Ueber die von drei Moduln erzeugte Dualgruppe.

Von

R. Dedekind in Braunschweig.

In der vierten Auflage von Dirichlet's Vorlesungen über Zahlentheorie (die im Folgenden mit D. citirt 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 Theiler 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 Hülfe 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 Theiler (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 commutative und associative Gesetz

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

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

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

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

*) Vergl. § 4 meines Aufsatzes Ueber Zerlegungen von Zahlen durch ihre grössten gemeinsamen Theiler in der Festschrift unserer Technischen Hochschule für die Naturforscher-Versammlung 1897.

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

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

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

Wenn zwei Operationen $\pm$ aus je zwei Elementen a, b eines (endlichen oder unendlichen) Systems $\mathfrak{S}$ zwei Elemente $a \pm b$ 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 Gesammtheit aller Moduln ist daher eine Dualgruppe bezüglich der beiden Operationen, welche in der Bildung des grössten gemeinsamen Theilers und des kleinsten gemeinsamen Vielfachen bestehen*). Zunächst betrachten wir aber einige Eigenschaften, welche *jeder* Dualgruppe $\mathfrak{S}$ zukommen.

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

Für zwei beliebige Elemente a, b ergiebt sich aus (2) und (4), wenn man b, c resp. durch a, b ersetzt,

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

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

$$(6) \qquad (a + b) + (a - b) = a + b, \qquad (a - b) - (a + b) = a - b;$$

mithin bilden die vier Elemente a, b, $(a + b)$, $(a - b)$ gewiss eine Dualgruppe, und es fragt sich nur, wie viele von ihnen *verschieden* sind.

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

Machen wir jetzt die (allgemeinere) Annahme, es sei $a + b$ identisch mit einem der beiden Elemente a, b, also z. B. $a + b = a$, so folgt aus $(3'')$ durch Vertauschung von a mit b auch $a - b = b$, und umgekehrt, wenn Letzteres der Fall ist, so ergiebt sich aus $(3')$ auch $a + b = a$. Da dieser Fall sehr häufig auftritt, so übertragen wir die in der Modultheorie übliche Ausdrucks- und Bezeichnungsweise (D. § 169) auf alle Dualgruppen $\mathfrak{S}$

*) Andere Beispiele von Dualgruppen findet man in der oben erwähnten Schrift (1897). Vergl. den Schluss (§ 8) der gegenwärtigen Abhandlung.

und sagen*): das Element $\mathfrak{b}$ ist *theilbar* durch das Element $\mathfrak{a}$, zugleich heisst $\mathfrak{b}$ ein *Vielfaches* von $\mathfrak{a}$, und $\mathfrak{a}$ ein *Theiler* von $\mathfrak{b}$; diese Theilbarkeit wird durch $\mathfrak{a} < \mathfrak{b}$ oder $\mathfrak{b} > \mathfrak{a}$ bezeichnet, und es ist daher jede der vier Aussagen

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

gleichbedeutend mit jeder der drei übrigen; zwei solche Elemente $\mathfrak{a}$, $\mathfrak{b}$ bilden für sich allein eine Dualgruppe. Es ist zweckmässig, hierbei den Fall $\mathfrak{a} = \mathfrak{b}$ nicht auszuschliessen; wenn aber $\mathfrak{a}$ und $\mathfrak{b}$ verschieden sind, so soll $\mathfrak{b}$ ein *echtes* Vielfaches von $\mathfrak{a}$ und zugleich $\mathfrak{a}$ ein *echter* Theiler von $\mathfrak{b}$ heissen.

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

Für die durch (7) charakterisirte Theilbarkeit von $\mathfrak{b}$ durch $\mathfrak{a}$ ergeben sich durch alleinige Anwendung der Grundgesetze (1), (2), (3) die folgenden Sätze, deren Beweise der Leser leicht finden wird.

I. Immer ist $\mathfrak{a} < \mathfrak{a}$, $\mathfrak{a} > \mathfrak{a}$.

II. Aus $\mathfrak{a} < \mathfrak{b}$ und $\mathfrak{a} > \mathfrak{b}$ folgt $\mathfrak{a} = \mathfrak{b}$.

III. Aus $\mathfrak{a} < \mathfrak{b}$ und $\mathfrak{b} < \mathfrak{c}$, was kurz in $\mathfrak{a} < \mathfrak{b} < \mathfrak{c}$ zusammengefasst wird, folgt $\mathfrak{a} < \mathfrak{c}$.

IV. Immer ist $\mathfrak{a} + \mathfrak{b} < \mathfrak{a}$ und $\mathfrak{a} < \mathfrak{a} - \mathfrak{c}$, also auch $\mathfrak{a} + \mathfrak{b} < \mathfrak{a} - \mathfrak{c}$.

V. Aus $\mathfrak{a} < \mathfrak{b}$, $\mathfrak{a}' < \mathfrak{b}'$ folgt $\mathfrak{a} + \mathfrak{a}' < \mathfrak{b} + \mathfrak{b}'$ und $\mathfrak{a} - \mathfrak{a}' < \mathfrak{b} - \mathfrak{b}'$.

VI. Aus $\mathfrak{a} < \mathfrak{b}$, $\mathfrak{a}' < \mathfrak{b}$ folgt $\mathfrak{a} - \mathfrak{a}' < \mathfrak{b}$, d. h. jedes gemeinsame Vielfache $\mathfrak{b}$ von $\mathfrak{a}$, $\mathfrak{a}'$ ist theilbar durch $\mathfrak{a} - \mathfrak{a}'$, und aus $\mathfrak{a} < \mathfrak{b}$, $\mathfrak{a} < \mathfrak{b}'$ folgt $\mathfrak{a} < \mathfrak{b} + \mathfrak{b}'$, d. h. jeder gemeinsame Theiler $\mathfrak{a}$ von $\mathfrak{b}$, $\mathfrak{b}'$ ist Theiler von $\mathfrak{b} + \mathfrak{b}'$. Wegen der Analogie mit der Zahlen- und Modultheorie heisst daher $\mathfrak{a} - \mathfrak{a}'$ das *kleinste* gemeinsame Vielfache von $\mathfrak{a}$, $\mathfrak{a}'$, und $\mathfrak{b} + \mathfrak{b}'$ heisst der *grösste* gemeinsame Theiler von $\mathfrak{b}$, $\mathfrak{b}'$. Diese Ausdrucksweise dehnen wir auch auf mehr als zwei Elemente aus, und durch wiederholte Anwendung des Vorhergehenden ergiebt sich der Satz: ist jedes der Elemente $\mathfrak{a}', \mathfrak{a}'', \mathfrak{a}''' \cdots$ ein Theiler von jedem der Elemente $\mathfrak{b}', \mathfrak{b}'', \mathfrak{b}''' \cdots$, so ist

$$\mathfrak{a}' - \mathfrak{a}'' - \mathfrak{a}''' - \cdots < \mathfrak{b}' + \mathfrak{b}'' + \mathfrak{b}''' + \cdots,$$

d. h. das kleinste gemeinsame Vielfache der Elemente $\mathfrak{a}$ ist ein Theiler des grössten gemeinsamen Theilers der Elemente $\mathfrak{b}$.

