Werk

Titel: Distributive Gruppen von endlicher Ordnung.

Autor: Burstin, C.; Mayer, W.

Jahr: 1929

PURL: https://resolver.sub.uni-goettingen.de/purl?243919689_0160|log12

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

Distributive Gruppen von endlicher Ordnung.

Von *C. Burstin* in Wien und *W. Mayer* in Wien.

§ 1. Die Axiomatik distributiver Gruppen.

Es sei ein System von endlich oder unendlich vielen Elementen gegeben:

$$a, b, c, \ldots$$

und eine Verknüpfung, die je zwei Elementen a, b in der bestimmten Reihenfolge a, b ein Element $a \,.\, b$, das Verknüpfungsresultat von a und b zuordnet. Sind dann die folgenden drei Axiome erfüllt, so wollen wir ein solches System eine *distributive Gruppe* nennen.

I. Axiom: Das Verknüpfungsresultat $a \,.\, b$ irgend zweier Elemente a und b des Systems ist ein Element des Systems.

II. Axiom: Seien a und b irgend zwei Elemente des Systems, so haben die beiden Gleichungen

$$a \,.\, x = b \quad \text{resp.} \quad y \,.\, a = b$$

im System je eine und nur eine Lösung.

(Dieses Axiom verlangt somit die Existenz und die Eindeutigkeit der inversen Operationen.)

III. Axiom: Seien a, b und c irgend drei Elemente des Systems, so bestehen identisch die beiden Relationen

$$(a \,.\, b) \,.\, c = (a \,.\, c) \,.\, (b \,.\, c), \qquad c \,.\, (a \,.\, b) = (c \,.\, a) \,.\, (c \,.\, b)$$

Die Axiome I und II sind Axiome der klassischen Gruppentheorie, an Stelle des dritten Axioms tritt dort das Axiom der assoziativen Verknüpfung: $(a \,.\, b) \,.\, c = a \,.\, (b \,.\, c)$, wir werden daher die Gruppen der klassischen Theorie zur Unterscheidung von den distributiven Gruppen *assoziative* Gruppen nennen.

Liegt ein Axiomensystem vor, so sind vor allem die Fragen nach der Unabhängigkeit und nach der Widerspruchslosigkeit der Axiome zu beantworten.

Wir zeigen an einem Beispiele die Unabhängigkeit des Axioms I von den Axiomen II und III:

Das System der Elemente seien die (positiven und negativen) *ganzen* Zahlen; für die Verknüpfung gelte $a \,.\, b = \dfrac{a + b}{2}$. Hier sind Axiom II und III erfüllt, dagegen nicht Axiom I.

Im Systeme *von endlich vielen* Elementen ist Axiom I eine Folge des Axiomes II.

Ein zweites Beispiel erweise die Unabhängigkeit des Axiomes II von den Axiomen I und III.

Das System enthalte n Elemente $a_1, a_2, \ldots, a_n$, für die Verknüpfung gelte

$$a_i \,.\, a_k = a_k \,.$$

Hier sind Axiom I und III erfüllt, dagegen II nicht.

Jede assoziative Gruppe, die mehr als ein Element enthält, ist ein Beispiel für die Unabhängigkeit des Axioms III von den Axiomen I und II. Wir werden nämlich zeigen, daß eine solche assoziative Gruppe nicht distributiv sein kann.

Die Widerspruchslosigkeit der Axiome I, II und III beweist man durch Aufstellung distributiver Gruppen.

1. *Beispiel*: Das System der Elemente seien die komplexen Zahlen. Die Verknüpfung $a \,.\, b$ ordne den Zahlen a und b die Zahl

$$a \,.\, b = \alpha a + \beta b$$

zu, wobei α und β festgewählte Zahlen sind, deren Summe $\alpha + \beta = 1$ ist.

2. *Beispiel*: Das System der Elemente seien die reellen positiven Zahlen, die Null ausgeschlossen, die Verknüpfung $a \,.\, b$ ordne den Zahlen a und b die Zahl $a \,.\, b = \sqrt{ab}$ (das geometrische Mittel) zu, oder allgemeiner $a^\alpha b^\beta$ mit $\alpha + \beta = 1$, α und β von Null verschiedene reelle Zahlen. Dabei ist $a^\alpha = e^{\alpha \ln a}$.

3. *Beispiel*: Das System der Elemente seien die Punkte des n-dimensionalen affinen Raumes. Die Verknüpfung $a \,.\, b$ ordne den Punkten a und b einen Punkt der Strecke $\overline{ab}$ zu, der diese Strecke nach einem gegebenen Verhältnisse $\alpha : \beta$ teilt (z. B. den Mittelpunkt der Strecke $\overline{ab}$).

4. *Beispiel*: Das System der Elemente seien die Punkte des n-dimensionalen projektiven Raumes mit Ausnahme der Punkte einer $(n-1)$-dimensionalen Hyperebene E_{n-1} dieses Raumes [1]).

Der Punkt $a \,.\, b$ liege dann auf der Geraden ab so, daß das Doppelverhältnis $(a, b, a \,.\, b, c)$, wobei c der Schnittpunkt der Geraden ab mit der E_{n-1} ist, einen bestimmten festen Wert $\varkappa$ hat.

Führt man projektive Koordinaten ein, und seien $a_1, \ldots, a_{n+1}; b_1, \ldots, b_{n+1}$ die Koordinaten der Punkte a und b, $A_i x_i = 0$, $i = 1, \ldots, n+1$ die Gleichung der E_{n-1}, so hat der Punkt $a \,.\, b = d$ die projektiven Koordinaten

$$d_i = A_t (a_i b_t - \varkappa b_i a_t), \qquad i, t = 1, \ldots, n+1.$$

Aus dieser Formel ist der Gruppennachweis einfach zu erbringen, wir werden im § 2 eine sehr einfache Methode, diesen Nachweis zu führen, geben.

Bevor wir daran gehen, Beispiele endlicher distributiver Gruppen zu geben, das sind Gruppen, die nur endlich viele Elemente enthalten, sei eine charakteristische Eigenschaft distributiver Gruppen besprochen. In einer assoziativen Gruppe ist bekanntlich ein Element, das Einheitselement ausgezeichnet, für dieses — es sei mit e bezeichnet — gilt

$$a \,.\, e = e \,.\, a = a$$

für jedes Element a der assoziativen Gruppe. In einer distributiven Gruppe dagegen gibt es keine ausgezeichneten Elemente, in einer solchen herrscht vielmehr *eine Homogenität* der Art, daß eine gruppentheoretische Eigenschaft, die einem Elemente einer solchen Gruppe zukommt, jedem Elemente dieser Gruppe zukommen muß (§ 2).

Wir wollen zeigen, daß eine distributive Gruppe, die mehr als ein Element enthält, kein Einheitselement enthalten kann. Setzen wir in eine der beiden Relationen des Axioms III $b = c = a$, wobei a ein beliebiges Element der Gruppe sei, so folgt aus $(a \,.\, a) \,.\, a = (a \,.\, a) \,.\, (a \,.\, a)$ wegen des zweiten Axiomes die wichtige Relation

$$a \,.\, a = a,$$

die also für jedes Element einer distributiven Gruppe zu gelten hat. Wäre nun in der Gruppe ein Einheitselement e vorhanden, so hätte $a \,.\, e = a \,.\, a$, $e = a$ zur Folge, d. h. jedes Element dieser Gruppe wäre das Einheitselement, diese Gruppe könnte also nur dieses Element enthalten, q. e. d.

---

[1]) *Dual*: Das System der Elemente seien die E_{n-1} eines projektiven R_n mit Ausnahme der E_{n-1}, die durch einen bestimmten Punkt des R_n gehen.

Die Gruppe, die nur ein Element a enthält, für das nach Axiom I $a \,.\, a = a$ zu gelten hat, ist das einzige Beispiel einer Gruppe, die zugleich assoziativ und distributiv ist.

(Eine solche Gruppe kann nur ein Element enthalten, sonst könnte sie als distributive Gruppe das Einheitselement nicht enthalten, dagegen als assoziative müßte sie es enthalten.)

Eine distributive Gruppe, die nur zwei Elemente enthält, gibt es nicht. Seien a und b diese zwei Elemente, so folgt aus $a \,.\, a = a$, $b \,.\, b = b$, daß $a \,.\, b$ weder a noch b sein kann, daß also Axiom I nicht erfüllbar ist.

Dagegen gibt es eine distributive Gruppe von drei Elementen, — sie ist kommutativ.

Seien a, b, c die Elemente dieser Gruppe, so gilt $a \,.\, a = a$, $b \,.\, b = b$, $c \,.\, c = c$. $a \,.\, b$ kann weder a noch b, muß also gleich c sein. Ebenso ist $b \,.\, a = c$. Das *Cayley*schema der Gruppe ist:

	a	b	c
a	a	c	b
b	c	b	a
c	b	a	c

Anschließend zeigen wir, daß jede endliche kommutative distributive Gruppe von ungerader Ordnung ist.

Sei $G\{a_1, a_2, \ldots, a_n\}$ eine kommutative distributive Gruppe der Ordnung n. Wir heben ein beliebiges Element, z. B. a_1, heraus und fassen das Restsystem $a_2, a_3, \ldots, a_n$ ins Auge.

Sei a_i ein Element dieses Restsystems, so gibt es in G ein „zugeordnetes" Element $a_{\sigma i}$ für das

$$a_i \,.\, a_{\sigma i} = a_1 \quad \text{ist.}$$

Da $a_i \neq a_1$ ist, so ist $a_{\sigma i}$ von a_1 und a_i verschieden. Das a_i zugeordnete Element ist demnach ein von a_i verschiedenes Element des Restsystemes. Dem Element $a_{\sigma i}$ ist — wegen der Kommutativität der Gruppe — wieder das Element a_i zugeordnet. Die Elemente des Restsystemes $a_2, \ldots, a_n$ sind somit in zugeordnete Elemente gepaart, ihre Anzahl ist daher gerade. Die Ordnung der kommutativen Gruppe selbst ist ungerade, q. e. d.

Dagegen gibt es zu jeder ungeraden Zahl $N = 2n + 1$ eine kommutative Gruppe dieser Ordnung.

Mit $1, 2, 3, \ldots, 2n + 1$ bezeichnen wir die Elemente dieser Gruppe, die Verknüpfung $a \,.\, b$ ordne den Elementen a und b das Element zu, das der Gleichung

$$a \,.\, b \equiv (n + 1)(a + b) \mod (2n + 1)$$

genügt. Man überzeugt sich leicht, daß eine kommutative Gruppe vorliegt.

Man kann diese kommutative Gruppe $(2n + 1)$-ter Ordnung anschaulich deuten, sobald man sie isomorph auf die Endpunkte des regulären $(2n + 1)$-Ecks abbildet. Das Verknüpfungselement $c = a \,.\, b$ liegt dann stets auf der Streckensymmetralen der Eckpunkte a und b.

Beweis: Da $a(n + 1) \equiv \frac{a}{2} \mod (2n + 1)$ ist, können wir die Verknüpfungsvorschrift in der Form

$$a \,.\, b \equiv \frac{a + b}{2} \mod (2n + 1)$$

ansetzen. Sei nun $a < b$, so sei:

1. $\quad b = a + 2d, \quad c \equiv \frac{2a + 2d}{2} \equiv a + d \mod (2n + 1),$

also $c = a + d, \quad b = c + d.$

2. $b = a + 2d + 1, \quad c \equiv \dfrac{a + b + 2n + 1}{2} \equiv a + d + n + 1 \equiv b + (n - d) \mod (2n + 1),$

also $c = b + (n - d), \quad c + (n - d) = b + 2(n - d) = a + 2n + 1 \equiv a,$ q. e. d.

Wenn es auch kommutative Gruppen gerader Ordnung nicht gibt, so gibt es doch nicht kommutative; die *Gruppe vierter Ordnung* sei ein Beispiel. Wenn wir mit a_1, a_2, a_3, a_4 die Elemente bezeichnen, so können wir stets $a_1 . a_2 = a_3$ ansetzen ($a_1 . a_2$ kann nur a_3 oder a_4 sein, wir können durch event. Umnumerierung stets $a_1 . a_2 = a_3$ erreichen).

