besserer Titel: Über Dualgruppen.

Über die von drei Moduln erzeugte Dualgruppe.

Von R. Dedekind zu 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 vorgeführt, die aus drei beliebigen Moduln durch fortgesetzte Bildung des gemeinsamen größten Theilers 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 Bemerkungen über allgemeine Dualgruppen.x)

§1. Allgemeine Eigenschaften der Dualgruppen.

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

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

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

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

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

Die beiden Operationen ± sind ferner durch die beiden Gesetze

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

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

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

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 ± aus je zwei Elementen a, b eines (endlichen oder unendlichen) Systems ~~A~~ G zwei Elemente a ± b desselben Systems ~~A~~ G erzeugen und zugleich den Gesetzen (1), (2), (3) genügen, so ~~A~~ soll G mit Bezug auf dieses Operationspaar ± 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 G zukommen.

Zufolge (4) bildet jedes ~~Modul~~ Element a [einer Dualgruppe G für sich allein eine Dualgruppe.

Für zwei beliebige ~~Moduln~~ Elemente a, b ergiebt sich aus (2) und (4) auch

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

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

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

mithin bilden die vier ~~Moduln~~ Elemente a, b, (a+b), (a−b) gewiß eine Dualgruppe, und es fragt sich nun, wie viele von ihnen *verschieden* sind.

[Absatz

[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 ~~die~~ alle vier ~~Moduln~~ elementaren identisch mit einander. [Absatz

[Machen wir jetzt die (allgemeinere) Annahme, es sei $a+b$ identisch mit einem der beiden ~~Moduln~~ Elemente a, b, also z. B. $a+b = a$, so folgt aus (3'') auch $a - b = b$ [durch Vertauschung von a mit 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 üblichen Ausdrucks- und Bezeichnungsweise (D. §. 169) auf alle Dualgruppen und sagen: das Element a ist theilbar durch das Element b; a oder b heißt ein Vielfaches von b, und b ein Theiler von a; diese Theilbarkeit (welche die Identität von a, b nicht ausschließt) wird auch durch $a < b$ oder $b > a$ bezeichnet, und es ist daher jede der vier Aussagen

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

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

[Absatz

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

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

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

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

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

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

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

VI. Aus $a < b$, $a' < b$ folgt $a-a' < b$, d. h. jedes gemeinsame ~~Theiler~~ Vielfache b von a, a' ist ~~Theiler~~ theilbar durch $a-a'$, und aus $a < b$, $a < b'$ folgt $a < b+b'$, d. h. jeder gemeinsame ~~Vielfache~~ Theiler a von b, b' ist ~~Vielfaches~~ Theiler von $b+b'$. Wegen der Analogie mit der Zahlen- und Modultheorie heißt daher $a-a'$ das kleinste gemeinsame Vielfache von a, a', und $b+b'$ heißt der größte gemeinsame Theiler von b, b'. Diese Ausdrucksweise dehnen wir auch auf mehr als zwei [illegible] Elemente aus, und durch wiederholte Anwendung des Vorhergehenden ergiebt sich der Satz: ist jedes der Elemente $\alpha', \alpha'', \alpha''' \ldots$ ein Theiler von jedem der Elemente $\beta', \beta'', \beta''' \ldots$, so ist

$$\alpha' - \alpha'' - \alpha''' - \cdots < \beta' + \beta'' + \beta''' + \cdots,$$

d. h. das kleinste gemeinsame Vielfache der Elemente α ist ein Theiler des größten gemeinsamen Theilers der Elemente β.

VII ~~[illegible]~~ Ist ϑ ein Theiler von m, also $\vartheta < m$, und η ein beliebiges Element, so ist

$$(\eta + m) - \vartheta < (\eta - \vartheta) + m;$$

denn jedes der beiden Elemente $\eta + m$, ϑ ist ein Theiler von jedem der beiden Elemente $\eta - \vartheta$, m.

~~Satz, welcher ist, wie schon bemerkt, eine nothwendige Folge der Grundgesetze (1), (2), (3) und der in (7) enthaltenen Erklärung der Zeichen > und <, und aus dem letzten Satze ergiebt sich als specieller Fall auch der folgende [illegible]: Ist $m > \vartheta$ und α beliebig, so ist~~

§. 2. Die ~~[illegible]~~ 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 sie sich vor anderen Dualgruppen von allgemeinerem Charakter auszeichnen. In der Modultheorie gilt nämlich der bei weitem schärfere Satz (D. §. 169. S. 498):

[Absatz

VIII. Ist der Modul ~~[illegible]~~ ϑ ein Theiler des Moduls m, also $\vartheta < m$, ~~[illegible]~~, und ~~[illegible]~~ η ein beliebiger Modul, so ist

$$(\eta + m) - \vartheta = (\eta - \vartheta) + m.$$

Aber dieses Gesetz ist, wie ich ~~an anderer Stelle~~ [illegible] bewiesen habe, schlechterdings nicht ableitbar aus den Grundgesetzen (1), (2), (3) und bildet daher eine für die Modultheorie wesentliche Ergänzung ~~dieser Grundgesetze~~ derselben. ~~[illegible]~~

[Modulgesetz

[im §. 4 meiner in der Einleitung citirten Aufsatzes

Wir formen dieses Gesetz zunächst in folgendes

Sind a, b, c drei beliebige Moduln, und ersetzt man y, m, d ~~[illegible]~~ resp. durch a, $b-c$, $b+c$, so ist die Bedingung $m > d$ erfüllt, und ~~[illegible]~~ es ergibt sich

$$(a+(b-c)) - (b+c) = (a-(b+c)) + (b-c) \quad (8)$$

und umgekehrt folgt hieraus wieder das Modulgesetz VIII, wenn man a, b, c resp. durch y, m, d ersetzt und die Annahme $m > d$ hinzufügt.

[D.

