XXX.

Über die von drei Moduln erzeugte Dualgruppe.

[Mathematische Annalen, Bd. 53, S. 371—403 (1900).]

In der vierten Auflage von Dirichlets Vorlesungen über Zahlentheorie (die im folgenden mit D. zitiert werden soll) habe ich gelegentlich (in den Anmerkungen auf S. 499, 510, 556) die Dualgruppe erwähnt, die aus drei beliebigen Moduln durch fortgesetzte Bildung der gemeinsamen größten Teiler und kleinsten Vielfachen erzeugt wird und im allgemeinen aus 28 verschiedenen Moduln besteht. Da die Gesetze dieser Gruppe sich auf ganz andere Gebiete übertragen lassen und oft eine nützliche Hilfe gewähren, so sollen dieselben im folgenden dargestellt werden; daran schließen sich verschiedene Untersuchungen über allgemeinere Dualgruppen*).

§ 1.

Allgemeine Eigenschaften der Dualgruppen.

Bezeichnet man (wie in D. § 169) mit $a + b$ den größten gemeinsamen Teiler (oder die Summe), mit $a - b$ das kleinste gemeinsame Vielfache (oder den Durchschnitt) der beiden Moduln a, b, so gilt für jede einzelne dieser beiden Operationen $\pm$ zunächst das kommutative und assoziative Gesetz

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

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

mit den bekannten Folgerungen, die sich auf eine beliebige endliche Anzahl von Elementen a, b, $c \cdots$ beziehen (D. § 2).

Die beiden Operationen $\pm$ sind ferner durch die beiden Gesetze

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

miteinander verbunden, und hieraus folgt ohne Zuziehung von (1), (2) auch

(4) $$a + a = a, \qquad a - a = a;$$

*) Vgl. § 4 meines Aufsatzes „Über Zerlegungen von Zahlen durch ihre größten gemeinsamen Teiler“ in der Festschrift unserer Technischen Hochschule für die Naturforscher-Versammlung 1897.

bezeichnet man nämlich die erste und zweite Hälfte einer Doppelgleichung (n) bzw. mit (n') und (n''), so ergibt sich (4'), wenn man $\mathfrak{b}$ in (3') durch $\mathfrak{a} + \mathfrak{b}$ ersetzt, mit Rücksicht auf (3''), und ebenso ergibt sich (4''), wenn man $\mathfrak{b}$ in (3'') durch $\mathfrak{a} - \mathfrak{b}$ ersetzt und (3') beachtet.

Wenn zwei Operationen $\pm$ aus je zwei Elementen $\mathfrak{a}$, $\mathfrak{b}$ eines (endlichen oder unendlichen) Systems $\mathfrak{S}$ zwei Elemente $\mathfrak{a} \pm \mathfrak{b}$ desselben Systems $\mathfrak{S}$ erzeugen und zugleich den Gesetzen (1), (2), (3) genügen, so soll $\mathfrak{S}$ in bezug auf dieses Operationspaar $\pm$ eine Dualgruppe heißen, wie auch sonst diese Elemente beschaffen sein mögen. Die Gesamtheit aller Moduln ist daher eine Dualgruppe bezüglich der beiden Operationen, welche in der Bildung des größten gemeinsamen Teilers und des kleinsten gemeinsamen Vielfachen bestehen*). Zunächst betrachten wir aber einige Eigenschaften, welche jeder Dualgruppe $\mathfrak{S}$ zukommen.

Zufolge (4) bildet jedes Element $\mathfrak{a}$ einer Dualgruppe $\mathfrak{S}$ für sich allein eine Dualgruppe.

Für zwei beliebige Elemente $\mathfrak{a}$, $\mathfrak{b}$ ergibt sich aus (2) und (4), wenn man $\mathfrak{b}$, $\mathfrak{c}$ bzw. durch $\mathfrak{a}$, $\mathfrak{b}$ ersetzt,

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

ersetzt man ferner $\mathfrak{c}$ in (2') durch $(\mathfrak{a} - \mathfrak{b})$, in (2'') durch $(\mathfrak{a} + \mathfrak{b})$, so folgt mit Rücksicht auf (3) auch

$$(6) \quad (\mathfrak{a} + \mathfrak{b}) + (\mathfrak{a} - \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}, \qquad (\mathfrak{a} - \mathfrak{b}) - (\mathfrak{a} + \mathfrak{b}) = \mathfrak{a} - \mathfrak{b};$$

mithin bilden die vier Elemente $\mathfrak{a}$, $\mathfrak{b}$, $(\mathfrak{a} + \mathfrak{b})$, $(\mathfrak{a} - \mathfrak{b})$ gewiß eine Dualgruppe, und es fragt sich nur, wie viele von ihnen verschieden sind.

Nimmt man an, es sei $\mathfrak{a} + \mathfrak{b} = \mathfrak{a} - \mathfrak{b}$, also auch $\mathfrak{a} + (\mathfrak{a} + \mathfrak{b}) = \mathfrak{a} + (\mathfrak{a} - \mathfrak{b})$, so folgt aus (5') und (3') auch $\mathfrak{a} + \mathfrak{b} = \mathfrak{a}$, und da die Annahme symmetrisch in bezug auf $\mathfrak{a}$, $\mathfrak{b}$ ist, so folgt ebenso $\mathfrak{a} + \mathfrak{b} = \mathfrak{b}$, also $\mathfrak{a} = \mathfrak{b}$; und umgekehrt, wenn $\mathfrak{a} = \mathfrak{b}$ ist, so sind alle vier Elemente identisch miteinander.

Machen wir jetzt die (allgemeinere) Annahme, es sei $\mathfrak{a} + \mathfrak{b}$ identisch mit einem der beiden Elemente $\mathfrak{a}$, $\mathfrak{b}$, also z. B. $\mathfrak{a} + \mathfrak{b} = \mathfrak{a}$, so folgt aus (3') durch Vertauschung von $\mathfrak{a}$ mit $\mathfrak{b}$ auch $\mathfrak{a} - \mathfrak{b} = \mathfrak{b}$, und umgekehrt, wenn letzteres der Fall ist, so ergibt sich aus (3') auch $\mathfrak{a} + \mathfrak{b} = \mathfrak{a}$. Da dieser Fall sehr häufig auftritt, so übertragen wir die in der Modultheorie übliche Ausdrucks- und Bezeichnungs-

*) Andere Beispiele von Dualgruppen findet man in der obenerwähnten Schrift (1897). Vgl. den Schluß (§ 8) der gegenwärtigen Abhandlung.

weise (D. § 169) auf alle Dualgruppen $\mathfrak{G}$ und sagen*): das Element b ist teilbar durch das Element a, zugleich heißt b ein Vielfaches von a, und a ein Teiler von b; diese Teilbarkeit wird durch $a < b$ oder $b > a$ bezeichnet, und es ist daher jede der vier Aussagen

$$(7) \qquad a + b = a, \quad a - b = b, \quad a < b, \quad b > a$$

gleichbedeutend mit jeder der drei übrigen; zwei solche Elemente a, b bilden für sich allein eine Dualgruppe. Es ist zweckmäßig, hierbei den Fall $a = b$ nicht auszuschließen; wenn aber a und b verschieden sind, so soll b ein echtes Vielfaches von a und zugleich a ein echter Teiler von b heißen.

Ist endlich keines der beiden Elemente a, b durch das andere teilbar, so besteht die durch sie erzeugte Dualgruppe aus vier verschiedenen Elementen a, b, $a + b$, $a - b$.

Für die durch (7) charakterisierte Teilbarkeit von b durch a ergeben sich durch alleinige Anwendung der Grundgesetze (1), (2), (3) die folgenden Sätze, deren Beweise der Leser leicht finden wird.

I. Immer ist $a < a$, $a > a$.

II. Aus $a < b$ und $a > b$ folgt $a = b$.

III. Aus $a < b$ und $b < c$, was kurz in $a < b < c$ zusammengefaßt wird, folgt $a < c$.

IV. Immer ist $a + b < a$ und $a < a - c$, also auch $a + b < a - c$.

V. Aus $a < b$, $a' < b'$ folgt $a + a' < b + b'$ und $a - a' < b - b'$.

VI. Aus $a < b$, $a' < b$ folgt $a - a' < b$, d. h. jedes gemeinsame Vielfache b von a, a' ist teilbar durch $a - a'$, und aus $a < b$, $a < b'$ folgt $a < b + b'$, d. h. jeder gemeinsame Teiler a von b, b' ist Teiler von $b + b'$. Wegen der Analogie mit der Zahlen- und Modultheorie heißt daher $a - a'$ das kleinste gemeinsame Vielfache von a, a', und $b + b'$ heißt der größte gemeinsame Teiler von b, b'. Diese Ausdrucksweise dehnen wir auch auf mehr als zwei Elemente aus, und durch wiederholte Anwendung des Vorhergehenden ergibt sich der Satz: ist jedes der Elemente a', a'', a''' $\cdots$ ein Teiler von jedem der Elemente b', b'', b''' $\cdots$, so ist

$$a' - a'' - a''' - \cdots < b' + b'' + b''' + \cdots,$$

d. h. das kleinste gemeinsame Vielfache der Elemente a ist ein Teiler des größten gemeinsamen Teilers der Elemente b.

*) Für besondere Dualgruppen $\mathfrak{G}$, deren Elemente schon eine bestimmte Bedeutung haben, kann diese Ausdrucksweise höchst unpassend erscheinen; man wird dann ganz andere, dem Gegenstande entsprechende Namen und Zeichen wählen, wodurch das Wesen der Gesetze offenbar nicht geändert wird.

VII. Ist $\mathfrak{d}$ ein Teiler von $\mathfrak{m}$, also $\mathfrak{d} < \mathfrak{m}$, und $\mathfrak{p}$ ein beliebiges Element, so ist

$$(\mathfrak{p} + \mathfrak{m}) - \mathfrak{d} < (\mathfrak{p} - \mathfrak{d}) + \mathfrak{m};$$

denn jedes der beiden Elemente $\mathfrak{p} + \mathfrak{m}$, $\mathfrak{d}$ ist ein Teiler von jedem der beiden Elemente $\mathfrak{p} - \mathfrak{d}$, $\mathfrak{m}$.

§ 2.

Die von drei Moduln erzeugte Dualgruppe $\mathfrak{D}$.

Hier ist nun der Ort, um eine besondere Eigenschaft der Moduln und der aus ihnen durch die Operationen $+$ erzeugten Dualgruppen hervorzuheben, durch welche die letzteren sich vor anderen Dualgruppen von allgemeinerem Charakter auszeichnen. In der Modultheorie gilt nämlich an Stelle des letzten Satzes VII der bei weitem schärfere Satz (D. § 169, S. 498):

VIII. Ist der Modul $\mathfrak{d}$ ein Teiler des Moduls $\mathfrak{m}$, also $\mathfrak{d} < \mathfrak{m}$, und $\mathfrak{p}$ ein beliebiger Modul, so ist

$$(\mathfrak{p} + \mathfrak{m}) - \mathfrak{d} = (\mathfrak{p} - \mathfrak{d}) + \mathfrak{m}.$$

Aber dieses Modulgesetz ist, wie ich in § 4 meines in der Einleitung zitierten Aufsatzes bewiesen habe*), schlechterdings nicht ableitbar aus den Grundgesetzen (1), (2), (3) und bildet daher eine für die Modultheorie wesentliche Ergänzung derselben. Wir formen dieses Gesetz zunächst in folgender Weise um. Sind $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ drei beliebige Moduln, und ersetzt man $\mathfrak{p}$, $\mathfrak{d}$, $\mathfrak{m}$ bzw. durch $\mathfrak{a}$, $\mathfrak{b} + \mathfrak{c}$, $\mathfrak{b} - \mathfrak{c}$, so ist die Bedingung $\mathfrak{d} < \mathfrak{m}$ erfüllt, und es ergibt sich

$$(8) \qquad (\mathfrak{a} + (\mathfrak{b} - \mathfrak{c})) - (\mathfrak{b} + \mathfrak{c}) = (\mathfrak{a} - (\mathfrak{b} + \mathfrak{c})) + (\mathfrak{b} - \mathfrak{c}),$$

und umgekehrt folgt hieraus wieder das Modulgesetz VIII, wenn man $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ bzw. durch $\mathfrak{p}$, $\mathfrak{d}$, $\mathfrak{m}$ ersetzt und die Annahme $\mathfrak{d} < \mathfrak{m}$ hinzufügt.

Hierauf wenden wir uns zu dem in der Überschrift bezeichneten Gegenstande, nämlich zur Beschreibung der aus drei beliebigen Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ durch die Operationen $+$ erzeugten Dualgruppe $\mathfrak{D}$. Dieselbe ist endlich und besteht aus 28 Moduln, die im allgemeinen voneinander verschieden sind. Vier von diesen Moduln sind symmetrisch aus $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ gebildet und sollen gemeinsam mit $\mathfrak{d}$ bezeichnet, aber durch Akzente und Indizes voneinander unterschieden werden, deren Bedeutung später einleuchten wird:

$$(9) \qquad \mathfrak{d}'''' = \mathfrak{a} + \mathfrak{b} + \mathfrak{c}, \qquad \mathfrak{d}_4 = \mathfrak{a} - \mathfrak{b} - \mathfrak{c},$$

$$(10) \quad \mathfrak{d}' = (\mathfrak{b} + \mathfrak{c}) - (\mathfrak{c} + \mathfrak{a}) - (\mathfrak{a} + \mathfrak{b}), \quad \mathfrak{d}_1 = (\mathfrak{b} - \mathfrak{c}) + (\mathfrak{c} - \mathfrak{a}) + (\mathfrak{a} - \mathfrak{b}).$$

*) Vgl. den Beweis des Satzes IX in § 6 des gegenwärtigen Aufsatzes.

Die übrigen 24 Moduln haben die Eigenschaft, durch alle Vertauschungen von $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ nur drei verschiedene Formen anzunehmen, und diejenigen acht Moduln, welche (wie z. B. $\mathfrak{a}$ selbst) durch Vertauschung von $\mathfrak{b}$ mit $\mathfrak{c}$ nicht geändert werden, sollen gemeinsam mit $\mathfrak{a}$ und zugehörigen Akzenten und Indizes bezeichnet werden, woraus die Bedeutung der mit $\mathfrak{b}$ und $\mathfrak{c}$ bezeichneten 16 Moduln von selbst erhellt. Da die drei Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ durch sich selbst erklärt sind, so bleiben nur die folgenden 21 Definitionen:

$$(11)\qquad \left.\begin{array}{ll} \mathfrak{a}''' = \mathfrak{b} + \mathfrak{c}, & \mathfrak{a}_3 = \mathfrak{b} - \mathfrak{c} \\ \mathfrak{b}''' = \mathfrak{c} + \mathfrak{a}, & \mathfrak{b}_3 = \mathfrak{c} - \mathfrak{a} \\ \mathfrak{c}''' = \mathfrak{a} + \mathfrak{b}, & \mathfrak{c}_3 = \mathfrak{a} - \mathfrak{b} \end{array}\right\},$$

$$(12)\qquad \left.\begin{array}{ll} \mathfrak{a}'' = (\mathfrak{c} + \mathfrak{a}) - (\mathfrak{a} + \mathfrak{b}), & \mathfrak{a}_2 = (\mathfrak{c} - \mathfrak{a}) + (\mathfrak{a} - \mathfrak{b}) \\ \mathfrak{b}'' = (\mathfrak{a} + \mathfrak{b}) - (\mathfrak{b} + \mathfrak{c}), & \mathfrak{b}_2 = (\mathfrak{a} - \mathfrak{b}) + (\mathfrak{b} - \mathfrak{c}) \\ \mathfrak{c}'' = (\mathfrak{b} + \mathfrak{c}) - (\mathfrak{c} + \mathfrak{a}), & \mathfrak{c}_2 = (\mathfrak{b} - \mathfrak{c}) + (\mathfrak{c} - \mathfrak{a}) \end{array}\right\},$$

$$(13)\qquad \left.\begin{array}{ll} \mathfrak{a}' = \mathfrak{a} + (\mathfrak{b} - \mathfrak{c}), & \mathfrak{a}_1 = \mathfrak{a} - (\mathfrak{b} + \mathfrak{c}) \\ \mathfrak{b}' = \mathfrak{b} + (\mathfrak{c} - \mathfrak{a}), & \mathfrak{b}_1 = \mathfrak{b} - (\mathfrak{c} + \mathfrak{a}) \\ \mathfrak{c}' = \mathfrak{c} + (\mathfrak{a} - \mathfrak{b}), & \mathfrak{c}_1 = \mathfrak{c} - (\mathfrak{a} + \mathfrak{b}) \end{array}\right\},$$

$$(14)\qquad \left.\begin{array}{l} \mathfrak{a}_0 = (\mathfrak{a} + (\mathfrak{b} - \mathfrak{c})) - (\mathfrak{b} + \mathfrak{c}) = (\mathfrak{a} - (\mathfrak{b} + \mathfrak{c})) + (\mathfrak{b} - \mathfrak{c}) \\ \mathfrak{b}_0 = (\mathfrak{b} + (\mathfrak{c} - \mathfrak{a})) - (\mathfrak{c} + \mathfrak{a}) = (\mathfrak{b} - (\mathfrak{c} + \mathfrak{a})) + (\mathfrak{c} - \mathfrak{a}) \\ \mathfrak{c}_0 = (\mathfrak{c} + (\mathfrak{a} - \mathfrak{b})) - (\mathfrak{a} + \mathfrak{b}) = (\mathfrak{c} - (\mathfrak{a} + \mathfrak{b})) + (\mathfrak{a} - \mathfrak{b}) \end{array}\right\}.$$

Hier sind überall, wie schon in (9) und (10), die beiden Formen nebeneinander gestellt, welche durch Vertauschung der beiden Operationen $\pm$ auseinander hervorgehen, und hiermit ist immer eine Vertauschung eines oberen Akzentes mit dem entsprechenden unteren Index verbunden; die Doppeldefinitionen (14) beruhen auf dem oben hervorgehobenen Modulgesetz (8).