Im *Cayley*schema sind somit folgende Verknüpfungen bekannt:

	a_1	a_2	a_3	a_4
a_1	a_1	a_3	.	.
a_2		a_2		
a_3			a_3	
a_4				a_4

In der ersten Zeile sind an die beiden freien Stellen a_2 und a_4 zu setzen, a_4 kann an letzter Stelle wegen $a_4 . a_4 = a_4$ nicht stehen, somit muß $a_1 . a_3 = a_4$ und $a_1 . a_4 = a_2$ sein. Mit Hilfe des Axiomes II ist man aber dann schon in der Lage die übrigen freien Stellen des Schemas auszufüllen und erhält:

	a_1	a_2	a_3	a_4
a_1	a_1	a_3	a_4	a_2
a_2	a_4	a_2	a_1	a_3
a_3	a_2	a_4	a_3	a_1
a_4	a_3	a_1	a_2	a_4

An der Hand des Schemas beweist man nun leicht die Gültigkeit des Axioms III. Es gibt also eine und nur eine distributive Gruppe der Ordnung vier.

Gruppen der Ordnung fünf gibt es, eine — die kommutative — haben wir eben aufgestellt, eine Gruppe der Ordnung sechs gibt es wieder nicht. Die Aufgabe alle Gruppen einer bestimmten Ordnung aufzustellen, scheint ebenso kompliziert zu sein wie die entsprechende bei den assoziativen Gruppen.

Im § 3 geben wir weitere Beispiele.

§ 2. Die Homogenität distributiver Gruppen.

Sei G eine distributive Gruppe und A

$$A\{a_1, a_2, \ldots\}$$

eine Untergruppe von G. (Sie muß nicht abzählbar sein, nur der einfacheren Schreibweise wegen haben wir die Elemente numeriert.)

Sei dann p irgendein Element von G, so ist

$$B = A . p, \quad \text{das ist der Inbegriff} \quad \{b_1 = a_1 . p, b_2 = a_2 . p, \ldots\},$$

eine zur Gruppe A isomorphe Untergruppe von G.

Dabei nennen wir — in der Bezeichnungsweise der klassischen Gruppentheorie — zwei Gruppen $\{a_1, a_2, \ldots\}$ und $\{b_1, b_2, \ldots\}$ einstufig isomorph, sobald eine ein-eindeutige Zuordnung ihrer Elemente $a_i \rightleftarrows b_i$ der Art hergestellt werden kann, daß dem Verknüpfungsresultat $a_i . a_k$ von a_i und a_k das Verknüpfungsresultat $b_i . b_k$ der a_i und a_k zugeordneten Elemente b_i und b_k zugeordnet ist.

Beweis: Ist A eine Gruppe endlicher Ordnung, so folgt aus $a_i . a_k = a_l$ durch rechts-

seitige Verknüpfung mit $p : b_i \,.\, b_k = b_l$. Das *Cayley*schema *des Systemes* $\{b_1, b_2, \ldots\}$ entspricht somit dem *Cayley*schema *der Gruppe* $\{a_1, a_2, \ldots\}$ und fällt mit diesem zusammen, sobald man den Buchstaben b durch den Buchstaben a ersetzt. Damit ist aber bewiesen, daß B eine zu A isomorphe Untergruppe von G ist.

Für nicht endliche Gruppen gilt der Beweis ebenfalls durch sinngemäße Übertragung des Begriffes des *Cayley*schemas auf solche Gruppen.

Für $A \equiv G$ lautet das Resultat: *Ist p irgend ein Element von G, so ist durch die Zuordnung $a_i \leftrightarrows a_i \,.\, p$ die Gruppe G auf sich selbst isomorph bezogen.*

Wir können p nach Axiom II stets so wählen, daß (a_i, a_k fest gewählte Elemente) $a_i \,.\, p = a_k$ ist, daraus folgt:

Eine distributive Gruppe läßt sich einstufig isomorph auf sich so beziehen, daß einem Elemente a_i das beliebige Element a_k zugeordnet ist.

Daraus folgt die „Homogenität" distributiver Gruppen.

Es gibt keine gruppentheoretische Eigenschaft, die einem Elemente einer distributiven Gruppe zukäme, ohne für alle Elemente dieser Gruppe zu gelten.

1. *Folgerung*: Kommt ein Element a_i in h verschiedenen (und in nicht mehr als h verschiedenen) ν-gliedrigen Untergruppen (d. h. Untergruppen der Ordnung ν) einer Gruppe G vor, so trifft dies für jedes Element der Gruppe zu.

Enthalte demnach G, eine endliche Gruppe der Ordnung N, n solche ν-gliedrige Untergruppen

$$A_1, A_2, \ldots, A_n$$

so ist in dieser Gesamtheit jedes Element von G in derselben Anzahl h vorhanden. Somit gilt $Nh = n\nu$.

2. *Folgerung*: Sei wieder A_1 eine ν-gliedrige Untergruppe von G (Gruppe N-ter Ordnung) und

$$A_2, A_3, \ldots, A_m$$

die Gesamtheit der zu A_1 isomorphen Untergruppen von G. Infolge der Definition isomorpher Gruppen sind damit je zwei Gruppen des Systems

$$(\alpha) \qquad A_1, A_2, \ldots, A_m$$

isomorph. *$A_i \,.\, p$ ist zu A_i also zu jeder der Gruppen dieses Systemes isomorph, also selbst eine Gruppe des Systemes.*

Kommt also ein Element a_i in q Gruppen (α) vor, so trifft dies für jedes Element von G zu.

Zählen wir somit alle Elemente von G, die in den Gruppen (α) enthalten sind ab, so erhalten wir

$$Nq = m\nu.$$

Wir diskutieren den interessanten Fall $q = 1$, für den die Gruppe G durch die Gruppen des Systemes (α) sich darstellen läßt

$$G = A_1 + A_2 + \cdots + A_m \,.$$

Bezeichnen wir mit A irgend eine der Untergruppen $A_1, \ldots, A_m$, so fällt die Gesamtheit der *verschiedenen* Untergruppen der Gesamtheit

$$A \,.\, a, A \,.\, b, \ldots \text{ usw., wo } G = \{a, b, \ldots\}$$

ist, mit den Gruppen (α) zusammen.

Unser Satz läßt sich dann folgendermaßen aussprechen:

Ist A eine Untergruppe von G der Eigenschaft, mit keiner von A verschiedenen und mit A isomorphen Untergruppe ein Element gemeinsam zu haben, so gilt die Zerlegung

$$G = A + A \,.\, \beta + A \,.\, \gamma + \cdots + A \,.\, \varepsilon.$$

Die Untergruppen A, $A \,.\, \beta, \ldots$ usw., als Elemente betrachtet, bilden selbst eine distributive Gruppe Γ, und G ist ν-stufig isomorph zu Γ.

Um diese Behauptung zu verstehen, müssen wir das Verknüpfungsresultat zweier Gruppen $C\{c_1, c_2, \ldots\}$ und $D\{d_1, d_2, \ldots\}$ erklären. *Unter $C \,.\, D$ verstehen wir den Inbegriff der Elemente $c_i \,.\, d_k$, $i, k = 1, 2, \ldots$ Wir haben (Axiom I) zu beweisen*, daß $A_i \,.\, A_k$ ein A_l, d. h. eine Gruppe des Systems (α) ist.

Wir bezeichnen mit $a_1^r, a_2^r, \ldots, a_\nu^r$ die Elemente der Gruppe A_r, $r = 1, \ldots, m$ und betrachten die beiden isomorphen Gruppen

$$a_1^i \,.\, A_k \quad \text{resp.} \quad A_i \,.\, a_t^k,$$

die im System (α) enthalten sind. Sie haben das Element $a_1^i a_t^k$ gemeinsam und müssen demnach zusammenfallen. Also gilt

$$A_l = a_1^i \,.\, A_k = A_i \,.\, a_1^k = A_i \,.\, a_2^k = \cdots = A_i \,.\, A_k,$$

und Axiom I ist nachgewiesen.

Um Axiom II zu beweisen, ist zu zeigen, daß die Gleichung

$$A_i \,.\, X = A_l$$

innerhalb des Systems (α) eine und nur eine Lösung zuläßt.

Nun gibt es in G ein Element $x = a_t^k$, das der Gleichung $a_1^i \,.\, a_1^k = a_1^l$ genügt. Daraus folgt aber $A_i \,.\, A_k = A_l$, also $X = A_k$. Gäbe es noch eine zweite Lösung A_j, gälte also $A_i \,.\, A_j = A_i \,.\, A_k$, so folgt daraus $a_1^i \,.\, A_j = a_1^i \,.\, A_k$ und somit $A_j = A_k$. Somit ist auch Axiom II bewiesen. Für $Y \,.\, A_l = A_k$ beweist man es in der gleichen Weise.

Der Nachweis des Axioms III ist ebenso einfach: $(A_i \,.\, A_k) \,.\, A_l$ ist eine Gruppe von (α), ebenfalls $(A_i \,.\, A_l) \,.\, (A_k \,.\, A_l)$. Beide Gruppen enthalten das Element

$$(a_1^i \,.\, a_1^k) \,.\, a_1^l = (a_1^i \,.\, a_1^l) \,.\, (a_1^k \,.\, a_1^l)$$

und fallen somit zusammen.

Wir bringen drei Beispiele von Systemen isomorpher Untergruppen, für die $q = 1$ ist.

1. *Beispiel*: A ist eine ν-gliedrige Untergruppe der Gruppe N-ter Ordnung G der Eigenschaft, mit keiner von A verschiedenen Untergruppe ν-ter Ordnung ein Element gemeinsam zu haben.

Dann kann auch A mit keiner von A verschiedenen und mit A isomorphen Untergruppe ein Element gemeinsam haben, und die Bedingungen des Satzes sind erfüllt.

2. *Beispiel*: Sei G eine Gruppe N-ter Ordnung und a_1 ein Element von G. Wir behaupten: Die Elemente x von G, die die Gleichung

$$a_1 \,.\, x = x \,.\, a_1$$

befriedigen, bilden eine Untergruppe A von G, die mit keiner isomorphen ein Element gemeinsam hat.

Da die Lösungselemente $x = a_1, a_2, \ldots$ in endlicher Zahl vorhanden sind, so ist des Gruppennachweises wegen nur die Gültigkeit des Axioms I zu überprüfen. Nun folgt aus $a_1 \,.\, x = x \,.\, a_1$ und $a_1 \,.\, y = y \,.\, a_1 : a_1 \,.\, (x \,.\, y) = (x \,.\, y) \,.\, a_1$; d. h. mit x und y ist $x \,.\, y$ auch eine Lösung. Bezeichnen wir die Untergruppe der Lösungen mit

$$A : \{a_1, a_2, \ldots, a_\nu\}$$

so muß, da a_1 mit jedem Element der Gruppe A vertauschbar ist, dies für jedes andere Element der Gruppe gelten. [Vertauschbar im Sinne: $a_1 \,.\, a_i = a_i \,.\, a_1$]. Heben wir aus A also irgend ein Element a_i heraus, so stellt A die Gesamtheit der mit a_i vertauschbaren Elemente von G dar, denn jedes Element, das mit a_i vertauschbar ist, ist mit a_1 vertauschbar.

Sei dann B eine zu A isomorphe Untergruppe. Sie ist ebenfalls ν-ter Ordnung und enthält wegen der Homogenität der Gruppe G die Gesamtheit aller Elemente, die mit einem

beliebigen Elemente von B kommutativ sind. Haben A und B ein Element gemeinsam, so müssen sie zusammenfallen, da durch dieses Element A und B eindeutig definiert ist. Unsere Behauptung ist erwiesen.

Ehe wir ein drittes Beispiel behandeln, führen wir eine neue Bezeichnung ein. Wir schreiben

$$a \,.\, (a \,.\, b) = \overset{2}{a} \,.\, b$$
$$a \,.\, [a \,.\, (a \,.\, b)] = \overset{3}{a} \,.\, b, \ldots \text{ usw.}$$

3. *Beispiel.* Sei G eine Gruppe N-ter Ordnung und a_1 ein Element von G. Wir behaupten: Die Elemente x von G, die der Gleichung

$$\overset{r}{a}_1 \,.\, x = x$$

genügen, bilden eine Untergruppe A von G, die mit keiner isomorphen ein Element gemeinsam hat. Der Gruppennachweis wird wie im Beispiele 2 erbracht. Bezeichnen wir die Gruppe der Lösungen mit

$$A\{a_1, a_2, \ldots, a_\nu\}\,^{1}),$$

so muß, da $\overset{r}{a}_1 \,.\, a_i = a_i$ $(i = 1, 2, \ldots, \nu)$ gilt, wegen der Homogenität von A $\overset{r}{a}_t \,.\, a_i = a_i$ $(i = 1, 2, \ldots, \nu)$ für $t = 1, 2, \ldots, \nu$ gelten, d. h. die Gruppe A ist durch irgend eines ihrer Elemente a_t infolge $\overset{r}{a}_t \,.\, x = x$ eindeutig fixiert. Sei dann $B = \{b_1, b_2, \ldots, b_\nu\}$ eine zu A isomorphe Untergruppe von G, so ist sie durch irgend ein Element b_t und die Gleichung $\overset{r}{b}_t \,.\, x = x$ eindeutig fixiert [2]). Haben somit A und B ein Element gemeinsam, so fallen sie zusammen.