---

*) 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 Theiler 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 Theiler 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 Theiler 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 citirten 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 $\mathfrak{p}$, $\mathfrak{d}$, $\mathfrak{m}$ resp. durch $\mathfrak{a}$, $\mathfrak{b} + \mathfrak{c}$, $\mathfrak{b} - \mathfrak{c}$, so ist die Bedingung $\mathfrak{d} < \mathfrak{m}$ erfüllt, und es ergiebt 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 $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ resp. durch $\mathfrak{p}$, $\mathfrak{d}$, $\mathfrak{m}$ ersetzt und die Annahme $\mathfrak{d} < \mathfrak{m}$ hinzufügt.

Hierauf wenden wir uns zu dem in der Ueberschrift 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 von einander 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 Accente und Indices von einander unterschieden werden, deren Bedeutung später einleuchten wird:

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

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

Die übrigen 24 Moduln haben die Eigenschaft, durch alle Vertauschungen

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

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 Accenten und Indices 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 neben einander gestellt, welche durch Vertauschung der beiden Operationen $+$ aus einander hervorgehen, und hiermit ist immer eine Vertauschung eines oberen Accentes mit dem entsprechenden unteren Index verbunden; die Doppeldefinitionen (14) beruhen auf dem oben hervorgehobenen Modulgesetz (8).

Wir haben nun zu zeigen, dass der Complex $\mathfrak{D}$ dieser 28 Moduln wirklich eine Dualgruppe ist, dass also, wenn $\mathfrak{m}$, $\mathfrak{n}$ irgend zwei dieser Moduln bedeuten, auch die beiden Moduln $\mathfrak{m} + \mathfrak{n}$ 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 $\mathfrak{n}$ theilbar ist, so dass $\mathfrak{m} + \mathfrak{n} = \mathfrak{n}$, $\mathfrak{m} - \mathfrak{n} = \mathfrak{m}$ wird, was wir wieder durch $\mathfrak{m} > \mathfrak{n}$ oder $\mathfrak{n} < \mathfrak{m}$ bezeichnen. Des Raumes wegen begnügen wir uns, von diesen 261 Theilbarkeiten nur die 48 *ursprünglichen*, d. h. diejenigen aufzuschreiben,

*) Weiter unten wird durch ein Beispiel bewiesen, dass die 28 Moduln wirklich alle von einander 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.

aus welchen die übrigen 213 nach dem obigen Satze III in § 1 sich ableiten lassen:

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

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

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

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

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

Fügt man zu diesen ursprünglichen Theilbarkeiten 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 Theiler $\mathfrak{n}$ von $\mathfrak{m}$, welche von $\mathfrak{m}$ und von einander verschieden sind, so ergiebt sich successive

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

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 Theilbarkeiten $\mathfrak{m} > \mathfrak{n}$. Dass hiermit auch *alle* Theilbarkeiten innerhalb der allgemeinen Gruppe $\mathfrak{D}$ erschöpft sind, ergiebt sich zugleich aus dem Folgenden.

Wir wenden uns jetzt zu den übrigen Paaren $\mathfrak{m}$, $\mathfrak{n}$, um die entsprechenden Moduln $\mathfrak{m} \dot{+} \mathfrak{n}$ anzugeben; des Raumes und des leichteren Ueberblicks 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 Gesammtanzahl $= 3 \cdot 19 + 6 \cdot 10 = 117$ ergiebt.

(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) getheilt sind, ist nun keineswegs so mühselig, wie man auf den ersten Blick befürchten könnte. Zunächst ergiebt sich aus dem dualistischen Charakter der Grundgesetze (1), (2), (3) und des specifischen Modulgesetzes VIII oder (8), sowie aus der entsprechenden Bezeichnung durch obere Accente und untere Indices in den Definitionen (9) bis (14), dass von jedem Doppelsatze nur der erste, auf die Operation $+$ bezügliche Theil bewiesen zu werden braucht, weil hieraus durch gänzliche Vertauschung von $+$ mit $-$ der zweite Theil 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 Theilbarkeiten (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 $\mathfrak{d} < \mathfrak{m}$ geltenden Modulgesetze VIII

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

Setzt man nämlich $\mathfrak{p} = \mathfrak{b}$, $\mathfrak{d} = \mathfrak{c} + \mathfrak{a} = \mathfrak{b}'''$, $\mathfrak{m} = \mathfrak{a}$, so ist die Voraussetzung $\mathfrak{d} < \mathfrak{m}$ erfüllt, und zufolge der schon bewiesenen Sätze (23″), (26″) wird $\mathfrak{p} - \mathfrak{d} = \mathfrak{b} - \mathfrak{b}''' = \mathfrak{b}_1$, also $(\mathfrak{p} - \mathfrak{d}) + \mathfrak{m} = \mathfrak{b}_1 + \mathfrak{a}$, ferner $\mathfrak{p} + \mathfrak{m} = \mathfrak{b} + \mathfrak{a} = \mathfrak{c}'''$, $(\mathfrak{p} + \mathfrak{m}) - \mathfrak{d} = \mathfrak{c}''' - \mathfrak{b}''' = \mathfrak{a}''$, wodurch (21′) bewiesen ist. Setzt man aber $\mathfrak{p} = \mathfrak{a}$, $\mathfrak{d} = \mathfrak{b} + \mathfrak{c} = \mathfrak{a}'''$, $\mathfrak{m} = \mathfrak{b} - (\mathfrak{c} + \mathfrak{a}) = \mathfrak{b}_1$, so ist zufolge IV in § 1 die Voraussetzung $\mathfrak{d} < \mathfrak{m}$ erfüllt, und zufolge der schon bewiesenen Sätze (23″), (21′), (25″) wird $\mathfrak{p} - \mathfrak{d} = \mathfrak{a} - \mathfrak{a}''' = \mathfrak{a}_1$, also $(\mathfrak{p} - \mathfrak{d}) + \mathfrak{m} = \mathfrak{a}_1 + \mathfrak{b}_1$, ferner $\mathfrak{p} + \mathfrak{m} = \mathfrak{a} + \mathfrak{b}_1 = \mathfrak{a}''$, $(\mathfrak{p} + \mathfrak{m}) - \mathfrak{d} = \mathfrak{a}'' - \mathfrak{a}''' = \mathfrak{d}'$, 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 Systeme enthaltene Moduln $\mathfrak{m} \dotplus \mathfrak{n}$ erzeugen; mithin bilden diese 28 Moduln wirklich eine *Dualgruppe* $\mathfrak{D}$. Die Gesammtheit aller Erzeugnisse $\mathfrak{m} \dotplus \mathfrak{n}$ ist in der beigefügten *Tabelle* (S. 380, 381) 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 Theilung der Tabelle in Rechtecke von verschiedener Grösse entspricht der später (in § 5) zu betrachtenden Eintheilung 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 mit einander identisch sein müssen. Dass diese Frage zu *verneinen* ist, dass also diese 28 Moduln im Allgemeinen wirklich von einander verschieden sind, ergiebt 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 Product $(b-c)(c-a)(a-b)$ 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:

Tabelle der grössten gemeinsamen Theiler (+) und der von 28 Moduln, welche durch drei

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

kleinsten gemeinsamen Vielfachen (—) in der Dualgruppe beliebige Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ erzeugt wird.

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

$$[d_2] = [p_2, q_2], \qquad [dd_2] = [pp_2, pq_2, qp_2, qq_2, p_1q_2 - q_1p_2],$$

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

und

$$\left[\frac{1}{m}\right] = \left[\frac{1}{p}, \frac{1}{q}\right], \qquad dd_2 mm_2 = pp_2 qq_2,$$

$$\frac{m}{p} m_1 \equiv Ap_1, \qquad \frac{m}{q} m_1 \equiv Bq_1 \pmod{m},$$

wo

$$A = (\mathfrak{p}, \mathfrak{q}) = \frac{qq_2}{dd_2} = \frac{mm_2}{pp_2}, \qquad B = (\mathfrak{q}, \mathfrak{p}) = \frac{pp_2}{dd_2} = \frac{mm_2}{qq_2}.$$

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 Theilbarkeiten (15) bis (18) nirgends eine Identität auftritt, dass sie also *echte* Theilbarkeiten sind (D. § 169, S. 496).

§ 3.

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

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

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

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

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 ergiebt 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 ergiebt sich, dass man sechs Zahlen a', b', c', a_1, b_1, c_1 in folgender Weise durch je sechs Gleichungen definiren kann:

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

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

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 ergiebt sich, dass man eine siebente Zahl d definiren kann durch die zwölf Gleichungen

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

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

Die sämmtlichen in unserer Dualgruppe $\mathfrak{D}$ auftretenden Symbole $(\mathfrak{m}, \mathfrak{n})$, deren Anzahl $= 28 \cdot 28 = 784$ ist, zerfallen nun in drei Classen, je nachdem die Theilbarkeit $\mathfrak{m} > \mathfrak{n}$ oder $\mathfrak{m} < \mathfrak{n}$ oder keine solche Theilbarkeit besteht. Aus der Definition des Symbols folgt unmittelbar (D. S. 510), dass alle 289 Symbole der ersten Classe, zu denen wir auch die 28 Symbole $(\mathfrak{m}, \mathfrak{m})$ rechnen, $= 1$ sind*). Die 234 Symbole der dritten Classe lassen

*) Stützt man sich nicht auf die Definition des Symbols, sondern nur auf die beiden Sätze (27), (28), so ergiebt sich zwar, dass alle Symbole der ersten Classe denselben Werth haben; dass aber dieser Werth $= 1$ 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. Aehnliches gilt für das in den Göttinger Nachrichten (1895. Heft 2) erklärte Modulsymbol $(\mathfrak{a}; \mathfrak{b})$. — Vergl. § 8 des gegenwärtigen Aufsatzes.

sich vermöge der Sätze (27), (28) auf zwei Arten durch Symbole der zweiten Classe ausdrücken. Unter den 261 Symbolen dieser zweiten Classe befinden sich zunächst die 48 Symbole (29), (30), (31), deren Werthe 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 Theilbarkeit $\mathfrak{m} < \mathfrak{n}$ keine ursprüngliche, sondern eine abgeleitete ist, lassen sich als Producte 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 $(\mathfrak{m}, \mathfrak{n})$ der dritten Classe durchzuführen, in denen $\mathfrak{m}, \mathfrak{n}$ 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 ergiebt sich durch zweimalige Anwendung von (32)

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

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

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

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 Dirichlet's 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 mit einander verwandt. Dies ergiebt sich unmittelbar daraus, dass alle Factoren, welche in den vorstehenden Ausdrücken (33) oder (34) oder (35) von $(\mathfrak{b},\mathfrak{c})$ und $(\mathfrak{c},\mathfrak{b})$ auftreten, auch Factoren 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* eintheilen, indem man je zwei Moduln in dieselbe oder in verschiedene Familien aufnimmt, je nachdem sie mit einander 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 von einander verschieden sind; wir wollen jetzt einen besonders bemerkenswerthen 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 *Multiplication* 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:

$$(37)\quad \left\{\begin{array}{ccc} \mathfrak{a} = \mathfrak{q}'\mathfrak{r}'\mathfrak{p}_1\mathfrak{d}'''', & \mathfrak{b} = \mathfrak{r}'\mathfrak{p}'\mathfrak{q}_1\mathfrak{d}'''', & \mathfrak{c} = \mathfrak{p}'\mathfrak{q}'\mathfrak{r}_1\mathfrak{d}'''' \\ \mathfrak{a}''' = \mathfrak{p}'\mathfrak{d}'''', & \mathfrak{b}''' = \mathfrak{q}'\mathfrak{d}'''', & \mathfrak{c}''' = \mathfrak{r}'\mathfrak{d}'''' \\ \mathfrak{a}'' = \mathfrak{a}' = \mathfrak{q}'\mathfrak{r}'\mathfrak{d}'''', & \mathfrak{b}'' = \mathfrak{b}' = \mathfrak{r}'\mathfrak{p}'\mathfrak{d}'''', & \mathfrak{c}'' = \mathfrak{c}' = \mathfrak{p}'\mathfrak{q}'\mathfrak{d}'''' \\ \multicolumn{3}{c}{\mathfrak{d}' = \mathfrak{a}_0 = \mathfrak{b}_0 = \mathfrak{c}_0 = \mathfrak{d}_1 = \mathfrak{p}'\mathfrak{q}'\mathfrak{r}'\mathfrak{d}''''} \\ \mathfrak{a}_1 = \mathfrak{a}_2 = \mathfrak{p}_1\mathfrak{d}_1, & \mathfrak{b}_1 = \mathfrak{b}_2 = \mathfrak{q}_1\mathfrak{d}_1, & \mathfrak{c}_1 = \mathfrak{c}_2 = \mathfrak{r}_1\mathfrak{d}_1 \\ \mathfrak{a}_3 = \mathfrak{q}_1\mathfrak{r}_1\mathfrak{d}_1, & \mathfrak{b}_3 = \mathfrak{r}_1\mathfrak{p}_1\mathfrak{d}_1, & \mathfrak{c}_3 = \mathfrak{p}_1\mathfrak{q}_1\mathfrak{d}_1 \\ & \mathfrak{d}_4 = \mathfrak{p}_1\mathfrak{q}_1\mathfrak{r}_1\mathfrak{d}_1 & \end{array}\right\};$$

jedes der drei Paare von Producten

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

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

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

über.