Wir haben nun zu zeigen, daß der Komplex $\mathfrak{D}$ dieser 28 Moduln wirklich eine Dualgruppe ist, daß also, wenn $\mathfrak{m}$, $\mathfrak{n}$ irgend zwei dieser Moduln bedeuten, auch die beiden Moduln $\mathfrak{m} \pm \mathfrak{n}$ in $\mathfrak{D}$ enthalten sind. Zufolge (4) brauchen wir nur solche Paare zu betrachten, die aus zwei verschiedenen*) Moduln $\mathfrak{m}$, $\mathfrak{n}$ bestehen, und deren Anzahl $= 14 \cdot 27 = 378$ ist. Es ist zweckmäßig, zunächst diejenigen 261 Paare auszusondern, in welchen der eine Modul, z. B. $\mathfrak{m}$ durch den anderen $\mathfrak{n}$ teilbar ist, so daß $\mathfrak{m} + \mathfrak{n} = \mathfrak{n}$, $\mathfrak{m} - \mathfrak{n} = \mathfrak{m}$ wird, was wir wieder durch $\mathfrak{m} > \mathfrak{n}$

*) Weiter unten wird durch ein Beispiel bewiesen, daß die 28 Moduln wirklich alle voneinander verschieden sein können, und der Kürze halber nennen wir sie auch hier verschieden, obgleich sie z. B. in dem Falle $\mathfrak{a} = \mathfrak{b} = \mathfrak{c}$ alle $= \mathfrak{a}$ sind.

oder $n < m$ bezeichnen. Des Raumes wegen begnügen wir uns, von diesen 261 Teilbarkeiten nur die 48 ursprünglichen, d. h. diejenigen aufzuschreiben, aus welchen die übrigen 213 nach dem obigen Satze III in § 1 sich ableiten lassen:

$$(15) \qquad \mathfrak{b}'''' < \mathfrak{a}''', \ \mathfrak{b}''', \ \mathfrak{c}''' ; \quad \mathfrak{b}_4 > \mathfrak{a}_3, \ \mathfrak{b}_3, \ \mathfrak{c}_3,$$

$$(16) \qquad \left\{\begin{array}{lll} \mathfrak{a}''' < \mathfrak{b}'', \ \mathfrak{c}'' & ; & \mathfrak{a}_3 > \mathfrak{b}_2, \ \mathfrak{c}_2 \\ \mathfrak{b}''' < \mathfrak{c}'', \ \mathfrak{a}'' & ; & \mathfrak{b}_3 > \mathfrak{c}_2, \ \mathfrak{a}_2 \\ \mathfrak{c}''' < \mathfrak{a}'', \ \mathfrak{b}'' & ; & \mathfrak{c}_3 > \mathfrak{a}_2, \ \mathfrak{b}_2 \end{array}\right\},$$

$$(17) \qquad \left\{\begin{array}{lll} \mathfrak{a}'' < \mathfrak{b}', \ \mathfrak{a}' & ; & \mathfrak{a}_2 > \mathfrak{b}_1, \ \mathfrak{a}_1 \\ \mathfrak{b}'' < \mathfrak{b}', \ \mathfrak{b}' & ; & \mathfrak{b}_2 > \mathfrak{b}_1, \ \mathfrak{b}_1 \\ \mathfrak{c}'' < \mathfrak{b}', \ \mathfrak{c}' & ; & \mathfrak{c}_2 > \mathfrak{b}_1, \ \mathfrak{c}_1 \end{array}\right\},$$

$$(18) \qquad \left\{\begin{array}{lll} \mathfrak{b}' < \mathfrak{a}_0, \ \mathfrak{b}_0, \ \mathfrak{c}_0 & ; & \mathfrak{b}_1 > \mathfrak{a}_0, \ \mathfrak{b}_0, \ \mathfrak{c}_0 \\ \mathfrak{a}' < \mathfrak{a} \ , \ \mathfrak{a}_0 & ; & \mathfrak{a}_1 > \mathfrak{a} \ , \ \mathfrak{a}_0 \\ \mathfrak{b}' < \mathfrak{b} \ , \ \mathfrak{b}_0 & ; & \mathfrak{b}_1 > \mathfrak{b} \ , \ \mathfrak{b}_0 \\ \mathfrak{c}' < \mathfrak{c} \ , \ \mathfrak{c}_0 & ; & \mathfrak{c}_1 > \mathfrak{c} \ , \ \mathfrak{c}_0 \end{array}\right\}.$$

Die Teilbarkeiten (15) folgen unmittelbar aus der Vergleichung von (9) mit (11), ebenso ergibt sich (16) aus (11) und (12). Von den Teilbarkeiten (17) folgen die auf $\mathfrak{b}'$ und $\mathfrak{b}_1$ bezüglichen aus dem Vergleich von (10) mit (12), die übrigen aus (12) und (13) nach dem Satze VI in § 1. Von den Teilbarkeiten (18) fließen die auf $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ bezüglichen unmittelbar aus (13); da ferner $\mathfrak{a}_0 = \mathfrak{a}' - (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}_1 + (\mathfrak{b} - \mathfrak{c})$ ist, so folgt z. B. $\mathfrak{a}' < \mathfrak{a}_0 < \mathfrak{a}_1$; da endlich $\mathfrak{b}' = \mathfrak{a}'' - (\mathfrak{b} + \mathfrak{c})$ und $\mathfrak{b}_1 = \mathfrak{a}_2 + (\mathfrak{b} - \mathfrak{c})$, zufolge (17) aber auch $\mathfrak{a}'' < \mathfrak{a}'$ und $\mathfrak{a}_2 > \mathfrak{a}_1$ ist, so ergibt sich $\mathfrak{b}' < \mathfrak{a}_0 < \mathfrak{b}_1$, womit (18) vollständig bewiesen ist.

Fügt man zu diesen ursprünglichen Teilbarkeiten noch diejenigen hinzu, welche aus ihnen nach Satz III in § 1 ableitbar sind, und bezeichnet man mit $\varphi(\mathfrak{m})$ die Anzahl aller so erhaltenen Teiler $\mathfrak{n}$ von $\mathfrak{m}$, welche von $\mathfrak{m}$ und voneinander verschieden sind, so ergibt sich sukzessive

$$\begin{array}{llll} \varphi(\mathfrak{b}'''') = 0, & \varphi(\mathfrak{a}''') = 1, & \varphi(\mathfrak{a}'') = 3, & \varphi(\mathfrak{b}') = 7, \\ \varphi(\mathfrak{a}') = 4, & \varphi(\mathfrak{a}) = 5, & \varphi(\mathfrak{a}_0) = 9, & \varphi(\mathfrak{b}_1) = 14, \\ \varphi(\mathfrak{a}_1) = 11, & \varphi(\mathfrak{a}_2) = 17, & \varphi(\mathfrak{a}_3) = 21, & \varphi(\mathfrak{b}_4) = 27; \end{array}$$

rechnet man noch die entsprechenden Anzahlen für die mit $\mathfrak{b}$, $\mathfrak{c}$ bezeichneten Moduln hinzu, so wird die Summe aller $\varphi(\mathfrak{m}) = 261$, und dies ist also die Anzahl aller auf diesem Wege gewonnenen Teilbarkeiten $\mathfrak{m} > \mathfrak{n}$. Daß hiermit auch alle Teilbarkeiten innerhalb der allgemeinen Gruppe $\mathfrak{D}$ erschöpft sind, ergibt sich zugleich aus dem folgenden.

Wir wenden uns jetzt zu den übrigen Paaren $\mathfrak{m}$, $\mathfrak{n}$, um die entsprechenden Moduln $\mathfrak{m} \pm \mathfrak{n}$ anzugeben; des Raumes und des leichteren Überblicks wegen begnügen wir uns, nur 29 solche Paare zu betrachten, aus denen die übrigen durch Vertauschungen von $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ hervorgehen; unter diesen 29 dualistischen Formelpaaren sind 19 Repräsentanten von je 3, und 10 Repräsentanten von je 6 Formelpaaren, woraus sich ihre Gesamtanzahl $= 3 \cdot 19 + 6 \cdot 10 = 117$ ergibt.

(19)
$$\left.\begin{array}{ll} \mathfrak{a} + \mathfrak{a}''' = \mathfrak{d}'''', & \mathfrak{a} - \mathfrak{a}_3 = \mathfrak{d}_4 \\ \mathfrak{a}' + \mathfrak{a}''' = \mathfrak{d}'''', & \mathfrak{a}_1 - \mathfrak{a}_3 = \mathfrak{d}_4 \\ \mathfrak{a}'' + \mathfrak{a}''' = \mathfrak{d}'''', & \mathfrak{a}_2 - \mathfrak{a}_3 = \mathfrak{d}_4 \\ \mathfrak{b}''' + \mathfrak{a}''' = \mathfrak{d}'''', & \mathfrak{b}_3 - \mathfrak{a}_3 = \mathfrak{d}_4 \end{array}\right\},$$

(20)
$$\left.\begin{array}{ll} \mathfrak{b} + \mathfrak{c} = \mathfrak{a}''', & \mathfrak{b} - \mathfrak{c} = \mathfrak{a}_3 \\ \mathfrak{b} + \mathfrak{c}' = \mathfrak{a}''', & \mathfrak{b} - \mathfrak{c}_1 = \mathfrak{a}_3 \\ \mathfrak{b}' + \mathfrak{c}' = \mathfrak{a}''', & \mathfrak{b}_1 - \mathfrak{c}_1 = \mathfrak{a}_3 \\ \mathfrak{b} + \mathfrak{c}'' = \mathfrak{a}''', & \mathfrak{b} - \mathfrak{c}_2 = \mathfrak{a}_3 \\ \mathfrak{b}' + \mathfrak{c}'' = \mathfrak{a}''', & \mathfrak{b}_1 - \mathfrak{c}_2 = \mathfrak{a}_3 \\ \mathfrak{b}'' + \mathfrak{c}'' = \mathfrak{a}''', & \mathfrak{b}_2 - \mathfrak{c}_2 = \mathfrak{a}_3 \end{array}\right\},$$

(21)
$$\left.\begin{array}{ll} \mathfrak{a} + \mathfrak{b}_1 = \mathfrak{a}'', & \mathfrak{a} - \mathfrak{b}' = \mathfrak{a}_2 \\ \mathfrak{a} + \mathfrak{b}_0 = \mathfrak{a}'', & \mathfrak{a} - \mathfrak{b}_0 = \mathfrak{a}_2 \\ \mathfrak{a}' + \mathfrak{b}_1 = \mathfrak{a}'', & \mathfrak{a}_1 - \mathfrak{b}' = \mathfrak{a}_2 \\ \mathfrak{a}' + \mathfrak{b}_0 = \mathfrak{a}'', & \mathfrak{a}_1 - \mathfrak{b}_0 = \mathfrak{a}_2 \\ \mathfrak{a} + \mathfrak{d}' = \mathfrak{a}'', & \mathfrak{a} - \mathfrak{d}_1 = \mathfrak{a}_2 \\ \mathfrak{a}' + \mathfrak{d}' = \mathfrak{a}'', & \mathfrak{a}_1 - \mathfrak{d}_1 = \mathfrak{a}_2 \end{array}\right\},$$

(22)
$$\left.\begin{array}{ll} \mathfrak{a}_1 + \mathfrak{b}_1 = \mathfrak{d}', & \mathfrak{a}' - \mathfrak{b}' = \mathfrak{d}_1 \\ \mathfrak{a}_0 + \mathfrak{b}_1 = \mathfrak{d}', & \mathfrak{a}_0 - \mathfrak{b}' = \mathfrak{d}_1 \\ \mathfrak{a}_0 + \mathfrak{b}_0 = \mathfrak{d}', & \mathfrak{a}_0 - \mathfrak{b}_0 = \mathfrak{d}_1 \end{array}\right\},$$

(23)
$$\left.\begin{array}{ll} \mathfrak{a} + \mathfrak{a}_3 = \mathfrak{a}', & \mathfrak{a} - \mathfrak{a}''' = \mathfrak{a}_1 \\ \mathfrak{a} + \mathfrak{b}_2 = \mathfrak{a}', & \mathfrak{a} - \mathfrak{b}'' = \mathfrak{a}_1 \\ \mathfrak{a} + \mathfrak{d}_1 = \mathfrak{a}', & \mathfrak{a} - \mathfrak{d}' = \mathfrak{a}_1 \\ \mathfrak{a} + \mathfrak{a}_0 = \mathfrak{a}', & \mathfrak{a} - \mathfrak{a}_0 = \mathfrak{a}_1 \end{array}\right\},$$

(24)
$$\left.\begin{array}{ll} \mathfrak{a}_1 + \mathfrak{a}_3 = \mathfrak{a}_0, & \mathfrak{a}' - \mathfrak{a}''' = \mathfrak{a}_0 \\ \mathfrak{a}_1 + \mathfrak{b}_2 = \mathfrak{a}_0, & \mathfrak{a}' - \mathfrak{b}'' = \mathfrak{a}_0 \\ \mathfrak{a}_1 + \mathfrak{d}_1 = \mathfrak{a}_0, & \mathfrak{a}' - \mathfrak{d}' = \mathfrak{a}_0 \end{array}\right\},$$

(25)
$$\left.\begin{array}{ll} \mathfrak{a}_2 + \mathfrak{a}_3 = \mathfrak{d}_1, & \mathfrak{a}'' - \mathfrak{a}''' = \mathfrak{d}' \\ \mathfrak{a}_2 + \mathfrak{b}_2 = \mathfrak{d}_1, & \mathfrak{a}'' - \mathfrak{b}'' = \mathfrak{d}' \end{array}\right\},$$

(26)
$$\mathfrak{b}_3 + \mathfrak{c}_3 = \mathfrak{a}_2, \qquad \mathfrak{b}''' - \mathfrak{c}''' = \mathfrak{a}''.$$

Der Beweis dieser 29 Doppelsätze, welche hier in acht Gruppen, (19) bis (26), geteilt sind, ist nun keineswegs so mühselig, wie man auf den ersten Blick befürchten könnte. Zunächst ergibt sich aus dem dualistischen Charakter der Grundgesetze (1), (2), (3) und des spezifischen Modulgesetzes VIII oder (8), sowie aus der entsprechenden Bezeichnung durch obere Akzente und untere Indizes in den Definitionen (9) bis (14), daß von jedem Doppelsatze nur der erste, auf die Operation + bezügliche Teil bewiesen zu werden braucht, weil hieraus durch gänzliche Vertauschung von + mit — der zweite Teil von selbst hervorgeht. Sodann überzeugt man sich leicht, daß von den in einer Gruppe vereinigten Sätzen immer nur der erste $\mathfrak{m} + \mathfrak{n} = \mathfrak{p}$ besonders zu beweisen ist, weil die übrigen die gemeinsame Form $\mathfrak{m}' + \mathfrak{n}' = \mathfrak{p}$ haben, wo $\mathfrak{m}'$, $\mathfrak{n}'$ zufolge der schon bewiesenen Teilbarkeiten (15) bis (18) den Bedingungen $\mathfrak{m} > \mathfrak{m}' > \mathfrak{p}$, $\mathfrak{n} > \mathfrak{n}' > \mathfrak{p}$ genügen, woraus nach den Sätzen V und III in § 1 wirklich $\mathfrak{m}' + \mathfrak{n}' = \mathfrak{p}$ folgt. Hiernach erledigt sich unser Beweis durch die folgenden Betrachtungen.

Der erste Satz in der Gruppe (19′) folgt unmittelbar aus den Definitionen (9′) und (11′) von $\mathfrak{b}''''$ und $\mathfrak{a}'''$.

Die ersten Sätze in den fünf Gruppen (20′), (23′), (24′), (25′), (26′) erscheinen nur als Wiederholungen der Definitionen (11′), (13′), (14″), (10″), (12″), wenn man die Definitionen (11″), (13″), (12″) beachtet.

Stützt man sich hierauf, so ergeben sich endlich auch die ersten Sätze in den beiden Gruppen (21′), (22′) auf folgende Weise aus dem unter der Voraussetzung $\mathfrak{b} < \mathfrak{m}$ geltenden Modulgesetze VIII

$$(\mathfrak{p} - \mathfrak{b}) + \mathfrak{m} = (\mathfrak{p} + \mathfrak{m}) - \mathfrak{b}.$$

Setzt man nämlich $\mathfrak{p} = \mathfrak{b}$, $\mathfrak{b} = \mathfrak{c} + \mathfrak{a} = \mathfrak{b}'''$, $\mathfrak{m} = \mathfrak{a}$, so ist die Voraussetzung $\mathfrak{b} < \mathfrak{m}$ erfüllt, und zufolge der schon bewiesenen Sätze (23″), (26″) wird $\mathfrak{p} - \mathfrak{b} = \mathfrak{b} - \mathfrak{b}''' = \mathfrak{b}_1$, also $(\mathfrak{p} - \mathfrak{b}) + \mathfrak{m} = \mathfrak{b}_1 + \mathfrak{a}$, ferner $\mathfrak{p} + \mathfrak{m} = \mathfrak{b} + \mathfrak{a} = \mathfrak{c}'''$, $(\mathfrak{p} + \mathfrak{m}) - \mathfrak{b} = \mathfrak{c}''' - \mathfrak{b}''' = \mathfrak{a}''$, wodurch (21′) bewiesen ist. Setzt man aber $\mathfrak{p} = \mathfrak{a}$, $\mathfrak{b} = \mathfrak{b} + \mathfrak{c} = \mathfrak{a}'''$, $\mathfrak{m} = \mathfrak{b} - (\mathfrak{c} + \mathfrak{a}) = \mathfrak{b}_1$, so ist zufolge IV in § 1 die Voraussetzung $\mathfrak{b} < \mathfrak{m}$ erfüllt, und zufolge der schon bewiesenen Sätze (23″), (21′), (25″) wird $\mathfrak{p} - \mathfrak{b} = \mathfrak{a} - \mathfrak{a}''' = \mathfrak{a}_1$, also $(\mathfrak{p} - \mathfrak{b}) + \mathfrak{m} = \mathfrak{a}_1 + \mathfrak{b}_1$, ferner $\mathfrak{p} + \mathfrak{m} = \mathfrak{a} + \mathfrak{b}_1 = \mathfrak{a}''$, $(\mathfrak{p} + \mathfrak{m}) - \mathfrak{b} = \mathfrak{a}'' - \mathfrak{a}''' = \mathfrak{b}'$, wodurch auch (22′) bewiesen ist.

Hiermit ist der vollständige Beweis erbracht, daß je zwei Moduln $\mathfrak{m}$, $\mathfrak{n}$ unseres Systems $\mathfrak{D}$ immer zwei in demselben System enthaltene Moduln $\mathfrak{m} \pm \mathfrak{n}$ erzeugen; mithin bilden diese 28 Moduln wirklich eine Dualgruppe $\mathfrak{D}$. Die Gesamtheit aller Erzeugnisse $\mathfrak{m} \pm \mathfrak{n}$ ist in der beigefügten Tabelle (S. 246, 247) dargestellt, zu deren Erläuterung ich nur folgendes bemerke. Je nachdem das Kreuzungsfeld der Zeile $\mathfrak{m}$ mit der Spalte $\mathfrak{n}$ in die rechte obere oder in die linke untere Hälfte fällt, enthält dasselbe den Modul $\mathfrak{m} + \mathfrak{n}$ oder den Modul $\mathfrak{m} - \mathfrak{n}$, und um die Trennung zwischen diesen beiden Hälften für das Auge recht deutlich zu machen, sind die den Fällen $\mathfrak{m} = \mathfrak{n} = \mathfrak{m} \pm \mathfrak{n}$ entsprechenden Diagonalfelder leer gelassen; die durch stärkere Linien bewirkte Teilung der Tabelle in Rechtecke von verschiedener Größe entspricht der später (in § 5) zu betrachtenden Einteilung aller 28 Moduln in neun verschiedene Stufen.