Bemerkung: Wir hätten anstelle der Gleichung $\overset{r}{a}_1 \,.\, x = x$ eine Gleichung

$$a_1 \,.\, [(x \,.\, a_1) \,.\, a_1] = x \,.\, a_1$$

oder eine ähnliche (x darf rechts und links nur einmal auftreten) setzen können.

§ 3. Erzeugungsprinzipien distributiver Gruppen.

A. Erzeugung aus assoziativen kommutativen Gruppen.

Sei $G_a\{a_1, a_2, \ldots, a_{2n+1}\}$ eine assoziative kommutative Gruppe der Ordnung $2n + 1$, sei ferner α eine ganze Zahl und α und $\alpha - 1$ relativ prim zu $2n + 1$ (z. B. $\alpha = 2$, $\alpha = n + 1$). Das Verknüpfungsresultat der Elemente a_i und a_k der Gruppe G_a bezeichnen wir mit

$$a_i \circ a_k,$$

dann gilt nach Voraussetzung $a_i \circ a_k = a_k \circ a_i$, $(a_i \circ a_k) \circ a_l = a_i \circ (a_k \circ a_l)$. Mit a_i^α bezeichnen wir das Element $a_i \circ a_i \circ \ldots \ldots \circ a_i$, α-mal iteriert. *Durchläuft i die Reihe* $1, 2, \ldots, 2n + 1$, *so durchläuft a_i^α alle Elemente von G_a.* Im entgegengesetzten Falle würde für $a_i \neq a_k$, $a_i^\alpha = a_k^\alpha$ gelten. Bezeichnen wir mit a_k^{-1} wie üblich das inverse Element von a_k in G_a, so folgt

$$a_i^\alpha \circ (a_k^{-1})^\alpha = 1 = (a_i \circ a_k^{-1})^\alpha.$$

$a_i \circ a_k^{-1}$ kann nicht das Einheitselement sein, sonst gälte $a_k^{-1} = a_i^{-1}$, also $a_k = a_i$ gegen Voraussetzung. Bezeichnen wir $a_i \circ a_k^{-1} = a_l$, so erfüllt a_l die Gleichung $a_l^\alpha = 1$; daraus folgt, daß es in G_a eine Untergruppe der Ordnung ν geben müßte, wobei ν ein Teiler von α wäre. Da aber dann ν auch Teiler von $2n + 1$ sein müßte, so wären gegen die Voraussetzung α und $2n + 1$ nicht relativ prim. Somit ist die Gleichung $x^\alpha = a_i$, also $x = \overset{1}{a_i^\alpha}$ [3]) eindeutig in G_a lösbar. Dasselbe gilt natürlich für $\alpha - 1$ anstelle von α.

---

[1]) Wir wollen die Zahl r den Grad der Gruppe ν-ter Ordnung A nennen.

[2]) Infolge der Homogenität der Gesamtgruppe G.

[3]) Wir können in der Reihe $1, 2, \ldots, 2n+1$ immer eine Zahl β finden, daß $\overset{1}{a^\alpha} = a^\beta$ ist. In der Tat,

Wir zeigen nun, daß wir die Elemente von G_a als Elemente einer distributiven Gruppe G_a der Ordnung $2n+1$ auffassen können, wenn wir als neue Verknüpfungsoperation

$$a_i \,.\, a_k = a_i^{\alpha} \circ a_k^{1-\alpha}$$

ansetzen. Die Axiome I und II sind infolge unserer Voraussetzungen erfüllt, somit bleibt uns nur, den Nachweis für das Axiom III zu erbringen. Nun ist

$$(a_i \,.\, a_k) \,.\, a_l = (a_i^{\alpha} \circ a_k^{1-\alpha})^{\alpha} \circ a_l^{1-\alpha} = a_i^{\alpha^2} \circ a_k^{\alpha(1-\alpha)} \circ a_l^{1-\alpha},$$

ferner ist

$$(a_i \,.\, a_l) \,.\, (a_k \,.\, a_l) = (a_i^{\alpha} \circ a_l^{1-\alpha})^{\alpha} \circ (a_k^{\alpha} \circ a_l^{1-\alpha})^{1-\alpha} = a_i^{\alpha^2} \circ a_k^{\alpha(1-\alpha)} \circ a_l^{1-\alpha}.$$

Also gilt Axiom III, q. e. d.

Erste Bemerkung: Für die spezielle, kommutative Gruppe G_a $(2n+1)$-ter Ordnung, deren Elemente $1, 2, \ldots, 2n+1$ der Verknüpfung $a \circ b \equiv a + b \bmod 2n+1$ unterliegen, ist $a^{\alpha} = \alpha a$, also

$$a \,.\, b \equiv \alpha a + (1-\alpha) b \quad \bmod 2n+1.$$

Beispiel 1, § 1.

Zweite Bemerkung: Betrachten wir die nichtendliche kommutative G_a, deren Elemente alle reellen Zahlen sind und deren Verknüpfungsgesetz $a \,.\, b = a + b$ ist, so ist ebenfalls $a \,.\, b = \alpha a + \beta b$ mit $\alpha + \beta = 1$ das Verknüpfungsgesetz der entsprechenden distributiven Gruppe.

Dritte Bemerkung: Sei A_a eine Untergruppe ν-ter Ordnung von G_a, dann ist ν als Teiler von $2n+1$ zu α und $\alpha - 1$ relativ prim. Sind $b_1, b_2, \ldots, b_\nu$ die Elemente von A_a, so bildet dieses System vermöge der Verknüpfung

$$b_i \,.\, b_k = b_i^{\alpha} \circ b_k^{1-\alpha}$$

eine distributive Gruppe, d. h. *die Elemente einer Untergruppe A_a der Gruppe G_a bilden eine Untergruppe A_d der Gruppe G_d.*

Die Elemente

$$A_d \,.\, p = \{b_1 \,.\, p, b_2 \,.\, p, \ldots, b_\nu \,.\, p\} = \{b_1^{\alpha} \circ p^{1-\alpha}, \ldots, b_\nu^{\alpha} \circ p^{1-\alpha}\} = \{b_1^{\alpha}, \ldots, b_\nu^{\alpha}\} \circ p^{1-\alpha} = A^{\alpha} \circ p^{1-\alpha}$$

der distributiven Untergruppe $A_d \,.\, p$ bilden eine „Nebengruppe" $A_a \circ p^{1-\alpha}$ der Untergruppe A_a von G_a. Somit: Haben $A_d \,.\, p$ und $A_d \,.\, q$ ein Element gemeinsam, so fallen sie zusammen, und es gilt die Zerlegung:

$$G_d = A_d + A_d \,.\, p + \cdots + A_d \,.\, t.$$

Sei nun

$$b_i \,.\, p = b_i^{\alpha} \circ p^{1-\alpha} \text{ ein Element von } A_d \,.\, p$$
$$b_j \,.\, q = b_j^{\alpha} \circ q^{1-\alpha} \text{ ein Element von } A_d \,.\, q,$$

dann ist

$$(b_i \,.\, p) \,.\, (b_j \,.\, q) = (b_i^{\alpha} \circ p^{1-\alpha})^{\alpha} \circ (b_j^{\alpha} \circ q^{1-\alpha})^{1-\alpha} =$$
$$= (b_i^{\alpha} \circ b_j^{1-\alpha})^{\alpha} \circ (p^{\alpha} \circ q^{1-\alpha})^{1-\alpha} = (b_i \,.\, b_j) \,.\, (p \,.\, q).$$

Da aber dieses Element in der Gruppe $A_d \,.\, (p \,.\, q)$ liegt, so bilden die Untergruppen

$$A_d, A_d \,.\, p, \ldots, A_d \,.\, t,$$

als Elemente betrachtet, selbst eine distributive Gruppe. (Axiom II und III sind erfüllt, Beweis wie früher.)

Ferner gilt die Verknüpfungsgleichung:

---

aus $a = a^{\alpha\beta}$ folgt $a^{\alpha\beta-1} = 1$. Nun ist dies stets für $\alpha\beta - 1 = 2n+1$ der Fall, also für $\alpha\beta \equiv 1 \bmod (2n+1)$, und da α relativ prim zu $2n+1$ ist, gibt es ein solches β.

$$(b_i \,.\, p) \,.\, (b_j \,.\, q) = (b_i \,.\, b_j) \,.\, (p \,.\, q).$$

Sind $B_d\colon \{b_1, \ldots, b_\mu\}$, $C_d\colon \{c_1, \ldots, c_\nu\}$ zwei Untergruppen von G_d, so folgt aus

$$(b_i \,.\, c_k) \,.\, (b_j \,.\, c_l) = (b_i \,.\, b_j) \,.\, (c_k \,.\, c_l)$$

der Gruppencharakter des Elementsystemes

$$\{\ldots, (b_i \,.\, c_k), \ldots\}, \quad i = 1, \ldots, \mu, \; k = 1, \ldots, \nu.$$

B. Erzeugung distributiver Gruppen aus distributiven Gruppen.

(Gilt auch für assoziative Gruppen.)

Seien $A\,\{a_1, \ldots, a_\nu\}$ mit der Verknüpfung $a_i \,.\, a_k$ und
$B\,\{b_1, \ldots, b_\mu\}$ mit der Verknüpfung $b_i \circ b_k$
zwei distributive Gruppen der Ordnung ν resp. μ, so bildet das Elementsystem $\{\ldots, (a_i, b_k), \ldots\}$ mit der Verknüpfung $(a_i, b_k) \times (a_j, b_l) = (a_i \,.\, a_j, b_k \circ b_l)$ eine distributive Gruppe der Ordnung $\mu\nu$. Man überzeugt sich sofort, daß die Axiome I bis III erfüllt sind.

Eine so konstruierte Gruppe, deren Elemente (a_i, b_k) durch zwei Indizes numeriert sind, wollen wir eine *Zweiindizesgruppe* nennen.

Analog kann man *Dreiindizesgruppen* usw. bilden.

Bemerkung: Setzen wir statt der Verknüpfung $a \,.\, b = a^\alpha \circ b^{1-\alpha}$ die Verknüpfung $a \,.\, b = a^\alpha \circ b^\beta$, wobei α, β relativ prim zu $2n + 1$ sind, so sind im entsprechenden *Cayley*-schema Axiom I und II erfüllt, an Stelle von III tritt

$$(a \,.\, d) \,.\, (b \,.\, d) = (a \,.\, b) \,.\, (d \,.\, d), \text{ resp. } (d \,.\, a) \,.\, (d \,.\, b) = (d \,.\, d) \,.\, (a \,.\, b),$$

resp. die allgemeinere

$$(a \,.\, b) \,.\, (c \,.\, d) = (a \,.\, c) \,.\, (b \,.\, d).$$

Es gelten für solche Gruppen die in diesem Paragraphen aufgestellten Beziehungen zu den *Abel*schen Gruppen ungerader Ordnung.

Ist A eine Untergruppe, so stellt $A \,.\, p$ eine „Nebengruppe" dar, wie bei den assoziativen Gruppen.

§ 4. Untergruppen, Indexsatz.

Definition der einfachen Gruppe: *Wir nennen eine Gruppe einfach, wenn sie keine echte Untergruppe der Ordnung größer als eins enthält.* Daraus folgt, daß eine einfache Gruppe durch irgend zwei ihrer Elemente vollständig bestimmt ist.

Sei $A\{a_1, \ldots, a_\nu\}$ *eine einfache Untergruppe der Gruppe* G *und* p *ein beliebiges Element von* G, *so beweisen wir, daß* $A \,.\, (A \,.\, p)$ *eine* ν*-gliedrige Gruppe* $A \,.\, t$ *ist.* Wir bezeichnen die Gruppe $A \,.\, p$ mit B $(a_i \,.\, p = b_i, \; i = 1, \ldots, \nu)$, dann gilt

$$a_i \,.\, b_1 = a_i \,.\, (a_1 \,.\, p) = (a_i \,.\, a_1) \,.\, b_i = a_j \,.\, b_i,$$

wenn $a_i \,.\, a_1 = a_j$ ist.