Wir wollen die drei in diesem Falle auftretenden Specialgesetze*) $\mathfrak{a}'' = \mathfrak{a}'$, $\mathfrak{a}_2 = \mathfrak{a}_1$, $\mathfrak{b}' = \mathfrak{b}_1$, d. h. die Gesetze

$$(39)\quad (\mathfrak{c}+\mathfrak{a})-(\mathfrak{a}+\mathfrak{b}) = \mathfrak{a}+(\mathfrak{b}-\mathfrak{c}), \quad (\mathfrak{c}-\mathfrak{a})+(\mathfrak{a}-\mathfrak{b}) = \mathfrak{a}-(\mathfrak{b}+\mathfrak{c}),$$

$$(40)\quad (\mathfrak{b}+\mathfrak{c})-(\mathfrak{c}+\mathfrak{a})-(\mathfrak{a}+\mathfrak{b}) = (\mathfrak{b}-\mathfrak{c})+(\mathfrak{c}-\mathfrak{a})+(\mathfrak{a}-\mathfrak{b})$$

noch etwas näher betrachten und beweisen, dass, wenn in irgend einer Dualgruppe $\mathfrak{Z}$ ausser den Grundgesetzen (1), (2), (3) noch eins dieser Specialgesetze allgemein gilt, gewiss auch das Modulgesetz VIII und die beiden anderen Gesetze gelten. In der That folgt VIII (unter der Voraussetzung $\mathfrak{d} < \mathfrak{m}$) aus (39′) oder (39″) oder (40), wenn man $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ resp. durch $\mathfrak{m}$, $\mathfrak{d}$, $\mathfrak{p}$ oder $\mathfrak{d}$, $\mathfrak{m}$, $\mathfrak{p}$ oder $\mathfrak{p}$, $\mathfrak{d}$, $\mathfrak{m}$ ersetzt; mithin gelten in $\mathfrak{Z}$ auch alle Sätze (19) bis (26). Nimmt man nun an, es gelte das erste Specialgesetz $\mathfrak{a}'' = \mathfrak{a}'$, also auch $\mathfrak{b}'' = \mathfrak{b}'$, so folgt daraus das zweite $\mathfrak{a}_2 = \mathfrak{a}_1$ und das dritte $\mathfrak{d}_1 = \mathfrak{d}'$, weil zufolge (21″), (23″), (22″), (25″) resp. $\mathfrak{a}_2 = \mathfrak{a} - \mathfrak{b}'$, $\mathfrak{a}_1 = \mathfrak{a} - \mathfrak{b}''$, $\mathfrak{d}_1 = \mathfrak{a}' - \mathfrak{b}'$, $\mathfrak{d}' = \mathfrak{a}'' - \mathfrak{b}''$ ist. Ebenso folgt umgekehrt das erste Gesetz aus dem zweiten, weil $\mathfrak{a}'' = \mathfrak{a} + \mathfrak{d}_1$,

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

$\mathfrak{a}' = \mathfrak{a} + \mathfrak{b}_2$, und aus dem dritten, weil $\mathfrak{a}'' = \mathfrak{a} + \mathfrak{b}'$, $\mathfrak{a}' = \mathfrak{a} + \mathfrak{b}_1$ ist. Hiermit ist unsere Behauptung offenbar erwiesen, und wir können jedes der drei äquivalenten Gesetze (39), (40) als das *Idealgesetz* bezeichnen; jede Dualgruppe $\mathfrak{J}$ vom Idealtypus ist auch eine Gruppe vom Modultypus, während umgekehrt, wie aus dem Beispiele 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 $\mathfrak{d}$ soll in $\mathfrak{G}$ ein *nächster Theiler**) des Elementes $\mathfrak{m}$ heissen, wenn erstens $\mathfrak{d} < \mathfrak{m}$, zweitens $\mathfrak{d}$ verschieden von $\mathfrak{m}$, also ein *echter* Theiler von $\mathfrak{m}$ ist, und wenn es drittens in *dieser* Gruppe $\mathfrak{G}$ ausser $\mathfrak{d}$ und $\mathfrak{m}$ kein Element giebt, das ein Theiler 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 Theiler 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 Theiler von $\mathfrak{m}$ ist; so lange 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 Theilbarkeiten (15) bis (18) sich alle und nur solche Paare von Moduln $\mathfrak{d}$, $\mathfrak{m}$ finden, von denen der eine $\mathfrak{d}$ ein nächster Theiler des anderen $\mathfrak{m}$ in $\mathfrak{D}$ ist. Die vier Moduln $\mathfrak{d}''''$, $\mathfrak{d}'$, $\mathfrak{d}_1$, $\mathfrak{d}_4$ bilden aber für sich eine Dualgruppe $\mathfrak{E}$, und jeder von ihnen ist in $\mathfrak{E}$, aber nicht in $\mathfrak{D}$, ein nächster Theiler 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 Theiler von $\mathfrak{a}_3$.

---

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

Unter einer *Kette* der Dualgruppe $\mathfrak{G}$ wollen wir eine endliche Folge von mindestens zwei Elementen in $\mathfrak{G}$ verstehen, deren jedes ein nächster Theiler des nächstfolgenden Elementes ist; diese Elemente sollen die *Glieder* der Kette, und das erste und letzte Glied sollen resp. 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 *Theilkette* 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 Theilbarkeiten (15) bis (18) ergeben müssen. Wir wollen nur einige von ihnen betrachten. Es giebt 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

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

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 Theilketten 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 $\mathfrak{D}$ thatsächlich nachzuweisen, vertheilen 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

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

Betrachtet man nun zwei beliebige aufeinander folgende Stufen S_{n-1} und S_n, so lehrt ein Blick auf die Theilbarkeiten (15) bis (18), *dass die nächsten Vielfachen eines beliebigen Elementes der Stufe S_{n-1} sämmtlich in der Stufe S_n enthalten sind*, woraus von selbst folgt, *dass auch die nächsten Theiler eines beliebigen Elementes der Stufe S_n sämmtlich 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 $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ einer beliebigen Dualgruppe $\mathfrak{H}$, welche eine Theilbarkeit

$$\mathfrak{b} < \mathfrak{c}, \quad \mathfrak{b} + \mathfrak{c} = \mathfrak{b}, \quad \mathfrak{b} - \mathfrak{c} = \mathfrak{c}$$