Aber nun könnte die Frage aufgeworfen werden, ob nicht in der Natur der Moduln gewisse, bis jetzt verborgen gebliebene Eigenschaften liegen, vermöge deren einige, äußerlich zwar verschieden gebildete Moduln dieser Gruppe $\mathfrak{D}$ doch immer miteinander identisch sein müssen. Daß diese Frage zu verneinen ist, daß also diese 28 Moduln im allgemeinen wirklich voneinander verschieden sind, ergibt sich aus dem folgenden Beispiel von zweigliedrigen Moduln (D. § 168, S. 494). Es seien a, b, c, d vier natürliche Zahlen, alle > 1 und so beschaffen, daß je zwei der drei Zahlen a, b, c relative Primzahlen sind, und daß d relative Primzahl zu dem Produkt $(b-c)(c-a)(a-b)$ ist (die kleinsten Zahlen dieser Art sind $a = 2$, $b = 3$, $c = d = 5$); bedeutet ferner ω eine irrationale Zahl, und setzt man

$$\mathfrak{a} = [ad,\ 1 + bc\omega], \quad \mathfrak{b} = [bd,\ 1 + ca\omega], \quad \mathfrak{c} = [cd,\ 1 + ab\omega],$$

so wird

$$\begin{aligned}
\mathfrak{b}'''' &= [1,\ \omega], & \mathfrak{b}_4 &= abcd[1,\ \omega],\\
\mathfrak{b}' &= [1,\ abc\omega], & \mathfrak{b}_1 &= d[1,\ abc\omega],\\
\mathfrak{a}''' &= [1,\ a\omega], & \mathfrak{a}_3 &= bcd[1,\ a\omega],\\
\mathfrak{a}'' &= [1,\ bc\omega], & \mathfrak{a}_2 &= ad[1,\ bc\omega],\\
\mathfrak{a}' &= [d,\ 1 + bc\omega], & \mathfrak{a}_1 &= a[d,\ 1 + bc\omega],\\
& & \mathfrak{a}_0 &= [d,\ a + abc\omega],
\end{aligned}$$

woraus die übrigen 14 Moduln durch Vertauschungen von a, b, c hervorgehen. Der allgemeine Satz, aus welchem diese Bestimmungen

folgen und auf den ich bei einer anderen Gelegenheit zurückkommen werde, lautet: Sind p, p_1, p_2, q, q_1, q_2 sechs (ganze oder gebrochene) rationale Zahlen, von denen wir p, p_2, q, q_2 als positiv voraussetzen wollen, und setzt man

$$\mathfrak{p} = [p, p_1 + p_2\omega], \qquad \mathfrak{q} = [q, q_1 + q_2\omega],$$

so wird

$$\mathfrak{p} + \mathfrak{q} = [d, d_1 + d_2\omega], \qquad \mathfrak{p} - \mathfrak{q} = [m, m_1 + m_2\omega],$$

wo die sechs Zahlen d, d_1, d_2, m, m_1, m_2, von denen man d, d_2, m, m_2 positiv wählen kann, durch folgende Regeln bestimmt werden:

$$[d_2] = [p_2, q_2], \quad [d\,d_2] = [p\,p_2, p\,q_2, q\,p_2, q\,q_2, p_1 q_2 - q_1 p_2],$$

$$\frac{p_2}{d_2} d_1 \equiv p_1, \qquad \frac{q_2}{d_2} d_1 \equiv q_1 \pmod{d}$$

und

$$\left[\frac{1}{m}\right] = \left[\frac{1}{p}, \frac{1}{q}\right], \qquad d\,d_2 m\,m_2 = p\,p_2 q\,q_2,$$

$$\frac{m}{p} m_1 \equiv A p_1, \qquad \frac{m}{q} m_1 \equiv B q_1 \pmod{m},$$

wo

$$A = (\mathfrak{p}, \mathfrak{q}) = \frac{q\,q_2}{d\,d_2} = \frac{m\,m_2}{p\,p_2}, \qquad B = (\mathfrak{q}, \mathfrak{p}) = \frac{p\,p_2}{d\,d_2} = \frac{m\,m_2}{q\,q_2}.$$

Den Beweis dieses Satzes unterdrücke ich der Kürze halber, und ebenso überlasse ich es dem Leser, die Verschiedenheit der obigen 28 Moduln zu bestätigen, wobei es offenbar nur darauf ankommt zu zeigen, daß in den Teilbarkeiten (15) bis (18) nirgends eine Identität auftritt, daß sie also echte Teilbarkeiten sind (D. § 169, S. 496).

§ 3.

Das Symbol (m, n) in der Dualgruppe $\mathfrak{D}$.

Ist die Anzahl der nach dem Modul n inkongruenten Zahlen des Moduls m endlich, so wird sie durch das Symbol (m, n) bezeichnet, während im entgegengesetzten Falle (m, n) = 0 gesetzt wird (D. § 171, S. 509—510). Zufolge dieser Bedeutung des Symbols gelten für je zwei Moduln m, n zunächst die beiden Sätze

(27) $$(\mathfrak{m}, \mathfrak{n}) = (\mathfrak{m} + \mathfrak{n}, \mathfrak{n}),$$

(28) $$(\mathfrak{m}, \mathfrak{n}) = (\mathfrak{m}, \mathfrak{m} - \mathfrak{n}),$$

Tabelle der größten gemeinsamen Teiler (+) und Dualgruppe von 28 Moduln, welche durch

	$\mathfrak{d}'''$	$\mathfrak{a}'''$	$\mathfrak{b}'''$	$\mathfrak{c}'''$	$\mathfrak{a}''$	$\mathfrak{b}''$	$\mathfrak{c}''$	$\mathfrak{d}'$	$\mathfrak{a}'$	$\mathfrak{b}'$	$\mathfrak{c}'$	$\mathfrak{a}$	$\mathfrak{b}$	$\mathfrak{c}$
$\mathfrak{d}'''$		$\mathfrak{d}'''$	$\mathfrak{d}'''$	$\mathfrak{d}'''$	$\mathfrak{d}'''$	$\mathfrak{d}'''$	$\mathfrak{d}'''$	$\mathfrak{d}'''$	$\mathfrak{d}'''$	$\mathfrak{d}'''$	$\mathfrak{d}'''$	$\mathfrak{d}'''$	$\mathfrak{d}'''$	$\mathfrak{d}'''$
$\mathfrak{a}'''$	$\mathfrak{a}'''$		$\mathfrak{d}'''$	$\mathfrak{d}'''$	$\mathfrak{d}'''$	$\mathfrak{a}'''$	$\mathfrak{a}'''$	$\mathfrak{a}'''$	$\mathfrak{d}'''$	$\mathfrak{a}'''$	$\mathfrak{a}'''$	$\mathfrak{d}'''$	$\mathfrak{a}'''$	$\mathfrak{a}'''$
$\mathfrak{b}'''$	$\mathfrak{b}'''$	$\mathfrak{c}''$		$\mathfrak{d}'''$	$\mathfrak{b}'''$	$\mathfrak{d}'''$	$\mathfrak{b}'''$	$\mathfrak{b}'''$	$\mathfrak{b}'''$	$\mathfrak{d}'''$	$\mathfrak{b}'''$	$\mathfrak{b}'''$	$\mathfrak{d}'''$	$\mathfrak{b}'''$
$\mathfrak{c}'''$	$\mathfrak{c}'''$	$\mathfrak{b}''$	$\mathfrak{a}''$		$\mathfrak{c}'''$	$\mathfrak{c}'''$	$\mathfrak{d}'''$	$\mathfrak{c}'''$	$\mathfrak{c}'''$	$\mathfrak{c}'''$	$\mathfrak{d}'''$	$\mathfrak{c}'''$	$\mathfrak{c}'''$	$\mathfrak{d}'''$
$\mathfrak{a}''$	$\mathfrak{a}''$	$\mathfrak{d}'$	$\mathfrak{a}''$	$\mathfrak{a}''$		$\mathfrak{c}'''$	$\mathfrak{b}'''$	$\mathfrak{a}''$	$\mathfrak{a}''$	$\mathfrak{c}'''$	$\mathfrak{b}'''$	$\mathfrak{a}''$	$\mathfrak{c}'''$	$\mathfrak{b}'''$
$\mathfrak{b}''$	$\mathfrak{b}''$	$\mathfrak{b}''$	$\mathfrak{d}'$	$\mathfrak{b}''$	$\mathfrak{d}'$		$\mathfrak{a}'''$	$\mathfrak{b}''$	$\mathfrak{c}'''$	$\mathfrak{b}''$	$\mathfrak{a}'''$	$\mathfrak{c}'''$	$\mathfrak{b}''$	$\mathfrak{a}'''$
$\mathfrak{c}''$	$\mathfrak{c}''$	$\mathfrak{c}''$	$\mathfrak{c}''$	$\mathfrak{d}'$	$\mathfrak{d}'$	$\mathfrak{d}'$		$\mathfrak{c}''$	$\mathfrak{b}'''$	$\mathfrak{a}'''$	$\mathfrak{c}''$	$\mathfrak{b}'''$	$\mathfrak{a}'''$	$\mathfrak{c}''$
$\mathfrak{d}'$	$\mathfrak{d}'$	$\mathfrak{d}'$	$\mathfrak{d}'$	$\mathfrak{d}'$	$\mathfrak{d}'$	$\mathfrak{d}'$	$\mathfrak{d}'$		$\mathfrak{a}''$	$\mathfrak{b}''$	$\mathfrak{c}''$	$\mathfrak{a}''$	$\mathfrak{b}''$	$\mathfrak{c}''$
$\mathfrak{a}'$	$\mathfrak{a}'$	$\mathfrak{a}_0$	$\mathfrak{a}'$	$\mathfrak{a}'$	$\mathfrak{a}'$	$\mathfrak{a}_0$	$\mathfrak{a}_0$	$\mathfrak{a}_0$		$\mathfrak{c}'''$	$\mathfrak{b}'''$	$\mathfrak{a}'$	$\mathfrak{c}'''$	$\mathfrak{b}'''$
$\mathfrak{b}'$	$\mathfrak{b}'$	$\mathfrak{b}'$	$\mathfrak{b}_0$	$\mathfrak{b}'$	$\mathfrak{b}_0$	$\mathfrak{b}'$	$\mathfrak{b}_0$	$\mathfrak{b}_0$	$\mathfrak{d}_1$		$\mathfrak{a}'''$	$\mathfrak{c}'''$	$\mathfrak{b}'$	$\mathfrak{a}'''$
$\mathfrak{c}'$	$\mathfrak{c}'$	$\mathfrak{c}'$	$\mathfrak{c}'$	$\mathfrak{c}_0$	$\mathfrak{c}_0$	$\mathfrak{c}_0$	$\mathfrak{c}'$	$\mathfrak{c}_0$	$\mathfrak{d}_1$	$\mathfrak{d}_1$		$\mathfrak{b}'''$	$\mathfrak{a}'''$	$\mathfrak{c}'$
$\mathfrak{a}$	$\mathfrak{a}$	$\mathfrak{a}_1$	$\mathfrak{a}$	$\mathfrak{a}$	$\mathfrak{a}$	$\mathfrak{a}_1$	$\mathfrak{a}_1$	$\mathfrak{a}_1$	$\mathfrak{a}$	$\mathfrak{a}_2$	$\mathfrak{a}_2$		$\mathfrak{c}'''$	$\mathfrak{b}'''$
$\mathfrak{b}$	$\mathfrak{b}$	$\mathfrak{b}$	$\mathfrak{b}_1$	$\mathfrak{b}$	$\mathfrak{b}_1$	$\mathfrak{b}$	$\mathfrak{b}_1$	$\mathfrak{b}_1$	$\mathfrak{b}_2$	$\mathfrak{b}$	$\mathfrak{b}_2$	$\mathfrak{c}_3$		$\mathfrak{a}'''$
$\mathfrak{c}$	$\mathfrak{c}$	$\mathfrak{c}$	$\mathfrak{c}$	$\mathfrak{c}_1$	$\mathfrak{c}_1$	$\mathfrak{c}_1$	$\mathfrak{c}$	$\mathfrak{c}_1$	$\mathfrak{c}_2$	$\mathfrak{c}_2$	$\mathfrak{c}$	$\mathfrak{b}_3$	$\mathfrak{a}_3$	
$\mathfrak{a}_0$	$\mathfrak{a}_0$	$\mathfrak{a}_0$	$\mathfrak{a}_0$	$\mathfrak{a}_0$	$\mathfrak{a}_0$	$\mathfrak{a}_0$	$\mathfrak{a}_0$	$\mathfrak{a}_0$	$\mathfrak{a}_0$	$\mathfrak{d}_1$	$\mathfrak{d}_1$	$\mathfrak{a}_1$	$\mathfrak{b}_2$	$\mathfrak{c}_2$
$\mathfrak{b}_0$	$\mathfrak{b}_0$	$\mathfrak{b}_0$	$\mathfrak{b}_0$	$\mathfrak{b}_0$	$\mathfrak{b}_0$	$\mathfrak{b}_0$	$\mathfrak{b}_0$	$\mathfrak{b}_0$	$\mathfrak{d}_1$	$\mathfrak{b}_0$	$\mathfrak{d}_1$	$\mathfrak{a}_2$	$\mathfrak{b}_1$	$\mathfrak{c}_2$
$\mathfrak{c}_0$	$\mathfrak{c}_0$	$\mathfrak{c}_0$	$\mathfrak{c}_0$	$\mathfrak{c}_0$	$\mathfrak{c}_0$	$\mathfrak{c}_0$	$\mathfrak{c}_0$	$\mathfrak{c}_0$	$\mathfrak{d}_1$	$\mathfrak{d}_1$	$\mathfrak{c}_0$	$\mathfrak{a}_2$	$\mathfrak{b}_2$	$\mathfrak{c}_1$
$\mathfrak{d}_1$	$\mathfrak{d}_1$	$\mathfrak{d}_1$	$\mathfrak{d}_1$	$\mathfrak{d}_1$	$\mathfrak{d}_1$	$\mathfrak{d}_1$	$\mathfrak{d}_1$	$\mathfrak{d}_1$	$\mathfrak{d}_1$	$\mathfrak{d}_1$	$\mathfrak{d}_1$	$\mathfrak{a}_2$	$\mathfrak{b}_2$	$\mathfrak{c}_2$
$\mathfrak{a}_1$	$\mathfrak{a}_1$	$\mathfrak{a}_1$	$\mathfrak{a}_1$	$\mathfrak{a}_1$	$\mathfrak{a}_1$	$\mathfrak{a}_1$	$\mathfrak{a}_1$	$\mathfrak{a}_1$	$\mathfrak{a}_1$	$\mathfrak{a}_2$	$\mathfrak{a}_2$	$\mathfrak{a}_1$	$\mathfrak{c}_3$	$\mathfrak{b}_3$
$\mathfrak{b}_1$	$\mathfrak{b}_1$	$\mathfrak{b}_1$	$\mathfrak{b}_1$	$\mathfrak{b}_1$	$\mathfrak{b}_1$	$\mathfrak{b}_1$	$\mathfrak{b}_1$	$\mathfrak{b}_1$	$\mathfrak{b}_2$	$\mathfrak{b}_1$	$\mathfrak{b}_2$	$\mathfrak{c}_3$	$\mathfrak{b}_1$	$\mathfrak{a}_3$
$\mathfrak{c}_1$	$\mathfrak{c}_1$	$\mathfrak{c}_1$	$\mathfrak{c}_1$	$\mathfrak{c}_1$	$\mathfrak{c}_1$	$\mathfrak{c}_1$	$\mathfrak{c}_1$	$\mathfrak{c}_1$	$\mathfrak{c}_2$	$\mathfrak{c}_2$	$\mathfrak{c}_1$	$\mathfrak{b}_3$	$\mathfrak{a}_3$	$\mathfrak{c}_1$
$\mathfrak{a}_2$	$\mathfrak{a}_2$	$\mathfrak{a}_2$	$\mathfrak{a}_2$	$\mathfrak{a}_2$	$\mathfrak{a}_2$	$\mathfrak{a}_2$	$\mathfrak{a}_2$	$\mathfrak{a}_2$	$\mathfrak{a}_2$	$\mathfrak{a}_2$	$\mathfrak{a}_2$	$\mathfrak{a}_2$	$\mathfrak{c}_3$	$\mathfrak{b}_3$
$\mathfrak{b}_2$	$\mathfrak{b}_2$	$\mathfrak{b}_2$	$\mathfrak{b}_2$	$\mathfrak{b}_2$	$\mathfrak{b}_2$	$\mathfrak{b}_2$	$\mathfrak{b}_2$	$\mathfrak{b}_2$	$\mathfrak{b}_2$	$\mathfrak{b}_2$	$\mathfrak{b}_2$	$\mathfrak{c}_3$	$\mathfrak{b}_2$	$\mathfrak{a}_3$
$\mathfrak{c}_2$	$\mathfrak{c}_2$	$\mathfrak{c}_2$	$\mathfrak{c}_2$	$\mathfrak{c}_2$	$\mathfrak{c}_2$	$\mathfrak{c}_2$	$\mathfrak{c}_2$	$\mathfrak{c}_2$	$\mathfrak{c}_2$	$\mathfrak{c}_2$	$\mathfrak{c}_2$	$\mathfrak{b}_3$	$\mathfrak{a}_3$	$\mathfrak{c}_2$
$\mathfrak{a}_3$	$\mathfrak{a}_3$	$\mathfrak{a}_3$	$\mathfrak{a}_3$	$\mathfrak{a}_3$	$\mathfrak{a}_3$	$\mathfrak{a}_3$	$\mathfrak{a}_3$	$\mathfrak{a}_3$	$\mathfrak{a}_3$	$\mathfrak{a}_3$	$\mathfrak{a}_3$	$\mathfrak{d}_4$	$\mathfrak{a}_3$	$\mathfrak{a}_3$
$\mathfrak{b}_3$	$\mathfrak{b}_3$	$\mathfrak{b}_3$	$\mathfrak{b}_3$	$\mathfrak{b}_3$	$\mathfrak{b}_3$	$\mathfrak{b}_3$	$\mathfrak{b}_3$	$\mathfrak{b}_3$	$\mathfrak{b}_3$	$\mathfrak{b}_3$	$\mathfrak{b}_3$	$\mathfrak{b}_3$	$\mathfrak{d}_4$	$\mathfrak{b}_3$
$\mathfrak{c}_3$	$\mathfrak{c}_3$	$\mathfrak{c}_3$	$\mathfrak{c}_3$	$\mathfrak{c}_3$	$\mathfrak{c}_3$	$\mathfrak{c}_3$	$\mathfrak{c}_3$	$\mathfrak{c}_3$	$\mathfrak{c}_3$	$\mathfrak{c}_3$	$\mathfrak{c}_3$	$\mathfrak{c}_3$	$\mathfrak{c}_3$	$\mathfrak{d}_4$
$\mathfrak{d}_4$	$\mathfrak{d}_4$	$\mathfrak{d}_4$	$\mathfrak{d}_4$	$\mathfrak{d}_4$	$\mathfrak{d}_4$	$\mathfrak{d}_4$	$\mathfrak{d}_4$	$\mathfrak{d}_4$	$\mathfrak{d}_4$	$\mathfrak{d}_4$	$\mathfrak{d}_4$	$\mathfrak{d}_4$	$\mathfrak{d}_4$	$\mathfrak{d}_4$
—	$\mathfrak{d}'''$	$\mathfrak{a}'''$	$\mathfrak{b}'''$	$\mathfrak{c}'''$	$\mathfrak{a}''$	$\mathfrak{b}''$	$\mathfrak{c}''$	$\mathfrak{d}'$	$\mathfrak{a}'$	$\mathfrak{b}'$	$\mathfrak{c}'$	$\mathfrak{a}$	$\mathfrak{b}$	$\mathfrak{c}$

der kleinsten gemeinsamen Vielfachen (—) in der drei beliebige Moduln a, b, c erzeugt wird.