Sei nun $a_i \neq a_1$, dann ist auch $a_i \neq a_j$ und also $b_i \neq b_j$. Die Gruppen $a_j \,.\, B$ und $A \,.\, b_1$ sind mit A einstufig isomorph, also einfache Gruppen, sie haben die Elemente $a_j \,.\, b_1$ und $a_i \,.\, b_1 = a_j \,.\, b_i$ gemeinsam, fallen demnach als einfache Gruppen zusammen, d. h. es gilt

$$A \,.\, b_1 = a_j \,.\, B, \quad j = 2, 3, \ldots, \nu.$$

Genau so hätte man

$$A \,.\, b_2 = a_h \,.\, B, \quad h = 1, 3, 4, \ldots, \nu$$

abgeleitet, woraus

$$a_1 \,.\, B = a_2 \,.\, B = \cdots = a_\nu \,.\, B = A \,.\, B = A \,.\, (A \,.\, p)$$

folgt, q. e. d.

Wir wollen den Satz auf Untergruppen ausdehnen, die durch zwei (aber nicht beliebige zwei) ihrer Elemente gegeben sind.

Wir beweisen vorerst den Hilfssatz: Sei eine solche Untergruppe A gegeben, und a_l und a_k zwei sie bestimmende Elemente, so bestimmen sowohl a_l und a_j als auch a_k und a_j die Untergruppe, wobei $a_l \,.\, a_j = a_k$ ist.

Beweis: Durch a_l und a_j ist eine kleinste Gruppe $\bar{A}$ bestimmt, für die $\bar{A} \leqq A$ gilt; $\bar{A}$ enthält aber a_k, demnach A, somit gilt $\bar{A} \geqq A$, demnach $\bar{A} = A$, q. e. d.

Ebenso beweist man, daß a_k und a_j A bestimmen.

Wir gehen nun an den Beweis des Satzes. Die Gruppe A sei durch ihre Elemente a_l und a_k bestimmt, ferner sei wie oben

(1) $a_l \,.\, a_j = a_k$ gesetzt, dann gilt

(2) $a_k \,.\, b_j = (a_k \,.\, a_j) \,.\, b_k$ und

(3) $a_l \,.\, b_j = (a_l \,.\, a_j) \,.\, b_l = a_k \,.\, b_l = (a_k \,.\, a_l) \,.\, b_k$.

Die einstufig isomorphen Gruppen $A \,.\, b_j$ und $A \,.\, b_k$ enthalten die zwei Elemente $a_k \,.\, b_j = (a_k \,.\, a_j) \,.\, b_k$ sowie $a_l \,.\, b_j = (a_k \,.\, a_l) \,.\, b_k$.

Nun wird durch die Elemente $a_k \,.\, b_j$ und $a_l \,.\, b_j$ die Gruppe $A \,.\, b_j$ völlig bestimmt, ebenso bestimmen $(a_k \,.\, a_j) \,.\, b_k$ und $(a_k \,.\, a_l) \,.\, b_k$ völlig die Gruppe $A \,.\, b_k$, somit gilt $A \,.\, b_j = A \,.\, b_k$.

Seien nun $x_1, x_2, \ldots$ alle jene Elemente in G, für die $A \,.\, x_1 = A \,.\, x_2 = \cdots = A \,.\, b_j$ gilt, so bilden diese Elemente eine Untergruppe von G. Da ihre Anzahl endlich ist, so ist nur Axiom I nachzuweisen. Aus

$$A \,.\, (x_p \,.\, x_q) \leqq (A \,.\, x_p) \,.\, (A \,.\, x_q) = (A \,.\, x_p) \,.\, (A \,.\, x_p) = A \,.\, x_p = A \,.\, b_j$$

folgt die Gruppeneigenschaft. Diese Gruppe enthält aber b_j und b_k somit die Untergruppe B, also gilt

$$A \,.\, b_1 = A \,.\, b_2 = \cdots = A \,.\, b_\nu = A \,.\, B, \qquad \text{q. e. d.}$$

Sei nun $A\{a_1, a_2, \ldots, a_\nu\}$ eine Untergruppe der Eigenschaft, daß für irgendwelche zwei Elemente a_i und a_k von A eine Gleichung

$$a_i = \overset{2}{a}_k \cdot a_i$$

nicht bestehe, so ist $A \,.\, (A \,.\, p) = A \,.\, t$. Wir knüpfen an Formel 1, 2 und 3 an.

In $A \,.\, b_j$ sind die beiden Elemente $a_k \,.\, b_j = (a_k \,.\, a_j) \,.\, b_k$ und $a_l \,.\, b_j = (a_k \,.\, a_l) \,.\, b_k$ enthalten, dabei ist k ein beliebiger Index der Reihe $1, 2, \ldots, \nu$. Ihr Produkt $(a_l \,.\, a_k) \,.\, b_j = [a_k \,.\, (a_l \,.\, a_j)] \,.\, b_k = (a_k \,.\, a_k) \,.\, b_k = a_k \,.\, b_k$ ist somit in $A \,.\, b_j$ enthalten.

Jede der Gruppen $A \,.\, b_j$ enthält somit die folgenden Elemente

(4) $$a_1 \,.\, b_1, \quad a_2 \,.\, b_2 \quad , \ldots, a_\nu \,.\, b_\nu.$$

Sind diese Elemente alle verschieden, dann bestimmen sie genau die Gruppe $A \,.\, b_j$, und es gilt $A \,.\, b_1 = A \,.\, b_2 = \cdots = A \,.\, b_\nu = A \,.\, B$.

Wir wollen nun sehen, was aus

(4′) $$a_r \,.\, b_r = a_l \,.\, b_l$$

folgt. In A gibt es ein Element a_k für das

(4″) $$a_r \,.\, a_k = a_l$$

gilt. Nun ist

$$\begin{aligned} a_r \,.\, b_k &= (a_r \,.\, a_k) \,.\, b_r = a_l \,.\, b_r = (a_l \,.\, a_r) \,.\, b_l \\ &= (a_l \,.\, b_l) \,.\, (a_r \,.\, b_l) = (a_r \,.\, b_r) \,.\, (a_r \,.\, b_l) = a_r \,.\, (b_r \,.\, b_l), \end{aligned}$$

daraus folgt $b_k = b_r \,.\, b_l$, somit

(4‴) $$a_k = a_r \,.\, a_l.$$

Aus (4″) und (4‴) schließen wir $a_l = a_r \,.\, (a_r \,.\, a_l) = \overset{2}{a}_r \,.\, a_l$. Ebenso gilt natürlich $a_r = \overset{2}{a}_l \,.\, a_r$.

Nach Voraussetzung besteht zwischen den Elementen von A keine derartige Relation, somit folgt $A \,.\, (A \,.\, p) = A \,.\, t$, q. e. d.

Bemerkung: Wir zeigen, daß aus $a_l = \overset{2}{a}_r \,.\, a_l$ die Beziehung (4′) folgt. Wir setzen wieder $a_r \,.\, a_l = a_k$ und erhalten $a_l = a_r \,.\, a_k$. Nun ist

$$a_r \,.\, b_k = a_r \,.\, (b_r \,.\, b_l) = (a_r \,.\, b_r) \,.\, (a_r \,.\, b_l),$$

ferner gilt auch

$$a_r \,.\, b_k = (a_r \,.\, a_k) \,.\, b_r = a_l \,.\, b_r = (a_l \,.\, a_r) \,.\, b_l = (a_l \,.\, b_l) \,.\, (a_r \,.\, b_l).$$

Der Vergleich ergibt $a_r \,.\, b_r = a_l \,.\, b_l$, q. e. d.

Ist $A\{a_1, \ldots, a_\nu\}$ eine kommutative Gruppe, die keine Untergruppe der Ordnung drei enthält, so gilt $A \,.\, (A \,.\, p) = A \,.\, t$.

Dies ist eine direkte Folge der vorhergehenden Betrachtung.

Bestünde eine Relation $a_j = a_i \,.\, (a_i \,.\, a_j)$, so folgt aus $a_i \,.\, a_j = a_k$, $a_j = a_i \,.\, a_k$. Ferner ist dann $a_j \,.\, a_k = (\ _i \,.\, a_k) \,.\, (a_i \,.\, a_j) = a_i \,.\, (a_k \,.\, a_j)$, woraus $a_j \,.\, a_k = a_i$ folgt, d. h. die Elemente a_i, a_j und a_k bilden eine Untergruppe der Ordnung 3, im Widerspruch zu unserer Voraussetzung.

1. *Satz*: *Für Untergruppen A, für die $A \,.\, (A \,.\, p) = A \,.\, t$ ist, gilt die Zerlegung*

$$G = A + A \,.\, p + A \,.\, q + \cdots + A \,.\, w.$$

Wir beweisen dies, indem wir zeigen, daß zwei Untergruppen $A \,.\, p$ und $A \,.\, q$ identisch oder elementfremd sind.

Beweis: Die beiden Untergruppen mögen ein Element c gemeinsam enthalten. Nun gilt

(5′) $A \,.\, (A \,.\, p) = A \,.\, c$ resp. (5″) $A \,.\, (A \,.\, q) = A \,.\, c$, somit $A \,.\, (A \,.\, p) = A \,.\, (A \,.\, q)$, also (5‴) $a_1 \,.\, (A \,.\, p) = a_1 \,.\, (A \,.\, q)$, also (5⁗) $A \,.\, p = A \,.\, q$, q. e. d.

Wir zeigen nun für spätere Zwecke, daß für eine einfache Untergruppe der Ordnung ν, $A\{a_1, a_2, \ldots, a_\nu\}$, auch $(A \,.\, p) \,.\, A$ eine ν-gliedrige Gruppe $t \,.\, A$ ist.

Es gilt

(6) $(a_i \,.\, p) \,.\, a_k = (a_i \,.\, a_k) \,.\, (p \,.\, a_k) = a_l \,.\, (p \,.\, a_k) = (a_l \,.\, p) \,.\, (a_l \,.\, a_k) = (a_l \,.\, p) \,.\, a_h$,

wobei

(6′) $a_i \,.\, a_k = a_l$ und (6″) $a_l \,.\, a_k = a_h$

ist. Ferner gilt

(7) $(a_l \,.\, p) \,.\, a_h = (a_l \,.\, a_h) \,.\, (p \,.\, a_h) = a_s \,.\, (p \,.\, a_h) = (a_s \,.\, p) \,.\, (a_s \,.\, a_h) = (a_s \,.\, p) \,.\, a_t$,

wobei

(7′) $a_l \,.\, a_h = a_s$ und (7″) $a_s \,.\, a_h = a_t$ ist. Für a_s und a_t berechnen wir

$$(8) \qquad \begin{cases} a_s = a_l \,.\, a_h = (a_i \,.\, a_k) \,.\, (a_l \,.\, a_k) = (a_i \,.\, a_l) \,.\, a_k \\ a_t = a_s \,.\, a_r = [(a_i \,.\, a_l) \,.\, a_k] \,.\, (a_l \,.\, a_k) = [(a_i \,.\, a_l) \,.\, a_l] \,.\, a_k. \end{cases}$$

Die beiden einfachen Gruppen $(a_i \,.\, p) \,.\, A$ und $(A \,.\, p) \,.\, a_h$ haben die Elemente

(8′) $(a_i \,.\, p) \,.\, a_h$ und $(a_i \,.\, p) \,.\, a_k = (a_l \,.\, p) \,.\, a_h$ gemeinsam. Sei $a_i \neq a_k$, so ist nach (6′) $a_k \neq a_l$. Also ist nach (6″) $a_h \neq a_k$, d. h. die beiden Elemente (8′) sind verschieden.

$$(a_i \,.\, p) \,.\, A = (A \,.\, p) \,.\, a_h,$$

wobei $a_i \,.\, a_k = a_l$, $a_l \,.\, a_k = a_h$, also $(a_i \,.\, a_k) \,.\, a_k = a_h$ ist.

