XXVIII.

Über Zerlegungen von Zahlen durch ihre größten gemeinsamen Teiler.

[Festschrift der Technischen Hochschule zu Braunschweig bei Gelegenheit der 69. Versammlung Deutscher Naturforscher und Ärzte, S. 1—40 (1897).]

Liegt ein endliches System von natürlichen Zahlen vor, und bildet man alle größten gemeinsamen Teiler von zwei oder mehreren dieser Zahlen, so werden die letzteren hierdurch auf mannigfaltige Weise in Faktoren zerlegt. Obgleich nun diese Faktoren im allgemeinen bekanntlich keine Primzahlen sind, so leisten sie doch für manche Untersuchungen ausreichende Dienste, und es verlohnt sich daher wohl der Mühe, die hierbei auftretenden Gesetze im Zusammenhang darzustellen. Dies ist der nächste Gegenstand des vorliegenden Aufsatzes, doch soll zugleich die ursprüngliche Aufgabe soviel wie möglich verallgemeinert und auch auf Gebiete übertragen werden, in denen es gar keine Zerlegungen in eigentliche Primfaktoren gibt. Hierbei verliert zwar die Untersuchung ihr arithmetisches Gepräge fast ganz, so daß sie mathematische Kenntnisse kaum noch voraussetzt, aber zugleich treten die Gesetze und ihre Gründe deutlicher hervor, und ich darf hoffen, daß in dieser Hinsicht meine Arbeit doch einigen Mathematikern willkommen sein mag.

§ 1.

Drei Zahlen.

Sind a, b, c drei gegebene natürliche Zahlen, so will ich den größten gemeinsamen Teiler

$$(1)\quad \begin{cases} \text{der Zahlen } b, c & \text{mit } a_1, \\ \text{„ „ } c, a & \text{„ } b_1, \\ \text{„ „ } a, b & \text{„ } c_1, \\ \text{„ „ } a, b, c & \text{„ } d \end{cases}$$

bezeichnen, dann kann man, weil d offenbar auch der größte gemeinsame Teiler von je zwei der drei Zahlen a_1, b_1, c_1 ist,

$$(2) \qquad a_1 = da', \quad b_1 = db', \quad c_1 = dc'$$

setzen, wo a', b', c' relative Primzahlen sind, womit in üblicher Weise ausgedrückt sein soll, daß je zwei äußerlich verschiedene dieser Zahlen, z. B. b', c', relative Primzahlen sind. Hieraus folgt, daß $db'c'$ das kleinste gemeinsame Vielfache der Zahlen b_1, c_1 ist, und da a zufolge 1 durch beide teilbar ist, so erhält man die Zerlegungen

$$(3) \qquad a = db'c'a'', \quad b = dc'a'b'', \quad c = da'b'c'',$$

wo a'', b'', c'' ebenfalls natürliche Zahlen sind. Die drei gegebenen Zahlen a, b, c erscheinen daher als Produkte von je vier der sieben Zahlen d, a', b', c', a'', b'', c'', welche wir die Kerne des Systems a, b, c nennen wollen (vgl. § 7). Zugleich ergibt sich aus der Bedeutung von a_1, b_1, c_1, daß jedes der drei Paare

$$c'b'' \text{ und } b'c'', \quad a'c'' \text{ und } c'a'', \quad b'a'' \text{ und } a'b''$$

aus zwei relativen Primzahlen besteht; hierin liegt zunächst wieder, daß die drei Zahlen a', b', c' relative Primzahlen sind; dasselbe gilt offenbar von den drei Zahlen a'', b'', c'', und außerdem besteht jedes der drei Paare

$$a' \text{ und } a'', \quad b' \text{ und } b'', \quad c' \text{ und } c''$$

aus zwei relativen Primzahlen, während die anderen Paare, wie a' und b'', diese Eigenschaft nicht zu besitzen brauchen. Ist z. B.

$$a = 420, \quad b = 800, \quad c = 216,$$

so findet man

$$\begin{aligned} a_1 &= 8, \quad b_1 = 12, \quad c_1 = 20, \quad d = 4, \\ a' &= 2, \quad b' = 3, \quad c' = 5, \\ a'' &= 7, \quad b'' = 20, \quad c'' = 9. \end{aligned}$$

Zufolge (2) und (3) lassen sich die sieben Kerne d, a', b', c', a'', b'', c'' durch die drei gegebenen Zahlen a, b, c und die aus ihnen gebildeten vier größten gemeinsamen Teiler a_1, b_1, c_1, d in folgender Weise darstellen:

$$(4) \qquad \begin{cases} d = d, \\ a' = \dfrac{a_1}{d}, \quad b' = \dfrac{b_1}{d}, \quad c' = \dfrac{c_1}{d}, \\ a'' = \dfrac{ad}{b_1c_1}, \quad b'' = \dfrac{bd}{c_1a_1}, \quad c'' = \dfrac{cd}{a_1b_1}. \end{cases}$$

Diese Kerne bleiben, mit Ausnahme von d, ungeändert, wenn man a, b, c durch drei beliebige, ihnen proportionale Zahlen ersetzt, welche auch gebrochen sein dürfen, falls man unter dem größten gemeinsamen Teiler von rationalen Zahlen u, v, w... immer diejenige positive rationale Zahl e versteht, für welche die Quotienten

$$\frac{u}{e}, \quad \frac{v}{e}, \quad \frac{w}{e} \cdots$$

ganze Zahlen ohne gemeinsamen Teiler werden*).

Ersetzt man aber die drei Zahlen a, b, c durch drei ihnen umgekehrt proportionale Zahlen, z. B. durch bc, ca, ab oder durch a^{-1}, b^{-1}, c^{-1}, so vertauscht sich a' mit a'', b' mit b'', c' mit c''; diese Erscheinung steht in unmittelbarem Zusammenhang mit dem Dualismus zwischen den Begriffen des größten gemeinsamen Teilers und des kleinsten gemeinsamen Vielfachen**). Für jetzt mögen indessen folgende Bemerkungen genügen. Bezeichnet man das kleinste gemeinsame Vielfache

$$(5) \quad \begin{cases} \text{der Zahlen } b, c & \text{mit } a_2, \\ \text{„ „ } c, a & \text{„ } b_2, \\ \text{„ „ } a, b & \text{„ } c_2, \\ \text{„ „ } a, b, c & \text{„ } m, \end{cases}$$

so erhält man nach bekannten Regeln

$$(6) \quad \begin{cases} a_2 = \dfrac{bc}{a_1} = da'b'c'b''c'', \\ b_2 = \dfrac{ca}{b_1} = da'b'c'c''a'', \\ c_2 = \dfrac{ab}{c_1} = da'b'c'a''b''. \end{cases}$$

Da ferner nach dem Obigen a'' relative Primzahl zu $a'b''c''$ ist, so haben die Zahlen a und a_2 zufolge (3) und (6) den größten gemeinsamen Teiler $db'c'$, und da m zufolge (5) ihr kleinstes gemeinsames Vielfaches, also $m \cdot db'c' = aa_2$ ist, so ergibt sich

$$(7) \quad m = da'b'c'a''b''c'' = \frac{abcd}{a_1b_1c_1}.$$

*) Dirichlets Vorlesungen über Zahlentheorie, 4. Aufl., § 172, S. 515; dies Werk soll künftig mit D. zitiert werden.

**) Vgl. D. § 178, S. 555.

§ 2.

Vier Zahlen.

Hat man mehr als drei gegebene Zahlen zu betrachten, so wird eine andere Bezeichnungsweise zweckmäßig, deren Gebrauch jetzt erörtert werden soll. Die gegebenen Zahlen seien

(1) $$(1,0),\ (2,0),\ (3,0),\ (4,0)\ldots,$$

und man bezeichne den größten gemeinsamen Teiler

(2)
$$\begin{cases} \text{der Zahlen } (1,0),\ (2,0) \text{ mit } (12,0), \\ \text{„ „ } (1,0),\ (2,0),\ (3,0) \text{ mit } (123,0), \\ \text{„ „ } (1,0),\ (2,0),\ (3,0),\ (4,0) \text{ mit } (1234,0) \end{cases}$$

usw.,

wobei natürlich alle Ziffern miteinander vertauscht werden dürfen. Beschränken wir uns auf den nächsten Fall, wo vier Zahlen gegeben sind, so entstehen auf diese Weise elf größte gemeinsame Teiler, nämlich sechs von der Form (12,0), vier von der Form (123,0) und einer von der Form (1234,0). Dieser letzte ist offenbar zugleich der größte gemeinsame Teiler von je zweien der Form (123,0), (124,0), und folglich kann man

(3)
$$\begin{cases} (123,0) = (1234,0)\ (123,4), \\ (124,0) = (1234,0)\ (124,3), \\ (134,0) = (1234,0)\ (134,2), \\ (234,0) = (1234,0)\ (234,1) \end{cases}$$

setzen, wo die vier ganzen Zahlen

(4) $$(123,4),\ (124,3),\ (134,2),\ (234,1)$$

relative Primzahlen sind. Hieraus folgt z. B., daß das Produkt

$$(1234,0)\ (123,4)\ (124,3)$$

das kleinste gemeinsame Vielfache der beiden Zahlen (123,0), (124,0) ist; da andererseits diese letzteren Zahlen beide Teiler von (1,0) und (2,0), also auch Teiler von deren größtem gemeinsamen Teiler (12,0) sind, so muß der letztere auch durch das vorstehende Produkt teilbar sein. Man erhält daher die Zerlegungen

(5)
$$\begin{cases} (12,0) = (1234,0)\ (123,4)\ (124,3)\ (12,34), \\ (13,0) = (1234,0)\ (123,4)\ (134,2)\ (13,24), \\ (14,0) = (1234,0)\ (124,3)\ (134,2)\ (14,23), \\ (23,0) = (1234,0)\ (123,4)\ (234,1)\ (23,14), \\ (24,0) = (1234,0)\ (124,3)\ (234,1)\ (24,13), \\ (34,0) = (1234,0)\ (134,2)\ (234,1)\ (34,12), \end{cases}$$

in welchen sechs neue ganze Zahlen

$$(6) \qquad \begin{cases} (12,34),\ (13,24),\ (14,23), \\ (34,12),\ (24,13),\ (23,14) \end{cases}$$

auftreten. Setzt man nun

$$a = (12,0), \quad b = (13,0), \quad c = (14,0),$$

und wendet man auf diese drei Zahlen die Betrachtungen und Bezeichnungen des § 1 an mit Rücksicht auf (2), (3), (5), so ergibt sich

$$a_1 = (134,0), \quad b_1 = (124,0), \quad c_1 = (123,0), \quad d = (1234,0),$$
$$a' = (134,2), \quad b' = (124,3), \quad c' = (123,4),$$
$$a'' = (12,34), \quad b'' = (13,24), \quad c'' = (14,23),$$

also

$$m = (1234,0)\ (123,4)\ (124,3)\ (134,2)\ (12,34)\ (13,24)\ (14,23).$$

Da nun die Zahl (1,0) zufolge (2) durch jede der drei Zahlen a, b, c, also auch durch deren kleinstes gemeinsames Vielfaches m teilbar ist, so erhält man schließlich die folgenden Zerlegungen:

$$(7) \qquad \begin{cases} (1,0) = (1234,0)\ (123,4)\ (124,3)\ (134,2)\ (12,34)\ (13,24)\ (14,23)\ (1,234), \\ (2,0) = (1234,0)\ (123,4)\ (124,3)\ (234,1)\ (12,34)\ (23,14)\ (24,13)\ (2,134), \\ (3,0) = (1234,0)\ (123,4)\ (134,2)\ (234,1)\ (13,24)\ (23,14)\ (34,12)\ (3,124), \\ (4,0) = (1234,0)\ (124,3)\ (134,2)\ (234,1)\ (14,23)\ (24,13)\ (34,12)\ (4,123), \end{cases}$$

in welchen abermals vier neue ganze Zahlen:

$$(8) \qquad (1,234),\ (2,134),\ (3,124),\ (4,123)$$

auftreten, Aus (3), (5), (7) ergeben sich umgekehrt die Darstellungen der in (4), (6), (8) bezeichneten vierzehn Zahlen durch die fünfzehn in (1) und (2) definierten Zahlen; man erhält z. B.

$$(9) \qquad (123,4) = \frac{(123,0)}{(1234,0)},$$

$$(10) \qquad (12,34) = \frac{(12,0)\ (1234,0)}{(123,0)\ (124,0)},$$

$$(11) \qquad (1,234) = \frac{(1,0)\ (123,0)\ (124,0)\ (134,0)}{(12,0)\ (13,0)\ (14,0)\ (1234,0)}.$$

Fügen wir zu diesen Gleichungen noch die selbstverständliche

$$(12) \qquad (1234,0) = (1234,0)$$

hinzu, und nennen wir (wie in § 1) die fünfzehn Zahlen (4), (6), (8), (12) die Kerne des Systems (1) der vier gegebenen Zahlen, so erscheint jede der letzteren in (7) als Produkt von acht Kernen, und ebenso erscheinen in den Gleichungen (5), (3), (12) die aus den gegebenen

Zahlen gebildeten größten gemeinsamen Teiler (2) als Produkte von Kernen, während umgekehrt die fünfzehn Kerne in den Gleichungen (9), (10), (11), (12) durch die fünfzehn Zahlen (1) und (2) ausgedrückt sind.

§ 3.

Kombinationen.

Um diese Betrachtungen auf ein beliebiges System von n gegebenen Zahlen

$$(1,0),\ (2,0)\cdots(n,0)$$

auszudehnen, und um ihnen zugleich eine viel allgemeinere Bedeutung unterzulegen, ist es nötig, einige Bemerkungen über die Kombinationen $\alpha, \beta, \gamma\cdots$ vorauszuschicken, welche sich aus dem System der n verschiedenen Elemente

$$1, 2, \cdots, n$$

bilden lassen. Die letzteren, welche hier nicht als Zahlen, sondern nur als Unterscheidungszeichen aufzufassen sind und durch irgendwelche andere Zeichen ersetzt werden dürften, bilden zugleich die Kombinationen ersten Grades. Jedes System α von r verschiedenen solchen Elementen heißt bekanntlich eine Kombination $r$ten Grades; hierbei kommt es auf die Reihenfolge, in welcher die Elemente des Systems α genannt oder geschrieben werden, gar nicht an, und man kann die Kombination selbst (wie in § 2) am einfachsten durch die natürliche Folge ihrer Elemente bezeichnen, so daß z. B. 235 die aus den drei Elementen 2, 3, 5 bestehende Kombination bedeutet; wenn freilich $n > 9$ ist, so müssen die Elemente einer Kombination deutlicher voneinander getrennt werden. Eine Kombination α ist also bestimmt, wenn über jedes der n Elemente $1, 2, \cdots, n$ die Entscheidung getroffen ist, ob es in α aufgenommen wird oder nicht; läßt man daher — was bekanntlich sehr zweckmäßig ist — auch die leere Kombination 0ten Grades zu, welche gar kein Element enthält und im folgenden immer mit 0 bezeichnet werden soll, so ist 2^n die Anzahl aller verschiedenen Kombinationen. Wenn jedes Element von α auch Element der Kombination β ist, so heißt α ein Teil von β, und wenn zugleich β auch ein Teil von α ist, so ist α identisch mit β, was immer durch $\alpha = \beta$ ausgedrückt wird. Die Kombination 0 ist ein Teil von jeder Kombination.

Unter der Summe $\alpha + \beta$ von zwei Kombinationen α, β soll die Kombination verstanden werden, welche aus allen in α oder in β

(oder in beiden) enthaltenen Elementen besteht, während ihr Durchschnitt $\alpha - \beta$ aus denjenigen Elementen bestehen soll, welche beiden Kombinationen α, β gemeinsam angehören; ist kein solches gemeinsames Element vorhanden, also $\alpha - \beta = 0$, so sollen α, β fremde Kombinationen heißen. Die Kombination 0 ist fremd zu jeder Kombination.