a_0	b_0	c_0	b_1	a_1	b_1	c_1	a_2	b_2	c_2	a_3	b_3	c_3	b_4	+
b''''	b''''	b''''	b''''	b''''	b''''	b''''	b''''	b''''	b''''	b''''	b''''	b''''	b''''	b''''
a'''	a'''	a'''	a'''	a'''	a'''	a'''	a'''	a'''	a'''	a'''	a'''	a'''	a'''	a'''
b'''	b'''	b'''	b'''	b'''	b'''	b'''	b'''	b'''	b'''	b'''	b'''	b'''	b'''	b'''
c'''	c'''	c'''	c'''	c'''	c'''	c'''	c'''	c'''	c'''	c'''	c'''	c'''	c'''	c'''
a''	a''	a''	a''	a''	a''	a''	a''	a''	a''	a''	a''	a''	a''	a''
b''	b''	b''	b''	b''	b''	b''	b''	b''	b''	b''	b''	b''	b''	b''
c''	c''	c''	c''	c''	c''	c''	c''	c''	c''	c''	c''	c''	c''	c''
b'	b'	b'	b'	b'	b'	b'	b'	b'	b'	b'	b'	b'	b'	b'
a'	a''	a''	a'	a'	a''	a''	a'	a'	a'	a'	a'	a'	a'	a'
b''	b'	b''	b'	b''	b'	b''	b'	b'	b'	b'	b'	b'	b'	b'
c''	c''	c'	c'	c''	c''	c'	c'	c'	c'	c'	c'	c'	c'	c'
a'	a''	a''	a'	a	a''	a''	a	a'	a'	a'	a	a	a	a
b''	b'	b''	b'	b''	b	b''	b'	b	b'	b	b'	b	b	b
c''	c''	c'	c'	c''	c''	c	c'	c'	c	c	c	c'	c	c
	b'	b'	a_0	a_0	b'	b'	a_0	a_0	a_0	a_0	a_0	a_0	a_0	a_0
b_1		b'	b_0	b'	b_0	b'	b_0	b_0	b_0	b_0	b_0	b_0	b_0	b_0
b_1	b_1		c_0	b'	b'	c_0	c_0	c_0	c_0	c_0	c_0	c_0	c_0	c_0
b_1	b_1	b_1		a_0	b_0	c_0	b_1	b_1	b_1	b_1	b_1	b_1	b_1	b_1
a_1	a_2	a_2	a_2		b'	b'	a_1	a_0	a_0	a_0	a_1	a_1	a_1	a_1
b_2	b_1	b_2	b_2	c_3		b'	b_0	b_1	b_0	b_1	b_0	b_1	b_1	b_1
c_2	c_2	c_1	c_2	b_3	a_3		c_0	c_0	c_1	c_1	c_1	c_0	c_1	c_1
a_2	a_2	a_2	a_2	a_2	c_3	b_3		b_1	b_1	b_1	a_2	a_2	a_2	a_2
b_2	b_2	b_2	b_2	c_3	b_2	a_3	c_3		b_1	b_2	b_1	b_2	b_2	b_2
c_2	c_2	c_2	c_2	b_3	a_3	c_2	b_3	a_3		c_2	c_2	b_1	c_2	c_2
a_3	a_3	a_3	a_3	b_4	a_3	a_3	b_4	a_3	a_3		c_2	b_2	a_3	a_3
b_3	b_3	b_3	b_3	b_3	b_4	b_3	b_3	b_4	b_3	b_4		a_2	b_3	b_3
c_3	c_3	c_3	c_3	c_3	c_3	b_4	c_3	c_3	b_4	b_4	b_4		c_3	c_3
b_4	b_4	b_4	b_4	b_4	b_4	b_4	b_4	b_4	b_4	b_4	b_4	b_4		b_4
a_0	b_0	c_0	b_1	a_1	b_1	c_1	a_2	b_2	c_2	a_3	b_3	c_3	b_4	

die wir jetzt auf unsere durch drei beliebige Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ erzeugte Dualgruppe $\mathfrak{D}$ anwenden wollen. Hierbei wählen wir für $\mathfrak{m}$, $\mathfrak{n}$ immer das letzte Modulpaar, welches in den Sätzen (19) bis (26) des § 2 auftritt. Auf diese Weise ergibt sich aus (19) und (26), wenn man $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ zweckmäßig vertauscht,

$$(\mathfrak{b}'''', \mathfrak{a}''') = (\mathfrak{b}''', \mathfrak{a}''') = (\mathfrak{b}''', \mathfrak{c}''),$$
$$(\mathfrak{a}_3, \mathfrak{b}_4) = (\mathfrak{a}_3, \mathfrak{b}_3) = (\mathfrak{c}_2, \mathfrak{b}_3),$$

hierauf aus (20) und (25)

$$(\mathfrak{b}''', \mathfrak{c}'') = (\mathfrak{a}'', \mathfrak{c}'') = (\mathfrak{a}'', \mathfrak{b}'),$$
$$(\mathfrak{c}_2, \mathfrak{b}_3) = (\mathfrak{c}_2, \mathfrak{a}_2) = (\mathfrak{b}_1, \mathfrak{a}_2),$$

hierauf aus (21) und (24)

$$(\mathfrak{a}'', \mathfrak{b}') = (\mathfrak{a}', \mathfrak{b}') = (\mathfrak{a}', \mathfrak{a}_0),$$
$$(\mathfrak{b}_1, \mathfrak{a}_2) = (\mathfrak{b}_1, \mathfrak{a}_1) = (\mathfrak{a}_0, \mathfrak{a}_1),$$

endlich aus (23)

$$(\mathfrak{a}', \mathfrak{a}_0) = (\mathfrak{a}, \mathfrak{a}_0) = (\mathfrak{a}, \mathfrak{a}_1),$$
$$(\mathfrak{a}_0, \mathfrak{a}_1) = (\mathfrak{a}_0, \mathfrak{a}) = (\mathfrak{a}', \mathfrak{a}).$$

Wendet man auf diese Kette von Gleichungen alle Vertauschungen von $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ an, so ergibt sich, daß man sechs Zahlen a', b', c', a_1, b_1, c_1 in folgender Weise durch je sechs Gleichungen definieren kann:

$$(29)\quad \left\{\begin{aligned} a' &= (\mathfrak{b}'''', \mathfrak{a}''') = (\mathfrak{b}''', \mathfrak{c}'') = (\mathfrak{c}''', \mathfrak{b}'') = (\mathfrak{a}'', \mathfrak{b}') = (\mathfrak{a}', \mathfrak{a}_0) = (\mathfrak{a}, \mathfrak{a}_1) \\ b' &= (\mathfrak{b}'''', \mathfrak{b}''') = (\mathfrak{c}''', \mathfrak{a}'') = (\mathfrak{a}''', \mathfrak{c}'') = (\mathfrak{b}'', \mathfrak{b}') = (\mathfrak{b}', \mathfrak{b}_0) = (\mathfrak{b}, \mathfrak{b}_1) \\ c' &= (\mathfrak{b}'''', \mathfrak{c}''') = (\mathfrak{a}''', \mathfrak{b}'') = (\mathfrak{b}''', \mathfrak{a}'') = (\mathfrak{c}'', \mathfrak{b}') = (\mathfrak{c}', \mathfrak{c}_0) = (\mathfrak{c}, \mathfrak{c}_1) \end{aligned}\right\},$$

$$(30)\quad \left\{\begin{aligned} a_1 &= (\mathfrak{a}_3, \mathfrak{b}_4) = (\mathfrak{c}_2, \mathfrak{b}_3) = (\mathfrak{b}_2, \mathfrak{c}_3) = (\mathfrak{b}_1, \mathfrak{a}_2) = (\mathfrak{a}_0, \mathfrak{a}_1) = (\mathfrak{a}', \mathfrak{a}) \\ b_1 &= (\mathfrak{b}_3, \mathfrak{b}_4) = (\mathfrak{a}_2, \mathfrak{c}_3) = (\mathfrak{c}_2, \mathfrak{a}_3) = (\mathfrak{b}_1, \mathfrak{b}_2) = (\mathfrak{b}_0, \mathfrak{b}_1) = (\mathfrak{b}', \mathfrak{b}) \\ c_1 &= (\mathfrak{c}_3, \mathfrak{b}_4) = (\mathfrak{b}_2, \mathfrak{a}_3) = (\mathfrak{a}_2, \mathfrak{b}_3) = (\mathfrak{b}_1, \mathfrak{c}_2) = (\mathfrak{c}_0, \mathfrak{c}_1) = (\mathfrak{c}', \mathfrak{c}) \end{aligned}\right\}.$$

In ganz ähnlicher Weise folgt aus (21) und (24)

$$(\mathfrak{a}'', \mathfrak{a}') = (\mathfrak{b}', \mathfrak{a}') = (\mathfrak{b}', \mathfrak{a}_0),$$
$$(\mathfrak{a}_1, \mathfrak{a}_2) = (\mathfrak{a}_1, \mathfrak{b}_1) = (\mathfrak{a}_0, \mathfrak{b}_1),$$

und aus (22)

$$(\mathfrak{b}', \mathfrak{a}_0) = (\mathfrak{b}_0, \mathfrak{a}_0) = (\mathfrak{b}_0, \mathfrak{b}_1),$$
$$(\mathfrak{a}_0, \mathfrak{b}_1) = (\mathfrak{a}_0, \mathfrak{b}_0) = (\mathfrak{b}', \mathfrak{b}_0),$$

und wenn man in diesen Gleichungen alle Vertauschungen von $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ vornimmt, so ergibt sich, daß man eine siebente Zahl d definieren kann durch die zwölf Gleichungen

$$(31)\quad \left\{\begin{aligned} d &= (\mathfrak{a}'', \mathfrak{a}') = (\mathfrak{b}'', \mathfrak{b}') = (\mathfrak{c}'', \mathfrak{c}') = (\mathfrak{b}', \mathfrak{a}_0) = (\mathfrak{b}', \mathfrak{b}_0) = (\mathfrak{b}', \mathfrak{c}_0) \\ &= (\mathfrak{a}_1, \mathfrak{a}_2) = (\mathfrak{b}_1, \mathfrak{b}_2) = (\mathfrak{c}_1, \mathfrak{c}_2) = (\mathfrak{a}_0, \mathfrak{b}_1) = (\mathfrak{b}_0, \mathfrak{b}_1) = (\mathfrak{c}_0, \mathfrak{b}_1) \end{aligned}\right\}.$$

Offenbar enthalten die Gleichungen (29), (30), (31) alle diejenigen 48 Symbole (m, n), in welchen die Moduln m, n eine der 48 in (15) bis (18) aufgestellten ursprünglichen Teilbarkeiten $m < n$ darbieten.

Die sämtlichen in unserer Dualgruppe $\mathfrak{D}$ auftretenden Symbole (m, n), deren Anzahl $= 28 \cdot 28 = 784$ ist, zerfallen nun in drei Klassen, je nachdem die Teilbarkeit $m > n$ oder $m < n$ oder keine solche Teilbarkeit besteht. Aus der Definition des Symbols folgt unmittelbar (D. S. 510), daß alle 289 Symbole der ersten Klasse, zu denen wir auch die 28 Symbole (m, m) rechnen, $= 1$ sind*). Die 234 Symbole der dritten Klasse lassen sich vermöge der Sätze (27), (28) auf zwei Arten durch Symbole der zweiten Klasse ausdrücken. Unter den 261 Symbolen dieser zweiten Klasse befinden sich zunächst die 48 Symbole (29), (30), (31), deren Werte wir durch die sieben Zahlen d, a', b', c', a_1, b_1, c_1 bezeichnet haben, und die übrigen 213 Symbole, in welchen die Teilbarkeit $m < n$ keine ursprüngliche, sondern eine abgeleitete ist, lassen sich als Produkte dieser Zahlen darstellen; hierzu reichen aber die beiden Sätze (27), (28) nicht aus, sondern dies geht aus einem dritten Satze (D. S. 510) hervor, welcher darin besteht, daß aus $\mathfrak{p} < \mathfrak{q} < \mathfrak{r}$ stets

$$(\mathfrak{p}, \mathfrak{r}) = (\mathfrak{p}, \mathfrak{q})\,(\mathfrak{q}, \mathfrak{r}) \tag{32}$$

folgt.

Wir begnügen uns, das hiernach einzuschlagende Verfahren an denjenigen Symbolen (m, n) der dritten Klasse durchzuführen, in denen m, n mit zwei der drei Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ übereinstimmen. Aus (27) und (11′) folgt zunächst

$$(\mathfrak{b}, \mathfrak{c}) = (\mathfrak{a}''', \mathfrak{c});$$

nach (16′), (17′), (18′) ist aber

$$\mathfrak{a}''' < \mathfrak{c}'' < \mathfrak{c}' < \mathfrak{c},$$

mithin ergibt sich durch zweimalige Anwendung von (32)

$$(\mathfrak{b}, \mathfrak{c}) = (\mathfrak{a}''', \mathfrak{c}'')\,(\mathfrak{c}'', \mathfrak{c}')\,(\mathfrak{c}', \mathfrak{c});$$

*) Stützt man sich nicht auf die Definition des Symbols, sondern nur auf die beiden Sätze (27), (28), so ergibt sich zwar, daß alle Symbole der ersten Klasse denselben Wert haben; daß aber dieser Wert $= 1$ ist, folgt erst aus dem dritten Satze (32), wenn man außerdem noch die Voraussetzung hinzufügt, daß das Symbol $(\mathfrak{a}, \mathfrak{b})$ nicht für alle Modulpaare $\mathfrak{a}$, $\mathfrak{b}$ verschwindet. Ähnliches gilt für das in den Göttinger Nachrichten (1895, Heft 2) erklärte Modulsymbol $(\mathfrak{a}; \mathfrak{b})$. — Vgl. § 8 des gegenwärtigen Aufsatzes.

vertauscht man hierin $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ miteinander und drückt man die Faktoren rechter Hand durch die kürzeren Zeichen in (29), (30), (31) aus, so erhält man

$$(33)\qquad \left\{\begin{array}{ll}(\mathfrak{b},\mathfrak{c}) = b'dc_1, & (\mathfrak{c},\mathfrak{b}) = c'db_1\\ (\mathfrak{c},\mathfrak{a}) = c'da_1, & (\mathfrak{a},\mathfrak{c}) = a'dc_1\\ (\mathfrak{a},\mathfrak{b}) = a'db_1, & (\mathfrak{b},\mathfrak{a}) = b'da_1\end{array}\right\}.$$

Zu demselben Resultate gelangt man aber auch, wenn man den Satz (28) statt (27) anwendet; man erhält zunächst $(\mathfrak{b},\mathfrak{c}) = (\mathfrak{b},\mathfrak{a}_3)$, und da $\mathfrak{b} < \mathfrak{b}_1 < \mathfrak{b}_2 < \mathfrak{a}_3$ ist, so folgt

$$(\mathfrak{b},\mathfrak{c}) = (\mathfrak{b},\mathfrak{b}_1)(\mathfrak{b}_1,\mathfrak{b}_2)(\mathfrak{b}_2,\mathfrak{a}_3),$$

was mit (33′) identisch ist. Auch in allen anderen Beispielen würde sich zeigen, daß die verschiedenen Wege, welche man zur Darstellung eines Symbols $(\mathfrak{m},\mathfrak{n})$ durch die sieben Zahlen d, a', b', c', a_1, b_1, c_1 einschlagen kann, immer zu identischen Resultaten führen, daß also keine Relationen zwischen diesen Zahlen bestehen; doch wollen wir auf den Beweis dieser Behauptung hier nicht eingehen.

Aus den Darstellungen (33), welchen man auch die Form

$$(34)\qquad \left\{\begin{array}{ll}(\mathfrak{b},\mathfrak{c}) = (\mathfrak{b},\mathfrak{b}''')(\mathfrak{c}'',\mathfrak{c}), & (\mathfrak{c},\mathfrak{b}) = (\mathfrak{c},\mathfrak{c}''')(\mathfrak{b}'',\mathfrak{b})\\ (\mathfrak{c},\mathfrak{a}) = (\mathfrak{c},\mathfrak{c}''')(\mathfrak{a}'',\mathfrak{a}), & (\mathfrak{a},\mathfrak{c}) = (\mathfrak{a},\mathfrak{a}''')(\mathfrak{c}'',\mathfrak{c})\\ (\mathfrak{a},\mathfrak{b}) = (\mathfrak{a},\mathfrak{a}''')(\mathfrak{b}'',\mathfrak{b}), & (\mathfrak{b},\mathfrak{a}) = (\mathfrak{b},\mathfrak{b}''')(\mathfrak{a}'',\mathfrak{a})\end{array}\right\}$$

oder die Form

$$(35)\qquad \left\{\begin{array}{ll}(\mathfrak{b},\mathfrak{c}) = (\mathfrak{b},\mathfrak{b}_2)(\mathfrak{c}_3,\mathfrak{c}), & (\mathfrak{c},\mathfrak{b}) = (\mathfrak{c},\mathfrak{c}_2)(\mathfrak{b}_3,\mathfrak{b})\\ (\mathfrak{c},\mathfrak{a}) = (\mathfrak{c},\mathfrak{c}_2)(\mathfrak{a}_3,\mathfrak{a}), & (\mathfrak{a},\mathfrak{c}) = (\mathfrak{a},\mathfrak{a}_2)(\mathfrak{c}_3,\mathfrak{c})\\ (\mathfrak{a},\mathfrak{b}) = (\mathfrak{a},\mathfrak{a}_2)(\mathfrak{b}_3,\mathfrak{b}), & (\mathfrak{b},\mathfrak{a}) = (\mathfrak{b},\mathfrak{b}_2)(\mathfrak{a}_3,\mathfrak{a})\end{array}\right\}$$

geben kann, fließt auch der Satz

$$(36)\qquad (\mathfrak{b},\mathfrak{c})(\mathfrak{c},\mathfrak{a})(\mathfrak{a},\mathfrak{b}) = (\mathfrak{c},\mathfrak{b})(\mathfrak{a},\mathfrak{c})(\mathfrak{b},\mathfrak{a}),$$

welchen ich zuerst in der zweiten Auflage von Dirichlets Vorlesungen über Zahlentheorie erwähnt habe (Anmerkung auf S. 490). Daselbst findet sich auch (in etwas abweichender Ausdrucksweise) die folgende Bemerkung. Nennt man zwei Moduln $\mathfrak{a}$, $\mathfrak{b}$ verwandt, wenn $(\mathfrak{a},\mathfrak{b})$ und $(\mathfrak{b},\mathfrak{a})$ von Null verschieden sind (im Sinne von D. § 171, S. 509), so sind je zwei mit $\mathfrak{a}$ verwandte Moduln $\mathfrak{b}$, $\mathfrak{c}$ auch miteinander verwandt. Dies ergibt sich unmittelbar daraus, daß alle Faktoren, welche in den vorstehenden Ausdrücken (33) oder (34) oder (35) von $(\mathfrak{b},\mathfrak{c})$ und $(\mathfrak{c},\mathfrak{b})$ auftreten, auch Faktoren von mindestens einem der vier Symbole $(\mathfrak{a},\mathfrak{b})$, $(\mathfrak{b},\mathfrak{a})$, $(\mathfrak{a},\mathfrak{c})$, $(\mathfrak{c},\mathfrak{a})$ sind. Man kann

daher alle Moduln in Familien einteilen, indem man je zwei Moduln in dieselbe oder in verschiedene Familien aufnimmt, je nachdem sie miteinander verwandt sind oder nicht; jede Familie ist durch jeden in ihr enthaltenen Modul als Repräsentanten vollständig bestimmt.

§ 4.

Idealgruppen.