Nun sind zwei Fälle zu unterscheiden:

1. *Fall*: Für zwei Werte a_k (a_k und $a_{\bar{k}}$) seien a_h und $a_{\bar{h}}$ verschieden. Dann folgt

$$(A \,.\, p) \,.\, a_h = (A \,.\, p) \,.\, a_{\bar{h}} = (A \cdot p) \cdot A.$$

2. *Fall*: Wie man auch $k \neq i$ wähle, stets sei in $a_h = (a_i \,.\, a_k) \,.\, a_k$: a_h von a_k unabhängig. Dann muß $a_h = a_i$ sein, denn wäre $a_h = a_t$, $t \neq i$, so gälte $a_t = (a_i \,.\, a_t) \,.\, a_t$, d. h. $a_i \,.\, a_t = a_t$, d. h. $t = i$, was ein Widerspruch ist. Also muß

(9) $$a_i = (a_i \,.\, a_k) \,.\, a_k$$

gelten.

Nun war auch a_i völlig willkürlich, somit muß (9) für irgend zwei Elemente von A gelten (oder wir hätten den Fall 1). Dann aber folgt aus (8) $a_t = a_i \,.\, a_k$, und die einfachen Gruppen $(a_i \,.\, p) \,.\, A$ und $(A \,.\, p) \,.\, a_t$ enthalten die zwei verschiedenen Elemente $(a_i \,.\, p) \,.\, a_t$ und $(a_i \,.\, p) \,.\, a_k = (a_s \,.\, p) \,.\, a_t$. (Da $a_t \neq a_k$, wenn $a_i \neq a_k$ ist.) Es gilt also

(10) $$(a_i \,.\, p) \,.\, A = (A \,.\, p) \,.\, a_t.$$

Durchläuft k die Zahlen $1, 2, \ldots, i-1, i+1, \ldots, \nu$, so durchläuft t diese Zahlen in geänderter Folge, d. h. es gilt

$(a_i \,.\, p) \,.\, A = (A \,.\, p) \,.\, a_1 = (A \,.\, p) \,.\, a_2 = \cdots = (A \,.\, p) \,.\, a_x$, da ja a_i willkürlich gewählt war, q. e. d.

Sei $A\{a_1, \ldots, a_\nu\}$ *eine Untergruppe und bestehen für keine zwei Elemente die Gleichungen* $(a_i \,.\, a_p) \,.\, a_p = a_i$ *oder* $(a_p \,.\, a_i) \,.\, a_p = a_i$, *so ist* $(A \,.\, p) \,.\, A = t \,.\, A$. Wir beziehen uns auf die Formeln (6) bis (8). Die Gruppe $(a_i \,.\, p) \,.\, A$ enthält die Elemente $(a_i \,.\, p) \,.\, a_h$ und $(a_i \,.\, p) \,.\, a_k = (a_l \,.\, p) \,.\, a_h$, somit die Gesamtheit der Elemente $(x_r \,.\, p) \,.\, a_h$, wo x_r irgendein Element der die Elemente a_i und a_l umfassenden kleinsten Gruppe $\{a_i, a_l\}$ ist.

Dieser Gruppe gehören die Elemente a_k, a_h, a_s, a_t an, somit enthält $(a_i \,.\, p) \,.\, A$ die Elemente $(a_h \,.\, p) \,.\, a_h$, wobei $a_h = (a_i \,.\, a_k) \,.\, a_k$ ist.

Wir behaupten, daß mit a_k auch a_h alle Elemente von A durchläuft. Aus $(a_i \,.\, a_k) \,.\, a_k = (a_i \,.\, a_p) \,.\, a_p = a_r$ schließen wir wie folgt:

Setzen wir $a_i \,.\, a_k = a_l$, $a_i \,.\, a_p = a_q$, so gilt $a_l \,.\, a_k = a_q \,.\, a_p$, weiter ist $a_l \,.\, (a_p \,.\, a_k) = (a_i \,.\, a_k) \,.\, (a_p \,.\, a_k) = a_q \,.\, a_k$, ebenfalls gilt

$$a_l \,.\, (a_p \,.\, a_k) = (a_l \,.\, a_p) \,.\, (a_l \,.\, a_k) = (a_l \,.\, a_p)\,(a_q \,.\, a_p) = (a_l \,.\, a_q) \,.\, a_p = [a_i \,.\, (a_k \,.\, a_p)]a_p = a_q \,.\, [(a_k \,.\, a_p) \,.\, a_p],$$

der Vergleich ergibt somit $a_k = (a_k \,.\, a_p) \,.\, a_p$, was gegen die Voraussetzung ist. Also sind in $(a_i \,.\, p) \,.\, A$ alle Elemente

(γ) $$(a_1 \,.\, p) \,.\, a_1, \quad (a_2 \,.\, p) \,.\, a_2, \ldots, \quad (a_\nu \,.\, p) \,.\, a_\nu$$

enthalten.

Es sei nun, $b_t = a_t \,.\, p$ *gesetzt,* $b_l \,.\, a_l = b_k \,.\, a_k$.

Ist $a_r \,.\, a_k = a_l$, so bilden wir

$$b_r \,.\, a_k = (a_r \,.\, p) \,.\, a_k = a_l \,.\, (p \,.\, a_k) = b_l \,.\, (a_l \,.\, a_k) = (b_l \,.\, a_l) \,.\, (b_l \,.\, a_k) = (b_k \,.\, a_k) \,.\, (b_l \,.\, a_k) = (b_k \,.\, b_l) \,.\, a_k.$$

Das hätte nun $b_r = b_k \,.\, b_l$, also $a_r = a_k \,.\, a_l$ zur Folge, oder $(a_k \,.\, a_l) \,.\, a_k = a_l$, gegen die Voraussetzung. Somit enthalten alle Gruppen $(a_i \,.\, p) \,.\, A$ die ν *verschiedenen* Elemente (γ), und es gilt

$$(a_1 \,.\, p) \,.\, A = (a_2 \,.\, p) \,.\, A = \cdots = (a_\nu \,.\, p) \,.\, A = (A \,.\, p) \,.\, A, \quad \text{q. e. d.}$$

Folgerungen aus Satz 1.

1. Eine Gruppe der Ordnung einer Primzahl ist einfach.

2. Die Ordnung einer einfachen Untergruppe, einer Untergruppe, die durch zwei Elemente bestimmt ist, endlich einer Untergruppe, deren Elemente keiner Gleichung $a_i^2 \cdot a_k = a_k$ genügen, ist ein Teiler der Ordnung der Gruppe.

3. Für Untergruppen einer kommutativen Gruppe, deren Ordnung nicht durch drei teilbar ist, gilt der Indexsatz (die Ordnung der Untergruppe ist Teiler der Ordnung der Gruppe).

Zum Schlusse dieses Paragraphen notieren wir den

Satz: Ist $(A \,.\, p) \,.\, A = t \,.\, A$, *so ist auch* $A \,.\, (p \,.\, A) = A \,.\, \tau$, *denn es gilt stets* $(A \,.\, p) \,.\, A = A \,.\, (p \,.\, A)$.

Sei $(a_i \,.\, p) \,.\, a_k$ ein Element von $(A \,.\, p) \,.\, A$, so liegt es wegen

$$(a_i \,.\, p) \,.\, a_k = (a_i \,.\, a_k) \,.\, (p \,.\, a_k)$$

in $A \,.\, (p \,.\, A)$, somit ist

$$(A \,.\, p) \,.\, A \leqq A \,.\, (p \,.\, A).$$

Sei $a_i \,.\, (p \,.\, a_k) = (a_i \,.\, p) \,.\, (a_i \,.\, a_k)$ ein Element von $A \,.\, (p \,.\, A)$, so liegt es auch in $(A \,.\, p) \,.\, A$, somit gilt

$$(A \,.\, p) \,.\, A \geqq A \,.\, (p \,.\, A),$$

also ist $(A \,.\, p) \,.\, A = A \,.\, (p \,.\, A)$, q. e. d.

Bemerkung: Sei $G\{a_1, a_2, \ldots, a_\nu\}$ eine distributive Gruppe und die Gleichung $(a_i \,.\, a_k) \,.\, a_k = a_i$ innerhalb der Gruppe nicht erfüllbar. Wir definieren dann durch

$$a_i \circ a_k = (a_i \,.\, a_k) \,.\, a_k$$

eine neue Verknüpfung. Das System $\{a_1, \ldots, a_\nu\}$ erfüllt dann Axiom I und II und

$$(a_i \circ a_k) \circ (a_j \circ a_k) = [(a_i \,.\, a_k) \,.\, a_k] \circ [(a_j \,.\, a_k) \,.\, a_k]$$
$$= \{[(a_i \,.\, a_k) \,.\, a_k] \,.\, [(a_j \,.\, a_k) \,.\, a_k]\} \,.\, [(a_j \,.\, a_k) \,.\, a_k] = \{[(a_i \,.\, a_j) \,.\, a_k] \,.\, a_k\} \,.\, [(a_j \,.\, a_k) \,.\, a_k]$$
$$= \{[(a_i \,.\, a_j) \,.\, a_j] \,.\, a_k\} \,.\, a_k = (a_i \circ a_j) \circ a_k,$$

dagegen wird die linksseitige Distributivität im allgemeinen nicht erfüllt sein.

§ 5. Struktur der distributiven Gruppen.

Wir setzen in diesem Paragraphen voraus, daß für jede Untergruppe A von G $A \,.\, (A \,.\, p)$ und $(A \,.\, p) \,.\, A$ Untergruppen der Ordnung von A sind.

In Formeln: $\begin{cases} A \,.\, (A \,.\, p) = A \,.\, t \\ (A \,.\, p) \,.\, A = A \,.\, (p \,.\, A) = A \,.\, \tau. \end{cases}$

Diese Voraussetzung ist nach den Ergebnissen des § 4 jedenfalls für Gruppen G erfüllt, für die keine der Gleichungen

$$(x \,.\, y) \,.\, y = x, \quad (y \,.\, x) \,.\, y = x, \quad y \,.\, (y \,.\, x) = x$$

für zwei verschiedene Elemente x, y von G erfüllbar ist. Gruppen G dieser Eigenschaft wollen wir ausgezeichnete Gruppen nennen.

Bezeichnung: *Eine Untergruppe $A \,.\, p$ bezeichnen wir kurz $[A]$.*

Hilfssatz I: *Sind A, B und C Untergruppen der gleichen Ordnung ν, so folgt aus $A \cdot B = C$:*

$$B = [A],\ C = [A],\ A = [B],\ C = [B],\ A = [C],\ B = [C].$$

Beweis: Aus $A \,.\, B = C$ folgt $C = [A]$. Die Elemente von A seien mit a_t, von B mit b_t und von C mit c_t, $t = 1, 2, \ldots, \nu$ bezeichnet.

In G gibt es ein Element r für das $a_1 \,.\, r = b_1$ ist. Dann gilt

$$A \,.\, B = A \,.\, b_1 = A \,.\, (a_1 \,.\, r) = A \,.\, (A \,.\, r),$$

also $B = [A]$. Ferner sei $a_1 = b_1 \,.\, q$, dann gilt

$$C = A \,.\, B = a_1 \,.\, B = (b_1 \,.\, q) \,.\, B = (B \,.\, q) \,.\, B = B \,.\, (q \,.\, B),$$

somit $C = [B]$ und $A = [B]$.

Endlich ist $A \,.\, C = A \,.\, [A] = A \,.\, \sigma$, somit nach dem Vorhergehenden $A = [C]$, und ebenso folgt aus $B \,.\, C = B \,.\, [B] = B \,.\, \tau$, daß $B = [C]$ ist.

Hilfssatz II: *Sind A, B und C ν-gliedrige Untergruppen, so folgt aus $A \,.\, B =$ ν-gliedrige Untergruppe und $A = [C]$, $B = [C]$, daß $A \,.\, B = [C]$ ist.*

In der Tat ist $A = C \,.\, \varrho$, $B = C \,.\, \tau$, somit

$$A \,.\, B = (C \,.\, \varrho) \,.\, (C \,.\, \tau) \geqq C \,.\, (\varrho \,.\, \tau).$$

Da aber $A \,.\, B$ ν-gliedrig ist, so folgt $A \,.\, B = C \,.\, (\varrho \,.\, \tau) = [C]$.