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

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

definiren. Zunächst ergeben sich die folgenden 11 *ursprünglichen* Theilbarkeiten

$$\begin{aligned} \mathfrak{c}''' &< \mathfrak{b}, \mathfrak{b}'''; & \mathfrak{b}_3 &> \mathfrak{c}, \mathfrak{c}_3, \\ \mathfrak{b} &< \mathfrak{b}_1; & \mathfrak{c} &> \mathfrak{c}', \\ \mathfrak{b}''' &< \mathfrak{a}, \mathfrak{b}_1; & \mathfrak{c}_3 &> \mathfrak{a}, \mathfrak{c}', \\ \mathfrak{b}_1 &< \mathfrak{c}'; & \mathfrak{c}' &> \mathfrak{b}_1, \end{aligned}$$

deren letzte mit dem Satze VII in § 1 übereinstimmt, wenn dort die Elemente $\mathfrak{p}$, $\mathfrak{b}$, $\mathfrak{m}$ resp. durch $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ ersetzt werden; die übrigen folgen mit Rücksicht auf $\mathfrak{b} < \mathfrak{c}$ unmittelbar aus den Definitionen. Es giebt nur sechs Paare von Elementen, welche keine Theilbarkeit darbieten; die beiden Paare $\mathfrak{a}$, $\mathfrak{c}$ und $\mathfrak{a}$, $\mathfrak{b}$ erzeugen durch die Operationen $+$ die oben definirten Elemente $\mathfrak{b}_3$, $\mathfrak{b}'''$, $\mathfrak{c}'''$, $\mathfrak{c}_3$; für die übrigen vier Paare ergiebt sich aus den Definitionen:

$$\mathfrak{b} + \mathfrak{b}''' = \mathfrak{c}''', \qquad \mathfrak{c} - \mathfrak{c}_3 = \mathfrak{b}_3,$$

$$\mathfrak{b} - \mathfrak{b}''' = \mathfrak{b}_1, \qquad \mathfrak{c} + \mathfrak{c}_3 = \mathfrak{c}',$$

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

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

und zwar folgen die Sätze (43) aus den Sätzen (42) mit Rücksicht auf $\mathfrak{b}_1 < \mathfrak{c}'$, $\mathfrak{b}''' < \mathfrak{b}_1$, $\mathfrak{c}_3 > \mathfrak{c}'$.

Hiermit ist bewiesen, dass die neun Elemente

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

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

	$\mathfrak{c}'''$	$\mathfrak{b}$	$\mathfrak{b}'''$	$\mathfrak{b}_1$	$\mathfrak{a}$	$\mathfrak{c}'$	$\mathfrak{c}_3$	$\mathfrak{c}$	$\mathfrak{b}_3$	$+$
$\mathfrak{c}'''$		$\mathfrak{c}'''$	$\mathfrak{c}'''$	$\mathfrak{c}'''$	$\mathfrak{c}'''$	$\mathfrak{c}'''$	$\mathfrak{c}'''$	$\mathfrak{c}'''$	$\mathfrak{c}'''$	$\mathfrak{c}'''$
$\mathfrak{b}$	$\mathfrak{b}$		$\mathfrak{c}'''$	$\mathfrak{b}$	$\mathfrak{c}'''$	$\mathfrak{b}$	$\mathfrak{b}$	$\mathfrak{b}$	$\mathfrak{b}$	$\mathfrak{b}$
$\mathfrak{b}'''$	$\mathfrak{b}'''$	$\mathfrak{b}_1$		$\mathfrak{b}'''$	$\mathfrak{b}'''$	$\mathfrak{b}'''$	$\mathfrak{b}'''$	$\mathfrak{b}'''$	$\mathfrak{b}'''$	$\mathfrak{b}'''$
$\mathfrak{b}_1$	$\mathfrak{b}_1$	$\mathfrak{b}_1$	$\mathfrak{b}_1$		$\mathfrak{b}'''$	$\mathfrak{b}_1$	$\mathfrak{b}_1$	$\mathfrak{b}_1$	$\mathfrak{b}_1$	$\mathfrak{b}_1$
$\mathfrak{a}$	$\mathfrak{a}$	$\mathfrak{c}_3$	$\mathfrak{a}$	$\mathfrak{c}_3$		$\mathfrak{b}'''$	$\mathfrak{a}$	$\mathfrak{b}'''$	$\mathfrak{a}$	$\mathfrak{a}$
$\mathfrak{c}'$	$\mathfrak{c}'$	$\mathfrak{c}'$	$\mathfrak{c}'$	$\mathfrak{c}'$	$\mathfrak{c}_3$		$\mathfrak{c}'$	$\mathfrak{c}'$	$\mathfrak{c}'$	$\mathfrak{c}'$
$\mathfrak{c}_3$	$\mathfrak{c}_3$	$\mathfrak{c}_3$	$\mathfrak{c}_3$	$\mathfrak{c}_3$	$\mathfrak{c}_3$	$\mathfrak{c}_3$		$\mathfrak{c}'$	$\mathfrak{c}_3$	$\mathfrak{c}_3$
$\mathfrak{c}$	$\mathfrak{c}$	$\mathfrak{c}$	$\mathfrak{c}$	$\mathfrak{c}$	$\mathfrak{b}_3$	$\mathfrak{c}$	$\mathfrak{b}_3$		$\mathfrak{c}$	$\mathfrak{c}$
$\mathfrak{b}_3$	$\mathfrak{b}_3$	$\mathfrak{b}_3$	$\mathfrak{b}_3$	$\mathfrak{b}_3$	$\mathfrak{b}_3$	$\mathfrak{b}_3$	$\mathfrak{b}_3$	$\mathfrak{b}_3$		$\mathfrak{b}_3$
$-$	$\mathfrak{c}'''$	$\mathfrak{b}$	$\mathfrak{b}'''$	$\mathfrak{b}_1$	$\mathfrak{a}$	$\mathfrak{c}'$	$\mathfrak{c}_3$	$\mathfrak{c}$	$\mathfrak{b}_3$	

Das Durchschnittsfeld der Zeile $\mathfrak{m}$ und der Spalte $\mathfrak{n}$ enthält das Element $\mathfrak{m} + \mathfrak{n}$ oder $\mathfrak{m} - \mathfrak{n}$, 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 Ueberblicks 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 ergiebt sich aus der Constitution 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 Modulgesetzt 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* Theiler 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 von einander *verschieden* sind;

---

*) Denn je zwei Elemente m, n in $\mathfrak{G}$ erzeugen zwei in $\mathfrak{G}$ enthaltene Elemente $m \pm n$, 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 $\mathfrak{H}$ existirt, 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 citirten Schrift (1897) wirklich geschehen; in der That geht die erste der beiden dort auf S. 14 angeführten Dualgruppen in unsere Gruppe $\mathfrak{G}$ über, wenn man α, β, γ, δ, ε resp. 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 Verification 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 $\mathfrak{A}$ giebt es mindestens ein Ding μ_2 in $\mathfrak{A}$ von der Art, dass α, β beide in dem System μ_2' enthalten sind.

