Werk

Titel: Gesammelte mathematische Werke 2*
Jahr: 1931
Kollektion: Mathematica
Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen
Werk Id: PPN235693928
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN235693928
OPAC: http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=235693928

Übergeordnetes Werk

Werk Id: PPN235685380
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN235685380
OPAC: http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=235685380

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

Richard Dedekind

Gesammelte mathematische Werke

Herausgegeben von

Robert Fricke †
in Braunschweig

Emmy Noether
in Göttingen

Öystein Ore
in New Haven

Zweiter Band

Druck und Verlag von Friedr. Vieweg & Sohn Akt.-Ges.
Braunschweig 1931

Printed in Germany

Inhaltsverzeichnis.

XX.

Zur Theorie der aus n Haupteinheiten gebildeten komplexen Größen.

[Nachrichten von der Königlichen Gesellschaft der Wissenschaften zu Göttingen, Jahrgang 1885, S. 141—159.]

Der unter der gleichen Überschrift in Nr. 10 des Jahrgangs 1884 dieser Nachrichten veröffentlichte Brief des Herrn Weierstrass an Herrn Schwarz behandelt einen Gegenstand, mit welchem ich mich ebenfalls vorübergehend beschäftigt habe. Die Untersuchung derjenigen Zahlgebiete, die ich Körper nenne, gab mir hierzu die unmittelbare Veranlassung, weil die analytische Behandlung, welche die Theorie der endlichen Körper verlangt, sich fast wörtlich auf die Theorie der aus n Haupteinheiten gebildeten überkomplexen Größen anwenden läßt; man braucht nur den Körper der rationalen Zahlen, auf welchen bei jener Untersuchung die Koordinaten beschränkt waren, zu ersetzen durch den Körper aller reellen oder lieber durch den Körper aller komplexen Zahlen, unter welchem Namen ich im Folgenden immer die gewöhnlichen, jetzt allgemein eingeführten komplexen Zahlen verstehe. Die betreffenden analytischen Untersuchungen sind im § 159 der zweiten, im Jahre 1871 erschienenen Auflage der Dirichletschen Vorlesungen über Zahlentheorie veröffentlicht; in die dritte Auflage sind sie nicht wieder aufgenommen, weil sie für die Theorie der algebraischen Zahlen entbehrlich sind, und weil ich diese Theorie mit den geringsten Hilfsmitteln zu begründen wünschte. Bei der genannten Übertragung ergab sich nun, daß wahrhaft neue Zahlindividuen auf diesem Wege nicht zu gewinnen sind; in der Tat, jedes System von n Haupteinheiten $e_1, e_2 \ldots e_n$ kann immer aufgefaßt werden als ein System von n gewöhnlichen komplexen Zahlen oder vielmehr als Kollektivrepräsentant von n solchen Systemen; derartige mehrwertige Größensysteme sind aber in unserer höheren Algebra längst eingebürgert. Mit diesem Resultat begnügte ich mich, weil ich in ihm die Bedeutung und die volle Bestätigung

der bekannten Bemerkung von Gauß gefunden zu haben glaubte. Da nun diese Auffassung der Haupteinheiten in dem Briefe des Herrn Weierstrass*) zwar gestreift, aber doch nicht so, wie sie es mir zu verdienen scheint, als der eigentliche Kern der ganzen Frage deutlich hervorgehoben ist, da ferner z. B. die Erscheinung, daß ein Produkt von zwei nicht verschwindenden überkomplexen Größen verschwinden kann, bei dieser Auffassung wohl ihre natürlichste Erklärung findet, so erlaube ich mir, im folgenden eine Darstellung derselben mitzuteilen, wobei sich zugleich eine kleine Vereinfachung der von Herrn Weierstrass aufgestellten Zulässigkeitsbedingungen ergeben wird.