Reihe um

~~[illegible]~~

Hierauf wenden wir uns zu dem in der Einleitung ~~Überschrift~~ bezeichneten Gegenstande, nämlich zur Beschreibung der aus drei beliebigen Moduln a, b, c durch die Operationen $\pm$ erzeugten Dualgruppe. Dieselbe ist endlich und besteht aus 28 Moduln, die im Allgemeinen von einander verschieden sind. Vier von diesen Moduln sind symmetrisch aus a, b, c gebildet und sollen gemeinsam mit d bezeichnet, aber durch Accente und Indices von einander unterschieden werden, deren Bedeutung später einleuchten wird:

$$d'''' = a + b + c \,, \quad d_4 = a - b - c \qquad (9)$$

20

$$d' = (b+c) - (c+a) - (a+b) \,, \quad d_1 = (b-c) + (c-a) + (a-b) \qquad (10)$$

Die übrigen 24 Moduln haben die Eigenschaft, durch alle ~~[illegible]~~ Vertauschungen von a, b, c nur drei verschiedene Formen anzunehmen, und diejenigen 8 Moduln, welche (wie z. B. a selbst) durch Vertauschung von b mit c nicht geändert werden, sollen gemeinsam mit a und zugehörigen Accenten und Indices bezeichnet werden, woraus die Bedeutung der mit b und c bezeichneten 16 Moduln von selbst erhellt. Da die drei Moduln a, b, c durch sich selbst erklärt sind, so bleiben uns die folgenden 21 Definitionen:

$$\left.\begin{array}{ll} a''' = b + c \,, & a_3 = b - c \\ b''' = c + a \,, & b_3 = c - a \\ c''' = a + b \,, & c_3 = a - b \end{array}\right\} \quad (11)$$

$$\left.\begin{array}{ll} a'' = (c+a) - (a+b)\,, & a_2 = (c-a) + (a-b) \\ b'' = (a+b) - (b+c)\,, & b_2 = (a-b) + (b-c) \\ c'' = (b+c) - (c+a)\,, & c_2 = (b-c) + (c-a) \end{array}\right\} \quad (12)$$

$$\left.\begin{array}{ll} a' = a + (b-c)\,, & a_1 = a - (b+c) \\ b' = b + (c-a)\,, & b_1 = b - (c+a) \\ c' = c + (a-b)\,, & c_1 = c - (a+b) \end{array}\right\} \quad (13)$$

$$\left.\begin{array}{l} a_0 = (a - (b+c)) + (b-c) = (a + (b-c)) - (b+c) \\ b_0 = (b - (c+a)) + (c-a) = (b + (c-a)) - (c+a) \\ c_0 = (c - (a+b)) + (a-b) = (c + (a-b)) - (a+b) \end{array}\right\} \quad (14)$$

umstellen

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 ~~[illegible]~~ unteren Index verbunden; die doppelten Definitionen (14) beruhen auf dem oben hervorgehobenen Modulgesetz (8).

Wir haben nun zu zeigen, daß der Complex ~~[illegible]~~ D ~~[illegible]~~ dieser 28 Moduln wirklich eine Dualgruppe ist, daß also, wenn m, n irgend zwei dieser Moduln bedeuten, auch die beiden Moduln $m \pm n$ in ~~[illegible]~~ enthalten sind. [~~[illegible]~~ D] Zufolge (4) brauchen wir nur ~~[illegible]~~ solche Paare zu betrachten, die aus zwei ~~[illegible]~~ verschiedenen x) Moduln m, 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. m durch den andern n theilbar ist, so daß $m + n = n$, $m - n = m$ wird, was wir kürzer durch $m > n$ oder $n < m$ bezeichnen. Der Raumes wegen begnügen wir uns, von diesen 261 ~~[illegible]~~ Theilbarkeiten nur die 48 ursprünglichen, d. h. diejenigen aufzuschreiben, aus welchen die übrigen 213 nach dem obigen Satze III sich ableiten lassen: [in D. 1]

x) Weiter unten wird durch ein Beispiel bewiesen, daß die 28 Moduln wirklich alle von einander verschieden sein können, und ~~[illegible]~~ der Einfachheit halber nennen wir sie auch hier verschieden, obgleich sie z. B. in dem Falle $a = b = c$ alle $= a$ sind.

$$d'''' < a''', b''', c''' \;;\; d_4 > a_3, b_3, c_3 \qquad (15)$$

$$\left.\begin{array}{ll} a''' < b'', c'' & ;\; a_3 > b_2, c_2 \\ b''' < c'', a'' & ;\; b_3 > c_2, a_2 \\ c''' < a'', b'' & ;\; c_3 > a_2, b_2 \end{array}\right\} \qquad (16)$$

$$\left.\begin{array}{ll} a'' < d', a' & ;\; a_2 > d_1, a_1 \\ b'' < d', b' & ;\; b_2 > d_1, b_1 \\ c'' < d', c' & ;\; c_2 > d_1, c_1 \end{array}\right\} \qquad (17)$$

$$\left.\begin{array}{ll} d' < a_0, b_0, c_0 & ;\; d_1 > a_0, b_0, c_0 \\ a' < a, a_0 & ;\; a_1 > a, a_0 \\ b' < b, b_0 & ;\; b_1 > b, b_0 \\ c' < c, c_0 & ;\; c_1 > c, c_0 \end{array}\right\} \qquad (18)$$

Die Theilbarkeiten (15) folgen unmittelbar aus der Vergleichung von (9) mit (11), ebenso ergiebt sich (16) aus (11) und (12); von den Theilbarkeiten (17) ~~[illegible]~~ folgen die auf d' und d_1 bezüglichen aus dem Vergleich von (10) mit (12), die übrigen aus (12) und (13) nach dem obigen Satze ~~III~~ VI in §. 1. Von den Theilbarkeiten (18) fließen die auf a, b, c bezüglichen unmittelbar aus (13); da ferner a_0 ~~[illegible]~~ $= a' - (b+c) = a_1 + (b-c)$ ist, so folgt z. B. $a' < a_0 < a_1$; da endlich $d' = a'' - (b+c)$ und $d_1 = a_2 + (b-c)$, ferner $a'' < a'$ und $a_2 > a_1$ ist zufolge (17), so ergiebt sich auch $d' < a_0 < d_1$, 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 $\varphi(m)$ die Anzahl aller so erhaltenen Theiler n von m, welche ~~[illegible]~~ von m und von einander verschieden sind, so ergiebt sich successive $\varphi(d'''') = 0$, $\varphi(a''') = 1$, $\varphi(a'') = 3$, $\varphi(d') = 7$, $\varphi(a') = 4$, $\varphi(a) = 5$, $\varphi(a_0) = 9$, $\varphi(d_1) = 14$, $\varphi(a_1) = 11$, $\varphi(a_2) = 17$, $\varphi(a_3) = 21$, $\varphi(d_4) = 27$; rechnet man noch die entsprechenden Anzahlen für die mit b, c bezeichneten Moduln hinzu, so ~~[illegible]~~ wird die Summe aller $\varphi(m) = 261$, und dies ist also die Anzahl aller auf diesem Wege gewonnenen Theilbarkeiten $m > n$. Daß hiermit auch alle Theilbarkeiten innerhalb der allgemeinen Gruppe erschöpft sind, ergiebt sich später aus dem Folgenden.