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

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

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

und behaupten zunächst, dass

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

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 Theiler oder ein Vielfaches von $\mathfrak{a}$ sein kann, und hieraus ergiebt sich weiter, dass in (44) und (45) nur *echte* Theilbarkeiten 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 von einander 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* Theiler 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 Theiler 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 Theilgruppen 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 Theilers 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 That leicht überzeugen, dass das Kettengesetz in einer Dualgruppe $\mathfrak{H}$ gültig und doch in einer Theilgruppe $\mathfrak{G}$ 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 $+$ gemäss (4) und (1) durch $n + n = n$, $m + n = n + m$, und zwar im Einzelnen durch

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

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

definirt. Die genaue Prüfung (vergl. die letzte Anmerkung) ergiebt 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

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

genügen, eine gegenseitige eindeutige Correspondenz, welche durch jede der beiden, wechselseitig aus einander folgenden Beziehungen

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

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

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

Beweis. Unsere Behauptung besteht darin, dass aus (47) und (49) sich (48) und (50) ergiebt, 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 Theiler von b, so ist a ein nächster Theiler von $a - b$, und umgekehrt.

Beweis. Ist $a + b$ ein nächster, also auch ein echter Theiler von b, so folgt zunächst, dass a auch ein echter Theiler 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 Theiler von $a - b$. Umgekehrt, wenn Letzteres der Fall, also a auch ein echter Theiler von $a - b$ ist, so folgt zunächst, dass $a + b$ auch ein echter Theiler 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) definirte 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 Theiler von b, w. z. b. w.

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

Beweis. Aus der Annahme $b < m$ folgt nach dem Modulgesetz VIII, dass man ein Element q in der doppelten Form

$$q = (p + m) - b = (p - b) + m$$

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

und da $\mathfrak{p} - (\mathfrak{p} + \mathfrak{m}) = \mathfrak{p}$ ist, so folgt $\mathfrak{p} - \mathfrak{m} = \mathfrak{p} - \mathfrak{b}$; setzt man jetzt $\mathfrak{a} = \mathfrak{b}$, $\mathfrak{b} = \mathfrak{p} + \mathfrak{m}$, so wird $\mathfrak{a} + \mathfrak{b} = \mathfrak{p} + \mathfrak{m} + \mathfrak{b} = \mathfrak{p} + \mathfrak{b}$, $\mathfrak{a} - \mathfrak{b} = \mathfrak{m}$; es ist daher $\mathfrak{a}$ ein uächster Theiler von $\mathfrak{a} - \mathfrak{b}$, also nach dem vorigen Satze auch $\mathfrak{p} + \mathfrak{b}$ ein nächster Theiler 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 Theiler $\mathfrak{a}$, $\mathfrak{b}$, so ist $\mathfrak{a} - \mathfrak{b} = \mathfrak{m}$, und $\mathfrak{a} + \mathfrak{b}$ ist ein nächster Theiler von $\mathfrak{a}$ und von $\mathfrak{b}$.

Beweis. Zufolge der *ersten* Annahme ist $\mathfrak{d}$ ein gemeinsamer Theiler von $\mathfrak{a}$, $\mathfrak{b}$, also auch ein Theiler vou $\mathfrak{a} + \mathfrak{b}$, 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 Theiler 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 Theiler von $\mathfrak{a}$ und $\mathfrak{b}$, woraus nach XII folgt, dass $\mathfrak{b}$ und $\mathfrak{a}$ nächste Theiler 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 $\mathfrak{a} - \mathfrak{b}$ verschieden von $\mathfrak{m}$, so müsste, weil $\mathfrak{a}$ und $\mathfrak{b}$ nächste Theiler von $\mathfrak{m}$ sind, $\mathfrak{a} - \mathfrak{b} = \mathfrak{a} = \mathfrak{b}$ sein, was unserer Annahme widerspricht; mithin ist $\mathfrak{a} - \mathfrak{b} = \mathfrak{m}$ ein nächstes Vielfaches von $\mathfrak{a}$ und $\mathfrak{b}$, woraus nach XII folgt, dass $\mathfrak{a} + \mathfrak{b}$ ein nächster Theiler von $\mathfrak{b}$ und $\mathfrak{a}$ 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 Theilbarkeiten in (15) bis (18) zu vergleichen; so erhält man

$$\begin{aligned}
\mathfrak{a}''' + \mathfrak{b}''' &= \mathfrak{d}'''', & \mathfrak{a}''' - \mathfrak{b}''' &= \mathfrak{c}'',\\
\mathfrak{a}'' + \mathfrak{b}'' &= \mathfrak{c}''', & \mathfrak{a}'' - \mathfrak{b}'' &= \mathfrak{d}',\\
\mathfrak{a}' + \mathfrak{d}' &= \mathfrak{a}'', & \mathfrak{a}' - \mathfrak{d}' &= \mathfrak{a}_0,\\
\mathfrak{a}_0 + \mathfrak{b}_0 &= \mathfrak{d}', & \mathfrak{a}_0 - \mathfrak{b}_0 &= \mathfrak{d}_1,\\
\mathfrak{a} + \mathfrak{a}_0 &= \mathfrak{a}', & \mathfrak{a} - \mathfrak{a}_0 &= \mathfrak{a}_1,\\
\mathfrak{a}_1 + \mathfrak{d}_1 &= \mathfrak{a}_0, & \mathfrak{a}_1 - \mathfrak{d}_1 &= \mathfrak{a}_2,\\
\mathfrak{a}_2 + \mathfrak{b}_2 &= \mathfrak{d}_1, & \mathfrak{a}_2 - \mathfrak{b}_2 &= \mathfrak{c}_3,\\
\mathfrak{a}_3 + \mathfrak{b}_3 &= \mathfrak{c}_2, & \mathfrak{a}_3 - \mathfrak{b}_3 &= \mathfrak{d}_4.
\end{aligned}$$

