sind Γ und Γ' zwei irreduzible Darstellungen von $\mathfrak{G}$, so besteht zwischen den beiden Charaktersystemen die Gleichung:*

$$\sum_S \chi(S)\chi'(S^{-1}) = \begin{cases} 0 & \text{wenn } \Gamma \textit{ nicht äquivalent mit } \Gamma', \\ g & \text{wenn } \Gamma \textit{ äquivalent mit } \Gamma'. \end{cases}$$

Beweis: $\sum_S \chi(S)\chi'(S)$ ist nach der Bezeichnungsweise des Satzes 106 gleich $\sum_{i=1}^{n}\sum_{k=1}^{n'} s_{iikk}$ und diese Terme sind sämtlich 0, außer wenn Γ' mit Γ_t äquivalent ist, und für $\Gamma' = \Gamma_t$ ist

$$s_{iikk} = \begin{cases} 0 & \text{für } i \neq k \\ \frac{g}{n} & \text{für } i = k. \end{cases}$$

Ist $\chi'(S)$ Charakter von Γ', so wird die konjugiert imaginäre Zahl $\bar{\chi}'(S)$ nach Satz 103 gleich dem Charakter von Γ_t' und es gilt $\bar{\chi}'(S) = \chi'(S^{-1})$. Daher ist die Summe nur dann von 0 verschieden, wenn Γ_t' mit Γ_t, also Γ' mit Γ äquivalent ist.

Satz 109: *Die notwendige und hinreichende Bedingung für die Äquivalenz zweier irreduziblen Darstellungen besteht in der Gleichheit des Charaktersystems.*

Beweis: Durch Transformation ändert sich der Charakter einer Matrix nicht, daher ist Gleichheit des Charakterensystems eine notwendige Bedingung. Nunmehr seien Γ und Γ' zwei irreduzible Darstellungen mit demselben Charakterensystem $\chi(S)$ $(S = E, A, \ldots)$. Γ ist adjungierte Darstellung von Γ_t, daher gilt: $\sum_S \chi(S)\bar{\chi}(S) = g$. Da χ auch Charakter von Γ' ist, so folgt, daß Γ' äquivalent mit Γ

ist. Man hat bloß im vorigen Satz Γ_t unter Γ zu verstehen, also Γ unter Γ_t und den zweiten Fall zu berücksichtigen.

Satz 110: *Eine reduzible Darstellung von $\mathfrak{G}$ läßt sich auf eine und nur eine Weise als Summe irreduzibler Bestandteile darstellen.*

Beweis: Sei

$$\Gamma = c_1\Gamma_1 + c_2\Gamma_2 + \ldots + c_r\Gamma_r = c_1'\Gamma_1 + \ldots + c_r'\Gamma_r.$$

Bezeichnen wir die Charaktere von Γ mit χ, diejenigen von Γ_i mit $\chi^{(i)}$, so gilt allgemein für jedes Element von $\mathfrak{G}$:

$$\chi = c_1\chi^{(1)} + c_2\chi^{(2)} + \ldots + c_r\chi^{(1)} = c_1'\chi^{(1)} + \ldots + c_r'\chi^{(r)}.$$

Daraus wird weiter, wegen Satz 108:

$$\sum_S \chi(S)\chi^{(i)}(S^{-1}) = c_i g = c_i' g,$$

also $c_i = c_i'$.

Satz 111: *Die notwendige und hinreichende Bedingung für die Äquivalenz zweier Darstellungen von $\mathfrak{G}$ besteht in der Gleichheit ihres Charaktersystems.*

Beweis: Zunächst ist die Bedingung notwendig. Sie ist aber auch hinreichend, denn wie im vorigen Beweis folgt, daß die beiden Darstellungen dieselben irreduziblen Bestandteile besitzen, sie lassen sich also in dieselbe vollständig reduzierte Gestalt transformieren und sind daher äquivalent.

§ 45. Weitere Relationen zwischen den Gruppencharakteren.

In § 6 haben wir eine Einteilung der Elemente einer Gruppe in Klassen kennen gelernt. Wir bezeichnen die Klassen mit $\mathfrak{C}_1, \mathfrak{C}_2, \ldots, \mathfrak{C}_r$ und die Anzahl der Elemente in $\mathfrak{C}_i$ sei h_i. Wenn $\mathfrak{C}_i$ aus den Elementen $A_1^{(i)}, \ldots, A_{h_i}^{(i)}$ besteht, so schreiben wir: $\mathfrak{C}_i = A_1^{(i)} + \ldots + A_{h_i}^{(i)}$. Man kann nun das Produkt $\mathfrak{C}_i\mathfrak{C}_k$ definieren als:

$$(A_1^{(i)} + \ldots + A_{h_i}^{(i)})(A_1^{(k)} + \ldots + A_{h_k}^{(k)}) = \sum_{l=1}^{h_i}\sum_{m=1}^{h_k} A_l^{(i)}A_m^{(k)},$$

und diese neue Summe ist wiederum eine Summe von Klassen, denn transformiert man die linke Seite durch ein beliebiges Element, so erfahren die Elemente jeder Klammer unter sich eine Permutation. Indem wir rechts abzählen, wie oft jedes Element auftritt, erhalten wir die Gleichung:

$$\mathfrak{C}_i\mathfrak{C}_k = \sum_{l=1}^{r} c_{ikl}\mathfrak{C}_l,$$

wobei die Koeffizienten c ganze positive Zahlen oder 0 sind. Mit Hilfe dieser Koeffizienten lassen sich nun Gleichungen definieren, denen die Charaktere jedes Systems genügen.

Wir bemerken zunächst, daß unter den Charakteren $\chi(S)$ einer Darstellung von $\mathfrak{G}$ höchstens r verschiedene vorkommen, denn die Matrizen derselben Klasse von $\mathfrak{G}$ besitzen denselben Charakter. Zu jeder Klasse gehört ein Wert von χ und wir setzen $\chi(A) = \chi_i$, wenn A zu $\mathfrak{C}_i$ gehört. Speziell wird $\chi(E) = \chi_1 = n$.

Alsdann lassen sich die Relationen von Satz 108 auch so schreiben:

$$\sum_{i=1}^{r} h_i \chi_i \bar{\chi}_i' = \begin{cases} 0 & \text{für } \chi' \neq \chi \\ g & \text{für } \chi' = \chi . \end{cases}$$

Ferner gelten die weiteren Beziehungen:

Satz 112: *Zwischen den Charakteren einer irreduziblen Darstellung von $\mathfrak{G}$ gelten die Gleichungen:*

$$\frac{h_i \chi_i}{\chi_1} \cdot \frac{h_k \chi_k}{\chi_1} = \sum_{l=1}^{r} c_{ikl} \frac{h_l \chi_l}{\chi_1} \quad \text{oder} \quad h_i \chi_i h_k \chi_k = \chi_1 \sum_{l=1}^{r} c_{ikl} h_l \chi_l .$$

Beweis: Die Stellenzeilen $(e_{ik}, a_{ik}, \ldots)$ einer irreduziblen Darstellung Γ sind linear unabhängig, denn wenn eine Relation

$$\sum_{i,k=1}^{n} u_{ik} s_{ik} = 0 \qquad (s = e, a, b, \ldots)$$

bestände, so multipliziere man die linke Seite mit $s_{11}\,(s = e, a, b, \ldots)$ und addiere. Wegen Satz 106 folgt $u_{11} = 0$. Genau gleich beweist man, daß alle Koeffizienten verschwinden. Daraus folgt, daß man in der Matrix:

$$E x_E + A x_A + \ldots = \left(\sum_{S} s_{ik} x_S\right) = \mathsf{M}$$

die Variablen x so bestimmen kann, daß sie einer beliebigen Matrix von n^2 Zahlenkoeffizienten gleich wird. Nun sei die Matrix N mit allen Matrizen von Γ vertauschbar, dann ist sie auch mit M und daher mit jeder Matrix vom Grade n vertauschbar. Nimmt man speziell eine Diagonalmatrix mit n verschiedenen Koeffizienten

$$\begin{pmatrix} a_1 & 0 \ldots 0 \\ 0 & a_2 \ldots 0 \\ \ldots\ldots\ldots \\ 0 & 0 \ldots a_n \end{pmatrix} = M',$$

so folgt aus $M'N = NM'$, daß N eine Diagonalmatrix sein muß, und nimmt man weiter eine Matrix von der Gestalt:

$$M'' = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix}$$

so erkennt man aus $M''N = NM''$, daß N die Gestalt hat cE.

Bildet man die Summe aller Matrizen der Klasse $\mathfrak{C}_i$, so erhält man eine Matrix, die wir mit C_i bezeichnen. C_i ist nun mit allen Matrizen von Γ vertauschbar, weil die Elemente einer Klasse bei Transformation mit einem beliebigen Element der Gruppe nur eine Vertauschung erleiden. Daher wird $C_i = \eta_i E$ und hieraus folgt weiter, daß die η den Gleichungen genügen:

$$\eta_i \eta_k = \sum_{l=1}^{r} c_{ikl} \eta_l .$$

Der Charakter von C_i ist $n \eta_i = \chi_1 \eta_i$. Andererseits ist er auch die Summe der Charaktere der h_i Matrizen der Klasse, also $= h_i \chi_i$. Daraus folgt: $\chi_1 \eta_i = h_i \chi_i$ oder $\eta_i = \frac{h_i \chi_i}{\chi_1}$, womit der Satz bewiesen ist.

Man kann auch zwischen den Charakteren der Matrizen, die in den verschiedenen irreduziblen Darstellungen zum selben Element gehören, Relationen angeben.

Seien $\Gamma_1, \ldots, \Gamma_{r'}$ Repräsentanten der verschiedenen irreduziblen Darstellungen und sei die vollständige Reduktion von $\Gamma_i \Gamma_k$ durch folgende Formeln gegeben:

$$\Gamma_i \Gamma_k = \sum_{l=1}^{r'} g_{ikl} \Gamma_l .$$

Der Charakter der zum Element A gehörigen Matrix in $\Gamma_i \Gamma_k$ ist Produkt der entsprechenden Charaktere in Γ_i und Γ_k, daher wird

$$\chi^{(i)}(S)\, \chi^{(k)}(S) = \sum_{l=1}^{r'} g_{ikl} \chi^{(l)}(S),$$

oder:

$$\chi_j^{(i)} \chi_j^{(k)} = \sum_{l=1}^{r'} g_{ikl} \chi_j^{(l)} \qquad (j = 1, \ldots, r').$$

Es bleibt bloß noch übrig, r, die Anzahl der nicht äquivalenten Darstellungen, zu bestimmen. Bis jetzt können wir bloß sagen, daß $r' \leqq r$ ist. Denn wäre $r' > r$, so bestände zwischen den r' Charakterensystemen mindestens eine lineare Relation:

$$\sum_{i=1}^{r'} \alpha_i \chi_k^{(i)} = 0 \qquad (k = 1, \ldots, r).$$

Multipliziert man sie mit $\bar{\chi}_k^{(i)}$ $(k = 1, \ldots, r)$ und addiert, so folgt $\alpha_i = 0$.

Im nächsten Paragraphen werden wir zeigen, daß $r = r'$.

§ 46. Die Gruppendeterminante.

Die Quelle aller Darstellungen einer Gruppe ist diejenige durch eine ***reguläre*** Permutationsgruppe, die man erhält, indem man die Elemente $E, A, B, \ldots$ rechts der Reihe nach mit $E, A, B, \ldots$ multipliziert. Um die Gruppe leichter in Formeln darstellen zu

können, multipliziert man die Matrizen mit der zugehörigen Variablen $x_E, x_A, \ldots$ und addiert sie. Dann erhält man die folgende Matrix (vgl. die Gruppentafel auf S. 4)

$$(x_{P-1Q}) \quad P, Q = E, A, B, \ldots$$

Diese Matrix heißt die ***reguläre Gruppenmatrix,*** ihre Determinante die ***reguläre Gruppendeterminante.*** In der Tat: Die erste Zeile lautet offenbar $x_E, x_A, x_B, \ldots$, für die zweite hat man $AS\,x_S$ in die Reihenfolge $E, A, B, \ldots$ zu bringen, d. h. S in die Reihenfolge $A^{-1}E, A^{-1}A, A^{-1}B, \ldots$ usw.

In dieser Darstellung ist $\chi(E) = g$, $\chi(A) = 0$ für $A \neq E$, da die Permutationen, die zu den von E verschiedenen Elementen gehören, kein Element in Ruhe lassen. Wir bezeichnen diese Darstellung mit Π und setzen sie vollständig reduziert folgendermaßen an:

$$\Pi = n_1 \Gamma_1 + \ldots + n_{r'} \Gamma_{r'}.$$

Wenn wir die Charaktere links und rechts einander gleichsetzen, folgt:

$$\sum_{i=1}^{r'} n_i \chi^{(i)}(A) = \begin{cases} 0 \text{ für } A \neq E \\ g \text{ für } A = E. \end{cases}$$

Multipliziert man diese Gleichung mit $\chi^{(i)}(A^{-1})$ und addiert über alle Matrizen A, so erhält man rechts $g \cdot \chi^{(i)}(E)$, links wegen Satz 108 $n_i g$ und hieraus: $n_i = \chi^{(i)}(E)$. Hiermit sind nach der Methode vom letzten Paragraphen die irreduziblen Bestandteile von Π gefunden und wir haben den

Satz 113: *Die reguläre Darstellung Π von $\mathfrak{G}$ enthält jede irreduzible Darstellung so oft, als deren Grad beträgt.*

Zu jeder Klasse $\mathfrak{C}_i$ von Elementen gibt es eine Klasse, welche aus den inversen Elementen von $\mathfrak{C}_i$ besteht. Wir bezeichnen sie mit $\mathfrak{C}_{i'}$ und bemerken, daß $i = i'$ sein kann. $\mathfrak{C}_i$ und $\mathfrak{C}_{i'}$ bestehen aus gleichvielen, $h_i = h_{i'}$, Elementen. $\mathfrak{C}_i \mathfrak{C}_{i'}$ enthält die Klasse $\mathfrak{C}_1 = E$ genau h_i mal, während $\mathfrak{C}_i \mathfrak{C}_k \; (k \neq i') \; \mathfrak{C}_1$ nicht enthält.

Hieraus folgt, daß

$$c_{ik1} = \begin{cases} 0 \text{ für } k \neq i' \\ h_i \text{ für } k = i'. \end{cases}$$

Summieren wir nun die Gleichungen von Satz 112:

$$h_i \chi_i^{(v)} h_k \chi_k^{(v)} = \chi_1^{(v)} \sum_{l=1}^{r} c_{ikl} h_l \chi_l^{(v)}$$

über alle Werte $v = 1, \ldots, r'$, so folgt, da $h_1 = 1$ ist:

$$\sum_{v=1}^{r'} h_i \chi_i^{(v)} h_k \chi_k^{(v)} = \begin{cases} 0 \text{ für } k \neq i' \\ g h_i \text{ für } k = i' \end{cases}$$

und, da wir $h_i h_k$ vor das Summationszeichen setzen können, erhalten wir den

Satz 114: *Zwischen den Charakteren bestehen folgende Relationen:*

$$\sum_{v=1}^{r'} \chi_i^{(v)} \chi_k^{(v)} = \begin{cases} 0 & \text{für } k \neq i' \\ \frac{g}{h_i} & \text{für } k = i'. \end{cases}$$

Hieraus schließen wir, daß die r Reihen:

$$\begin{array}{cccc} \chi_1^{(1)} & \chi_1^{(2)} & \cdots & \chi_1^{(r')} \\ \chi_2^{(1)} & \chi_2^{(2)} & \cdots & \chi_2^{(r')} \\ \cdots & \cdots & \cdots & \cdots \\ \chi_r^{(1)} & \chi_r^{(2)} & \cdots & \chi_r^{(r')} \end{array}$$

linear unabhängig sind und daraus weiter, daß $r \leqq r'$. In Verbindung mit $r' \leqq r$ ergibt sich $r = r'$:

Satz 115: *Die Anzahl der nicht äquivalenten irreduziblen Darstellungen von $\mathfrak{G}$ ist gleich der Anzahl der Klassen der Elemente in $\mathfrak{G}$.*

§ 47. Übersicht.

Um eine Übersicht über die Relationen zwischen den Gruppencharakteren zu erhalten, bilden wir folgendes quadratische Schema:

	$\mathfrak{C}_1$	$\mathfrak{C}_2$	....	$\mathfrak{C}_r$
Γ_1	$\chi_1^{(1)}$	$\chi_2^{(1)}$	....	$\chi_r^{(1)}$
Γ_2	$\chi_1^{(2)}$	$\chi_2^{(2)}$	....	$\chi_r^{(2)}$
....	....	....	....	....
Γ_r	$\chi_1^{(r)}$	$\chi_2^{(r)}$	....	$\chi_r^{(r)}$

In jeder Zeile stehen die Charaktere einer irreduziblen Darstellung nach den Klassen von $\mathfrak{G}$ geordnet, in jeder Spalte diejenigen, welche zur selben Klasse von $\mathfrak{G}$ gehören, nach den verschiedenen Darstellungen geordnet.

1. *Zwischen den Zeilen* bestehen die bilinearen Beziehungen:

$$\sum_{i=1}^{r} h_i \chi_i^{(v)} \chi_i^{(w)} = \begin{cases} 0 & w \neq v' \\ g & w = v', \end{cases}$$

wobei $\chi^{(v')}$ den zu $\chi^{(v)}$ konjugiert imaginären Charakter bezeichnet, d. h. den zur adjungierten Darstellung gehörigen.

2. *Zwischen den Spalten* bestehen die Gleichungen:

$$\sum_{v=1}^{r} \chi_i^{(v)} \chi_k^{(v)} = \begin{cases} 0 & k \neq i' \\ \frac{g}{h_i} & k = i', \end{cases}$$

wobei $\chi_{i'}$ den zur inversen Klasse von χ_i gehörigen Charakter bezeichnet. Auch χ_i und $\chi_{i'}$ sind konjugiert imaginär.

3. Zwischen den Charakteren einer beliebigen *Zeile* bestehen die Gleichungen:

$$h_i h_k \chi_i \chi_k = \chi_1 \sum_{l=1}^{r} c_{ikl} h_l \chi_l .$$

4. Zwischen den Charakteren einer *Spalte* bestehen die Gleichungen:

$$\chi^{(u)} \chi^{(v)} = \sum_{w=1}^{r} g_{uvw} \chi^{(w)} .$$

Wir bemerken, daß 1 und 2 auseinander folgen, wenn man den Satz anwendet, daß zwei inverse Matrizen M und M^{-1} vertauschbar sind: $M M^{-1} = M^{-1} M = E$.

In der Tat: bezeichnet man die Matrix

$$(\chi_i^{(v)}) \qquad \begin{matrix} i = 1, \ldots, r \\ v = 1, \ldots, r \end{matrix}$$

mit X, so wird X^{-1} wegen der Relationen 1 gleich der transponierten Matrix zu

$$\left(\frac{h_i}{g} \chi_i^{(v')} \right).$$

Bildet man nun $X^{-1} X$, so erhält man:

$$\sum_{v=1}^{r} \frac{h_i}{g} \chi_i^{(v')} \chi_k^{(v)} = \begin{cases} 0 & i \neq k \\ 1 & i = k . \end{cases}$$

Nun ist $\chi_i^{(v')} = \chi_{i'}^{(v)}$, also:

$$\sum \chi_{i'}^{(v)} \chi_k^{(v)} = \begin{cases} 0 & i = k \\ \frac{g}{h_i} & i \neq k , \end{cases}$$

was gerade die Formeln 2 sind.

Die Größen c_{ikl} sind gewissen einfach anzugebenden Beschränkungen unterworfen. So ist: $c_{ikl} = c_{kil}$, denn $\mathfrak{C}_i \mathfrak{C}_k = \mathfrak{C}_k \mathfrak{C}_i$. Ferner wird, wie schon bemerkt,

$$c_{ik1} = \begin{cases} 0 & k \neq i' \\ h_i & k = i' . \end{cases}$$

Außerdem:

$$c_{1kl} = c_{k1l} = \begin{cases} 0 & l \neq k \\ 1 & l = k . \end{cases}$$

Schließlich gelten noch die komplizierten, aber für die Theorie der hyperkomplexen Zahlen fundamentalen Beziehungen, welche aus dem Bestehen der assoziativen Gesetze folgen: $(\mathfrak{C}_i \mathfrak{C}_j) \mathfrak{C}_k = \mathfrak{C}_i (\mathfrak{C}_j \mathfrak{C}_k)$.

Es wird:

$$(\mathfrak{C}_i \mathfrak{C}_j) \mathfrak{C}_k = \sum_{l=1}^{r} c_{ijl} \mathfrak{C}_l \mathfrak{C}_k = \sum_{l=1}^{r} \sum_{m=1}^{r} c_{ijl} c_{lkm} \mathfrak{C}_m .$$

Ebenso

$$\mathfrak{C}_i(\mathfrak{C}_j\mathfrak{C}_k) = \sum_{l=1}^{r} c_{jkl}\mathfrak{C}_i\mathfrak{C}_l = \sum_{l=1}^{r}\sum_{m=1}^{r} c_{jkl}c_{ilm}\mathfrak{C}_m.$$

Daher:

$$\sum_{l=1}^{r} c_{ijl}c_{lkm} = \sum_{l=1}^{r} c_{jkl}c_{ilm}.$$

Hierbei ist vom Bestehen des kommutativen Gesetzes kein Gebrauch gemacht.

Für die Größen g_{ikl} gelten ganz entsprechende Gleichungen:

$$g_{ikl} = g_{kil} \qquad \sum_{l=1}^{r} g_{ijl}g_{lkm} = \sum_{l=1}^{r} g_{jkl}g_{ilm},$$

$$g_{1kl} = g_{k1l} = \begin{cases} 0 & k \neq l \\ 1 & k = l, \end{cases}$$

$$g_{ik1} = \begin{cases} 0 & k \neq i' \\ 1 & k = i'. \end{cases}$$

Die Zahlen c_{ikl} und g_{uvw} lassen sich durch die Charaktere ausdrücken. So folgt aus:

$$h_i h_k \chi_i^{(v)}\chi_k^{(v)} = \chi_1^{(v)} \sum_{l=1}^{r} c_{ikl}\, h_l \chi_l^{(v)}$$

nach Multiplikation mit $\dfrac{\chi_{l'}^{(v)}}{\chi_1^{(v)}}$ und Summierung über v:

$$h_i h_k \sum_{v=1}^{r} \frac{\chi_i^{(v)}\chi_k^{(v)}\chi_{l'}^{(v)}}{\chi_1^{(v)}} = c_{ikl}\cdot g.$$

Ebenso findet man aus:

$$\chi_i^{(u)}\chi_i^{(v)} = \sum_{w=1}^{r} g_{uvw}\chi_i^{(w)}$$

nach Multiplikation mit $h_i\chi_i^{(w')}$ und Summation über i:

$$\sum_{i=1}^{r} h_i \chi_i^{(u)}\chi_i^{(v)}\chi_i^{(w')} = g_{uvw}\cdot g.$$

Aus dieser Gleichung ersieht man sofort, daß $g_{uvw} = g_{vuw}$, ferner $g_{uvw} = g_{w'vu'} = g_{uw'v'}$. Da die rechte Seite reell ist, bleibt die linke ungeändert, wenn man alle Zahlen durch die konjugiert komplexen, d. h. u durch u', v durch v', w' durch w ersetzt und man erhält $g_{uvw} = g_{u'v'w'}$.

Setzt man in der Relation 2. $i = k = 1$, so wird $h_i = 1$ und man erhält den

Satz 116: *Die Grade $\chi_1^{(1)}, \ldots, \chi_1^{(r)}$ der irreduziblen Darstellungen von $\mathfrak{G}$ genügen der Gleichung:*

$$\chi_1^{(1)2} + \cdots + \chi_1^{(r)2} = g.$$

Die Charaktere sind, als Summen von Einheitswurzeln, ganze algebraische Zahlen. Dasselbe gilt von den Ausdrücken $\frac{h_i \chi_i^{(v)}}{\chi_1^{(v)}}$. Denn bezeichnen wir sie bei festgehaltenem v mit $x_1, \ldots, x_r$, so genügen sie den Gleichungen:

$$x_i x_k = \sum_{l=1}^{r} c_{ikl} x_l .$$

Halten wir hierin den Index k fest, so folgt in bekannter Weise aus dem Bestehen der r Gleichungen $i = 1, \ldots, r$, daß x_k der Gleichung von t genügen muß:

$$\begin{vmatrix} c_{1k1} - t & c_{1k2} & \cdots & c_{1kr} \\ c_{2k1} & c_{2k2} - t & \cdots & c_{2kr} \\ \cdots & \cdots & \cdots & \cdots \\ c_{rk1} & c_{rk2} & \cdots & c_{rkr} - t \end{vmatrix} = 0 .$$

Hierin ist $(-1)^r$ der Koeffizient von t^r, die übrigen Koeffizienten sind ganze rationale Zahlen. Die r Wurzeln dieser Gleichung sind die r Zahlen:

$$\frac{h_k \chi_k^{(v)}}{\chi_1^{(v)}} \qquad (v = 1, \ldots, r)$$

Multipliziert man die Zahl $\frac{h_i \chi_i^{(v)}}{\chi_1^{(v)}}$ mit $\chi_i^{(v')}$ und summiert über i, so erhält man $\frac{g}{\chi_1^{(v)}}$. Nun muß die Summe ganzer Zahlen wiederum eine ganze Zahl sein und wir erhalten den

Satz 117: *Die Grade der irreduziblen Darstellungen von* $\mathfrak{G}$ *sind Teiler der Ordnung von* $\mathfrak{G}$.

Wir betrachten noch die Darstellungen ersten Grades von $\mathfrak{G}$. Eine solche ist zyklisch und homomorph mit der Faktorgruppe eines Normalteilers $\mathfrak{N}$ von $\mathfrak{G}$. Der Normalteiler $\mathfrak{N}$ enthält die Kommutatorgruppe von $\mathfrak{G}$. Umgekehrt ist jede Darstellung von $\mathfrak{G}/\mathfrak{C}$ auch Darstellung von $\mathfrak{G}$ und vom ersten Grade, falls sie irreduzibel ist, denn $\mathfrak{G}/\mathfrak{C}$ ist *Abel*sch. Daraus folgt der

Satz 118: *Ist* s *der Index der Kommutationsgruppe* $\mathfrak{C}$ *von* $\mathfrak{G}$, *so gibt es genau* s *irreduzible Darstellungen von* $\mathfrak{G}$, *die den Grad* 1 *haben, nämlich die* s *Darstellungen von* $\mathfrak{G}/\mathfrak{C}$.

Mit den Matrizen bilden auch deren Determinanten eine Darstellung von $\mathfrak{G}$, und zwar eine solche vom Grade 1. Daraus folgt der

Satz 119: *Diejenigen Substitutionen von* Γ, *deren Determinante* 1 *ist, bilden einen Normalteiler, dessen Faktorgruppe zyklisch ist.*

So besteht z. B. die alternierende Gruppe aus denjenigen Permutationen, deren Determinante $+1$ ist, während die übrigen die Determinante -1 haben.

§ 48. Vollständige Reduktion der Gruppenmatrix.

Die Formeln des vorigen Paragraphen erschöpfen nicht die ganze Fülle der Beziehungen zwischen den Koeffizienten der irreduziblen Substitutionsgruppen. Um diese zu finden, wenden wir ein neues Verfahren an mit Hilfe der hyperkomplexen Zahlen. Bereits im vorigen Paragraphen sind die Summen $\mathfrak{C}_i$ gebildet worden. Wir definieren jetzt allgemein:

Definition: Sind $e_1, e_2, \ldots, e_g$ Elemente einer Gruppe, so heißt $\zeta = a_1 e_1 + \ldots + a_g e_g$ eine ***hyperkomplexe Zahl***, wobei die Koeffizienten a irgendwelche reelle oder komplexe Zahlen sind. Ist $\eta = b_1 e_1 + \ldots + b_g e_g$ eine weitere, so heißt

$$\zeta + \eta = (a_1 + b_1) e_1 + \ldots + (a_g + b_g) e_g$$

die Summe und

$$\zeta \cdot \eta = a_1 b_1 e_1^2 + a_1 b_2 e_1 e_2 + \ldots + a_g b_g e_g^2$$

das Produkt von ζ und η. Offenbar gilt das assoziative und distributive Gesetz, dagegen nicht das kommutative für die Multiplikation. Ferner setzen wir fest: Ist $\zeta = \eta$, so ist $a_i = b_i$. Daraus folgt: Zwischen den n Zahlen $\zeta^{(k)} = a_1^{(k)} e_1 + \ldots + a_g^{(k)} e_g$ $(k = 1, \ldots, n)$ besteht dann und nur dann eine lineare Beziehung, wenn die sämtlichen n-reihigen Determinanten der Matrix $(a_i^{(k)})$ verschwinden. Die Relationen zwischen den hyperkomplexen Zahlen sind genau dieselben wie diejenigen zwischen den Zeilen in dieser Matrix.

Nunmehr betrachten wir irgendeine Darstellung Γ von $\mathfrak{G}$ durch Substitutionen. Die Matrizen seien $E, A, B, \ldots, S, \ldots$, die Elemente $e_E, e_A, e_B, \ldots, e_S, \ldots$, so daß, wenn $AB = C$, auch $e_A e_B = e_C$ ist; nun bilden wir die Matrix:

$$E \cdot e_E + A e_A + \ldots + S e_S + \ldots = \sum_S S e_S = M.$$

M kann offenbar auch durch (ζ_{ik}) bezeichnet werden, wobei

$$\zeta_{ik} = e_{ik} e_E + a_{ik} e_A + \ldots + s_{ik} e_S + \ldots$$

Setzt man M mit S^{-1} rechts zusammen, so ergibt sich:

$$M S^{-1} = S^{-1} e_E + A S^{-1} e_A + \ldots = E e_S + A e_{AS} + \ldots = M e_S$$

Bilden wir die erste Zeile rechts und links, so folgt:

$$\begin{aligned}
\zeta_{11} e_S &= \zeta_{11} \bar{s}_{11} + \zeta_{12} \bar{s}_{12} + \ldots + \zeta_{1n} \bar{s}_{1n} \\
\zeta_{12} e_S &= \zeta_{11} \bar{s}_{21} + \zeta_{12} \bar{s}_{22} + \ldots + \zeta_{1n} \bar{s}_{2n} \\
&\ldots\ldots\ldots\ldots\ldots\ldots \\
\zeta_{1n} e_S &= \zeta_{11} \bar{s}_{n1} + \zeta_{12} \bar{s}_{n2} + \ldots + \zeta_{1n} \bar{s}_{2n},
\end{aligned}$$

wobei $(\bar{s}_{ik})$ die zu S adjungierte Matrix bedeutet, d. h. die transponierte Matrix von S^{-1}.