Hilfssatz III: *Seien $A_1, A_2, \ldots, A_\sigma$ ν-gliedrige Untergruppen der Eigenschaft,*

daß die Produkte $A_i . A_k$, $(i, k = 1, \ldots, \sigma)$ *v-gliedrige Gruppen sind, und ergänzt man dieses System von v-gliedrigen Untergruppen durch Adjunktion jener Produkte* $A_i . A_k$, *die im System noch nicht vorhanden sind, so erhält man ein neues System* $A_1, A_2, \ldots, A_{\sigma+\tau}$ *der Eigenschaft, daß die Produkte* $A_i . A_k$, $i, k = 1, 2, \ldots, \sigma + \tau$ *ebenfalls v-gliedrige Gruppen sind.*

Wir haben nur zu beweisen, daß $A_i . A_{\sigma+k}$, $A_{\sigma+k} . A_i$ und $A_{\sigma+h} . A_{\sigma+k}$, $(i = 1, 2, \ldots, \sigma;\ h, k = 1, 2, \ldots, \tau)$ v-gliedrige Gruppen sind.

Aus $A_i . A_p = v$-gliedriger Gruppe, folgt $A_i = [A_p]$, $i, p = 1, \ldots, \sigma$ (Hilfssatz I), und da $A_i . A_k$ eine v-gliedrige Gruppe ist, folgt nach Hilfssatz II:

$$A_i . A_k = [A_p],\ p, i, k = 1, 2, \ldots, \sigma.$$

Somit ist $A_{\sigma+k} = [A_i]$, denn es ist $A_{\sigma+k} = A_\tau . A_s$ nach Voraussetzung, also ist in der Tat $A_i . A_{\sigma+k}$ (ebenfalls dann $A_{\sigma+k} . A_i$) eine v-gliedrige Gruppe.

Daraus wieder schließen wir $A_i = [A_{\sigma+k}]$, $i = 1, \ldots, \sigma$, $k = 1, \ldots, \tau$. Sei nun $A_{\sigma+h} = A_p . A_q$, so ist $A_p = [A_{\sigma+k}]$ und $A_q = [A_{\sigma+k}]$, und da $A_p . A_q$ v-gliedrig ist, so ist (Hilfssatz II) $A_p . A_q = A_{\sigma+h} = [A_{\sigma+k}]$, somit sind $A_{\sigma+h} . A_{\sigma+k}$ $(h, k = 1, 2, \ldots, \tau)$ v-gliedrige Gruppen, q. e. d. Nun sind wir in der Lage den Satz zu beweisen:

Satz I: Seien $A_1, A_2, \ldots, A_\sigma$ *v-gliedrige Untergruppen der Eigenschaft, daß die Produkte* $A_i . A_k$ $(i = 1, 2, \ldots, \sigma)$ *v-gliedrig sind, so können wir eine distributive Gruppe, deren Elemente v-gliedrige Untergruppen sind, bilden, die* $A_1, \ldots, A_\sigma$ *als Elemente enthält.*

Beweis: Wir vervollständigen das System $A_1, A_2, \ldots, A_\sigma$ durch ihre Produkte $A_i . A_k$, sofern sie im System noch nicht enthalten sind, und erhalten ein neues System $A_1, \ldots, A_{\sigma+\tau}$, das wir in der gleichen Art vervollständigen und so weiter, bis wir zu einem System

$$(\alpha) \qquad A_1, A_2, \ldots, A_\varepsilon$$

gelangen der Eigenschaft, alle Produkte $A_i . A_k$ schon zu enthalten. Zu einem solchen System müssen wir der Endlichkeit der Grundgruppe G wegen gelangen, da alle Gruppen A_k, $k = 1, 2, \ldots, \varepsilon$ wegen $A_i . A_k$ v-gliedrig die Form $A_k = [A_1]$ haben und somit elementfremd sind [1]). Das System (α) genügt somit dem Axiom I. Sei A_i eine Untergruppe von (α), so durchläuft

$$A_i . A_k \text{ resp. } A_k . A_i \text{ mit } k = 1, 2, \ldots, \varepsilon$$

alle Elemente des Systems (α), denn aus

$$A_i . A_k = A_i . A_j \text{ folgt } a_1^i . A_k = a_1^i . A_j, \text{ also } A_k = A_j.$$

Somit ist Axiom II erfüllt.

Wir beweisen noch eine der beiden Relationen des Axioms III, z. B.

$$(A_i . A_k) . A_j = (A_i . A_j) . (A_k . A_j).$$

Die Gruppen $(A_i . A_k) . A_j$ und $(A_i . A_j) . (A_k . A_j)$ sind nach Axiom I in (α) enthalten und sind, da sie das Element $(a_1^i . a_1^k) . a_1^j = (a_1^i . a_1^j) . (a_1^k . a_1^j)$ gemeinsam haben, identisch.

Der Satz ist somit bewiesen.

Als Anwendung bringen wir den

Zusatz: Aus A und A . p läßt sich stets eine distributive Gruppe bilden, deren Elemente Untergruppen der Form A . h sind, und die als Elemente A und A . p enthält.

$A_1 = A$ und $A_2 = A . p$ erfüllen in der Tat die Voraussetzungen des eben bewiesenen Satzes.

Bezeichnung: Sei G eine Gruppe, so nennen wir eine Untergruppe A von G eine *maximale Untergruppe*, wenn durch die Elemente $a_1, a_2, \ldots, a_\nu$ von A und ein in $G - A$

[1]) Satz 1, § 4.

enthaltenes Element p, also durch $\{A, p\}$ die Gruppe G völlig bestimmt ist. (D. h. G ist die kleinste $a_1, a_2, \ldots, a_\nu, p$ enthaltende Gruppe.)

Dann gilt $G \geqq A + A \,.\, q_1 + A \,.\, q_2 + \cdots + A \,.\, q_\sigma$, $A \,.\, q_1$ enthalte p, und da die Gruppe $\{A, p\}$ mit G zusammenfallen muß, so gilt $G = A + Aq_1 + \cdots + Aq_\sigma$.

Setzen wir nun $A = G_1$, so gilt das Analoge für einen Maximalteiler A_1 von G_1:

$$A = A_1 + A_1 \,.\, r_1 + A_1 \,.\, r_2 + \cdots + A_1 \,.\, r_\iota \qquad \text{usw.}$$

Wir können so fortfahrend reduzieren, bis wir auf eine einfache Gruppe (die also keinen Teiler und natürlich keinen Maximalteiler enthält) stoßen.

Denn jede endliche Gruppe muß einen Maximalteiler, der für einfache Gruppen von der Ordnung 1 ist, enthalten.

Sei nämlich A eine Untergruppe von G und $\{A, p\}$ [1]) noch nicht die Gruppe G, so ist $\{A, p\} = A_1 > A$ eine echte Untergruppe von G. $\{A_1, p_1\}$ ist dann entweder gleich G, oder wieder ein echter Teiler A_2 von G, usw.

Da die Gruppe G endlich ist, so müssen wir zu einem Ende gelangen.

I. Nachtrag [2]).

Wir bezeichnen den Komplex

(2) $\qquad (A \,.\, p) \,.\, (A \,.\, q)$, *A einfache Gruppe*, mit H_{pq}

und wollen ihn genauer untersuchen.

Alle folgenden Sätze über den Komplex H_{pq} gelten selbstverständlich auch für den Fall, daß $H_{pq} = A \,.\, (p \,.\, q)$ ist.

1. Satz: *H_{pq} hat ν oder ν^2 Elemente, wenn ν die Ordnung von A ist.*

Beweis: Wir zeigen, daß wenn H_{pq} $t < \nu^2$ Elemente hat, $t = \nu$ ist. Ist $t < \nu^2$, so gibt es zwei Elemente $(a_h \,.\, p) \,.\, (a_k \,.\, q)$ und $(a_{\bar{h}} \,.\, p) \,.\, (a_{\bar{k}} \,.\, q)$, wobei $h \neq \bar{h}$ und $k \neq \bar{k}$ ist, von der Art, daß

(3) $\qquad (a_h \,.\, p) \,.\, (a_k \,.\, q) = (a_{\bar{h}} \,.\, p) \,.\, (a_{\bar{k}} \,.\, q)$

ist; dann ist aber zufolge Satz 1, § 4

(4) $\qquad (A \,.\, p) \,.\, (a_k \,.\, q) = (A \,.\, p) \,.\, (a_{\bar{k}} \,.\, q).$

Da aber $k \neq \bar{k}$ ist und $A \,.\, p$ durch zwei Elemente vollständig bestimmt ist, so folgt aus (4)

(5) $\quad (A \,.\, p) \,.\, (a_1 \,.\, q) = (A \,.\, p) \,.\, (a_2 \,.\, q) = \cdots = (A \,.\, p) \,.\, (A \,.\, q) = A \,.\, (p \,.\, q).$

Es ist also in diesem Falle $t = \nu$, w. z. b. w.

Bemerkung: Hat H_{pq} ν Elemente, so ist $H_{pq} = A \,.\, (p \,.\, q)$, besitzt aber H_{pq} ν^2 Elemente, so ist

(6) $\quad H_{pq} = (A \,.\, p) \,.\, (a_1 \,.\, q) + (A \,.\, p) \,.\, (a_2 \,.\, q) + \cdots + (A \,.\, p) \,.\, (a_\nu \,.\, q)$.

2. Satz: *H_{pq} ist eine Gruppe.*

Beweis: Hat H_{pq} ν Elemente, so ist $H_{pq} = A \,.\, (p \,.\, q)$, demnach eine ν-gliedrige Gruppe. Wir müssen also nur zeigen, daß H_{pq} mit ν^2 Elementen eine Gruppe ist. Zufolge (6) ist

(6′) $\qquad H_{pq} = (A \,.\, p) \,.\, (a_1 \,.\, q) + \cdots + (A \,.\, p) \,.\, (a_\nu \,.\, q).$

Den Komplex

(6″) $\qquad [(A \,.\, p) \,.\, (a_r \,.\, q)] \,.\, [(A \,.\, p) \,.\, (a_s \,.\, q)]$

bezeichnen wir mit K_{rs} und zeigen, daß er weniger als ν^2 Elemente hat, demnach zufolge Satz 1 eine ν-gliedrige Gruppe von der Form

---

[1]) Mit $\{A, p\}$ ist die kleinste p und die Elemente von A enthaltende Untergruppe von G bezeichnet.

[2]) Der Nachweis $(A \,.\, p) \,.\, (A \,.\, q) =$ Gruppe der Ordnung der Gruppe A ist uns nicht gelungen. Ob dieser Satz richtig ist, steht also offen. Die Sätze des Nachtrages entstanden bei den Versuchen, unsere Vermutung zu verifizieren.

(7) $$K_{rs} = (A \,.\, p) \,.\, [(a_r \,.\, a_s) \,.\, q)] = (A \,.\, p) \,.\, (a_t \,.\, q)$$

ist, wobei

(8) $$a_r \,.\, a_s = a_t$$

ist. Es ist einerseits

(9) $$[(a_t \,.\, p) \,.\, (a_r \,.\, q)] \,.\, [(a_t \,.\, p) \,.\, (a_s \,.\, q)] = (a_t \,.\, p) \,.\, [(a_r \,.\, a_s) \,.\, q] = (a_t \,.\, p) \,.\, (a_t \,.\, q) = a_t \,.\, (p \,.\, q),$$

andererseits ist auch

(9′) $$[(a_r \,.\, p) \,.\, (a_r \,.\, q)] \,.\, [(a_s \,.\, p) \,.\, (a_s \,.\, q)] = (a_r \,.\, a_s) \,.\, (p \,.\, q) = a_t \,.\, (p \,.\, q).$$

Aus (9) und (9′) folgt, daß K_{rs} weniger als ν^2 Elemente besitzt, also von der Form (7) ist. Zufolge (6) und (7) ist

(10) $H_{pq} > K_{rs}$, d. h. H_{pq} ist eine Gruppe, w. z. b. w.