In § 2 ist gezeigt, daß die 28 Moduln, aus denen unsere Dualgruppe $\mathfrak{D}$ besteht, im allgemeinen voneinander verschieden sind; wir wollen jetzt einen besonders bemerkenswerten Fall anführen, in welchem die Anzahl der verschiedenen Moduln erheblich geringer ist. Dies tritt immer dann ein, wenn die drei erzeugenden Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ und folglich auch die übrigen Moduln der Gruppe $\mathfrak{D}$ Ideale (oder auch Idealbrüche) eines endlichen Körpers Ω sind, weil dann sehr einfache Beziehungen zwischen den beiden durch $+$ bezeichneten Operationen und der Multiplikation der Moduln bestehen (D. § 178); alle Moduln der Gruppe, von denen höchstens 18 verschieden sein können, lassen sich, wie man leicht findet, in folgender Weise durch $\mathfrak{d}''''$ und sechs vollständig bestimmte Ideale $\mathfrak{p}'$, $\mathfrak{q}'$, $\mathfrak{r}'$, $\mathfrak{p}_1$, $\mathfrak{q}_1$, $\mathfrak{r}_1$ ausdrücken:

$$(37)\quad \left\{\begin{array}{lll} \mathfrak{a} = \mathfrak{q}'\mathfrak{r}'\mathfrak{p}_1\mathfrak{d}'''', & \mathfrak{b} = \mathfrak{r}'\mathfrak{p}'\mathfrak{q}_1\mathfrak{d}'''', & \mathfrak{c} = \mathfrak{p}'\mathfrak{q}'\mathfrak{r}_1\mathfrak{d}'''' \\ \mathfrak{a}''' = \mathfrak{p}'\mathfrak{d}''', & \mathfrak{b}''' = \mathfrak{q}'\mathfrak{d}''', & \mathfrak{c}''' = \mathfrak{r}'\mathfrak{d}''' \\ \mathfrak{a}'' = \mathfrak{a}' = \mathfrak{q}'\mathfrak{r}'\mathfrak{d}''', & \mathfrak{b}'' = \mathfrak{b}' = \mathfrak{r}'\mathfrak{p}'\mathfrak{d}''', & \mathfrak{c}'' = \mathfrak{c}' = \mathfrak{p}'\mathfrak{q}'\mathfrak{d}'''' \\ \mathfrak{d}' = \mathfrak{a}_0 = \mathfrak{b}_0 = \mathfrak{c}_0 = \mathfrak{d}_1 = \mathfrak{p}'\mathfrak{q}'\mathfrak{r}'\mathfrak{d}'''' & & \\ \mathfrak{a}_1 = \mathfrak{a}_2 = \mathfrak{p}_1\mathfrak{d}_1, & \mathfrak{b}_1 = \mathfrak{b}_2 = \mathfrak{q}_1\mathfrak{d}_1, & \mathfrak{c}_1 = \mathfrak{c}_2 = \mathfrak{r}_1\mathfrak{d}_1 \\ \mathfrak{a}_3 = \mathfrak{q}_1\mathfrak{r}_1\mathfrak{d}_1, & \mathfrak{b}_3 = \mathfrak{r}_1\mathfrak{p}_1\mathfrak{d}_1, & \mathfrak{c}_3 = \mathfrak{p}_1\mathfrak{q}_1\mathfrak{d}_1 \\ & \mathfrak{d}_4 = \mathfrak{p}_1\mathfrak{q}_1\mathfrak{r}_1\mathfrak{d}_1 & \end{array}\right\};$$

jedes der drei Paare von Produkten

$$\mathfrak{q}'\mathfrak{r}_1 \text{ und } \mathfrak{r}'\mathfrak{q}_1, \qquad \mathfrak{r}'\mathfrak{p}_1 \text{ und } \mathfrak{p}'\mathfrak{r}_1, \qquad \mathfrak{p}'\mathfrak{q}_1 \text{ und } \mathfrak{q}'\mathfrak{p}_1$$

besteht aus zwei relativen Primidealen, und wenn N die Norm im Körper Ω bedeutet, so gehen die Gleichungen (29), (30), (31) in

$$(38)\quad \left\{\begin{array}{lll} a' = N(\mathfrak{p}'), & b' = N(\mathfrak{q}'), & c' = N(\mathfrak{r}') \\ a_1 = N(\mathfrak{p}_1), & b_1 = N(\mathfrak{q}_1), & c_1 = N(\mathfrak{r}_1) \\ & d = 1 & \end{array}\right\}$$

über.

Wir wollen die drei in diesem Falle auftretenden Spezialgesetze*) $a'' = a'$, $a_2 = a_1$, $b' = b_1$, d. h. die Gesetze

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

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

noch etwas näher betrachten und beweisen, daß, wenn in irgendeiner Dualgruppe $\mathfrak{Z}$ außer den Grundgesetzen (1), (2), (3) noch eins dieser Spezialgesetze allgemein gilt, gewiß auch das Modulgesetz VIII und die beiden anderen Gesetze gelten. In der Tat folgt VIII (unter der Voraussetzung $b < m$) aus (39′) oder (39″) oder (40), wenn man a, b, c bzw. durch m, b, p oder b, m, p oder p, b, m ersetzt; mithin gelten in $\mathfrak{Z}$ auch alle Sätze (19) bis (26). Nimmt man nun an, es gelte das erste Spezialgesetz $a'' = a'$, also auch $b'' = b'$, so folgt daraus das zweite $a_2 = a_1$ und das dritte $b_1 = b'$, weil zufolge (21″), (23″), (22″), (25″) bzw. $a_2 = a - b'$, $a_1 = a - b''$, $b_1 = a' - b'$, $b' = a'' - b''$ ist. Ebenso folgt umgekehrt das erste Gesetz aus dem zweiten, weil $a'' = a + b_1$, $a' = a + b_2$, und aus dem dritten, weil $a'' = a + b'$, $a' = a + b_1$ ist. Hiermit ist unsere Behauptung offenbar erwiesen, und wir können jedes der drei äquivalenten Gesetze (39), (40) als das Idealgesetz bezeichnen; jede Dualgruppe $\mathfrak{Z}$ vom Idealtypus ist auch eine Gruppe vom Modultypus, während umgekehrt, wie aus dem Beispiel der zweigliedrigen Moduln in § 2 erhellt, durchaus nicht jede Gruppe vom Modultypus auch den Idealtypus besitzt.

§ 5.

Das Kettengesetz in der Dualgruppe $\mathfrak{D}$.

Die nun folgenden Betrachtungen sind dazu bestimmt, das Wesen des Modulgesetzes VIII noch tiefer zu ergründen und dessen Folgen für alle Dualgruppen $\mathfrak{M}$ vom Modultypus zu entwickeln, durch welche diese sich unter den allgemeinen Dualgruppen $\mathfrak{G}$ auszeichnen. Hierzu führen wir die folgenden, für jede Dualgruppe $\mathfrak{G}$ gültigen Benennungen ein. Ein Element b soll in $\mathfrak{G}$ ein nächster Teiler**) des Elementes m

*) Sie entsprechen in gewisser Weise dem Operationsgebiet, das in Schröders Algebra der Logik (Bd. 1, S. 291) als der identische Calcul bezeichnet wird, im Gegensatz zu dem logischen Calcul, dem unsere allgemeinen Dualgruppen entsprechen.

**) Vgl. D. § 171, S. 511, wo in der Anmerkung diese Benennung für die aus allen Moduln bestehende Dualgruppe eingeführt ist.

heißen, wenn erstens $\mathfrak{d} < \mathfrak{m}$, zweitens $\mathfrak{d}$ verschieden von $\mathfrak{m}$, also ein echter Teiler von $\mathfrak{m}$ ist, und wenn es drittens in dieser Gruppe $\mathfrak{G}$ außer $\mathfrak{d}$ und $\mathfrak{m}$ kein Element gibt, das ein Teiler von $\mathfrak{m}$ und zugleich ein Vielfaches von $\mathfrak{d}$ ist; zugleich soll $\mathfrak{m}$ ein nächstes Vielfaches von $\mathfrak{d}$ in $\mathfrak{G}$ heißen. Nach dieser Erklärung ist es also, wie wir hervorheben müssen, sehr wohl möglich, daß ein Element $\mathfrak{d}$, welches in $\mathfrak{G}$ ein nächster Teiler des Elementes $\mathfrak{m}$ ist, in einer größeren Dualgruppe $\mathfrak{H}$, welche außer den Elementen von $\mathfrak{G}$ noch andere Elemente enthält, zwar immer ein echter, aber doch kein nächster Teiler von $\mathfrak{m}$ ist; solange es sich aber nur um die Elemente einer einzigen bestimmten Gruppe $\mathfrak{G}$ handelt, wollen wir unbedenklich den Zusatz „in $\mathfrak{G}$“ fortlassen.

Nehmen wir als Beispiel unsere aus drei beliebigen Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ erzeugte Gruppe $\mathfrak{D}$, und setzen wir voraus, daß alle 28 Moduln dieser Gruppe verschieden sind, so leuchtet ein, daß in den 48 ursprünglichen Teilbarkeiten (15) bis (18) sich alle und nur solche Paare von Moduln $\mathfrak{d}$, $\mathfrak{m}$ finden, von denen der eine $\mathfrak{d}$ ein nächster Teiler des anderen $\mathfrak{m}$ in $\mathfrak{D}$ ist. Die vier Moduln $\mathfrak{b}''''$, $\mathfrak{b}'$, $\mathfrak{b}_1$, $\mathfrak{b}_4$ bilden aber für sich eine Dualgruppe $\mathfrak{E}$, und jeder von ihnen ist in $\mathfrak{E}$, aber nicht in $\mathfrak{D}$, ein nächster Teiler des folgenden. Ebenso bilden die vier Moduln $\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{a}'''$, $\mathfrak{a}_3$ für sich eine Gruppe $\mathfrak{A}$, und $\mathfrak{b}$, $\mathfrak{c}$ sind in $\mathfrak{A}$, aber nicht in $\mathfrak{D}$, nächste Vielfache von $\mathfrak{a}'''$ und nächste Teiler von $\mathfrak{a}_3$.

Unter einer Kette der Dualgruppe $\mathfrak{G}$ wollen wir eine endliche Folge von mindestens zwei Elementen in $\mathfrak{G}$ verstehen, deren jedes ein nächster Teiler des nächstfolgenden Elementes ist; diese Elemente sollen die Glieder der Kette, und das erste und letzte Glied sollen bzw. der Anfang und das Ende der Kette heißen; die um eins verminderte Anzahl der Glieder nennen wir die Länge der Kette. Wenn zwei Ketten denselben Anfang und dasselbe Ende haben, so mögen sie äquivalent heißen, und wenn alle Glieder einer Kette $\mathfrak{H}$ auch Glieder einer Kette $\mathfrak{K}$ sind, so nennen wir $\mathfrak{H}$ eine Teilkette von $\mathfrak{K}$.

Nehmen wir als Beispiel wieder unsere aus 28 verschiedenen Moduln bestehende Gruppe $\mathfrak{D}$, so leuchtet ein, daß alle in ihr vorhandenen Ketten sich ebenfalls aus den Teilbarkeiten (15) bis (18) ergeben müssen. Wir wollen nur einige von ihnen betrachten. Es gibt zwei verschiedene äquivalente Ketten

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

welche vom Anfang $\mathfrak{d}''''$ zum Ende $\mathfrak{a}$ führen, während acht verschiedene äquivalente Ketten

$$\begin{array}{ll} \mathfrak{d}''''\,\mathfrak{b}'''\,\mathfrak{a}''\,\mathfrak{a}'\,\mathfrak{a}_0, & \mathfrak{d}''''\,\mathfrak{c}'''\,\mathfrak{a}''\,\mathfrak{a}'\,\mathfrak{a}_0, \\ \mathfrak{d}''''\,\mathfrak{b}'''\,\mathfrak{a}''\,\mathfrak{d}'\,\mathfrak{a}_0, & \mathfrak{d}''''\,\mathfrak{c}'''\,\mathfrak{a}''\,\mathfrak{d}'\,\mathfrak{a}_0, \\ \mathfrak{d}''''\,\mathfrak{c}'''\,\mathfrak{b}''\,\mathfrak{d}'\,\mathfrak{a}_0, & \mathfrak{d}''''\,\mathfrak{a}'''\,\mathfrak{b}''\,\mathfrak{d}'\,\mathfrak{a}_0, \\ \mathfrak{d}''''\,\mathfrak{a}'''\,\mathfrak{c}''\,\mathfrak{d}'\,\mathfrak{a}_0, & \mathfrak{d}''''\,\mathfrak{b}'''\,\mathfrak{c}''\,\mathfrak{d}'\,\mathfrak{a}_0 \end{array}$$

den Anfang $\mathfrak{d}''''$ und das Ende $\mathfrak{a}_0$ haben. Man überzeugt sich ferner leicht, daß jede von $\mathfrak{d}''''$ nach $\mathfrak{d}_4$ führende Kette einen und nur einen der sechs Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{a}_0$, $\mathfrak{b}_0$, $\mathfrak{c}_0$ als Glied enthalten muß, und aus der Symmetrie der Gruppe $\mathfrak{D}$ folgt, daß die Anzahl aller dieser verschiedenen äquivalenten Ketten $= 3 \cdot 2^2 + 3 \cdot 8^2 = 204$ ist; in diesen Ketten sind alle anderen als Teilketten enthalten.

Die wichtigste Erscheinung in dieser Modulgruppe $\mathfrak{D}$ besteht aber darin, daß je zwei äquivalente Ketten auch dieselbe Gliederanzahl, also auch dieselbe Länge besitzen. Um dieses Kettengesetz in $\mathfrak{D}$ tatsächlich nachzuweisen, verteilen wir die 28 Moduln in neun verschiedenen Stufen S_n, wo n die ganzen Zahlen von -4 bis $+4$ durchläuft, und zwar soll bestehen die Stufe

$$(41)\quad \left\{\begin{array}{ll} S_{-4} \text{ aus } \mathfrak{d}'''', & S_4 \text{ aus } \mathfrak{d}_4 \\ S_{-3} \text{ „ } \mathfrak{a}''', \mathfrak{b}''', \mathfrak{c}''', & S_3 \text{ „ } \mathfrak{a}_3, \mathfrak{b}_3, \mathfrak{c}_3 \\ S_{-2} \text{ „ } \mathfrak{a}'', \mathfrak{b}'', \mathfrak{c}'', & S_2 \text{ „ } \mathfrak{a}_2, \mathfrak{b}_2, \mathfrak{c}_2 \\ S_{-1} \text{ „ } \mathfrak{d}', \mathfrak{a}', \mathfrak{b}', \mathfrak{c}', & S_1 \text{ „ } \mathfrak{d}_1, \mathfrak{a}_1, \mathfrak{b}_1, \mathfrak{c}_1 \\ & S_0 \text{ aus } \mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{a}_0, \mathfrak{b}_0, \mathfrak{c}_0 \end{array}\right\}.$$

Betrachtet man nun zwei beliebige aufeinanderfolgende Stufen S_{n-1} und S_n, so lehrt ein Blick auf die Teilbarkeiten (15) bis (18), daß die nächsten Vielfachen eines beliebigen Elementes der Stufe S_{n-1} sämtlich in der Stufe S_n enthalten sind, woraus von selbst folgt, daß auch die nächsten Teiler eines beliebigen Elementes der Stufe S_n sämtlich der Stufe S_{n-1} angehören. Hat man sich hiervon überzeugt, so leuchtet die Wahrheit des obigen Kettengesetzes unmittelbar ein; denn, wenn der Anfang einer Kette in der Stufe S_m, ihr Ende in der Stufe S_{m+n} liegt, so ist offenbar ihre Länge $= n$.

§ 6.

Beziehung zwischen dem Modul- und dem Kettengesetz.

Durch die Wahl der Bezeichnung in der Gruppe $\mathfrak{D}$ von 28 Moduln erscheint das eben besprochene Kettengesetz so selbstverständlich, daß man versucht sein könnte zu glauben, es müsse in jeder Dualgruppe herrschen. Um dieser Meinung sogleich entgegenzutreten, stellen wir folgenden Satz auf:

IX. Wenn in einer Dualgruppe $\mathfrak{H}$ das Modulgesetz VIII nicht allgemein gilt, so ist in $\mathfrak{H}$ eine aus fünf verschiedenen Elementen bestehende Dualgruppe $\mathfrak{G}$ enthalten, in welcher weder das Modulgesetz noch das Kettengesetz gilt.

Beweis. Wir wollen zunächst den auch sonst nützlichen Satz beweisen, daß drei Elemente a, b, c einer beliebigen Dualgruppe $\mathfrak{H}$, welche eine Teilbarkeit

$$b < c, \quad b + c = b, \quad b - c = c$$

darbieten, im allgemeinen eine aus neun Elementen bestehende Dualgruppe $\mathfrak{H}'$ erzeugen; dieselbe enthält außer a, b, c noch sechs Elemente, die wir wie in (11) und (13) durch

$$\begin{aligned} b_3 &= a - c, & c''' &= a + b, \\ b''' &= a + c, & c_3 &= a - b, \\ b_1 &= b - (a + c), & c' &= c + (a - b) \end{aligned}$$

definieren. Zunächst ergeben sich die folgenden 11 ursprünglichen Teilbarkeiten

$$\begin{aligned} c''' &< b\,,\ b'''; & b_3 &> c\,,\ c_3, \\ b &< b_1 \quad ; & c &> c', \\ b''' &< a\,,\ b_1\,; & c_3 &> a\,,\ c', \\ b_1 &< c' \quad ; & c' &> b_1, \end{aligned}$$

deren letzte mit dem Satze VII in § 1 übereinstimmt, wenn dort die Elemente p, b, m bzw. durch a, b, c ersetzt werden; die übrigen folgen mit Rücksicht auf $b < c$ unmittelbar aus den Definitionen. Es gibt nur sechs Paare von Elementen, welche keine Teilbarkeit darbieten; die beiden Paare a, c und a, b erzeugen durch die Ope-

rationen $\pm$ die oben definierten Elemente b_3, b''', c''', c_3; für die übrigen vier Paare ergibt sich aus den Definitionen:

$$b + b''' = c''', \qquad c - c_3 = b_3,$$
$$b - b''' = b_1, \qquad c + c_3 = c',$$

(42) $$a + c' = b''', \qquad a - b_1 = c_3,$$

(43) $$a + b_1 = b''', \qquad a - c' = c_3,$$

und zwar folgen die Sätze (43) aus den Sätzen (42) mit Rücksicht auf $b_1 < c'$, $b''' < b_1$, $c_3 > c'$.

Hiermit ist bewiesen, daß die neun Elemente

$$c''', \; b, \; b''', \; b_1, \; a, \; c', \; c_3, \; c, \; b_3$$

wirklich eine in $\mathfrak{H}$ enthaltene Dualgruppe $\mathfrak{H}'$ bilden, und wir wollen ihre Konstitution, weil sie für manche Untersuchungen wichtig ist, in der folgenden Tabelle darstellen.

	c'''	b	b'''	b_1	a	c'	c_3	c	b_3	$+$
c'''		c'''	c'''	c'''	c'''	c'''	c'''	c'''	c'''	c'''
b	b		c'''	b	c'''	b	b	b	b	b
b'''	b'''	b_1		b'''	b'''	b'''	b'''	b'''	b'''	b'''
b_1	b_1	b_1	b_1		b'''	b_1	b_1	b_1	b_1	b_1
a	a	c_3	a	c_3		b'''	a	b'''	a	a
c'	c'	c'	c'	c'	c_3		c'	c'	c'	c'
c_3	c_3	c_3	c_3	c_3	c_3	c_3		c'	c_3	c_3
c	c	c	c	c	b_3	c	b_3		c	c
b_3	b_3	b_3	b_3	b_3	b_3	b_3	b_3	b_3		b_3
—	c'''	b	b'''	b_1	a	c'	c_3	c	b_3	

Das Durchschnittsfeld der Zeile m und der Spalte n enthält das Element $m + n$ oder $m - n$, je nachdem dieses Feld der rechten oberen oder der linken unteren Hälfte der Tabelle angehört; die Diagonalfelder, welche den Fällen $m = n = m \pm n$ entsprechen, sind zur Erleichterung des Überblicks leer gelassen.