Entprechende Formeln erhalten wir für die übrigen Zeilen. Das ergibt den

Satz 120: *Bei rechtsseitiger Multiplikation der Zahlen $\zeta_{i1}, \ldots, \zeta_{in}$ mit e_S erfahren sie die Substitutionen $\bar{S}$ von Γ_t.*

Genau gleich beweist man den analogen Satz:

Satz 121: *Bei linksseitiger Multiplikation mit $e_{S^{-1}}$ erfährt jede Spalte $\zeta_{1k}, \ldots, \zeta_{nk}$ die Substitution S.*

Nunmehr sei Γ irreduzibel. Es wird

$$\zeta_{ik} e_S = \sum_{j=1}^{n} \zeta_{ij} s_{kj}.$$

Multipliziert man diese Gleichung mit s_{lm} und addiert über alle S, so erhält man wegen Satz 106

$$\zeta_{ik} \cdot \sum_S s_{lm} e_S = \begin{cases} 0 & k \neq l \\ \frac{g}{\chi_1} \zeta_{im} & k = l. \end{cases}$$

Daher:

$$\zeta_{ik} \zeta_{lm} = 0 \quad k \neq l$$
$$\zeta_{ik} \zeta_{km} = \frac{g}{\chi_1} \zeta_{im},$$

entnimmt man dagegen die s'_{lm} aus irgendeiner irreduziblen, mit Γ nicht äquivalenten Darstellung von $\mathfrak{G}$, so erhält man $\zeta_{ik} \zeta'_{lm} = 0$.

Daraus erhalten wir den

Fundamentalsatz 122: *Zwischen den hyperkomplexen Zahlen ζ_{ik} der irreduziblen Substitutionsgruppe Γ bestehen die Beziehungen*

$$\zeta_{ik} \cdot \zeta_{lm} = 0 \quad (k \neq l)$$
$$\zeta_{ik} \zeta_{km} = \frac{g}{\chi_1} \zeta_{im}.$$

Stammt ζ'_{lm} aus einer mit Γ nicht äquivalenten irreduziblen Darstellung Γ', so gilt

$$\zeta_{ik} \zeta'_{lm} = 0$$

für alle Indizes.

Betrachtet man speziell die Koeffizienten von e_E, so erhält man die Beziehungen des Satzes 106 zurück, die übrigen ergeben neue Relationen.

Nunmehr sei $\Gamma_1, \ldots, \Gamma_r$ ein vollständiges System nicht äquivalenter irreduzibler Darstellungen von $\mathfrak{G}$.

Wir schreiben die Zahlen ζ_{ik} von $\Gamma_l (l = 1, 2, \ldots, r)$ in der nach Zeilen geordneten Reihenfolge auf: $\zeta_{11} \zeta_{12} \ldots \zeta_{1n} \zeta_{21} \zeta_{2n} \ldots \zeta_{nn}$; dann erhalten wir, wegen $\sum_{l=1}^{r} \chi_1^{(l)2} = g$, gerade g Zahlen, die mit $\zeta_1, \ldots, \zeta_g$ be-

zeichnet werden sollen. Multipliziert man sie rechts mit $e_S (S = E, A, \ldots)$, so erhält man eine Darstellung von $\mathfrak{G}$ in vollständig reduzierter Gestalt. Jeder irreduzible Bestandteil tritt darin gerade so oft auf, als sein Grad beträgt. Die g Zahlen $\zeta_1, \ldots, \zeta_g$ sind linear unabhängig. Ihre Matrix besteht nämlich aus den g Stellenzeilen der irreduziblen Darstellungen $\Gamma_1, \ldots, \Gamma_r$. Wir bezeichnen sie mit N. Nunmehr gehen wir über zu den adjungierten Darstellungen, die wir mit $\overline{\Gamma}_1, \ldots, \overline{\Gamma}_r$ bezeichen und bilden hierfür die Matrix $\overline{N}$. Setzen wir N mit $\overline{N}$ Zeile für Zeile zusammen, so erhalten wir, wegen Satz 106, eine Diagonalmatrix, deren Determinante sich leicht berechnet zu $\frac{g^g}{\prod_{\nu=1}^{r} \chi_1^{(\nu)} \chi_1^{(\nu)2}}$. Daher ist auch die Determinante von N von 0 verschieden. Hieraus folgt nun leicht der

Satz 123: *Die reguläre Gruppenmatrix läßt sich durch Transformation mit der aus einem vollständigen System irreduzibler Darstellungen genommenen Matrix N vollständig reduzieren.*

Beweis: Man erhält die reguläre Darstellung durch die Zahlen: e_E, $e_A, \ldots$, indem man sie der Reihe nach mit $e_S (S = E, A, B, \ldots)$ multipliziert. Aus ihnen gehen die Zahlen $\zeta_1, \ldots, \zeta_g$ durch die lineare Substitution N hervor, diese erfahren daher die durch N transformierten Substitutionen bei Multiplikation mit e_S.

Ist Γ eine beliebige Darstellung von $\mathfrak{G}$ mit den Matrizen $E, A, B, \ldots$, so kann man die Gruppenmatrix $(E x_E + A x_A + B x_B + \ldots)$ bilden. Ihre Determinante, die Gruppendeterminante, ist eine Form vom selben Grad wie Γ in den Variabeln $x_E, x_A, \ldots$. Wir bezeichnen sie mit $\Phi(x)$. Wenn nun Γ vollständig reduziert die Gestalt hat:

$$\Gamma = n_1 \Gamma_1 + \ldots + n_r \Gamma_r,$$

so wird $\Phi(x) = \Phi_1^{n_1}(x) \Phi_2^{n_2}(x) \ldots \Phi_r^{n_r}(x)$, wobei $\Phi_i(x)$ die Gruppendeterminante von Γ_i bedeutet. Die Formen Φ_i sind unzerlegbar, denn die Determinante (x_{ik}) ist als Funktion der n^2 Variablen x_{ik} betrachtet, unzerlegbar und Φ_i läßt sich durch eine lineare Substitution mit nicht verschwindender Determinante in diese Funktion transformieren, weil die n^2 Linearformen in der Gruppenmatrix von Γ_i linear unabhängig sind. Die reguläre Gruppendeterminante ist daher das Produkt der $\chi_1^{(i)}$-ten Potenzen aller $\Phi_i(x)$ und damit in ihre unzerlegbaren Bestandteile zerlegt.

Wie man sieht, entspricht jedem unzerlegbaren Faktor einer Gruppendeterminante ein irreduzibler Bestandteil der zugehörigen Substitutionsgruppe.

Zum Schluß soll noch gezeigt werden, wie man für zwei äquivalente irreduzible Darstellungen Γ und Γ' eine Substitution U finden

kann, welche Γ in Γ' überführt. Wir setzen, wie früher, $\zeta_{ik} = \sum_S s_{ik} e_S$ und weiter $\eta_{lm} = \sum_S s'_{lm} e_S$, wobei (s'_{ik}) die Matrizen von Γ' darstellen. Nun gilt offenbar:

$$U^{-1}(\zeta_{ik})\, U = (\eta_{ik}).$$

Setzt man $U = (u_{ik})$, $U^{-1} = (u^*_{ik})$, so wird

$$\eta_{ik} = \sum_{h,j} u^*_{ij}\, \zeta_{jh}\, u_{hk}.$$

Daher wird wegen Satz 122:

$$\eta_{ik}\, \zeta_{lm} = \frac{g}{\chi_1} \sum_j u^*_{ij}\, u_{lk}\, \zeta_{jm}.$$

Nun betrachte man auf beiden Seiten den Koeffizienten von e_E. Rechts ist er nur in ζ_{mm} von Null verschieden und gleich 1, daher ist rechts der Koeffizient von e_E gleich $u^*_{im}\, u_{lk} \frac{g}{\chi_1}$. Links ist er, wenn man die Matrix S^{-1} mit $(\bar{s}_{ik})$ bezeichnet, gleich $\sum_S s'_{ik}\, \bar{s}_{lm}$. Daher wird

$$\sum_S s'_{ik}\, \bar{s}_{lm} = \frac{g}{\chi_1}\, u^*_{im}\, u_{lk}.$$

Setzt man z. B. $i = m = 1$, so erhält man

$$\sum_S s'_{1k}\, \bar{s}_{l1} = \frac{g}{\chi_1}\, u^*_{11}\, u_{lk}$$

und kann so, falls u^*_{11} von 0 verschieden ist, die Größen u_{lk} bis auf einen gemeinsamen Faktor finden. Jedes U ist damit gefunden, denn U ist genau bis auf einen solchen Faktor bestimmt durch die Bedingung $U^{-1} \Gamma U = \Gamma'$.

§ 49. Einige Beispiele für die Darstellung von Gruppen.

Für *Abelsche Gruppen* lassen sich leicht die sämtlichen Darstellungen angeben. $A_1, \ldots, A_m$ mögen eine Basis von $\mathfrak{G}$ bilden und die zugehörigen Ordnungen seien $a_1, \ldots, a_m$. Nun bezeichne ε_i eine primitive a_i-te Einheitswurzel. Ersetzt man A_i durch irgendeine Potenz von ε_i $(i = 1, \ldots, m)$, so ist damit jedem Element ein Zahlwert zugeordnet. Man kann so den m Basiselementen auf $a_1 \cdot \ldots \cdot a_m$ verschiedene Weisen Zahlwerte zuordnen und hat also die sämtlichen irreduziblen Darstellungen auf diese Weise erhalten.

Bei der Komposition reproduzieren sie sich und bilden eine mit $\mathfrak{G}$ homomorphe Gruppe. Man ordne nämlich die Darstellung, bei der A_i durch $\varepsilon_i^{b_i}$ $(i = 1, \ldots, m)$ ersetzt ist, dem Element $A_1^{b_1} \ldots A_m^{b_m}$ zu. Ist bei einer weiteren A_i durch $\varepsilon_i^{c_i}$ dargestellt, so wird bei der komponierten A_i durch $\varepsilon_i^{b_i + c_i}$ ersetzt und für die zugeordneten Elemente gilt:

$$A_1^{b_1} \ldots A_m^{b_m} \cdot A_1^{c_1} \ldots A_m^{c_m} = A_1^{b_1 + c_1} \ldots A_m^{b_m + c_m}.$$

Wir gehen nunmehr über zu den *Diedergruppen*. Sie sind gegeben durch folgende Gleichungen:

$$A^m = E \qquad B^2 = E \qquad B^{-1} A B = A^{-1}.$$

Offenbar bildet $\{A\}$ einen Normalteiler vom Index 2. Daher erhält man zunächst 2 Darstellungen, nämlich die identische $A = B = (1)$ und die folgenden $A = (1) \quad B = (-1)$.

Weitere findet man in folgender Weise:

Sei ε eine primitive m-te Einheitswurzel und

$$A = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Diese Matrizen genügen den drei Bedingungen.

Allgemein erhält man die Darstellungen:

$$A = \begin{pmatrix} \varepsilon^i & 0 \\ 0 & \varepsilon^{-i} \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Ist zunächst m ungerade $= 2l + 1$, so erhält man, wenn man $i = 1, \ldots, l$ setzt, l verschiedene Darstellungen, weil für sie die charakteristischen Wurzeln von A sämtlich verschieden sind. Sie sind ferner irreduzibel, denn sie bilden keine kommutative Gruppe. Wir haben so l Gruppen vom Grade 2 und 2 vom Grade 1. Addiert man die Quadrate der Grade, so kommt:

$$l \cdot 4 + 2 = 2(2l + 1) = 2m = \text{Ordnung der Gruppe.}$$

Wir haben also alle Darstellungen der Diedergruppe gefunden. Sie sind sämtlich monomial.

Ist m gerade, so ergibt der Fall $i = \frac{m}{2}$ eine reduzible Darstellung: $A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, die in zwei verschiedenen Darstellungen vom Grade 1 zerfällt:

$$A = (-1) \quad B = (1) \quad \text{und} \quad A = (-1) \quad B = (-1).$$

Hier gibt es 4 Darstellungen vom Grade 1 und $\frac{m}{2} - 1$ vom Grade 2. Es wird wieder $4\left(\frac{m}{2} - 1\right) + 4 = 2m$.

Die *Quaternionen-Gruppe* ist definiert durch die Gleichungen:

$$A^4 = E \qquad B^2 = A^2 \qquad A^{-1} B A = B^{-1}.$$

$B^2 = A^2$ ist das einzige Element von der Ordnung 2. Es erzeugt einen Normalteiler mit zyklischer Faktorgruppe, deren Ordnung 4 ist. Dies ergibt 4 Darstellungen vom ersten Grad. Um eine weitere zu finden, wenden wir die Methoden der monomialen Darstellung an. $\{A\}$ ist zyklischer Normalteiler. Wir bilden:

$$E + i A + i^2 A^2 + i^3 A^3$$
$$B + i A B + i^2 A^2 B + i^3 A^3 B.$$

Man findet sofort, daß rechtsseitige Multiplikation mit A die Substitution ergibt:

$\begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$, während B die Substitution liefert: $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

Damit ist die irreduzible, weil nicht *Abel*sche Darstellung gefunden:

$$A = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Diese und die 4 vom Grade 1 bilden ein vollständiges System irreduzibler Darstellungen.

Man verifiziere in allen Fällen, daß die Anzahl der verschiedenen Darstellungen gleich der Anzahl der Klassen von Elementen ist.

Wir gehen nun über zur Untersuchung von *transitiven Permutationsgruppen* und beweisen den

Satz 124: *Jede transitive Permutationsgruppe Γ enthält die identische Darstellung genau einmal. Ist sie zweifach transitiv, so besteht sie vollständig reduziert aus der Summe der identischen und* ***einer*** *weiteren irreduziblen Darstellung.*

Beweis: Der Charakter einer Permutation ist gleich der Anzahl der Variablen, die ungeändert bleiben bei der Permutation. Nun ist nach Satz 73 die Summe aller Charaktere gleich der Ordnung der Gruppe, also enthält sie die identische Darstellung genau einmal. Es sei

$$\Gamma = n_1 \Gamma_1 + \ldots + n_r \Gamma_r,$$

daher der Charakter χ von Γ:

$$\chi = n_1 \chi_1 + \ldots + n_r \chi_r.$$

χ stimmt mit dem konjugierten Charakter überein. Wir bilden:

$$\sum_S \chi^2(S) = \sum_S (n_1 \chi_1(S) + \ldots + n_r \chi_r(S))\,(n_1 \bar{\chi}_1(S) + \ldots + n_r \bar{\chi}_r(S)).$$

Wegen der Relation 1 folgt:

$$\sum_S \chi^2(S) = g \cdot (n_1^2 + \ldots + n_r^2).$$

Nun ist nach dem Satz 74 $\sum_S \chi^2(S)$ gleich g mal der Anzahl der transitiven Systeme, in denen die Untergruppe, welche eine Variable ungeändert läßt, die Variablen permutiert. Ist die Gruppe zweifach transitiv, so wird also:

$$\sum_S \chi^2(S) = 2g.$$

Da nun $n_1 = 1$ ist, so folgt, daß nur noch eines der n von 0 verschieden und gleich 1 ist, womit der Satz bewiesen ist.

Es ist leicht, aus einer Permutationsgruppe die identische Darstellung herauszuschaffen. Sind $x_1, \ldots, x_n$ die Variabeln, so bilde man

$$y_1 = x_2 - x_1, \ldots, y_{n-1} = x_n - x_1.$$

Bei irgendeiner Permutation möge eine solche Differenz in $x_k - x_i$ übergehen. Dann drückt sich diese neue Differenz durch die alte aus mit Hilfe der Gleichungen:

$$x_k - x_i = y_{k+1} - y_{i+1}.$$

Bereits die $n-1$ Variablen $y_1, \ldots, y_{n-1}$ erfahren also eine lineare Substitution.

Mit Hilfe dieses Satzes können wir die sämtlichen Darstellungen der *Tetraedergruppe* bestimmen. Sie ist gleich der alternierenden Gruppe von 4 Variablen und besitzt 4 Klassen, nämlich 1. E, 2. die Elemente von der Ordnung 2: $(12)(34)$, $(13)(24)$, $(14)(23)$. Die Elemente von der Ordnung 3 zerfallen in 2 Klassen:

3. (123), (214), (341), (432) und
4. (124), (213), (342), (431).

Die 4 Charaktere sind 4, 0, 1, 1. Da die Gruppe zweifach transitiv ist, so bleibt nach Wegnahme von Γ_1 eine irreduzible Darstellung übrig, deren Charaktersystem folgendes ist: 3, -1, 0, 0. In der Tat ist:

$$1 \cdot 3^2 + 3 \cdot (-1)^2 + 4 \cdot 0^2 + 4 \cdot 0^2 = 12.$$

Die Gruppe besitzt einen Normalteiler von der Ordnung 4 und daher 3 Darstellungen 1. Grades, für welche sich die Charaktere leicht berechnen lassen. Sei ε eine 3. Einheitswurzel, so lautet die Tafel der Charaktere:

	$\mathfrak{C}_1$	$\mathfrak{C}_2$	$\mathfrak{C}_3$	$\mathfrak{C}_4$
Γ_1	1	1	1	1
Γ_2	1	1	ε	ε^{-1}
Γ_3	1	1	ε^{-1}	ε
Γ_4	3	-1	0	0

Das *Ikosaeder* gibt uns zu einigen weiteren Bemerkungen Anlaß. Seine Gruppe gestattet eine Darstellung durch reelle orthogonale Substitutionen von drei Variablen, entsprechend den Drehungen des Ikosaeders. Jede orthogonale Substitution von ungeradem Grade besitzt $+1$ als eine charakteristische Wurzel. In der Tat, ist A eine solche, so wird $A^{-1} = A^0$ die transponierte Matrix zu A. Ferner wird

$$(A - E)\, A^{-1} = (E - A^0).$$

Geht man zur Determinante über und bedenkt, daß $|A| = 1$ ist, so wird

$$|A - E| = |E - A|.$$

Andererseits wird $|A - E| = (-1)^n |E - A|$, wobei n der Grad von A ist. Daraus folgt, wenn n ungerade, $|A - E| = 0$, d. h. 1 ist charakteristische Wurzel von A.

Hiernach ist es leicht, die Charaktere der Darstellung zu berechnen. Die Gruppe besitzt 5 Klassen: E, ferner die 15 Substitutionen von der Ordnung 2, deren Wurzeln $(1, -1, -1)$ sind (Drehung um eine Achse mit Winkel 180^0), die 20 Substitutionen von der Ordnung 3. Die übrigen 24 von der Ordnung 5 zerfallen in zwei Klassen, solche von Drehungen um die Winkel $\pm\frac{2\pi}{5}$, resp. $\pm 2\cdot\frac{2\pi}{5}$. Die charakteristischen Wurzeln der Matrizen von der Ordnung 3 sind $1, \varepsilon, \varepsilon^{-1}$ ($\varepsilon =$ 3-te Einheitswurzel), da sie einer reellen Gleichung vom Grade 3 genügen, diejenigen der Matrizen von der Ordnung 5: $1, \eta, \eta^{-1}$ resp. $1, \eta^2, \eta^{-2}$ ($\eta =$ 5-te Einheitswurzel).

Die Charaktere sind infolgedessen:

2.) $3, -1, 0, 1+\eta+\eta^{-1}, 1+\eta^2+\eta^{-2}$, resp.

3.) $3, -1, 0, 1+\eta^2+\eta^{-2}, 1+\eta+\eta^{-1}$.

Hierbei ist (vgl. S. 134):

$$1+\eta+\eta^{-1}=\frac{+1+\sqrt{5}}{2}, \quad 1+\eta^2+\eta^{-2}=\frac{+1-\sqrt{5}}{2}.$$

Die Gruppe ist irreduzibel, denn:

$$1\cdot 3^2+15(-1)^2+20\cdot 0^2+12\cdot\left(\left(\frac{+1+\sqrt{5}}{2}\right)^2+\left(\frac{+1-\sqrt{5}}{2}\right)^2\right)=60.$$

Ferner repräsentiert sie zwei verschiedene irreduzible Darstellungen, deren Charakter durch 2.) resp. 3.) gegeben wird. Wir beweisen diese Behauptung durch die folgende Überlegung. Sei Γ eine beliebige Darstellung von $\mathfrak{G}$ und sei ferner irgendein Automorphismus von $\mathfrak{G}$ gegeben. Diesen führen wir in Γ, aber nicht in $\mathfrak{G}$ aus, und erhalten so offenbar eine neue Darstellung von $\mathfrak{G}$. Sie ist dann und nur dann nicht äquivalent mit Γ, wenn der Automorphismus auch im Charakterensystem eine Permutation hervorruft. In unserem speziellen Fall besitzt die Ikosaedergruppe einen derartigen Automorphismus. Als alternierende Gruppe ist sie Normalteiler vom Index 2 der symmetrischen Gruppe von 5 Variablen. Transformiert man sie durch ein Element dieser letzteren außerhalb der alternierenden Gruppe, so werden, wie man sich leicht überzeugt, gerade die beiden Klassen mit den Elementen von der Ordnung 5 vertauscht und bei diesem Automorphismus geht offenbar 2.) in 3.) über und 3.) in 2.)

Die weiteren irreduziblen Darstellungen sind nun leicht gefunden:

Als alternierende Gruppe von 5 Variablen besitzt sie eine Darstellung vom Grade 5 durch gerade Permutationen. Die Charaktere der Klassen sind folgende:

$$\mathfrak{C}_1:5 \qquad \mathfrak{C}_2:1 \qquad \mathfrak{C}_3:2 \qquad \mathfrak{C}_4 \text{ und } \mathfrak{C}_5:0.$$

Denn für $\mathfrak{C}_2$ kommt nur der Typus $(1\ 2)\ (3\ 4)$ in Betracht, für $\mathfrak{C}_3:(1\ 2\ 3)$, für $\mathfrak{C}_4$ und $\mathfrak{C}_5:(1\ 2\ 3\ 4\ 5)$.

Wir erhalten nach Wegnahme von Γ_1 eine Darstellung Γ_4 mit den Charakteren 4, 0, 1, -1, -1.

Um noch Γ_5 zu erhalten, beachten wir, daß sich die Gruppe auch als Permutationsgruppe von 6 Variablen darstellen läßt, nämlich der sechs Durchmesser, welche gegenüberliegende Ecken verbinden. Eine Drehung um einen solchen Durchmesser liefert ein Element von der Ordnung 5, und hierbei bleibt nur dieser eine Durchmesser ungeändert. Alle weiteren Drehungen, außer E_1 vertauschen alle Durchmesser.

Die Charaktere sind also hier 6, 0, 0, 1, 1, daher diejenigen von Γ_5: 5, -1, -1, 0, 0 und hier ist $1\cdot 5^2 + 15\cdot(-1)^2 + 20(-1)^2 = 60$, also ist Γ_5 irreduzibel. Wir bilden so die Tabelle:

	$\mathfrak{C}_1$	$\mathfrak{C}_2$	$\mathfrak{C}_3$	$\mathfrak{C}_4$	$\mathfrak{C}_5$
Γ_1	1	1	1	1	1
Γ_2	3	-1	0	$\frac{+1+\sqrt{5}}{2}$	$\frac{+1-\sqrt{5}}{2}$
Γ_3	3	-1	0	$\frac{+1-\sqrt{5}}{2}$	$\frac{+1+\sqrt{5}}{2}$
Γ_4	4	0	1	-1	-1
Γ_5	5	-1	-1	0	0

Als Beispiel für die Formel auf S. 122 geben wir:

$$g_{442}\cdot 60 = 1\cdot 4^2\cdot 3 + 15\cdot 0 + 20\cdot 0 + 12\left(\frac{1+\sqrt{5}}{2} + \frac{1-\sqrt{5}}{2}\right) = 60$$

$$g_{442} = 1,$$

d. h. in $\Gamma_4{}^2$ kommt Γ_2 genau einmal vor. Ebenso Γ_3 einmal. Ferner wird:

$$60\cdot g_{444} = 1\cdot 4^3 + 15\cdot 0 + 20\cdot 1^3 + 12\left((-1)^3 + (-1)^3\right) = 60$$

$$g_{444} = 1$$

und schließlich

$$60\cdot g_{445} = 1\cdot 4^2\cdot 5 + 15\cdot 0 + 20\cdot 1^2\cdot(-1) + 0 + 0 = 60.$$

Daher wird

$$\Gamma_4{}^2 = \Gamma_1 + \Gamma_2 + \Gamma_3 + \Gamma_4 + \Gamma_5.$$

Die bisherigen Überlegungen reichen vollkommen aus, um die Darstellungen selber zu berechnen. Für Γ_2 und Γ_3 kann man die Matrizen aus der analytischen Geometrie bestimmen als Drehungen des Raumes. Wir wollen sie jedoch direkt durch Reduktion einer Darstellung gewinnen und schicken noch einige allgemeine Bemerkungen voraus.

Um eine *Permutation* und die durch sie erzeugte zyklische Gruppe vollständig zu reduzieren, hat man sie erst in ihre Zyklen

zu zerlegen und diese zu reduzieren. Sei $(x_1, x_2, \ldots, x_n)$ ein solcher Zyklus, so bilde man, unter ε eine primitive n-te Einheitswurzel verstanden, die Ausdrücke

$$\begin{aligned}
&x_1 + x_2 + x_3 + \ldots + x_n = y_1,\\
&x_1 + \varepsilon x_2 + \varepsilon^2 x_3 + \ldots + \varepsilon^{n-1} x_n = y_2,\\
&x_1 + \varepsilon^2 x_2 + \varepsilon^4 x_3 + \ldots + \varepsilon^{2(n-1)} x_n = y_3,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&x_1 + \varepsilon^{n-1} x_2 + \varepsilon^{2(n-1)} x_3 + \ldots + \varepsilon^{(n-1)(n-1)} x_n = y_n.
\end{aligned}$$

Unter der zyklischen Vertauschung wird y_i mit dem Faktor $\varepsilon^{-(i-1)}$ versehen und die Reduktion ist geleistet. Die Matrix der n Linearformen, $(\varepsilon^{(i-1)(k-1)})$ $\begin{cases} i = 1, \ldots, n \\ k = 1, \ldots, n \end{cases}$, leistet diese Reduktion.

Ein wichtiges Hilfsmittel zur Auffindung irreduzibler Darstellungen bilden die transitiven *monomialen Gruppen*. Falls sie nicht schon Permutationsgruppen sind, enthalten sie die identische Darstellung nicht. Man erkennt leicht aus den Ausführungen von § 37, daß $\sum_S s_{ii} = 0$ ist, d. h. daß die Summe der Charaktere verschwindet. Nun gestattet die Ikosaedergruppe eine solche Darstellung vom Grade 6, denn sie besitzt eine Untergruppe von der Ordnung 10, die selbst einen Normalteiler vom Index 2 enthält. Geometrisch ist sie so zu definieren, daß man die 6 Durchmesser, welche gegenüberliegende Ecken verbinden, mit einem Richtungssinn versieht. Bei den Drehungen erfahren sie eine Vertauschung, teilweise verbunden mit Richtungsänderung. Findet Änderung statt, so versehe man die Variable mit dem Minuszeichen. Diese Darstellung ist reduzibel, und weil sie die identische Darstellung nicht enthält, kann sie nur Γ_2 und Γ_3 enthalten.

Beginnt man mit einer Drehung A von der Ordnung 5, so kann man die zugehörige Substitution mit $(x_1)\,(x_2, x_3, \ldots, x_6)$ bezeichnen. Sei B eine Drehung von der Ordnung 2, welche der Gleichung genügt $B^{-1}AB = A^{-1}$, so kann man B wählen als:

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ -x_1 & -x_2 & -x_6 & -x_5 & -x_4 & -x_3 \end{pmatrix}.$$

Als Permutationen der alternierenden Gruppe von 5 Variablen werden $A = (1\,2\,3\,4\,5)$, $B = (1\,4)(2\,3)$. Wählt man noch $C = (1\,2)(3\,4)$, so wird in monomialer Gestalt, wie man sich am Modell leicht überzeugt:

$$C = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ x_2 & x_1 & x_6 & -x_4 & -x_5 & x_3 \end{pmatrix}.$$

Setzt man $\{A\} = \mathfrak{H}$, $\mathfrak{H} + B\mathfrak{H} = \mathfrak{K}$, so wird die ganze Gruppe

$$\mathfrak{G} = \mathfrak{K} + \mathfrak{K}C + \mathfrak{K}CA + \mathfrak{K}CA^2 + \mathfrak{K}CA^3 + \mathfrak{K}CA^4.$$

Um die Gruppe zu reduzieren, hat man dies bloß bei A, B und C auszuführen. Wir beginnen mit A und führen daher die neuen Variablen ein:

$$y_1 = x_1, \qquad y_5 = x_2 + \varepsilon^2 x_3 + \dots + \varepsilon^8 x_6,$$
$$y_2 = x_2 + \varepsilon x_3 + \dots + \varepsilon^4 x_6, \qquad y_6 = x_2 + \varepsilon^{-2} x_3 + \dots + \varepsilon^{-8} x_6,$$
$$y_3 = x_2 + \varepsilon^{-1} x_3 + \dots \varepsilon^{-4} x_6, \qquad \varepsilon^5 = 1.$$
$$y_4 = x_2 + x_3 + \dots + x_6,$$

Übt man nun A aus, so erfahren die Variablen y die Substitution:

$$y_1' = y_1, \quad y_2' = \varepsilon^{-1} y_2, \quad y_3' = \varepsilon y_3,$$
$$y_4' = y_4, \quad y_5' = \varepsilon^{-2} y_5, \quad y_6' = \varepsilon^2 y_6.$$

Wenn man dagegen B ausübt, so wird:

$$y_1' = -y_1, \quad y_2' = -y_3, \quad y_3' = -y_2,$$
$$x_4' = -y_4, \quad y_5' = -y_6, \quad y_6' = -y_5.$$

Etwas umständlicher gestaltet sich die Ausübung von C. Wir setzen $\varepsilon + \varepsilon^{-1} = \alpha$, $\varepsilon^2 + \varepsilon^{-2} = \beta$ und finden, daß α und β der Gleichung genügen: $x^2 + x - 1 = 0$.