Wir wenden uns jetzt zu den übrigen 117 Paaren m, n, um die entsprechenden Moduln $m \pm n$ anzugeben; des Raumes und des leichteren Überblickes wegen begnügen wir uns, nur 29 solche Paare zu betrachten, aus denen die übrigen durch Vertauschungen von a, b, c ~~[illegible]~~ hervorgehen; ~~[illegible]~~ unter diesen 29 Formelpaaren sind 19 ~~[illegible]~~ dualistische ~~[illegible]~~ Repräsentanten von je 3, und 10 Repräsentanten von je 6 Formelpaaren, woraus sich ihre Gesammtanzahl $= 3 \cdot 19 + 6 \cdot 10 = 117$ ergiebt.

$$\left.\begin{array}{ll} a + a''' = d'''', & a - a_3 = d_4 \\ a' + a''' = d'''', & a_1 - a_3 = d_4 \\ a'' + a''' = d'''', & a_2 - a_3 = d_4 \\ b''' + a''' = d'''', & b_3 - a_3 = d_4 \end{array}\right\} \qquad (19)$$

$$\left.\begin{array}{ll} b+c = a''' , & b-c = a_3 \\ b+c' = a''' , & b-c_1 = a_3 \\ b'+c' = a''' , & b_1-c_1 = a_3 \\ b+c'' = a''' , & b-c_2 = a_3 \\ b'+c'' = a''' , & b_1-c_2 = a_3 \\ b''+c'' = a''' , & b_2-c_2 = a_3 \end{array}\right\} (20)$$

$$\left.\begin{array}{ll} a+b_1 = a'' , & a-b' = a_2 \\ a+b_0 = a'' , & a-b_0 = a_2 \\ a'+b_1 = a'' , & a_1-b' = a_2 \\ a'+b_0 = a'' , & a_1-b_0 = a_2 \\ a+d' = a'' , & a-d_1 = a_2 \\ a'+d' = a'' , & a_1-d_1 = a_2 \end{array}\right\} (21)$$

$$\left.\begin{array}{ll} a_1+b_1 = d' , & a'-b' = d_1 \\ a_0+b_1 = d' , & a_0-b' = d_1 \\ a_0+b_0 = d' , & a_0-b_0 = d_1 \end{array}\right\} (22)$$

$$\left.\begin{array}{ll} a+a_3 = a' , & a-a''' = a_1 \\ a+b_2 = a' , & a-b'' = a_1 \\ a+d_1 = a' , & a-d' = a_1 \\ a+a_0 = a' , & a-a_0 = a_1 \end{array}\right\} (23)$$

$$\left.\begin{array}{ll} a_1+a_3 = a_0 , & a'-a''' = a_0 \\ a_1+b_2 = a_0 , & a'-b'' = a_0 \\ a_1+d_1 = a_0 , & a'-d' = a_0 \end{array}\right\} (24)$$

$$\left.\begin{array}{ll} a_2+a_3 = d_1 , & a''-a''' = d' \\ a_2+b_2 = d_1 , & a''-b'' = d' \end{array}\right\} (25)$$

$$b_3+c_3 = a_2 , \quad b'''-c''' = a'' \qquad (26)$$

Der Beweis dieser 29 Doppelsätze, welche hier in 8 Gruppen (19) bis (26) getheilt sind, ist nun keineswegs so mühselig, wie es auf den ersten Blick zu befürchten steht. Zunächst ~~Allgem~~ ergiebt sich aus dem dualistischen Charakter der Grundgesetze (1), (2), (3) und der specifischen Modul, gesetzes (VIII oder (8), zeigt aus der entsprechenden Bezeichnung durch obere Accente und untere Indices zu 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 $m + n = y$ besonders zu beweisen ist, weil die übrigen die gemeinsame Form $m' + n' = y$ haben, wo m', n' zufolge der schon bewiesenen Theilbarkeiten (15) bis (18) den Bedingungen $m > m' > y$, $n > n' > y$ genügen, woraus nach den Sätzen V und III in §. 1 wirklich $m' + n' = y$ folgt. Hiernach erledigt sich unser Beweis durch die folgenden Betrachtungen. ~~Hiernach beruht unser Beweis auf den folgenden Betrachtungen.~~

Der erste Satz in der Gruppe (19') folgt unmittelbar aus den Definitionen (9') und (11') von d'''' und a'''.

22

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''), (12''), (13'') beachtet.

~~Der erste Satz in der Gruppe (20) ist nur eine Wiederholung der Definition (11) von a'''. Der erste Satz in der Gruppe (21) ergiebt sich aus dem [illegible] Modulgesetz VIII, wenn man dort [illegible] setzt. [illegible] folgt aus die Definitionen (12) und (13) [illegible] beachtet. Der erste Satz in der Gruppe (22) folgt ebenfalls aus VIII, wenn man dort [illegible] $m = b_1$, $d = b + c = a'''$ setzt, wodurch die Bedingung $m > d$ zufolge (16), (17), (18) erfüllt sind; auf diese Weise ergiebt sich nämlich~~

$$\cancel{b_1 + (a - (b+c)) = (b_1 + a) - (b+c)},$$

~~und dies stimmt mit unserm Satze überein, weil links $a - (b+c) = a_1$ zufolge (13), und rechts $b_1 + a = a''$ zufolge (21), also die rechte Seite zufolge (12) und (10) mit d' identisch ist.~~