Ich mache zunächst darauf aufmerksam, daß alle Beziehungen zwischen den überkomplexen Größen, soweit es sich nicht bloß um Addition oder Subtraktion handelt, vollständig bestimmt werden durch die von Herrn Weierstrass mit $\varepsilon_{t,r,s}$, von mir im folgenden mit $\eta_{t,rs}$ bezeichneten Koeffizienten, welche in der Gleichung (5) seiner Abhandlung als Koordinaten des Produktes

$$e_r e_s = \sum e_\iota \eta_{\iota,rs}$$

auftreten. (Ich bezeichne in der Folge mit ι, ι', $\iota''\ldots$ stets Summationsbuchstaben, welche die n Werte $1, 2 \ldots n$ durchlaufen sollen, und ein einfaches Summenzeichen Σ bezieht sich immer auf alle, hinter demselben auftretenden ι, ι', $\iota''\ldots$, während $r, s\ldots$ konstante Indizes aus derselben Reihe bedeuten.) Da das System der Haupteinheiten von vornherein als irreduktibel vorausgesetzt wird, oder mit anderen Worten, da jede überkomplexe Zahl

$$x = \sum e_\iota \xi_\iota$$

nur ein einziges, völlig bestimmtes System von n Koordinaten ξ_ι besitzt, so ergibt sich, wie Herr Weierstrass erwähnt, aus den Forderungen

$$e_r e_s = e_s e_r, \quad (e_r e_s) e_t = (e_r e_t) e_s$$

eine Anzahl von Bedingungen, denen die Zahlen $\eta_{t,rs}$ genügen müssen. Dieselben lauten offenbar folgendermaßen

(1) $$\eta_{t,rs} = \eta_{t,sr}$$

(2) $$\sum \eta_{u,t\iota} \eta_{\iota,rs} = \sum \eta_{u,s\iota} \eta_{\iota,rt},$$

*) S. 410—411. Der daselbst ausgesprochenen, auf die Meinung von Gauß bezüglichen Vermutung kann ich mich nicht anschließen.

wo r, s, t, u irgendwelche Indizes aus der Reihe $1, 2 \ldots n$ bedeuten. Diese Bedingungen, zu welchen Herr Weierstrass im Verlaufe seiner Untersuchung noch einige, später zu erwähnende hinzufügt, stimmen, wie es in der Natur der Sache liegt, vollständig mit denjenigen überein, welche in der Theorie der endlichen Körper bei der Forderung auftreten, daß die Zahlen sich durch Multiplikation reproduzieren sollen.

Ich will nun im ersten Teil meiner Darstellung einen Weg angeben, auf welchem man nach Belieben unendlich viele solche Systeme von Zahlen $\eta_{t,rs}$ erzeugen kann, und im zweiten Teil beweisen, daß umgekehrt auf diese Weise auch alle solche Systeme erzeugt werden. Hierbei bemerke ich, daß von jetzt ab ausschließlich von den bis jetzt allgemein eingeführten komplexen Zahlen die Rede sein wird.

Es sei ein System E von n^2 Zahlen $e_r^{(s)}$ nach Belieben angenommen, welche nur der einzigen Bedingung unterworfen sind, daß ihre Determinante

$$e = \sum \pm e_1' e_2'' \ldots e_n^{(n)} \tag{3}$$

von Null verschieden ist. Ich betrachte nun ein System von n Größen

$$e_1, e_2 \ldots e_n, \tag{4}$$

welches insofern als mehrwertig anzusehen ist, als es fähig sein soll, durch n verschiedene Substitutionen in die n bestimmten Spezialsysteme

$$e_1^{(s)}, e_2^{(s)} \ldots e_n^{(s)} \tag{5}$$

überzugehen, welche den n verschiedenen Werten des Index s entsprechen; diese Substitutionen sind natürlich so zu verstehen, daß gleichzeitig jede der n Größen e_r den mit gleichem Index r behafteten Wert $e_r^{(s)}$ annimmt. Andere Spezialisierungen der Größen e_r sollen gänzlich ausgeschlossen sein. Wir stellen uns die Aufgabe, alle rationalen Beziehungen zwischen diesen mehrwertigen Größen e_r und den völlig bestimmten, einwertigen Zahlen aufzufinden, nämlich alle solche Beziehungen, welche für jedes einzelne der n Spezialsysteme (5) gültig sind; nur von diesen Beziehungen wird im folgenden gesprochen werden.