Um diese einfachen Begriffe durch ein Beispiel zu erläutern, wähle ich die drei Kombinationen

$$\alpha = 2347, \quad \beta = 1357, \quad \gamma = 1267;$$

dann wird

$$\beta + \gamma = 123567, \quad \gamma + \alpha = 123467, \quad \alpha + \beta = 123457,$$
$$\beta - \gamma = 17, \qquad \gamma - \alpha = 27, \qquad \alpha - \beta = 37.$$

Man überzeugt sich nun ohne weiteres, daß für diese beiden Operationen $\pm$ die folgenden sechs Fundamentalgesetze gelten, deren Inbegriff wir mit A bezeichnen wollen:

$$(1') \qquad \alpha + \beta = \beta + \alpha,$$
$$(1'') \qquad \alpha - \beta = \beta - \alpha,$$
$$(2') \qquad (\alpha + \beta) + \gamma = \alpha + (\beta + \gamma),$$
$$(2'') \qquad (\alpha - \beta) - \gamma = \alpha - (\beta - \gamma),$$
$$(3') \qquad \alpha + (\alpha - \beta) = \alpha,$$
$$(3'') \qquad \alpha - (\alpha + \beta) = \alpha.$$

Die vier Doppelgesetze (1), (2) spricht man bekanntlich so aus daß jede der beiden Operationen symmetrisch (kommutativ) und assoziativ ist, und hieraus folgt (vgl. D. § 2), daß die Bildung der Summe oder des Durchschnitts von drei oder mehr Kombinationen von der Reihenfolge ganz unabhängig ist, nach welcher man immer ein Paar der vorhandenen Kombinationen auswählt, um daraus die Summe oder den Durchschnitt zu bilden. Durch das letzte Doppelgesetz (3) treten aber die beiden Operationen in eine dualistische Verbindung, aus welcher zunächst

$$(4') \qquad \alpha + \alpha = \alpha,$$
$$(4'') \qquad \alpha - \alpha = \alpha$$

folgt; denn (4') geht unmittelbar aus (3') hervor, wenn man β durch $(\alpha + \beta)$ ersetzt und (3'') berücksichtigt, und in ähnlicher Weise folgt (4'') aus (3'').

Nun leuchtet freilich die Wahrheit dieses abgeleiteten Doppelgesetzes (4) auch unmittelbar aus dem Begriff der Operationen $\pm$ ein,

aber diese Ableitbarkeit ist doch an sich nicht ohne Bedeutung. Ganz anders verhält es sich nämlich mit dem folgenden Doppelgesetz:

$$(5') \qquad (\alpha - \beta) + (\alpha - \gamma) = \alpha - (\beta + \gamma),$$
$$(5'') \qquad (\alpha + \beta) - (\alpha + \gamma) = \alpha + (\beta - \gamma),$$

welches aus den obigen sechs Fundamentalgesetzen A schlechterdings nicht ableitbar ist, wie später (in § 4) noch weiter besprochen werden soll; hier ist es vielmehr erforderlich, nochmals auf die Bedeutung der Symbole zurückzugehen. Bedeutet μ die linke, ν die rechte Seite der Gleichung (5'), so haben wir zu zeigen, daß jedes Element μ' von μ auch in ν, und ebenso, daß jedes Element ν' von ν auch in μ enthalten ist. Zufolge des Summenbegriffes ist μ' in $(\alpha - \beta)$ oder in $(\alpha - \gamma)$ enthalten, und da der Satz zufolge (1') symmetrisch in bezug auf β, γ ist, so dürfen wir das erstere annehmen; dann ist μ' gemeinsames Element von α und β, und da jedes Element von β auch in $(\beta + \gamma)$ enthalten ist, so ist μ' auch in dem Durchschnitt ν der Kombinationen α und $(\beta + \gamma)$ enthalten. Umgekehrt, jedes Element ν' dieses Durchschnittes ν ist gewiß in α und außerdem in β oder γ, also in einem der beiden Durchschnitte $(\alpha - \beta)$, $(\alpha - \gamma)$, mithin auch in deren Summe μ enthalten, w. z. b. w.

Auf ganz ähnliche Weise ließe sich der Satz (5'') beweisen, was wir dem Leser überlassen; aber es ist bemerkenswert, daß dieser Satz schon eine notwendige Folge des Satzes (5') und der Gesetze A ist. Ersetzt man nämlich α, β, γ in (5') bzw. durch $\alpha + \gamma$, α, β, so folgt

$$[(\alpha + \gamma) - \alpha] + [(\alpha + \gamma) - \beta] = (\alpha + \gamma) - (\alpha + \beta),$$

was zufolge A zunächst die Form

$$(6'') \qquad (\alpha + \beta) - (\alpha + \gamma) = \alpha + [\beta - (\alpha + \gamma)]$$

annimmt; da ferner aus (5'), wenn α mit β vertauscht wird, sich

$$\beta - (\alpha + \gamma) = (\alpha - \beta) + (\beta - \gamma)$$

ergibt, so geht vermöge A die rechte Seite von (6'') in

$$\alpha + [(\alpha - \beta) + (\beta - \gamma)] = [\alpha + (\alpha - \beta)] + (\beta - \gamma) = \alpha + (\beta - \gamma)$$

über, womit der Satz (5'') bewiesen ist.

Da das System A in dem Sinne dualistisch ist, daß es sich durch die Vertauschung der beiden Operationen $\pm$ vollständig reproduziert, so ist offenbar der Satz (5') umgekehrt eine notwendige Folge von (5'')

und A; wollte man dies, was aber nicht mehr nötig ist, auf dieselbe Weise wie oben dartun, so würde der Weg über den Zwischensatz

$$(6') \qquad (\alpha - \beta) + (\alpha - \gamma) = \alpha - [\beta + (\alpha - \gamma)]$$

führen, welcher das Gegenstück zu dem Satz (6″) bildet.

Auf die allgemeinen Beziehungen zwischen den Gesetzen A und den vier Sätzen (5), (6) werde ich im folgenden § 4 noch näher eingehen, obgleich diese Untersuchung für unseren eigentlichen Gegenstand nicht erforderlich ist. Dagegen werden wir später (in §§ 7, 8) Gebrauch zu machen haben von dem folgenden

Satz. Genügen die vier Kombinationen α, β, γ, δ der Bedingung

$$(7) \qquad \alpha + \beta = \gamma + \delta,$$

so gibt es immer drei Kombinationen ϱ, σ, ω, welche den Bedingungen

$$(8) \qquad \beta = \varrho + \omega, \quad \delta = \sigma + \omega,$$

$$(9) \qquad \alpha + \varrho = \gamma + \sigma = \alpha + \gamma$$

genügen.

Der Beweis ergibt sich unmittelbar aus den obigen Sätzen, ohne daß es nötig wäre, auf die Bedeutung unserer Zeichen zurückzukommen. Setzt man nämlich

$$\varrho = \beta - \gamma, \quad \sigma = \alpha - \delta, \quad \omega = \beta - \delta$$

und

$$\tau = \alpha - \gamma,$$

so fließen aus dem Satze (5′) in Verbindung mit der Annahme (7) und mit dem Satze (3″) die Relationen

$$\begin{aligned} \sigma + \tau &= \alpha - (\gamma + \delta) = \alpha - (\alpha + \beta) = \alpha, \\ \varrho + \omega &= \beta - (\gamma + \delta) = \beta - (\alpha + \beta) = \beta, \\ \varrho + \tau &= \gamma - (\alpha + \beta) = \gamma - (\gamma + \delta) = \gamma, \\ \sigma + \omega &= \delta - (\alpha + \beta) = \delta - (\gamma + \delta) = \delta, \end{aligned}$$

deren zweite und vierte mit (8) übereinstimmen, während aus den beiden anderen folgt, daß jede der drei in (9) auftretenden Kombinationen $= \varrho + \sigma + \tau$ ist, w. z. b. w.

Der Vollständigkeit wegen erwähnen wir ferner, daß offenbar immer

$$(10) \qquad \alpha + 0 = \alpha, \quad \alpha - 0 = 0$$

ist, und um die späteren Untersuchungen nicht zu unterbrechen, fügen wir noch folgende Bemerkungen hinzu. Nennt man eine Kombination

paar oder unpaar, je nachdem ihr Grad gerade oder ungerade ist, so besitzt jede Kombination α, deren Grad $r > 0$ ist, offenbar ebenso viele paare wie unpaare Teile, nämlich 2^{r-1}; die ersteren, zu denen immer die Kombination 0 gehört, sollen mit α'', die letzteren mit α' bezeichnet werden. Die Kombination 0 dagegen besitzt nur einen einzigen, und zwar paaren Teil, nämlich 0 selbst. Sind nun α, β irgend zwei fremde Kombinationen, ist also $\alpha - \beta = 0$, so leuchtet ein, daß die paaren Teile $(\alpha + \beta)''$ der Summe $(\alpha + \beta)$ mit allen Kombinationen von der Form $\alpha'' + \beta''$ und von der Form $\alpha' + \beta'$, und daß die unpaaren Teile $(\alpha + \beta)'$ mit allen Kombinationen von der Form $\alpha' + \beta''$ und von der Form $\alpha'' + \beta'$ übereinstimmen; auch ist jeder Teil von $\alpha + \beta$ nur in einer dieser vier Formen, und zwar nur auf eine einzige Weise darstellbar. Ist ferner $\beta = 0$, so fallen die Formen aus, in welchen β' auftritt.

§ 4.

Bemerkungen über Dualgruppen.

Die im vorhergehenden § 3 enthaltenen Betrachtungen sind ihrem größten Teile nach keineswegs neu; da eine Kombination nichts anderes als ein System von Elementen ist, so gehören sie in die allgemeine Systemlehre, welche wohl am vollständigsten in dem umfassenden und durch eine Fülle origineller Betrachtungen fesselnden Werke Die Algebra der Logik von E. Schröder, behandelt ist. Zur Erleichterung der Vergleichung mache ich darauf aufmerksam, daß der Durchschnitt $\alpha - \beta$ der Systeme α, β in diesem Werke das Produkt von α, β genannt und demgemäß mit $\alpha\beta$ bezeichnet wird; diese Ausdrucks- und Bezeichnungsweise mag manche Vorzüge besitzen, doch schien mir die meinige für den gegenwärtigen Zweck hauptsächlich deshalb geeigneter, weil hier eine Übereinstimmung mit der in der Modul- und Idealtheorie von mir eingeführten Bezeichnungsart wünschenswert war. Hiernach entsprechen die in § 3 mit (1), (2), (3), (4), (5) bezeichneten Doppelsätze bzw. den Doppelsätzen (12), (13), (23), (14), (27) auf S. 254, 255, 276, 259, 282 im ersten Bande des genannten Werkes; im folgenden wird meine Bezeichnung der Sätze beibehalten, und unter A ist immer das System der Doppelsätze (1), (2), (3) zu verstehen, deren notwendige Folge der Doppelsatz (4) ist.

Auf S. 292 bis 293 zeigt Herr Schröder ebenfalls, aber auf etwas andere Weise, als es hier in § 3 geschehen ist, daß jeder der

beiden Sätze (5) auf den anderen vermöge des Systems A zurückführbar ist. Von besonderem Interesse ist aber die zuerst auf S. 286 ausgesprochene, später auf S. 643 und abermals auf S. 686 bewiesene Behauptung, daß keiner der beiden Sätze (5) eine notwendige Folge des Systems A ist.

Seit vielen Jahren habe ich mich ebenfalls mit diesen Fragen beschäftigt; doch hat mich hierzu nicht das Studium der Logik, sondern die Theorie derjenigen Zahlensysteme veranlaßt, welche ich Moduln nenne*). Bei dem Bestreben, diese Theorie auf die kleinste Anzahl von Grundgesetzen zurückzuführen, habe ich ebenfalls — nicht ohne große Anstrengung — die eben erwähnte Tatsache erkannt, und da der von mir eingeschlagene Weg vielleicht noch einiges Neue enthält, auch wohl etwas einfacher zu sein scheint als die von Herrn Schröder gegebenen Beweise, die er selbst als nicht mühelose bezeichnet, so erlaube ich mir, aus einer größeren, halb vollendeten Abhandlung einige Betrachtungen hier mitzuteilen, obgleich sie für den vorliegenden Aufsatz nicht erforderlich sind. Zuvor bemerke ich, daß selbstverständlich die Priorität für die Entdeckung der genannten Tatsache durchaus Herrn Schröder gebührt; auch muß ich gestehen, daß es mir noch nicht gelungen ist, die späteren Bände seines großen Werkes vollständig durchzuarbeiten, und so muß ich um Nachsicht bitten, wenn manche der folgenden Betrachtungen, bei welchen ich die leicht zu findenden Beweise größtenteils unterdrücke, schon bekannt sein sollten. Ich beginne mit der folgenden Erklärung.

Ein System $\mathfrak{A}$ von irgendwelchen Dingen $\alpha, \beta, \gamma \cdots$ soll eine Dualgruppe heißen, wenn es zwei Operationen $\pm$ gibt, welche aus je zwei Dingen α, β zwei ebenfalls in $\mathfrak{A}$ enthaltene Dinge $\alpha \pm \beta$ erzeugen und zugleich den Bedingungen A genügen.

Um zu zeigen, wie verschiedenartig die Gebiete sind, auf welche dieser Begriff angewendet werden kann, erwähne ich folgende Beispiele:

1. Das nächste und überall unentbehrliche Beispiel liefert die oben erwähnte Systemlehre der Logik; bedeuten die Dinge $\alpha, \beta, \gamma \cdots$ endliche oder unendliche Systeme (Kombinationen) von Elementen, und bezeichnet man mit $\alpha + \beta$ die logische Summe, mit $\alpha - \beta$ den Durchschnitt (das logische Produkt $\alpha\beta$ nach Schröder) von α, β, so bildet der Inbegriff $\mathfrak{A}$ aller Systeme $\alpha, \beta, \gamma \cdots$ eine Dualgruppe.

*) Vgl. S. 442, 479, 493 der zweiten, dritten, vierten Auflage von Dirichlets Vorlesungen über Zahlentheorie.

2. Der Inbegriff $\mathfrak{A}$ aller Zahlensysteme α, β, $\gamma \cdots$, welche ich Moduln nenne, bildet eine Dualgruppe, wenn unter $\alpha + \beta$ der größte gemeinsame Teiler, unter $\alpha - \beta$ das kleinste gemeinsame Vielfache der beiden Moduln α, β verstanden wird. Dies Beispiel ist keineswegs in dem vorigen enthalten; denn hier enthält der Modul $\alpha + \beta$ außer den in α oder β enthaltenen Zahlen (im allgemeinen) noch unendlich viele andere Zahlen (Elemente), während $\alpha - \beta$ auch hier der Durchschnitt der Systeme α, β, d. h. der Inbegriff aller den Moduln α, β gemeinsamen Zahlen ist.

3. Einen speziellen Fall der Moduln bilden die Ideale*) α, β, $\gamma \cdots$ eines endlichen Körpers, und da die daraus erzeugten Ideale $\alpha \pm \beta$ demselben Körper angehören, so ist der Inbegriff $\mathfrak{A}$ aller dieser Ideale eine Dualgruppe.

4. Ist ω eine endliche oder unendliche**) Abelsche oder auch Galoissche Gruppe, so bildet der Inbegriff $\mathfrak{A}$ aller Gruppen α, β, $\gamma \cdots$, welche als Teiler in ω enthalten sind (und zu denen auch ω selbst gehört), eine Dualgruppe, wenn unter $\alpha + \beta$ das kleinste gemeinsame Vielfache, unter $\alpha - \beta$ der größte gemeinsame Teiler der beiden Gruppen α, β verstanden wird.

5. Der Inbegriff $\mathfrak{A}$ aller Zahlensysteme α, β, $\gamma \cdots$, welche ich Körper***) nenne, bildet eine Dualgruppe, wenn unter $\alpha + \beta$ das kleinste gemeinsame Multiplum, unter $\alpha - \beta$ der größte gemeinsame Divisor der beiden Körper α, β verstanden wird.

6. Als letztes Beispiel mag das folgende dienen. Unter einem Punkte α des reellen Zahlenraumes von n Dimensionen sei jede Folge von n reellen Zahlen α_1, $\alpha_2 \cdots \alpha_n$ verstanden, welche umgekehrt die erste, zweite $\cdots$ $n$te Koordinate des Punktes α heißen mögen; definiert man nun für je zwei Punkte α, β die Punkte $\alpha \pm \beta$ dadurch, daß die Koordinate $(\alpha + \beta)_r$ die algebraisch größte, die Koordinate $(\alpha - \beta)_r$ die algebraisch kleinste der beiden Koordinaten α_r, β_r sein soll, so bildet der Raum $\mathfrak{A}$ als Inbegriff aller Punkte α, β, $\gamma \cdots$ eine Dualgruppe.

---

*) Vgl. S. 452, 508, 551 der zweiten, dritten, vierten Auflage von Dirichlets Zahlentheorie.

**) Vgl. § 5 dieses Aufsatzes.

***) Vgl. S. 424, 435, 452 der zweiten, dritten, vierten Auflage von Dirichlets Zahlentheorie.

Wir wenden uns nun zur Untersuchung über die Gültigkeit der in § 3 mit (5) und (6) bezeichneten Doppelsätze innerhalb der allgemeinen Theorie der Dualgruppen. Es ist dort schon gezeigt, daß die beiden Sätze (5′) und (5″) vermöge der Grundgesetze A wechselseitig auseinander folgen; dieses Doppelgesetz (5) gilt zufolge § 3 wirklich in dem ersten der eben aufgeführten Beispiele, in der Systemlehre der Logik; es gilt*) aber auch in dem dritten Beispiel, in der aus allen Idealen eines endlichen Körpers bestehenden Dualgruppe; aus diesem Grunde will ich diesen Doppelsatz (5) hier das Idealgesetz nennen, und jede Dualgruppe, in welcher dies Gesetz gilt mag eine Dualgruppe vom Idealtypus heißen.