Wir haben

$$\alpha = \frac{-1+\sqrt{5}}{2}, \qquad \beta = \frac{-1-\sqrt{5}}{2}, \qquad \alpha - \beta = \sqrt{5}.$$

Dann wird

$$2 - \alpha = +\sqrt{5}\,\alpha, \qquad 2 - \beta = -\sqrt{5}\,\beta.$$

Nach leichter Rechnung findet man, daß die y die Substitution erfahren:

$$\begin{pmatrix}
0 & \frac{1}{5} & \frac{1}{5} & \frac{1}{5} & \frac{1}{5} & \frac{1}{5} \\
1 & \frac{\beta}{\sqrt{5}} & \frac{\alpha}{\sqrt{5}} & \frac{1}{\sqrt{5}} & 0 & 0 \\
1 & \frac{\alpha}{\sqrt{5}} & \frac{\beta}{\sqrt{5}} & \frac{1}{\sqrt{5}} & 0 & 0 \\
1 & \frac{1}{\sqrt{5}} & \frac{1}{\sqrt{5}} & 0 & \frac{-1}{\sqrt{5}} & \frac{-1}{\sqrt{5}} \\
1 & 0 & 0 & \frac{-1}{\sqrt{5}} & \frac{-\alpha}{\sqrt{5}} & \frac{-\beta}{\sqrt{5}} \\
1 & 0 & 0 & \frac{-1}{\sqrt{5}} & \frac{-\beta}{\sqrt{5}} & \frac{-\alpha}{\sqrt{5}}
\end{pmatrix}$$

Nun setze man

$$z_1 = \sqrt{5}\,y_1 + y_4, \qquad z_2 = y_2, \qquad z_3 = y_3,$$
$$z_4 = -\sqrt{5}\,y_1 + y_4, \qquad z_5 = y_5, \qquad z_6 = y_6.$$

Alsdann bleiben A und B ungeändert, während C übergeht in:

$$\begin{pmatrix} \frac{1}{\sqrt{5}} & \frac{2}{\sqrt{5}} & \frac{2}{\sqrt{5}} & 0 & 0 & 0 \\ \frac{1}{\sqrt{5}} & \frac{\beta}{\sqrt{5}} & \frac{\alpha}{\sqrt{5}} & 0 & 0 & 0 \\ \frac{1}{\sqrt{5}} & \frac{\alpha}{\sqrt{5}} & \frac{\beta}{\sqrt{5}} & 0 & 0 & 0 \\ 0 & 0 & 0 & -\frac{1}{\sqrt{5}} & -\frac{2}{\sqrt{5}} & -\frac{2}{\sqrt{5}} \\ 0 & 0 & 0 & -\frac{1}{\sqrt{5}} & \frac{-\alpha}{\sqrt{5}} & \frac{-\beta}{\sqrt{5}} \\ 0 & 0 & 0 & -\frac{1}{\sqrt{5}} & \frac{-\beta}{\sqrt{5}} & \frac{-\alpha}{\sqrt{5}} \end{pmatrix}$$

Hiermit ist die Reduktion ausgeführt und wir finden für Γ_2:

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \varepsilon^{-1} & 0 \\ 0 & 0 & \varepsilon \end{pmatrix}, \quad B = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}, \quad C = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 2 & 2 \\ 1 & \beta & \alpha \\ 1 & \alpha & \beta \end{pmatrix}.$$

Hierbei hat die Gruppe nicht reelle Gestalt, trotzdem sie mit einer orthogonalen Gruppe äquivalent ist. Man findet leicht, daß die quadratische Form $x_1^2 + x_2 x_3$ invariant ist gegenüber den drei Substitutionen.

12. Kapitel.

Anwendungen der Theorie der Gruppencharaktere.

§ 50. Ein Satz von *Burnside* über einfache Gruppen.

Frobenius und *Burnside* haben mit Hilfe der Gruppencharaktere wichtige Sätze über abstrakte Gruppen bewiesen.

Wir haben gesehen, daß stets $\frac{h_i \chi_i}{\chi_1}$ eine ganze algebraische Zahl ist. h_i und χ_1 sind ganze rationale Zahlen. Wenn daher h_i prim ist zu χ_1, so muß $\frac{\chi_i}{\chi_1}$ eine ganze algebraische Zahl sein. χ_i ist eine Summe von χ_1 Einheitswurzeln. Wir wollen annehmen, daß diese Einheitswurzeln nicht sämtlich untereinander übereinstimmen, andernfalls gehört die Substitution zum Zentrum. Indem man χ_i in der komplexen Zahlenebene als Summe von χ_1 Einheitsvektoren deutet, deren Richtung nicht stets dieselbe ist, erkennt man, daß $|\chi_i| < \chi_1$ ist. Daher wird $\left|\frac{\chi_i}{\chi_1}\right| < 1$. Für die konjugiert algebraischen Zahlen zu $\frac{\chi_i}{\chi_1}$ läßt sich dieselbe Ungleichung aufstellen. Daher wird das

Produkt derselben, die Norm von $\frac{\chi_i}{\chi_1}$, ihrem Betrag nach kleiner als 1, und da $\frac{\chi_i}{\chi_1}$ eine ganze Zahl sein muß, so wird $\chi_i = 0$. Hieraus folgt der

Satz 125: *Ist in einer irreduziblen Substitutionsgruppe der Grad prim zu der Anzahl der Elemente in einer Klasse $\mathfrak{C}_i$, so ist entweder der Charakter der Elemente von $\mathfrak{C}_i$ gleich 0 oder $\mathfrak{C}_i$ besteht aus einem Element des Zentrums der Gruppe.*

Wir beweisen nun den

Satz 126: *Wenn die Anzahl der Elemente einer Klasse eine Primzahlpotenz ist, so ist die Gruppe nicht einfach.*

Beweis: Sei A ein Element aus einer Klasse, die aus p^m Elementen besteht. Es gibt gewiß eine von Γ_1 verschiedene Darstellung, deren Grad prim ist zu p, denn $\sum(\chi_1^i)^2 = g$ und $\chi_1^1 = 1$. χ_i sei der Charakter von A in einer solchen Darstellung. Dann ist wegen dem vorigen Satz $\chi_i = 0$ oder A gehört zum Zentrum in der betreffenden Darstellung. Dieser letztere Fall kann bei einfachen Gruppen nicht auftreten. Nun gilt $\sum_{k=1}^{r} \chi_1^k \chi_i^k = 0$. In Γ_1 ist $\chi_i^1 = 1$, sonst ist stets $\chi_1^k \chi_i^k$ entweder 0 oder durch p teilbar und wir erhalten den Widerspruch

$$1 \equiv 0 \pmod{p}.$$

Es gibt also eine mit der Gruppe isomorphe Gruppe, deren Zentrum Elemente von der Ordnung p enthält.

Satz 127[1]**:** *Wenn die Ordnung einer Gruppe bloß durch zwei verschiedene Primzahlen teilbar ist, so ist die Gruppe auflösbar.*

Beweis: Sei $g = p^a q^b$. Eine p-*Sylow*gruppe enthält ein Zentrum. Sei A ein Element daraus, so ist die Anzahl der Elemente in der Klasse von A eine Potenz von q. Daher enthält die Gruppe einen Normalteiler. Für ihn und seine Faktorgruppe gilt dasselbe.

§ 51. Primitive und imprimitive Substitutionsgruppen.

Definition: Eine Substitutionsgruppe heißt ***imprimitiv***, wenn ihre Variablen dergestalt in Systeme eingeteilt werden können, daß die Variablen eines jeden Systems in lineare Formen der Variablen desselben oder eines andern Systems übergeführt werden. Mit demselben Ausdruck bezeichnet man auch alle äquivalenten Gruppen.

Geht ein System über in Formen eines zweiten, so müssen beide

[1]) *Burnside*: Theory of groups, 2nd ed., S. 323.

Systeme dieselbe Anzahl von Variablen enthalten. Als Beispiel wählen wir folgendes in drei Systemen

$$\begin{pmatrix} 0 & P & 0 \\ 0 & 0 & Q \\ R & 0 & 0 \end{pmatrix}.$$

Dabei bedeuten 0 quadratische Matrizen von r Zeilen, deren Koeffizienten sämtlich verschwinden, während P, Q und R Matrizen mit von 0 verschiedener Determinante bedeuten. Hier erfahren die Systeme eine zyklische Permutation nebst Substitutionen.

Permutationsgruppen sind spezielle Fälle, denn hier bildet jede Variable für sich ein derartiges System. Dasselbe gilt von den monomialen Gruppen.

Definition: Eine Gruppe heißt ***transitiv***, wenn jedes System in ein beliebiges anderes übergeführt werden kann. Sei $\mathfrak{G}$ eine imprimitive transitive Substitutionsgruppe, $\mathfrak{H}$ diejenige Untergruppe, welche das erste System in sich substituiert, G_i eine Substitution, welche das erste in das i-te überführt, so wird

$$\mathfrak{G} = \mathfrak{H} + \mathfrak{H} G_2 + \ldots + \mathfrak{H} G_n,$$

wobei n den Index von $\mathfrak{H}$ oder, was damit gleichbedeutend ist, die Anzahl der Systeme bezeichnet.

Die Substitutionen, welche das erste System unter $\mathfrak{H}$ erfährt, bilden eine Darstellung von $\mathfrak{H}$. Wir sagen, die imprimitive Substitutionsgruppe ist ***erzeugt*** durch diese Darstellung von $\mathfrak{H}$. Eine Permutationsgruppe ist demnach erzeugt durch die *identische* Darstellung von $\mathfrak{H}$, eine monomiale durch irgendeine solche vom Grade 1. Man erkennt leicht, daß alle diese Definitionen logische Erweiterungen der früheren über Permutationsgruppen sind. Es gilt nun auch der folgende Satz, der Satz 94 als Spezialfall enthält

Satz 128: *Ist eine imprimitive Substitutionsgruppe gegeben, welche durch die Darstellung Γ der Untergruppe $\mathfrak{H}$ in $\mathfrak{G}$ erzeugt ist, so läßt sie sich dergestalt transformieren, daß die Teilmatrizen (im Beispiel P, Q, R) lauter Matrizen aus Γ sind.*

Beweis: G_i möge das erste System in das i-te überführen, es sei etwa S diese Substitutionsmatrix. Man übe auf das i-te System S^{-1} aus, dann wird G_i die Variabeln des ersten Systems einzeln in die Variabeln des i-ten Systems überführen, die Substitutionsmatrix wird die Einheitsmatrix. Macht man das für $i = 2, \ldots, n$, so erkennt man, daß diejenigen Teilmatrizen, welche das erste System in irgendein anderes überführen, in Γ enthalten sind. Denn jede Substitution hat die Gestalt $H G_i$, wobei H in $\mathfrak{H}$ ist. Nunmehr möge die beliebige Substitution K das i-te System in das k-te überführen und S sei die Substitutionsmatrix. Dann wird $G_i K$ das erste System in das k-te

überführen und S wird immer noch die Substitutionsmatrix sein. Daher ist S in Γ.

Satz 129: *Sei Γ eine Substitutionsgruppe mit einem Abelschen Normalteiler N, der nicht zum Zentrum gehört. Wenn N vollständig reduziert ist, so ist Γ intransitiv oder imprimitiv.*

Beweis: Der Normalteiler N wird vollständig reduziert bloß Darstellungen vom Grade 1 enthalten und es sei

$$\mathsf{N} = n_1 \mathsf{N}_1 + n_2 \mathsf{N}_2 + \ldots + n_n \mathsf{N}_n,$$

wobei N_i irreduzible Bestandteile von N sind. Die Matrizen von N sind Diagonalmatrizen, und wir können annehmen, daß ihre Hauptdiagonalen die Gestalt haben (ε_1(n_1-mal), ε_2(n_2-mal), ...), indem zunächst n_1-mal die Darstellung N_1, dann n_2-mal die Darstellung N_2 usw. steht. Nun sind die n Darstellungen $\mathsf{N}_1, \ldots, \mathsf{N}_n$ linear unabhängig. Man kann daher n Zahlen $\alpha_1, \ldots, \alpha_n$ finden dergestalt, daß $\sum_{i=1}^{n} \alpha_i A_i$, wobei A_i die Gruppe N durchläuft, eine beliebige Diagonalmatrix D mit der Hauptdiagonalen (η_1(n_1-mal), η_2(n_2-mal) usw.) darstellt. Insbesondere können wir annehmen, daß die *Zahlen η sämtlich untereinander verschieden sind*

Transformiert man N durch eine Substitution aus Γ, so erhält man einen Automorphismus von N. Die irreduziblen Darstellungen in N sind immer noch dieselben, weil sich bei der Transformation der Charakter der Substitutionen von N nicht ändert, aber die Reihenfolge der irreduziblen Bestandteile hat sich geändert. Zwar stehen immer noch an den n_1 ersten Stellen der Hauptdiagonalen gleiche Zahlen, aber die gehören eventuell einer anderen Darstellung an. *Bei der Transformation erfahren die verschiedenen irreduziblen Darstellungen N_i eine Vertauschung.* Hierbei kann N_i nur dann in N_k übergehen, wenn $n_i = n_k$. Insbesondere geht D über in diejenige Diagonalmatrix, welche durch die entsprechende Vertauschung der η hervorgerufen wird. An dieser Matrix machen wir nun die weiteren Überlegungen. Wir nehmen an, daß bei den Transformationen von Γ nicht alle η ineinander übergeführt werden können. Setzen wir die Hauptdiagonale von D (also die η)

$$= (a_1, \ldots, a_r, b_{r+1}, \ldots, b_n),$$

so mögen stets die a unter sich, die b unter sich vertauscht werden, während alle a von allen b verschieden sind. Ist nun S eine beliebige Substitution von Γ, so sei

$$S^{-1} D S = D',$$

wobei die Hauptdiagonale von D' sei $(a'_1, \ldots, a'_r, b'_{r+1}, \ldots, b'_n)$, dann wird

$$D S = S D'.$$

Es wird also:

$$\begin{aligned} a_i s_{ik} &= a'_k s_{ik} && i, k \leqq r \\ a_i s_{ik} &= b'_k s_{ik} && i \leqq r,\ k > r \\ b_i s_{ik} &= a'_k s_{ik} && i > r,\ k \leqq r \\ b_i s_{ik} &= b'_k s_{ik} && i, k > r \end{aligned}$$

Wenn $s_{ik} \neq 0$, so kann man diesen Faktor auf beiden Seiten wegheben. In den mittleren Fällen kommt dann eine unmögliche Gleichung heraus, also sind alle

$$\begin{aligned} s_{ik} = 0 \text{ für } & i \leqq r \quad k > r \\ & i > r \quad k \leqq r, \end{aligned}$$

d. h. die Gruppe ist intransitiv.

Genau gleich verläuft der Beweis im transitiven Fall. Hier sind alle n_i einander gleich und die η erfahren eine transitive Permutationsgruppe. Indem man wiederum die Gleichung $D S = S D'$ diskutiert, folgt die Tatsache, daß die Gruppe imprimitiv ist. Sie wird erzeugt durch diejenigen Substitutionen, welche η_1 bei der Transformation in sich überführen.

Satz 130[1]: *Jede Gruppe, deren Ordnung eine Primzahlpotenz ist, läßt sich auf monomiale Gestalt transformieren.*

Beweis: Da der Satz für Gruppen von der Ordnung p und alle *Abel*schen Gruppen gilt, kann man vollständige Induktion anwenden. Wenn $\mathfrak{P}$ nicht *Abel*sch ist, so besitzt $\mathfrak{P}$ gewiß einen *Abel*schen Normalteiler, der nicht zum Zentrum gehört. Denn das Zentrum ist selber in einem Normalteiler von $\mathfrak{P}$ als Untergruppe vom Index p enthalten und dieser ist selbstverständlich *Abel*sch. Daher ist die Gruppe intransitiv oder imprimitiv. Da es offenbar genügt, den Satz für irreduzible, also transitive Gruppen zu beweisen, so können wir annehmen, die Gruppe sei imprimitiv. Sie sei erzeugt durch die Untergruppe $\mathfrak{H}$ von $\mathfrak{P}$ und deren Darstellung Γ. Von Γ können wir voraussetzen, daß sie monomiale Gestalt hat, da die Ordnung von $\mathfrak{H}$ niedriger als diejenige von $\mathfrak{P}$ ist, und nach Satz 94 folgt, daß die Teilmatrizen von $\mathfrak{P}$ sämtlich als Matrizen von $\mathfrak{H}$, also als monomiale Matrizen angenommen werden dürfen. Das heißt aber, daß $\mathfrak{P}$ selbst monomiale Gestalt hat.

Hiermit ist für alle Gruppen, deren Ordnung eine Primzahlpotenz ist, eine *kanonische Gestalt* gewonnen. Es wäre eine interessante Aufgabe, zu untersuchen, was für spezielle Eigenschaften diejenigen Untergruppen haben, die irreduzible Darstellungen erzeugen.

---

[1]) Der erste einwandfreie Beweis des Satzes stammt wohl von *Blichfeldt* in Miller, Blichfeldt, Dickson, Finite groups, S. 231.

Satz 131: *Gruppen, deren Ordnung ein Produkt von lauter verschiedenen Primzahlen ist, lassen sich stets auf monomiale Gestalt transformieren.*

Beweis: Wir bilden eine Hauptreihe, die das Zentrum enthält. Hierin kommt ein Normalteiler vor, der das Zentrum als Untergruppe vom Primzahlindex enthält. Dieser Normalteiler ist *Abel*sch, und nun verläuft der Beweis genau so wie im vorigen Fall.

Satz 132: *Wenn sämtliche Darstellungen einer Gruppe als monomiale geschrieben werden können, so ist ihre Kommutatorgruppe eine eigentliche Untergruppe oder E.*

Beweis: Wir können uns auf den nicht *Abel*schen Fall beschränken und betrachten eine nicht *Abel*sche Darstellung vom niedrigsten Grad größer als 1. Wir nehmen sie in monomialer Gestalt an und ersetzen alle Einheitswurzeln durch 1. Alsdann erhalten wir eine Darstellung der Gruppe durch Permutationen, welche sicher nicht alle der identischen Permutation gleich sind. Die Gruppe ist reduzibel und kann bloß aus irreduziblen Darstellungen vom Grade 1 bestehen. Darunter gibt es solche, die von der identischen Darstellung verschieden sind, womit der Satz bewiesen ist.

Wir beweisen nun noch den allgemeinen

Satz 133: *Wenn eine irreduzible Substitutionsgruppe einen Normalteiler enthält, der vollständig reduziert mindestens zwei verschiedene Darstellungen besitzt, so ist die Gruppe imprimitiv.*

Beweis: Wir denken uns den Normalteiler N vollständig reduziert und betrachten die Substitutionen einer Klasse von N. Addieren wir sie, so erhalten wir Diagonalmatrizen. Jeder irreduzible Bestandteil liefert so viele gleiche Koeffizienten in der Hauptdiagonale, als sein Grad beträgt, und sie hängen in bekannter Weise mit den Charakteren zusammen.

Bei der Transformation von N mit einer beliebigen Substitution der Gruppe erfahren die Darstellungen im allgemeinen eine Vertauschung und man zeigt genau, wie im Beweis zu Satz 129, daß die Gruppe intransitiv oder imprimitiv ist. Als irreduzible Gruppe ist sie daher imprimitiv.

§ 52. Vollständige Reduktion imprimitiver Gruppen.

Man erhält einen tieferen Einblick in die imprimitiven Gruppen, wenn man sie mit der Gruppenmatrix in Beziehung setzt.

Sei $\mathfrak{G}$ die Gruppe und $\mathfrak{H}$ eine Untergruppe. Ordnet man nun die Elemente von $\mathfrak{G}$ nach $\mathfrak{H}$ und ihren rechtsseitigen Nebengruppen:

$$\mathfrak{G} = \mathfrak{H} + \mathfrak{H}S_2 + \cdots + \mathfrak{H}S_n$$

und bildet die Gruppenmatrix von $\mathfrak{G}$, so hat sie die Gestalt:

$$\begin{vmatrix} \mathsf{M} & \mathsf{M}S_2 & \dots & \mathsf{M}S_n \\ S_2^{-1}\mathsf{M} & S_2^{-1}\mathsf{M}S_2 & \dots & S_2^{-1}\mathsf{M}S_n \\ \dots & \dots & \dots & \dots \\ S_n^{-1}\mathsf{M} & S_n^{-1}\mathsf{M}S_2 & \dots & S_r^{-1}\mathsf{M}S_n \end{vmatrix}.$$

Hierbei bedeutet M die Gruppenmatrix $(x_{P^{-1}Q})$ von $\mathfrak{H}$ und P, Q durchlaufen die Elemente von $\mathfrak{H}$. Ferner bedeutet allgemein $S\mathsf{M}T$ die Matrix $(x_{SP^{-1}QT})$, wobei P und Q wiederum die Elemente von $\mathfrak{H}$ durchlaufen. Ersetzt man jedes Element A von $\mathfrak{H}$ durch das Element SAT, so geht M über in $S\mathsf{M}T$. Hieraus ersieht man, daß die reguläre Darstellung von $\mathfrak{G}$ angesehen werden kann als imprimitive Gruppe, erzeugt durch irgendeine reguläre Darstellung einer Untergruppe.

In der Hauptdiagonalen stehen die Gruppenmatrizen von $\mathfrak{H}$ und den konjugierten Gruppen. Da die Matrizen $S_i^{-1}\mathsf{M}S_k$ nur in der Bezeichnung der Variablen sich unterscheiden, so können sie alle durch dieselbe Substitution A in vollständig reduzierte Gestalt transformiert werden. Durch die Substitution

$$\begin{pmatrix} A & 0 & \dots & 0 \\ 0 & A & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & A \end{pmatrix}$$

wird die Gruppenmatrix dergestalt transformiert, daß die irreduziblen Bestandteile von $\mathfrak{H}$ hervorgehoben sind. Dies liefert gleichzeitig eine (nicht vollständige) Reduktion der Gruppenmatrix von $\mathfrak{G}$. *Ersetzt man* M *durch irgendeine irreduzible Gruppenmatrix von* $\mathfrak{H}$, *so erhält man die durch diese Darstellung von* $\mathfrak{H}$ *erzeugte imprimitive Darstellung von* $\mathfrak{G}$.

Die Gruppenmatrix wird nun zerlegt in solche imprimitive Darstellungen und jede tritt so oft auf, als der Grad der sie erzeugenden irreduziblen Darstellung von $\mathfrak{H}$ beträgt. Diese teilweise Zerlegung der Gruppenmatrix ist besonders wichtig für Fragen über die Zahlkörper, die zur Darstellung von Gruppen notwendig sind, denn hier treten offenbar nur solche Körper auf, die zur vollständigen Reduktion der Gruppenmatrix einer *Untergruppe* $\mathfrak{H}$ erfordert werden.

Wir beweisen folgenden

Satz 134 von *Schur*: *Ist n das kleinste gemeinsame Vielfache der Ordnungen der Elemente von $\mathfrak{G}$ und ist $\mathfrak{G}$ eine auflösbare Gruppe, so ist für jede Darstellung von $\mathfrak{G}$ höchstens der Körper der n-ten Einheitswurzeln erforderlich.*

Beweis: Wir wenden vollständige Induktion an und setzen den Satz als bewiesen voraus für Gruppen von niedrigerer Ordnung. Wir

werden also den Satz bloß für primitive Gruppen zu beweisen haben. Ein größter Normalteiler $\mathfrak{N}$ besitzt eine Primzahl als Index. Seine irreduziblen Bestandteile N stimmen überein nach Satz 133. Die Gruppe ist enthalten in einer der imprimitiven Darstellungen, die durch Benutzung der Gruppenmatrix von $\mathfrak{N}$ entstehen, und zwar, indem man sie etwa durch den irreduziblen Bestandteil N' ersetzt. Sehen wir nun zu, was für weitere Darstellungen von $\mathfrak{N}$ hierin enthalten sind, so erkennen wir, daß es die folgenden sind: $S_i^{-1}\mathsf{N}'S_i$ $(i=2,\ldots,r)$, d. h. es sind Darstellungen, die aus N' durch einen Automorphismus hervorgehen. Da unser Normalteiler einen Primzahlindex, etwa p, besitzt, so sind diese p irreduziblen Darstellungen entweder alle äquivalent oder alle verschieden.

Betrachten wir den ersteren Fall und nehmen wir die irreduzible Darstellung $\mathsf{N}'=\mathsf{N}$ von $\mathfrak{N}$ für sich. Da der Automorphismus $S^{-1}\mathfrak{N}S$ eine äquivalente Darstellung liefert, so gibt es eine Substitution $\bar{S}$, welche denselben Automorphismus für N leistet, und sie ist bis auf einen Faktor a bestimmt. S^p liefert einen inneren Automorphismus von $\mathfrak{N}$, daher stimmt $\bar{S}^p$ bis auf einen Faktor mit einer Substitution A aus N überein. Sei $\bar{S}^p=bA$, so setzen wir $a^p=\frac{1}{b}$, $\frac{1}{a}=\sqrt[p]{b}$. Dann wird $a\bar{S}=S$ eine Substitution sein, für die $S^p=A$ ist, und diese zusammen mit N liefert eine Darstellung von $\mathfrak{G}$, bei der $\mathfrak{N}$ irreduzibel ist. S erfordert außer dem Körper, in dem die Koeffizienten von N liegen, nur noch den Körper, in dem der Charakter dieser irreduziblen Darstellung von $\mathfrak{G}$ liegt. Denn S kann als eine Substitution genommen werden mit von 0 verschiedenem Charakter, weil es notwendigerweise außerhalb von $\mathfrak{N}$ solche geben muß. Aus $S^{-1}\mathfrak{N}S$ läßt sich S bestimmen bis auf den Faktor als eine Substitution im Körper der Darstellung von $\mathfrak{N}$. Aus dem Charakter von S bestimmt sich nun weiter der Faktor, so daß die Behauptung erwiesen ist.

Wenden wir uns dem zweiten Fall zu, so erkennen wir, daß die imprimitive Gruppe irreduzibel ist. Denn der Bestandteil $\mathfrak{N}$ besteht aus einer Summe von p verschiedenen irreduziblen Darstellungen. Bei der Transformation mit S und seinen Potenzen erfahren sie eine zyklische Vertauschung. Wenn die Gruppe zerlegbar wäre, so könnte $\mathfrak{N}$ in einem Bestandteil nur einen Teil dieser p Darstellungen enthalten, während doch eine zyklische Vertauschung aller p Darstellungen stattfindet.

Hiermit ist der Satz zurückgeführt auf den Fall eines Unterkörpers, denn der Charakter einer Darstellung ist gewiß in dem im Satz angegebenen Kreiskörper enthalten.

Über die vollständige Reduzierung einer imprimitiven Gruppe läßt sich folgender bemerkenswerte Satz beweisen:

Satz 135: *Wenn die durch die irreduzible Darstellung Δ der Untergruppe $\mathfrak{H}$ erzeugte imprimitive Darstellung Γ von $\mathfrak{G}$ die irreduzible Darstellung $\Gamma^{(u)}$ von $\mathfrak{G}$ genau k-mal enthält, so enthält in $\Gamma^{(u)}$ die Untergruppe $\mathfrak{H}$ vollständig reduziert Δ genau k-mal. Umgekehrt, wenn $\Gamma^{(u)}$ Δ k-mal enthält, so ist $\Gamma^{(u)}$ in der durch Δ erzeugten Darstellung von $\mathfrak{G}$ genau k-mal enthalten.*

Beweis: Bezeichnen wir mit $\chi(A)$ den Charakter der imprimitiven Darstellung Γ von $\mathfrak{G}$, mit $\psi(A)$ denjenigen von Δ, ferner mit $\chi^u(A)$ den Charakter der irreduziblen Darstellung $\Gamma^{(u)}$ von $\mathfrak{G}$, so ist:

$$\sum_{\mathfrak{G}} \chi(A)\chi^{(u')}(A) = kg,$$

wobei k angibt, wie oft $\Gamma^{(u)}$ in Γ enthalten ist. Um diese Summe zu bilden, benutzt man die Darstellung von Γ durch die Tabelle am Anfang des Paragraphen. Man sieht, daß

$$\sum_{\mathfrak{G}} \chi(A)\chi^{(u')}(A) = \sum_{\mathfrak{H}} \psi(A)\chi^{(u')}(A) + \sum_{S_2^{-1}\mathfrak{H}S_2} \psi(A)\chi^{(u')}(A) + \ldots.$$

Ist Δ in $\Gamma^{(u)}$ genau l mal enthalten, so wird $\sum_{\mathfrak{H}} \psi(A)\chi^{(u')}(A) = l \cdot h$. Alsdann haben aber die weiteren $n-1$ Summen den nämlichen Wert, denn konjugierte Untergruppen erfahren die nämliche Zerlegung. Daher hat die Summe links den Wert $l \cdot h \cdot n = lg$. Also ist $k = l$.

Aus diesem Satz lassen sich leicht die wichtigen Formeln von *Frobenius* herleiten, welche die Charaktere einer Gruppe mit denjenigen einer Untergruppe verknüpfen.

Sei $\Delta^{(v)}$ eine Darstellung von $\mathfrak{H}$ und $\psi^{(v)}$ ihr Charakter. In $\Gamma^{(u)}$ sei die Untergruppe $\mathfrak{H}$ vollständig reduziert und

$$\{\Gamma^{(u)}\} = \sum_v k_{uv} \Delta^{(v)},$$

wobei $\{\Gamma^{(u)}\}$ die Darstellung von $\mathfrak{H}$ als Untergruppe von $\Gamma^{(u)}$ bedeutet. Sei $\varphi^{(v)}$ der Charakter der durch $\Delta^{(v)}$ erzeugten imprimitiven Darstellung von $\mathfrak{G}$. Dann wird:

$$\varphi^{(v)} = \sum_u k_{uv} \chi^{(u)}.$$

Nun läßt sich aber $\varphi^{(v)}$ durch $\psi^{(v)}$ ausdrücken. Sei S irgendein Element aus $\mathfrak{H}$ und $\mathfrak{C} = S + T + \ldots$ die Klasse in $\mathfrak{G}$, zu der S gehört. Wir bestimmen den Wert der Summe:

$$\varphi^{(v)}(\mathfrak{C}) = \varphi^{(v)}(S) + \varphi^{(v)}(T) + \ldots = h_S \varphi^{(v)}(S),$$

wobei h_S die Anzahl der Elemente in $\mathfrak{C}$ bedeutet. Indem wir wiederum auf die Tabelle S. 141 zurückgehen, finden wir für die erste Matrix der Hauptdiagonalen $\Delta^{(v)}$ den Beitrag:

$$\sum_S \psi^{(v)}(S)$$

erstreckt über die Elemente S in $\mathfrak{C}$, die in $\mathfrak{H}$ vorkommen. Die übrigen

Matrizen der Hauptdiagonale: $S_i^{-1} A^{(v)} S_i$ liefern offenbar denselben Beitrag, und daher wird:

$$\varphi^{(v)}(\mathfrak{C}) = \frac{g}{h} \sum_S \psi^{(v)}(S).$$

So erhalten wir die Formel:

$$\sum_u k_{uv} \chi^{(u)}(S) = \frac{g}{h \cdot h_S} \sum_T \psi^{(v)}(T),$$

die Summe rechts erstreckt über die Elemente der Klasse von S, die in $\mathfrak{H}$ auftreten.