Wenn in der Dualgruppe $\mathfrak{H}$ das Modulgesetz VIII herrscht, so ist $\mathfrak{b}_1 = \mathfrak{c}'$, und die durch $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ erzeugte Dualgruppe $\mathfrak{H}'$ besteht also aus höchstens acht Elementen. Dasselbe ergibt sich aus der Konstitution der oben betrachteten Gruppe $\mathfrak{D}$ von 28 Moduln; denn aus der jetzigen Annahme $\mathfrak{b} < \mathfrak{c}$ folgen leicht die 20 Identitäten

$$\mathfrak{c}'' = \mathfrak{c}' = \mathfrak{b}' = \mathfrak{a}_0 = \mathfrak{b}_0 = \mathfrak{c}_0 = \mathfrak{b}_1 = \mathfrak{b}_1 = \mathfrak{b}_2,$$

$$\mathfrak{a}''' = \mathfrak{b}'' = \mathfrak{b}' = \mathfrak{b}; \qquad \mathfrak{c} = \mathfrak{c}_1 = \mathfrak{c}_2 = \mathfrak{a}_3,$$

$$\mathfrak{b}''' = \mathfrak{a}'' = \mathfrak{a}'; \qquad \mathfrak{a}_1 = \mathfrak{a}_2 = \mathfrak{c}_3,$$

$$\mathfrak{b}'''' = \mathfrak{c}'''; \qquad \mathfrak{b}_3 = \mathfrak{b}_4.$$

Wenn aber, wie wir im folgenden annehmen wollen, in der Dualgruppe $\mathfrak{H}$ das Modulgesetz VIII nicht allgemein gilt, so dürfen wir voraussetzen, die obigen drei Elemente $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ seien mit Berücksichtigung der Bedingung $\mathfrak{b} < \mathfrak{c}$ aus $\mathfrak{H}$ so ausgewählt, daß $\mathfrak{b}_1$ verschieden von $\mathfrak{c}'$, also $\mathfrak{b}_1$ ein echter Teiler von $\mathfrak{c}'$ ist. Wir wollen nun zeigen, daß in diesem Falle die fünf Elemente

$$\mathfrak{b}''', \mathfrak{b}_1, \mathfrak{a}, \mathfrak{c}', \mathfrak{c}_3,$$

welche zufolge der mittleren 25 Felder der obigen Tabelle offenbar für sich eine Dualgruppe $\mathfrak{G}$ bilden*), gewiß voneinander verschieden

*) Denn je zwei Elemente $\mathfrak{m}$, $\mathfrak{n}$ in $\mathfrak{G}$ erzeugen zwei in $\mathfrak{G}$ enthaltene Elemente $\mathfrak{m} \pm \mathfrak{n}$, und außerdem gelten die Grundgesetze (1), (2), (3) für alle Elemente der Dualgruppe $\mathfrak{H}$, also auch für alle Elemente von $\mathfrak{G}$. Dieser Schluß beruht also auf der Hypothese, daß wirklich eine Dualgruppe $\mathfrak{H}$ existiert, in welcher das Modulgesetz nicht allgemein gilt, und es bleibt daher immer noch zweifelhaft, ob diese Hypothese unseres durchaus richtigen Satzes IX an sich zulässig ist, weil sie vielleicht den Grundgesetzen (1), (2), (3) einer jeden Dualgruppe widersprechen könnte. Dieser Zweifel, welcher für den allgemeinen Begriff der Dualgruppe von Bedeutung ist, wird nur dadurch beseitigt, daß für das System $\mathfrak{G}$, in welchem die Zeichen $\pm$ durch die obige Tabelle und die Annahme der Gesetze (1) und (4) vollständig erklärt sind, auch die Gesetze (2) und (3) als identisch erfüllt nachgewiesen werden. Dies ist in § 4 meiner in der Einleitung zitierten Schrift (1897) wirklich geschehen; in der Tat geht die erste der beiden dort auf S. 14 angeführten Dualgruppen in unsere Gruppe $\mathfrak{G}$ über, wenn man α, β, γ, δ, ε bzw. durch $\mathfrak{c}'$, $\mathfrak{a}$, $\mathfrak{b}_1$, $\mathfrak{b}'''$, $\mathfrak{c}_3$ ersetzt. Der auf S. 17 daselbst gegebene Beweis besteht aber nicht in der unmittelbaren Verifikation aller Identitäten (2) und (3), sondern er beruht auf einer allgemeinen Transformation der Grundgesetze (1), (2), (3) in eine ganz andere Gestalt, in welcher die Operationen $\pm$ selbst gar nicht mehr auftreten. Ich bemerke hierbei, daß für endliche Dualgruppen $\mathfrak{A}$ die dortige Eigenschaft VI auf S. 15 durch die folgende einfachere ersetzt werden kann: Für je zwei Dinge α, β in $\mathfrak{A}$ gibt es mindestens ein Ding μ_2 in $\mathfrak{A}$ von der Art, daß α, β beide in dem System μ_2' enthalten sind.

sind; hierbei stützen wir uns auf die Identitäten (42), (43) und auf die schon vorher aufgestellten Teilbarkeiten

(44) $$\mathfrak{b}''' < \mathfrak{a} < \mathfrak{c}_3,$$

(45) $$\mathfrak{b}''' < \mathfrak{b}_1 < \mathfrak{c}' < \mathfrak{c}_3$$

und behaupten zunächst, daß

(46) $$\text{weder } \mathfrak{b}_1 < \mathfrak{a} \text{ noch } \mathfrak{a} < \mathfrak{c}'$$

sein kann. Wäre nämlich $\mathfrak{b}_1 < \mathfrak{a}$, so würde aus (43′), (42″), (43″), (42′) der Reihe nach $\mathfrak{b}_1 = \mathfrak{b}'''$, $\mathfrak{a} = \mathfrak{c}_3$, $\mathfrak{c}' < \mathfrak{a}$, $\mathfrak{c}' = \mathfrak{b}'''$, also auch $\mathfrak{b}_1 = \mathfrak{c}'$ folgen, und zu demselben Widerspruch mit unserer Voraussetzung würde die Annahme $\mathfrak{a} < \mathfrak{c}'$ führen, weil hieraus nach (43″), (42′), (43′), (42″) sich $\mathfrak{c}' = \mathfrak{c}_3$, $\mathfrak{a} = \mathfrak{b}'''$, $\mathfrak{a} < \mathfrak{b}_1$, $\mathfrak{b}_1 = \mathfrak{c}_3$ ergeben würde. Da ferner $\mathfrak{b}_1 < \mathfrak{c}'$ ist, so folgt aus (46) offenbar, daß keins der beiden Elemente $\mathfrak{b}_1$, $\mathfrak{c}'$ ein Teiler oder ein Vielfaches von $\mathfrak{a}$ sein kann, und hieraus ergibt sich weiter, daß in (44) und (45) nur echte Teilbarkeiten auftreten; wäre nämlich $\mathfrak{b}''' = \mathfrak{a}$ oder $\mathfrak{a} = \mathfrak{c}_3$, so würde aus (45) entsprechend $\mathfrak{a} < \mathfrak{c}'$ oder $\mathfrak{b}_1 < \mathfrak{a}$ folgen, und wäre $\mathfrak{b}''' = \mathfrak{b}_1$ oder $\mathfrak{c}' = \mathfrak{c}_3$, so würde aus (44) entsprechend $\mathfrak{b}_1 < \mathfrak{a}$ oder $\mathfrak{a} < \mathfrak{c}'$ folgen, was alles im Widerspruch mit (46) steht. Wir schließen hieraus, daß alle fünf Elemente der Dualgruppe $\mathfrak{G}$ wirklich voneinander verschieden sind, weil auch jede der beiden Annahmen $\mathfrak{a} = \mathfrak{b}_1$ oder $\mathfrak{a} = \mathfrak{c}'$ durch (46) verboten ist.

In dieser Dualgruppe $\mathfrak{G}$ gilt das Modulgesetz VIII nicht, denn sonst müßte, weil $\mathfrak{b}_1 < \mathfrak{c}'$ ist, auch $(\mathfrak{a} - \mathfrak{b}_1) + \mathfrak{c}' = (\mathfrak{a} + \mathfrak{c}') - \mathfrak{b}_1$ sein, während doch aus (42) folgt, daß

$$(\mathfrak{a} - \mathfrak{b}_1) + \mathfrak{c}' = \mathfrak{c}_3 + \mathfrak{c}' = \mathfrak{c}' \quad \text{und} \quad (\mathfrak{a} + \mathfrak{c}') - \mathfrak{b}_1 = \mathfrak{b}''' - \mathfrak{b}_1 = \mathfrak{b}_1$$

ist. Wir behaupten endlich, daß die drei Elemente $\mathfrak{b}'''$, $\mathfrak{a}$, $\mathfrak{c}_3$ in (44) und ebenso die vier Elemente $\mathfrak{b}'''$, $\mathfrak{b}_1$, $\mathfrak{c}'$, $\mathfrak{c}_3$ in (45) eine Kette in $\mathfrak{G}$ bilden; wäre nämlich $\mathfrak{b}'''$ kein nächster Teiler von $\mathfrak{a}$, oder $\mathfrak{c}_3$ kein nächstes Vielfaches von $\mathfrak{a}$, so müßte mindestens eins der beiden anderen Elemente $\mathfrak{b}_1$, $\mathfrak{c}'$ ein Teiler oder ein Vielfaches von $\mathfrak{a}$ sein, was, wie schon erwähnt, zufolge (46) unmöglich ist, und aus demselben Grunde folgt offenbar, daß auch die vier Elemente in (45) eine Kette bilden. Da nun beide Ketten denselben Anfang $\mathfrak{b}'''$ und dasselbe Ende $\mathfrak{c}_3$, aber verschiedene Länge besitzen, so gilt in der Gruppe $\mathfrak{G}$ auch das Kettengesetz nicht.

Den hiermit bewiesenen Satz IX können wir offenbar auch so aussprechen:

X. Wenn in einer Dualgruppe $\mathfrak{H}$ und in allen ihren Teilgruppen das Kettengesetz gilt, so gilt in ihr auch das Modulgesetz.

Hierzu ist folgendes wohl zu bemerken. Man könnte es vielleicht für erlaubt halten, die strenge Prämisse dieses Satzes dahin abzuschwächen, daß die Gültigkeit des Kettengesetzes nur für die Gruppe $\mathfrak{H}$ selbst vorausgesetzt wird; von dieser irrigen Meinung wird man aber sogleich zurückkommen, wenn man sich erinnert, daß die Definitionen eines nächsten Teilers und einer Kette in $\mathfrak{H}$ sich wesentlich auf die Betrachtung aller Elemente von $\mathfrak{H}$ und nur dieser Elemente stützen (§ 5). Man kann sich in der Tat leicht überzeugen, daß das Kettengesetz in einer Dualgruppe $\mathfrak{H}$ gültig und doch in einer Teilgruppe $\mathfrak{G}$ von $\mathfrak{H}$ ungültig sein kann. Das einfachste Beispiel dieser Erscheinung erhält man, wenn man zu den fünf verschiedenen Elementen $m = b'''$, b_1, a, c', c_3, aus denen die eben betrachtete Dualgruppe $\mathfrak{G}$ besteht, noch ein von ihnen verschiedenes sechstes Element n hinzufügt und für dasselbe die Operationen $\pm$ gemäß (4) und (1) durch $n \pm n = n$, $m \pm n = n \pm m$, und zwar im einzelnen durch

$$n + b''' = b''', \quad n + b_1 = b''', \quad n + a = a, \quad n + c' = b''', \quad n + c_3 = n,$$
$$n - b''' = n, \quad n - b_1 = c_3, \quad n - a = n, \quad n - c' = c_3, \quad n - c_3 = c_3$$

definiert. Die genaue Prüfung (vgl. die letzte Anmerkung) ergibt dann, daß diese sechs Elemente wirklich eine Dualgruppe $\mathfrak{H}$ bilden, und daß in derselben das Kettengesetz gilt, weil das einzige Paar äquivalenter verschiedener Ketten aus den beiden Ketten $b''' a n c_3$ und $b''' b_1 c' c_3$ besteht, welche dieselbe Länge 3 besitzen.

Nennen wir jede Dualgruppe $\mathfrak{M}$, in welcher das Modulgesetz VIII allgemein gilt, eine Modulgruppe, auch wenn ihre Elemente keine Moduln sind, so wollen wir nun umgekehrt zeigen, daß in jeder solchen Gruppe auch das Kettengesetz gilt. Dies geschieht durch die folgende Reihe von Sätzen.

XI. Sind a, b zwei beliebige Elemente einer Modulgruppe $\mathfrak{M}$, so besteht zwischen der Gruppe aller derjenigen Elemente b' in $\mathfrak{M}$, welche den Bedingungen

$$(47) \qquad a + b < b' < b$$

genügen, und der Gruppe aller derjenigen Elemente a_1 in $\mathfrak{M}$, welche den Bedingungen

(48) $$a < a_1 < a - b$$

genügen, eine gegenseitige eindeutige Korrespondenz, welche durch jede der beiden, wechselseitig auseinander folgenden Beziehungen

(49) $$a_1 = a - b',$$

(50) $$b' = b + a_1$$

ausgedrückt wird (D. § 169, S. 499, Anmerkung).

Beweis. Unsere Behauptung besteht darin, daß aus (47) und (49) sich (48) und (50) ergibt, und umgekehrt. Aus (47) folgt zunächst $a - (a + b) < a - b' < a - b$, was zufolge (3) und (49) mit (48) übereinstimmt, und da $b' < b$ ist, so folgt nach dem Modulgesetz VIII auch $(a + b) - b' = (a - b') + b$, was nach (47) und (49) mit (50) übereinstimmt. Umgekehrt folgt aus (48) und (50) zunächst $a + b < a_1 + b < (a - b) + b$, also (47), und da $a < a_1$ ist, so folgt nach dem Modulgesetz auch $(a - b) + a_1 = (a_1 + b) - a$, was zufolge (48) und (50) mit (49) übereinstimmt, w. z. b. w.

XII. Sind a, b Elemente einer Modulgruppe $\mathfrak{M}$, und ist $a + b$ ein nächster Teiler von b, so ist a ein nächster Teiler von $a - b$, und umgekehrt.

Beweis. Ist $a + b$ ein nächster, also auch ein echter Teiler von b, so folgt zunächst, daß a auch ein echter Teiler von $a - b$ ist, weil aus $a = a - b$ auch $a + b = b$ folgen würde; genügt nun ein in $\mathfrak{M}$ enthaltenes Element a_1 den Bedingungen (48), so gehört auch das entsprechende Element b' in (50) der Gruppe $\mathfrak{M}$ an, und da zugleich (47) und (49) gilt, so ist entweder $b' = a + b$, also $a_1 = (a + b) - a = a$, oder $b' = b$, also $a_1 = a - b$; mithin ist wirklich a ein nächster Teiler von $a - b$. Umgekehrt, wenn letzteres der Fall, also a auch ein echter Teiler von $a - b$ ist, so folgt zunächst, daß $a + b$ auch ein echter Teiler von b ist, weil aus $a + b = b$ auch $a = a - b$ folgen würde; genügt nun ein in $\mathfrak{M}$ enthaltenes Element b' den Bedingungen (47), so gehört auch das durch (49) definierte Element a_1 der Gruppe $\mathfrak{M}$ an, und da zugleich (48) und (50) gilt, so ist entweder $a_1 = a$, also $b' = a + b$, oder $a_1 = a - b$, also $b' = (a - b) + b = b$; mithin ist wirklich $a + b$ ein nächster Teiler von b, w. z. b. w.

XIII. Ist $\mathfrak{d}$ ein nächster Teiler von $\mathfrak{m}$ in der Modulgruppe $\mathfrak{M}$ und $\mathfrak{p}$ ein beliebiges Element in $\mathfrak{M}$, so ist entweder $\mathfrak{p}+\mathfrak{d}=\mathfrak{p}+\mathfrak{m}$ und $\mathfrak{p}-\mathfrak{d}$ ein nächster Teiler von $\mathfrak{p}-\mathfrak{m}$, oder es ist $\mathfrak{p}-\mathfrak{d}=\mathfrak{p}-\mathfrak{m}$ und $\mathfrak{p}+\mathfrak{d}$ ein nächster Teiler von $\mathfrak{p}+\mathfrak{m}$.

Beweis. Aus der Annahme $\mathfrak{d}<\mathfrak{m}$ folgt nach dem Modulgesetz VIII, daß man ein Element $\mathfrak{q}$ in der doppelten Form

$$\mathfrak{q}=(\mathfrak{p}+\mathfrak{m})-\mathfrak{d}=(\mathfrak{p}-\mathfrak{d})+\mathfrak{m}$$

definieren kann; dasselbe ist offenbar in $\mathfrak{M}$ enthalten und genügt den Bedingungen $\mathfrak{d}<\mathfrak{q}<\mathfrak{m}$, mithin muß, weil $\mathfrak{d}$ ein nächster Teiler von $\mathfrak{m}$ ist, einer und nur einer der beiden Fälle $\mathfrak{q}=\mathfrak{d}$ oder $\mathfrak{q}=\mathfrak{m}$ eintreten. Im ersten Falle ist $\mathfrak{d}=(\mathfrak{p}-\mathfrak{d})+\mathfrak{m}$, und da $\mathfrak{p}+(\mathfrak{p}-\mathfrak{d})=\mathfrak{p}$ ist, so folgt hieraus $\mathfrak{p}+\mathfrak{d}=\mathfrak{p}+\mathfrak{m}$; setzt man nun $\mathfrak{a}=\mathfrak{p}-\mathfrak{d}$, $\mathfrak{b}=\mathfrak{m}$, so wird $\mathfrak{a}+\mathfrak{b}=\mathfrak{d}$, $\mathfrak{a}-\mathfrak{b}=\mathfrak{p}-\mathfrak{d}-\mathfrak{m}=\mathfrak{p}-\mathfrak{m}$; es ist daher $\mathfrak{a}+\mathfrak{b}$ ein nächster Teiler von $\mathfrak{b}$, also nach dem vorigen Satze auch $\mathfrak{p}-\mathfrak{d}$ ein nächster Teiler von $\mathfrak{p}-\mathfrak{m}$. Im zweiten Falle ist $\mathfrak{m}=(\mathfrak{p}+\mathfrak{m})-\mathfrak{d}$, und da $\mathfrak{p}-(\mathfrak{p}+\mathfrak{m})=\mathfrak{p}$ ist, so folgt $\mathfrak{p}-\mathfrak{m}=\mathfrak{p}-\mathfrak{d}$; setzt man jetzt $\mathfrak{a}=\mathfrak{d}$, $\mathfrak{b}=\mathfrak{p}+\mathfrak{m}$, so wird $\mathfrak{a}+\mathfrak{b}=\mathfrak{p}+\mathfrak{m}+\mathfrak{d}=\mathfrak{p}+\mathfrak{b}$, $\mathfrak{a}-\mathfrak{b}=\mathfrak{m}$; es ist daher $\mathfrak{a}$ ein nächster Teiler von $\mathfrak{a}-\mathfrak{b}$, also nach dem vorigen Satze auch $\mathfrak{p}+\mathfrak{b}$ ein nächster Teiler von $\mathfrak{p}+\mathfrak{m}$, w. z. b. w.

XIV. Wenn ein Element $\mathfrak{d}$ einer Modulgruppe $\mathfrak{M}$ zwei verschiedene nächste Vielfache $\mathfrak{a}$, $\mathfrak{b}$ besitzt, so ist $\mathfrak{a}+\mathfrak{b}=\mathfrak{d}$, und $\mathfrak{a}-\mathfrak{b}$ ist ein nächstes Vielfaches von $\mathfrak{a}$ und von $\mathfrak{b}$. Besitzt ein Element $\mathfrak{m}$ zwei verschiedene nächste Teiler $\mathfrak{a}$, $\mathfrak{b}$, so ist $\mathfrak{a}-\mathfrak{b}=\mathfrak{m}$, und $\mathfrak{a}+\mathfrak{b}$ ist ein nächster Teiler von $\mathfrak{a}$ und von $\mathfrak{b}$.