Von ebenso großer Wichtigkeit sind aber auch die in § 3 mit (6′) und (6″) bezeichneten Sätze, sowie der folgende, bisher noch nicht erwähnte Satz

$$(M) \qquad [\alpha + (\beta - \gamma)] - (\beta + \gamma) = [\alpha - (\beta + \gamma)] + (\beta - \gamma),$$

welcher symmetrisch in bezug auf β, γ und zugleich sein eigenes dualistisches Gegenstück ist. Ich bemerke zunächst, daß je zwei dieser drei Sätze (6′), (6″), (M) äquivalent sind, d. h. wechselseitig vermöge der Grundgesetze A auseinander folgen. Bezeichnet man nämlich kurz mit (λ, μ, ν) eine Substitution, welche darin besteht, daß die drei Dinge α, β, γ bzw. durch die drei Dinge λ, μ, ν ersetzt werden, so überzeugt man sich leicht, daß

(6′)	durch	$(\alpha + \gamma, \beta, \alpha)$	in	(6″),
(6″)	„	$(\alpha - \gamma, \beta, \alpha)$	„	(6′),
(6′)	„	$(\beta + \gamma, \alpha, \beta - \gamma)$	„	(M),
(M)	„	$(\beta, \alpha, \alpha - \gamma)$	„	(6′),
(6″)	„	$(\beta - \gamma, \alpha, \beta + \gamma)$	„	(M),
(M)	„	$(\beta, \alpha, \alpha + \gamma)$	„	(6″)

übergeht. Dieses dreiförmige Gesetz gilt**) nun wirklich in dem zweiten der obigen Beispiele, in der aus allen Moduln bestehenden Dualgruppe; ich will es daher das Modulgesetz nennen, und jede Dualgruppe, in welcher es herrscht, mag eine Dualgruppe vom Modultypus heißen.

*) Dies folgt leicht aus D. § 178.

**) Vgl. D. § 169; die dortigen Sätze (7), (8), (8′) stimmen bzw. überein mit den obigen (M), (6″), (6′); zuerst erwähnt sind sie auf S. 17 meiner Schrift: Über die Anzahl der Idealklassen in den verschiedenen Ordnungen eines endlichen Körpers (Braunschweig 1877).

Da ferner in § 3 die Sätze (6′), (6″) lediglich vermöge der Grundgesetze A aus den Sätzen (5″), (5′) abgeleitet sind, so leuchtet die Wahrheit der folgenden Behauptung ein:

Jede Dualgruppe vom Idealtypus besitzt auch den Modultypus.

Hiernach entspringen naturgemäß die beiden Fragen:

Gibt es Dualgruppen, welche den Modultypus nicht besitzen?

Gibt es Dualgruppen vom Modultypus, welche den Idealtypus nicht besitzen?

Daß diese Fragen beide zu bejahen sind, habe ich — nicht ohne Mühe — dadurch entschieden, daß ich mir die bestimmte Aufgabe stellte, jedesmal die kleinste Dualgruppe aufzusuchen, welche die fragliche Eigenschaft hat. Die auf diese Weise gefundenen Gruppen bestehen aus je fünf verschiedenen Dingen, α, β, γ, δ, ε, und sind in den beiden folgenden Tabellen dargestellt:

	α	β	γ	δ	ε
α		δ	γ	δ	α
β	ε		δ	δ	β
γ	α	ε		δ	γ
δ	α	β	γ		δ
ε	ε	ε	ε	ε	

	α	β	γ	δ	ε
α		δ	δ	δ	α
β	ε		δ	δ	β
γ	ε	ε		δ	γ
δ	α	β	γ		δ
ε	ε	ε	ε	ε	

Zur Erläuterung dienen folgende Bemerkungen. Bedeutet (μ, ν) den Buchstaben, welcher sich im Durchschnittsfeld der Zeile μ und der Spalte ν findet, so hätten die Felder der Diagonale eigentlich mit den Buchstaben $(\mu, \mu) = \mu$ besetzt werden sollen; des deutlicheren Überblickes wegen sind sie aber leer gelassen, um die oberhalb und unterhalb der Diagonale gelegenen Hälften der Tabellen für das Auge leichter zu trennen; in der oberen Hälfte finden sich die Buchstaben $(\mu, \nu) = \mu + \nu = \nu + \mu$, in der unteren die Buchstaben $(\mu, \nu) = \mu - \nu = \nu - \mu$. Die durch die richtigen Buchstaben $(\mu, \mu) = \mu$

$= \mu + \mu = \mu - \mu$ besetzt zu denkenden Diagonalfelder gehören sowohl zu der oberen wie zu der unteren Hälfte. Die Tabellen enthalten daher für beide Operationen $\pm$ die vollständige Anweisung zu ihrer Ausführung.

Die genaue Prüfung ergibt, daß in beiden Tabellen die Grundgesetze A, in der zweiten auch die Gesetze (6′), (6″) erfüllt sind; das System $\mathfrak{A}$ der fünf Dinge $\alpha, \beta, \gamma, \delta, \varepsilon$ bildet daher in beiden Beispielen eine Dualgruppe, und die zweite dieser beiden Dualgruppen besitzt den Modultypus. Aus der ersten Tabelle folgt nun

$$(\alpha + \beta) - (\alpha + \gamma) = \delta - \gamma = \gamma,$$
$$\alpha + [\beta - (\alpha + \gamma)] = \alpha + (\beta - \gamma) = \alpha + \varepsilon = \alpha,$$

mithin gilt in der ersten Dualgruppe das Modulgesetz (6″) nicht. Aus der zweiten Tabelle folgt

$$(\alpha + \beta) - (\alpha + \gamma) = \delta - \delta = \delta,$$
$$\alpha + (\beta - \gamma) = \alpha + \varepsilon = \alpha,$$

mithin gilt in der zweiten Dualgruppe das Idealgesetz (5″) nicht. Hiermit sind die obigen Behauptungen gerechtfertigt.

Die eben dem Leser überlassene Prüfung, ob die durch die Tabellen definierten Operationen $\pm$ innerhalb eines Systems $\mathfrak{A}$ den Grundgesetzen A, eventuell auch dem Modulgesetz genügen, erweist sich bei der wirklichen Ausführung schon bei diesen einfachen Beispielen, wo das System $\mathfrak{A}$ endlich ist und nur aus fünf verschiedenen Dingen besteht, als ziemlich mühsam. Dies veranlaßt mich, hier noch eine Transformation der Grundgesetze A zu besprechen, durch welche deren Prüfung im allgemeinen wohl etwas erleichtert wird, und die zugleich ein neues Licht auf das Wesen der Dualgruppen wirft.

Ist α ein bestimmtes Ding in einer Dualgruppe $\mathfrak{A}$, so will ich mit α' das System aller in der Form $\alpha + \omega$ darstellbaren Dinge α_1 bezeichnen*), wo ω jedes Ding in $\mathfrak{A}$ bedeuten kann. Diese Systeme von der Form α' besitzen die folgenden sechs charakteristischen Eigenschaften, in welchen die beiden Operationen $\pm$ gar nicht mehr auftreten:

I. Jedem Dinge α in $\mathfrak{A}$ entspricht ein vollständig bestimmter Teil α' von $\mathfrak{A}$.

---

*) Diese Systeme α' und die später folgenden Systeme α'' dürfen nicht mit den in § 3 erklärten unpaaren und paaren Teilen einer Kombination α verwechselt werden.

II. Das Ding α ist in α' enthalten.

III. Aus $\alpha' = \beta'$ folgt $\alpha = \beta$.

IV. Ist das Ding α_1 in α' enthalten, so ist das System α_1' ein Teil von α'.

V. Der Durchschnitt von je zwei Systemen α', β' (d. h. der Inbegriff aller ihnen gemeinsamen Dinge) ist selbst wieder ein System ν'.

VI. Für je zwei Dinge α, β in $\mathfrak{A}$ gibt es ein Ding μ in $\mathfrak{A}$, welches den beiden folgenden Bedingungen genügt: α' und β' sind Teile von μ', und wenn α', β' Teile von einem System μ_2' sind, so ist auch μ' ein Teil von μ_2'.

Daß wirklich diese Eigenschaften eine unmittelbare Folge der Grundgesetze A und der obigen Definition der Systeme α' sind, wird der Leser ohne jede Mühe finden, und zwar wird V. durch $\nu = \alpha + \beta$, und VI. durch $\mu = \alpha - \beta$ erfüllt.

Läßt man nun die Erinnerung an die Operationen $\pm$ gänzlich fallen, und nimmt man lediglich an, es gelten in einem System $\mathfrak{A}$ die vorstehenden sechs Eigenschaften, so kann man den Systemen α' eine zweite Klasse von Systemen α'' innerhalb $\mathfrak{A}$ gegenüberstellen, deren Erklärung die folgende ist. Bedeutet α irgendein Ding in $\mathfrak{A}$, so gibt es zufolge II. mindestens ein Ding α_2 von der Art, daß α in α_2' enthalten ist, und mit α'' soll der Inbegriff aller dieser Dinge α_2 bezeichnet werden. Man wird sich leicht überzeugen, daß diese Systeme α'' (wenn man zugleich α_1, ν, μ, μ_2 bzw. durch α_2, μ, ν, ν_1 ersetzt) genau dieselben sechs Eigenschaften besitzen wie die Systeme α', und rückwärts ergibt sich aus den Systemen α'', falls diese gegeben sind, auf dieselbe Weise wieder die Konstruktion der Systeme α'.

Wenn nun in $\mathfrak{A}$ eine der beiden Klassen von Systemen α', α'' und folglich auch die andere gegeben ist, so kann man in $\mathfrak{A}$ zwei Operationen $\pm$ eindeutig dadurch definieren, daß $\alpha + \beta = \nu$, $\alpha - \beta = \mu$ gesetzt wird, wo ν, μ die in V., VI. angegebene Bedeutung haben, und man zeigt leicht, daß diese Operationen die Grundgesetze A einer Dualgruppe $\mathfrak{A}$ erfüllen, und daß die Systeme α', α'' bzw. die Inbegriffe aller in den Formen $\alpha + \omega$, $\alpha - \omega$ darstellbaren Dinge α_1, α_2 sind.

Aus diesem Kreislauf von den Operationen $\pm$ zu den Systemen α', α'', und zurück von diesen zu jenen ergibt sich einerseits, daß in einer Dualgruppe $\mathfrak{A}$ nur die eine der beiden Operationen $\pm$ durch

eine (endliche oder unendliche) Tabelle gegeben zu sein braucht, daß die andere hierdurch zugleich vollständig bestimmt ist. Dasselbe ergibt sich übrigens auch ohne die Einführung der Systeme α', α'' leicht aus den Grundgesetzen A; nimmt man nämlich an, eine dritte Operation | erfülle für sich allein und in Verbindung mit der Operation $+$ dieselben Gesetze A wie die Operation $-$, so ergibt sich, wie der Leser sogleich finden wird, daß immer $\alpha \mid \beta = \alpha - \beta$, also die Operation | identisch mit $-$ sein muß.

Andererseits lehrt dieser Kreislauf, daß eine Dualgruppe $\mathfrak{A}$ statt durch eine Tabelle, in welcher die Resultate der Operationen $\pm$ oder vielmehr nur eine dieser Operationen dargestellt sind, auch auf ganz andere Art, nämlich durch Angabe aller Systeme α', oder aller Systeme α'' vollständig definiert werden kann.

So z. B. tritt an die Stelle der beiden obigen Tabellen (oder deren Hälften) je eine Hälfte der beiden folgenden Tabellen:

ω	ω'	ω''
α	α, γ, δ	α, ε
β	β, δ	β, ε
γ	γ, δ	$\alpha, \gamma, \varepsilon$
δ	δ	$\alpha, \beta, \gamma, \delta, \varepsilon$
ε	$\alpha, \beta, \gamma, \delta, \varepsilon$	ε

ω	ω'	ω''
α	α, δ	α, ε
β	β, δ	β, ε
γ	γ, δ	γ, ε
δ	δ	$\alpha, \beta, \gamma, \delta, \varepsilon$
ε	$\alpha, \beta, \gamma, \delta, \varepsilon$	ε

Diese Tabellen ergeben nun, ohne die Feder zu gebrauchen, durch den bloßen Anblick der Zeilen die Bestätigung der obigen sechs Eigenschaften, also den Beweis, daß die beiden Systeme $\mathfrak{A}$ wirklich Dualgruppen sind, und es ist wohl anzunehmen, daß auch bei komplizierteren Beispielen unsere zweite Art der Darstellung von Dualgruppen Vorzüge vor der früheren Art besitzen wird. Auch die Prüfung, ob eine Dualgruppe den Modultypus oder gar den Idealtypus besitzt, läßt sich wohl erleichtern, doch kann ich hierauf nicht mehr eingehen*).

Zum Schluß erwähne ich noch folgendes. Ist α_1 in der Form $\alpha + \omega$ darstellbar, also in dem System α' enthalten, so folgt $\alpha + \alpha_1$

*) Vgl. D. § 169, S. 499, Anmerkung.

$= \alpha_1$ und hieraus $\alpha - \alpha_1 = \alpha - (\alpha + \alpha_1) = \alpha$; umgekehrt folgt auch $\alpha + \alpha_1 = \alpha_1$ aus $\alpha - \alpha_1 = \alpha$, und α ist in dem System α_1'' enthalten. Diese Beziehung zwischen zwei Dingen α, α_1 einer Dualgruppe $\mathfrak{A}$ tritt so häufig auf, daß eine noch kürzere Bezeichnung derselben wünschenswert ist. In der aus allen Moduln bestehenden Dualgruppe $\mathfrak{A}$ habe ich hierfür die doppelte Bezeichnung*)

$$\alpha > \alpha_1, \quad \alpha_1 < \alpha$$

eingeführt, die freilich bei der Übertragung auf andere Beispiele von Dualgruppen dem Sinne, welcher sonst den Zeichen $>$, $<$ beigelegt wird, oft widersprechen mag, aber für die allgemeine Theorie doch ganz unbedenklich ist. Aus der großen Anzahl von Sätzen über den Gebrauch dieser Zeichen erwähne ich erstens, daß aus $\alpha_1 < \alpha$ und $\alpha < \alpha_2$, was bequem in $\alpha_1 < \alpha < \alpha_2$ zusammengezogen werden kann, stets $\alpha_1 < \alpha_2$ folgt, und zweitens, daß aus $\alpha_1 < \alpha$ und $\alpha_1 > \alpha$ immer $\alpha_1 = \alpha$ folgt. Nun ist oben gezeigt, daß es Dualgruppen gibt, in welchen weder das Idealgesetz (5), noch das Modulgesetz (6) herrscht; dagegen gelten in jeder Dualgruppe die folgenden Gesetze:

$$(\alpha - \beta) + (\alpha - \gamma) > \alpha - [\beta + (\alpha - \gamma)],$$
$$(\alpha + \beta) - (\alpha + \gamma) < \alpha + [\beta - (\alpha + \gamma)]$$

und

$$\alpha - [\beta + (\alpha - \gamma)] > \alpha - (\beta + \gamma),$$
$$\alpha + [\beta - (\alpha + \gamma)] < \alpha + (\beta - \gamma),$$

also auch die beiden folgenden**):

$$(\alpha - \beta) + (\alpha - \gamma) > \alpha - (\beta + \gamma),$$
$$(\alpha + \beta) - (\alpha + \gamma) < \alpha + (\beta - \gamma).$$

Die Herstellung der leicht zu findenden Beweise muß ich aber dem Leser überlassen.

§ 5.

Abelsche Gruppe $\mathfrak{G}$.

Nach dieser Abschweifung kehren wir zu der Aufgabe zurück, die wir in den §§ 1 und 2 für natürliche oder allgemeiner für (positive) rationale Zahlen behandelt haben. Diese Aufgabe soll aber jetzt in doppelter Weise verallgemeinert werden, zunächst dadurch, daß statt

*) D. § 169, S. 495. Vgl. auch das oben zitierte Werk von Schröder, S. 270, Satz (20).