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 $d < m$ geltenden Modulgesetze ~~VIII~~

$$(y - d) + m = (y + m) - d.$$

Setzt man nämlich

$$y = b,\ d = c + a = b''',\ m = a,$$

so ist die Voraussetzung $d < m$ erfüllt, und der schon bewiesenen Sätze zufolge (23''), (26'') wird $y - d = b - b''' = b_1$, also $(y - d) + m = a + b_1$, ferner $y + m = b + a = c'''$, $(y + m) - d = c''' - b''' = a''$, wodurch (21') bewiesen ist. Setzt man aber

$$y = a,\ d = b + c = a''',\ m = b - (c + a) = b_1,$$

so ist zufolge IV in §. 1 die Voraussetzung $d < m$ erfüllt, und zufolge (der schon bewiesenen Sätze) (23''), (21'), (25'') wird $y - d = a - a''' = a_1$, also $(y - d) + m = a_1 + b_1$, ferner $y + m = a + b_1 = a''$, $(y + m) - d = a'' - a''' = d'$, wodurch auch (22') bewiesen ist.

~~Der erste Satz in der Gruppe (23) ist zufolge der Definition (11) von t_3 nur eine Wiederholung der Definition (13) von a.~~

~~Der erste Satz in der Gruppe (24) ist zufolge der Definitionen (13) und (11) von a_1 und t_3 nur eine Wiederholung der Definition (14) von a_0.~~

~~Der erste Satz in der Gruppe (25) ist zufolge der Definitionen (12) und (11) von a_2 und a_3 nur eine Wiederholung der Definition (10) von d_1.~~

~~Endlich ist der Satz (26) zufolge der Definitionen (11) von b_3, c_3 nur eine Wiederholung der Definition (12) von a_2.~~

Hiermit ist der vollständige Beweis erbracht, daß je zwei Moduln m, n unseres Systems D (in demselben System enthalten) immer zwei Moduln m ± n erzeugen; mithin bilden diese 28 Moduln wirklich eine Dualgruppe D. Die Gesammtheit aller Erzeugnisse m ± n ist in der beigefügten Tabelle dargestellt, zu welcher (?) ist Folgendes zu bemerken. Je nachdem das Kreuzungsfeld der Zeile m mit der Spalte n der rechten oberen oder der linken unteren Hälfte angehört, enthält dasselbe den Modul m + n oder den Modul m − n, und um diese Trennung zwischen diesen beiden Hälften für das Auge recht deutlich zu machen, sind die den Fällen m = n = m ± 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 es könnte die Frage aufgeworfen werden, ob nicht in der Natur der Moduln gewisse, bis jetzt verborgen gebliebene Eigenschaften liegen, vermöge deren einige, äußerlich verschieden gebildete Moduln dieser Gruppe 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 Produkt $(b-c)(c-a)(a-b)$ ist (die kleinsten Zahlen dieser Art sind $a = 2$, $b = 3$, $c = d = 5$); bedeutet ferner ω eine irrationale Zahl, und setzt man

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

so wird

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

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

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

so wird

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

wo die sechs Zahlen d, d_1, d_2, m, m_1, m_2, 23
von denen man d, d_2, m, m_2 positiv wählen kann, durch folgende Regeln bestimmt werden:

$$[d_2] = [p_2, q_2]\ ,\ [dd_2] = [pp_2, pq_2, qp_2, qq_2, p_1q_2 - q_1p_2]$$
$$\frac{p_2}{d_2}\, d_1 \equiv p_1\ ,\ \frac{q_2}{d_2} \equiv q_1 \pmod{d}$$

und

$$\left[\frac{1}{m}\right] = \left[\frac{1}{p}, \frac{1}{q}\right]\ ,\ dd_2\, m m_2 = pp_2\, qq_2\ ,$$
$$\frac{m}{p}\, m_1 \equiv A p_1\ ,\ \frac{m}{q}\, m_1 \equiv B q_1 \pmod{m}\ ,$$

wo

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

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

~~Wir kehren nun zu der allgemeinen, aus drei beliebigen Moduln a, b, c erzeugten Dualgruppe zurück und stellen uns die Aufgabe, für je zwei Moduln m, n dieser Gruppe die Bestimmung des Symbols (m, n) auf die einfachsten Fälle zurückzuführen. Hierbei wollen wir die eigentliche Bedeutung dieses Symbols (D. §. 171. S. 509) ganz unbeachtet lassen und uns zunächst nur auf die beiden fundamentalen Sätze~~

§. 3. Das Symbol (m, n) in der Modulgruppe D.

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

$$(m, n) = (m+n, n) \qquad (27)$$

$$(m, n) = (m, m-n) \qquad (28)$$

die wir ~~[illegible]~~ jetzt ~~[illegible]~~ auf die, durch drei Moduln a, b, c erzeugte Dualgruppe D anwenden wollen. Hierbei wählen wir für m, n immer das letzte Modulpaar, welches in den Sätzen (19) bis (26) des §. 2 auftritt

~~stützen (D. S. 510), in denen wir für m, n immer das letzte Modulpaar wählen, das in den obigen Sätzen (19) bis (26) auftritt.~~ Auf diese Weise ergibt sich aus (19) ~~[illegible]~~ und (26) ~~[illegible]~~, wenn man a, b, c zyklisch permutirt,

$(d''', a''') = (b''', a''') = (b''', c'')$

$(a_3, d_4) = (a_3, b_3) = (c_2, b_3)$

hieraus aus (20) und (25)

$(b''', c'') = (a'', c'') = (a'', d')$

$(c_2, b_3) = (c_2, a_2) = (d_1, a_2)$

hieraus aus (21) und (24)

$(a'', d') = (a', d') = (a', a_0)$

$(d_1, a_2) = (d_1, a_1) = (a_0, a_1)$

zuletzt ~~hieraus~~ aus (23)