Dies ist die Formel von *Frobenius;* sie läßt sich auch mit Hilfe der Relationen zwischen den Gruppencharakteren herleiten (vgl. *Burnside,* Theory of groups, S. 330). Über die Zahlen k_{uv} sei noch bemerkt, daß stets $k_{uv} = k_{u'v'}$ ist, wenn $\chi^{(u')}$ resp. $\psi^{(v')}$ die zu $\chi^{(u)}$ resp. $\psi^{(v)}$ adjungierten Charaktere sind. Ferner ist

$$k_{u1} = \begin{cases} 1 \text{ für } u = 1 \\ 0 \text{ „ } u > 1 \end{cases}.$$

Aus diesen Formeln hat *Frobenius* (Berl. Ber. 1901) folgenden Satz hergeleitet:

Satz 136: *Wenn $\mathfrak{G}$ eine Untergruppe $\mathfrak{H}$ besitzt, die mit keinem Element außerhalb von $\mathfrak{H}$ vertauschbar ist und mit keiner ihrer konjugierten ein Element außer E gemeinsam hat, so bilden die Elemente außerhalb von $\mathfrak{H}$ und den dazu konjugierten Gruppen zusammen mit E einen Normalteiler von $\mathfrak{G}$.*

Als Satz über Permutationsgruppen lautet er folgendermaßen: *Wenn außer E alle Permutationen einer transitiven Gruppe vom Grade n höchstens eine Variable ungeändert lassen, so bilden diejenigen, welche alle Variablen permutieren, zusammen mit E einen Normalteiler von der Ordnung n.*

Beweis: Stellen wir $\mathfrak{G}$ als Permutationsgruppe dar, indem wir $\mathfrak{H}$ als erzeugende Untergruppe nehmen, so hat jedes Element von $\mathfrak{H}$ und seinen konjugierten Gruppen den Charakter 1, außer E, das den Charakter n (= Index von $\mathfrak{G}$) hat. Die übrigen Elemente besitzen 0 als Charakter. Nimmt man die identische Darstellung weg, so hat E den Charakter $n-1$, die $n-1$ Elemente außerhalb $\mathfrak{H}$ und seinen konjugierten Gruppen haben den Charakter -1, alle übrigen 0. Nun sei $\Gamma^{(u)}$ eine Darstellung von $\mathfrak{G}$, welche nicht in dieser Permutationsgruppe enthalten ist. Dann gilt offenbar $(n-1)\chi_1^{(u)} = \sum \chi^{(u)}(S)$ die Summe erstreckt über die erwähnten $n-1$ Elemente. Rechts steht eine Summe von $\chi_1^{(u)}(n-1)$ Einheitswurzeln. Da sie gleich $(n-1)\chi_1^{(u)}$ sein muß, so muß jede Wurzel gleich 1 sein, wie die geometrische Deutung sofort zeigt, daher gehören diese $n-1$ Elemente zusammen mit E zu einem Normalteiler $\mathfrak{N}$ von $\mathfrak{G}$. Aber außer diesen gibt es

kein Element mehr, dessen charakteristische Wurzeln sämtlich gleich 1 sind, also ist der Satz bewiesen. Alles kommt darauf an, zu zeigen, daß die Permutationsgruppe nicht jede Darstellung von $\mathfrak{G}$ enthält.

Wiederum seien $\Gamma^{(u)}$ und $\chi^{(u)}$ die irreduziblen Darstellungen von $\mathfrak{G}$ und ihre Charaktere, $\Delta^{(v)}$ und $\psi^{(v)}$ dasselbe für $\mathfrak{H}$. Ferner sei $E^{(v)}$ und $\varphi^{(v)}$ die imprimitive Darstellung von $\mathfrak{G}$, welche durch $\Delta^{(v)}$ erzeugt ist, und ihr Charakter. Dann gilt:

$$\varphi^{(v)} = \sum_u k_{uv}\chi^{(u)}.$$

Nun ist offenbar

$$\varphi^{(v)}(E) = n\cdot\psi^{(v)}(E)$$
$$\varphi^{(v)}(S) = \psi^{(v)}(S) \qquad (S \neq E \text{ und in } \mathfrak{H}).$$

Damit ist $\varphi^{(v)}$ für jedes Element von $\mathfrak{H}$ und seinen konjugierten Gruppen bestimmt. Für alle übrigen $(n-1)$ ist

$$\varphi^{(v)}(S) = 0.$$

Wir bilden nunmehr

$$\sum_{\mathfrak{G}} \varphi^{(v)}(S)\varphi^{(w')}(S) = \sum_{\mathfrak{G}} \{(\sum_u k_{uv}\chi^{(u)}(S))(\sum_u k_{uw'}\chi^{(u)}(S))\}$$
$$= g\sum_u k_{uv}k_{u'w'} = g\sum_u k_{uv}k_{uw}.$$

Andererseits findet man, wenn man die Werte von φ berücksichtigt:

$$\sum_{\mathfrak{H}} \varphi^{(v)}(S)\varphi^{(w')}(S) = \sum_{\mathfrak{H}} \psi^{(v)}(S)\psi^{(w')}(S) + (n^2-1)\psi^{(v)}(E)\psi^{(w')}(E).$$

Die erste Summe rechts ist $= h$ oder $= 0$, je nachdem $w = v$ oder $w \neq v$. Dasselbe erhält man, wenn man über die konjugierten Gruppen von $\mathfrak{H}$ summiert. Addiert man alles, so erhält man $\sum_{\mathfrak{G}} \varphi^{(v)}(S)\varphi^{(w')}(S)$, nur ist das Einheitselement n-mal gezählt. Daher findet man für die Summe $g\sum_u k_{uv}k_{uw}$:

$$g + n\cdot(n^2-1)\psi^{(v)}(E)\psi^{w'}(E) - (n-1)n^2\psi^{(v)}(E)\psi^{(w')}(E) \qquad w = v$$
$$0 + \ldots\ldots\ldots\ldots\ldots\ldots \qquad w \neq v$$

oder, da $\psi^{(w')}(E) = \psi^{(w)}(E)$ ist:

$$\sum_u k_{uv}k_{uw} = \begin{cases} \frac{n-1}{h}\psi^{(v)}(E)\psi^{(w)}(E) + 1 & (w = v) \\ \frac{n-1}{h}\psi^{(v)}(E)\psi^{(w)}(E) & (w \neq v). \end{cases}$$

Berechnet man nun $\sum_u (k_{uv} - \psi^{(v)}(E)k_{u1})^2$, so erhält man:

$$\sum_u (k_{uv} - \psi^{(v)}(E)k_{u1})^2 = 1 + (\psi^{(v)}(E))^2.$$

Der erste Term in der Summe $(u = 1)$ ist:

$$(k_{1v} - \psi^{(v)}(E)\cdot k_{11})^2 = \psi^{(v)}(E)^2 \qquad \text{für } v > 1.$$

Daher wird

$$\sum_{u=2}^{r}(k_{uv} - \psi^{(v)}(E)\,k_{u1})^2 = 1 \qquad \text{für } v > 1.$$

Folglich wird gerade ein Term $= \pm 1$, die andern $r - 2$ verschwinden. Genau gleich zeigt man, daß

$$\sum_{u=2}^{r}(k_{uv} - \psi^{(v)}(E)\,k_{u1})(k_{uw} - \psi^{(w)}(E)\,k_{u1}) = 0$$

für $w > 1$ und $v > 1$ und untereinander verschieden.

Daher sind die Werte von u, für die

$$k_{uv} - \psi^{(v)}(E)\,k_{u1} \quad \text{und} \quad k_{uw} - \psi^{(w)}(E)\,k_{u1}$$

von 0 verschieden sind, verschieden, und eine geeignete Numerierung ergibt die Formeln:

$$k_{aa} - \psi^{(a)}(E)\,k_{a1} = \pm 1 \qquad (a = 2, 3, \ldots)$$
$$k_{ab} - \psi^{(b)}(E)\,k_{a1} = 0 \qquad a \neq b, \quad a > 1.$$

Nun war:

$$\sum_{u} k_{uv}\,\chi^{(u)}(E) = \psi^{(v)}(E)\cdot n$$

und speziell

$$\sum_{u} k_{u1}\,\chi^{(u)}(E) = n.$$

Daher wird:

$$\sum_{u}(k_{uv} - \psi^{(v)}(E)\,k_{u1})\,\chi^{(u)}(E) = 0.$$

Als ersten Term $u = 1$ erhalten wir (da $v > 1$): $-\psi^{(v)}(E)$. Sonst sind alle $= 0$, außer demjenigen mit $u = v$, der den Wert hat $\pm\chi^{(v)}(E)$. Daher wird

$$-\psi^{(v)}(E) \pm \chi^{(v)}(E) = 0,$$

es gilt also stets das Zeichen $+$ und es wird

$$\chi^{(v)}(E) = \psi^{(v)}(E).$$

Nimmt man nun die Darstellung vom niedrigsten Grade nächst $\Gamma^{(1)}$, etwa $\Gamma^{(2)}$, so ist dieser Grad auch der niedrigste für die Darstellungen von $\mathfrak{H}$, nächst der identischen. Da die Untergruppe $\mathfrak{H}$ in $\Gamma^{(2)}$ nicht die identische sein kann, so muß sie irreduzibel sein. Sie enthält also die identische Darstellung nicht. $\Gamma^{(2)}$ ist die gesuchte Gruppe $\Gamma^{(u)}$; womit der Satz bewiesen ist.

13. Kapitel.

Arithmetische Untersuchungen über Substitutionsgruppen.

§ 53. Beschränkung auf algebraische Zahlkörper.

Satz 137: *Jede endliche Gruppe linearer Substitutionen läßt sich so transformieren, daß ihre Koeffizienten in einem algebraischen Zahlkörper liegen.*

Beweis: Es genügt, den Satz für irreduzible Gruppen zu beweisen. Γ sei eine solche vom Grade n und

$$\mathsf{M} = E\,x_E + A\,x_A + \ldots = (z_{ik})$$

sei ihre Gruppenmatrix. Die Determinante von M besitzt als Koeffizienten Zahlen des durch den Charakter von Γ bestimmten Körpers k. Die z_{ik} sind n^2 Linearformen der x, welche unabhängig voneinander sind. Daraus folgt, daß die charakteristische Gleichung der Gruppenmatrix unzerlegbar ist; man kann daher nach einem Satz von *Hilbert* (Crelle's Journ. 110 S. 104) den Variabeln x solche Werte aus k beilegen, daß die charakteristische Gleichung lauter verschiedene Wurzeln hat. Eine solche Matrix sei M, die x mögen also Zahlen aus k bedeuten. M läßt sich als Matrix mit lauter verschiedenen Wurzeln auf die Diagonalform transformieren. Dieselbe Transformation denken wir uns auf $E, A, B, \ldots$ ausgeübt und nehmen unter Beibehaltung der bisherigen Bezeichnung an, daß M die Diagonalform hat. Ihre Hauptdiagonale sei

$$\alpha_1, \alpha_2, \ldots, \alpha_n.$$

Mit M sind auch sämtliche Potenzen lineare Ausdrücke der Substitutionen von Γ. Nun sei S eine beliebige Substitution von Γ. Der Charakter von MS ist einerseits

$$\alpha_1 s_{11} + \alpha_2 s_{22} + \ldots + \alpha_n s_{nn} = \gamma,$$

andererseits gleich dem Charakter von

$$S\,x_E + A\,S\,x_A + \ldots,$$

d. h. eine Zahl aus k. Macht man dasselbe für die Potenzen von M, so findet man, daß

$$^i s_{11} + \alpha_2^i s_{22} + \ldots + \alpha_n^i s_{nn} = \gamma_i \qquad (i = 1, 2, \ldots, n)$$

sämtlich Zahlen aus k sind. Aus diesen n Gleichungen lassen sich die Zahlen $s_{11}, \ldots, s_{nn}$ berechnen und man findet, daß sie dem Zahlkörper K angehören, der durch k und die Wurzeln $\alpha_1, \ldots, \alpha_n$ bestimmt ist. Diese Tatsache gilt für alle Matrizen von Γ.

Nun bilden wir wie in § 48 die Matrix

$$E e_E + A e_A + \ldots = (\xi_{ik}).$$

Die Koeffizienten von ξ_{11} liegen in K. Multipliziert man ξ_{11} rechts mit allen e_S, so erhält man genau n unabhängige hyperkomplexe Zahlen, deren Koeffizienten sämtlich in K liegen, alle übrigen drücken sich linear und mit Koeffizienten aus K durch sie aus. Multipliziert man diese daher rechts mit e_S, so erfahren sie eine Substitution mit Koeffizienten aus K. Die so entstehende Gruppe ist äquivalent mit der adjungierten zu Γ, womit der Satz bewiesen ist.

Satz 138: *Wenn Γ eine Substitution S enthält, welche eine ihrer charakteristischen Wurzeln, z. B. ε, nur einmal enthält, so läßt sie sich so transformieren, daß ihre Koeffizienten in dem durch die Charaktere von Γ und durch ε bestimmten Zahlkörper k liegen.*

Beweis: Wir nehmen Γ in einem algebraischen Zahlkörper an, dann reduzieren wir S auf die Diagonalform, was nur algebraische Irrationalitäten erfordert. Γ möge jetzt im Körper K liegen, die *Galois*sche Gruppe von K in k sei $\mathfrak{Z}$. Übt man auf die Koeffizienten von Γ die Substitutionen von $\mathfrak{Z}$ aus, so erhält man lauter äquivalente Gruppen $\Gamma, \Gamma', \ldots$, denn die Charaktere bleiben ungeändert. Es sei z. B. $T^{-1}\Gamma T = \Gamma'$. Nun bedenken wir, daß S seine Diagonalform beibehält und daß ε, welches die Stelle s_{11} einnehmen möge, ungeändert bleibt. Es folgt daraus, daß T reduzierte Gestalt hat und in einen Bestandteil vom Grade 1 nebst einem solchen vom Grade $n-1$ zerfällt. Daher bleiben unter T die Koeffizienten $a_{11}, b_{11}, \ldots$ aller Substitutionen von Γ ungeändert, d. h. diese Stellenzeile liegt in k. Daraus folgt der Satz 138.

Satz 139: *Wenn $m\Gamma$ in einem Zahlkörper k irreduzibel ist, so ist m ein Teiler des Grades n von Γ. Hierbei bedeutet Γ eine absolut irreduzible Gruppe.*

Beweis: Die Substitutionen von $m\Gamma$ seien $E, A, B, \ldots$ Wir bilden

$$E e_E + A e_A + \ldots = (\xi_{ik})$$

und betrachten die Zeilen

$$\xi_{i1}, \xi_{i2}, \ldots, \xi_{il} \qquad (i = 1, 2, \ldots, l;\ l = m.n).$$

Jede dieser Zeilen erfährt bei rechtsseitiger Multiplikation mit e_S die Substitutionen der zu $m\Gamma$ adjungierten Gruppe. Die Zahlen jeder Zeile sind linear unabhängig, denn die Beziehungen ließen sich in K herstellen und daher wäre die Gruppe in K reduzibel.

Betrachten wir nun die l Systeme hyperkomplexer Zahlen

$$x_1 \xi_{i1} + \ldots + x_l \xi_{il} \qquad (i = 1, 2, \ldots, l),$$

wo die x alle Zahlen von K durchlaufen. Wenn das erste mit dem

zweiten gemeinsame Zahlen hat, so sind sie identisch, denn die gemeinsamen Zahlen lassen sich durch eine Basis darstellen und ihre Gesamtheit bleibt unverändert bei rechtsseitiger Multiplikation mit e_S. Man erkennt, daß die Anzahl der unabhängigen Zahlen ein Vielfaches von l ist. Andererseits ist diese Zahl gleich n^2, weil Γ der einzige absolut irreduzible Bestandteil ist. Daher ist m ein Teiler von n.

Satz 140: *Zwei in einem beliebigen Zahlkörper K irreduzible Gruppen sind entweder äquivalent oder sie haben keinen gemeinsamen absolut irreduziblen Bestandteil.*

Beweis: Für die beiden Gruppen seien

$$(\xi_{ik}) \quad \text{und} \quad (\eta_{ik})$$

die im vorigen Beweis benutzten Matrizen hyperkomplexer Zahlen. Für die Zahlen, die sich durch die ξ_{ik} ausdrücken lassen, bilden gewisse Zeilen der Matrix (ξ_{ik}) eine Basis, dasselbe gilt für η_{ik}. Falls die beiden Gruppen gemeinsame, absolut irreduzible Bestandteile haben, müssen zwischen den ξ und η Beziehungen bestehen, deren Koeffizienten selbstverständlich in K liegen. Eine Basis für das durch die ξ und η bestimmte System läßt sich durch Zeilen aus (ξ_{ik}) und (η_{ik}) angeben. Nimmt man hierfür zunächst die Basis der ξ, so können die hinzukommenden Zeilen von (η_{ik}) keine Basis aller η_{ik} bilden, weil sonst die beiden Systeme unabhängig wären.

$$\eta_1, \ldots, \eta_r$$

sei eine Basiszeile der η_{ik}, die nicht in der ausgewählten Basis des zusammengesetzten Systems vorkommt. Wir drücken sie durch die letztere aus. η_i wird dann die Summe zweier Zahlen

$$\eta_i = \alpha_i + \beta_i \qquad (i = 1, 2, \ldots, r), \qquad (1)$$

wobei die α_i blos durch die erste Zeile ξ_{1k} dargestellt sind und die β_i durch die übrigen Zahlen der Basis des zusammengesetzten Systems. Statt der ersten Zeile kann auch eine andere Basiszeile aus den ξ_{ik} hervorgehoben werden. Bei rechtsseitiger Multiplikation mit e_S erfahren die α_i, die β_i und die η_i wegen (1) dieselbe Substitution aus der zur zweiten Gruppe adjungierten. Wären die α_i nicht unabhängig, so wäre diese Gruppe reduzibel, daher sind sie unabhängig und die beiden Gruppen erweisen sich als äquivalent. Ohne weiteres folgt nun

Satz 141: *Eine Gruppe läßt sich auf eine und nur eine Weise in Bestandteile zerlegen, die in einem Zahlkörper K irreduzibel sind. Mit einem absolut irreduzibeln Bestandteil kommen stets diejenigen gemeinsam vor, deren Charakterensysteme relativ zu K konjugiert sind.*

Für absolut irreduzible Gruppen Γ erweitern wir die Überlegungen von Satz 138. Wenn eine Substitution S eine Wurzel ε genau r-mal enthält, so läßt sich $r\Gamma$ in dem durch das Charakterensystem und ε bestimmten Körper k darstellen. Man denke sich S reduziert und ε an

die r ersten Stellen der Hauptdiagonale gebracht. Dann beweist man genau wie früher, daß

$$\xi_{11} + \xi_{22} + \cdots + \xi_{rr}$$

in K liegt, womit die Behauptung bewiesen ist.

Nun möge die Substitution S die Wurzel ε genau r-mal enthalten und d sei der größte gemeinschaftliche Teiler aller r, die man erhält, indem S alle Substitutionen von Γ und ε alle ihre charakteristischen Wurzeln durchläuft. Dann gilt der

Satz 142: *$d\Gamma$ läßt sich in dem durch sämtliche Wurzeln der charakteristischen Gleichungen bestimmten Körper darstellen.*

Beweis: Ist $\bar{d}\,\Gamma$ die im angegebenen Körper irreduzible Darstellung, so muß $\bar{d}$ ein Teiler aller r und daher auch von d sein.

I. Schur beweist folgenden

Satz 143: *Ist $s\,\Gamma$ irreduzibel in einem Körper K, so läßt sich Γ selber darstellen in einem Körper, dessen Relativgrad gegenüber K gleich s ist.*

Der Beweis erfolgt durch ein Verfahren wie im Beweis von Satz 137[1]).

§ 54. Gruppen im Körper der rationalen Zahlen.

Es gilt der

Satz 144: *Jede Gruppe mit rationalen Koeffizienten läßt sich so transformieren, daß sie ganzzahlige rationale Koeffizienten besitzt.*

Beweis: Es genügt, den Satz für Gruppen Γ zu beweisen, die im rationalen Zahlkörper irreduzibel sind. Es sei N der Generalnenner aller Koeffizienten von Γ. Übt man auf $N x_1$ alle Substitutionen von Γ aus, so erhält man lauter ganzzahlige Formen der n Variabeln von Γ, und zwar kommen darunter n linear unabhängige vor, sonst wäre Γ reduzibel. Wir bilden nun das System aller Formen, die sich durch die soeben abgeleiteten linear und mit ganzzahligen Koeffizienten zusammensetzen lassen. Diese bilden einen sogenannten ***Modul.*** Betrachten wir die sämtlichen auftretenden Koeffizienten von x_1. Mit je zweien kommt auch ihre Differenz vor und man kann daher in ihrem System den euklidischen Algorithmus ausüben, d. h. das System besteht aus den sämtlichen Vielfachen einer bestimmten ganzen Zahl d_1. L_1 sei eine Form mit d_1 als erstem Koeffizienten. Ist L eine beliebige andere, so kann man in der Gestalt $L - a\,L_1$ eine Form herstellen, die zum Modul gehört und deren erster Koeffizient 0 ist; a wird eine ganze Zahl. Es sei d_2 der gemeinsame Teiler aller Ko-

[1]) Weitere Sätze geben *Speiser*: Zahlentheoretische Sätze aus der Gruppentheorie. Math. Z. 5, S. 1; *I. Schur*: Einige Bemerkungen zu der vorstehenden Arbeit des Herrn *A. Speiser*. Math. Z. 5, S. 7.

effizienten von x_2 in denjenigen Formen, deren erster Koeffizient verschwindet, und L_2 sei eine solche mit d_2 als Koeffizient von x_2. Dann lassen sich a und b so als ganze Zahlen bestimmen, daß $L - a L_1 - b L_2$ von x_1 und x_2 unabhängig ist. Man fahre wie bisher fort und findet, daß unser Modul eine Basis von n Formen besitzt, die folgende Gestalt haben:

$$\begin{aligned} L_1 &= d_{11} x_1 + d_{12} x_2 + \ldots + d_{1n} x_n \\ L_2 &= \qquad d_{22} x_2 + \ldots + d_{2n} x_n \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ L_n &= \qquad\qquad\qquad d_{nn} x_n . \end{aligned}$$

Übt man auf die Variabeln x die Substitutionen von Γ aus, so erfahren die Formen unseres Moduls nur unter sich eine Vertauschung und die Basis geht wieder in eine solche über, d. h. die n Linearformen erfahren eine ganzzahlige Substitutionsgruppe. Diese ist äquivalent mit Γ, denn sie entsteht durch Transformation von Γ mit (d_{ik}), womit der Satz bewiesen ist.

Für Substitutionen mit algebraischen Koeffizienten läßt sich ein ähnlicher Satz beweisen. Die Koeffizienten von x_1 bilden dort ein Ideal $\mathfrak{a}$. Geht man zum Klassenkörper über, so ist $\mathfrak{a}$ Hauptideal; man braucht aber nicht die Existenz dieses Körpers vorauszusetzen, denn es gibt bekanntlich immer eine gewisse Potenz von $\mathfrak{a}$, die Hauptideal ist. Wenn

$$(\mathfrak{a})^m = (\alpha),$$

so adjungiere man dem Körper die m-te Wurzel aus α. Es wird dann

$$\mathfrak{a} = \left(\sqrt[m]{\alpha}\right).$$

Somit läßt sich das Verfahren im Beweis zum vorigen Satz fortsetzen und man erhält den

Satz 145: *Wenn Γ im Körper K liegt, so läßt sich stets eine äquivalente Gruppe mit ganzen Zahlen eines Körpers angeben, dessen Galoissche Gruppe in K auflösbar ist.*

Wir kehren nun zurück zu den Gruppen mit rationalen Koeffizienten. Aus einer Gruppe mit ganzzahligen Koeffizienten lassen sich durch Transformation mit unimodularen ganzzahligen Matrizen eine unendliche Menge neuer gewinnen. Wir fassen diese zu einer ***Klasse*** zusammen, dann gilt der

Satz 146: *Die äquivalenten ganzzahligen, rational irreduziblen Gruppen zerfallen in eine endliche Anzahl Klassen.*

Der Beweis dieses Satzes wurde zum erstenmal von *C. Jordan* geführt (Journ. de l'école polyt. 48). Weitere Beweise gaben *H. Minkowski* (Diskontinuitätsbereich für arithmetische Äquivalenz, Crelle's Journal Bd. 129 und Werke Bd. II, S. 53—100) und *L. Bieberbach* (Gött. Nach-

richten 1912). Alle diese Beweise benutzen die Theorie der quadratischen Formen und ihre Wiedergabe übersteigt den Rahmen unseres Buches. Wir begnügen uns daher, zwei extreme Fälle zu behandeln, und weisen schon hier auf den Schlußabschnitt hin, wo dem vorliegenden Theorem seine zentrale Stellung in der allgemeinen Zahlentheorie vindiziert wird.

1. Fall: Γ ist zyklisch und von der Ordnung m. Der Grad ist dann $\varphi(m)$. Auch die adjungierte Gruppe $\bar{\Gamma}$ ist ganzzahlig, und mit ihrer Hilfe bilden wir die Matrix:

$$\sum_1^n \varepsilon^i \bar{A}^i = \mathsf{M},$$

wobei ε eine primitive m-te Einheitswurzel bedeutet. Nun gilt

$$\varepsilon \mathsf{M} \bar{A} = \mathsf{M}.$$

Bezeichnen wir die erste Zeile von M mit

$$\zeta_1, \zeta_2, \ldots, \zeta_n,$$

so gelten die Gleichungen

$$\varepsilon \zeta_i = \sum_1^n a_{ik} \zeta_k \ (a_{ik}) = A \tag{1}$$

Die ζ_i sind ganze Zahlen des durch ε bestimmten Zahlkörpers k und das Gleichungssystem (1) besagt, daß $\zeta_1, \ldots, \zeta_n$ die Basis eines Ideales bilden. Umgekehrt, bilden diese Zahlen die Basis eines Ideales, so erhält man durch Multiplikation mit ε eine ganzzahlige Darstellung der zyklischen Gruppe. Weil ε eine einfache Wurzel von A ist, so sind durch die Gleichungen (1) die Zahlen ζ_i bis auf einen gemeinschaftlichen Faktor, die zugehörigen Ideale also als Ideale einer Idealklasse bestimmt. Es gibt genau so viele Klassen ganzzahliger Darstellungen, als es Idealklassen in k gibt, und diese Zahl ist bekanntlich endlich.

2. Fall: Die Gruppe Γ ist vollständig irreduzibel, was z. B. bei den Darstellungen der symmetrischen Gruppen (*Frobenius*) immer der Fall ist. Hier benutzen wir die Formeln des Satzes 122 auf Seite 125. Die hyperkomplexen Zahlen besitzen ganze rationale Zahlenkoeffizienten und erfahren bei rechtsseitiger Multiplikation mit e_S die Substitutionen der adjungierten, ebenfalls ganzzahligen Gruppe $\bar{\Gamma}$, die wir als die gegebene betrachten. Wiederum bezeichnen wir die erste Zeile der ζ_{ik} mit

$$\zeta_1, \zeta_2, \ldots, \zeta_n.$$

Äquivalente ganzzahlige Darstellungen, die zu verschiedenen Klassen gehören, erhält man durch Transformation mit Matrizen, die man als ganzzahlig annehmen kann, aber mit einer von ± 1 verschiedenen Determinante. Den größten gemeinsamen Teiler der Koeffizienten darf man

als 1 voraussetzen. Wenn es also mehrere Klassen gibt, so muß es möglich sein, lineare Formen der ζ_k zu bilden mit ganzzahligen Koeffizienten u_{ik}:

$$\eta_i = \sum u_{ik}\zeta_k,$$

die bei rechtsseitiger Multiplikation mit e_S ganzzahlige Substitutionen erfahren. Bilden wir den Modul

$$x_1\eta_2 + x_2\eta_2 + \ldots + x_n\eta_n,$$

wobei die x_i alle ganzen Zahlen durchlaufen, so erhält man durch Multiplikation mit e_S lauter Zahlen dieses Moduls. Dasselbe gilt daher auch bei rechtsseitiger Multiplikation mit ζ_{ik}. Multiplizieren wir die Größen η_i der Reihe nach mit allen ζ_{k1}, so kommt heraus $u_{ik}c\zeta_1$, wobei $c = \frac{g}{n}$ ist. Da die u_{ik} teilerfremd sind, so kommt im Modul auch $c\zeta_1$ vor, und ebenso $c\zeta_i$. Damit ist die Anzahl der Moduln limitiert und der Satz bewiesen.

H. Minkowski verdankt man wichtige Sätze über die Ordnung von rationalen Substitutionsgruppen. Da die charakteristische Determinante einer Substitution in diesem Falle eine Funktion mit rationalen Koeffizienten ist, so ist die Ordnung der Substitutionen durch den Grad n der Gruppe limitiert. Ist h eine solche Ordnung, so gilt für die zahlentheoretische Funktion $\varphi(h)$ folgende Ungleichung:

$$\varphi(h) \leqq n.$$

denn eine h-te Einheitswurzel genügt einer irreduziblen Gleichung mit rationalen Koeffizienten vom Grade $\varphi(h)$. Für $n = 2$ und $n = 3$ findet man folgende möglichen Werte für h: 1, 2, 3, 4, 6. Für $n = 4$ und 5 treten noch die Werte 5, 8, 10, 12 hinzu.

Weiterhin gilt folgender

Satz 147: *Reduziert man eine Gruppe mit rationalen Koeffizienten modulo einer ungeraden Primzahl, so erhält man eine holoedrisch isomorphe Kongruenzgruppe.*

Beweis: Wir zeigen, daß keine ganzzahlige Substitution endlicher Ordnung (mod p) der Einheitssubstitution kongruent ist, außer E. Es sei $S = E + p^a U$, wobei der größte gemeinsame Teiler der Koeffizienten von U zu p prim ist. Bildet man die Potenzen von S, so darf man die Binomialformel anwenden. S habe die Primzahlordnung l, dann wird

$$S^l = E + \binom{l}{1} p^a U + \ldots + p^{al} U^l = E.$$

Wenn p von l verschieden ist, so folgt, daß $S^l \pmod{p^{a+1}}$ kongruent ist $E + l p^a U$, also nicht kongruent E, was einen Widerspruch gibt. Ist $p = l$, so erinnere man sich daran, daß die Binomialkoeffizienten

durch p teilbar sind, außer dem ersten und dem letzten. Reduziert man daher mod p^{a+2}, so gelangt man wie vorher zu einem Widerspruch. Auch für $p = 2$ gilt der Satz, wenn $l \neq 2$ ist und schließlich auch für $p = l = 2$, wenn a größer als 1 ist. *Kennt man also die Modulsubstitutionen modulo einer ungeraden Primzahl, so sind damit auch die rationalen Gruppen des betreffenden Grades bekannt. Die Gruppen ungerader Ordnung erhält man bereits durch Reduktion mod* 2. Die Ordnung einer ganzzahligen Gruppe vom Grade n muß Teiler von

$$(p^n - 1)(p^n - p)(p^n - p^2)\dots(p^n - p^{n-1})$$

sein für alle ungeraden Primzahlen p. Daraus folgt eine obere Grenze für die Primzahlpotenz l^a, die in g aufgehen kann. Es sei l^u eine genügend hohe Potenz von l, so daß jedenfalls $l^u > n\,l$ ist. Nun wähle man p aus einer primitiven Restklasse mod l^u. Aus Satz 38 folgt, daß

$$(p^n - 1)(p^{n-1} - 1)\dots(p - 1)$$

genau durch die folgende Potenz von l teilbar ist, falls $l \neq 2$

$$\left[\frac{n}{l-1}\right] + \left[\frac{n}{l(l-1)}\right] + \left[\frac{n}{l^2(l-1)}\right] + \dots,$$

wobei $[a]$ die größte ganze Zahl $\leqq a$ darstellt. Für $l = 2$ findet man

$$n + 2\left[\frac{n}{2}\right] + \left[\frac{n}{4}\right] + \dots$$

§ 55. Beziehungen zur Kristallographie.