3. Satz: Für die Gruppe H_{pq} gilt neben (6) *auch die Darstellung*

(11) $H_{pq} = A \,.\, \tau_1 + A \,.\, \tau_2 + \cdots + A \,.\, \tau_\nu$, *wobei* $\tau_1 = p \,.\, q$ *ist.*

Beweis: Es ist $A \,.\, p = A \,.\, (A \,.\, r)$ und $A \,.\, q = A \,.\, (A \,.\, s)$, demnach

(12) $$(A \,.\, p) \,.\, (A \,.\, q) = [A \,.\, (A \,.\, r)] \,.\, [A \,.\, (A \,.\, s)] \geqq A \,.\, [(A \,.\, r) \,.\, (A \,.\, s)].$$

Da aber

(13) $$[a_l \,.\, (a_h \,.\, r)] \,.\, [a_{\bar{l}} \,.\, (a_{\bar{h}} \,.\, s)] = [a_l \,.\, (a_h \,.\, r)] \,.\, [a_l \,.\, (a_{\bar{h}} \,.\, s)]^{1}) = a_{\bar{h}} \,.\, [(a_h \,.\, r) \,.\, (a_{\bar{h}} \,.\, s)]$$

ist, so folgt daraus

(13′) $$[A \,.\, (A \,.\, r)] \,.\, [A \,.\, (A \,.\, s)] \leqq A \,.\, [(A \,.\, r) \,.\, (A. \, s)].$$

Aus (12) und (13′) folgt

$$H_{pq} = (A \,.\, p) \,.\, (A \,.\, q) = A \,.\, [(A \,.\, r) \,.\, (A \,.\, s)] \text{ und}$$

(14) $$H_{pq} = A \,.\, \sigma_1 + \cdots + A \,.\, \sigma_{\nu^2} = A \,.\, \tau_1 + \cdots + A \,.\, \tau_\nu,$$

was man ohne weiteres einsieht, indem man aus $(A \,.\, r) \,.\, (A \,.\, s)$ die Elemente σ_i der Reihe nach herausgreift und berücksichtigt, daß H_{pq} nur ν^2 Elemente hat.

4. Satz: Gilt für ein bestimmtes k von (11) *und für ein bestimmtes l von* (6) *die Beziehung*

(15) $$A \,.\, \tau_k = (A \,.\, p) \,.\, (a_l \,.\, q),$$

so ist H_{pq} ν-gliedrig und umgekehrt.

Wir beweisen zuerst den ersten Teil des Satzes. Zu diesem Zwecke bezeichnen wir mit $\vartheta(A \,.\, B)$ den Durchschnitt der beiden Komplexe A und B. Es sei H_{pq} ν^2-gliedrig, dann ist für $h = 1, 2, \ldots, \nu$

(16) $\vartheta(A \,.\, \tau_1, (A \,.\, p) \,.\, (a_h \,.\, q)) \geqq a_h \,.\, (p \,.\, q)$, da $\tau_1 = p \,.\, q$ ist.

Es kann also $A \,.\, \tau_k$ nicht $A \,.\, \tau_1$ sein, da $\vartheta(A \,.\, \tau_k, (A \,.\, p) \,.\, (a_h \,.\, q)) = 0$ für $h \neq l$ ist. Da aber $A \,.\, \tau_k = (A \,.\, p) \,.\, (a_l \,.\, q)$ ist, so wäre zufolge (16)

(17) $\vartheta(A \,.\, \tau_1, A \,.\, \tau_k) \geqq a_l \,.\, (p \,.\, q)$, was aber unmöglich ist, da alle $A\tau_i$, $i = 1, \ldots, \nu$ (im Falle H_{pq} ν^2-gliedrig) elementfremd sind. Es muß also H_{pq} ν-gliedrig sein, w. z. b. w.

Die Umkehrung des Satzes ist evident.

Zusatz zum Satz 4: Hat H_{pq} ν^2 Elemente, so hat eine Untergruppe $A \,.\, \tau_k$ mit einer Untergruppe $(A \,.\, p) \,.\, (a_l \,.\, q)$ genau ein Element gemeinsam.

Dies folgt aus den beiden Zerlegungen (6) und (11), denn hätten diese beiden Untergruppen zwei Elemente gemeinsam, so fielen sie als einfache Gruppen zusammen, und H_{pq} wäre ν-gliedrig.

5. Satz: Aus der Beziehung

(18) $$\vartheta(H_{pq}, H_{pr}) \neq 0$$

folgt $H_{pq} = H_{pr}$.

---

[1]) Es ist ein Element $a_{\bar{h}} \,.\, s$ in allen Gruppen $A \,.\, s$ enthalten, für welches die Relation $a_{\bar{l}} \,.\, (a_{\bar{h}} \,.\, s) = a_l \,.\, (a_{\bar{h}} \,.\, s)$ gilt, da $A \,.\, (A \,.\, s)$ eine ν-gliedrige Gruppe ist.

Für H_{pq} resp. H_{pr} gelten die Zerlegungen

(18′) $\quad H_{pq} = A \,.\, \tau_1 + \cdots + A \,.\, \tau_\nu, \qquad H_{pr} = A \,.\, \sigma_1 + \cdots + A \,.\, \sigma_\nu,$

(wobei nicht notwendig die $A \,.\, \tau_i$ resp. $A \,.\, \sigma_i$ alle verschieden sind). Sei nach Voraussetzung

(19) $\quad (a_h \,.\, p) \,.\, (a_k \,.\, q) = (a_{\bar{h}} \,.\, p) \,.\, (a_{\bar{k}} \,.\, r)$, so folgt daraus

(20) $\quad (A \,.\, p) \,.\, (a_k \,.\, q) = (A \,.\, p) \,.\, (a_{\bar{k}} \,.\, r).$

Wir zeigen nun, daß irgend eine Gruppe $A \,.\, \tau_i$ von H_{pq} mit einer $A \,.\, \sigma_j$ von H_{pr} identisch ist, d. h. dann, daß $H_{pq} = H_{pr}$ ist.

In der Tat! Sei $A \,.\, \tau_i$ diese Gruppe, so hat sie mit $(A \,.\, p) \,.\, (a_k \,.\, q)$ sicher ein Element x gemeinsam, also auch nach (20) mit $(A \,.\, p) \,.\, (a_{\bar{k}} \,.\, r)$. Letztere Gruppe aber hat dieses Element x ihrerseits mit einem $A \,.\, \sigma_j$ von H_{pr} gemeinsam.

Somit haben $A \,.\, \tau_i$ und $A \,.\, \sigma_j$ das Element x gemeinsam und fallen demnach zusammen.

Zuzatz zum Satz 5: *Enthält die Gruppe* $(A \,.\, p) \,.\, l$ *ein Element* a_i *der Gruppe* A, *so ist* $(A \,.\, p) \,.\, l \equiv A$.

In der Tat, da $A \,.\, (A \,.\, p) = A \,.\, r$ ist, so ist zufolge § 5, I. II. Hilfssatz: $A = (A \,.\, p) \,.\, s$. Die Komplexe $A \,.\, [(A \,.\, p) \,.\, h] = [(A \,.\, p) \,.\, s] \,.\, [(A \,.\, p) \,.\, l]$ und $A \,.\, A = [(A \,.\, p) \,.\, s] \,.\, [(A \,.\, p) \,.\, s] = A$ haben das Element a_i gemeinsam und sind somit identisch. Da $A \,.\, A = \nu$-gliedrig ist, so muß also der Komplex $A \,.\, [(A \,.\, p) \,.\, l$ ν-gliedrig sein, und es gilt:

$$A \,.\, [(A \,.\, p) \,.\, l] = A \,.\, A = A, \text{ d. h. } (A \,.\, p) \,.\, l = A, \quad \text{q. e. d.}$$

6. Satz: *Es gilt für die Untergruppen* (11) *die Relation*

(21) $\qquad (A \,.\, \tau_k) \,.\, (A \,.\, \tau_l) = A \,.\, (\tau_k \,.\, \tau_l).$

Beweis: Da H_{pq} eine Gruppe ist, so ist $(A \,.\, \tau_k) \,.\, (A \,.\, \tau_l) < H_{pq}$. Wäre $(A \,.\, \tau_k) \,.\, (A \,.\, \tau_l)$ ν^2-gliedrig, so wäre

(22) $\quad (A \,.\, \tau_k) \,.\, (A \,.\, \tau_l) = H_{pq}$; da aber $(A \,.\, \tau_k) \,.\, (A \,.\, \tau_k) = (A \,.\, \tau_k) < H_{pq}$

ist, so wäre

(22′) $\qquad \vartheta[(A \,.\, \tau_k) \,.\, (A \,.\, \tau_l), \; (A \,.\, \tau_k) \,.\, (A \,.\, \tau_k)] = A \,.\, \tau_k,$

also zufolge Satz 5

(22″) $\qquad (A \,.\, \tau_k) \,.\, (A \,.\, \tau_l) = A \,.\, \tau_k,$

d. h. $(A \,.\, \tau_k) \,.\, (A \,.\, \tau_l)$ müßte ν-gliedrig sein, demnach führt die Annahme, $(A \,.\, \tau_k) \,.\, (A \,.\, \tau_l)$ sei ν^2-gliedrig, zu einem Widerspruch. Es muß das $(A \,.\, \tau_k) \,.\, (A \,.\, \tau_l)$ ν-gliedrig, also $A \,.\, (\tau_k \,.\, \tau_l)$ gleich sein, w. z. b. w.

Sei G eine Gruppe und A eine einfache Untergruppe von G, so gilt dann die Darstellung

(23) $\qquad G = A \,.\, l_0 + A \,.\, l_1 + \cdots + A \,.\, l_s, \quad$ wobei $\quad l_0 < A$

ist. Wir erinnern, daß $A \,.\, (A \,.\, p) = A \,.\, t$ gilt. Im allgemeinen braucht $(A \,.\, l_j) \,.\, (A \,.\, p) =$ ν-gliedrige Gruppe nicht zuzutreffen. Die Gruppen $A \,.\, l_j$ der Eigenschaft

(24) $\qquad (A \,.\, l_j) \,.\, (A \,.\, l_h) = A \,.\, (l_j \,.\, l_h) \quad$ für jedes $\quad h = 0, 1, \ldots, s,$

zu denen A gehört, seien mit $A \,\widetilde{.}\, l_j$ bezeichnet.

Sei (24′) $A \,\widetilde{.}\, l_0 = A$, $A \,\widetilde{.}\, l_1, \ldots, A \,\widetilde{.}\, l_r$ die Gesamtheit dieser Gruppen, so gilt für sie

7. Satz: *Die Gruppen* (24′) *sind Elemente einer distributiven Gruppe* Γ. *Mit* Σ *sei die Untergruppe von* G *bezeichnet, die alle Elemente von* G *enthält, die in Elementen von* Γ *auftreten.*

Beweis: Wir zeigen, daß

(25) $\qquad (A \,\widetilde{.}\, l_k) \,.\, (A \,\widetilde{.}\, l_h) = \widetilde{A \,.\, (l_k \,.\, l_h)}$

ist. Nach Voraussetzung gilt

$$(26)\qquad \begin{cases} (A\widetilde{.}l_k).(A.l_x) = A.(l_k.l_x) \\ (A\widetilde{.}l_h).(A.l_x) = A.(l_h.l_x), \end{cases}$$

speziell also

$$(25')\qquad (A\widetilde{.}l_k).(A\widetilde{.}l_h) = A.(l_k.l_h).$$

Aus (26) schließen wir $A\widetilde{.}l_k = (A.l_x).p$, $A\widetilde{.}l_h = (A.l_x).q$, somit $(A\widetilde{.}l_k).(A\widetilde{.}l_h) = (A.l_x).(p.q)$. Nun ist $\widetilde{A.(l_k.l_h)}$ zu beweisen, d. h. $[A.(l_k.l_h)].(A.l_x) = \nu$-gliedrig. In der Tat gilt $[A.(l_k.l_h)].(A.l_x) = [(A.l_x).(p.q)].(A.l_x) = \nu$-gliedrig, w. z. b. w.

8. Satz: Es sei G eine ausgezeichnete Gruppe (siehe § 5), A eine einfache Gruppe von G der Ordnung ν und R eine A enthaltende Untergruppe von G der Ordnung ν^2. Ist

$$(26')\qquad R = A\cdot l_1 + A\cdot l_2 + \cdots + A\cdot l_\nu, \quad \textit{wobei } l_1 < A \textit{ ist,}$$

eine Zerlegung vermittels der Gruppe A, so ist $A.l_h = A\widetilde{.}l_h$, $h = 1, \ldots, \nu$.