$(a', a_0) = (a, a_0) = (a, a_1)$

$(a_0, a_1) = (a_0, a) = (a', a)$

~~Wendet~~ Wendet man auf diese Kette von Gleichungen alle Vertauschungen von a, b, c an, so ergibt sich, daß man sechs Zahlen $a', b', c', a_1, b_1, c_1$ in folgender Weise [durch je sechs Gleichungen] definiren kann:

$$\left.\begin{aligned} a' &= (d'''', a''') = (b''', c'') = (c''', b'') = (a'', d') = (a', a_0) = (a, a_1) \\ b' &= (d'''', b''') = (c''', a'') = (a''', c'') = (b'', d') = (b', b_0) = (b, b_1) \\ c' &= (d'''', c''') = (a''', b'') = (b''', a'') = (c'', d') = (c', c_0) = (c, c_1) \end{aligned}\right\} \qquad (29)$$

$$\left.\begin{aligned} a_1 &= (a_3, d_4) = (c_2, b_3) = (b_2, c_3) = (d_1, a_2) = (a_0, a_1) = (a', a) \\ b_1 &= (b_3, d_4) = (a_2, c_3) = (c_2, a_3) = (d_1, b_2) = (b_0, b_1) = (b', b) \\ c_1 &= (c_3, d_4) = (b_2, a_3) = (a_2, b_3) = (d_1, c_2) = (c_0, c_1) = (c', c) \end{aligned}\right\} \qquad (30)$$

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

$$(a'', a') = (d', a') = (d', a_0)$$

$$(a_1, a_2) = (a_1, d_1) = (a_0, d_1)$$

und aus (22)

$$(d', a_0) = (b_0, a_0) = (b_0, d_1)$$

$$(a_0, d_1) = (a_0, b_0) = (d', b_0),$$

und wenn man in diesen Gleichungen alle Vertauschungen von a, b, c vornimmt, so ergiebt sich, daß man die siebente Zahl d durch die zwölf Gleichungen

$$\left.\begin{array}{l} d = (a'', a') = (b'', b') = (c'', c') = (d', a_0) = (d', b_0) = (d', c_0) \\ \quad = (a_1, a_2) = (b_1, b_2) = (c_1, c_2) = (a_0, d_1) = (b_0, d_1) = (c_0, d_1) \end{array}\right\} \quad (31)$$

definiren kann. Offenbar enthalten die Gleichungen (29), (30), (31) ~~(27), (28), (29)~~ alle diejenigen 48 Symbole (m, n), in welchen die Moduln m, n eine der 48 in (15) bis (18) aufgestellten ursprünglichen Theilbarkeiten m < n darbieten.

Man kann nun begreifen, ~~Es lässt sich nun zeigen~~, daß durch diese sieben Zahlen $d, a', b', c', a_1, b_1, c_1$ alle in unserer Dualgruppe D auftretenden Symbole (m, n), deren Anzahl $= 28 \cdot 28 = 784$ ist, sich ausdrücken lassen. Hierzu reichen aber die beiden Sätze (27), (28) nicht aus, sondern man bedarf noch des dritten Fundamentalsatzes über das Modulsymbol (m, n), welcher darin besteht, daß aus $y < q < r$ stets

$$(y, r) = (y, q)(q, r) \quad (32)$$

folgt (D. §. 171. S. 509).

Wendet man dies auf den Fall $y = q = r$ an, so ergiebt sich $(y, y) = (y, y)^2$; nach der Bedeutung des Modulsymbols (D. §. 171. S. 509) ist aber (y, y) niemals $= 0$, sondern immer $(y, y) = 1$. Mit Zuziehung dieser Ergänzung

ergiebt sich offenbar, daß alle Symbole (m, n) innerhalb unserer Dualgruppe D durch die sieben Zahlen $a', b', c', a_1, b_1, c_1, d$ darstellbar sind. Wir begnügen uns, dies für den Fall durchzuführen, wo m, n mit zwei der drei Moduln a, b, c übereinstimmen. Aus (27) und (31) folgt zunächst

$$(b, c) = (a''', c),$$

und da zufolge (16), (17), (18)

$$a''' < c'' < c' < c$$

ist, so folgt nach (32)

$$(b, c) = (a''', c'')(c'', c')(c', c);$$

wendet man hierin alle Vertauschungen von

Aus denselben beiden Sätzen (27), (28), auch wenn man die Bedeutung der Symbole gar nicht kennt, ergiebt sich ferner, daß alle diejenigen Symbole (m, n), in welchen $m > n$, also $m + n = n$, $m - n = m$ ist, mit einander identisch sind. Denn zunächst folgt hieraus $(m, n) = (n, n) = (m, m)$, und es braucht daher nur gezeigt zu werden, daß das Symbol (m, m) gänzlich unabhängig von dem Modul m, also $= (y, y)$ ist, wo y jeden beliebigen Modul bedeutet; ~~dies~~ zuerst ergiebt sich aber sofort aus (27), (28), wenn man n durch $m + y$ ersetzt und nachher m mit y vertauscht. – Dasselbe Resultat aber ohne Weiteres aus der Definition des Symbols, nach welcher aus $m > n$ stets $(m, n) = 1$ folgt*).

---

*) Daß umgekehrt aus $(m, n) = 1$ auch stets $m > n$ folgt (D. §. 171. S. 510), werden wir später (§. 8) zur Geltung bringen.

a, b, c an und drückt man die Factoren rechter Hand durch die kürzeren Zeichen in (29), (30), (31) aus, so erhält man

$$\left.\begin{array}{ll} (b,c) = b'\partial c_1 &, (c,b) = c'\partial b_1 \\ (c,a) = c'\partial a_1 &, (a,c) = a'\partial c_1 \\ (a,b) = a'\partial b_1 &, (b,a) = b'\partial a_1 \end{array}\right\} \quad (33)$$

Zu denselben Resultaten ~~[illegible]~~ gelangt man aber auch, wenn man den Satz (28) statt (27) anwendet; man erhält zunächst $(b,c) = (b,a_3)$, und da $b < b_1 < b_2 < a_3$ ist, so folgt

$$(b,c) = (b,b_1)(b_1,b_2)(b_2,a_3),$$

was mit (33) identisch ist. Die sieben Zahlen $a', b', c', a_1, b_1, c_1, \partial$ sind wirklich unabhängig von einander, d. h. es gelingt nicht, irgend welche Relationen zwischen ihnen abzuleiten; doch will ich auf den Beweis dieser Behauptung hier nicht näher eingehen.