**) Vgl. Satz (25) auf S. 280 des Werkes von Schröder.

drei oder vier Zahlen beliebig viele in endlicher Anzahl n gegeben sein sollen, wobei uns die in § 3 enthaltenen Betrachtungen über Kombinationen nützliche Dienste leisten werden. Die zweite Art der Verallgemeinerung besteht darin, daß wir an Stelle der rationalen Zahlen die Elemente a, b, $c \cdots$ einer endlichen oder unendlichen Abelschen Gruppe $\mathfrak{G}$ treten lassen. Wir setzen also voraus, es gäbe eine der Multiplikation der Zahlen ähnliche Operation, welche aus je zwei Elementen a, b der Gruppe $\mathfrak{G}$ ein in derselben enthaltenes Element ab erzeugt; wir nennen diese Gruppenoperation unbedenklich eine Multiplikation und das erzeugte Element ab das Produkt aus den Faktoren a, b. Über diese Operation machen wir drei Annahmen, deren erste darin besteht, daß das Kommutations- und Assoziationsgesetz

$$(1) \qquad ab = ba, \quad (ab)c = a(bc)$$

erfüllt ist. Wir setzen zweitens voraus, es gäbe in $\mathfrak{G}$ ein Element o, welches der Zahl 1 bei der Multiplikation der Zahlen insofern entspricht, daß die Gleichung

$$(2) \qquad ao = a$$

für jedes Element a der Gruppe $\mathfrak{G}$ gilt; es kann nur ein einziges solches Element o geben, weil, wenn p dieselbe Eigenschaft besitzt, op sowohl $= p$ wie $= o$ sein muß; dieses Element o heißt das Hauptelement der Gruppe $\mathfrak{G}$. Unsere dritte und letzte Annahme besteht darin, daß zu jedem Element a der Gruppe $\mathfrak{G}$ ein reziprokes, mit a^{-1} zu bezeichnendes Element von $\mathfrak{G}$ gehört, welches der Bedingung

$$(3) \qquad aa^{-1} = o$$

genügt; es kann nur ein einziges solches Element geben, weil, falls $aq = o$ angenommen wird, das Produkt qaa^{-1} sowohl $= (qa)a^{-1} = a^{-1}$ wie $= q(aa^{-1}) = q$ ist. Offenbar ist a das reziproke Element von a^{-1}, ferner $o^{-1} = o$.

Wir können nun auch eine der Gruppenoperation entgegengesetzte Division einführen; dies ist zwar für unseren Zweck nicht durchaus erforderlich, aber die Schreibweise mancher Formeln wird dadurch für das Auge übersichtlicher. Wir definieren daher den aus dem Zähler a und dem Nenner b gebildeten Bruch oder Quotienten durch

$$(4) \qquad a:b = \frac{a}{b} = ab^{-1},$$

woraus

$$\left(\frac{a}{b}\right) b = a \tag{5}$$

folgt. Zugleich leuchtet ein, daß alle Regeln der Multiplikation Division, Erweiterung und Hebung von Zahlbrüchen sich auf diese neuen Brüche übertragen, und daß jedes Element a der Gruppe auch als Bruch $(a : o)$ angesehen werden kann.

Es wird im folgenden oft von Produkten Πa die Rede sein, wo das Produktzeichen Π sich auf alle m Elemente $a = a_1, a_2 \cdots a_m$ bezieht, welche unter einer gemeinsamen Form enthalten sind oder gewissen Bedingungen genügen; ein solches Produkt ist also erklärt durch

$$\Pi a = a_1 a_2 \cdots a_m. \tag{6}$$

Es kommt aber auch vor, daß die Anzahl m der fraglichen Elemente a auf 1 oder 0 herabsinkt, und wir wollen festsetzen, daß unter Πa im ersten Falle immer das einzige Element a_1 selbst, im letzteren Falle immer das Hauptelement o der Gruppe zu verstehen ist.

Dieselbe Regel soll auch für die Potenz a^m gelten, d. h. für ein Produkt aus lauter gleichen Faktoren a, deren Anzahl der Exponent m ist; es wird daher $a^1 = a$, und $a^0 = o$ zu setzen sein. Versteht man ferner unter einer Potenz a^{-m} mit negativem Exponenten $(-m)$ die $m$te Potenz von a^{-1}, so gelten für Produkte und Quotienten von Potenzen dieselben Regeln, wie in der Arithmetik.

Nach diesen Vorbereitungen wenden wir uns zu unserem eigentlichen Gegenstand. Wir bezeichnen, wie in § 3, mit $\alpha, \beta, \gamma \cdots$ alle Kombinationen, welche sich aus den n Unterscheidungszeichen

$$1, 2, \cdots, n \tag{7}$$

bilden lassen, und deren Anzahl $= 2^n$ ist. Für jede solche Kombination α wählen wir willkürlich aus unserer Abelschen Gruppe $\mathfrak{G}$ ein Element, welches wir durch

$$(\alpha, 0) \tag{8}$$

bezeichnen wollen*). Nachdem dies geschehen ist, definieren wir für jedes Paar von Kombinationen α, β ein zugehöriges Element (α, β) der Gruppe $\mathfrak{G}$ durch

$$(\alpha, \beta) = \frac{\Pi(\alpha + \beta'', 0)}{\Pi(\alpha + \beta', 0)}, \tag{9}$$

*) Eine Beschränkung in der Freiheit dieser Wahl wird erst später in § 7 eintreten.

wo das Produktzeichen Π sich im Zähler auf alle (in § 3 definierten) paaren Teile β'', im Nenner auf alle unpaaren Teile β' der Kombination β bezieht*).

Wir bemerken zunächst, daß nach den obigen Festsetzungen über den Gebrauch des Zeichens Π das in (9) definierte Element (α, β), falls $\beta = 0$ sein sollte, von selbst mit dem in (8) gewählten oder gegebenen Element $(\alpha, 0)$ identisch wird, weil es in diesem Falle gar kein unpaares β' und nur ein einziges paares $\beta'' = 0$ gibt. Ist ferner ε ein Kombinationselement, d. h. eine der n Kombinationen ersten Grades (7), so gibt es ein einziges unpaares $\varepsilon' = \varepsilon$ und ein einziges paares $\varepsilon'' = 0$, und aus der Definition (9) fließt der Satz

$$(\alpha, 0) = (\alpha + \varepsilon, 0)\ (\alpha, \varepsilon), \tag{10}$$

welcher nur ein spezieller Fall der späteren Sätze (12) und (13) ist. Wir stellen nun einige auf die Quotienten (9) bezügliche Sätze auf.

Satz I. Ist $\alpha - \beta$ von 0 verschieden, haben also α und β mindestens ein Element ε gemeinsam, so ist

$$(\alpha, \beta) = 0. \tag{11}$$

Beweis. Denn wenn man $\beta = \varepsilon + \omega$ setzt, wo ω das Element ε nicht enthält, so bestehen die paaren Teile β'' der Kombination β teils aus allen paaren Teilen ω'' der Kombination ω, teils aus allen Kombinationen von der Form $\varepsilon + \omega'$, wo ω' jeden unpaaren Teil von ω bedeutet; ebenso bestehen die unpaaren Teile β' von β teils aus diesen Kombinationen ω', teils aus allen Kombinationen $\varepsilon + \omega''$. Bedenkt man nun, daß ε auch in α enthalten, also $\alpha + \varepsilon = \alpha$ ist, so bestehen die Kombinationen $\alpha + \beta''$ aus allen $\alpha + \omega''$ und allen $\alpha + \omega'$, und ebenso bestehen die Kombinationen $\alpha + \beta'$ aus allen $\alpha + \omega'$ und allen $\alpha + \omega''$; mithin ist das System der Kombinationen $\alpha + \beta''$ identisch mit dem der Kombinationen $\alpha + \beta'$, und zufolge der Definition (9) wird $(\alpha, \beta) = 0$, w. z. b. w.

Satz II. Ist ε eine Kombination ersten Grades, so ist

$$(\alpha, \beta) = (\alpha + \varepsilon, \beta)\ (\alpha, \beta + \varepsilon). \tag{12}$$

Beweis. Falls ε in β enthalten, also $\beta + \varepsilon = \beta$ ist, leuchtet der Satz unmittelbar ein, weil nach dem vorhergehenden Satze $(\alpha + \varepsilon, \beta) = 0$ ist. Im entgegengesetzten Falle sind die paaren Teile $(\beta + \varepsilon)''$

*) Beispiele solcher Quotienten finden sich am Schlusse von § 2.

teils $= \beta''$, teils $= \varepsilon + \beta'$, und die unpaaren Teile $(\beta\ \varepsilon)'$ + teils $= \beta'$, teils $= \varepsilon + \beta''$; die Definition (9) gibt daher

$$(\alpha, \beta + \varepsilon) = \frac{\Pi(\alpha + \beta'', 0)\,\Pi(\alpha + \varepsilon + \beta', 0)}{\Pi(\alpha + \beta', 0)\,\Pi(\alpha + \varepsilon + \beta'', 0)},$$

woraus durch Vergleichung mit (9) und mit

$$(\alpha + \varepsilon, \beta) = \frac{\Pi(\alpha + \varepsilon + \beta'', 0)}{\Pi(\alpha + \varepsilon + \beta', 0)}$$

die Gleichung (12) folgt, w. z. b. w.

Satz III. Sind α, β, γ beliebige Kombinationen, so ist

$$(\alpha, \beta) = \Pi(\alpha + \gamma_1, \beta + \gamma_2), \tag{13}$$

wo das Produktzeichen Π sich auf alle verschiedenen Paare von Kombinationen γ_1, γ_2 bezieht, die den Bedingungen

$$\gamma_1 + \gamma_2 = \gamma, \quad \gamma_1 - \gamma_2 = 0 \tag{14}$$

genügen.

Beweis. Der Satz gilt für $\gamma = 0$, weil in diesem Falle γ nur eine einzige Zerlegung $\gamma_1 = 0$, $\gamma_2 = 0$ besitzt; er gilt nach dem vorhergehenden Satze auch, wenn γ ein Kombinationselement ist, weil dann γ nur die beiden Zerlegungen $\gamma_1 = \gamma$, $\gamma_2 = 0$ und $\gamma_1 = 0$ $\gamma_2 = \gamma$ besitzt. Der Induktionsbeweis wird daher vollendet sein, wenn wir annehmen, der Satz gelte für jede Kombination γ vom Grade r, und hieraus seine Gültigkeit für jede Kombination δ vom Grade $r + 1$ ableiten. Offenbar kann man $\delta = \gamma + \varepsilon$ setzen, wo ε ein beliebig gewähltes Element von δ bedeutet, während γ die aus den übrigen r Elementen von δ bestehende Kombination ist. Behalten nun γ_1, γ_2 ihre obige Bedeutung, so zerfallen alle Paare δ_1, δ_2, welche den Bedingungen $\delta_1 + \delta_2 = \delta$, $\delta_1 - \delta_2 = 0$ genügen, in zwei verschiedene Arten, je nachdem das Element ε in δ_1 oder δ_2 aufgenommen wird; im ersten Falle ist $\delta_1 = \varepsilon + \gamma_1$, $\delta_2 = \gamma_2$, im zweiten $\delta_1 = \gamma_1$, $\delta_2 = \varepsilon + \gamma_2$, und folglich wird das auf alle Paare δ_1, δ_2 ausgedehnte Produkt

$$\Pi(\alpha + \delta_1, \beta + \delta_2) = \Pi(\alpha + \varepsilon + \gamma_1, \beta + \gamma_2)\,\Pi(\alpha + \gamma_1, \beta + \varepsilon + \gamma_2).$$

Da nach unserer Annahme der Satz (13) für jede Kombination γ vom Grade r gilt, so ist auch

$$(\alpha + \varepsilon, \beta) = \Pi(\alpha + \varepsilon + \gamma_1, \beta + \gamma_2),$$
$$(\alpha, \beta + \varepsilon) = \Pi(\alpha + \gamma_1, \beta + \varepsilon + \gamma_2),$$

woraus mit Rücksicht auf den vorhergehenden Satz (12) sich

$$\Pi(\alpha + \delta_1,\ \beta + \delta_2) = (\alpha, \beta)$$

ergibt, w. z. b. w.

Beispiele zu diesem, im folgenden sehr häufig anzuwendenden Satze, den wir kurz den Produktsatz nennen wollen, findet man in den Gleichungen (3), (5), (7) des § 2. Wir wollen noch bemerken, daß der Satz zufolge I auch dann gilt, wenn man die zweite der Bedingungen (14) fallen läßt; doch würde diese Verallgemeinerung nur eine scheinbare und kaum von Nutzen sein.

Satz IV. Sind α, β, γ beliebige Kombinationen, so ist

$$(15) \qquad (\alpha, \beta + \gamma) = \frac{\Pi(\alpha + \gamma'', \beta)}{\Pi(\alpha + \gamma', \beta)},$$

wo γ'' alle paaren, γ' alle unpaaren Teile von γ durchläuft.

Beweis. Der Satz gilt offenbar für $\gamma = 0$, weil es dann nur ein einziges $\gamma'' = 0$ und gar kein γ' gibt, also der Nenner $= 0$ wird. Gilt der Satz für jede Kombination γ vom Grade r, und setzt man irgendeine Kombination δ vom Grade $r + 1$ wieder in die Form $\gamma + \varepsilon$, wo ε ein Element von δ bedeutet, so bestehen die paaren Teile δ'' teils aus den Kombinationen γ'', teils aus den Kombinationen $\varepsilon + \gamma'$, und die unpaaren Teile δ' bestehen aus den Kombinationen γ' und $\varepsilon + \gamma''$; mithin wird

$$\Pi(\alpha + \delta'', \beta) = \Pi(\alpha + \gamma'', \beta)\ \Pi(\alpha + \varepsilon + \gamma', \beta),$$
$$\Pi(\alpha + \delta', \beta) = \Pi(\alpha + \gamma', \beta)\ \Pi(\alpha + \varepsilon + \gamma'', \beta),$$

also nach unserer Induktionsannahme

$$\frac{\Pi(\alpha + \delta'', \beta)}{\Pi(\alpha + \delta', \beta)} = \frac{(\alpha, \beta + \gamma)}{(\alpha + \varepsilon, \beta + \gamma)},$$

und da die rechte Seite zufolge (12), wenn dort β durch $\beta + \gamma$ ersetzt wird, $= (\alpha, \beta + \gamma + \varepsilon) = (\alpha, \beta + \delta)$ ist, so gilt unser Satz auch für jede Kombination δ vom Grade $r + 1$, also allgemein, w. z. b. w.

Satz V. Sind α, β, γ beliebige Kombinationen, so ist

$$(16) \qquad (\alpha + \gamma, \beta) = \frac{\Pi(\alpha, \beta + \gamma'')}{\Pi(\alpha, \beta + \gamma')},$$

wo γ'' alle paaren, γ' alle unpaaren Teile von γ durchläuft.

Den auf dieselbe Weise wie im vorigen Satze zu führenden Induktionsbeweis dürfen wir dem Leser überlassen. Als einen bemerkenswerten speziellen Fall wollen wir aber noch den Satz

$$(17) \qquad (\alpha, \beta) = \frac{\Pi(0, \beta + \alpha'')}{\Pi(0, \beta + \alpha')}$$

hervorheben, der sich aus (16) ergibt, wenn man α, γ bzw. durch $0, \alpha$ ersetzt; hieraus geht nämlich hervor, daß die durch (9) definierten Elemente $(0, \omega)$ unserer Abelschen Gruppe $\mathfrak{G}$ unabhängige Funktionen von den willkürlich gewählten oder gegebenen Elementen $(\omega, 0)$ sind, insofern die letzteren und überhaupt alle (α, β) sich durch die ersteren ausdrücken lassen.

§ 6.

Ganze Elemente in $\mathfrak{G}$.

Auch die im vorhergehenden § 5 enthaltenen Sätze sind nur als Vorbereitungen für unser eigentliches Ziel anzusehen, welches darin besteht, die in den §§ 1 und 2 beschriebenen Zahlenbildungen soweit wie möglich zu verallgemeinern. Zu ihrer Übertragung auf die Abelsche Gruppe $\mathfrak{G}$ fehlt aber bis jetzt immer noch das wesentlichste Moment, nämlich die Unterscheidung der ganzen und nicht ganzen Elemente dieser Gruppe, also auch der Begriff der Teilbarkeit und eine Operation, welche der Bildung des größten gemeinsamen Teilers von zwei Zahlen entspricht. Der Kürze wegen beginnen wir, weil daraus alles andere folgt, mit dem zuletzt genannten Punkte und machen die neue Annahme, es gäbe in unserer Abelschen Gruppe $\mathfrak{G}$ außer der eigentlichen Gruppenoperation (der Multiplikation), welche aus je zwei Elementen $\mathfrak{a}$, $\mathfrak{b}$ deren Produkt $\mathfrak{a}\mathfrak{b}$ erzeugt, noch eine zweite Operation $+$, die wir unbedenklich Addition nennen wollen, und welche aus $\mathfrak{a}$, $\mathfrak{b}$ ein Element $\mathfrak{a} + \mathfrak{b}$ derselben Gruppe $\mathfrak{G}$, die Summe der Glieder $\mathfrak{a}$, $\mathfrak{b}$ erzeugt; und zwar setzen wir voraus, daß diese Operation $+$ für sich allein und in Verbindung mit der Gruppenoperation den vier folgenden Fundamentalgesetzen

$$(1) \qquad \mathfrak{a} + \mathfrak{a} = \mathfrak{a},$$

$$(2) \qquad \mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a},$$

$$(3) \qquad (\mathfrak{a} + \mathfrak{b}) + \mathfrak{c} = \mathfrak{a} + (\mathfrak{b} + \mathfrak{c}),$$

$$(4) \qquad (\mathfrak{a} + \mathfrak{b})\mathfrak{c} = \mathfrak{a}\mathfrak{c} + \mathfrak{b}\mathfrak{c}$$

gehorcht, deren Inbegriff wir kurz mit G bezeichnen wollen. Diese Gesetze herrschen, wenn die Operation $+$ als Bildung des größten gemeinsamen Teilers gedeutet wird, tatsächlich in der Theorie der rationalen Zahlen, ebenso auch in der allgemeineren Theorie der Moduln*), und mit gewissen Vorbehalten kann man behaupten, daß sie umgekehrt das Wesen der genannten Bildung erschöpfen.