Wir wollen zeigen, daß das Problem, die ganzzahligen Gruppen des Grades n zu finden, gleichbedeutend ist mit der Aufsuchung aller Gitter des n-dimensionalen Raumes mit besonderen Symmetrien.

Es seien $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_n$ die Fundamentalvektoren eines n-dimensionalen Gitters, so daß man alle Gitterpunkte erhält, indem man die Gesamtheit der Vektoren

$$x_1\mathfrak{p}_1 + \dots + x_n\mathfrak{p}_n$$

von einem festen Punkt 0 aus abträgt. Hierbei durchlaufen $x_1, \dots, x_n$ alle ganzen Zahlen. Die Länge des Vektors $\mathfrak{p}_i$ sei $+\sqrt{a_{ii}}$, ferner setzen wir

$$\sqrt{a_{ii}}\sqrt{a_{kk}} \cdot \cos(\mathfrak{p}_i, \mathfrak{p}_k) = a_{ik} = a_{ki},$$

dann wird das Quadrat der Länge des Vektors

$$x_1\mathfrak{p}_1 + \dots + x_n\mathfrak{p}_n$$

gegeben durch die quadratische Form

$$\sum_{i=1}^{n}\sum_{k=1}^{n} a_{ik}x_ix_k.$$

Umgekehrt ist durch eine beliebige definite quadratische Form der n Variablen x_i ein Gitter definiert bis auf die Lage im Raum und bis auf eine Symmetrie. Man kennt alsdann nämlich die Länge der Fundamentalvektoren und die Winkel zwischen ihnen. Wählt man $n-1$ aus ihnen aus, so spannen sie eine $(n-1)$-dimensionale lineare Teilmannigfaltigkeit aus und man kann den letzten Vektor auf zwei zu ihr symmetrische Weisen hinzufügen. Man kann zeigen, daß es nur zwei zu einer Fundamentalform gehörige Gitter gibt. Wir wählen eines derselben.

Die Variablen $x_1, \ldots, x_n$ sind die Koordinaten des Endpunktes des Vektors $x_1\mathfrak{p}_1 + \ldots + x_n\mathfrak{p}_n$ in demjenigen Koordinatensystem, dessen Achsen die Richtungen der Vektoren $\mathfrak{p}_i$ haben, während die Einheitsstrecke der i-ten Achse durch den Vektor $\mathfrak{p}_i$ gegeben ist. Die Determinante $|a_{ik}|$ stellt das Quadrat des Inhaltes des Fundamentalparallelepipedes dar. Man kann das Gitter auf unendlich viele Arten durch Fundamentalvektoren aufbauen, man erhält sie alle, wenn man auf die Vektoren $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ die sämtlichen ganzzahligen Substitutionen mit der Determinante ± 1 ausübt. Die „metrische" Fundamentalform $\sum\sum a_{ik}x_ix_k$ erfährt dabei die transponierten Substitutionen, denn eine Substitution auf die $\mathfrak{p}_i$ in $x_1\mathfrak{p}_1 + \ldots + x_n\mathfrak{p}_n$ kann auch als die transponierte auf die x_i gedeutet werden.

Falls das Gitter eine Symmetrie aufweist, muß es möglich sein, neue Fundamentalvektoren einzuführen, welche dieselbe Konfiguration bilden wie die vorigen (Bewegung) oder die symmetrische (Symmetrie zweiter Art), d. h. die zugehörigen Substitutionen müssen die metrische Fundamentalform in sich überführen.

Umgekehrt: wenn wir eine ganzzahlige endliche Gruppe haben, so besitzt sie eine invariante definite quadratische Form. Man hat bloß auf $x_1^2 + \ldots + x_n^2$ alle Substitutionen auszuüben und die entstehenden Formen zu addieren. Es gibt daher Gitter, welche die betreffende Symmetrie aufweisen. Damit ist das Problem, symmetrische Gitter aufzusuchen, als identisch erwiesen mit der Frage nach den ganzzahligen Substitutionsgruppen.

Äquivalente Gruppen besitzen dieselben Operationen, sie lassen sich auf dieselbe orthogonale Gruppe transformieren. Sie definieren dieselbe ***Kristallklasse.*** Es besteht infolgedessen der

Satz 148: *Es gibt nur endlich viele Kristallklassen in n Dimensionen.*

Beweis: Als abstrakte Gruppen kommen nach Satz 147 nur endlich viele in Betracht und diese lassen nur endlich viele nicht äquivalente Darstellungen in n Variablen zu.

Dasselbe Gitter gehört nur zu solchen ganzzahligen Gruppen, die durch ganzzahlige unimodulare Substitutionen ineinander transformierbar sind.

Satz 149: *Wenn die ganzzahlige Gruppe im Gebiet der rationalen Zahlen irreduzibel ist, so gibt es nur eine endliche Anzahl verschiedener Gitter der zugehörigen Klasse.*

Der Beweis folgt ohne weiteres aus Satz 146.

Hier ist jedoch noch folgende Bemerkung von Wichtigkeit: Wenn die Gruppe reduzibel ist, so besitzt sie mindestens zwei linear unabhängige invariante quadratische Formen. f_1 und f_2 seien zwei solche. Dann ist die Gesamtheit der quadratischen Formen

$$a_1 f_1 + a_2 f_2$$

invariant, wobei a_1 und a_2 zwei beliebige reelle Zahlen sind. Insbesondere bilden die Formen

$$t f_1 + (1 - t) f_2,$$

in denen t von 0 nach 1 stetig variiert, eine Schar positiv-definiter Formen, welche f_1 mit f_2 stetig verbindet. Zu unserer Gruppe gehört daher eine unendliche Menge von Gittern, aber sie lassen sich durch stetige Deformation, ohne die Symmetrie zu verlieren, ineinander überführen. Eine solche Schar betrachten wir nur als *ein* Gitter. So sind wir auch bei drei Dimensionen vorgegangen: nur das kubische Gitter besaß keinen Freiheitsgrad, abgesehen von der Wahl der Einheitsstrecke.

Der Vollständigkeit halber wollen wir noch einige Hilfsmittel zur Behandlung der Raumgitter herleiten. Wir benutzen hierbei die von *Einstein* herrührende Vereinfachung der Bezeichnung, welche in der Regel besteht, daß über doppelt auftretende Indizes stets von 1 bis n summiert wird.

Die metrische Fundamentalform ist $a_{ik} x_i x_k$. Unter einer Ebene durch 0 verstehen wir die $(n-1)$-dimensionale Mannigfaltigkeit der Punkte, welche einer Gleichung $l_i x_i = 0$ genügen. Sie enthält dann und nur dann ein $(n-1)$-dimensionales Teilgitter unsres Gitters, wenn die l_i rationale Zahlen sind. Wir normieren die l_i, indem wir sie als teilerfremde ganze Zahlen annehmen, und nennen sie alsdann die ***Indizes*** der Ebene. Es ist von Wichtigkeit, die Größe des Fundamentalparallelogrammes der Ebene zu kennen, da durch sie die ***„Belastung"*** der Gitterebene bestimmt ist. Man erhält alle parallelen Gitterebenen in der Gestalt $l_i x_i = l$, wobei l alle ganzen Zahlen durchläuft, insbesondere ist $l_i x_i = 1$ eine benachbarte Ebene zu $l_i x_i = 0$. Wir bestimmen ihren Abstand von 0, indem wir das Minimum von $a_{ik} x_i x_k$ unter der Nebenbedingung $l_i x_i = 1$ aufsuchen. Indem wir $a_{ik} x_i x_k - 2\lambda l_i x_i$ nach x_k differenzieren, bekommen wir

$$a_{ik} x_i - \lambda l_k = 0.$$

Wir multiplizieren mit x_k und summieren, es ergibt sich

$$\lambda = a_{ik} x_i x_k = \varrho^2,$$

wenn wir unter e die gesuchte Entfernung verstehen. Andrerseits lösen wir die Gleichungen nach den x_i auf, indem wir die aus den Unterdeterminanten A_{ik} der Matrix (a_{ik}) gebildete Determinante $|A_{ik}|$ benutzen. Es ergibt sich

$$A x_i = e^2 l_k A_{ik}, \qquad A = |a_{ik}|.$$

Wir multiplizieren mit l_i und summieren.

$$A = e^2 A_{ik} l_i l_k.$$

$A_{ik} l_i l_k$ heißt die zu $a_{ik} x_i x_k$ ***adjungierte quadratische Form.*** Ziehen wir die Quadratwurzel, so ergibt sich links der Inhalt des Fundamentalparallelepipedes des ganzen Gitters. Dieser ist nun aber gleich dem Inhalt desjenigen unserer Ebene multipliziert mit dem Abstand zweier benachbarter Ebenen (Inhalt = Basis mal Höhe). Hieraus folgt der

Satz 150: *Das Fundamentalparallelogramm der Ebene mit den Indizes l_i hat den Inhalt:*

$$\sqrt{A_{ik} l_i l_k}.$$

Diesen Satz hat bereits *Gauss* gekannt (vgl. Geometrische Seite der ternären Formen, Werke B. 2, S. 305).

Indizes und Variable stehen in kontragredientem Verhältnis, sie erfahren in unserer Terminologie adjungierte Substitutionen bei Einführung neuer Fundamentalvektoren resp. bei den Gittersymmetrien.

14. Kapitel.

Gruppen von gegebenem Grade.

§ 56. Die endlichen Substitutionsgruppen vom Grade n.

Eine Gruppe Γ des Grades n, deren Ordnung eine Primzahlpotenz p^a ist, kann immer auf monomiale Gestalt transformiert werden. Ist p^b die höchste in $n!$ aufgehende Potenz von p, so enthält $\mathfrak{G}$ einen *Abel*schen Normalteiler, dessen Index ein Teiler von p^b ist. Das Problem, alle Substitutionsgruppen n-ten Grades, deren Ordnung eine Potenz von p ist, aufzustellen, ist zurückgeführt auf das Problem, die *Sylow*gruppe von der Ordnung p^b für die symmetrische Gruppe von n Variablen zu bestimmen. Wir sind noch weit davon entfernt, ein ähnliches Konstruktionsprinzip für alle endlichen Gruppen des Grades n anzugeben, aber einige hochwichtige Resultate sind in dieser Hinsicht bereits erzielt worden.

Satz 151: *Wenn eine irreduzible Substitutionsgruppe Matrizen besitzt, deren Charaktere im Körper der p^a-ten, der q^b-ten usw., aber nicht der p^{a-1}-ten, der q^{b-1}-ten usw. Einheitswurzeln liegen, so enthält*

sie auch eine Substitution von der Ordnung $p^a q^b \ldots$. Hierbei bedeuten $p, q, \ldots$ verschiedene Primzahlen.

Beweis: Zwischen den Potenzen einer primitiven p^a-ten Einheitswurzel ε bestehen in einem beliebigen Körper, der prim ist zu dem durch ε bestimmten, genau die folgenden linearen Beziehungen:

$$\varepsilon^i + \varepsilon^i\varepsilon_1 + \varepsilon^i\varepsilon_1^2 + \ldots + \varepsilon^i\varepsilon_1^{p-1} = 0, \quad (i = 0, 1, \ldots, p^{a-1} - 1),$$
$$\varepsilon_1 = \varepsilon^{p^{a-1}},$$

und diejenigen, welche sich aus diesen durch lineare Verbindungen herleiten. Die Darstellung einer Zahl als Summe von Einheitswurzeln ist daher nicht eindeutig. Wenn in jeder Darstellung eine primitive s-te Einheitswurzel vorkommt, so sagen wir kurz: Die Zahl *bedarf* der s-ten Einheitswurzeln. Wir nehmen nun an, ein Charakter χ_i bedürfe der s-ten Einheitswurzeln und s sei prim zu p. Es gibt ferner nach der Voraussetzung einen Charakter χ_k, welcher der p^a-ten Einheitswurzeln bedarf. Es gilt nach Satz 112 folgende Gleichung

$$h_i\chi_i \cdot h_k\chi_k = \chi_1 \sum_{l=1}^{r} c_{ikl} h_l \chi_l . \tag{1}$$

Auf beiden Seiten stehen Summen von Einheitswurzeln, deren jede Produkt einer bestimmten (primitiven oder imprimitiven) p^a-ten und einer dazu primen Einheitswurzel ist. Wir greifen diejenigen heraus, deren erster Faktor eine der Zahlen

$$\varepsilon\varepsilon_1^k, \quad (k = 1, 2, \ldots, p), \quad (\varepsilon_1^p = 1)$$

ist. Links steht

$$\varepsilon(a_1\varepsilon_1 + a_2\varepsilon_1^2 + \ldots + a_p\varepsilon_1^p)\chi_i$$

und wir dürfen ε so gewählt denken, daß nicht alle a_i einander gleich sind, sonst bedürfte χ_k nicht der p^a-ten Einheitswurzeln. Rechts stehe

$$\varepsilon(\alpha_1\varepsilon_1 + \ldots + \alpha_p\varepsilon_1^p),$$

wobei die Zahlen α der p-ten Einheitswurzeln nicht bedürfen. Beide Seiten müssen einander gleich sein und es ergibt sich

$$a_1\chi_i - \alpha_1 = a_2\chi_i - \alpha_2 = \ldots = a_p\chi_i - \alpha_p$$

Nun sei etwa $a_1 - a_2 = b$ von 0 verschieden, dann folgt

$$b\chi_i = \alpha_1 - \alpha_2 .$$

Da diese Differenz der s-ten Einheitswurzeln bedarf, so gilt dasselbe mindestens von α_1 oder von α_2. Daraus folgt, daß die rechte Seite von (1) eine primitive $p^a s$-te Einheitswurzel enthält und infolgedessen auch einer ihrer Summanden χ_l. Es gibt also eine Substitution, deren charakteristische Wurzeln eine primitive $p^a s$-te Einheitswurzel enthalten, und daher auch eine solche von der Ordnung $p^a s$. Durch vollständige Induktion beweist man ohne weiteres unsern Satz.

Aus diesem Hilfssatz aus der Theorie der Kreiskörper folgt nun folgender

Satz 152: *Eine irreduzible Substitutionsgruppe n-ten Grades von der Ordnung $n_1 n_2$, wobei die Primfaktoren von n_1 größer, diejenigen von n_2 kleiner oder gleich $n+1$ sind, besitzt eine Abelsche Untergruppe von der Ordnung n_1.*

Beweis: Wir nehmen zunächst an, daß alle Substitutionen die Determinante 1 haben. Jede Untergruppe von einer Ordnung, die in n_1 aufgeht, ist *Abel*sch, denn der Grad ihrer irreduzibeln Darstellungen muß ein Teiler von n_1 und gleichzeitig höchstens gleich n sein. Es kommt also nur 1 in Betracht.

Wir setzen $n_1 = p^a q^b \ldots$ Die Charaktere der Substitutionen von der Ordnung p resp. q usw. bedürfen der p-ten, q-ten usw. Einheitswurzeln und es gibt daher eine Substitution S der Ordnung $pq \ldots$ Ihre Zerlegung in vertauschbare Faktoren von den Ordnungen p, q, ... sei

$$S = PQ \ldots .$$

P, Q, ... können nicht zum Zentrum der Gruppe gehören, denn sonst wären sie Multiplikationen und ihre Determinante wäre von 1 verschieden. Die (*Abel*schen) *Sylow*gruppen, welche P, Q, ... enthalten, seien $\mathfrak{P}, \mathfrak{Q}, \ldots$. Die mit P vertauschbaren Elemente bilden eine Untergruppe und für solche nehmen wir den Satz als bewiesen an. Da unsere Untergruppe sowohl $\mathfrak{P}$ als S enthält, so ist jedes Element von $\mathfrak{P}$ mit S vertauschbar. Genau dasselbe beweist man für die Elemente von $\mathfrak{Q}$ usw. Daher ist die Ordnung der Untergruppe bestehend aus allen mit S vertauschbaren Elementen durch n_1 teilbar, sie enthält also eine *Abel*sche Untergruppe von der Ordnung n_1.

Falls eine Substitution P eine von 1 verschiedene Determinante ε besitzt, so multipliziere man sie mit η, welches der Gleichung genügt $\eta^n = \varepsilon^{-1}$. Man erweitere ferner das Zentrum durch ηE. In derselben Weise verfährt man mit allen Substitutionen, soweit sie nicht bereits zum Zentrum gehören. Die so erweiterte Gruppe besitzt einen Normalteiler, bestehend aus den Substitutionen mit der Determinante 1 und für seine Nebengruppen kann man Substitutionen aus dem Zentrum wählen. Daher gilt auch für diese Gruppe der Satz. Diejenigen Substitutionen der *Abel*schen Untergruppe, welche bereits in der ursprünglichen Gruppe liegen, bilden eine Untergruppe von der Ordnung n_1.

§ 57. Der Satz von Jordan.

Eine endliche Substitutionsgruppe vom Grade n besitzt einen Abelschen Normalteiler, dessen Index eine gewisse von n allein abhängige Schranke nicht überschreiten kann.

Diesen Satz hat *C. Jordan* in seinem Mémoire sur les équations différentielles linéaires à intégrale algébrique (Crelles Journal **84**, S. 89 bis 215) durch einen auch in seiner logischen Form höchst bemerkenswerten Beweis erhärtet. Gleichzeitig hat er alle primitiven Gruppen der Grade 2 und 3 aufgestellt. Inzwischen ist der Satz von verschiedenen Seiten in Angriff genommen worden. *Blichfeldt* (G. A. Miller, H. F. Blichfeldt, L. E. Dickson: Theory and applications of finite groups, New York 1916, chapter XII) hat zahlentheoretische Methoden angewendet. *Bieberbach*[1]) benutzt kontinuierliche Veränderliche. Seine Methode ist von *Frobenius*[2]) verschärft worden, und wir folgen hier zunächst dessen zweiter Abhandlung über unitäre Matrizen, Berliner Sitzungsberichte S. 373 bis 378, 1911.

Jede endliche Gruppe läßt sich auf die unitäre Form transformieren (§ 42). Die charakteristischen Wurzeln der Matrizen deuten wir in der komplexen Zahlenebene. Sie liegen auf dem Einheitskreis mit 0 als Zentrum. Es gilt nun der

Satz 153: *Sei* $C = A\,B\,A^{-1}B^{-1}$ *der Kommutator der beiden Substitutionen* A *und* B. *Die Wurzeln von* B *mögen nicht ganz einen Halbkreis einnehmen. Ist dann* A *mit* C *vertauschbar, so ist auch* A *mit* B *vertauschbar, also* $C = E$.

Beweis: Wir nehmen B in der Diagonalform und A als unitär an. Die charakteristischen Wurzeln seien

$$e^{i\varphi_k}, \qquad (k = 1,\ 2,\ \ldots,\ n).$$

φ_k nennen wir die *Phasen* der Wurzeln. Weil A mit $BA^{-1}B^{-1}$ vertauschbar ist, so ergibt sich

$$C = A(BA^{-1}B^{-1}) = (BA^{-1}B^{-1})A = AB\bar{A}_t\bar{B} = B\bar{A}_t\bar{B}A.$$

Hierbei bedeutet S_t die zu S transponierte, $\bar{S}$ die zu S konjugiert imaginäre Matrix.

Für die Koeffizienten der Hauptdiagonale von C findet man

$$c_{ii} = \sum_k a_{ik} b_k \bar{a}_{ik} \bar{b}_i = \sum_k b_i \bar{a}_{ki} \bar{b}_k a_{ki}$$

und durch Vergleichung der imaginären Teile

$$\sum_k (|a_{ik}|^2 + |a_{ki}|^2) \sin(\varphi_k - \varphi_i) = 0.$$

Nun sei

$$\varphi_1 = \varphi_2 = \ldots = \varphi_r < \varphi_{r+1} = \ldots = \varphi_s < \ldots \leqq \varphi_n < \varphi_1 + \pi.$$

---

[1]) *Bieberbach, L.:* Über einen Satz des Herrn C. Jordan in der Theorie der endlichen Gruppen linearer Substitutionen. Berl. Ber. S. 231 bis 240, 1911.

[2]) *Frobenius, G.:* Über den von L. Bieberbach gefundenen Beweis eines Satzes von C. Jordan. Berl. Ber. S. 241 bis 248, 1911. Außerdem die oben erwähnte Abhandlung über unitäre Matrizen.

Setzt man $i = 1$, so werden alle Glieder positiv und es werden alle a_{ik} gleich Null, für welche einer der Indizes größer als r, der andere aber kleiner oder gleich r ist. A zerfällt in zwei Teilmatrizen, von denen die erste mit B vertauschbar ist. Die zweite kann man in derselben Weise behandeln und findet, daß auch sie reduzierte Gestalt hat und mit B vertauschbar ist, womit der Satz bewiesen ist.

Satz 154: *Liegen die Wurzeln A oder B auf einem Kreisbogen der Größe σ, so liegen die Phasen des Kommutators zwischen $-\sigma$ und $+\sigma$.*

Beweis: Aus der unitären Matrix $P = (p_{kl})$ bilde man die Form

$$\sum_{kl} p_{kl} x_k \bar{x}_l .$$

Übt man auf die x die unitäre Substitution S und gleichzeitig auf die $\bar{x}$ die konjugiert komplexe $\bar{S}$ aus, so entsteht eine neue Form, deren Matrix $S_t P \bar{S}$ ist. $\bar{S}$ und S_t sind aber inverse Matrizen. Man kann daher die Form auf die Normalform transformieren

$$\sum' r_{ii} x_i \bar{x}_i ,$$

wobei die r die charakteristischen Wurzeln von P sind. Die Phasen derselben mögen zwischen φ und $\varphi + \sigma$ liegen, dann liegt auch die Phase von

$$s_1 r_{11} + \cdots + s_n r_{nn} ,$$

wo die s positive reelle Zahlen bedeuten, innerhalb derselben Grenzen, wie man sofort erkennt, wenn man die r_{ii} vektoriell deutet. Setzt man nun in $\sum_i' r_{ii} x_i \bar{x}_i$ für x_i und $\bar{x}_i$ konjugiert imaginäre Werte ein, so erhält man nur Zahlen, deren Phasen in denselben Grenzen liegen, und dasselbe gilt schließlich von der Form $\sum_{i,k} p_{ik} x_i \bar{x}_k$, die durch konjugiert imaginäre Substitutionen auf die x und $\bar{x}$ erhalten wird und also dieselben Werte annimmt.

Nun seien P und Q zwei unitäre Matrizen und s eine charakteristische Wurzel von PQ^{-1}, also eine Wurzel der Gleichung

$$|PQ^{-1} - sE| = 0 \quad \text{oder} \quad |P - sQ| = 0.$$

Dann kann man $x_1, \ldots, x_n$ so bestimmen, daß

$$\sum_k p_{kl} x_k = s \sum_k q_{kl} x_k .$$

Es wird dann

$$\sum_{k,l} p_{kl} x_k \bar{x}_l = s \sum_{k,l} q_{kl} x_k \bar{x}_l .$$

Wenn daher die Phasen der Wurzeln von P und Q zwischen φ und $\varphi + \sigma$ liegen, so liegt diejenige von s zwischen $-\sigma$ und $+\sigma$. Setzt man jetzt $P = A$ und $Q = BAB^{-1}$, so ist der Satz bewiesen.

Satz 155 von Frobenius: *In einer endlichen Substitutionsgruppe ist jede Substitution A, deren Wurzeln nicht ganz den sechsten Teil des Kreises einnehmen, mit jeder Substitution vertauschbar, deren Wurzeln nicht ganz den halben Kreis einnehmen.*

Beweis: B sei irgendeine Substitution der Gruppe, und wir bilden folgende Reihe von Kommutatoren:

$$ABA^{-1}B^{-1} = C,\ ACA^{-1}C^{-1} = D,\ \ldots,\ ALA^{-1}L^{-1} = M,$$
$$AMA^{-1}M^{-1} = N,\ \ldots$$

Die Wurzeln aller dieser Kommutatoren C, D, ... haben ihre Phasen zwischen $-\frac{\pi}{3}$ und $+\frac{\pi}{3}$.

Nun bezeichne $\vartheta(P)$ für eine beliebige Matrix P die Summe der Normen der Koeffizienten, d. h. $\sum_{k,l} p_{kl}\bar{p}_{kl}$. Wir nennen sie die ***Spannung*** von P, sie ist gleich dem Charakter der Matrix $P\bar{P}_t$ oder auch von $\bar{P}_t P$. Sind U und V unitär, so wird

$$\vartheta(UP) = \chi(\bar{P}_t\bar{U}_t UP) = \chi(\bar{P}_t P) = \vartheta(P)$$

und

$$\vartheta(P) = \vartheta(UPV).$$

Wir setzen nun voraus, daß A auf die Diagonalform transformiert sei und die charakteristischen Wurzeln $a_1, \ldots, a_n$ habe. Dann wird:

$$\vartheta(E - C) = \vartheta(E - AB(BA)^{-1}) = \vartheta(BA - AB)$$
$$= \vartheta(A(E - B) - (E - B)A),$$
$$= \sum_{kl} |a_k(e_{kl} - b_{kl}) - (e_{kl} - b_{kl})a_l|^2 = \sum_{kl} |a_k - a_l|^2\, |e_{kl} - b_{kl}|^2.$$

Hier ist $|a_k - a_l|$ kleiner als die Seite des regulären Sechsecks. Ist $\varkappa$ der größte dieser Werte, so ist $\varkappa < 1$.

Es wird nun

$$\vartheta(E - C) < \varkappa^2\,\vartheta(E - B) = b\varkappa^2$$

und

$$\vartheta(E - N) < b\varkappa^{2\nu}.$$

Erzeugen A und B eine endliche Gruppe, so muß einmal $\vartheta(E-N)=0$ werden und daher $N = E$. Es wird infolgedessen A mit M und nach Satz 153 auch mit L, ..., D, C vertauschbar, und wenn die Wurzeln von B nicht ganz einen Halbkreis einnehmen, auch mit B.

Nun bedeute $Z(n)$ die Anzahl der Primzahlen $\leqq n + 1$. Dann läßt sich der Satz von Jordan in folgender präziseren Weise aussprechen:

Satz 156: *Eine endliche Substitutionsgruppe in n Variablen besitzt stets einen Abelschen Normalteiler, dessen Index kleiner ist als*

$$n!\, 12^n (Z(n) + 1).$$

Beweis: Eine *Sylow*gruppe besitzt einen *Abel*schen Normalteiler, dessen Index ein Teiler von $n!$ ist. Seine Ordnung sei $\geqq 12^n - 10$.

Man teile den Einheitskreis in 12 gleiche Teile und rechne jeweils einen der Grenzpunkte zum Intervall, den anderen zum benachbarten. Für die Verteilung der n Wurzeln einer Substitution unserer *Abel*schen Gruppe, die wir in Normalform voraussetzen, kommen 12^n Möglichkeiten in Betracht. Daher müssen entweder bei einer Substitution außer E die sämtlichen Wurzeln im selben Fach liegen, oder aber es gibt zwei, etwa A und B, bei denen die Verteilung gleich ist. Im letzteren Fall nehmen die Wurzeln von AB^{-1} nicht ganz den sechsten Teil des Kreises ein. Es gibt also sicher Substitutionen von dieser Beschaffenheit. Diese sind aber mit allen Substitutionen ihrer Klasse vertauschbar und erzeugen daher einen *Abel*schen Normalteiler.

Für jede Primzahl $\leqq n+1$ machen wir diese Überlegung. Indem wir ferner den Satz 152 beachten, ergibt sich der Beweis unseres Satzes.

Auf zahlentheoretischem Weg läßt sich folgender Satz beweisen:

Satz 157: *Falls die Primzahl p größer als $2n^2+1$ ist, so bildet die zugehörige Sylowgruppe einen Abelschen Normalteiler.*

Beweis: A und B seien zwei Substitutionen dieser *Sylow*gruppe. Für ihre Charaktere gelten folgende Gleichungen:

$$h_i \chi_i \cdot h_k \chi_k = \chi_1 \sum_{l=1}^{r} c_{ikl} h_l \chi_l .$$

Rechts und links stehen Summen von gleich vielen Einheitswurzeln; links kommen aber höchstens $n^2 < \frac{p-1}{2}$ verschiedene vor und eine solche Zahl läßt sich auf keine andere Weise durch gleich viel oder weniger Einheitswurzeln additiv darstellen. Daher stehen auch rechts nur Charaktere von Substitutionen, deren Ordnung eine Potenz von p ist. Das Produkt von A und B gehört infolgedessen auch zu ihnen und die *Sylow*gruppe bildet einen Normalteiler. Dieser ist wegen $p > n$ *Abel*sch.

Für Gruppen ungerader Ordnung gilt der Satz schon bei $p > n^2+1$.

Beschränkt man sich auf primitive Gruppen, deren Substitutionen die Determinante 1 haben (vgl. dazu den Schluß des Beweises zu Satz 152), so muß der *Abel*sche Normalteiler zum Zentrum gehören und kann höchstens die Ordnung n haben, denn seine Substitutionen sind Multiplikationen. Daher gilt folgender

Satz 158: *Die Ordnung einer irreduziblen primitiven Substitutionsgruppe, deren Substitutionen die Determinante 1 haben, ist kleiner als*

$$n!\, n\,(Z(n)+1)\, 12^n.$$

Es gibt nur endlich nicht äquivalente Gruppen.

§ 58. Substitutionen in *Galois*feldern.