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

~~[illegible]~~

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

oder

$$\left.\begin{array}{ll} (b,c) = (b,b_2)(c_3,c) &, (c,b) = (c,c_2)(b_3,b) \\ (c,a) = (c,c_2)(a_3,a) &, (a,c) = (a,a_2)(c_3,c) \\ (a,b) = (a,a_2)(b_3,b) &, (b,a) = (b,b_2)(a_3,a) \end{array}\right\} \quad (35)$$

geben kann, fließt auch der Satz

$$(b,c)(c,a)(a,b) = (c,b)(a,c)(b,a), \quad (36)$$

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 a, b verwandt, wenn (a, b) und (b, a) von Null verschieden sind (im Sinne von D. §. 171. S. 509), so sind ja zwei mit a verwandte

Moduln b, c auch mit einander verwandt. Dies ergiebt sich unmittelbar daraus, daß alle Factoren, welche in den vorstehenden Ausdrücken (33) oder (34) oder (35) von (b, c) und (c, b) auftreten, auch Factoren von mindestens einem der vier Symbole (a, b), (b, a), (a, c), (c, 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. —

Dies und Seite 16 erst später und in anderer Form!

Die obige, aus drei Moduln a, b, c erzeugte Dualgruppe G von 28 Moduln bietet nun noch einige bemerkenswerthe Erscheinungen dar, bei deren Beschreibung wir der Einfachheit halber voraussetzen wollen, diese 28 Moduln seien sämmtlich von einander verschieden. Diese Eigenschaften beruhen wesentlich auf den ursprünglichen Theilbarkeiten (15) bis (18), in welchen, wie eine eingehende Untersuchung x) ergeben würde, die ganze Constitution der Gruppe G ausschließlich der Sätze (19) bis (26) schon enthalten ist. Wir begnügen uns hier Folgendes hervorzuheben, ~~[illegible]~~ alle Moduln der Gruppe G in neun ~~[illegible]~~ verschiedene Stufen ~~[illegible]~~, die wir auf folgende Weise bezeichnen:

25

Wir nennen in unserer Gruppe G den Modul m einen nächsten Theiler des Moduls n, umgekehrt n ein nächstes Vielfaches von m, wenn erstens m < n, wenn zweitens m von n ver- ~~[illegible]~~ schieden ist, und wenn drittens außer m und n kein Modul in der Gruppe G giebt, der ein Vielfaches von m und zugleich Theiler von n ist. Dann treten in den Theilbarkeiten (15) bis (18) alle und nur solche Paare von nächsten Moduln ~~m, n~~ m, n auf, und hierauf gründet sich eine Vertheilung

$$\left.\begin{array}{ll}
\text{Stufe } S_{-4} & : d'''' \\
\text{"} \quad S_{-3} & : a''', b''', c''' \\
\text{"} \quad S_{-2} & : a'', b'', c'' \\
\text{"} \quad S_{-1} & : d', a', b', c' \\
\text{"} \quad S_{0} & : a, b, c, a_0, b_0, c_0 \\
\text{"} \quad S_{1} & : d_1, a_1, b_1, c_1 \\
\text{"} \quad S_{2} & : a_2, b_2, c_2 \\
\text{"} \quad S_{3} & : a_3, b_3, c_3 \\
\text{"} \quad S_{4} & : d_4
\end{array}\right\} \quad (37)$$

x)

und für welche die folgenden Gesetze gelten:

IX. Sind S_{n-1}, S_n zwei auf einander folgende Stufen, so entspricht jedem Modul m der Stufe S_{n-1} mindestens ein Modul n der Stufe S_n, welcher ~~die Bedingung m < n genügt~~ ein nächstes Vielfaches von m ist, und jedem Modul n der Stufe S_n entspricht mindestens ein Modul m der Stufe S_{n-1}, welcher ~~die derselben Bedingung m < n genügt~~ ein nächster Theiler von n ist.

X. Sind S_{n-1}, S_n, S_{n+1} drei auf einander folgende Stufen, und entsprechen einem Modul m der Stufe S_{n-1} zwei verschiedene Moduln n, p der Stufe S_n, welche ~~die Bedingungen m < n, m < p~~ nächste Vielfache von m sind, ~~genügen~~, so ist $\boxed{m = n + p}$, und es giebt in der Stufe S_{n+1} einen und nur einen Modul q, welcher ~~die Bedingungen n < q, p < q genügt~~ ein nächstes Vielfaches von n und von p ist. Umgekehrt: entsprechen einem Modul q der Stufe S_{n+1} zwei verschiedene Moduln n, p der Stufe S_n, welche ~~die Bedingungen n < q, p < q genügen~~ nächste Theiler von q sind, so ist $\boxed{n - p = q}$, und es giebt in der Stufe S_{n-1} einen und nur einen Modul m, welcher ~~die Bedingungen m < n, m < p genügt~~ ein nächster Theiler von n und von p ist.

Zu dem letzten Satze liefert unsere Gruppe D acht wesentlich verschiedene Beispiele, aus denen die übrigen durch Vertauschungen von a, b, c hervorgehen; sie sind in der folgenden Tabelle zusammengestellt:

n	m	n	p	q	~~39~~ 38	~~41~~ 39
−3	d''''	a'''	b''	c''	19	26
−2	a'''	b''	c''	d'	20	25
−1	a''	d'	a'	a_0	21	24
0	d'	a_0	b_0	d_1	22	22
0	a'	a	a_0	a_1	23	23
1	a_0	d_1	a_1	a_2	24	21
2	d_1	a_2	b_2	c_3	25	20
3	a_2	b_3	c_3	d_4	26	19

S_m

~~m < n, n < p (38)~~

$\boxed{m = n + p \qquad (38)}$

~~n < q, p < q (40)~~

~~(40)~~

$\boxed{n - p = q \qquad (39)}$

~~(38)~~

§. 4. Idealgruppen.