Indem wir die aus (2) und (3) fließenden bekannten Folgerungen übergehen (D. § 2), bemerken wir, daß zufolge (4), wenn $\mathfrak{c}$ durch $\mathfrak{c}^{-1}$ ersetzt wird, auch die Regeln der Buchstabenrechnung für die Addition von Brüchen gelten; durch das Gesetz (1) treten aber wesentliche Vereinfachungen ein, und wir heben namentlich die beiden folgenden, leicht zu beweisenden Sätze

$$(5) \qquad (\mathfrak{a}+\mathfrak{b}+\mathfrak{c})(\mathfrak{b}\mathfrak{c}+\mathfrak{c}\mathfrak{a}+\mathfrak{a}\mathfrak{b}) = (\mathfrak{b}+\mathfrak{c})(\mathfrak{c}+\mathfrak{a})(\mathfrak{a}+\mathfrak{b}),$$

$$(6) \qquad (\mathfrak{a}+\mathfrak{b})^m = \mathfrak{a}^m + \mathfrak{a}^{m-1}\mathfrak{b} + \cdots + \mathfrak{a}\mathfrak{b}^{m-1} + \mathfrak{b}^m$$

hervor (D. § 170, S. 503), von denen wir sogleich Gebrauch machen werden. Multipliziert man die rechte Seite in (6), wo $m \geqq 0$ ist, mit $(\mathfrak{a}^m + \mathfrak{b}^m)$, so wird sie $= (\mathfrak{a}+\mathfrak{b})^{2m}$, mithin ist in unserer Gruppe auch $(\mathfrak{a}+\mathfrak{b})^m = \mathfrak{a}^m + \mathfrak{b}^m$.

Vor allem müssen wir darauf aufmerksam machen, daß durch die Annahme der Existenz der Operation $+$ innerhalb der Abelschen Gruppe $\mathfrak{G}$ die Allgemeinheit der letzteren eine wesentliche Beschränkung erlitten hat; dies leuchtet unmittelbar ein durch den folgenden

Satz: Die einzige in $\mathfrak{G}$ als Teiler enthaltene endliche Gruppe besteht aus dem Hauptelement $\mathfrak{o}$.

Beweis. Ist $\mathfrak{H}$ eine aus h Elementen $\mathfrak{a}$ bestehende Teilgruppe in $\mathfrak{G}$, so ist bekanntlich $\mathfrak{a}^h = \mathfrak{o}$; aus (6) ergibt sich ferner

$$(\mathfrak{a}+\mathfrak{o})^{h-1} = \mathfrak{a}^{h-1} + \mathfrak{a}^{h-2} + \cdots + \mathfrak{a} + \mathfrak{o},$$

also

$$\mathfrak{a}(\mathfrak{a}+\mathfrak{o})^{h-1} = \mathfrak{o} + \mathfrak{a}^{h-1} + \cdots + \mathfrak{a}^2 + \mathfrak{a} = (\mathfrak{a}+\mathfrak{o})^{h-1},$$

mithin $\mathfrak{a} = \mathfrak{o}$, w. z. b. w.

Eine Abelsche Gruppe $\mathfrak{G}$, in welcher die Operation $+$ existiert, muß daher, falls sie nicht aus einem einzigen Element $\mathfrak{o}$ bestehen soll — welchen interesselosen Fall wir ausschließen wollen —, jeden-

*) Vgl. D. § 169, S. 496 und § 170, S. 502. — Die Moduln $\mathfrak{a}$ bilden aber in ihrer Gesamtheit keine Abelsche Gruppe; denn wenn es auch einen Modul $\mathfrak{o} = [1]$ gibt, welcher der Bedingung (2) in § 5 genügt (D. § 170, S. 500), so gibt es doch im allgemeinen keine reziproken Moduln $\mathfrak{a}^{-1}$, welche der Bedingung (3) in § 5 genügen.

falls eine unendliche Gruppe sein. Eine unmittelbare Folge hiervon ist auch der

Satz: Ist a von o verschieden, so folgt aus $a^r = a^s$ immer $r = s$.

Beweis. Denn wenn man annimmt, es sei z. B. $r > s$, so folgt $a^{r-s} = o$, und die Potenzen o, a, $a^2 \cdots a^{r-s-1}$, mögen sie verschieden oder teilweise einander gleich sein, bilden jedenfalls eine endliche Gruppe, woraus im Widerspruch mit unserer Annahme folgen würde, daß $a = o$ ist.

Betrachten wir nun die denkbar einfachste unendliche Abelsche Gruppe $\mathfrak{G}$, welche aus allen Potenzen a^r eines von o verschiedenen Elementes a besteht, so wollen wir uns die Frage stellen: kann es in einer solchen Gruppe $\mathfrak{G}$ eine Operation $+$ geben, die den obigen Gesetzen $\mathfrak{G}$ gehorcht? Gesetzt, es sei der Fall, so muß es eine ganze Zahl e geben, welche der Bedingung

$$o + a = a^e \tag{7}$$

genügt. Falls nun diese Zahl e positiv ist, so addieren wir unter Beachtung von (1) auf beiden Seiten alle Potenzen a^r, deren Exponenten r der Bedingung $1 \leqq r \leqq e$ genügen, und erhalten

$$o + a + \cdots + a^e = a + \cdots + a^e,$$

also

$$(o + a)^e = a\,(o + a)^{e-1},\quad o + a = a,$$

mithin muß $e = 1$ sein. Ist $m \geqq 0$, so folgt hieraus

$$a^m = (o + a)^m = o + a + \cdots + a^m,$$

also zufolge (1) auch

$$o + a^m = a^m,$$

und hieraus ergibt sich das allgemeine Gesetz

$$a^r + a^s = a^h, \tag{8}$$

wo h die algebraisch größte der beiden ganzen rationalen Zahlen r, s bedeutet. Sieht man umgekehrt dieses Gesetz als Definition der Operation $+$ innerhalb der Potenzengruppe $\mathfrak{G}$ an, so leuchtet ein, daß hierdurch die Gesetze G wirklich erfüllt sind. Auf ähnliche Weise läßt sich auch die zweite Annahme behandeln, daß der in (7) auftretende Exponent e nicht positiv ist; doch kann dieser Fall kürzer auf den vorigen zurückgeführt werden. Bedenkt man nämlich, daß unsere Gruppe $\mathfrak{G}$ auch als Inbegriff aller Potenzen des reziproken Elementes $b = a^{-1}$ aufgefaßt werden kann, wodurch (7) die Form

$\mathfrak{o} + \mathfrak{b} = \mathfrak{b}^{1-e}$ annimmt, so muß der nach der jetzigen Annahme positive Exponent $1 - e = 1$, also $e = 0$ sein, und aus dem obigen Gesetz $\mathfrak{b}^r + \mathfrak{b}^s = \mathfrak{b}^h$ ergibt sich für diesen Fall das Gesetz

$$\mathfrak{a}^r + \mathfrak{a}^s = \mathfrak{a}^k, \tag{9}$$

wo k die algebraisch kleinste der Zahlen r, s bedeutet. In der aus allen Potenzen eines Elementes $\mathfrak{a}$ bestehenden unendlichen Abelschen Gruppe $\mathfrak{G}$ gibt es daher zwei verschiedene Operationen $+$, deren jede zufolge ihrer Definition (8) oder (9) den vier Gesetzen G genügt.

Nachdem das Wesen dieser Gesetze durch das vorstehende Beispiel der Potenzengruppe einigermaßen erläutert ist, will ich noch zwei Beispiele von Abelschen Gruppen $\mathfrak{G}$ anführen, in welchen es außer der Gruppenoperation (Multiplikation) auch Operationen $+$ (Additionen) gibt, welche den genannten Gesetzen gehorchen. Das System aller Idealbrüche $\mathfrak{a}$ eines endlichen Körpers Ω, unter denen auch die Ideale als ganze Idealbrüche enthalten sind, bildet eine Abelsche Gruppe $\mathfrak{G}$, insofern ihre Multiplikation (die Gruppenoperation) die in § 5 angegebenen Gesetze (1), (2), (3) erfüllt (D. § 178, S. 560, Anmerkung); ferner ist der größte gemeinsame Teiler $\mathfrak{a} + \mathfrak{b}$ von je zwei solchen Idealbrüchen $\mathfrak{a}$, $\mathfrak{b}$ ebenfalls in $\mathfrak{G}$ enthalten, und die hierdurch definierte Operation $+$ genügt, weil die Idealbrüche zugleich Moduln sind, auch den obigen Gesetzen G. Dieses Beispiel besitzt noch die besondere Eigenschaft, daß jedes Element $\mathfrak{a}$ der Gruppe $\mathfrak{G}$ stets und nur auf eine einzige Weise als Produkt von Potenzen $\mathfrak{p}^r$ darstellbar ist, deren Basen $\mathfrak{p}$ gewisse ausgezeichnete Elemente der Gruppe $\mathfrak{G}$, nämlich die Primideale des Körpers Ω sind, während die Exponenten r alle ganzen rationalen Zahlen durchlaufen können; um nun zu zeigen, daß diese Eigenschaft nicht etwa, wie man vermuten könnte, den tieferen Grund für die Existenz der Operation $+$ in der Gruppe $\mathfrak{G}$ bildet, will ich noch ein zweites Beispiel anführen, dem die genannte Eigenschaft fehlt.

Ist a eine bestimmte von Null verschiedene algebraische Zahl*) und $\mathfrak{o}$ das System aller algebraischen Einheiten**), so bilden alle mit a assoziierten Zahlen, d. h. alle Produkte von der

*) Vgl. S. 427, 452, 524 der zweiten, dritten, vierten Auflage von Dirichlets Zahlentheorie.

**) Daselbst, S. 439, 457, 532.

Form ae, wo e alle Einheiten durchläuft, ein System $\mathfrak{a}$, welches ungeändert bleibt, wenn a selbst durch irgendeine in $\mathfrak{a}$ enthaltene Zahl ae ersetzt wird; dies beruht darauf, daß die Produkte und Quotienten von irgend zwei Einheiten ebenfalls Einheiten sind. Jede in $\mathfrak{a}$ enthaltene Zahl kann daher als Repräsentant oder erzeugende Zahl von $\mathfrak{a}$ angesehen werden. Offenbar ist $\mathfrak{o}$ selbst ein solches System, als dessen Repräsentant die Zahl 1 oder jede andere Einheit gelten kann. Ist $\mathfrak{b}$ ebenfalls ein solches, durch die Zahl b erzeugtes System, so leuchtet ein, daß alle aus je einem Faktor des Systems $\mathfrak{a}$ und je einem Faktor des Systems $\mathfrak{b}$ gebildeten Produkte dem durch das Produkt ab erzeugten System angehören; nennen wir dieses letztere System (dessen Zahlen umgekehrt immer, und zwar auf unendlich viele Arten als solche Produkte von Zahlen aus $\mathfrak{a}$ und $\mathfrak{b}$ dargestellt werden können) das Produkt der Systeme $\mathfrak{a}$, $\mathfrak{b}$, und bezeichnen wir dasselbe mit $\mathfrak{ab}$, so bildet der Inbegriff aller dieser Systeme $\mathfrak{a}$ vermöge dieser Operation der Multiplikation offenbar eine Abelsche Gruppe $\mathfrak{G}$, deren Hauptelement das System $\mathfrak{o}$ aller Einheiten ist, während das zu $\mathfrak{a}$ reziproke Element $\mathfrak{a}^{-1}$ durch die Zahl a^{-1} erzeugt wird. Auf einem viel tiefer liegenden Grunde beruht aber die Möglichkeit, in diese Gruppe $\mathfrak{G}$ eine zweite Operation $+$ einzuführen, welche den Gesetzen G gehorcht. Ich habe bewiesen*) daß je zwei algebraische Zahlen a, b einen sogenannten größten gemeinsamen Teiler d besitzen, welcher dadurch charakterisiert ist daß es vier ganze**) algebraische Zahlen a', b', x, y gibt, welche den Bedingungen

$$(10) \qquad a = da', \quad b = db', \quad ax + by = d$$

genügen; dieser Satz ist zwar nur für den damals allein wichtigen Fall bewiesen, wo a und b (also auch d) ganze Zahlen sind; da aber zwei beliebige algebraische Zahlen a, b durch Multiplikation mit einem von Null verschiedenen Faktor m stets in ganze Zahlen ma, mb verwandelt werden können***), so leuchtet die allgemeine Gültigkeit des Satzes sofort ein, wenn man den größten gemeinsamen Teiler der ganzen Zahlen ma, mb mit md bezeichnet. Aus der Form der charakteristischen Gleichungen (10) ergibt sich ferner, daß

*) Vgl. S. 465, 541, 577 der zweiten, dritten, vierten Auflage von Dirichlets Zahlentheorie.

**) Daselbst, S. 437, 452, 524.

***) Daselbst, S. 439, 493, 525.

zu zwei gegebenen Zahlen a, b immer unendlich viele solche Zahlen d gehören, deren Inbegriff das in der obigen Weise durch irgendeine von ihnen erzeugte System $\mathfrak{d}$ ist, und dieses System $\mathfrak{d}$ bleibt auch ungeändert, wenn a, b durch irgendwelche Zahlen der ihnen entsprechenden Systeme $\mathfrak{a}$, $\mathfrak{b}$ ersetzt werden. Das Element $\mathfrak{d}$ unserer Gruppe $\mathfrak{G}$ ist daher durch die Elemente $\mathfrak{a}$, $\mathfrak{b}$ vollständig bestimmt, und folglich wird eine neue Operation $+$ durch die Festsetzung $\mathfrak{a} + \mathfrak{b} = \mathfrak{d}$ eindeutig erklärt; daß dieselbe den vier Gesetzen G genügt, wird der Leser ohne Mühe aus den Gleichungen (10) ableiten. Ich bemerke aber zum Schluß, daß in dieser Gruppe $\mathfrak{G}$ eine Darstellung aller Elemente $\mathfrak{a}$ als Produkte von Potenzen von festen Primelementen nicht vorhanden ist (vgl. D., § 174).

Wir verlassen diese Beispiele und wenden uns zur Betrachtung irgendeiner Abelschen Gruppe $\mathfrak{G}$, in welcher es eine Addition $+$ mit den obigen Eigenschaften gibt. Indem wir nun eine Reihe von Benennungen einführen, die denen der Zahlentheorie nachgebildet sind, bemerken wir vor allen Dingen, daß dieselben sich stets auf diese eine Operation $+$ beziehen; dies muß deshalb hervorgehoben werden, weil es, wie sich bald zeigen wird, in jeder solchen Gruppe $\mathfrak{G}$ mindestens zwei verschiedene solche Operationen $+$ gibt (vgl. das obige Beispiel der aus allen Potenzen a^r bestehenden Gruppe auf S. 128).

Wir nennen ein Element $\mathfrak{a}$ der Gruppe $\mathfrak{G}$ ganz, wenn $\mathfrak{a} + \mathfrak{o} = \mathfrak{o}$ ist, im entgegengesetzten Falle gebrochen. Dann ergibt sich zunächst, daß alle Produkte und Summen von ganzen Elementen ebenfalls ganz sind; denn durch Addition der beiden Gleichungen $\mathfrak{a} + \mathfrak{o} = \mathfrak{o}$, $\mathfrak{b} + \mathfrak{o} = \mathfrak{o}$ erhält man $(\mathfrak{a} + \mathfrak{b}) + \mathfrak{o} = \mathfrak{o}$; multipliziert man ferner die erste mit $\mathfrak{b}$, so folgt $\mathfrak{a}\mathfrak{b} + \mathfrak{b} = \mathfrak{b}$, und wenn man auf beiden Seiten $\mathfrak{o}$ addiert, so ergibt sich $\mathfrak{a}\mathfrak{b} + \mathfrak{o} = \mathfrak{o}$, w. z. b. w.