Bereits bei der Behandlung der Automorphismen *Abel*scher Gruppen § 35 sind wir auf lineare Substitutionen gekommen, deren Koeffizienten die Reste der ganzen Zahlen nach dem Modul einer Primzahl sind, während die Determinanten der Null nicht kongruent sind, und wir haben die Ordnung dieser Gruppen bestimmt. Wir erweitern diese Betrachtungen, indem wir ein beliebiges *Galois*feld $GF(p^f)$ zugrunde legen. Eine solche Substitution sei

$$\begin{aligned} x_1' &= s_{11}x_1 + \ldots + s_{1n}x_n \\ &\cdots\cdots\cdots\cdots \\ x_n' &= s_{n1}x_1 + \ldots + s_{nn}x_n. \end{aligned}$$

x_1 kann durch eine beliebige Form ersetzt werden, die nicht identisch verschwindet, d. h. durch $p^{fn} - 1$ Formen. Sind S und T zwei Substitutionen, welche x_1 in dieselbe Form überführen, so läßt ST^{-1} die Variable x_1 ungeändert und hat folgende Gestalt:

$$\begin{vmatrix} 1 & 0 \\ A & B \end{vmatrix},$$

wobei A eine Spalte von $n-1$ Zahlen, B eine quadratische Matrix von $n-1$ Zeilen und Spalten bedeutet. Diese Substitutionen bilden eine Untergruppe, und bei festgehaltenem B kann die Spalte A aus beliebigen Größen des GF bestehen, es kommen also $p^{(n-1)f}$ Möglichkeiten vor. Diejenigen Substitutionen, bei denen A aus Nullen besteht, bilden eine Untergruppe, deren Ordnung wir mit $O(n-1)$ bezeichnen. Für die Ordnung $O(n)$ der ganzen Gruppe finden wir folgende Rekursionsformel:

$$O(n) = (p^{nf} - 1)\, p^{(n-1)f}\, O(n-1)$$

und erhalten damit folgenden

Satz 159: *Die Ordnung der Gruppe Γ aller homogenen linearen Substitutionen des Grades n im $GF(p^f)$ ist*

$$(p^{nf} - 1)(p^{nf} - p^f) \ldots (p^{nf} - p^{(n-1)f}).$$

Diese Gruppe besitzt einen Normalteiler Γ_1, dessen Faktorgruppe zyklisch und von der Ordnung $p^f - 1$ ist, bestehend aus den Substitutionen mit der Determinante 1. Außerdem besitzt sie ein Zentrum von derselben Ordnung, bestehend aus den Multiplikationen. Ist d der größte gemeinschaftliche Teiler von $p^f - 1$ und n, so enthält Γ_1 mit dem Zentrum eine Untergruppe von der Ordnung d gemeinsam, die wir mit Γ_2 bezeichnen. Es gilt der Satz, daß die Gruppe Γ_1/Γ_2 einfach ist, außer in den Fällen des $GF(2)$ und $GF(3)$ bei dem Grade 2. Für den Beweis verweisen wir auf die Monographie von

Dickson, Linear groups S. 83 [1]). Es gibt also für jeden Grad eine zweifach unendliche Schar verschiedener einfacher Gruppen, die wir in dieser Weise erhalten. Wir wollen nun die p-*Sylow*gruppen untersuchen und nachher diejenigen Untergruppen, deren Ordnung zu p prim ist.

Die Ordnung einer p-*Sylow*gruppe ist

$$p^{(1+2+\ldots+(n-1))f} = p^{\frac{n(n-1)}{2}f}.$$

Nun bilden diejenigen Substitutionen, deren Koeffizienten oberhalb der Hauptdiagonalen 0 sind, während die Hauptdiagonale lauter 1 enthält, eine Untergruppe, welche genau die angegebene Ordnung besitzt. Sie ist daher eine *Sylow*gruppe und jede andere Untergruppe von dieser Ordnung ist mit ihr äquivalent. Sie bildet eine Normalform für Untergruppen, deren Ordnung eine Potenz von p ist.

Satz 160: *Jede Substitutionsgruppe in einem* $GF(p^f)$*, deren Ordnung eine Potenz von* p *ist, läßt sich so transformieren, daß die Koeffizienten oberhalb der Hauptdiagonalen* 0 *sind, und diejenigen der Hauptdiagonalen* 1.

Zur näheren Untersuchung unserer Gruppen verwenden wir folgende Bezeichnung. Eine Substitution in der obigen Normalform bezeichnen wir mit $E + V$. Dabei hat V auch in der Hauptdiagonalen noch lauter 0 stehen. Wir betrachten die sich nach links unten daran anschließenden Diagonalen und zählen ab, wie viele davon mit 0 ausgefüllt sind. Sind die i ersten gleich 0, wobei die Hauptdiagonale mitgezählt wird, so bezeichnen wir diese Matrix mit V_i. Man verifiziert sogleich, daß $V_i V_k = V_{i+k}$. In dieser Symbolik bedeutet V nicht eine bestimmte Matrix, sondern nur den Typus. Nun seien zwei Matrizen gegeben

$$E + V_i \quad \text{und} \quad E + V_k'.$$

Ihr Produkt ist $E + V_i + V_k' + V_i V_k'$. Die beiden Matrizen sind also vertauschbar, wenn V_i und V_k' es sind. Für die p-te Potenz von $E + V_i$ finden wir

$$(E + V_i)^p = E + V_i^p.$$

Wenn also der Grad nicht größer als p ist, so ist die Ordnung aller Elemente der *Sylow*gruppe $= p$. Allgemein ergibt sich das zu $E + V_i$ inverse Element in der Gestalt

$$E - V_i + V_i^2 - V_i^3 + \ldots$$

wobei man so weit zu gehen hat, bis die Glieder verschwinden. Der

[1]) Wichtige Ergänzungen enthalten: *Dickson, L. E.:* On the group defined for any given field by the multiplication table: Am. math. Soc. Trans. **3**, S. 285—301, 1902. Modular theory of group characters: Am. math. Soc. Bull. (2) **13**, S. 477—488.

Beweis ergibt sich unmittelbar durch Multiplikation mit $E + V_i$. Nun möge in V_1 und V_1' die erste an die Hauptdiagonale stoßende Diagonale aus den Zahlen $a_1, a_2, \ldots, a_{n-1}$ resp. $b_1, b_2, \ldots, b_{n-1}$ bestehen. Dann lautet in $(E + V)(E + V')$ die entsprechende Diagonale

$$a_1 + b_1, \quad a_2 + b_2, \quad \ldots, \quad a_{n-1} + b_{n-1}.$$

Daher bilden die Substitutionen von der Gestalt $E + V_2$ einen Normalteiler, dessen Faktorgruppe *Abel*sch ist und durch die additive Gruppe der Moduln von $n - 1$ Größen des $GF(p^f)$ gebildet wird. Diese Gruppe hat die Ordnung $p^{f(n-1)}$ und den Typus $(p, p, \ldots)$. In derselben Weise bilden die Substitutionen von der Form $E + V_i$ einen Normalteiler $\mathfrak{N}_i$, und wir können den Satz aussprechen:

Satz 161: *Die Sylowgruppe $\mathfrak{P} = \mathfrak{N}_1$ besitzt eine Reihe von $n - 1$ Normalteilern $\mathfrak{N}_2, \mathfrak{N}_3, \ldots, \mathfrak{N}_{n-1}, E$, für welche $\mathfrak{N}_i/\mathfrak{N}_{i+1}$ Abelsch von der Ordnung $p^{f(n-i)}$ und vom Typus $(p, p, \ldots)$ ist. $\mathfrak{N}_i$ besteht aus allen Substitutionen von der Gestalt $E + V_i$.*

Wenden wir uns jetzt zu den Gruppen, deren Ordnung zu p prim ist. Wir beweisen den fundamentalen

Satz 162: *Eine Substitutionsgruppe des $GF(p^f)$, deren Ordnung zu p prim ist, läßt sich stets als Gruppe mit algebraischen Zahlenkoeffizienten schreiben. Die erstere entsteht aus der letzteren durch Reduktion nach einem Primidealteiler von p.*

Beweis: Es sei $\mathfrak{G}$ eine Gruppe mit zu p primer Ordnung. Wir zeigen, daß die vollständige Zerfällung der Gruppendeterminante in den *Galois*feldern genau in derselben Weise erfolgt, wie in gewöhnlichen komplexen Zahlen. Eine irreduzible Darstellung mit Zahlenkoeffizienten kann stets so transformiert werden, daß ihre Koeffizienten algebraische Zahlen sind. Es sei K ein Körper, in dem alle irreduziblen Darstellungen von $\mathfrak{G}$ gegeben werden können, und f sei der Grad eines Primidealteilers $\mathfrak{p}$ von p. Reduziert man (mod $\mathfrak{p}$), so erhält man Darstellungen von $\mathfrak{G}$ durch Substitutionen im $GF(p^f)$. Aus irreduziblen Darstellungen entstehen so immer *irreduzible* Darstellungen im $GF(p^f)$, wie folgendermaßen bewiesen werden kann: Man nimmt ein vollständiges System irreduzibler nicht äquivalenter Darstellungen von $\mathfrak{G}$ und bildet die Matrix ihrer Stellenzeilen. Diese ist quadratisch und ihre Determinante ist nur durch Primzahlen teilbar, die auch in der Ordnung von $\mathfrak{G}$ aufgehen. Sie ist daher zu p prim, infolgedessen sind die Stellenzeilen auch (mod $\mathfrak{p}$) unabhängig. Daraus folgt, daß eine algebraisch irreduzible Darstellung auch (mod $\mathfrak{p}$) irreduzibel bleibt, denn im anderen Fall wären ihre Stellenzeilen (mod $\mathfrak{p}$) nicht unabhängig.

Wir müssen nun noch zeigen, daß es keine weiteren irreduziblen Darstellungen gibt, und daß jede halb reduzible Gruppe auch voll-

ständig reduzibel ist. Wir greifen zu diesem Zweck zurück auf die Formeln von Satz 122. ξ_{ik} und η_{ik} seien die hyperkomplexen Zahlen, welche durch zwei nicht äquivalente irreduzible Darstellungen geliefert werden. Dann gilt

$$\begin{aligned} \xi_{ik}\xi_{kl} &= c\,\xi_{il} \qquad \eta_{ik}\eta_{kl} = c'\,\eta_{il} \\ \xi_{ik}\xi_{lm} &= 0 \qquad\quad \eta_{ik}\eta_{lm} = 0 \qquad\quad (k \neq l) \\ \xi_{ik}\eta_{lm} &= 0\,. \end{aligned}$$

Eine irreduzible Darstellung im $GF(p^f)$, welche auch in jedem höheren GF irreduzibel bleibt, möge in entsprechender Weise die hyperkomplexen Zahlen liefern ζ_{ik}. Wir multiplizieren sie rechts mit allen Zahlen ξ_{ii}, welche durch die algebraisch irreduzibeln Darstellungen nach der Reduktion $(\mathrm{mod}\,\mathfrak{p})$ entstehen. Nicht alle so entstehenden Produkte können verschwinden, denn durch die Multiplikatoren ξ_{ii} setzt sich die Gruppeneinheit linear zusammen. Es sei beispielsweise $\zeta_{11}\cdot\xi_{11}$ von 0 verschieden. Dann erhält man durch rechtsseitige Multiplikation mit den hyperkomplexen Zahlen nur lineare Verbindungen folgender Größen: $\zeta_{11}\xi_{1i}\,(i = 1, 2, \ldots, n)$, und diese erfahren bei rechtsseitiger Multiplikation mit den Gruppenelementen die Substitutionen der adjungierten Gruppe zu derjenigen, aus welcher die ξ_{ik} entnommen sind; sie sind daher unabhängig und unsere irreduzible Darstellung ist äquivalent mit der zu ξ_{ik} gehörigen. Damit ist bewiesen, daß wir in den irreduzibeln algebraischen Darstellungen alle irreduzibeln Darstellungen im $GF(p^f)$ gefunden haben. Nun sei eine halbreduzierte Darstellung im $GF(p^f)$ gegeben. Wir können uns auf den Fall zweier irreduzibler Bestandteile beschränken, da der allgemeine Fall durch sukzessive Anwendung des speziellen Resultates bewiesen werden kann. Die Substitutionen mögen die Gestalt haben:

$$\begin{pmatrix} A & C \\ O & B \end{pmatrix}.$$

Die hyperkomplexen Zahlen der ersten Zeile seien

$$\xi_1, \ldots, \xi_n, \eta_1, \ldots, \eta_m\,.$$

Bei rechtsseitiger Multiplikation mit den Gruppenelementen erfahren sie die zu unserer Darstellung adjungierte, welche folgende Gestalt hat:

1. $$\begin{pmatrix} A' & O \\ C' & B' \end{pmatrix}.$$

Falls die $m + n$ Zahlen linear unabhängig sind, so führt bereits das oben angewendete Verfahren zum Ziel. Dies ist insbesondere der Fall, wenn die Darstellungen A und B nicht äquivalent sind. Nun sei $A = B$ und daher $m = n$. Falls die Beziehung besteht

$$a_1\xi_1 + \ldots + a_n\xi_n = b_1\eta_1 + \ldots + b_n\eta_n\,,$$

so bleibt sie richtig, wenn man mit einer beliebigen hyperkomplexen Zahl multipliziert, es lassen sich also die n unabhängigen Zahlen

$\xi_1, \xi_2, \ldots, \xi_n$ durch die n Zahlen η_i ausdrücken und die letzteren sind daher unabhängig. Wir können sie umgekehrt durch die ξ_i ausdrücken. Es gelte:

$$\eta_i = \sum_1^n a_{ik} \xi_k .$$

Nun führen wir durch die unimodulare Substitution

$$\xi_i' = \zeta' \qquad \eta_i' = \eta_i - \sum_1^n a_{ik} \xi_k$$

neue Veränderliche ein. Multipliziert man sie rechts mit den Gruppenelementen, so erfahren sie eine mit 1. äquivalente Substitution, welche in derselben Weise reduziert ist. Sie sei $\begin{pmatrix} A & O \\ C & B \end{pmatrix}$, insbesondere wird

$$\eta_i' e_S = c_{i1} \xi_1' + \ldots + c_{in} \xi_n' + b_{i1} \eta_1' + \ldots + b_{in} \eta_n' .$$

Nun sind aber die Variabeln η_i' Null und unsere Gleichung wird zu

$$c_{i1} \xi_1' + \ldots + c_{in} \xi_n' = 0 .$$

Da die ξ_i unabhängig sind, so müssen die Koeffizienten verschwinden, und wir finden $\mathfrak{C} = 0$, was zu beweisen war.

Als spezielle Resultate heben wir folgende hervor:

Eine *Abel*sche Substitutionsgruppe, deren Ordnung zu p prim ist, läßt sich auf die Diagonalform reduzieren. Hierzu ist im allgemeinen eine Erweiterung des *Galois*feldes notwendig.

Wenn eine Gruppe $\mathfrak{G}$ sich in einem $GF(p^f)$ darstellen läßt und ihre Ordnung zu p prim ist, so läßt sich zu jeder anderen Primzahl q ein Exponent f' bestimmen dergestalt, daß sich $\mathfrak{G}$ als Gruppe desselben Grades im $GF(q^{f'})$ darstellen läßt. Falls die erste Gruppe irreduzibel war, so können auch die übrigen als irreduzible Gruppen bestimmt werden, vorausgesetzt, daß die zugehörige Primzahl q die Ordnung von $\mathfrak{G}$ nicht teilt.

Ferner gilt der Satz 156 für den Fall, daß p zur Ordnung prim ist, in seinem vollen Umfange. Die Substitutionsgruppen im $GF(p^f)$ verdanken also ihre ungeheure Mannigfaltigkeit einzig dem Primteiler p in ihrer Ordnung. Für die anderen Untergruppen findet eine außerordentliche Ökonomie in den möglichen Typen statt.

Eine Aufstellung der für die verschiedenen Primzahlen p möglichen Typen von Gruppen, deren Ordnung zu p prim ist, hängt mit zahlentheoretischen Fragen zusammen. Fragen wir uns, wann eine solche Gruppe vom Grade 2 im $GF(p)$ die erweiterte Ikosaedergruppe § 63 darstellt, so muß die Ordnung durch 5 teilbar sein, d. h. es muß sein

$$p^2 \equiv 1 \pmod 5$$

oder p ist quadratischer Rest mod 5. Wenn diese Bedingung erfüllt ist, so enthält die Gruppe wirklich die erweiterte Ikosaedergruppe,

denn diese läßt sich im Körper $k(\sqrt{5})$ algebraisch darstellen, und hier zerfallen gerade diese Primzahlen in Primideale ersten Grades. Für die übrigen Primzahlen p sind die Untergruppen mit einer zu p primen Ordnung sämtlich auflösbar.

§ 59. Raumgruppen.

In § 24 haben wir die sämtlichen Raumgitter mit besonderen Symmetrien aufgestellt und in § 55 haben wir diese Betrachtungen vertieft und teilweise auf beliebig viele Dimensionen ausgedehnt. Wir haben es dabei bewenden lassen mit denjenigen Symmetrien, welche den Anfangspunkt festlassen. Jetzt wollen wir diese Schranke fallen lassen und die Gruppe aller Symmetrien betrachten, welche ein Gitter in sich überführen. In ihr ist eine Gruppe T enthalten, welche aus allen Translationen des Gitters in sich besteht, sie ist *Abel*sch und besitzt im Falle von n Dimensionen n Erzeugende. Durch eine geeignete Wahl des Koordinatensystems können wir erreichen, daß ihre erzeugenden Substitutionen T_i folgende Gestalt haben:

$$x_i' = x_i + 1 \qquad x_k' = x_k \qquad (k \neq i),$$

wobei i alle Zahlen 1 bis n durchläuft.

Wir wollen im folgenden dieses Koordinatensystem festhalten. Eine allgemeine Symmetrie des Raumes wird dann durch die Gleichungen gegeben:

$$x_k' = a_{k1}\, x_1 + \ldots + a_{kn}\, x_n + a_k \quad (k = 1, 2, \ldots, n).$$

Hierbei bedeuten die ungestrichenen Variabeln x_i diejenigen des *neuen* Punktes, in welchen der ursprüngliche Punkt durch die Symmetrie übergeht. Nur bei dieser Festsetzung gewinnen wir für die Zusammensetzung der Symmetrien die gewohnten Gesetze der Matrizenzusammensetzung von Zeilen und Kolonnen. Wir bezeichnen die Substitution symbolisch mit

$$\begin{pmatrix} A & a \\ 0 & 1 \end{pmatrix} = (A),$$

wobei A die quadratische Matrix a_{kl} bedeutet, a die Spalte der a_k und 0 eine Zeile von n Nullen. A heißt der ***rotative***, a der ***translative*** Teil. Ist (B) eine zweite solche Symmetrie, so findet man die zusammengesetzte (C), indem man die Matrizen zusammensetzt:

$$\begin{pmatrix} A & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} B & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} C & c \\ 0 & 1 \end{pmatrix}.$$

Offenbar wird

$$C = AB \qquad \text{und} \quad c = Ab + a.$$

Gruppen, die aus solchen Substitutionen gebildet sind, heißen ***Raumgruppen***. Die Untergruppe der Translationen ist stets Normalteiler.

Nun sei eine beliebige Raumgruppe gegeben mit einer Translationsgruppe $\mathfrak{T}$, die n unabhängige Translationen enthält. Außerdem möge noch die Symmetrieoperation (A) vorkommen. Dann ist $(A)\mathfrak{T} = \mathfrak{T}(A)$. Sehen wir zu, was aus dem Anfangspunkt des Koordinatensystems wird, wenn man die Operationen dieser Nebengruppe der Translationsgruppe auf ihn anwendet. Nehmen wir die Nebengruppe zuerst in der Anordnung $(A)\mathfrak{T}$. Unter A erfährt der Anfangspunkt eine gewisse Translation a, und indem man nun alle Translationen von $\mathfrak{T}$ ausübt, erhält man ein Gitter unseres n-dimensionalen Raumes. Nun gehen wir umgekehrt vor und üben auf den Anfangspunkt die Operationen $\mathfrak{T}(A)$ aus. Es müssen dieselben Punkte entstehen. Durch $\mathfrak{T}$ entsteht dasselbe Gitter wie vorher, bloß ist die Translation a noch nicht ausgeführt. Nun kommt noch (A) hinzu. Dies gibt die Translation a und die durch A repräsentierte Symmetrie. Bereits durch die Translation ist aber unser Gitter in die definitive Lage gekommen und die Symmetrie A muß daher das Gitter in sich selbst transformieren, sie muß zu einer der endlich vielen ganzzahligen Gruppen gehören. Damit haben wir folgenden Satz gewonnen:

Satz 163: *In einer Raumgruppe des n-dimensionalen Raumes mit einer Translationsgruppe, die n unabhängige Erzeugende besitzt, bilden die rotativen Bestandteile eine ganzzahlige Gruppe.*

Falls es in jeder Nebengruppe der Translationsgruppe eine Operation gibt, deren translativer Bestandteil verschwindet, so besteht die Gruppe aus den Translationen eines Gitters und einem Teil der zum Gitter gehörigen Symmetrien, die einen Gitterpunkt ungeändert lassen. Dies ist aber nicht immer der Fall, und die Anzahl der Raumgruppen wird dadurch erheblich vergrößert. Wir beginnen mit einem speziellen Beispiel.

Das *monokline Gitter* besitzt eine Zweierachse (A). Wir nehmen den Fall des nicht zentrierten Gitters. $(A)\mathfrak{T}$ besteht aus Schraubenachsen, deren rotativer Teil eine Drehung von 180^0 ist, während die Schraubung aus allen Vielfachen der Elementardistanz für die Achsenrichtung ist. Statt der Zweierachse nehmen wir jetzt eine Schraubenachse mit der halben Distanz als Schraubung. Übt man diese Operation zweimal aus, so erhält man eine Translation. Aus der Schraubenachse entstehen durch Zusammensetzung mit den Translationen neue parallele Schraubenachsen, deren Schraubungskomponente in der Elementardistanz gemessen die Länge hat: $\frac{1}{2} +$ eine beliebige ganze Zahl. Diese Achsen bilden zusammen mit den Translationen auch eine Gruppe, sie ist aber verschieden von der vorigen, denn sie enthält nur Schraubenachsen mit von 0 verschiedener Schraubung und Translationen, aber keine reinen Drehungen. Wenn wir dagegen vom zentrierten Gitter ausgehen, so gibt es nur eine Raumgruppe, denn

hier ist die Distanz zweier nächster Gitterebenen, die senkrecht zur Achse liegen, die Hälfte der Elementardistanz für die Achse. Da die Schraubungskomponente jedenfalls die Hälfte eines ganzzahligen Vielfachen der Elementardistanz ist, so kann sie durch eine Translation des Gitters weggeschafft werden. *Es gibt also drei Raumgruppen, die zu der monoklinen Hemimorphie gehören.* Bei einer *Dreierachse* kommen zwei Gitter in Betracht: das *rhomboedrische,* zu dem es nur *eine Raumgruppe* gibt, und das *hexagonale,* wo wir *drei* erhalten: die Schraubungskomponente kann 0, $\frac{1}{3}$, $\frac{2}{3}$ der Elementardistanz für die Achse sein. Die Viererachse ergibt in derselben Weise für ihre zwei Gitter im ganzen $4 + 2$ Gruppen und die Sechserachse 6.

Im ganzen gibt es 230 Raumgruppen. Ihre Aufstellung ist eine ziemlich mühsame Aufgabe. Sie wurde zuerst von *Schönflies* gelöst in seinem Werk Kristallsysteme und Kristallstruktur (Leipzig 1891). Seither hat *P. Niggli* (Geometrische Kristallographie des Diskontinuums, Leipzig 1919) diese Gruppen vollständig durchgerechnet, die Substitutionen angegeben und die gegenüber einzelnen derselben invarianten Punkte aufgesucht. Sein Buch stellt die gründlichste Untersuchung dar, welche jemals einem Spezialgebiet der Gruppentheorie zuteil geworden ist, und das darin enthaltene Zahlenmaterial wird für die algebraische Zahlentheorie von ebenso großem Wert sein, wie für die Bestimmung der Kristallstruktur.

Die Aufstellung sämtlicher Raumgruppen übersteigt bei weitem den Rahmen dieses Buches. Wir wollen uns darauf beschränken, das Problem analytisch zu formulieren und in die allgemeine Theorie einzuordnen.

Wir betrachten im folgenden nur Gruppen, deren rotativer Teil vollständig reduziert die identische Darstellung nicht enthält, und beweisen den

Satz 164: *Es gibt nur endlich viele nicht äquivalente Raumgruppen des n-dimensionalen Raumes, welche n unabhängige Translationen besitzen.*

Beweis: Die rotativen Bestandteile können wir als ganzzahlig annehmen, und hierfür kommen nur endlich viele nicht äquivalente Gruppen in Betracht. Es muß nun noch gezeigt werden, daß man auch die translativen Bestandteile limitieren kann. Hierfür kommt nur noch die richtige Wahl des Koordinatenanfangspunktes in Betracht. Die Translationsgruppe sei $\mathfrak{T}$. Wir wählen aus jeder ihrer Nebengruppen eine Substitution (S, s) aus, wobei S den rotativen, s den translativen Teil bedeutet. s ist nur bis auf beliebige ganze Zahlen bestimmt, die man zu seinen Komponenten addieren kann. S durchläuft jede Substitution des rotativen Teiles genau einmal. Die Anzahl derselben sei h. Nun üben wir auf einen beliebigen Punkt diese

h Substitutionen aus und bilden den Schwerpunkt dieser Punkte. Zu dem Zweck haben wir die Koordinaten dieser h Punkte zu addieren und durch h zu dividieren. Da die Summe aller Matrizen S verschwindet, so fallen hierbei die Koordinaten des ausgewählten Punktes heraus, und wir finden für den gesuchten Schwerpunkt

$$\frac{1}{h}\sum s .$$

Da die s nur bis auf Gittervektoren bestimmt sind, so bilden die Schwerpunkte ein mit dem Translationsgitter ähnliches Gitter, dessen Abmessungen den h-ten Teil betragen. Jede Operation unserer Raumgruppe muß dieses Gitter in sich selbst überführen. Legen wir daher den Anfangspunkt in einen Schwerpunkt, so können die translativen Bestandteile nur noch rationale Zahlen mit dem Nenner h sein, denn sie bilden diejenigen Punkte, welche in den Nullpunkt übergeführt werden und müssen daher Vektoren des Schwerpunktgitters sein. Hiermit ist gezeigt, daß die translativen Bestandteile durch die rotativen limitiert sind, und unsere Behauptung ist bewiesen.

Falls die Gruppe einen Normalteiler $\mathfrak{N}$ von der Ordnung k besitzt, dessen rotativer Bestandteil die identische Darstellung nicht enthält, so kann man den Nenner auf k beschränken, denn man zeigt leicht, daß bereits die Schwerpunkte der Punktsysteme, die durch den Normalteiler erzeugt werden, durch alle Operationen der Gruppe in sich transformiert werden. Allgemein werden nämlich die Schwerpunkte eines durch eine Untergruppe erzeugten Punktsystems durch die Operationen der Gruppe in solche übergeführt, welche durch konjugierte Untergruppen entstehen.

Aus dieser Bemerkung ist ersichtlich, daß im Falle des Symmetriezentrums als Nenner nur 2 auftritt. Ferner haben gerade die kompliziertesten Gruppen des R_3, nämlich diejenigen des kubischen Systems, einen *Abel*schen Normalteiler von der Ordnung 4, die Vierergruppe, so daß auch hier nur der Nenner 4 auftritt, statt 12 und 24. Diesem Umstand ist die relativ geringe Zahl der Raumgruppen des R_3 zu verdanken. Es ist dieselbe Tatsache, welche auch die Lösbarkeit der Gleichungen der vier ersten Grade durch Wurzeln ermöglicht.

Reduziert man in den Substitutionen die translativen Bestandteile nach dem Modul der ganzen Zahlen, so bilden sie eine mit der Gruppe der rotativen Teile homomorphe Gruppe Γ, und die Aufsuchung aller Raumgruppen einer Kristallklasse ist gleichbedeutend mit der Aufstellung dieser sämtlichen nicht äquivalenten Gruppen. Um über die gruppentheoretische Natur dieses Problems vollen Aufschluß zu erhalten, füge man zu Γ noch die sämtlichen Translationen hinzu, deren Komponenten rationale Zahlen mit dem Nenner h und echte Brüche sind. In der zusammengesetzten Gruppe Γ' bilden

die Translationen einen Normalteiler und Γ besteht aus den erzeugenden Elementen der Faktorgruppe. Das Problem besteht nun darin, *alle Systeme von Elementen zu finden, welche die Faktorgruppe erzeugen* ***und eine Gruppe bilden.*** Dieses Problem ist in seiner Allgemeinheit noch nicht gelöst.

Man kann die Voraussetzungen noch allgemeiner fassen und zeigen, daß jede Raumgruppe mit endlichem Fundamentalbereich im R_n gerade n unabhängige Translationen enthält, so daß der allgemeine Satz[1]) gilt:

Es gibt nur endlich viele nicht äquivalente Raumgruppen des R_n mit endlichem Fundamentalbereich.

Hierbei hat man natürlich im Falle der „zerlegbaren" Gruppen, insbesondere wenn der rotative Bestandteil die identische Darstellung enthält, den Begriff der Äquivalenz sinngemäß zu erweitern.

15. Kapitel.

Gleichungstheorie.

Die Gruppentheorie ist nach *Lagrange* die „wahre Metaphysik" der Gleichungen. Aber umgekehrt ist auch zu sagen, daß ihre Sätze durch die Übertragung auf algebraische Gleichungen häufig an Faßlichkeit gewinnen, ähnlich wie die Geometrie dem Verständnis der Analysis hilft. In noch viel höherem Maß gilt dies von der die Algebra verfeinernden Zahlentheorie. Diese bildet streckenweise eine beinahe unzertrennbare Einheit mit der Gruppentheorie. Dies soll in der folgenden kurzen Übersicht gezeigt werden.

§ 60. Die *Lagrange*sche Gleichungstheorie.

Ein System von Zahlen oder Funktionen bildet einen ***Körper,*** wenn die vier elementaren Rechnungsoperationen Addition, Subtraktion, Multiplikation und Division angewendet auf zwei Individuen des Systems nur solche Zahlen oder Funktionen ergeben, die bereits im System vorkommen. Hierbei ist die Division durch die Null auszunehmen.

Wir gehen aus von der Gesamtheit aller rationalen Funktionen der n Variabeln $x_1, x_2, \ldots, x_n$. Als numerische Koeffizienten lassen wir in diesem Paragraphen alle reellen und komplexen Zahlen zu. Diese Funktionen bilden einen Körper, den wir mit K bezeichnen. Diejenigen Funktionen aus K, welche bei sämtlichen Permutationen

[1]) *Bieberbach, L.:* Über die Bewegungsgruppen der Euklidischen Räume. Math. Ann. **70**, S. 297 und **72**, S. 400. — *Frobenius, G.:* Über die unzerlegbaren diskreten Bewegungsgruppen. Berliner Sitzungsberichte S. 654, 1911.

der n Variabeln ungeändert bleiben, bilden einen Körper, den wir mit S bezeichnen, er ist ein ***Teilkörper*** oder ***Unterkörper*** von K, da jede seiner Funktionen in K vorkommt. Die algebraische Beziehung zwischen S und K aufzudecken ist unsere Aufgabe.