Beweis: Es sei

$$(27)\qquad G = R + R\cdot p_1 + \cdots + R\cdot p_t.$$

Aus (26') folgt

$$(28)\qquad R.p_k = (A.l_1).p_k + \cdots + (A.l_\nu).p_k = (A.p_k).(l_1.p_k) + \cdots + (A.p_k).(l_\nu.p_k), \qquad k = 1, \ldots, t.$$

Wir zeigen, daß $R.p_k$ von der Form

$$(28')\qquad R.p_k = A.s_1^{(k)} + \cdots + A.s_\nu^{(k)}$$

ist. Da $A.(A.p_k)$ ν-gliedrig ist, so ist zufolge § 5, I. II. Hilfssatz: $A = (A.p_k).\sigma$. Betrachten wir jetzt die beiden Komplexe

(29) $A.(A.p_k) = [(A.p_k).\sigma].(A.p_k)$ und $A.[(A.p_k).(l_r.p_k)] = [(A.p_k).\sigma].[(A.p_k).(l_r.p_k)]$, $r = 1, \ldots, \nu$. Sie sind beide in der Gruppe $R.(R.p_k) = R.p_t$ enthalten, demnach müssen sie zufolge Satz 5 entweder zusammenfallen, oder beide ν-gliedrig sein. Da aber der erste Komplex ν-gliedrig ist, so ist es auch der zweite, und die Gruppe $(A.p_k).(l_r.p_k) = (A.l_r).p_k$ ist von der Form $A.s_\nu^{(k)}$, d. h. es ist

$$R.p_k = A.s_1^{(k)} + \cdots + A.s_\nu^{(k)}.$$

Ist $A.\tau$ irgendeine Untergruppe von G, so fällt sie zufolge (27) und (28') mit einer Untergruppe, z. B. $A.s_r^{(k)}$, zusammen. Indem man jetzt die beiden Komplexe

$$(30)\qquad A.(A.s_r^{(k)}) \text{ und } (A.l_k).(A.s_r^{(k)}), \quad k = 1, \ldots, \nu$$

betrachtet, schließt man auf dieselbe Weise wie vorher, da $A.(A.s_r^{(k)})$ ν-gliedrig ist, daß auch $(A.l_k).(A.s_r^{(k)})$ ν-gliedrig ist, d. h. daß $A.l_k = A\widetilde{.}l_k$ ist, w. z. b. w.

9. Satz: Jede ausgezeichnete Gruppe G ist entweder identisch mit Σ[1]) oder enthält mindestens ν Untergruppen $A\widetilde{.}l_k$.

Beweis: Ist für jedes $(A.p)$ und $(A\cdot q)$

$$(31)\qquad (A.p).(A.q) = A.(p.q), \quad \text{so ist } G \equiv \Sigma.$$

Ist das nicht der Fall, so existiert mindestens eine Untergruppe $A.p$, so daß $(A.p).(A.q) = H_{pq}$ ν^2-gliedrig ist. Es sei l ein Element von G, von der Art, daß

$$(32)\qquad [a_1.(p.q)].l = a_i, \quad (a_1, a_i \text{ Elemente von } A).$$

Die Gruppe $(H_{pq}).l$ enthält zufolge Zusatz zu Satz 5 die Gruppe A, es ist also

$$(33)\qquad (H_{pq}).l = A + A.\varrho_1 + \cdots + A.\varrho_{\nu-1}.$$

Die Gruppe $(H_{pq}).l$ hat demnach die Eigenschaften der Gruppe R des Satzes 8, demnach ist $A.\varrho_k = A\widetilde{.}\varrho_k$, $k = 1, 2, \ldots, \nu$, q. e. d.

---

[1]) d. h. jede Untergruppe $A.p$ der Gruppe G ist eine $\widetilde{A.p}$-Untergruppe.

Bemerkung: Ist G eine ausgezeichnete Gruppe von der Ordnung N, wobei $N = \prod_{i=1}^{n} p_i$ ist und p_i Primzahlen sind, von der Art, daß $p_i \neq p_k$ ist, wenn $i \neq k$ ist, so gilt dann für die Gruppe G der Relation

$$(34) \qquad (A \,.\, p) \,.\, (A \,.\, q) = A \,.\, (p \,.\, q)$$

für jede einfache Untergruppe A von G.

In der Tat! Wäre das nicht der Fall, so müßte $(A \,.\, p) \,.\, (A \,.\, q) = H_{pq}$ eine ν^2-gliedrige Gruppe sein. Da G eine ausgezeichnete Gruppe ist, so müßte dann zufolge § 4, Satz 1 N durch ν^2 teilbar sein, was gegen die Voraussetzung ist. Es gilt demnach (34). Gilt aber die Beziehung (34) für alle einfachen Untergruppen in G, so gilt sie auch für alle Untergruppen in G überhaupt (wie man leicht zeigen kann).

Da jede symmetrische distributive Gruppe G von der Ordnung $N = \prod_{i=1}^{n} p_i$, wobei N durch 3 nicht teilbar ist, eine ausgezeichnete Gruppe ist, so gilt für symmetrische Gruppen dieser Eigenschaften die Beziehung (34).

II. Nachtrag: Einiges über die Struktur distributiver Gruppen.

Sei $G = \{a_1, a_2, \ldots, a_\nu\}$ eine distributive Gruppe, so bilden wir aus zwei Elementen a_1 und a_2 den folgenden l-Cyklus (links-Cyklus) $a_1 \,.\, a_2 = a_3$, $a_1 \,.\, a_3 = a_4, \ldots, a_1 \,.\, a_{h-1} = a_h$. $a_1, a_2, \ldots, a_h$ sollen alle verschieden sein, dagegen möge $a_1 \,.\, a_h$ bereits in der Reihe $a_1, a_2, \ldots, a_h$ enthalten sein.

$a_1 \,.\, a_h$ muß von a_1 und a_h verschieden sein, ist also $a_1 \,.\, a_h = a_i$, so muß $i > 1$ sein, wir behaupten $i = 2$; wäre $i > 2$, so folgt aus

$$a_1 \,.\, a_h = a_i \text{ und } a_h = a_1 \,.\, a_{h-1},\ a_i = a_1 \,.\, a_{i-1},$$

daß $a_1 \,.\, a_{h-1} = a_{i-1}$; also müßte bereits $a_1 a_{h-1} = a_h = a_{i-1}$ in der Reihe $a_1, a_2, \ldots, a_{h-1}$ enthalten sein, gegen die Voraussetzung.

Der Cyklus lautet demnach:

$$(\alpha) \qquad a_1, a_2, a_3 = a_1 \,.\, a_2,\quad a_4 = a_1 \,.\, a_3,\quad a_h = a_1 \,.\, a_{h-1},\quad a_2 = a_1 \,.\, a_h.$$

Zwischen a_1 und a_2 besteht dann die Relation:

$$a_1^{h-1} \,.\, a_2 = a_2.$$

Der Gleichung $a_1^{h-1} \,.\, x = x$ genügen die Elemente einer Untergruppe, die die Elemente des Cyklus (α) enthält.

Zwischen je zwei Elementen a, b dieser Untergruppe (§ 2) besteht dann die Relation

$$a^{h-1} \,.\, b = b, \text{ also gilt auch } a_2^{h-1} \,.\, a_1 = a_1 \text{ usw.}$$

Wir nennen $h - 1$ den Grad des l-Cyklus a_1, a_2. Sei $A\{a_1 a_2, \ldots, a_\nu\}$ eine einfache Gruppe, so ist der Grad G des l-Cyklus je zweier Elemente a_p und a_q, $a_p \neq a_q$ eine der einfachen Gruppe charakteristische Zahl, d. h. dieser l-Grad ist von der besonderen Wahl der Elemente a_p und a_q unabhängig.

Beweis: Je zwei Elemente von A, a_p, a_q, haben einen bestimmten l-Grad g_{pq}; unter den ganzen Zahlen g_{pq} muß es eine kleinste geben. a_i und a_k sei eine Kombination, deren Cyklusgrad g sei, dann gilt $a_i^g \,.\, a_k = a_k$. Die Elemente x, die die Gleichung $a_i^g \,.\, x = x$ lösen, bilden eine Untergruppe von A die, da sie a_i und a_k enthält, mit A, da A einfach ist, zusammenfallen muß. Demnach gilt

$$a_p^g \,.\, a_q = a_q \text{ für alle Elemente von } A,$$

d. h. je zwei Elemente a_p und a_q haben den Cyklusgrad g, q. e. d.

Sei A eine einfache Gruppe, N ihre Ordnung und g ihr l-Cyklusgrad. Dann bilden wir mit a_1 und a_2 den Cyklus

$$(\alpha) \qquad a_1, a_2, a_3 = a_1 \cdot a_2, \ldots, a_{g+1} = a_1 \cdot a_g \ (a_2 = a_1 \cdot a_{g+1}).$$

Sind mit $a_1, a_2, \ldots, a_{g+1}$ noch nicht alle Elemente erschöpft, so sei a_{g+2} ein noch nicht in (α) enthaltenes Element. Wir bilden

$$(\beta) \qquad a_1, a_{g+2}, a_{g+3} = a_1 \cdot a_{g+2}, \ldots, a_{2g+1} = a_1 \cdot a_{2g} \ (a_{g+2} = a_1 \cdot a_{2g+1}).$$

Wäre $a_i = a_{g+k}$, $i, k = 2, 3, \ldots, g+1$, so folgte

$$a_1 \cdot a_i = a_{i+1} = a_1 \cdot a_{g+k} = a_{g+k+1} \qquad \text{usw.},$$

endlich $a_{g+2} = a_l$, gegen die Voraussetzung.

Somit sind die Reihen (α) und (β) vom gemeinsamen Element a_1 abgesehen teilerfremd.

Sei durch (α) und (β) A noch nicht erschöpft, so bilden wir mit a_1, a_{2g+2} einen neuen Cyklus usw., bis A erschöpft ist. Jede Reihe $(\alpha), (\beta) \ldots$ enthält $g+1$ Elemente, somit gilt $N = \sigma g + 1$, wobei σ ganze Zahl ist, oder

$$N \equiv 1 \bmod g.$$

Satz: Ist N die Ordnung und g der Cyklusgrad einer einfachen Gruppe, so gilt

$$N \equiv 1 \bmod g.$$

Das gleiche gilt natürlich für den r-Grad (Grad des rechtsseitigen Cyklus); wir haben nur die Verknüpfung

$$a_i \circ a_k = a_k \cdot a_i$$

anstelle von $a_i \cdot a_k$ zu betrachten, für die das System $A\{a_1, a_2, \ldots, a_\nu\}$ ebenfalls eine distributive Gruppe bildet.

Im allgemeinen ist der l-Grad vom r-Grad verschieden.

Sei $A\{a_0, a, \ldots, a_\nu\}$ ein System, dessen Elemente einen einzigen Cyklus bilden:

$$a_0, a_1, a_2 = a_0 \cdot a_1, a_3 = a_0 \cdot a_2, \ldots, a_\nu = a_0 \cdot a_{\nu-1} \ (a_0 \cdot a_\nu = a_1).$$

Wir zeigen dann, daß aus der Gültigkeit der Axiome I und II und der linksseitigen Distributivität die rechtsseitige Distributivität für das System A folgt. Da für solche Systeme auch die Homogenitätseigenschaft gilt, ist der Beweis gebracht, sobald

$$(a_i \cdot a_k) \cdot a_0 = (a_i \cdot a_0) \cdot (a_i \cdot a_0)$$

gilt. Wir bezeichnen mit a_ϱ das Element, für das

$$a_0 \cdot a_1 = a_\varrho \cdot a_0$$

gilt. Durch linksseitige Verknüpfung mit a_0 erhalten wir

$$(\alpha) \quad \left\{ \begin{array}{l} a_0 \cdot a_{[t]} = a_{[\varrho+t-1]} \cdot a_0, \quad a_{\varrho+t-1} = a_k \text{ gesetzt}, \quad t = k + 1 - \varrho \\ a_0 \cdot a_{[k+1-\varrho]} = a_{[k]} \cdot a_0 \end{array} \right\}.$$

Dabei ist $[i]$ jene Zahl der Reihe $1, 2, \ldots, \nu$, für die

$$[i] \equiv i \bmod \nu$$

gilt. Nun folgt aus (α), (β)

$$\begin{aligned} (a_t \cdot a_0) \cdot (a_s \cdot a_0) = [a_0 \cdot a_{[t+1-\varrho]}] \cdot [a_0 \cdot a_{s+1-\varrho}] &= a_0 \cdot [a_{[t+1-\varrho]} \cdot a_{[s+1-\varrho]}] \\ &= a_0 \cdot a_\mu = a_{[\varrho+\mu-1]} \cdot a_0, \end{aligned}$$

wobei

$$a_\mu = a_{[t+1-\varrho]} \cdot a_{[s+1-\varrho]} \qquad \text{ist.}$$

Linksseitig $(\varrho - 1)$-mal mit a_0 verknüpft ergibt dies:

$a_t \cdot a_s = a_{[\mu+\varrho-1]}$, somit lautet (β):

$(a_t \cdot a_0)(a_s \cdot a_0) = (a_t \cdot a_s) \cdot a_0$, q. e. d.

Eingegangen im November 1927.