Das (ganze oder gebrochene) Element $\mathfrak{a}$ soll teilbar durch $\mathfrak{b}$ heißen, wenn $\mathfrak{a} + \mathfrak{b} = \mathfrak{b}$ ist; dies kommt offenbar darauf hinaus, daß $\mathfrak{a}\mathfrak{b}^{-1}$ ein ganzes Element $\mathfrak{g}$, also $\mathfrak{a} = \mathfrak{b}\mathfrak{g}$ ist; wir nennen zugleich $\mathfrak{a}$ ein Vielfaches von $\mathfrak{b}$, und $\mathfrak{b}$ einen Teiler von $\mathfrak{a}$, und es leuchtet ein, daß die durch das Hauptelement $\mathfrak{o}$ teilbaren Elemente, und nur diese ganz sind. Benutzt man (wie in der Modultheorie) für diese Teilbarkeit die doppelte Bezeichnung

$$\mathfrak{a} > \mathfrak{b}, \quad \mathfrak{b} < \mathfrak{a},$$

so findet man leicht, daß aus $\mathfrak{a} > \mathfrak{b}$ und $\mathfrak{b} > \mathfrak{c}$ auch $\mathfrak{a} > \mathfrak{c}$, und daß aus $\mathfrak{a} > \mathfrak{b}$ und $\mathfrak{b} > \mathfrak{a}$ auch $\mathfrak{a} = \mathfrak{b}$ folgt.

Die Summe $a + b$ von zwei beliebigen Elementen a, b ist immer ein gemeinsamer Teiler derselben, und jeder gemeinsame Teiler n von a, b ist ein Teiler von der Summe $a + b$, weil aus $a + n = n$ und $b + n = n$ durch Addition auch $(a + b) + n = n$ folgt; der Analogie wegen kann man daher die Summe $a + b$ auch den größten gemeinsamen Teiler von a, b nennen.

Zwei Elemente a, b sollen fremd*) heißen, wenn ihre Summe $a + b = o$ ist; zwei solche Elemente a, b sind offenbar stets ganze Elemente, und o ist ihr einziger ganzer gemeinsamer Teiler.

Ist a fremd zu b und zu c, so ist a auch fremd zu bc; multipliziert man nämlich die erste der beiden Gleichungen $a + b = o$, $a + c = o$, aus deren letzter auch $c + o = o$, also $ac + a = a$ folgt, mit c, so erhält man $ac + bc = c$, und wenn man auf beiden Seiten a addiert, so folgt $(a + ac) + bc = a + c$, also $a + bc = o$, w. z. b. w.

Umgekehrt, wenn a fremd zu dem Produkt bc der beiden ganzen Elemente b, c ist, so ist a auch fremd zu jedem der beiden Faktoren b, c; denn aus der letzten der drei Annahmen $a + bc = o$, $b + o = o$, $c + o = o$ folgt $b = bc + b$, also $a + b = (a + bc) + b = o + b = o$, w. z. b. w.

Durch wiederholte Anwendung dieser beiden Sätze ergibt sich der allgemeinere: zwei Produkte p, q sind gewiß fremd, wenn jeder Faktor von p fremd zu jedem Faktor von q ist, und umgekehrt folgt das letztere auch aus dem ersteren, wenn zugleich alle diese Faktoren ganz sind.

Sind a, b beliebige Elemente, so sind die aus ihnen gebildeten Elemente

$$a' = \frac{a}{a + b}, \quad b' = \frac{b}{a + b}$$

immer fremd, d. h. es ist $a' + b' = o$; man kann daher

$$a = (a + b)a', \quad b = (a + b)b'$$

setzen, und jeder Quotient $(a : b)$, also auch jedes Element $a = (a : o)$, kann folglich in der Form $(a' : b')$, d. h. als Quotient von zwei fremden Elementen a', b' dargestellt werden; daß es nur eine einzige solche Darstellung gibt, ist leicht zu beweisen.

*) Dieses Wort wird hier in ganz anderem Sinne gebraucht wie bei den Kombinationen in § 3, nämlich analog dem Begriff der relativen Primzahlen in der Zahlentheorie.

Indem wir eine Reihe anderer, ebenso leicht zu beweisender Sätze über fremde Elemente übergehen, wenden wir uns zur Betrachtung der gemeinsamen Vielfachen c von zwei Elementen a, b, wobei wir die eben festgesetzte Bedeutung von a', b' beibehalten. Aus den Annahmen $c + a = a$, $c + b = b$ folgt durch Multiplikation mit b, a bzw. $bc + ab = ab$, $ac + ab = ab$, und hieraus durch Addition $(a + b)c + ab = ab$, oder wenn man durch $(a + b)$ dividiert und

$$m = \frac{ab}{a + b} = ab' = ba' = (a + b)a'b'$$

setzt, $c + m = m$, d. h. c ist teilbar durch m; da nun fremde Elemente a', b' stets ganz sind, so ist m ebenfalls teilbar durch a und b, mithin sind die gemeinsamen Vielfachen c von a, b identisch mit den sämtlichen Vielfachen dieses Elementes m, welches daher nach Analogie mit der Zahlentheorie das kleinste gemeinsame Vielfache von a, b heißen mag. Wir wollen nun die Bildung dieses Elementes m aus den Elementen a, b als eine neue Operation — in unsere Gruppe einführen; dieselbe wird also definiert durch

$$(11) \qquad a - b = \frac{ab}{a + b}$$

oder, was dasselbe sagt, durch

$$(12) \qquad a - b = (a^{-1} + b^{-1})^{-1},$$

und zugleich gilt der Satz

$$(13) \qquad (a + b)(a - b) = ab.$$

Vor allem bemerken wir, daß diese neue Operation — für sich allein und in Verbindung mit der Gruppenoperation — den vier folgenden Gesetzen

$$(1') \qquad a - a = a,$$

$$(2') \qquad a - b = b - a,$$

$$(3') \qquad (a - b) - c = a - (b - c),$$

$$(4') \qquad (a - b)c = ac - bc$$

gehorcht, welche vollständig den Gesetzen G entsprechen, und deren Inbegriff wir mit G' bezeichnen wollen. Die Beweise von (1') und (2') liegen auf der Hand. Ferner ergibt sich aus der Definition

$$(a - b) - c = \frac{(a - b)c}{(a - b) + c},$$

und wenn man den Bruch rechter Hand unter Beachtung von (13) durch $(a + b)$ erweitert, so erhält man

$$(a - b) - c = \frac{abc}{bc + ca + ab} = (a^{-1} + b^{-1} + c^{-1})^{-1},$$

woraus wegen der Symmetrie (3′) folgt. Ebenso ergibt sich die Gleichung (4′), weil jede ihrer beiden Seiten, wenn sie mit $(a + b)c = (ac + bc)$ multipliziert wird, dasselbe Produkt abc^2 gibt.

Es erscheint also hier die schon oben angekündigte merkwürdige Tatsache, daß, wenn es in einer Abelschen Gruppe $\mathfrak{G}$ eine Operation $+$ gibt, welche den Gesetzen G gehorcht, daraus immer eine zweite Operation — abgeleitet werden kann, welche genau dieselben Gesetze befolgt. Es fragt sich daher: können diese beiden Operationen $\pm$ vielleicht identisch sein? Nehmen wir an, zwei Elemente a, b genügen der Bedingung $a - b = a + b$, woraus durch Multiplikation mit $(a + b)$ auch $ab = (a + b)^2 = a^2 + ab + b^2$ folgt, so erhält man durch Addition von a^2 und von b^2 die beiden Gleichungen $a(a + b) = (a + b)^2$ und $b(a + b) = (a + b)^2$, mithin $a = b = a + b$; da also für je zwei verschiedene Elemente a, b auch $(a - b)$ verschieden von $(a + b)$ wird, so sind die beiden Operationen $\pm$ nicht identisch miteinander; aus (12) geht aber zugleich hervor, daß sie sich vollständig miteinander vertauschen, wenn jedes Element a der Gruppe $\mathfrak{G}$ durch das reziproke Element a^{-1} ersetzt wird (vgl. das oben angeführte Beispiel der einfachen Potenzengruppe). Hierbei wollen wir auch bemerken, daß der Satz (12), auf eine beliebige Anzahl von Elementen ausgedehnt, in der doppelten Form*)

$$(14) \qquad (a - b - c - \cdots)^{-1} = a^{-1} + b^{-1} + c^{-1} + \cdots,$$

$$(15) \qquad (a + b + c + \cdots)^{-1} = a^{-1} - b^{-1} - c^{-1} - \cdots$$

dargestellt werden kann, was durch vollständige Induktion leicht zu beweisen ist.

Es erscheint ferner die andere merkwürdige Tatsache, daß zwischen den beiden Operationen $\pm$ auch die Beziehungen

$$(16) \qquad a + (a - b) = a,$$

$$(17) \qquad a - (a + b) = a$$

bestehen, welche schon daraus folgen, daß $a - b$ durch a, und a durch $a + b$ teilbar ist; man kann sie aber auch dadurch beweisen,

*) Vgl. D. § 178, S. 555.

daß man die linke Seite der ersten Gleichung mit $(a+b)$, die der zweiten mit $(a-b)$ multipliziert, wodurch zufolge (13) bzw. die Produkte $a(a+b)$, $a(a-b)$ entstehen. Offenbar stimmen nun die sechs Gesetze (2), (3), (2'), (3'), (16), (17), in welchen die eigentliche Gruppenoperation gar nicht auftritt, genau mit den sechs Gesetzen A des § 3 überein, welche dann die Grundlage für die Betrachtungen des § 4 gebildet haben; wir können daher sagen, daß unsere Abelsche Gruppe $\mathfrak{G}$, wenn man von der Multiplikation ihrer Elemente ganz absieht und nur die beiden Operationen $\pm$ in das Auge faßt, auch eine Dualgruppe ist, und wir wollen zum Schluß noch zeigen, daß dieselbe den Idealtypus besitzt, d. h., daß in ihr das Doppelgesetz (5) des § 3 gilt:

$$(18) \qquad (a-b)+(a-c) = a-(b+c),$$

$$(19) \qquad (a+b)-(a+c) = a+(b-c).$$

Dies ergibt sich aus der Definition der Operation — durch die folgenden Rechnungen:

$$(a-b)+(a-c) = \frac{ab}{a+b}+\frac{ac}{a+c} = \frac{a(bc+ca+ab)}{(a+b)(c+a)},$$

$$a-(b+c) = \frac{a(b+c)}{a+b+c},$$

$$(a+b)-(a+c) = \frac{(a+b)(c+a)}{a+b+c},$$

$$a+(b-c) = a+\frac{bc}{b+c} = \frac{bc+ca+ab}{b+c},$$

und aus dem obigen Satze (5) folgt die Identität der beiden ersten und ebenso die der beiden letzten Ausdrücke, w. z. b. w.

§ 7.

Lösung der Aufgabe.

Wir kehren jetzt zurück zu der in §§ 1 und 2 für rationale Zahlen behandelten Aufgabe, um dieselbe auf ein beliebig gegebenes System von n Elementen

$$(1) \qquad a_1, a_2 \cdots a_n$$

der in den §§ 5 und 6 betrachteten Abelschen Gruppe $\mathfrak{G}$ zu übertragen. Es handelt sich darum, diejenigen Zerlegungen dieser Ele-

mente in Faktoren zu finden, welche sich aus der Bildung der größten gemeinsamen Teiler

$$\begin{aligned} &a_1 + a_2, \quad a_1 + a_3 \cdots, \\ &a_1 + a_2 + a_3, \quad a_1 + a_2 + a_4 \cdots, \\ &a_1 + a_2 + a_3 + a_4 \cdots, \\ &\cdots\cdots\cdots\cdots\cdots \end{aligned}$$

von irgendwelchen Kombinationen aus diesen Elementen ableiten lassen; diese größten gemeinsamen Teiler sind, da ihre Bildung als stets ausführbar angenommen wird, ebenfalls als gegeben anzusehen.

Zu diesem Zwecke benutzen wir die in § 5 beschriebene Bezeichnungsweise, indem wir zunächst die n gegebenen Elemente (1) der Reihe nach mit den Zeichen

$$(2) \qquad (1,0),\ (2,0) \cdots (n,\ 0)$$

belegen. Während nun in § 5 auch alle anderen Elemente von der Form $(\alpha,\ 0)$, wo α jede beliebige Kombination aus den n Unterscheidungszeichen $1,\ 2 \cdots n$ bedeutet, als willkürlich wählbar oder gegeben angesehen werden durften, so wollen wir jetzt diese Wahlfreiheit gänzlich aufheben, indem wir festsetzen, daß

$$(3) \qquad (\alpha,\ 0) = (\varepsilon_1,\ 0) + (\varepsilon_2,\ 0) + \cdots$$

sein soll, wo $\varepsilon_1,\ \varepsilon_2 \cdots$ die sämtlichen Kombinationen ersten Grades bedeuten, deren Summe die Kombination α ist; es wird also $(\alpha,\ 0)$ definiert als der größte gemeinsame Teiler aller derjenigen in der Reihe (2) enthaltenen Gruppenelemente $(\varepsilon,\ 0)$, welche den in α enthaltenen Kombinationselementen ε entsprechen; falls α selbst vom ersten Grade ist, so besteht die Summe (3) aus einem einzigen Gliede, welches das entsprechende Element in der Reihe (2) ist. Hiermit sind alle Elemente $(\alpha,\ 0)$ durch (2) vollständig gegeben, mit Ausnahme des Elementes (0,0), das vorläufig noch willkürlich bleiben mag.

Aus diesen Elementen $(\alpha,\ 0)$, deren Anzahl $= 2^n$ ist, bilden wir nun nach der Definition (9) in § 5, also durch Multiplikation und Division, alle Elemente von der Form $(\alpha,\ \beta)$; diese sind daher, wenn α von 0 verschieden ist, ebenfalls durch die n Elemente (2) vollständig gegeben, während in allen Ausdrücken von der Form $(0,\ \beta)$ auch das Element $(0,\ 0)$ auftritt. Dann gelten die in § 5 bewiesenen Sätze I bis V, und von diesen gibt der allgemeine Produktsatz III die vollständige Lösung unserer Aufgabe. Die Beschaffenheit

dieser Lösung wollen wir aber durch die folgenden Sätze deutlich machen, welche aus der Definition (3) fließen.

Satz I. Sind die Kombinationen α, β von 0 verschieden und ω beliebig, so ist

$$(4) \qquad (\alpha, \omega) + (\beta, \omega) = (\alpha + \beta, \omega).$$

Beweis. Zunächst leuchtet ein, daß dieser Satz für $\omega = 0$ gilt. Denn wenn ε alle Elemente der Kombination α, ebenso η alle Elemente der Kombination β durchläuft, so ist $(\alpha, 0)$ zufolge (3) die Summe aller $(\varepsilon, 0)$, ebenso ist $(\beta, 0)$ die Summe aller $(\eta, 0)$, und $(\alpha + \beta, 0)$ ist die Summe aller $(\theta, 0)$, wo θ alle Elemente der Kombination $(\alpha + \beta)$ durchläuft. Nun tritt zwar, wenn α und β gemeinsame Elemente $\varepsilon = \eta$ besitzen, das Glied $(\varepsilon, 0) = (\eta, 0)$ auf der linken Seite der zu beweisenden Gleichung (4) sowohl in der Summe $(\alpha, 0)$ wie in der Summe $(\beta, 0)$ auf, allein zufolge des Satzes $a + a = a$ braucht ein solches Glied nur einmal gezählt zu werden, und da die Elemente von α und die von β zugleich alle Elemente θ der Summe $(\alpha + \beta)$ erschöpfen, so ergibt sich die Wahrheit des Satzes für diesen Fall $\omega = 0$. Wir nehmen nun an, der Satz sei für alle Kombinationen ω vom Grade r bewiesen, und wollen zeigen, daß er dann (falls $r < n$ ist) auch für jede Kombination vom Grade $(r + 1)$ gilt. Jede solche Kombination läßt sich in die Form $\omega + \varepsilon$ setzen, wo ε jetzt irgendeine Kombination ersten Grades bedeutet, welche in der Kombination ω vom Grade r nicht enthalten ist. Setzen wir ferner zur Abkürzung

$$(\alpha, \omega) = a, \quad (\beta, \omega) = b, \quad (\varepsilon, \omega) = c,$$

so folgt aus unserer Induktionshypothese

$$(\alpha + \varepsilon, \omega) = a + c, \qquad (\beta + \varepsilon, \omega) = b + c,$$
$$(\alpha + \beta, \omega) = a + b, \quad (\alpha + \beta + \varepsilon, \omega) = a + b + c,$$

und aus dem speziellen Produktsatz II in § 5 ergibt sich

$$a = (a + c)(\alpha, \omega + \varepsilon), \quad b = (b + c)(\beta, \omega + \varepsilon),$$
$$a + b = (a + b + c)(\alpha + \beta, \omega + \varepsilon).$$

Hieraus folgt weiter

$$(a + c)(b + c)\{(\alpha, \omega + \varepsilon) + (\beta, \omega + \varepsilon)\} = a(b + c) + b(a + c)$$
$$= bc + ca + ab;$$

multipliziert man diese Gleichung mit der vorhergehenden, und dividiert man die Produktgleichung durch die Gleichung (5) in § 6, nämlich durch

$$(b + c)(c + a)(a + b) = (a + b + c)(bc + ca + ab),$$

so erhält man

$$(\alpha, \omega + \varepsilon) + (\beta, \omega + \varepsilon) = (\alpha + \beta, \omega + \varepsilon),$$

d. h. unser Satz gilt auch für jede Kombination $(\omega + \varepsilon)$ vom Grade $(r + 1)$, also allgemein, w. z. b. w.