Eine Funktion aus S heißt eine symmetrische Funktion der n Variabeln und sie kann als rationale Funktion der n elementarsymmetrischen Funktionen dargestellt werden. Für später ist hier noch hinzuzufügen, daß die Koeffizienten rationale Zahlen sind, wenn die Funktion aus S rationale Koeffizienten hatte. Wir bezeichnen die $n!$ Permutationen der Variabeln mit $E, A, \ldots, T, U, \ldots$ und die ganze symmetrische Gruppe mit $\mathfrak{S}$. Diejenigen Permutationen, welche eine Funktion aus K ungeändert lassen, bilden eine Untergruppe von $\mathfrak{S}$. Man sagt dann, die Funktion ***gehört*** zu dieser Untergruppe. Ist $f(x_1, \ldots, x_n)$ eine Funktion aus K, so bezeichnen wir diejenigen Funktionen, die aus ihr durch die Permutationen $E, A, B, \ldots$ entstehen, mit $f_E = f, f_A, f_B, \ldots$. Sie heißen die zu f ***konjugierten*** Funktionen und genügen einer Gleichung vom Grade $n!$, deren Koeffizienten symmetrische Funktionen sind, nämlich:

$$(t - f_E)(t - f_A)(t - f_B) \ldots = 0.$$

Wenn f zur Untergruppe $\mathfrak{H}$ von $\mathfrak{S}$ gehört, so kann man f auch mit $f_{\mathfrak{H}}$ bezeichnen. Ist

$$\mathfrak{S} = \mathfrak{H} + \mathfrak{H}S_2 + \ldots + \mathfrak{H}S_r,$$

so sind bloß r der mit f konjugierten Funktionen voneinander verschieden, nämlich in leicht verständlicher Bezeichnungsweise die Funktionen

$$f_{\mathfrak{H}}, \quad f_{\mathfrak{H}S_2}, \ldots, \quad f_{\mathfrak{H}S_r}.$$

Sie genügen im Körper S einer Gleichung vom Grade r.

Es gilt nun der

Satz 165: *Wenn f zu der Untergruppe $\mathfrak{H}$ gehört, so läßt sich jede Funktion y aus K, die bei den Permutationen von $\mathfrak{H}$ ungeändert bleibt, darstellen als ganze Funktion von f mit Koeffizienten aus S. Der Grad dieser Funktion von f kann immer auf $r - 1$ erniedrigt werden.*

Beweis: Man bildet nach Lagrange folgenden Ausdruck:

$$(t - f_{\mathfrak{H}})(t - f_{\mathfrak{H}S_2}) \ldots (t - f_{\mathfrak{H}S_r}) \left(\frac{y_{\mathfrak{H}}}{t - f_{\mathfrak{H}}} + \frac{y_{\mathfrak{H}S_2}}{t - f_{\mathfrak{H}S_2}} + \ldots + \frac{y_{\mathfrak{H}S_r}}{t - f_{\mathfrak{H}S_r}} \right) = G(t).$$

$G(t)$ ist eine ganze Funktion $(r - 1)$-ten Grades von t, deren Koeffizienten symmetrische Funktionen der n Variabeln x sind, d. h. G liegt in S. Dasselbe gilt von

$$H(t) = (t - f_{\mathfrak{H}})(t - f_{\mathfrak{H}S_2}) \ldots .$$

Setzt man nun $t = f$, so folgt

$$y = \frac{G(f)}{H'(f)}.$$

Multipliziert man Zähler und Nenner mit dem Produkt

$$H'(f_{\mathfrak{H}} s_2)\, H'(f_{\mathfrak{H}} s_3) \ldots H'(f_{\mathfrak{H}} s_r),$$

so wird der Nenner eine symmetrische Funktion und der Grad des Zählers kann mit Hilfe der Gleichung, der f in S genügt, mindestens auf $r - 1$ herabgesetzt werden.

Satz 166: *Zu jeder Untergruppe gehört ein Unterkörper von K, der S enthält.*

Beweis: Die Funktion

$$x_1 + 2x_2 + 3x_3 + \ldots + nx_n = y$$

gehört zu E, daher läßt sich jede Funktion aus K darstellen als ganze Funktion vom Grade $n! - 1$ von y mit Koeffizienten aus S. Ist nun $\mathfrak{H}$ irgendeine Untergruppe von $\mathfrak{S}$, so bilde man das Produkt

$$\prod_{\mathfrak{H}} y_S$$

von y mit den Linearformen, die durch die Permutationen von $\mathfrak{H}$ daraus hervorgehen. Diese Funktion gehört zu $\mathfrak{H}$ und erzeugt den zu $\mathfrak{H}$ gehörigen Körper.

Satz 167: *Außer den zu den verschiedenen Untergruppen von $\mathfrak{S}$ gehörigen Körpern gibt es keine weiteren Unterkörper von K, die S enthalten.*

Beweis: Wenn ein Körper zwei Funktionen enthält, die zu den Untergruppen $\mathfrak{H}$ und $\mathfrak{K}$ gehören, so enthält sie auch eine solche, die zum Durchschnitt $\mathfrak{D}$ von $\mathfrak{H}$ und $\mathfrak{K}$ gehört. Wir können nämlich die beiden Funktionen als Formen, z. B. als Produkte der y, annehmen und bezeichnen sie mit g und h. Alsdann bilden wir den Ausdruck

$$f + g^a,$$

wobei a eine ganze positive Zahl bedeutet, die so groß ist, daß der Grad von g^a größer ist als derjenige von f. Bei jeder Permutation außerhalb von $\mathfrak{D}$ ändert sich mindestens einer der Summanden, und in der Summe können sich die Änderungen wegen der Verschiedenheit der Grade nicht aufheben. Nun gehört in einem beliebigen Körper zwischen S und K jede Funktion zu einer bestimmten Untergruppe von $\mathfrak{S}$ und es folgt aus dem eben Bewiesenen, daß der Körper auch eine Funktion enthält, die zu dem Durchschnitt aller dieser Untergruppen gehört, d. h. unser Körper ist identisch mit dem zu diesem Durchschnitt gehörigen Körper.

Ersichtlich ist die Aufgabe, die algebraische Beziehung des Körpers K gegenüber dem Körper S zu bestimmen, identisch mit dem Problem der Auflösung der allgemeinen Gleichung n-ten Grades. Der gewaltige Fortschritt, den *Lagrange* erreicht hat, besteht in der vollen Übersicht, die man über die einzelnen Etappen des Weges gewinnt; daß man nicht direkt auf die Wurzeln lossteuern muß, sondern daß

man andere Größen des Körpers zu Hilfe nehmen kann, ist bereits im Ansatz der *Tschirnhausen*schen Transformation enthalten; seit *Lagrange* weiß man aber, welches die Hilfsfunktionen sind, die zum Ziele führen können. Die Gruppentheorie ist die „wahre Metaphysik" des Problemes.

Wie *Lagrange* seine Erkenntnis auf die Gleichungen 3. und 4. Grades angewendet hat, ist allgemein bekannt und in jedem Lehrbuch der Algebra nachzulesen, wir verzichten hier auf eine Reproduktion. Dagegen soll einiges über die sogenannten ***Lagrangeschen Resolventen*** hier Platz finden.

Satz 168: *Kennt man den zu einer zyklischen Untergruppe $\mathfrak{H}$ von der Ordnung h gehörigen Körper, so läßt sich der ganze Körper durch die Auflösung einer reinen Gleichung vom Grade h bestimmen.*

Beweis: Bei der zyklischen Gruppe möge die Variable x_1 übergehen in $x_2, x_3, \ldots, x_h$. Man bezeichne mit ε die Zahl

$$e^{\frac{2ki}{h}}$$

und bilde die Ausdrücke:

$$y_i = x_1 + \varepsilon^{-i} x_2 + \ldots + \varepsilon^{-i(h-1)} x_h \quad (i = 1, 2, \ldots, h).$$

Bei der zyklischen Permutation erhält y_i den Faktor ε^i. Daher bleiben die h-ten Potenzen bei $\mathfrak{H}$ ungeändert und lassen sich rational bestimmen. Wir bilden nun y_1, indem wir eine h-te Wurzel ziehen und erhalten dafür h verschiedene Werte. Jetzt sind die übrigen Größen y_i eindeutig durch y_1 bestimmt, denn die $h - 2$ Ausdrücke

$$y_1 y_{h-1}, \; y_1^2 y_{h-2}, \ldots, \; y_1^{h-2} y_2$$

gehören zu $\mathfrak{H}$. Durch Addition aller h Funktionen y_i findet man hx_1 und indem man für y_1 alle seine h Werte einsetzt, erhält man die h Wurzeln $x_1, x_2, \ldots, x_h$. Auf dieselbe Weise findet man die übrigen Variabeln.

Man kann das Resultat von *Lagrange* so formulieren: *Der zu einer zyklischen Gruppe von der Ordnung h gehörige Unterkörper enthält die h-te Potenz einer Funktion, die sich bei jeder Permutation außer E ändert.* Bei drei oder vier Variabeln kann man nach diesem Muster von dem Körper der symmetrischen Funktionen sukzessive bis zum Körper K gelangen. Aber erst *Galois* hat erkannt, daß diese Tatsache bereits aus der Beschaffenheit der Gruppe folgt.

§ 61. Die *Galois*sche Gleichungstheorie.

Für die weitere Entwicklung der Gruppentheorie sind von entscheidender Bedeutung die Disquisitiones arithmeticae von *Gauß* (1801). In der sectio VII werden die Kreisteilungsgleichungen behandelt, insbesondere die Gleichung

$$x^p = 1,$$

wobei p eine Primzahl ist. Ihre Wurzeln lassen sich bekanntlich mit Hilfe der trigonometrischen Funktionen angeben. *Gauß* untersuchte ihren algebraischen Charakter gegenüber den rationalen Zahlen. Er bewies, daß die Gleichung

$$x^{p-1} + x^{p-2} + \ldots + x + 1 = 0$$

im Bereich der rationalen Zahlen irreduzibel ist, d. h. nicht in zwei Faktoren niedrigeren Grades mit rationalen Koeffizienten zerfällt. *Ferner erkannte er, daß der Berechnung ihrer Wurzeln nicht das allgemeinste Lagrangesche Problem von $p-1$ Variablen zugrunde liegt, sondern bloß dasjenige mit zyklischer Gruppe von der Ordnung $p-1$,* und führte die Aufgabe zurück auf die Auflösung gewisser Hilfsgleichungen von Primzahlgrad, deren Wichtigkeit er betonte: Summam attentionem merentur aequationes auxiliares, ..., quae mirum in modum cum proprietatibus maxime reconditis numeri n (hier p) connexae sunt (art. 356). Dies ist die von *Abel* und *Galois* häufig zitierte „méthode de M. *Gauß*".

*Abel*s Untersuchungen über Gruppentheorie führen ihn zu dem Resultat, daß jede Gleichung mit kommutativer „*Abel*scher" Gruppe durch Wurzelzeichen lösbar ist (Mémoire sur une classe particulière d'équations résolubles algébriquement, Crelles Journ., Bd. 4, 1829 und Oeuvres, Bd. 1, S. 478, nouvelle édition). Weitere Untersuchungen über algebraisch auflösbare Gleichungen, sowie den Beweis der Unmöglichkeit, die allgemeine Gleichung 5. Grades algebraisch aufzulösen, führt er ohne explizite Heranziehung der Gruppentheorie.

Die allgemeine Idee der Gruppe einer Gleichung hat *E. Galois* erkannt und mit wunderbarer Klarheit und Schärfe in seinem Mémoire sur les conditions de résolubilité des équations par radicaux entwickelt. Diese Abhandlung vom Jahre 1830 wurde erst 1846 von *Liouville* in seinem Journal veröffentlicht (Oeuvres de *Galois*, S. 33). Dagegen erschien 1832 der Brief an *Auguste Chevalier*, den *Galois* am Abend vor seinem Tode geschrieben hat und in dem er seine wichtigsten mathematischen Entdeckungen mitteilt.

Es bedeutet nur eine unwesentliche Einschränkung, wenn wir im folgenden die Voraussetzung machen, daß die Gleichungen rationale Zahlen als Koeffizienten haben. Wir setzen voraus, daß wir jede ganze Funktion im Körper der rationalen Zahlen in ihre irreduziblen Faktoren zerlegen können. Mit Hilfe des euklidischen Algorithmus beweist man folgende Sätze:

Eine im Körper R der rationalen Zahlen irreduzible Funktion besitzt keine mehrfachen Wurzeln.

$f(t)$ und $g(t)$ seien zwei Funktionen in R mit einer gemeinsamen Wurzel und $f(t)$ sei irreduzibel, dann ist g teilbar durch f.

Es sei eine im Körper R der rationalen Zahlen irreduzible Gleichung mit Koeffizienten aus R gegeben:

$$f(t) = 0.$$

Ihre Wurzeln seien

$$\alpha_1, \alpha_2, \ldots, \alpha_n.$$

Die Gesamtheit der rationalen Funktionen der Wurzeln mit rationalen Zahlenkoeffizienten bilden einen *Zahlkörper* K, dessen algebraische Natur gegenüber dem Grundkörper R untersucht werden soll. Wir beweisen zunächst folgenden

Satz 169: *Man kann n rationale Zahlen A_i so bestimmen, daß die $n!$-Zahlen, die aus*

$$A_1\alpha_1 + A_2\alpha_2 + \ldots + A_n\alpha_n = \vartheta$$

hervorgehen, indem man auf die Wurzeln α_i die $n!$ Permutationen ausübt, sämtlich untereinander verschieden sind.

Beweis: Wir fassen die n Größen A_i zunächst als Variable auf. Übt man auf die Wurzeln in ϑ die Permutationen aus, so erhält man $n!$ voneinander verschiedene Linearformen der Variabeln A_i. Die Differenz zweier beliebiger dieser Formen ist wieder eine nicht verschwindende Linearform und das Produkt aller Differenzen ist eine Form der A_i, deren Koeffizienten symmetrische Funktionen der Wurzeln mit ganzzahligen Koeffizienten sind, d. h. die Koeffizienten sind rationale Zahlen. Man kann nun den Variabeln solche rationale Werte erteilen, daß die Form einen von 0 verschiedenen Wert annimmt, womit der Satz bewiesen ist.

Wir verstehen unter ϑ eine nach Satz 169 gewählte Zahl. Es läßt sich dann jede Zahl des Körpers als ganze Funktion vom $(n! - 1)$-ten Grade in ϑ mit rationalen Koeffizienten darstellen. Statt ϑ kann auch eine beliebige der $n!$ Zahlen gewählt werden, die durch die Permutationen daraus hervorgehen. Wir bezeichnen sie mit $\vartheta = \vartheta_1, \vartheta_2, \ldots, \vartheta_n$.

Die Gleichung

$$(t - \vartheta_1)(t - \vartheta_2)\ldots(t - \vartheta_{n!}) = 0$$

besitzt rationale Zahlenkoeffizienten, *sie braucht aber in R nicht irreduzibel zu sein.* $F(t)$ sei einer ihrer irreduzibeln Faktoren, $\vartheta, \vartheta', \ldots, \vartheta^{(g-1)}$ seien seine Wurzeln. Infolge des Bestehens der Gleichung $F(t) = 0$ läßt sich jede Zahl α von K bereits als Funktion $(g-1)$-ten Grades von ϑ ausdrücken:

$$x_1 + x_2\vartheta + \ldots + x_g\vartheta^{g-1} = \alpha.$$

Jetzt ersetzt man ϑ durch ϑ'. Die Zahlen von K erfahren dadurch eine bestimmte Permutation, die durch (ϑ, ϑ') symbolisiert werden kann. Allgemein definiert $(\vartheta, \vartheta^{(i)})$ eine Permutation und wir wollen ihre Eigenschaften durch folgende Sätze charakterisieren.

Satz 170: *Diejenigen Zahlen, welche bei allen Permutationen* $(\vartheta, \vartheta^{(i)})$ *ungeändert bleiben, bilden den Körper der rationalen Zahlen.*

Beweis: Wenn

$$\alpha = x_1 + x_2\vartheta + \ldots + x_g\vartheta^{g-1}$$

eine rationale Zahl ist, so ist

$$x_2 = x_3 = \ldots = x_g = 0, \qquad x_1 = \alpha,$$

denn andernfalls würde ϑ in K einer Gleichung vom Grade $g-1$ genügen. Hieraus folgt, daß die Substitutionen $(\vartheta, \vartheta^{(i)})$ ohne Einfluß auf die Zahl sind. Nun möge umgekehrt α bei den Substitutionen ungeändert bleiben. Man addiere die Ausdrücke

$$\alpha = x_1 + x_2\vartheta^{(i)} + \ldots + x_g\vartheta^{(i)g-1}$$

indem man für $\vartheta^{(i)}$ alle Wurzeln $\vartheta, \vartheta', \ldots, \vartheta^{(g-1)}$ einsetzt und findet, daß $g\alpha$ und daher auch α einen rationalen Zahlwert hat, weil dasselbe von den Potenzsummen der ϑ gilt.

Nun sei

$$\alpha = x_1 + x_2\vartheta + \ldots + x_g\vartheta^{g-1}$$

eine beliebige Zahl aus K, ferner setzen wir

$$\alpha^{(i)} = x_1 + x_2\vartheta^{(i)} + \ldots + x_g\vartheta^{(i)g-1} \qquad (i = 1, 2, \ldots, g-1)$$

und nennen $\alpha^{(i)}$ die zu α ***konjugierten Zahlen.***

Satz 171: *Es ist für zwei beliebige Zahlen aus K stets*

$$(\alpha + \beta)^{(i)} = \alpha^{(i)} + \beta^{(i)} \qquad (\alpha\beta)^{(i)} = \alpha^{(i)}\beta^{(i)}.$$

Beweis: Wir setzen

$$\alpha + \beta = \gamma \qquad \alpha\beta = \delta$$

und drücken die vier Zahlen $\alpha, \beta, \gamma, \delta$ durch ϑ aus. Dann erhalten wir zwei Gleichungen für ϑ mit rationalen Koeffizienten. Diese müssen auch erfüllt sein, wenn wir ϑ durch eine beliebige der konjugierten Zahlen $\vartheta^{(i)}$ ersetzen, womit der Satz bewiesen ist.

Satz 172: *Die Permutationen* $(\vartheta, \vartheta^{(i)})$ *bilden g Automorphismen des Körpers K, d. h. jede rationale Beziehung mit rationalen Koeffizienten, die zwischen Zahlen von K besteht, geht durch die Permutationen in richtige Beziehungen über.*

Beweis: Jede der angegebenen Beziehungen läßt sich auf die Gestalt bringen

$$F(\alpha, \beta, \gamma, \ldots) = 0,$$

wobei F eine ganze rationale Funktion der Zahlen $\alpha, \beta, \gamma, \ldots$ mit rationalen Koeffizienten ist. Indem man Satz 171 mehrere Male anwendet, findet man

$$F(\alpha, \beta, \gamma, \ldots)^{(i)} = F(\alpha^{(i)}, \beta^{(i)}, \gamma^{(i)}, \ldots) = 0^{(i)} = 0.$$

Hieraus folgt, daß die konjugierten Zahlen Wurzeln derselben irreduziblen Gleichung in R sind.

Satz 173: *Die Permutationen* $(\vartheta, \vartheta^{(i)})$ *bilden eine Gruppe, die* ***Galoissche Gruppe*** *des Körpers* K. *Sie ist identisch mit der Gruppe aller Automorphismen von* K.

Beweis: Führt man zwei Automorphismen nacheinander aus, so ist das Resultat wieder ein solcher, d. h. die Automorphismen bilden eine Gruppe. Da die rationalen Zahlen stets ungeändert bleiben, so kann ϑ nur in eine der Zahlen $\vartheta', \ldots, \vartheta^{(g-1)}$ übergehen und die beliebige Zahl

$$\alpha = x_1 + x_2\vartheta + \ldots + x_g\vartheta^{g-1}$$

bleibt entweder ungeändert oder sie geht in $\alpha^{(i)}$ über. Es gibt also nur die g Automorphismen

$$(\vartheta, \vartheta) \quad \text{und} \quad (\vartheta, \vartheta^{(i)}) \qquad (i = 1, 2, \ldots, g-1)$$

Satz 174: *Zu jeder Untergruppe der Galoisschen Gruppe* $\mathfrak{G}$ *gehört ein Unterkörper, jeder Unterkörper gehört zu einer Untergruppe.*

Beweis: wie zu Satz 166 und 167.

Die *verschiedenen* Zahlen $\alpha, \alpha', \ldots, \alpha^{(r-1)}$ welche aus α durch die Permutationen von $\mathfrak{G}$ hervorgehen, sind die Wurzeln der in R irreduzibeln Gleichung, welcher α genügt. Sie erfahren unter $\mathfrak{G}$ eine transitive Permutationsgruppe. Diejenigen Permutationen, welche α ungeändert lassen, bilden eine Untergruppe von $\mathfrak{G}$ vom Index r. Körper, die durch konjugierte Zahlen erzeugt werden, heißen konjugierte Körper. Sie gehören zu konjugierten Untergruppen.

Definition: Körper, die mit ihren konjugierten übereinstimmen, heißen ***Galoissche Körper.***

Satz 175: *Die notwendige und hinreichende Bedingung dafür, daß ein Unterkörper von* K *Galoissch ist, besteht darin, daß seine Gruppe ein Normalteiler von* $\mathfrak{G}$ *ist.*

Satz 176: *Ist* H *ein Galoisscher Unterkörper, der zu dem Normalteiler* $\mathfrak{N}$ *von* $\mathfrak{G}$ *gehört, so ist* $\mathfrak{G}/\mathfrak{N}$ *seine Gruppe in* R.

Beweis: Ist r der Index von $\mathfrak{N}$ unter $\mathfrak{G}$, so ist r auch der Grad von H und seine Gruppe hat daher die Ordnung r. Gerade so viele Automorphismen liefert aber die *Galois*sche Gruppe von K, denn die Zahlen von H bleiben bei $\mathfrak{N}$ ungeändert und erfahren unter $\mathfrak{G}$ eine Permutationsgruppe von der Gestalt $\mathfrak{G}/\mathfrak{N}$. Die *Galois*sche Gruppe von H ist isomorph mit derjenigen von K.

Die Resultate dieses Paragraphen lassen sich ohne weiteres auf den Fall übertragen, daß der Grundkörper ein beliebiger Körper R ist. Die *Galois*sche Gruppe besteht aus denjenigen Automorphismen von K, bei denen die Größen von R ungeändert bleiben. Man erhält alle Körper zwischen R und K, indem man alle Untergruppen der *Galois*schen Gruppe bestimmt. Zu einem Normalteiler gehören

Körper, die ***in*** R oder ***relativ zu*** R *Galois*sch sind. Hier ordnet sich auch der Fall des vorigen Paragraphen unter.

Satz 177: *Eine Gleichung ist dann und nur dann durch Wurzelzeichen auflösbar, wenn ihre Gruppe auflösbar ist.*

Beweis: Jeder Körper K, der aus R durch Wurzeloperationen erreichbar ist, kann offenbar folgendermaßen aufgebaut werden: man zieht aus einer Größe von R die p-te Wurzel, wobei p eine Primzahl ist, und fügt sie zu R hinzu. Hierdurch entstehe der Körper K_1. Wir setzen voraus, daß R die p-ten Einheitswurzeln enthält und finden, daß der neue Körper in R *Galois*sch ist. Sein Relativgrad ist p und seine Gruppe daher zyklisch und von der Ordnung p. Mit K_1 verfährt man gleich, selbstverständlich können Wurzeln von beliebigem Primzahlgrad vorkommen. Schließlich wird man K erreichen. Die eingeschalteten Körper seien $R, K_1, \ldots, K_{r-1}, K$. Jeder Körper ist *Galois*sch in dem vorhergehenden. Daraus folgt, daß die zu ihnen gehörenden Untergruppen eine Kompositionsreihe für $\mathfrak{G}$ mit lauter zyklischen Faktorgruppen bilden. Umgekehrt: Ist $\mathfrak{G}$ auflösbar und bildet $\mathfrak{G}, \mathfrak{H}_1, \mathfrak{H}_2, \ldots, \mathfrak{H}_{r-1}, E$ eine Kompositionsreihe, so bilden die zu dieser Reihe gehörigen Körper eine Folge von derselben Beschaffenheit wie die obige Reihe der Körper K, denn jeder ist *Galois*sch in dem vorhergehenden und seine Relativgruppe hat Primzahlordnung. Nach Satz 168 lassen sie sich also durch Wurzeln bestimmen.

Wenn ferner K ein Körper mit nicht auflösbarer Gruppe ist, so kann er nicht in einem auflösbaren Körper enthalten sein, das würde dem Satz über die Kompositionsreihe widersprechen: in einer auflösbaren Gruppe ist jede Untergruppe und jede Faktorgruppe auflösbar.

§ 62. Anwendungen der allgemeinen Gruppentheorie.

Jeder Satz der Gruppentheorie wird nun zu einem Satz über algebraische Körper. Wir geben hier einige Beispiele: Ein Unterkörper von K, der zu einer größten Untergruppe von $\mathfrak{G}$ gehört, möge ***primitiv*** in R heißen. Eine ihn erzeugende Zahl erfährt mit ihren konjugierten unter der *Galois*schen Gruppe eine primitive Permutationsgruppe. Wenn also K auflösbar ist, so ist der Grad seiner primitiven Unterkörper eine Primzahlpotenz.

Wenn ein Körper einen *Abel*schen Unterkörper enthält, so enthält er auch einen *größten Abel*schen Unterkörper, der alle anderen umfaßt, es ist der zur *Kommutatorgruppe* gehörige.

α sei eine Größe, welche zu der Untergruppe $\mathfrak{H}$ gehört und

$$f(t) = 0$$

sei die in R irreduzible Gleichung, der α genügt. Wie zerfällt sie in

dem zur Untergruppe $\mathfrak{R}$ gehörigen Körper? Um diese Frage zu beantworten, zerlege man $\mathfrak{G}$ nach dem Doppelmodul $(\mathfrak{H}, \mathfrak{R})$. Jedem Komplex dieser Zerlegung entspricht ein Faktor von f, dessen Grad gleich der Anzahl der Nebengruppen von $\mathfrak{H}$ in diesem Komplex ist. Adjungieren wir der Gleichung $f(t) = 0$ eine ihrer Wurzeln α, so wird sich nur der Faktor $t - \alpha$ abspalten, falls die Gruppe der Gleichung (die Permutationsgruppe ihrer Wurzeln) mindestens zweifach transitiv ist. Im anderen Falle ergeben jeweils die unter $\mathfrak{H}$ transitiv verbundenen Größen die Wurzeln eines irreduzibeln Faktors von $f(t)$.

Die Methoden lassen sich ferner auf die von *Galois* entdeckten Imaginären, die sogenannten *Galois*-Felder GF (vgl. § 16) übertragen. Ein solches ist vollkommen bestimmt, wenn die Anzahl seiner Elemente, die eine beliebige Primzahlpotenz sein kann, gegeben ist. Das $GF(p^f)$ enthält als Unterkörper das $GF(p)$, d. h. die Reste der ganzen Zahlen (mod p). Wir beweisen, daß seine Gruppe im $GF(p)$ zyklisch und von der Ordnung f ist. Ersetzt man nämlich jedes seiner Elemente durch seine p-te Potenz, so bleiben die Elemente aus $GF(p)$ ungeändert und die Elemente des $GF(p^f)$ erfahren einen Automorphismus. Es gilt ja

$$(\alpha \cdot \beta)^p = \alpha^p \cdot \beta^p \quad \text{und} \quad (\alpha + \beta)^p = \alpha^p + \beta^p,$$

letztere Gleichung deswegen, weil in der Binomialformel sämtliche Koeffizienten außer dem ersten und letzten durch p teilbar sind. Ist nun α ein erzeugendes (primitives) Element des $GF(p^f)$, so genügt es im $GF(p)$ einer irreduzibeln Gleichung vom Grade f. Wegen des Automorphismus sind die Wurzeln dieser Gleichung

$$\alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^f} = \alpha.$$

Die *Galois*sche Gruppe wird gebildet von den f Substitutionen

$$(\alpha, \alpha), (\alpha, \alpha^p), \ldots, (\alpha, \alpha^{p^{f-1}}).$$

Ist $f = rs$, so bilden die Elemente, die bei der Substitution (α, α^{p^s}) ungeändert bleiben, den Unterkörper $GF(p^r)$.

Die Tatsache, daß man die *Galois*sche Theorie der GF völlig beherrscht, ist von größter Wichtigkeit für die algebraische Zahlentheorie. Man zeigt dort, daß die Reste eines Primideals $\mathfrak{p}$, das in p aufgeht, ein $GF(p^f)$ bilden. f heißt der ***Grad*** von $\mathfrak{p}$.

Diejenige Untergruppe $\mathfrak{Z}$ der Gruppe des Zahlkörpers, welche das Primideal $\mathfrak{p}$ nicht ändert, heißt die ***Zerlegungsgruppe.*** Übt man sie auf die Zahlen des Körpers aus und reduziert (mod $\mathfrak{p}$), so erhält man einen Automorphismus des $GF(p^f)$. Ist $\mathfrak{T}$ die Untergruppe von $\mathfrak{Z}$, welche den identischen Automorphismus liefert, so ist $\mathfrak{T}$ Normalteiler von $\mathfrak{Z}$ und $\mathfrak{Z}/\mathfrak{T}$ zyklisch. $\mathfrak{T}$ heißt die ***Trägheitsgruppe*** von $\mathfrak{p}$ und man zeigt leicht, daß ihr Index genau gleich f ist. Um auch $\mathfrak{T}$ zu untersuchen, die nur für Diskriminantenteiler von E verschieden ist,

untersucht man nach *Hilbert* (Zahlbericht, S. 250ff. vgl. ferner *Speiser, A.*, Die Zerlegungsgruppe. Crelles Journ. **149**, S. 174—188) die Automorphismengruppe der Reste nach höheren Potenzen von $\mathfrak{p}$. Die Aufgabe wird dadurch erleichtert, daß man die erzeugende Zahl der Reste (mod. $\mathfrak{p}$) als unverändert durch $\mathfrak{T}$ annehmen kann. Ist nun Π eine durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbare Zahl, so sind alle Reste (mod $\mathfrak{p}^2$) darstellbar in der Gestalt

$$\alpha + \beta \Pi,$$

wobei α und β alle Reste (mod $\mathfrak{p}$) durchlaufen. Man erhält nun alle Automorphismen von $\mathfrak{T}$, indem man die Änderungen von Π angibt Offenbar darf Π übergehen in jeden Rest $\gamma \Pi$, wenn nur γ von 0 verschieden ist. Diese Substitutionen bilden wieder eine zyklische Gruppe von der Ordnung $p^n - 1$. Die Untergruppe, welche auch diese Reste ungeändert läßt, heißt die ***Verzweigungsgruppe*** $\mathfrak{V}$. Nimmt man die Reste (mod $\mathfrak{p}^3$), so sehen die Substitutionen von $\mathfrak{V}$ so aus:

$$\Pi \to \Pi + \alpha \Pi^2.$$

Setzt man zwei solche zusammen, etwa die obige und eine zweite mit β statt α, so erhält man die Substitution

$$\Pi \to \Pi + (\alpha + \beta) \Pi^2.$$

Die Gruppe ist also gleich beschaffen wie die additive Gruppe des $GF(p^f)$, d. h. sie ist *Abel*sch vom Typus $(p, p, \ldots)$ und von der Ordnung p^f. In dieser zuletzt angegebenen Weise geht es für die Reste nach höheren Potenzen von $\mathfrak{p}$ fort. Es ist jedoch zu bemerken, daß die wirklich auftretende Gruppe $\mathfrak{T}$ stets eine *Untergruppe* der vollen Gruppe aller Automorphismen ist.