Beweis. Zufolge der ersten Annahme ist $\mathfrak{d}$ ein gemeinsamer Teiler von $\mathfrak{a}$, $\mathfrak{b}$, also auch ein Teiler von $\mathfrak{a}+\mathfrak{b}$, mithin

$$\mathfrak{d}<\mathfrak{a}+\mathfrak{b}<\mathfrak{a}, \qquad \mathfrak{d}<\mathfrak{a}+\mathfrak{b}<\mathfrak{b};$$

wäre nun $\mathfrak{a}+\mathfrak{b}$ verschieden von $\mathfrak{d}$, so müßte, weil $\mathfrak{d}$ ein nächster Teiler von $\mathfrak{a}$ und von $\mathfrak{b}$ ist, $\mathfrak{a}+\mathfrak{b}=\mathfrak{a}$ und zugleich $\mathfrak{a}+\mathfrak{b}=\mathfrak{b}$, also auch $\mathfrak{a}=\mathfrak{b}$ sein, was unserer Annahme widerspricht; mithin ist $\mathfrak{a}+\mathfrak{b}=\mathfrak{d}$ ein nächster Teiler von $\mathfrak{a}$ und $\mathfrak{b}$, woraus nach XII folgt, daß $\mathfrak{b}$ und $\mathfrak{a}$ nächste Teiler von $\mathfrak{a}-\mathfrak{b}$ sind. Zufolge der zweiten Annahme ist $\mathfrak{m}$ ein gemeinsames Vielfaches von $\mathfrak{a}$, $\mathfrak{b}$, also auch ein Vielfaches von $\mathfrak{a}-\mathfrak{b}$, mithin

$$\mathfrak{a}<\mathfrak{a}-\mathfrak{b}<\mathfrak{m}, \qquad \mathfrak{b}<\mathfrak{a}-\mathfrak{b}<\mathfrak{m};$$

wäre nun $a - b$ verschieden von m, so müßte, weil a und b nächste Teiler von m sind, $a - b = a = b$ sein, was unserer Annahme widerspricht; mithin ist $a - b = m$ ein nächstes Vielfaches von a und b, woraus nach XII folgt, daß $a + b$ ein nächster Teiler von b und a ist, w. z. b. w.

Um alle wesentlich verschiedenen Beispiele zu diesem Satze zu finden, welche unsere obige Gruppe $\mathfrak{D}$ von 28 verschiedenen Moduln darbietet, braucht man nur die letzten Sätze in (19) bis (26) mit den Teilbarkeiten in (15) bis (18) zu vergleichen; so erhält man

$$\begin{aligned} a''' + b''' &= b'''', & a''' - b''' &= c'', \\ a'' + b'' &= c''', & a'' - b'' &= b', \\ a' + b' &= a'', & a' - b' &= a_0, \\ a_0 + b_0 &= b', & a_0 - b_0 &= b_1, \\ a + a_0 &= a', & a - a_0 &= a_1, \\ a_1 + b_1 &= a_0, & a_1 - b_1 &= a_2, \\ a_2 + b_2 &= b_1, & a_2 - b_2 &= c_3, \\ a_3 + b_3 &= c_2, & a_3 - b_3 &= b_4. \end{aligned}$$

Wir wollen ferner bemerken, daß die im ersten Teile des Satzes aufgestellte Behauptung $a + b = b$ offenbar für jede Dualgruppe gilt, während die auf $a - b$ bezügliche Behauptung wesentlich auf der Voraussetzung des Modulgesetzes beruht; betrachten wir z. B. die Dualgruppe $\mathfrak{S}$, welche wir bei dem Beweise des Satzes IX gebildet haben, so sind die beiden Elemente a, b_1 nächste Vielfache von $b''' = a + b_1$, aber nur a, nicht b_1, ist ein nächster Teiler von $c_3 = a - b_1$. Ebenso gilt im zweiten Teile nur die Behauptung $a - b = m$ allgemein für jede Dualgruppe, während die auf $a + b$ bezügliche wieder auf dem Modulgesetz beruht.

XV. Wenn in der Modulgruppe $\mathfrak{M}$ eine Kette $\mathfrak{K}$ aus den $n + 1$ Gliedern

$$\mathfrak{k}_0\, \mathfrak{k}_1\, \mathfrak{k}_2 \cdots \mathfrak{k}_{n-1}\, \mathfrak{k}_n \tag{51}$$

besteht, und wenn ein Element $\mathfrak{p}$ der Gruppe $\mathfrak{M}$ den Bedingungen

$$\mathfrak{k}_0 < \mathfrak{p} < \mathfrak{k}_n \tag{52}$$

genügt, so gibt es in $\mathfrak{M}$ mindestens eine mit $\mathfrak{K}$ äquivalente Kette $\mathfrak{P}$, in welcher das Glied $\mathfrak{p}$ auftritt.

Beweis. Durchläuft $\mathfrak{k}$ alle Elemente der Kette $\mathfrak{K}$, und bildet man alle Elemente $\mathfrak{p} \pm \mathfrak{k}$, so erhält man zufolge (52) die beiden Reihen

$$(53) \qquad \mathfrak{p} + \mathfrak{k}_0 = \mathfrak{k}_0,\ \mathfrak{p} + \mathfrak{k}_1 \cdots \mathfrak{p} + \mathfrak{k}_{n-1},\ \mathfrak{p} + \mathfrak{k}_n = \mathfrak{p},$$

$$(54) \qquad \mathfrak{p} - \mathfrak{k}_0 = \mathfrak{p},\ \mathfrak{p} - \mathfrak{k}_1 \cdots \mathfrak{p} - \mathfrak{k}_{n-1},\ \mathfrak{p} - \mathfrak{k}_n = \mathfrak{k}_n.$$

Sieht man die zweite als eine Fortsetzung der ersten an, so entsteht eine Gesamtreihe $\mathfrak{P}'$, in welcher offenbar jedes Element ein Teiler des folgenden ist. Sind zwei solche aufeinanderfolgende Elemente verschieden, so folgt aus dem Satze XIII, daß das erste ein nächster Teiler des folgenden ist; behält man daher von mehreren gleichen aufeinanderfolgenden Elementen immer nur eins bei, so entsteht aus $\mathfrak{P}'$ eine Kette $\mathfrak{P}$, deren Anfang $= \mathfrak{k}_0$, deren Ende $= \mathfrak{k}_n$ ist, und in welcher das Glied $\mathfrak{p}$ auftritt, w. z. b. w.

Zusatz. Diese Kette $\mathfrak{P}$ hat dieselbe Länge n wie $\mathfrak{K}$. Um dies zu beweisen, verteilen wir die n Indizes $0, 1, 2 \cdots (n-1)$ in zwei getrennte Klassen, deren erste alle diejenigen p Indizes r enthält, für welche $\mathfrak{p} + \mathfrak{k}_r$ verschieden von $\mathfrak{p} + \mathfrak{k}_{r+1}$ wird, während die zweite Klasse aus allen übrigen q Indizes s besteht, für welche also $\mathfrak{p} + \mathfrak{k}_s = \mathfrak{p} + \mathfrak{k}_{s+1}$ ist; dann ist $p + q = n$, und offenbar ist $p + 1$ die Anzahl aller verschiedenen, in der Reihe (53) enthaltenen Elemente. Aus dem Satze XIII (welcher bei dem vorhergehenden Beweise von XV nur teilweise benutzt ist) folgt aber, daß gleichzeitig $\mathfrak{p} - \mathfrak{k}_r = \mathfrak{p} - \mathfrak{k}_{r+1}$, und daß $\mathfrak{p} - \mathfrak{k}_s$ verschieden von $\mathfrak{p} - \mathfrak{k}_{s+1}$ ist; mithin ist $q + 1$ die Anzahl aller verschiedenen, in der Reihe (54) enthaltenen Elemente. Da ferner $\mathfrak{p}$ das einzige Element ist, welches in beiden Reihen zugleich auftritt, so ist die Anzahl aller in der Kette $\mathfrak{P}$ enthaltenen Elemente $= (p + 1) + (q + 1) - 1 = n + 1$, w. z. b. w.

Bezeichnet man die aufeinanderfolgenden Elemente dieser Kette $\mathfrak{P}$ mit

$$\mathfrak{p}_0\, \mathfrak{p}_1 \cdots \mathfrak{p}_{n-1}\, \mathfrak{p}_n,$$

so ist $\mathfrak{p}_0 = \mathfrak{k}_0$, $\mathfrak{p}_n = \mathfrak{k}_n$, und zugleich leuchtet aus der Bedeutung von p ein, daß $\mathfrak{p}_p = \mathfrak{p}$ ist.

Um diese durch ein Element $\mathfrak{p}$ bewirkte Transformation einer Kette $\mathfrak{K}$ in eine äquivalente Kette $\mathfrak{P}$ durch Beispiele zu erläutern, kehren wir zu der oben behandelten, aus 28 verschiedenen Moduln bestehenden Gruppe $\mathfrak{D}$ zurück und betrachten die aus neun Elementen

$$\mathfrak{b}''''\, \mathfrak{b}'''\, \mathfrak{a}''\, \mathfrak{a}'\, \mathfrak{a}\, \mathfrak{a}_1\, \mathfrak{a}_2\, \mathfrak{b}_3\, \mathfrak{b}_4$$

bestehende Kette $\mathfrak{K}$ von der Länge acht. Wählen wir $\mathfrak{p} = \mathfrak{c}'$, so bestehen die beiden Reihen (53), (54) aus den Elementen

$$\mathfrak{d}'''' \mathfrak{b}''' \mathfrak{b}''' \mathfrak{b}''' \mathfrak{b}''' \mathfrak{c}'' \mathfrak{c}' \mathfrak{c}' \mathfrak{c}'$$
$$\mathfrak{c}' \mathfrak{c}' \mathfrak{c}_0 \mathfrak{d}_1 \mathfrak{a}_2 \mathfrak{a}_2 \mathfrak{a}_2 \mathfrak{b}_3 \mathfrak{d}_4,$$

und die Kette $\mathfrak{P}$ wird

$$\mathfrak{d}'''' \mathfrak{b}''' \mathfrak{c}'' \mathfrak{c}' \mathfrak{c}_0 \mathfrak{d}_1 \mathfrak{a}_2 \mathfrak{b}_3 \mathfrak{d}_4;$$

zugleich ist $p = 3$, $q = 5$. Wählen wir aber $\mathfrak{p} = \mathfrak{b}$ und dieselbe Kette $\mathfrak{K}$, so bestehen die beiden Reihen (53), (54) aus den Elementen

$$\mathfrak{d}'''' \mathfrak{d}'''' \mathfrak{c}''' \mathfrak{c}''' \mathfrak{c}''' \mathfrak{b}'' \mathfrak{b}' \mathfrak{b}' \mathfrak{b}$$
$$\mathfrak{b} \mathfrak{b}_1 \mathfrak{b}_1 \mathfrak{b}_2 \mathfrak{c}_3 \mathfrak{c}_3 \mathfrak{c}_3 \mathfrak{d}_4 \mathfrak{d}_4,$$

und die Kette $\mathfrak{P}$ wird

$$\mathfrak{d}'''' \mathfrak{c}''' \mathfrak{b}'' \mathfrak{b}' \mathfrak{b} \mathfrak{b}_1 \mathfrak{b}_2 \mathfrak{c}_3 \mathfrak{d}_4;$$

zugleich ist $p = q = 4$.

Aus den beiden vorhergehenden Sätzen XIV und XV ergibt sich nun leicht das Kettengesetz, d. h. der Satz

XVI. In jeder Modulgruppe $\mathfrak{M}$ haben je zwei äquivalente Ketten dieselbe Länge.

Beweis. Um die Methode der vollständigen Induktion anzuwenden, sprechen wir den zu beweisenden Satz so aus: Wenn eine Kette $\mathfrak{K}$ der Modulgruppe $\mathfrak{M}$ die Länge m hat, so hat jede mit $\mathfrak{K}$ äquivalente Kette $\mathfrak{H}$ dieselbe Länge m. Die Wahrheit dieses Satzes für den Fall $m = 1$ ergibt sich daraus, daß eine Kette $\mathfrak{K}$ von der Länge 1 nur mit sich selbst äquivalent ist; besteht nämlich $\mathfrak{K}$ aus den beiden Elementen $\mathfrak{a}$, $\mathfrak{b}$, so ist $\mathfrak{a}$ ein nächster Teiler von $\mathfrak{b}$, und da jedes Element $\mathfrak{h}$ einer Kette $\mathfrak{K}$ ein Vielfaches von ihrem Anfang und zugleich ein Teiler von ihrem Ende ist, so muß, wenn $\mathfrak{H}$ mit $\mathfrak{K}$ äquivalent ist, $\mathfrak{a} < \mathfrak{h} < \mathfrak{b}$, mithin $\mathfrak{h} = \mathfrak{a}$ oder $\mathfrak{h} = \mathfrak{b}$ sein, woraus die Identität von $\mathfrak{H}$ und $\mathfrak{K}$ folgt. Nach dem Wesen der Induktionsmethode machen wir nun die Hypothese, daß, wenn n eine bestimmte natürliche Zahl bedeutet, unser Satz schon für jede Kette $\mathfrak{K}$ bewiesen sei, deren Länge $m = n$ ist, und haben zu zeigen, daß er dann gewiß auch für jede Kette $\mathfrak{K}$ gelten muß, deren Länge $m = n + 1$ ist. Es sei also $\mathfrak{K}$ eine aus den Gliedern

$$\mathfrak{a} \mathfrak{k}_1 \mathfrak{k}_2 \cdots \mathfrak{k}_{n-1} \mathfrak{k}_n \mathfrak{b}$$

bestehende Kette von der Länge $n + 1$, und irgendeine mit $\mathfrak{K}$ äquivalente Kette $\mathfrak{H}$ möge aus den $e + 2$ Gliedern

$$\mathfrak{a} \mathfrak{h}_1 \mathfrak{h}_2 \cdots \mathfrak{h}_{e-1} \mathfrak{h}_e \mathfrak{b}$$

bestehen; wir sollen beweisen, daß $e = n$ ist. Unterdrücken wir in beiden Ketten $\mathfrak{K}$, $\mathfrak{H}$ den gemeinsamen Anfang a, so entsteht aus $\mathfrak{K}$ eine Teilkette $\mathfrak{K}_1$ von der Länge n, deren Anfang und Ende bzw. die Elemente $\mathfrak{k}_1$, b sind, und ebenso entspringt aus $\mathfrak{H}$ eine Teilkette $\mathfrak{H}_1$ von der Länge e, deren Anfang und Ende bzw. die Elemente $\mathfrak{h}_1$, b sind. Falls nun $\mathfrak{k}_1 = \mathfrak{h}_1$ ist, so sind diese beiden Ketten $\mathfrak{K}_1$, $\mathfrak{H}_1$ äquivalent, und da die Länge der ersteren $= n$ ist, so muß nach unserer Hypothese auch $\mathfrak{H}_1$ dieselbe Länge haben, woraus wirklich $e = n$ folgt. Im entgegengesetzten Falle, wenn die beiden Elemente $\mathfrak{k}_1$, $\mathfrak{h}_1$ verschieden sind, schließen wir aus dem Satze XIV, daß sie als nächste Vielfache desselben Elementes a auch nächste Teiler desselben Elementes $\mathfrak{k}_1 - \mathfrak{h}_1$ sind, das wir mit $\mathfrak{p}$ bezeichnen wollen. Da $\mathfrak{k}_1$ und $\mathfrak{h}_1$ auch Teiler desselben Elementes b sind, so genügt $\mathfrak{p}$ offenbar den Bedingungen $\mathfrak{k}_1 < \mathfrak{p} < b$, und folglich gibt es nach dem Satze XV eine mit $\mathfrak{K}_1$ äquivalente Kette $\mathfrak{P}$, in welcher $\mathfrak{p}$ als Glied auftritt, und welche nach unserer Hypothese dieselbe Länge n besitzen muß wie $\mathfrak{K}_1$ (das letztere würde auch aus dem Zusatze zu XV folgen, den wir aber bei diesem Beweise nicht zu benutzen brauchen). Da ferner, wie schon bemerkt, $\mathfrak{k}_1$ ein nächster Teiler von $\mathfrak{p}$ ist, so muß in dieser Kette $\mathfrak{P}$ das Glied $\mathfrak{p}$ unmittelbar auf $\mathfrak{k}_1$ folgen; die Kette $\mathfrak{P}$ hat daher die Form

$$\mathfrak{k}_1\, \mathfrak{p} \cdots b.$$

Nun ist, wie oben bemerkt, auch $\mathfrak{h}_1$ ein nächster Teiler von $\mathfrak{p}$; ersetzen wir daher den Anfang $\mathfrak{k}_1$ der Kette $\mathfrak{P}$ durch $\mathfrak{h}_1$, so entsteht abermals eine Kette

$$\mathfrak{h}_1\, \mathfrak{p} \cdots b,$$

welche dieselbe Länge n besitzt wie $\mathfrak{P}$ und mit der Kette $\mathfrak{H}_1$ äquivalent ist; nach unserer Hypothese muß daher die Länge e dieser Kette $\mathfrak{H}_1$ ebenfalls $= n$ sein, w. z. b. w.

§ 7.

Stufen in endlichen Modulgruppen.

Nachdem durch die Sätze X und XVI die Beziehung zwischen dem Modulgesetz und dem Kettengesetz nachgewiesen ist, fügen wir noch einige Bemerkungen über endliche Modulgruppen hinzu, deren Beweise der Leser leicht finden wird. Unter den Elementen m

einer solchen Gruppe $\mathfrak{M}$ gibt es offenbar ein, und nur ein Element $\mathfrak{p}$, welches ein Teiler von allen $\mathfrak{m}$, und ebenso gibt es ein, und nur ein Element $\mathfrak{q}$, welches ein Vielfaches von allen $\mathfrak{m}$ ist. Wenn $\mathfrak{m}$ verschieden von $\mathfrak{q}$ ist, so gibt es in $\mathfrak{M}$ mindestens ein nächstes Vielfaches von $\mathfrak{m}$, und wenn $\mathfrak{m}$ verschieden von $\mathfrak{p}$ ist, so gibt es in $\mathfrak{M}$ mindestens einen nächsten Teiler von $\mathfrak{m}$. Wenn ferner $\mathfrak{a}$ ein echter Teiler von $\mathfrak{b}$ ist, so gibt es immer mindestens eine Kette, deren Anfang $\mathfrak{a}$ und deren Ende $\mathfrak{b}$ ist. Hierauf können wir alle Elemente der Gruppe $\mathfrak{M}$ in eine Reihe getrennter, aufeinanderfolgender Stufen S einteilen; die unterste oder niedrigste Stufe soll aus dem einzigen Element $\mathfrak{p}$ bestehen, und diese Stufe wollen wir mit S_p bezeichnen, wo p eine beliebig gewählte ganze rationale Zahl ist; wenn ferner $\mathfrak{m}$ ein von $\mathfrak{p}$ verschiedenes Element, also ein echtes Vielfaches von $\mathfrak{p}$ ist, und wenn h die gemeinsame Länge aller Ketten bedeutet, deren Anfang $\mathfrak{p}$ und deren Ende $\mathfrak{m}$ ist, so nennen wir die Summe $m = p + h$ die Stufenzahl von $\mathfrak{m}$ und nehmen $\mathfrak{m}$ in die Stufe S_m auf; ebenso nennen wir p die Stufenzahl des Elementes $\mathfrak{p}$; ist k die Länge aller von $\mathfrak{p}$ nach $\mathfrak{q}$ führenden Ketten, und $q = p + k$, so besteht die oberste oder höchste Stufe S_q offenbar aus dem einzigen Elemente $\mathfrak{q}$, und $k + 1$ ist die Anzahl aller verschiedenen Stufen. Ist $\mathfrak{m}$ ein Element der Stufe S_m, und $m < q$, so finden sich alle nächsten Vielfachen von $\mathfrak{m}$ in der Stufe S_{m+1}, und wenn $m > p$ ist, so finden sich alle nächsten Teiler von $\mathfrak{m}$ in der Stufe S_{m-1}. Bezeichnet man die Stufenzahl m des Elementes $\mathfrak{m}$ allgemein mit $s(\mathfrak{m})$, so gilt für je zwei Elemente $\mathfrak{a}$, $\mathfrak{b}$ der Satz

$$(55) \qquad s(\mathfrak{a}) + s(\mathfrak{b}) = s(\mathfrak{a} + \mathfrak{b}) + s(\mathfrak{a} - \mathfrak{b}),$$

dessen Beweis wir ausführen wollen. Falls eins der beiden Elemente, z. B. $\mathfrak{a}$ ein Teiler des andern $\mathfrak{b}$ ist, so leuchtet der Satz von selbst ein, weil dann $\mathfrak{a} + \mathfrak{b} = \mathfrak{a}$, $\mathfrak{a} - \mathfrak{b} = \mathfrak{b}$ ist. Wenn aber keins der beiden Elemente durch das andere teilbar, also $\mathfrak{a} + \mathfrak{b}$ ein echter Teiler von $\mathfrak{b}$ ist, so gibt es mindestens eine von $\mathfrak{a} + \mathfrak{b}$ nach $\mathfrak{b}$ führende Kette $\mathfrak{N}$, und wenn n ihre Länge bedeutet, so ist offenbar $s(\mathfrak{b}) = s(\mathfrak{a} + \mathfrak{b}) + n$; da nun jedes Element $\mathfrak{b}'$ dieser Kette den Bedingungen $\mathfrak{a} + \mathfrak{b} < \mathfrak{b}' < \mathfrak{b}$ genügt, so ist immer $\mathfrak{a} + \mathfrak{b}' = \mathfrak{a} + \mathfrak{b}$; sind daher $\mathfrak{b}$, $\mathfrak{m}$ irgend zwei aufeinanderfolgende Glieder dieser Kette, so ist auch $\mathfrak{a} + \mathfrak{b} = \mathfrak{a} + \mathfrak{m}$, woraus nach Satz XIII folgt, daß $\mathfrak{a} - \mathfrak{b}$ ein nächster Teiler von $\mathfrak{a} - \mathfrak{m}$ ist; mithin bilden die $n + 1$ Elemente

$\mathfrak{a}_1 = \mathfrak{a} - \mathfrak{b}'$ eine Kette, deren Anfang $\mathfrak{a} - (\mathfrak{a} + \mathfrak{b}) = \mathfrak{a}$, und deren Ende $\mathfrak{a} - \mathfrak{b}$ ist; hieraus folgt offenbar, daß $s(\mathfrak{a} - \mathfrak{b}) = s(\mathfrak{a}) + n$ ist, und wenn man hiermit das obige Resultat $s(\mathfrak{b}) = s(\mathfrak{a} + \mathfrak{b}) + n$ verbindet, so ergibt sich der zu beweisende Satz (55), dessen Zusammenhang mit dem Satze XI einleuchtet.