In §. 2 ist gezeigt, ~~Oben ist gezeigt~~, daß die 28 Moduln, aus denen unsere Dualgruppe besteht, im Allgemeinen von einander verschieden sind; wir wollen ~~aber~~ jetzt ~~noch~~ 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 a, b, c und folglich auch die übrigen Moduln der Gruppe Ideale (oder auch Idealbrüche) eines endlichen Körpers Ω sind, weil dann sehr einfache Beziehungen zwischen den beiden durch $\pm$ 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 d'''' und sechs vollständig bestimmte Ideale $p', q', r', p_1, q_1, r_1$ ausdrücken:

$$\left.\begin{array}{l}
a = q'r'p_1 d'''', \quad b = r'p'q_1 d'''', \quad c = p'q'r_1 d'''' \\
a''' = p'd'''', \quad b''' = q'd'''', \quad c''' = r'd'''' \\
a'' = a' = q'r'd'''', \quad b'' = b' = r'p'd'''', \quad c'' = c' = p'q'd'''' \\
d' = a_0 = b_0 = c_0 = d_1 = p'q'r'd'''' \\
a_1 = a_2 = p_1 d_1, \quad b_1 = b_2 = q_1 d_1, \quad c_1 = c_2 = r_1 d_1 \\
a_3 = q_1 r_1 d_1, \quad b_3 = r_1 p_1 d_1, \quad c_3 = p_1 q_1 d_1 \\
d_4 = p_1 q_1 r_1 d_1;
\end{array}\right\} \quad (37)$$

jedes der drei Paare von Producten

$q'r_1$ und $r'q_1$, $r'p_1$ und $p'r_1$, $p'q_1$ und $q'p_1$

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

$$\left.\begin{array}{l}
a' = N(p'), \quad b' = N(q'), \quad c' = N(r') \\
a_1 = N(p_1), \quad b_1 = N(q_1), \quad c_1 = N(r_1) \\
\qquad \partial = 1
\end{array}\right\} \quad (38)$$

über. Wir wollen die drei in diesem Falle auftretenden Specialgesetze $a'' = a'$, $a_2 = a_1$, $d' = d_1$, d. h. die Gesetze

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

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

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

noch etwas näher betrachten und beweisen, daß, wenn in irgend einer Dualgruppe $\mathfrak{J}$ 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 $m > d$ aus (39') oder (39'') oder (40), wenn man a, b, c resp. durch m, d, g oder d, m, g oder g, m, d ersetzt; mithin gelten auch alle Sätze (19) bis (26). Nimmt man nun an, es gelte das erste Specialgesetz $a'' = a'$, also auch $b'' = b'$, so folgt daraus das zweite $a_2 = a_1$ und das dritte $d_1 = d'$, weil zufolge (21), (23), (22), (25) $a_2 = a - b'$, $a_1 = a - b''$, $d_1 = a' - b'$, $d' = a'' - b''$ ist. Ebenso folgt umgekehrt das erste Gesetz aus dem zweiten, weil $a'' = a + b_1$, $a' = a + b_2$, und aus dem dritten, weil $a'' = a + d'$, $a' = a + d_1$ 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 obigen Beispiele der zweigliedrigen Moduln erhellt, durchaus nicht jede Gruppe $\mathfrak{M}$ vom Modultypus auch den Idealtypus besitzt. —

§. 5. Der Kettensatz in der Gruppe D.

Die nun folgenden Betrachtungen sind dazu bestimmt, das Wesen des Modulgesetzes VIII noch tiefer zu ergründen und dessen Folgen für alle Dualgruppen M vom Modultypus zu entwickeln, durch welche diese sich unter den allgemeinen Dualgruppen G auszeichnen.* Hierzu führen wir die folgenden, für jede Dualgruppe G gültigen Benennungen ein.
Ein Element d soll ein nächster Theiler des Elementes m heißen, wenn erstens ~~d~~] in G
zweitens d verschieden von m, also ein echter Theiler von m ist, und wenn es drittens in dieser Gruppe G außer d, m kein Element giebt, das ein Theiler von m und zugleich ein Vielfaches von d ist; zugleich soll m ein nächstes Vielfaches von d in G heißen. d < m,
Nach dieser Erklärung ist es also, wie wir hervorheben müssen, sehr wohl möglich, daß ein Element d, welches in G ein nächster Theiler des Elementes m ist, in einer größeren Dualgruppe H, welche außer den Elementen von G noch andere Elemente enthält, zwar immer ein echter, aber doch kein nächster Theiler von m ist; so lange es sich aber nur um die Elemente einer einzigen bestimmten Gruppe G handelt, wollen wir unbedenklich den Zusatz „in G" fortlassen. [Nehmen wir als Beispiel die aus drei beliebigen Moduln a, b, c erzeugte Gruppe] 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 d, m finden, von denen der eine d ein nächster Theiler des anderen m in] ist. Die vier Moduln d'''', d', d_1, d_4 bilden für sich eine Dualgruppe E, und jeder von ihnen ist in], aber nicht in D ein nächster Theiler des folgenden. Ebenso bilden die vier Moduln b, c, a''', a_3 für sich eine Gruppe A, und b, c sind in A, aber nicht in D, nächste Vielfache von a''' und nächste Theiler von a_3.

[Absatz

] D

] D

] E

Unter einer Kette der Dualgruppe G wollen wir eine endliche Folge von Elementen in G verstehen, deren jedes ein nächster Theiler des nächstfolgenden Elementes ist; diese Elemente sollen die Glieder der Kette, ~~[illegible] verminderte Anzahl dieser Glieder~~ 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. [~~Offenbar bilden alle Glieder einer Kette wieder eine Dualgruppe~~.