Satz II. Sind die Kombinationen α, β von 0 verschieden, so ist (α, β) ein ganzes Element der Gruppe $\mathfrak{G}$.

Beweis. Ist β von 0 verschieden, so sind die Elemente (β, β) und $(\alpha + \beta, \beta)$ nach Satz I in § 5 beide $= 0$, und da, wenn α ebenfalls von 0 verschieden ist, nach dem eben bewiesenen Satze $(\alpha, \beta) + (\beta, \beta) = (\alpha + \beta, \beta)$ ist, so ergibt sich $(\alpha, \beta) + 0 = 0$, w. z. b. w.

Satz III. Genügen die vier Kombinationen α, β, γ, δ der Bedingung $\alpha + \beta = \gamma + \delta$, und sind außerdem die Durchschnitte $\alpha - \delta$ und $\beta - \gamma$ beide von 0 verschieden, so sind (α, β) und (γ, δ) fremde Elemente, in Zeichen

$$(\alpha, \beta) + (\gamma, \delta) = 0. \tag{5}$$

Beweis. Wenn die Bedingung $\alpha + \beta = \gamma + \delta$ erfüllt ist, so wird nach einem in § 3 bewiesenen Satze (S. 111)

$$\beta = \varrho + \omega, \quad \delta = \sigma + \omega,$$
$$\alpha + \varrho = \gamma + \sigma = \alpha + \gamma,$$

wo zur Abkürzung

$$\beta - \gamma = \varrho, \quad \alpha - \delta = \sigma, \quad \beta - \delta = \omega$$

gesetzt ist. Wir wenden jetzt den allgemeinen Produktsatz III des § 5 auf die beiden Elemente (α, ω), (γ, ω) an, indem wir die dort mit γ bezeichnete Kombination einmal durch ϱ, das andere Mal durch σ ersetzen; in den so erhaltenen Gleichungen

$$(\alpha, \omega) = \Pi(\alpha + \varrho_1, \ \omega + \varrho_2),$$
$$(\gamma, \omega) = \Pi(\gamma + \sigma_1, \ \omega + \sigma_2)$$

bezieht sich das erste Produktzeichen auf alle Zerlegungen $\varrho = \varrho_1 + \varrho_2$ mit der Bedingung $\varrho_1 - \varrho_2 = 0$, das zweite auf alle Zerlegungen $\sigma = \sigma_1 + \sigma_2$ mit der Bedingung $\sigma_1 - \sigma_2 = 0$. Da nun nach unserer Annahme die beiden Durchschnitte ϱ, σ (also auch α, β, γ, δ) von 0 verschieden sind, so besteht jedes dieser beiden Produkte aus mindestens zwei Faktoren, und zwar sind die Faktoren $(\alpha + \varrho, \omega)$ und $(\gamma + \sigma, \omega)$, welche den Zerlegungen $\varrho_1 = \varrho$, $\varrho_2 = 0$ und $\sigma_1 = \sigma$, $\sigma_2 = 0$ entsprechen, identisch mit $(\alpha + \gamma, \omega)$; bezeichnen wir daher die Produkte aller übrigen Faktoren bzw. mit $\mathfrak{p}$ und $\mathfrak{q}$, so wird

$$(\alpha, \omega) = (\alpha + \gamma, \omega)\mathfrak{p}, \quad (\gamma, \omega) = (\alpha + \gamma, \omega)\mathfrak{q};$$

da ferner, wie schon bemerkt, auch α, γ von 0 verschieden sind, so ist $(\alpha + \gamma, \omega)$ nach Satz I die Summe der beiden vorstehenden Elemente, mithin

$$\mathfrak{p} + \mathfrak{q} = \mathfrak{o},$$

d. h. die genannten Produkte $\mathfrak{p}$, $\mathfrak{q}$ sind fremd zueinander. Nun war $\mathfrak{p}$ das Produkt aus allen denjenigen Faktoren $(\alpha + \varrho_1, \omega + \varrho_2)$, in welchen ϱ_2 von 0 verschieden ist, und da letzteres auch von α, also auch von $\alpha + \varrho_1$ und $\omega + \varrho_2$ gilt, so ist (nach Satz II) jeder solche Faktor $(\alpha + \varrho_1, \omega + \varrho_2)$ ein ganzes Element der Gruppe, und dasselbe gilt offenbar von jedem Faktor $(\gamma + \sigma_1, \omega + \sigma_2)$ des Produktes $\mathfrak{q}$, weil γ und σ_2, also auch $\gamma + \sigma_1$ und $\omega + \sigma_2$, von 0 verschieden sind. Da aber das Produkt $\mathfrak{p}$ der ganzen Faktoren $(\alpha + \varrho_1, \omega + \varrho_2)$, wie oben gezeigt ist, fremd zu dem Produkt $\mathfrak{q}$ der ganzen Faktoren $(\gamma + \sigma_1, \omega + \sigma_2)$ ist, so folgt nach einem in § 6 bewiesenen Satze (S. 132) daß auch jeder der Faktoren von $\mathfrak{p}$ fremd zu jedem der Faktoren von $\mathfrak{q}$ ist; unter den ersteren befindet sich aber der der Zerlegung $\varrho_1 = 0$, $\varrho_2 = \varrho$ entsprechende Faktor $(\alpha, \omega + \varrho) = (\alpha, \beta)$ und unter den letzteren befindet sich der der Zerlegung $\sigma_1 = 0$ $\sigma_2 = \sigma$ entsprechende Faktor $(\gamma, \omega + \sigma) = (\gamma, \delta)$; mithin ist (α, β) fremd zu (γ, δ), w. z. b. w.

Satz IV. Sind die Kombinationen α, β von 0 verschieden und ω beliebig, so ist

$$(\omega, \alpha) + (\omega, \beta) = (\omega, \alpha + \beta). \tag{6}$$

Beweis. Nach dem allgemeinen Produktsatz III des § 5 können wir

$$(\omega, \alpha) = \Pi(\omega + \beta_1, \quad \alpha + \beta_2),$$
$$(\omega, \beta) = \Pi(\omega + \alpha_1, \quad \beta + \alpha_2)$$

setzen, wo sich das erste Produktzeichen auf alle Zerlegungen $\beta = \beta_1 + \beta_2$ mit der Bedingung $\beta_1 - \beta_2 = 0$, das zweite auf alle Zerlegungen $\alpha = \alpha_1 + \alpha_2$ mit der Bedingung $\alpha_1 - \alpha_2 = 0$ bezieht. Da α, β nach unserer Annahme von 0 verschieden sind, so besteht jedes dieser beiden Produkte aus mindestens zwei Faktoren, und zwar sind die den beiden Zerlegungen $\beta_1 = 0$, $\beta_2 = \beta$ und $\alpha_1 = 0$, $\alpha_2 = \alpha$ entsprechenden Faktoren identisch mit $(\omega, \alpha + \beta)$; bezeichnen wir daher die Produkte aller übrigen Faktoren bzw. mit $\mathfrak{p}$ und $\mathfrak{q}$, so wird

$$(\omega, \alpha) = (\omega, \alpha + \beta)\,\mathfrak{p}, \quad (\omega, \beta) = (\omega, \alpha + \beta)\,\mathfrak{q}.$$

Vergleichen wir nun irgendeinen Faktor $(\omega + \beta_1, \alpha + \beta_2)$ von $\mathfrak{p}$ mit irgendeinem Faktor $(\omega + \alpha_1, \beta + \alpha_2)$ von $\mathfrak{q}$, so genügen die vier in ihnen auftretenden Kombinationen zunächst der Bedingung

$$(\omega + \beta_1) + (\alpha + \beta_2) = (\omega + \alpha_1) + (\beta + \alpha_2),$$

weil jede dieser beiden Summen $= \omega + \alpha + \beta$ ist; da ferner β_1 ein von 0 verschiedener Teil von β, und α_1 ein von 0 verschiedener Teil von α ist, so sind auch die Durchschnitte

$$(\omega + \beta_1) - (\beta + \alpha_2), \quad (\omega + \alpha_1) - (\alpha + \beta_2)$$

beide von 0 verschieden. Aus diesen Eigenschaften der vier Kombinationen folgt aber (nach Satz III), daß jeder Faktor $(\omega + \beta_1, \alpha + \beta_2)$ von $\mathfrak{p}$ fremd zu jedem Faktor $(\omega + \alpha_1, \beta + \alpha_2)$ von $\mathfrak{q}$ ist; nach einem in § 6 bewiesenen Satze (S. 132) ist daher auch $\mathfrak{p}$ fremd zu $\mathfrak{q}$, also

$$\mathfrak{p} + \mathfrak{q} = \mathfrak{o},$$

und hieraus folgt durch Addition der beiden letzten Darstellungen von (ω, α) und (ω, β) die Gleichung (6), w. z. b. w.

Satz V. Ist die Kombination α von 0 verschieden, ω beliebig, so ist (ω, α) die Summe aller (ω, ε), wo ε alle in α enthaltenen Kombinationen ersten Grades durchläuft.

Dies ist offenbar eine unmittelbare Folge des vorhergehenden Satzes IV. Vergleicht man den speziellen Fall $\omega = 0$ mit der obigen Definition (3) der Elemente $(\alpha, 0)$, so zeigt sich, daß die schon am Schluß von § 5 hervorgehobene Analogie zwischen den Elementen $(\alpha, 0)$ und $(0, \alpha)$ auch nach unseren jetzigen Beschränkungen hinsichtlich der Wahl dieser Elemente bestehen bleibt.

Satz VI. Ist die Kombination α von 0 verschieden, ω beliebig, so ist der Quotient

$$\frac{(\omega, 0)}{(\omega, \alpha)} \tag{7}$$

das kleinste gemeinsame Vielfache aller Elemente $(\omega + \varepsilon, 0)$, wo ε alle in α enthaltenen Kombinationen ersten Grades $\varepsilon_1, \varepsilon_2 \cdots$ durchläuft.

Beweis. Nach dem speziellen Produktsatz (10) des § 5 ist $(\omega, 0) = (\omega + \varepsilon, 0)(\omega, \varepsilon)$, also

$$(\omega, 0)(\omega + \varepsilon, 0)^{-1} = (\omega, \varepsilon).$$

Bezeichnet man nun das im Satze genannte kleinste gemeinsame Vielfache

$$(\omega + \varepsilon_1, 0) - (\omega + \varepsilon_2, 0) - \cdots$$

zur Abkürzung mit $\mathfrak{m}$, und wendet man den Satz (14) des § 6 an, so folgt

$$\mathfrak{m}^{-1} = (\omega + \varepsilon_1, 0)^{-1} + (\omega + \varepsilon_2, 0)^{-1} + \cdots,$$

also

$$(\omega, 0)\mathfrak{m}^{-1} = (\omega, \varepsilon_1) + (\omega, \varepsilon_2) + \cdots,$$

und da nach dem vorhergehenden Satze V diese Summe $= (\omega, \alpha)$ ist, so ergibt sich

$$(\omega, 0)\mathfrak{m}^{-1} = (\omega, \alpha), \quad \mathfrak{m} = \frac{(\omega, 0)}{(\omega, \alpha)},$$

w. z. b. w.

Hiermit sind wohl die wichtigsten Eigenschaften der Ausdrücke (α, β) erschöpft, welche zuerst in § 5 durch die Gleichung (9) eingeführt, jetzt aber durch die Definition (3) sämtlich auf die n gegebenen Elemente (2) und, falls $\alpha = 0$ ist, auf (0,0) zurückgeführt sind. Von diesen Ausdrücken (α, β), deren Anzahl $= 4^n$ ist, bieten diejenigen, in welchen $\alpha - \beta$ von 0 verschieden ist, gar kein Interesse dar, weil sie nach Satz I in § 5 alle $= 0$ sind; wir wollen daher nur noch die übrigen betrachten, in denen $\alpha - \beta = 0$, und deren Anzahl $= 3^n$ ist. Von diesen wollen wir vorläufig auch alle diejenigen ausschließen, in denen $\alpha = 0$ ist, also nur solche Elemente (α, β) beibehalten, die durch das System (2) ohne Zuziehung des Elementes (0, 0) gegeben sind. Bezeichnen wir nun mit ν immer die aus allen n Zeichen $1, 2 \cdots n$ bestehende Kombination, und nennen wir jedes Element (ν_1, ν_2), welches der Bedingung $\nu_1 + \nu_2 = \nu$ genügt, einen Kern [sc. des in (2) gegebenen Systems], so ergibt sich aus dem allgemeinen Produktsatz III des § 5, daß jedes andere Element (α, β) als ein Produkt von lauter Kernen darstellbar ist; wählt man nämlich dort für γ diejenige Kombination, welche aus allen in $(\alpha + \beta)$ fehlenden Kombinationselementen besteht, so leuchtet ein, daß alle Faktoren des Produktes

$$(8) \qquad (\alpha, \beta) = \Pi(\alpha + \gamma_1, \beta + \gamma_2)$$

Kerne sind, weil $(\alpha + \gamma_1) + (\beta + \gamma_2) = \alpha + \beta + \gamma = \nu$ ist. Die Anzahl aller Kerne [zu denen $(0, \nu)$ nicht gehört] ist $= 2^n - 1$, und wenn a, b, c die Grade der Kombinationen α, β, γ bedeuten, so ist $a + b + c = n$, und 2^c ist die Anzahl aller Kernfaktoren von (α, β). Von besonderer Wichtigkeit für diese Darstellungen, unter denen sich offenbar auch die in der Überschrift dieses Aufsatzes genannten Zerlegungen der n gegebenen Elemente (2) befinden, ist ferner unser

obiger Satz III, weil er lehrt, wann zwei Kerne gewiß zueinander fremd sind. Für den Fall $n = 4$ geben die Gleichungen (3), (5), (7) des § 2 die Kernzerlegungen der Elemente $(\alpha, 0)$; die übrigen Elemente (α, β) und ihre Zerlegungen, wie z. B.

$$(1,2) = (134,2)(13,24)(14,23)(1,234),$$

sind damals absichtlich gar nicht erwähnt, um die Aufmerksamkeit nicht von der Hauptsache, der Herstellung der Zerlegungen (7), abzulenken. Schließlich ist zu bemerken, daß zufolge des obigen Satzes II alle Kerne mit Ausnahme von $(\nu, 0)$ gewiß ganze Elemente der Gruppe $\mathfrak{G}$ sind, was für $(\nu, 0)$ dann, und nur dann gilt, wenn die gegebenen Elemente (2) sämtlich ganz sind.

Nun noch einige Worte über die Bedeutung der Elemente von der Form $(0, \alpha)$! Sie läßt sich am einfachsten aussprechen, wenn man für das bisher willkürliche Element $(0, 0)$ das Hauptelement $\mathfrak{o}$ der Gruppe $\mathfrak{G}$ wählt. Aus dem Satze VI geht dann, wenn $\omega = 0$ gesetzt wird, das spezielle, der Definition (3) dualistisch entsprechende Resultat hervor, daß $(0, \alpha)^{-1}$ das kleinste gemeinsame Vielfache aller Elemente $(\varepsilon, 0)$ ist, wo ε alle in α enthaltenen Kombinationen ersten Grades durchläuft. Wendet man aber auch auf diese Elemente $(0, \alpha)$ die Zerlegung (8) an, so ergibt sich

$$\mathfrak{o} = (0, 0) = \Pi(\nu_1, \nu_2), \quad (0, \alpha) = \Pi(\gamma_1, \alpha + \gamma_2);$$

in der ersten dieser beiden Formeln findet sich das Produkt aller Kerne multipliziert mit $(0, \nu)$, und folglich ist dieses Produkt das kleinste gemeinsame Vielfache aller n Elemente (2); auch die Faktoren des zweiten Produktes sind mit Ausnahme von $(0, \nu)$ lauter Kerne, und wenn man die erste Gleichung durch die zweite dividiert, so stellt sich auch das obengenannte kleinste gemeinsame Vielfache $(0, \alpha)^{-1}$ als Produkt von lauter Kernen dar, worauf wir aber hier nicht weiter eingehen wollen.

§ 8.

Endliche Dualgruppen in $\mathfrak{G}$.