Wir wollen ferner bemerken, dass die im *ersten* Theile des Satzes aufgestellte Behauptung $\mathfrak{a} + \mathfrak{b} = \mathfrak{d}$ offenbar für *jede* Dualgruppe gilt,

während die auf $\mathfrak{a} - \mathfrak{b}$ bezügliche Behauptung wesentlich auf der Voraussetzung des Modulgesetzes beruht; betrachten wir z. B. die Dualgruppe $\mathfrak{G}$, welche wir bei dem Beweise des Satzes IX gebildet haben, so sind die beiden Elemente $\mathfrak{a}$, $\mathfrak{b}_1$ nächste Vielfache von $\mathfrak{b}''' = \mathfrak{a} + \mathfrak{b}_1$, aber nur $\mathfrak{a}$, nicht $\mathfrak{b}_1$, ist ein nächster Theiler von $\mathfrak{c}_3 = \mathfrak{a} - \mathfrak{b}_1$. Ebenso gilt im *zweiten* Theile nur die Behauptung $\mathfrak{a} - \mathfrak{b} = \mathfrak{m}$ allgemein für *jede* Dualgruppe, während die auf $\mathfrak{a} + \mathfrak{b}$ 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 giebt 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

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

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

Sieht man die zweite als eine Fortsetzung der ersten an, so entsteht eine Gesammtreihe $\mathfrak{P}'$, in welcher offenbar jedes Element ein Theiler des folgenden ist. Sind zwei solche auf einander folgende Elemente *verschieden*, so folgt aus dem Satze XIII, dass das erste ein *nächster* Theiler des folgenden ist; behält man daher von mehreren *gleichen* auf einander folgenden 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, vertheilen wir die n Indices $0, 1, 2 \cdots (n-1)$ in zwei getrennte Classen, deren erste alle diejenigen p Indices r enthält, für welche $\mathfrak{p} + \mathfrak{k}_r$ verschieden von $\mathfrak{p} + \mathfrak{k}_{r+1}$ wird, während die zweite Classe aus allen übrigen q Indices 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 theilweise 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 auf einander folgenden 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

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

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

$$\mathfrak{d}''''\ \mathfrak{b}'''\ \mathfrak{b}'''\ \mathfrak{b}'''\ \mathfrak{b}'''\ \mathfrak{c}''\ \mathfrak{c}'\ \mathfrak{c}'\ \mathfrak{c}'$$

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

und die Kette $\mathfrak{P}$ wird

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

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

$$\mathfrak{d}''''\ \mathfrak{d}''''\ \mathfrak{c}'''\ \mathfrak{c}'''\ \mathfrak{c}'''\ \mathfrak{b}''\ \mathfrak{b}'\ \mathfrak{b}'\ \mathfrak{b}$$

$$\mathfrak{b}\ \ \mathfrak{b}_1\ \ \mathfrak{b}_1\ \ \mathfrak{b}_2\ \ \mathfrak{c}_3\ \ \mathfrak{c}_3\ \ \mathfrak{c}_3\ \ \mathfrak{b}_4\ \ \mathfrak{b}_4$$

und die Kette $\mathfrak{P}$ wird

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

zugleich ist $p = q = 4$.

Aus den beiden vorhergehenden Sätzen XIV und XV ergiebt 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 Induction 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 $m = 1$ ergiebt 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 Theiler $\mathfrak{b}$, und da jedes Element $\mathfrak{h}$ einer Kette $\mathfrak{K}$ ein Vielfaches von ihrem Anfang und zugleich ein Theiler 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 Inductionsmethode 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 irgend eine 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 $\mathfrak{a}$, so entsteht aus $\mathfrak{K}$ eine Theilkette $\mathfrak{K}_1$ von der Länge n, deren Anfang und Ende resp. die Elemente $\mathfrak{k}_1, \mathfrak{b}$ sind, und ebenso entspringt aus $\mathfrak{H}$ eine Theilkette $\mathfrak{H}_1$ von der Länge e, deren Anfang und Ende resp. die Elemente $\mathfrak{h}_1$, $\mathfrak{b}$ 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 $\mathfrak{a}$ auch *nächste* Theiler 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 Theiler desselben Elementes $\mathfrak{b}$ sind, so genügt $\mathfrak{p}$ offenbar den Bedingungen $\mathfrak{k}_1 < \mathfrak{p} < \mathfrak{b}$, und folglich giebt 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 Theiler 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

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

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

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

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 Modulgesetze und dem Kettengesetze nachgewiesen ist, fügen wir noch einige Bemerkungen über *endliche Modulgruppen* hinzu, deren Beweise der

Leser leicht finden wird. Unter den Elementen $\mathfrak{m}$ einer solchen Gruppe $\mathfrak{M}$ giebt es offenbar ein und nur ein Element $\mathfrak{p}$, welches ein Theiler von allen $\mathfrak{m}$, und ebenso giebt 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 giebt es in $\mathfrak{M}$ mindestens ein nächstes Vielfaches von $\mathfrak{m}$, und wenn $\mathfrak{m}$ verschieden von $\mathfrak{p}$ ist, so giebt es in $\mathfrak{M}$ mindestens einen nächsten Theiler von $\mathfrak{m}$. Wenn ferner $\mathfrak{a}$ ein echter Theiler von $\mathfrak{b}$ ist, so giebt 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, auf einander folgender *Stufen* S eintheilen; 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 Theiler 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

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

dessen Beweis wir ausführen wollen. Falls eins der beiden Elemente, z. B. $\mathfrak{a}$ ein Theiler 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 theilbar, also $\mathfrak{a} + \mathfrak{b}$ ein echter Theiler von $\mathfrak{b}$ ist, so giebt 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 $\mathfrak{d}$, $\mathfrak{m}$ irgend zwei auf einander folgende Glieder dieser Kette, so ist auch $\mathfrak{a} + \mathfrak{d} = \mathfrak{a} + \mathfrak{m}$, woraus nach Satz XIII folgt, dass $\mathfrak{a} - \mathfrak{d}$ ein nächster Theiler 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 ergiebt 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 $\mathfrak{p} = \mathfrak{d}''''$, $\mathfrak{q} = \mathfrak{d}_4$, $k = 8$, 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 $\mathfrak{d}_1$, $\mathfrak{b}_2$, $\mathfrak{c}_2$, $\mathfrak{a}_3$, $\mathfrak{d}_4$ für sich eine Modulgruppe mit vier Stufen S', von denen

$$\begin{aligned} S_1' &\text{ aus } \mathfrak{d}_1, \\ S_2' &\text{ „ } \mathfrak{b}_2, \mathfrak{c}_2, \\ S_3' &\text{ „ } \mathfrak{a}_3, \\ S_4' &\text{ „ } \mathfrak{d}_4 \end{aligned}$$

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 $\mathfrak{d}_4$ 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 Theilbarkeit $\mathfrak{m} > \mathfrak{d}$ immer $(\mathfrak{m}, \mathfrak{d}) = 1$ folgt; wir fügen jetzt noch hinzu, dass zufolge derselben Bedeutung auch umgekehrt aus $(\mathfrak{m}, \mathfrak{d}) = 1$ immer die Theilbarkeit $\mathfrak{m} > \mathfrak{d}$ folgt, dass also die beiden Aussagen