[mindestens zwei

[Wenn zwei Ketten denselben Anfang und dasselbe Ende haben, so mögen sie äquivalent heißen, und wenn alle Glieder einer Kette H auch Glieder einer Kette K sind, so nennen wir H eine Theilkette von 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 ~~[illegible]~~ äquivalente Ketten

$d'''' \quad b''' \quad a'' \quad a' \quad a$

$d'''' \quad c''' \quad a'' \quad a' \quad a$

welche vom Anfang d'''' zum Ende a führen, während acht äquivalente ~~verschiedene~~ Ketten

$d'''' \quad b''' \quad a'' \quad a' \quad a_0$

$d'''' \quad c''' \quad a'' \quad a' \quad a_0$

$d'''' \quad b''' \quad a'' \quad d' \quad a_0$

$d'''' \quad c''' \quad a'' \quad d' \quad a_0$

$d'''' \quad c''' \quad b'' \quad d' \quad a_0$

$d'''' \quad a''' \quad b'' \quad d' \quad a_0$

$d'''' \quad a''' \quad c'' \quad d' \quad a_0$

$d'''' \quad b''' \quad c'' \quad d' \quad a_0$

den Anfang d'''' und das Ende a_0 haben. Man überzeugt sich ferner leicht, daß jede von d'''' nach d_4 führende Kette eins und nur eins der sechs Moduln a, b, c, a_0, b_0, c_0 als Glied enthalten muß, und aus der Symmetrie der Gruppe ~~[illegible]~~ [$\mathfrak{D}$ folgt, daß die Anzahl aller dieser ~~[illegible]~~ äquivalenten ~~verschiedenen~~ Ketten $= 3.2^2 + 3.8^2 = 204$ ist; ~~[illegible]~~ in diesen Ketten sind alle anderen als Theilketten enthalten. [Absatz [Die wichtigste

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

$$\left.\begin{array}{lll}
S_{-4} & \text{aus} & d'''' \\
S_{-3} & " & a''', b''', c''' \\
S_{-2} & " & a'', b'', c'' \\
S_{-1} & " & d', a', b', c' \\
S_{0} & " & a, b, c, a_0, b_0, c_0 \\
S_{1} & " & d_1, a_1, b_1, c_1 \\
S_{2} & " & a_2, b_2, c_2 \\
S_{3} & " & a_3, b_3, c_3 \\
S_{4} & " & d_4.
\end{array}\right\} \quad (41)$$

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. Dualität der Modul- und Kettengesetze.

Durch die Wahl der Bezeichnung in ~~Ketten~~ der Gruppe D von 28 Moduln erscheint das eben besprochene Kettengesetz so selbstverständlich, daß man versucht sein könnte zu glauben, es müsse in jeder Dualgruppe ~~[illegible]~~

herrschen. Um dieser Meinung sogleich entgegenzutreten, stellen wir folgenden Satz auf.

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

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

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

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

$$b_3 = a - c \;,\; c''' = a + b$$
$$b''' = a + c \;,\; c_3 = a - b$$
$$b_1 = b - (a + c) \;,\; c' = c + (a - b)$$

definiren. Zunächst ergeben sich die folgenden 11 ursprünglichen Theilbarkeiten

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

deren letzte mit dem Satze III (in §. 1) übereinstimmt, wenn dort die Elemente y, d, m resp. durch a, b, c ersetzt werden; die übrigen folgen mit Rücksicht auf $b < c$ unmittelbar aus den Definitionen. Es giebt nur sechs Paare von Elementen, welche keine Theilbarkeit darbieten; die beiden Paare a, c und a, b erzeugen durch die Operationen $\pm$ die oben definirten Elemente b_3, b''', c''', c_3; für die übrigen vier Paare ergiebt sich aus den Definitionen

$$b + b''' = c''' \;,\; c - c_3 = b_3$$
$$b - b''' = b_1 \;,\; c + c_3 = c'$$
$$a + c' = b''' \;,\; a - b_1 = c_3 \qquad (42)$$
$$a + b_1 = b''' \;,\; a - c' = c_3 \qquad (43)$$

und zwar folgen die ~~[illegible]~~ Sätze (43) aus ~~[illegible]~~ (42) mit Rücksicht auf $b_1 < c'$, $b''' < b_1$, $c_3 > c'$.
~~[illegible]~~

Hiermit ist bewiesen, daß unsere neun Elemente

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

wirklich eine in G enthaltene Dualgruppe G' bilden, und wir wollen ihre Constitution, weil sie für manche Untersuchungen wichtig ist, in der folgenden Tabelle darstellen.

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

Das Durchschnittsfeld der Zeile m und der Spalte n enthält das Element $m+n$ oder $m-n$, je nachdem dieses Feld der rechten oberen oder der linken unteren Hälfte der Tabelle angehört; die Diagonalfelder, ~~die~~ welche den Fällen $m = n = m \pm n$ entsprechen, sind zur Erleichterung des Überblicks leer gelassen. ~~denn da eine Zeile m sich mit der Spalte m kreuzt, sollten eigentlich durch die entsprechenden Elemente m = m ± m ausgefüllt werden, sie sind aber leer gelassen, um die Trennung der beiden Hälften der Tabelle für das Auge deutlicher zu machen~~.

Wenn in der Dualgruppe G das Modulgesetz ~~VIII~~ herrscht, so ist $b_1 = c'$, und die durch a, b, c erzeugte Dualgruppe G' besteht also aus höchstens ~~[illegible]~~ acht Elementen. Dasselbe ergibt sich aus der Constitution der oben betrachteten ~~[illegible]~~gruppe von 28 Moduln; denn aus der jetzigen Annahme $\mathfrak{b} < \mathfrak{c}$ folgen leicht die 20 Identitäten

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

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

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

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

Wenn aber, wie wir ~~jetzt~~ [im Folgenden] annehmen wollen, in der Dualgruppe $\mathfrak{H}$ das Modulgesetz VIII nicht allgemein gilt, so dürfen wir voraussetzen, die obigen drei Elemente $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ seien mit Berücksichtigung der Bedingung $\mathfrak{b} < \mathfrak{c}$ aus $\mathfrak{H}$ so ausgewählt, daß $\mathfrak{b}_1$ verschieden von $\mathfrak{c}'$, also $\mathfrak{b}_1$ ein echter 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,x) gewiß von einander verschieden sind; hierbei stützen wir uns auf die Identitäten (42), (43) und auf die schon vorher aufgestellten Theilbarkeiten

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

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

und behaupten zunächst, daß

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

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 ~~folgt~~ ergiebt sich weiter, daß in (44) und (45) nur echte Theilbarkeiten auftreten; ~~Wäre~~ 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 Gruppe $\mathfrak{G}$ 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)

x) ~~Diese Gruppe ist identisch mit derjenigen, welche~~

[ersetzt durch Beiblatt