Wir wollen zum Schluß noch eine Anwendung von den besprochenen Zerlegungen machen. In § 6 ist gezeigt, daß die Abelsche Gruppe $\mathfrak{G}$, wenn es außer der Gruppenoperation (Multiplikation) in ihr noch eine Addition $+$ gibt, welche den dort angegebenen Gesetzen G gehorcht, keine endliche Gruppe (außer $\mathfrak{o}$) als Teiler

enthalten kann, wobei natürlich als Operation der Teilgruppe dieselbe Multiplikation angesehen wurde. Dieselbe Gruppe $\mathfrak{G}$ besitzt nun aber in bezug auf die beiden Operationen $\pm$ auch den Charakter einer Dualgruppe vom Idealtypus, und sie kann, so aufgefaßt, sehr wohl endliche Dualgruppen als Teiler enthalten. Nehmen wir wie in § 7 an, es sei ein System von n Elementen

$$(1) \qquad (1,0),\ (2,0) \cdots (n,0)$$

der Gruppe $\mathfrak{G}$ gegeben, und bilden wir aus ihnen durch stets wiederholte Anwendung beider Operationen $\pm$ immer neue Elemente, welche dem gegebenen System hinzugefügt werden, so wird, wie wir beweisen wollen, diese Bildung nach einer endlichen Anzahl von Schritten ihr Ende finden, insofern die Operationen $\pm$ aus je zwei Elementen, welche in dem so entstandenen System $\mathfrak{P}$ enthalten sind, nur noch solche Elemente erzeugen, welche schon in $\mathfrak{P}$ enthalten sind. Zugleich wird sich ergeben, daß alle Elemente dieser endlichen Dualgruppe $\mathfrak{P}$ sich durch die in § 7 betrachteten Kerne des Systems (1) ausdrücken lassen. Am kürzesten gelangt man synthetisch zum Ziele, indem man umgekehrt von der gemeinsamen Form dieser Ausdrücke ausgeht, deren Auffindung mir erst nach längerem Nachdenken gelungen ist.

Ich erinnere zunächst an die in der Gleichung (8) des § 7 enthaltene Darstellung jedes Elementes von der Form $(\alpha, 0)$, wo α, wie immer im folgenden, von 0 verschieden sein soll, als Produkt von lauter Kernen; stellt man die Kombination β, welche aus allen in α fehlenden Elementen besteht, auf alle verschiedenen Arten als Summe $\beta_1 + \beta_2$ von zwei fremden Kombinationen β_1, β_2 dar, so wird

$$(2) \qquad (\alpha, 0) = \Pi(\alpha + \beta_1, \beta_2),$$

und alle Faktoren $(\alpha + \beta_1, \beta_2)$ sind offenbar Kerne, weil $(\alpha + \beta_1) + \beta_2 = \alpha + \beta = \nu$ ist, wo ν wieder die aus allen n Elementen $1, 2 \cdots n$ bestehende Kombination bedeutet; der Zerlegung $\beta_1 = 0$, $\beta_2 = \beta$ entspricht der Kern (α, β), und ebenso wird der Kern $(\nu, 0)$ durch die Zerlegung $\beta_1 = \beta$, $\beta_2 = 0$ erzeugt.

Unter einem vollständigen Produkt $\mathfrak{p}$ verstehe ich nun jedes Produkt aus lauter verschiedenen*) Kernen $\mathfrak{k}$, welches folgende Eigenschaft besitzt: wenn unter den Faktoren $\mathfrak{k}$ sich der Kern (α, β) befindet,

*) Dies Wort ist hier und im folgenden immer nur im Sinne der äußerlichen Bezeichnung aufzufassen; es kann sehr wohl geschehen, daß in bestimmten Beispielen zwei äußerlich verschiedene Elemente einander gleich werden.

so enthält $\mathfrak{p}$ auch alle anderen Kernfaktoren $(\alpha + \beta_1, \beta_2)$ des Elementes $(\alpha, 0)$ in (2). Unser Ziel besteht darin, zu beweisen, daß die obengenannte Dualgruppe $\mathfrak{P}$ nichts anderes ist als der Inbegriff aller dieser vollständigen Produkte $\mathfrak{p}$. Hierzu führen die folgenden Betrachtungen.

Zunächst überzeugt man sich leicht, daß das Produkt $(\alpha, 0)$ in (2) selbst die genannte Eigenschaft besitzt; denn wenn man aus seinen Faktoren $\mathfrak{k}$ einen bestimmten Kern $(\alpha + \beta_1, \beta_2)$ herausgreift und die Kombination β_2 auf alle Arten als Summe $\beta_3 + \beta_4$ von zwei fremden Kombinationen β_3, β_4 darstellt, so erhält man

$$(\alpha + \beta_1, 0) = \Pi(\alpha + \beta_1 + \beta_3, \beta_4);$$

offenbar befinden sich aber alle Faktoren dieses Produktes auch unter den Faktoren $\mathfrak{k}$ des Produktes (2), und folglich ist $(\alpha, 0)$ wirklich ein vollständiges Produkt.

Aber diese Elemente $(\alpha, 0)$ sind keineswegs die einzigen vollständigen Produkte; wählen wir z. B. $n = 4$ und betrachten das aus sechs verschiedenen Kernen (α, β) gebildete Produkt

$$\mathfrak{p} = (1234,0)(123,4)(124,3)(134,2)(12,34)(13,24),$$

so erhält man nach (2) für die Elemente $(\alpha, 0)$ die Zerlegungen

$$\begin{aligned}
(1234,0) &= (1234,0),\\
(123,0) &= (1234,0)(123,4),\\
(124,0) &= (1234,0)(124,3),\\
(134,0) &= (1234,0)(134,2),\\
(12,0) &= (1234,0)(123,4)(124,3)(12,34),\\
(13,0) &= (1234,0)(123,4)(134,2)(13,24),
\end{aligned}$$

und da alle rechts auftretenden Kerne auch Faktoren des Produktes $\mathfrak{p}$ sind, so ist letzteres vollständig, während z. B. das Produkt

$$(1234,0)(134,2)(12,34)$$

unvollständig ist, weil unter seinen Faktoren die beiden in (12,0) enthaltenen Kerne (123,4), (124,3) fehlen.

Die wichtigste Grundlage für unsere Untersuchung bildet aber der folgende

Satz I. Sind $\mathfrak{p}, \mathfrak{q}$ vollständige Produkte, so gilt dasselbe auch von $\mathfrak{p} \pm \mathfrak{q}$, und zwar ist $\mathfrak{p} + \mathfrak{q}$ das Produkt aller derjenigen verschiedenen Kerne, welche beiden Produkten $\mathfrak{p}, \mathfrak{q}$

gemeinsam sind, und $\mathfrak{p} - \mathfrak{q}$ ist das Produkt aller verschiedenen Kernfaktoren von $\mathfrak{p}\mathfrak{q}$.

Beweis. Wir teilen die in den Produkten $\mathfrak{p}$, $\mathfrak{q}$ auftretenden Kerne in drei Arten ein, in solche (η, ϑ), welche beiden gemeinsam sind, ferner in solche (α, β), welche nur in $\mathfrak{p}$, nicht in $\mathfrak{q}$ auftreten, endlich in solche (γ, δ), welche nur in $\mathfrak{q}$, nicht in $\mathfrak{p}$ auftreten; setzen wir zur Abkürzung die drei entsprechenden Produkte

$$\Pi(\eta, \vartheta) = \mathfrak{r}, \quad \Pi(\alpha, \beta) = \mathfrak{m}, \quad \Pi(\gamma, \delta) = \mathfrak{n},$$

so wird

$$\mathfrak{p} = \mathfrak{r}\mathfrak{m}, \quad \mathfrak{q} = \mathfrak{r}\mathfrak{n}.$$

Wir vergleichen zunächst jeden Faktor (α, β) von $\mathfrak{m}$ mit jedem Faktor (γ, δ) von $\mathfrak{n}$ und setzen $\beta - \gamma = \varrho$, $\alpha - \delta = \sigma$. Macht man nun die Annahme, es sei $\sigma = 0$, so folgt aus dem in § 3, S. 111 bewiesenen Satze, daß $\beta = \varrho + \delta$, $\gamma = \alpha + \varrho$ ist; mithin ist $(\gamma, \delta) = (\alpha + \varrho, \delta)$ ein Kernfaktor von $(\alpha, 0)$, er muß daher, weil (α, β) ein Faktor des vollständigen Produktes $\mathfrak{p}$ ist, ebenfalls Faktor von $\mathfrak{p}$ sein; dies widerspricht aber der obigen Definition von (γ, δ), und folglich ist unsere obige Annahme $\sigma = 0$ unzulässig. Da aus denselben Gründen auch der Durchschnitt $\varrho = \beta - \gamma$ von 0 verschieden und außerdem $\alpha + \beta = \gamma + \delta = \nu$ ist, so folgt (nach Satz III in § 7), daß jeder Faktor (α, β) von $\mathfrak{m}$ fremd zu jedem Faktor (γ, δ) von $\mathfrak{n}$, mithin auch

$$\mathfrak{m} + \mathfrak{n} = \mathfrak{o}, \quad \mathfrak{p} + \mathfrak{q} = \mathfrak{r}(\mathfrak{m} + \mathfrak{n}) = \mathfrak{r}$$

ist. Betrachtet man nun irgendeinen Faktor (η, ϑ) von $\mathfrak{r}$ und zerlegt $(\eta, 0)$ in seine Kernfaktoren nach (2), so muß jeder solche Faktor, weil (η, ϑ) den beiden vollständigen Produkten $\mathfrak{p}, \mathfrak{q}$ gemeinsam ist, ebenfalls gemeinsamer Faktor von $\mathfrak{p}, \mathfrak{q}$, also auch Faktor von $\mathfrak{r}$ sein, und folglich ist $\mathfrak{r}$ ein vollständiges Produkt, womit die Behauptungen des Satzes über $\mathfrak{p} + \mathfrak{q}$ erwiesen sind. Der andere Teil des Satzes ergibt sich leicht aus

$$\mathfrak{p} - \mathfrak{q} = \frac{\mathfrak{p}\mathfrak{q}}{\mathfrak{p} + \mathfrak{q}} = \mathfrak{r}\mathfrak{m}\mathfrak{n} = \mathfrak{p}\mathfrak{n} = \mathfrak{q}\mathfrak{m};$$

denn jeder Faktor (λ, μ) dieses Produktes $\mathfrak{r}\mathfrak{m}\mathfrak{n}$ ist entweder in $\mathfrak{p}$ oder in $\mathfrak{q}$ enthalten, mithin ist auch jeder Kernfaktor von $(\lambda, 0)$ ebenfalls Faktor von $\mathfrak{p}$ oder $\mathfrak{q}$, also gewiß Faktor von $\mathfrak{p} - \mathfrak{q}$, und da auch alle Faktoren (λ, μ) verschieden sind, so ist auch $\mathfrak{p} - \mathfrak{q}$ ein vollständiges Produkt, w. z. b. w.

Durch wiederholte Anwendung dieses Satzes ergibt sich ohne weiteres, daß er auch für beliebig viele vollständige Produkte $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3 \cdots$ gilt; sowohl ihr größter gemeinsamer Teiler $\mathfrak{p}_1 + \mathfrak{p}_2 + \mathfrak{p}_3 + \cdots$ wie ihr kleinstes gemeinsames Vielfaches $\mathfrak{p}_1 - \mathfrak{p}_2 - \mathfrak{p}_3 - \cdots$ sind wieder vollständige Produkte; der erstere ist das Produkt aller derjenigen verschiedenen Kerne, welche allen Produkten $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3 \cdots$ gemeinsam sind, und das letztere ist das Produkt aller verschiedenen, in dem Produkt $\mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3 \cdots$ auftretenden Kerne. Hieraus ergibt sich sofort der

Satz II. Jedes vollständige Produkt $\mathfrak{p}$ von Kernen (α, β) ist das kleinste gemeinsame Vielfache aller ihnen entsprechenden Elemente $(\alpha, 0)$.

Beweis. Jedes Element $(\alpha, 0)$ ist, wie schon oben bemerkt, ein vollständiges Produkt (2), mithin ist ihr kleinstes gemeinsames Vielfaches $\mathfrak{a}$ (nach der eben bewiesenen Regel) das Produkt aller in dem Produkt $\Pi(\alpha, 0)$ auftretenden verschiedenen Kerne $\mathfrak{k}$; alle diese Kerne $\mathfrak{k}$ müssen aber auch in $\mathfrak{p}$ auftreten, weil $\mathfrak{p}$ als vollständiges Produkt zugleich mit (α, β) auch alle Kernfaktoren $\mathfrak{k}$ von $(\alpha, 0)$ zu Faktoren hat. Da umgekehrt jeder in $\mathfrak{p}$ auftretende Kern (α, β) auch ein Faktor des Elementes $(\alpha, 0)$, also einer der Kerne $\mathfrak{k}$ ist, und da alle diese Kerne (α, β) auch verschieden sind, so folgt $\mathfrak{p} = \mathfrak{a}$, w. z. b. w.

Wir kehren nun zu der Dualgruppe $\mathfrak{P}$ zurück, welche aus den gegebenen n Elementen (1) durch wiederholte Anwendung der beiden Operationen $\pm$ entstehen soll. Durch die Operation $+$ werden zunächst alle Elemente von der Form $(\alpha, 0)$ erzeugt, und diese sind, wie oben bemerkt, lauter vollständige Produkte; wendet man sodann auf beliebig viele Elemente $(\alpha, 0)$ des so erzeugten Systems die Operation $-$ an, so erhält man (nach Satz I) immer wieder vollständige Produkte, und zwar entstehen auf diese Weise (nach Satz II) alle vollständigen Produkte; endlich leuchtet ein, daß hiermit die Bildung des Systems $\mathfrak{P}$ schon vollendet ist, weil der Inbegriff aller vollständigen Produkte (nach Satz I) die charakteristischen Eigenschaften einer Dualgruppe besitzt*).

*) Vgl. D. § 169, S. 499, Anmerkung. — Die daselbst erwähnte, aus drei Moduln erzeugte Dualgruppe von 28 Moduln, welche den Idealtypus nicht besitzt, erfordert zu ihrer Bildung eine mehrmals abwechselnde Anwendung der beiden Operationen.

Die Anzahl der in dieser Gruppe $\mathfrak{P}$ enthaltenen Elemente scheint mit der Anzahl n der gegebenen Elemente (1) sehr rasch zu wachsen; sie ist $= 18$ im Falle $n = 3$, und (wenn ich nicht irre) $= 166$ im Falle $n = 4$; einen allgemeinen Ausdruck für diese Anzahl zu finden, habe ich noch nicht versucht. Dagegen leuchtet ein, daß die Elemente von $\mathfrak{P}$, d. h. die vollständigen Produkte $\mathfrak{p}$ sich nach der Anzahl der in ihnen auftretenden Kerne in $(2^n - 1)$ Stufen verteilen, und daß jede folgende Stufe die nächsten Vielfachen von den Elementen der vorhergehenden Stufe enthält. Endlich will ich bemerken, daß diejenigen Elemente von $\mathfrak{P}$, welche auf symmetrische Weise aus den Elementen (1) gebildet sind, in einfachen Beziehungen zu den symmetrischen Funktionen stehen, welche aus den Elementen (1) auf dieselbe Weise wie in der Algebra zusammengesetzt sind*); doch kann ich auf die Darstellung dieser Beziehungen hier nicht mehr eingehen.

Erläuterungen zur vorstehenden Abhandlung.

Diese wenig bekannte Arbeit ist vor allem interessant als frühe axiomatische Untersuchung. Die Dualgruppen werden axiomatisch festgelegt durch zwei Verknüpfungen und zwischen diesen bestehenden Rechengesetzen, wobei sich insbesondere die eine Verknüpfung als Mengen- oder auch als Modulsumme deuten läßt, die andere als Durchschnittsbildung. Zu den Dualgruppen gehören die Modul- und Idealbereiche, die durch das Hinzutreten von Modul- und Idealgesetz gekennzeichnet sind; die Unabhängigkeit dieser neuen Gesetze wird durch Konstruktion passender Beispiele erhärtet (§ 4).

Interessant ist auch der Nachweis des § 6, daß eine Abelsche Gruppe notwendig unendlich oder gleich der Einheit sein muß, wenn außerdem noch die eine Verknüpfung der Dualgruppe in ihr erklärt und distributiv mit der Gruppenverknüpfung verbunden ist. Und weiter, daß eine solche aus einem Element erzeugte Gruppe notwendig auf ganzzahlige, nichtarchimedische Bewertungen führt.

Die Idealtheorie auf Grund der Dedekindschen oder etwas modifizierter Axiome ist von H. Grell (Math. Ann. 97) und W. Krull (Math. Zeitschr. 28) entwickelt worden.

Noether.

---

*) Vgl. D. § 170, S. 503, Anmerkung.