Alles dies bestätigt sich an dem früher behandelten Beispiele der aus 28 verschiedenen Moduln bestehenden Gruppe $\mathfrak{D}$; hier ist $\mathfrak{p} = \mathfrak{b}''''$, $\mathfrak{q} = \mathfrak{b}_4$, $k = 8$, und da wir in (41) die Zahl $p = -4$ gewählt haben, so ist $q = +4$. Doch muß man nicht glauben, daß die Symmetrie, welche hier in dem Bau von je zwei gleichweit vom Anfang und Ende entfernten Stufen $S_{\pm m}$ auftritt, eine allgemeine Eigenschaft aller Modulgruppen $\mathfrak{M}$ ist. Es bilden z. B. die in dieser Gruppe enthaltenen fünf Elemente $\mathfrak{b}_1$, $\mathfrak{b}_2$, $\mathfrak{c}_2$, $\mathfrak{a}_3$, $\mathfrak{b}_4$ für sich eine Modulgruppe mit vier Stufen S', von denen

$$\begin{aligned} S'_1 &\text{ aus } \mathfrak{b}_1, \\ S'_2 &\text{ „ } \mathfrak{b}_2, \mathfrak{c}_2, \\ S'_3 &\text{ „ } \mathfrak{a}_3, \\ S'_4 &\text{ „ } \mathfrak{b}_4 \end{aligned}$$

besteht; die vier ersten Elemente bilden für sich eine symmetrische Modulgruppe mit den drei Stufen S'_1, S'_2, S'_3, aber diese Symmetrie wird durch das Hinzutreten des fünften Elementes $\mathfrak{b}_4$ gestört.

§ 8.

Beziehung zwischen dem Modulgesetz und dem Symbol $(\mathfrak{m}, \mathfrak{n})$.

Wir wollen nun noch den Zusammenhang besprechen, welcher zwischen dem Modulgesetz VIII und den Symbolgesetzen (27), (28), (32) besteht. Wir haben die letzteren schon in § 3 durch die Bemerkung vervollständigt, daß nach der Bedeutung, welche das Symbol $(\mathfrak{m}, \mathfrak{n})$ in der Modultheorie besitzt, aus der Teilbarkeit $\mathfrak{m} > \mathfrak{b}$ immer $(\mathfrak{m}, \mathfrak{b}) = 1$ folgt; wir fügen jetzt noch hinzu, daß zufolge derselben Bedeutung auch umgekehrt aus $(\mathfrak{m}, \mathfrak{b}) = 1$ immer die Teilbarkeit $\mathfrak{m} > \mathfrak{b}$ folgt, daß also die beiden Aussagen

$$(56) \qquad (\mathfrak{m}, \mathfrak{b}) = 1 \quad \text{und} \quad \mathfrak{m} > \mathfrak{b}$$

völlig gleichbedeutend sind (D. § 171, S. 510).

Nehmen wir nun an, in irgendeiner Dualgruppe $\mathfrak{H}$ entspreche je zwei Elementen $\mathfrak{m}$, $\mathfrak{n}$ ein mit $(\mathfrak{m}, \mathfrak{n})$ bezeichneter, und zwar von Null

verschiedener Zahlwert, und dieses Symbol gehorche den Gesetzen (27), (28), (32) und (56), so wollen wir beweisen, daß in dieser Dualgruppe $\mathfrak{H}$ auch das Modulgesetz VIII herrscht. In der Tat, wählen wir aus $\mathfrak{H}$ drei Elemente $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ aus, welche der Bedingung $\mathfrak{b} < \mathfrak{c}$ genügen, so erzeugen dieselben, wie aus dem Beweise des Satzes IX in § 6 hervorgeht, eine aus höchstens neun Elementen bestehende Dualgruppe $\mathfrak{H}'$, und wenn wir die dortigen Identitäten (42), (43) mit den Symbolgesetzen (27), (28) kombinieren, so ergibt sich

$$(\mathfrak{b}''', \mathfrak{b}_1) = (\mathfrak{a} + \mathfrak{b}_1, \mathfrak{b}_1) = (\mathfrak{a}, \mathfrak{b}_1) = (\mathfrak{a}, \mathfrak{a} - \mathfrak{b}_1) = (\mathfrak{a}, \mathfrak{c}_3),$$
$$(\mathfrak{b}''', \mathfrak{c}') = (\mathfrak{a} + \mathfrak{c}', \mathfrak{c}') = (\mathfrak{a}, \mathfrak{c}') = (\mathfrak{a}, \mathfrak{a} - \mathfrak{c}') = (\mathfrak{a}, \mathfrak{c}_3),$$

also

$$(\mathfrak{b}''', \mathfrak{b}_1) = (\mathfrak{b}''', \mathfrak{c}');$$

da ferner nach (45) auch $\mathfrak{b}''' < \mathfrak{b}_1 < \mathfrak{c}'$ ist, so folgt aus dem Symbolgesetz (32)

$$(\mathfrak{b}''', \mathfrak{c}') = (\mathfrak{b}''', \mathfrak{b}_1)(\mathfrak{b}_1, \mathfrak{c}'),$$

also auch

$$(\mathfrak{b}''', \mathfrak{b}_1)(\mathfrak{b}_1, \mathfrak{c}') = (\mathfrak{b}''', \mathfrak{b}_1),$$

und da nach unserer Annahme die Zahl $(\mathfrak{b}''', \mathfrak{b}_1)$ von Null verschieden ist, so ergibt sich $(\mathfrak{b}_1, \mathfrak{c}') = 1$, was nach (56) gleichbedeutend mit $\mathfrak{b}_1 > \mathfrak{c}'$ ist; da endlich auch $\mathfrak{b}_1 < \mathfrak{c}'$ ist, so folgt $\mathfrak{b}_1 = \mathfrak{c}'$, also ist in der Dualgruppe $\mathfrak{H}$ die Identität

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

eine notwendige Folge der Annahme $\mathfrak{b} < \mathfrak{c}$. Dies ist aber nichts anderes als das Modulgesetz VIII, welches mithin in jeder Dualgruppe $\mathfrak{H}$ herrschen muß, für welche die obigen Voraussetzungen gelten. —

Nachdem dieser Zusammenhang erkannt ist, liegt es nahe, eine besonders wichtige Klasse von Dualgruppen $\mathfrak{H}$ zu betrachten, in welchen die genannten Symbolgesetze wenigstens teilweise erfüllt sind, ich meine die Dualgruppen $\mathfrak{H}$, deren Elemente die sämtlichen Teilgruppen einer gewöhnlichen endlichen Galoisschen Gruppe $\mathfrak{g}$ sind. Die Elemente $\alpha, \beta, \gamma, \cdots$ einer solchen Gruppe $\mathfrak{g}$ reproduzieren sich bekanntlich durch eine Operation, welche in der Regel wie eine Multiplikation bezeichnet wird und dem assoziativen Gesetz $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ gehorcht; außerdem wird vorausgesetzt, daß sowohl aus $\alpha\gamma = \beta\gamma$ wie aus $\gamma\alpha = \gamma\beta$ immer $\alpha = \beta$ folgt. Sind $\mathfrak{a}, \mathfrak{b}$ irgendwelche Komplexe von Elementen in $\mathfrak{g}$, und bezeichnet man allgemein

mit $\mathfrak{a}\,\mathfrak{b}$ den Komplex aller in der Form $\alpha\beta$ enthaltenen Elemente, wo α, β bzw. alle Elemente in $\mathfrak{a}$, $\mathfrak{b}$ durchlaufen, so ist $\mathfrak{a}$ dann, und nur dann eine Gruppe, ein Teiler von $\mathfrak{g}$, wenn $\mathfrak{a}\,\mathfrak{a} = \mathfrak{a}$ ist. Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei solche Teilgruppen von $\mathfrak{g}$, so ist ihr größter gemeinsamer Teiler oder ihr Durchschnitt (d. h. der Inbegriff aller ihnen gemeinsamen Elemente) wieder eine Gruppe, die wir hier, um mit unserer bisherigen Ausdrucksweise im Einklang zu bleiben, durch $\mathfrak{a} + \mathfrak{b}$ bezeichnen wollen; aus demselben Grunde soll das Zeichen $\mathfrak{a} - \mathfrak{b}$ diejenige Gruppe bedeuten, welche durch fortgesetzte Multiplikation aus allen Elementen von $\mathfrak{a}$, $\mathfrak{b}$ erzeugt wird*) und das kleinste gemeinsame Vielfache von $\mathfrak{a}$, $\mathfrak{b}$ heißt; sie ist der Durchschnitt aller derjenigen Teilgruppen von $\mathfrak{g}$, welche (wie z. B. $\mathfrak{g}$ selbst) gemeinsame Vielfache von $\mathfrak{a}$, $\mathfrak{b}$ sind, d. h. welche sowohl $\mathfrak{a}$ als $\mathfrak{b}$ zum Teiler haben. Offenbar genügen diese beiden Operationen $\pm$ den Grundgesetzen (1), (2), (3), mithin ist der Inbegriff $\mathfrak{H}$ aller in $\mathfrak{g}$ als Teiler enthaltenen Gruppen $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c} \cdots$ eine Dualgruppe im Sinne von § 1, auf welche wir auch die Bedeutung der Teilbarkeitszeichen $<$ und $>$ übertragen wollen.

Hierzu tritt nun folgendes. Ist die Gruppe $\mathfrak{a}$ ein Teiler von $\mathfrak{g}$, und sind β, γ irgend zwei Elemente in $\mathfrak{g}$, so sind die beiden Komplexe $\mathfrak{a}\,\beta$, $\mathfrak{a}\,\gamma$ entweder vollständig identisch, oder sie haben kein einziges gemeinsames Element, und wenn $\mathfrak{b}$ ebenfalls eine Teilgruppe von $\mathfrak{g}$ bedeutet, so wollen wir durch das Gruppen-Symbol $(\mathfrak{a}, \mathfrak{b})$ die Anzahl aller voneinander verschiedenen Komplexe $\mathfrak{a}\,\beta$ bezeichnen, die allen Elementen β der Gruppe $\mathfrak{b}$ entsprechen, und aus welchen offenbar der Komplex $\mathfrak{a}\,\mathfrak{b}$ besteht**). Man überzeugt sich nun leicht, daß für dieses Gruppensymbol, welches immer eine natürliche, also von Null verschiedene Zahl ist, die drei Gesetze (27), (32) und (56) gelten, während man dasselbe von dem vierten Symbolgesetz (28) nicht allgemein behaupten kann. Offenbar sind nämlich alle Elemente des Komplexes $\mathfrak{a}\,\mathfrak{b}$ in der Gruppe $\mathfrak{a} - \mathfrak{b}$ enthalten, aber im allgemeinen wird die letztere noch andere Elemente enthalten, und da der Komplex $\mathfrak{a}\,\mathfrak{b}$ schon aus $(\mathfrak{a}, \mathfrak{b})$ verschiedenen Komplexen $\mathfrak{a}\,\beta$ besteht, so wird im allgemeinen $(\mathfrak{a}, \mathfrak{a} - \mathfrak{b})$ größer als $(\mathfrak{a}, \mathfrak{b})$ sein; der Fall

*) Es ist also $\mathfrak{a} - \mathfrak{b} = \mathfrak{a}\,\mathfrak{b}\,\mathfrak{a}\,\mathfrak{b}\,\mathfrak{a} \cdots = \mathfrak{b}\,\mathfrak{a}\,\mathfrak{b}\,\mathfrak{a} \cdots$, wenn diese Produkte hinreichend weit fortgesetzt werden.

**) Vgl. § 9 meiner Abhandlung: Über die Anzahl der Idealklassen in reinen kubischen Zahlkörpern (Crelle's Journal, Bd. 121, S. 77).

$(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{a}, \mathfrak{a} - \mathfrak{b})$ tritt daher immer und nur dann ein, wenn der Komplex $\mathfrak{a}\,\mathfrak{b}$ eine Gruppe, also $= \mathfrak{a} - \mathfrak{b}$ ist, und das charakteristische Merkmal hierfür besteht in der Identität $\mathfrak{a}\,\mathfrak{b} = \mathfrak{b}\,\mathfrak{a}$. Wenn also je zwei Teiler $\mathfrak{a}$, $\mathfrak{b}$ der Gruppe $\mathfrak{g}$ in diesem Sinne permutabel sind, so gelten in der Dualgruppe $\mathfrak{H}$ alle vier Symbolgesetze (27), (28), (32), (56), und hieraus folgt nach der vorhergehenden Betrachtung, daß in $\mathfrak{H}$ das Modulgesetz VIII, also auch das Kettengesetz herrscht*).

Dies bestätigt sich leicht auf folgende Weise. Da nach der jetzigen Voraussetzung immer $\mathfrak{a} - \mathfrak{b} = \mathfrak{a}\,\mathfrak{b} = \mathfrak{b}\,\mathfrak{a}$ ist, so nimmt das aus der Annahme $\mathfrak{b} < \mathfrak{m}$ zu beweisende Gesetz VIII die Gestalt $(\mathfrak{p} + \mathfrak{m})\,\mathfrak{b} = \mathfrak{p}\,\mathfrak{b} + \mathfrak{m}$ an. Nun steht jedes Element des Durchschnittes $\mathfrak{p}\,\mathfrak{b} + \mathfrak{m}$ unter der doppelten Form $\pi\,\delta = \mu$, wo π, δ, μ bzw. Elemente der Gruppen $\mathfrak{p}$, $\mathfrak{b}$, $\mathfrak{m}$ bedeuten, und da $\mathfrak{b}$ nach Voraussetzung ein Teiler von $\mathfrak{m}$, also δ auch Element von $\mathfrak{m}$ ist, so gilt dasselbe bekanntlich auch von π; mithin ist π in dem Durchschnitte $\mathfrak{p} + \mathfrak{m}$, also μ in der Gruppe $(\mathfrak{p} + \mathfrak{m})\,\mathfrak{b}$ enthalten; folglich ist die Gruppe $\mathfrak{p}\,\mathfrak{b} + \mathfrak{m}$ ein Teiler der Gruppe $(\mathfrak{p} + \mathfrak{m})\,\mathfrak{b}$, und da nach dem Satze VII umgekehrt $(\mathfrak{p} + \mathfrak{m})\,\mathfrak{b}$ gewiß ein Teiler von $\mathfrak{p}\,\mathfrak{b} + \mathfrak{m}$ ist, so sind beide Gruppen miteinander identisch, w. z. b. w. Offenbar stimmt dieser Beweis mutatis mutandis vollständig mit dem Beweise des entsprechenden Satzes in der Modultheorie überein (D. § 169, S. 498—499).

Zu den Gruppen $\mathfrak{g}$, deren sämtliche Teiler $\mathfrak{a}$, $\mathfrak{b}$ diese Eigenschaft $\mathfrak{a}\,\mathfrak{b} = \mathfrak{b}\,\mathfrak{a}$ besitzen, gehören augenscheinlich alle Abelschen Gruppen, ferner diejenigen, welche ich Hamiltonsche Gruppen genannt habe**), außerdem aber noch unendlich viele andere, von denen ich hier nur die beiden einfachsten Beispiele anführen will. Benutzt man die bekannte Bezeichnung der zyklischen Vertauschungen von beliebigen verschiedenen Dingen 0, 1, 2, 3 ···, so wird die erste Gruppe $\mathfrak{g}$ vom Grade 16 erzeugt durch die Elemente achten und zweiten Grades

$$\alpha = (01234567), \quad \beta = (04)\,(26),$$

welche der Bedingung $\beta\,\alpha = \alpha^5\,\beta$ genügen. Ebenso wird die zweite Gruppe $\mathfrak{g}$ vom Grade 27 erzeugt durch die Elemente neunten und dritten Grades

$$\alpha = (012345678), \quad \beta = (174)\,(258),$$

*) Doch lehrt schon das Beispiel der Gruppe $\mathfrak{g}$, welche aus den sechs Vertauschungen von drei Dingen besteht, daß dieser Satz nicht umgekehrt werden darf.

**) Mathematische Annalen, Bd. 48, S. 548.

welche der Bedingung $\beta\alpha = \alpha^4\beta$ genügen. Die allgemeine Theorie aller dieser Gruppen mit permutablen Teilern werde ich in einem besonderen Aufsatze behandeln.

Braunschweig, den 8. Januar 1900.

Erläuterungen zur vorstehenden Abhandlung.

Diese Arbeit, die in Inhalt und Auffassung direkt an XXVIII anschließt, ist vor allem interessant als axiomatische Untersuchung über die Gültigkeit des „Kettengesetzes" in Dualgruppen. Darunter wird der Kompositionsreihensatz verstanden, unter alleiniger Voraussetzung der Existenz einer Kompositionsreihe, in der durch die Axiomatik bedingten abgeschwächten Form von der Invarianz der Länge; genauer handelt es sich um Hauptreihen. Und zwar zeigt sich (§ 6) die völlige Äquivalenz von Modulgesetz, Kettengesetz und „zweitem Isomorphiesatz", letzterer ebenfalls in einer durch die Axiomatik bedingten Form: eineindeutiges Entsprechen aller Zwischengruppen durch Summen- und Durchschnittbildung (§ 6, XI). Zugleich wird noch eine Axiomatik des Normbegriffs gegeben und der Zusammenhang mit dem Modulgesetz untersucht (§ 8).

Die Tatsache, daß allein aus der Existenz einer Kompositionsreihe sich alle Folgerungen ziehen lassen, ist — anfangs unabhängig von der vorliegenden Arbeit wiedererkannt — ein wichtiges Hilfsmittel der neueren Algebra geworden.

Noether.