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

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

Nehmen wir nun an, in irgend einer Dualgruppe $\mathfrak{H}$ entspreche je zwei Elementen $\mathfrak{m}, \mathfrak{n}$ ein mit $(\mathfrak{m}, \mathfrak{n})$ bezeichneter und zwar von Null verschiedener Zahlwerth, 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 That, 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) combiniren, so ergiebt 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 ergiebt 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 nothwendige 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 Classe von Dualgruppen $\mathfrak{H}$ zu betrachten, in welchen die genannten Symbolgesetze wenigstens theilweise erfüllt sind, ich meine die Dualgruppen $\mathfrak{H}$, deren Elemente die sämmtlichen Theilgruppen einer gewöhnlichen endlichen *Galois'schen Gruppe* $\mathfrak{g}$ sind. Die Elemente $\alpha, \beta, \gamma, \cdots$ einer solchen Gruppe $\mathfrak{g}$ reproduciren sich bekanntlich durch eine Operation, welche in der Regel wie eine Multiplication bezeichnet wird und dem associativen 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 $\mathfrak{a}$, $\mathfrak{b}$ irgend welche Complexe von Elementen in $\mathfrak{g}$, und bezeichnet man allgemein mit $\mathfrak{ab}$ den Complex aller in der Form $\alpha\beta$ enthaltenen Elemente, wo α, β resp. alle Elemente in $\mathfrak{a}$, $\mathfrak{b}$ durchlaufen, so ist $\mathfrak{a}$ dann und nur dann eine *Gruppe*, ein *Theiler* von $\mathfrak{g}$, wenn $\mathfrak{aa} = \mathfrak{a}$ ist. Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei solche Theilgruppen von $\mathfrak{g}$, so ist ihr grösster gemeinsamer Theiler 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 Multiplication 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 Theilgruppen von $\mathfrak{g}$, welche (wie z. B. $\mathfrak{g}$

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

selbst) gemeinsame *Vielfache* von $\mathfrak{a}$, $\mathfrak{b}$ sind, d. h. welche sowohl $\mathfrak{a}$ als $\mathfrak{b}$ zum Theiler haben. Offenbar genügen diese beiden Operationen $+$ den Grundgesetzen (1), (2), (3), mithin ist der Inbegriff $\mathfrak{H}$ aller in $\mathfrak{g}$ als Theiler enthaltenen Gruppen $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c} \cdots$ eine *Dualgruppe* im Sinne von § 1, auf welche wir auch die Bedeutung der Theilbarkeitszeichen $<$ und $>$ übertragen wollen.

Hierzu tritt nun Folgendes. Ist die Gruppe $\mathfrak{a}$ ein Theiler von $\mathfrak{g}$, und sind β, γ irgend zwei Elemente in $\mathfrak{g}$, so sind die beiden Complexe $\mathfrak{a}\beta$, $\mathfrak{a}\gamma$ entweder vollständig identisch, oder sie haben kein einziges gemeinsames Element, und wenn $\mathfrak{b}$ ebenfalls eine Theilgruppe von $\mathfrak{g}$ bedeutet, so wollen wir durch das *Gruppen-Symbol* $(\mathfrak{a}, \mathfrak{b})$ die Anzahl aller von einander verschiedenen Complexe $\mathfrak{a}\beta$ bezeichnen, die allen Elementen β der Gruppe $\mathfrak{b}$ entsprechen, und aus welchen offenbar der Complex $\mathfrak{ab}$ 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* Symbolgesetze (28) nicht allgemein behaupten kann. Offenbar sind nämlich alle Elemente des Complexes $\mathfrak{ab}$ in der Gruppe $\mathfrak{a} - \mathfrak{b}$ enthalten, aber im Allgemeinen wird die letztere noch *andere* Elemente enthalten, und da der Complex $\mathfrak{ab}$ schon aus $(\mathfrak{a}, \mathfrak{b})$ verschiedenen Complexen $\mathfrak{a}\beta$ besteht, so wird im Allgemeinen $(\mathfrak{a}, \mathfrak{a}-\mathfrak{b})$ *grösser als* $(\mathfrak{a}, \mathfrak{b})$ sein; der Fall $(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{a}, \mathfrak{a}-\mathfrak{b})$ tritt daher immer und nur dann ein, wenn der Complex $\mathfrak{ab}$ eine *Gruppe*, also $= \mathfrak{a} - \mathfrak{b}$ ist, und das charakteristische Merkmal hierfür besteht in der Identität $\mathfrak{ab} = \mathfrak{ba}$. Wenn also je zwei Theiler $\mathfrak{a}$, $\mathfrak{b}$ 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 $\mathfrak{a} - \mathfrak{b} = \mathfrak{ab} = \mathfrak{ba}$ ist, so nimmt das aus der Annahme $\mathfrak{d} < \mathfrak{m}$ zu beweisende Gesetz VIII die Gestalt $(\mathfrak{p}+\mathfrak{m})\mathfrak{d} = \mathfrak{pd} + \mathfrak{m}$ an. Nun steht jedes Element des Durchschnittes $\mathfrak{pd} + \mathfrak{m}$ unter der doppelten Form $\pi\delta = \mu$, wo π, δ, μ resp. Elemente der Gruppen $\mathfrak{p}$, $\mathfrak{d}$, $\mathfrak{m}$ bedeuten, und da $\mathfrak{d}$ nach Voraussetzung ein Theiler 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 $(\mathfrak{p}+\mathfrak{m})\mathfrak{d}$ enthalten; folglich ist die Gruppe $\mathfrak{pd} + \mathfrak{m}$ ein Theiler der Gruppe $(\mathfrak{p}+\mathfrak{m})\mathfrak{d}$, und

*) Vergl. §. 9 meiner Abhandlung: Ueber die Anzahl der Idealclassen in reinen cubischen Zahlkörpern (Crelle's Journal Bd. 121, S. 77).

**) 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.

da nach dem Satze VII umgekehrt $(\mathfrak{p}+\mathfrak{m})\mathfrak{d}$ gewiss ein Theiler von $\mathfrak{p}\mathfrak{d}+\mathfrak{m}$ ist, so sind beide Gruppen mit einander 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 sämmtliche Theiler $\mathfrak{a}$, $\mathfrak{b}$ diese Eigenschaft $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$ besitzen, gehören augenscheinlich alle Abel'schen Gruppen, ferner diejenigen, welche ich Hamilton'sche 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 cyklischen Vertauschungen von beliebigen verschiedenen Dingen 0, 1, 2, 3 $\cdots$, 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

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

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

Braunschweig, den 8. Januar 1900.

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