Die Sätze über die *Automorphismen Abelscher Gruppen* finden ihre Anwendung in folgendem Problem der algebraischen Zahlkörper. Die Idealklassen bilden eine *Abel*sche Gruppe. Ist der Körper *Galois*sch und übt man die Substitutionen der Körpergruppe aus, so erfährt die Gruppe der Idealklassen eine Automorphismengruppe. Man gelangt auf diesem Wege direkt zu der Gruppe des Klassenkörpers. Man vergleiche hierüber die Arbeiten von *Fueter, Furtwängler* und *Takagi*.

Die *Basiseinheiten* eines *Galois*schen Körpers erfahren beim Übergang zu den konjugierten in ihren Exponenten eine *ganzzahlige Substitutionsgruppe*. Hier ist die Frage nach der *vollständigen Reduzierung im Bereich der ganzen rationalen Zahlen von großer Wichtigkeit*.

Betrachtet man schließlich die Körper, die durch die p-ten Wurzeln aus Einheiten oder beliebigen Zahlen und ihren konjugierten entstehen, so wird man auf *ganzzahlige Substitutionsgruppen* (mod p) geführt.

Wir haben hier nur einige charakteristische Beispiele von Anwendungen der Gruppentheorie gegeben, sie mögen einen Begriff geben von dem weiten Forschungsfeld, das hier offen liegt. Etwas ausführlicher wollen wir auf die Anwendungen der Substitutionsgruppen eingehen.

§ 63. Anwendung der Substitutionsgruppen.

Wir gehen aus von einer beliebigen Substitutionsgruppe Γ vom Grade n und von der Ordnung g. Ihre Matrizen seien $E, A, B, \ldots, S, \ldots$. Ferner sei K der Körper aller rationalen Funktionen von $x_1, \ldots, x_n$. Die numerischen Koeffizienten seien auf denjenigen Körper beschränkt, der durch die Koeffizienten der Matrizen von Γ bestimmt ist. R sei der Unterkörper von K, dessen Funktionen ungeändert bleiben, wenn man auf die Variabeln sämtliche Substitutionen von Γ ausübt.

Man zeigt leicht, daß es in K Funktionen gibt, die unter den Substitutionen g verschiedene Werte annehmen. Wiederum gehören die Unterkörper und die Untergruppen zusammen.

Das Problem, aus dem Körper R die Variabeln x_i und damit den Körper K zu bestimmen, heißt nach *F. Klein* das ***Formenproblem von*** Γ. Falls Γ eine Permutationsgruppe ist, so haben wir das *Lagrange*sche Problem vor uns, die allgemeinere Fassung gestattet in allen Fällen, das Problem zu vereinfachen. Wir zeigen das an zwei Beispielen, den Gleichungen 3. und 5. Grades.

Die *symmetrische Gruppe dreier Variabler* läßt sich folgendermaßen als monomiale Gruppe zweiten Grades schreiben:

$$S = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^2 \end{pmatrix} \qquad T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Sie besitzt folgende zwei *Invarianten:*

$$I_1 = x_1 x_2 \qquad I_2 = x_1^3 + x_2^3.$$

Als Auflösung findet man:

$$x_2 = \frac{I_1}{x_1} \quad \text{und} \quad x_1 = \sqrt[3]{\frac{I_2}{2} \pm \sqrt{\frac{I_2^2}{4} - I_1^3}},$$

ein Ausdruck, der gleich gebaut ist wie die *Cardani*sche Formel.

Dieses Formenproblem löst jede Gleichung dritten Grades. Zum Beweis bezeichnen wir die 6 Matrizen E, S, S^2, T, TS, TS^2 in dieser Reihenfolge mit $A_1, \ldots, A_6$ und ordnen gleichzeitig S die Permutation $(\alpha_1 \alpha_2 \alpha_3)$, T die Permutation $(\alpha_2 \alpha_3)$ der Wurzeln unserer Gleichung zu. Die Funktion $f(\alpha_1, \alpha_2, \alpha_3)$ möge durch die Permutationen übergehen in $f = f_1, f_2, \ldots, f_6$. Alsdann bilden wir, wie in § 48, die Matrix

$$A_1 f_1 + \ldots + A_6 f_6 = \mathsf{M}.$$

Übt man auf die α_i eine Permutation aus und setzt man gleichzeitig M rechts mit der entsprechenden Matrix A zusammen, so bleibt M ungeändert, denn die Matrizen A_k und die Funktionen f_k erfahren dadurch dieselbe Permutation. Durch die Permutation der α_i geht M in eine Matrix M_A mit konjugierten Koeffizienten über und wir finden

$$\mathsf{M}_A A = \mathsf{M} \quad \text{oder} \quad \mathsf{M}_A = \mathsf{M} A^{-1}.$$

Daraus folgt, daß die Zeilen von M beim Übergang zu den konjugierten Werten die Substitutionen der adjungierten Gruppe erfahren, d. h. sie sind *Lösungen des zugehörigen Formenproblems*. Wählen wir für f speziell α_1, so erhalten wir die *Cardanische Formel*: Es wird

$$\mathsf{M} = \begin{pmatrix} \alpha_1 + \varepsilon\alpha_2 + \varepsilon^2\alpha_3, & \alpha_1 + \varepsilon^2\alpha_2 + \varepsilon\alpha_3 \\ \alpha_1 + \varepsilon^2\alpha_2 + \varepsilon\alpha_3, & \alpha_1 + \varepsilon\alpha_2 + \varepsilon^2\alpha_3 \end{pmatrix}.$$

Die beiden Funktionen

$$x_1 = \alpha_1 + \varepsilon\alpha_2 + \varepsilon^2\alpha_3 \qquad x_2 = \alpha_1 + \varepsilon^2\alpha_2 + \varepsilon\alpha_3$$

erfahren unter den Permutationen die Substitutionen unserer Gruppe Γ und setzen wir sie in den Invarianten ein, so gehen diese in symmetrische Funktionen von $\alpha_1\alpha_2\alpha_3$ über. So wird:

$$I_1 = x_1 \cdot x_2 = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + (\varepsilon + \varepsilon^2)(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1),$$

wobei $\varepsilon + \varepsilon^2 = -1$ ist. Ähnlich wird

$$I_2 = x_1^3 + x_2^3 = 2(\alpha_1^3 + \alpha_2^3 + \alpha_3^3) - 3(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1 + \alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2) + 12\,\alpha_1\alpha_2\alpha_3.$$

Drückt man diese Formen durch die elementarsymmetrischen Formen der α aus, d. h. durch die Koeffizienten der Gleichung

$$x^3 - a x^2 + b x - c = 0,$$

der die α genügen, so findet man:

$$I_1 = a^2 - 3b, \quad I_2 = 2a^3 - 9ab + 27c.$$

Hieraus erhält man x_1 und x_2 und schließlich findet man:

$$\alpha_1 = a + x_1 + x_2 \qquad \alpha_2 = a + \varepsilon^2 x_1 + \varepsilon x_2 \qquad \alpha_3 = a + \varepsilon x_1 + \varepsilon^2 x_2.$$

Dies ist aber die *Cardani*sche Formel.

Wir gehen nunmehr über zu den Gleichungen vom fünften Grad. Bekanntlich besitzt die symmetrische Gruppe einen Normalteiler vom Index zwei, die alternierende Gruppe, und das Differenzenprodukt ist eine zu dieser gehörige Funktion. So bleibt noch ein Gleichungsproblem vom sechzigsten Grade übrig, und seine Gruppe ist die Ikosaedergruppe, eine einfache Gruppe, die wir eingehend behandelt haben. Insbesondere haben wir eine Darstellung derselben in drei Variabeln gegeben in § 49, und nach der eben angegebenen Methode muß sich die Gleichung durch ein Formenproblem von 3 Dimensionen lösen lassen. Wir geben hier die diesbezüglichen Formeln und be-

merken noch, daß das Problem, das wir behandeln, Gegenstand der „Vorlesungen über das Ikosaeder“ von *F. Klein* ist[1]).

Die Ikosaedergruppe kann durch drei Elemente erzeugt werden. In § 49 haben wir sie mit A, B, und C bezeichnet, wir wollen aber jetzt, um die Bezeichnungen von *Klein* nicht zu verändern, die Buchstaben S, T und U benutzen und S statt A, T statt B, U statt C setzen. Wir nehmen als Darstellung Γ die adjungierte zu derjenigen vom Schluß des § 49. Da T und U die Ordnung 2 haben, so brauchen wir ihre Matrizen nur zu transponieren. So finden wir:

$$S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \varepsilon & 0 \\ 0 & 0 & \varepsilon^4 \end{pmatrix} \qquad T = \begin{pmatrix} \frac{1}{\sqrt{5}} & \frac{1}{\sqrt{5}} & \frac{1}{\sqrt{5}} \\ \frac{2}{\sqrt{5}} & \frac{\varepsilon^2+\varepsilon^3}{\sqrt{5}} & \frac{\varepsilon+\varepsilon^4}{\sqrt{5}} \\ \frac{2}{\sqrt{5}} & \frac{\varepsilon+\varepsilon^4}{\sqrt{5}} & \frac{\varepsilon^2+\varepsilon^3}{\sqrt{5}} \end{pmatrix}$$

$$U = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}.$$

Wenn wir unter f eine beliebige rationale Funktion der 5 Variablen $x_1, \ldots, x_5$ verstehen und die 60 Matrizen der adjungierten Gruppe $\bar{\Gamma}$ mit $\bar{A}_i$ $(i = 1, \ldots, 60)$ bezeichnen, so haben wir auf f die sämtlichen Permutationen der alternierenden Gruppe auszuüben und den Ausdruck zu bilden:

$$\sum f_i \bar{A}_i = \bar{\mathsf{M}}(x_1, \ldots, x_5).$$

Falls $\bar{\mathsf{M}}$ nicht identisch verschwindet, werden ihre Zeilen bei den Permutationen der Variablen die Substitutionen der Gruppe Γ erfahren. Wir wählen nun f in besonders geeigneter Weise, indem wir für sie eine Funktion ω nehmen, die zu der durch S erzeugten zyklischen Gruppe gehört. Zerlegen wir die Ikosaedergruppe nach dieser Untergruppe und ihren Nebengruppen, so können wir als repräsentierende Elemente der letzteren die folgenden 12 wählen:

$$E,\ U,\ T,\ UT,\ TS,\ UTS,\ \ldots,\ TS^4,\ UTS^4.$$

Für $\bar{\Gamma}$ ist:

$$\bar{S} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \varepsilon^4 & 0 \\ 0 & 0 & \varepsilon \end{pmatrix}, \quad \begin{array}{l} \bar{T} = \text{transponierte Substitution zu } T \\ \bar{U} = U. \end{array}$$

Nun haben wir zu bilden: $\sum_{i=1}^{60} \omega_i \bar{A}_i$. Summieren wir erst über

[1]) Vgl. ferner: *Speiser, A.*: Gruppendeterminante und Körperdiskriminante. Math. Ann. 77, S. 546.

die fünf Matrizen der zyklischen Untergruppe, so ändert sich ω nicht, und wir erhalten:

$$\sum_{1}^{5} \bar{S}^i = \begin{pmatrix} 5 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \bar{H}.$$

Nun üben wir die Substitution U aus, wobei ω in ω' übergehen möge.

Summieren wir wieder über die 5 Elemente $\bar{S}^i \bar{U}$, wobei ω immer in dieselbe Funktion ω' übergeht, so finden wir

$$\bar{H}\,\bar{U} = \begin{pmatrix} -5 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Indem wir in dieser Weise fortfahren, erhalten wir:

$$\bar{H}\,\bar{T} = \begin{pmatrix} \sqrt{5}, & 2\sqrt{5}, & 2\sqrt{5} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\bar{H}\,\bar{T}\,\bar{S}^i = \begin{pmatrix} \sqrt{5} & 2\varepsilon^i\sqrt{5} & 2\varepsilon^{4i}\sqrt{5} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Die mit ω konjugierten Funktionen bezeichnen wir in der angegebenen Reihenfolge mit $\omega, \omega', \ldots, \omega^{(11)}$ und setzen nun:

$$\omega - \omega' = u_\infty \qquad \omega'' - \omega''' = u_0, \qquad \omega^{(4)} - \omega^{(5)} = u_4, \ldots,$$
$$\omega^{(10)} - \omega^{(11)} = u_1,$$

indem wir die Bezeichnung von *Klein* (l. c. S. 154) benutzen. Man findet, daß nur die erste Zeile von 0 verschieden ist, und zwar lautet sie:

$$\begin{aligned} &5u_\infty + \sqrt{5}(u_0 + u_1 + u_2 + u_3 + u_4) \\ &2\sqrt{5}(u_0 + \varepsilon^4 u_1 + \varepsilon^3 u_2 + \varepsilon^2 u_3 + \varepsilon u_4) \\ &2\sqrt{5}(u_0 + \varepsilon u_1 + \varepsilon^2 u_2 + \varepsilon^3 u_3 + \varepsilon^4 u_4). \end{aligned}$$

Diese 3 Funktionen von $x_1, \ldots, x_5$, erfahren also bei den Vertauschungen der alternierenden Gruppe die ternären Ikosaedersubstitutionen. Indem wir sie noch durch 5 dividieren, bezeichnen wir sie mit $\mathsf{A}_0, \mathsf{A}_1, \mathsf{A}_2$ und erhalten:

$$\begin{aligned} \mathsf{A}_0 \cdot \sqrt{5} &= u_\infty \sqrt{5} + u_0 + u_1 + u_2 + u_3 + u_4 \\ \mathsf{A}_1 \sqrt{5} &= \quad 2(u_0 + \varepsilon^4 u_1 + \varepsilon^3 u_2 + \varepsilon^2 u_3 + \varepsilon u_4) \\ \mathsf{A}_2 \sqrt{5} &= \quad 2(u_0 + \varepsilon u_1 + \varepsilon^2 u_2 + \varepsilon^3 u_3 + \varepsilon^4 u_4). \end{aligned}$$

Hiermit sind wir jedoch noch nicht zu Ende, sondern wir können eine weitere Tatsache benutzen, nämlich, daß sich die Ikosaedergruppe

auch als lineare gebrochene Substitutionsgruppe einer Variablen darstellen läßt. Projiziert man die Ikosaederdrehungen stereographisch auf die komplexe Zahlenebene, so erhält man sie. Eine leichte Überlegung, die man bei *Klein* (l. c. S. 39) nachlesen kann, gestattet, sie herzustellen. Wir schreiben sie gleich in homogener Form auf, indem wir $z = \frac{x}{y}$ setzen und die Determinanten so normieren, daß sie alle $= 1$ werden. Hierdurch sind die Matrizen bis auf das Vorzeichen bestimmt:

$$S = \begin{pmatrix} \pm\varepsilon^3 & 0 \\ 0 & \pm\varepsilon^2 \end{pmatrix} \qquad T = \begin{pmatrix} \mp\frac{\varepsilon-\varepsilon^4}{\sqrt{5}} & \pm\frac{\varepsilon^2-\varepsilon^3}{\sqrt{5}} \\ \pm\frac{\varepsilon^2-\varepsilon^3}{\sqrt{5}} & \pm\frac{\varepsilon-\varepsilon^4}{\sqrt{5}} \end{pmatrix}$$

$$U = \begin{pmatrix} 0 & \mp 1 \\ \pm 1 & 0 \end{pmatrix}.$$

Die 120 Substitutionen bilden eine Gruppe, welche einen Normalteiler von der Ordnung 2 enthält, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ und $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. Seine Fakorgruppe ist die Ikosaedergruppe.

Diese 120 Substitutionen übe man nun aus auf die Variabeln x und y der quadratischen Form

$$ax^2 + bxy + cy^2.$$

Bezeichnet man eine der so entstehenden Formen mit

$$a'x^2 + b'xy + c'y^2,$$

so sind die neuen Koeffizienten lineare Formen der alten, d. h. die Koeffizienten a, b und c erfahren eine ternäre Substitution, die (nach einer von *Hurwitz* eingeführten Bezeichnungsweise) ***induziert*** ist durch die Substitution auf die Variabeln. Die induzierte Substitutionsgruppe ist nur noch von der Ordnung 60 und mit der Ikosaedergruppe homomorph, sie muß also mit Γ oder $\bar{\Gamma}$ äquivalent sein. Eine elementare Rechnung zeigt, daß, wenn man die binäre Form in der Gestalt annimmt

$$A_1x^2 + 2A_0xy - A_2y^2 = f(x, y)$$

und die transformierte entsprechend mit

$$A_1'x^2 + 2A_0'xy - A_2'y^2 = f'(xy)$$

bezeichnet, die drei Koeffizienten A_0, A_1, A_2 gerade die Substitutionen Γ erfahren.

Folgende drei Operationen erzeugen also aus der Form

$$A_1x^2 + 2A_0xy - A_2y^2$$

dieselben 60 Formen:

1. Man übt auf die Variabeln x und y die 120 binären Substitutionen aus.

2. Man übt auf die Koeffizienten A_0, A_1, A_2, die 60 Substitutionen von Γ aus.

3. Man ersetzt die Formen, die ja im Ikosaederkörper liegen, durch die konjugierten.

Jetzt setzen wir die Form $f(x, y)$ gleich Null und erhalten:

$$\frac{x}{y} = \frac{-A_0 \pm \sqrt{A_0^2 + A_1 A_2}}{A_1} = \alpha .$$

Der Ausdruck unter dem Wurzelzeichen:

$$A_0^2 + A_1 A_2 = d$$

stellt die Determinante der Form dar und bleibt daher für alle 60 Formen derselbe, d. h. d liegt im Grundkörper. Seine Quadratwurzel ist eine akzessorische Irrationalität, die mit dem Ikosaederkörper nichts zu tun hat, deren Adjunktion zum Grundkörper wir aber nicht vermeiden können.

Die Wurzeln der übrigen Formen sind nun identisch mit den zu α konjugierten Größen. Wegen 1. erhält man sie jedoch, indem man in der Gleichung

$$\frac{x}{y} = \alpha$$

auf die linke Seite die gebrochenen linearen Substitutionen anwendet und nach $\frac{x}{y}$ auflöst, also mit andern Worten: indem man auf α die inversen gebrochenen linearen Ikosaedersubstitutionen ausführt. Diese gehören aber zur selben Gruppe, und wir haben daher in α eine Größe des Ikosaederkörpers, welche beim Übergang zu den konjugierten eben diese gebrochene Substitutionsgruppe erfährt. Setzt man sie in der zugehörigen Invariante (Klein l. c. § 13)

$$Z = \frac{[-z^{20} - 1 + 228\,(z^{15} - z^5) - 494\,z^{10}]^3}{1728\,[z(z^{10} + 11\,z^5 - 1)]^5} = F(z)$$

ein, so erhält man für Z eine Größe des Grundkörpers. Man erhält also durch Auflösung der Gleichung

$$f(z) = Z$$

jeden Ikosaederkörper und wir können in jedem solchen Körper von vornherein eine Zahl α angeben, welche dieser Gleichung im Grundkörper genügt, wobei wir stets voraussetzen, daß $\sqrt{d}$ mit zum Grundkörper gerechnet wird.

Schluß.

Es sei uns gestattet, zum Schluß noch auf ein Problem hinzuweisen, das uns für die Gruppentheorie von ganz besonderer Wichtigkeit zu sein scheint, wir meinen die Zahlentheorie der hyperkomplexen Zahlen. Absichtlich haben wir mehrere Überlegungen von § 48 an mit Methoden geführt, die dorther stammen, und der Grund wird sofort klar, wenn man sich etwa überlegt, wie unleserlich in gewöhnlicher Darstellung z. B. die Formeln des Satzes 122 geworden wären. Dem analog wäre es, wenn jemand die algebraische Zahlentheorie in die Sprache der zerlegbaren Formen zurückübersetzen wollte.

Gehen wir zum § 48 zurück, so handelt es sich für uns nur um solche Fälle, in denen die Koeffizienten der Elemente algebraische Zahlen sind und wir schlagen vor, in diesem Falle das abschreckende Wort „hyperkomplexe Zahlen" zu ersetzen durch die Bezeichnung ***Gruppenzahlen.*** Wir zeigen nun, daß das schwierige und tiefliegende Problem der Gitter in n Dimensionen, wie es in den §§ 54 und 55 behandelt wurde, im wesentlichen herauskommt auf eine Theorie der rechts- und linksseitigen Ideale in dem Gruppenkörper, welcher durch die Gruppe der Gittersymmetrien gegeben ist, wobei als Koeffizienten nur rationale Zahlen zugelassen werden.

Das Gelenk, welches die Theorie der Substitutionen mit der eben beschriebenen Zahlentheorie verbindet, ist Satz 120 und 121, womit ferner zu vergleichen ist Satz 68 und 94. Bezeichnet man Gruppenzahlen mit ganzen rationalen Koeffizienten als ***ganze Zahlen,*** so liefern die Zeilen einer ganzzahligen Substitutionsgruppe nach Satz 120 Systeme von n ganzen Gruppenzahlen, welche bei rechtsseitiger Multiplikation mit den Gruppenelementen eine ganzzahlige Substitution erfahren. Der durch eine Zeile erzeugte Modul mit ganzzahligen Koeffizienten a_k:

$$a_1 \zeta_{i1} + a_2 \zeta_{i2} + \ldots + a_n \zeta_{in}$$

bildet daher ein rechtsseitiges Ideal. Ganzzahlig äquivalente Substitutionsgruppen derselben Klasse (vgl. den für diese Theorie grundlegenden Satz 146 auf Seite 151) ergeben dasselbe Ideal.

Satz 141 besagt nun, daß jeder Gruppenkörper „Summe" von rational irreduziblen Gruppenkörpern ist, die keine Zahl gemeinsam haben, und aus Satz 122 folgt sogar, daß das Produkt von zwei Zahlen aus verschiedenen Bestandteilen verschwindet. Jeder der rational irreduzibeln Bestandteile muß für sich betrachtet werden, damit eine klare Zahlentheorie entstehen kann. Es ist dies die genaue Verallgemeinerung der Tatsache, daß der Körper der p-ten Einheitswurzeln bloß den Grad $p - 1$ hat.

Die Struktur dieser rational irreduziblen Gruppenkörper wird nun durch Satz 141 vollständig aufgeklärt. Auch ist ersichtlich, daß rechtsseitige Ideale im allgemeinen weniger Basiszahlen haben als der Körper, daß dagegen zweiseitige Ideale stets gleichviel Basiszahlen benötigen wie der Körper. Ideale, die aus einer Zeile einer rational irreduziblen Gruppe gebildet sind, mögen ***irreduzible rechtsseitige Ideale*** heißen. Geht man nun von einer äquivalenten ganzzahligen Gruppe einer andern Klasse aus, so erhält man ein neues Ideal, und zu jedem rechtsseitigen irreduziblen Ideal gehört eine ganzzahlige Darstellung der Gruppe. Die linksseitigen Ideale gehören zur adjungierten Gruppe.

Am einfachsten zu verfolgen sind die Verhältnisse bei den zyklischen Gruppen. So sind z. B. die Sätze, daß es in der Ebene nur je ein Gitter gibt, das Drehungen von der Ordnung 4 bzw. 6 gestattet, identisch mit der Tatsache, daß die Körper der 4. bzw. der 6. Einheitswurzeln die Klassenanzahl 1 haben. Es stehen also in der Tat „wesentliche Eigenschaften der Materie mit der Zerlegung der Primzahlen in zwei Quadrate im Zusammenhang“ (*Minkowski*, Gedächtnisrede auf *Dirichlet*).

Im vierdimensionalen euklidischen Raum gibt es eine zyklische Symmetrie von der Ordnung 10 und zu ihr gehört genau ein Gitter, denn die Klassenanzahl des Körpers der 5 Einheitswurzeln ist 1. Dieses Gitter hat 2 Freiheitsgrade.

Auch ein nicht *Abel*scher Gruppenkörper hat bereits seine Bearbeitung gefunden, nämlich der Quaternionenkörper in den glänzenden Vorlesungen über die Zahlentheorie der Quaternionen von *A. Hurwitz* (Berlin 1919). Hier läßt sich die Zerlegung der Zahlen auf einfache Gesetze bringen. Der betreffende Körper ist rational irreduzibel und vom Grade 4. Die irreduziblen Ideale benötigen ebenfalls 4 Basiszahlen, denn die Substitutionsgruppe vom Grade 4 zerfällt erst nach Adjunktion von i in ihre irreduziblen Bestandteile vom Grade 2.

Die durch Satz 141 aufgedeckte Struktur der irreduziblen Gruppenkörper und ihrer Ideale ist Prototyp für die entsprechende Theorie bei den allgemeinen hyperkomplexen Zahlen mit Haupteinheit und rationalen Zahlenkoeffizienten, die Gruppentheorie spielt ihnen gegenüber die gleiche Rolle, wie die Theorie der Kreiskörper gegenüber der allgemeinen algebraischen Zahlentheorie.

Hier endigt die selbständige Stellung der Gruppentheorie. Sie mündet in die allgemeine Zahlentheorie, indem sie dieser wertvolle neue Erkenntnis zuführt.

Namenverzeichnis.

Die Zahlen geben die Seiten an.

Sachverzeichnis.

Die Zahlen geben die Seiten an.

DIE GRUNDLEHREN DER MATHEMATISCHEN WISSENSCHAFTEN

IN EINZELDARSTELLUNGEN

MIT BESONDERER BERÜCKSICHTIGUNG DER ANWENDUNGSGEBIETE

Gemeinsam mit

W. Blaschke, Hamburg, **M. Born**, Göttingen
C. Runge, Göttingen

herausgegeben von

R. Courant
Göttingen

Band I:

Vorlesungen über Differential-Geometrie und geometrische Grundlagen von Einsteins Relativitätstheorie. I. Elementare Differential-Geometrie. Von **Wilhelm Blaschke**, ord. Professor der Mathematik an der Universität Hamburg. Mit 38 Textfiguren. 1921. GZ. 7,5; gebunden GZ. 10

Band II:

Theorie und Anwendung der unendlichen Reihen. Von Dr. **Konrad Knopp**, ord. Professor der Mathematik an der Universität Königsberg. Mit 12 Textfiguren. 1922. GZ. 15; gebunden GZ. 18

Band III:

Vorlesungen über allgemeine Funktionentheorie und elliptische Funktionen. Von **Adolf Hurwitz** †, weil. ord. Professor der Mathematik am Eidgenössischen Polytechnikum Zürich. Herausgegeben und ergänzt durch einen Abschnitt über:

Geometrische Funktionentheorie von **R. Courant**, ord. Professor der Mathematik an der Universität Göttingen. Mit 122 Textfiguren. 1922. GZ. 13; gebunden GZ. 16

Band IV:

Die mathematischen Hilfsmittel des Physikers. Von Dr. **E. Madelung**, ord. Professor der theoretischen Physik an der Universität Frankfurt a. M. Mit 20 Textfiguren. 1922. GZ. 8,25; gebunden GZ. 10

Die Grundzahlen (GZ.) entsprechen den ungefähren Vorkriegspreisen und ergeben mit dem jeweiligen Entwertungsfaktor (Umrechnungsschlüssel) vervielfacht den Verkaufspreis. Über den zur Zeit geltenden Umrechnungsschlüssel geben alle Buchhandlungen sowie der Verlag bereitwilligst Auskunft.

Felix Klein, Gesammelte mathematische Abhandlungen.
In drei Bänden mit einem Registerband.
Band I: **Liniengeometrie — Grundlegung der Geometrie — Zum Erlanger Programm.** Herausgegeben von **R. Fricke** und **A. Ostrowski** (von F. Klein mit ergänzenden Zusätzen versehen). Mit einem Bildnis. 1921. GZ. 18
Band II: **Anschauliche Geometrie — Substitutions-Gruppen und Gleichungstheorie — Zur mathematischen Physik.** Herausgegeben von **R. Fricke** und **H. Vermeil** (von F. Klein mit ergänzenden Zusätzen versehen). Mit 185 Textfiguren. 1922. GZ. 18
Band III: **Funktionentheorie** (elliptische Funktionen, insbes. Modulfunktionen, hyperelliptische und Abelsche Funktionen, allgemeine Riemannsche Funktionentheorie und automorphe Funktionen.) Herausgegeben von **R. Fricke, H. Vermeil** und **E. Bessel-Hagen.** Mit etwa 140 Textfiguren. Erscheint im Frühjahr 1923.

Theorie der reellen Funktionen. Von Dr. **Hans Hahn,** Professor der Mathematik an der Universität Bonn. In zwei Bänden. Erster Band: Mit 18 Textfiguren. 1921. GZ. 22

Darstellung und Begründung einiger neuerer Ergebnisse der Funktionentheorie. Von Dr. **Edmund Landau**, o. ö. Professor der Mathematik an der Universität Göttingen. Mit 11 Textfiguren. 1916. GZ. 4,8

Formeln und Lehrsätze zum Gebrauche der elliptischen Funktionen. Nach Vorlesungen und Aufzeichnungen des Herrn K. Weierstraß bearbeitet und herausgegeben von **H. A. Schwarz**, Professor an der Universität Göttingen. Zweite Ausgabe. 1893. GZ. 10

Allgemeine Untersuchungen über die unendliche Reihe $1+\frac{\alpha\beta}{1\cdot\gamma}x+$ usw. Von **Carl Friedrich Gauß.** Mit Einschluß der nachgelassenen Fortsetzung aus dem Lateinischen übersetzt von Dr. Heinrich Simon. 1888. GZ. 3

Untersuchungen über höhere Arithmetik. (Disquisitiones arithmeticae. Theorematis arithmetici demonstratio nova. Summatio quarundam serierum singularium. Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et ampliationes novae. Theoria residuorum biquadraticorum, commentatio prima et secunda. Etc.) Von **Carl Friedrich Gauß.** Deutsch herausgegeben von H. Maser. 1889.
GZ. 14; gebunden GZ. 15,4

Grundzüge der mehrdimensionalen Differential-Geometrie in direkter Darstellung. Von **D. J. Struik**, Rotterdam. Mit 4 Textfiguren. 1922. GZ. 12

Die Grundzahlen (GZ.) entsprechen den ungefähren Vorkriegspreisen und ergeben mit dem jeweiligen Entwertungsfaktor (Umrechnungsschlüssel) vervielfacht den Verkaufspreis. Über den zur Zeit geltenden Umrechnungsschlüssel geben alle Buchhandlungen sowie der Verlag bereitwilligst Auskunft.