Zu diesem Zweck betrachten wir das Gebiet G aller mit bestimmten Zahlkoeffizienten behafteten ganzen rationalen Funktionen der n Größen e_r. Jede solche Funktion x wird durch die Substitution (5) einen entsprechenden Wert annehmen, den wir mit $x^{(s)}$

bezeichnen wollen. Sind diese n Werte x', $x''\ldots x^{(n)}$ bekannt oder auch willkürlich angenommen, so läßt sich die mehrwertige Größe x immer und nur auf eine einzige Weise als homogene lineare Funktion der Größen e_r, also in der Form

$$x = \sum e_\iota \xi_\iota \tag{6}$$

darstellen, wo die n Zahlen ξ_ι einwertig bestimmt sind; sie sollen die Koordinaten der Größe x in bezug auf die Basis (4) heißen. In der Tat. die vorstehende Gleichung soll nach dem Obigen nichts anderes bedeuten, als daß die den n verschiedenen Indizes s entsprechenden n Gleichungen

$$x^{(s)} = \sum e_\iota^{(s)} \xi_\iota \tag{7}$$

bestehen; da nun die Determinante (3) von Null verschieden ist, so ergeben sich hieraus durch Umkehrung für die n Koordinaten Ausdrücke von der Form

$$\xi_r = \sum f_r^{(\iota)} x^{(\iota)}; \tag{8}$$

das System F der hier auftretenden n^2 Zahlen $f_r^{(s)}$ ist das Komplement des gegebenen Systems E. Wir setzen im folgenden stets

$$(r, s) = 1 \text{ oder } = 0, \tag{9}$$

je nachdem die Indizes r, s gleich oder ungleich sind; dann bestehen zwischen den beiden komplementären Systemen E, F bekanntlich die Relationen

$$\sum e_r^{(\iota)} f_s^{(\iota)} = \sum e_\iota^{(r)} f_\iota^{(s)} = (r, s). \tag{10}$$

In der eben bewiesenen völligen Bestimmtheit der zu einer Größe x gehörenden Koordinaten ξ_r liegt auch die Irreduktibilität der Basis (4), insofern die Gleichung

$$\sum e_\iota \xi_\iota = 0$$

durch n bestimmte Zahlen ξ_ι nicht anders befriedigt werden kann, als wenn diese sämtlich verschwinden. Jedes einzelne Spezialsystem (5), für sich allein betrachtet, besitzt natürlich, sobald $n > 1$ ist, diese Irreduktibilität niemals *).

*) Der Fall $e = 0$, und allgemeiner die Untersuchung solcher mehrwertiger Systeme $e_1, e_2 \ldots e_n$, für welche die Anzahl der erlaubten Substitutionen (5) kleiner oder größer als n ist, läßt sich leicht auf den hier behandelten Fall zurückführen.

Nach dem Vorhergehenden ist es nun auch erlaubt, die n Zahlen $f_r', f_r'' \dots f_r^{(n)}$ als die Spezialwerte einer demselben Gebiet G angehörenden Größe f_r anzusehen, und man erhält so eine zu der Basis (4) komplementäre, ebenfalls n-wertige Basis

$$f_1, f_2 \dots f_n. \tag{11}$$

Bezeichnen wir ferner mit dem Symbol $S(x)$ die aus allen Spezialwerten von x gebildete Summe

$$S(x) = \sum x^{(\iota)}, \tag{12}$$

so kann die Beziehung (10) zwischen den beiden Basen auch durch

$$S(e_r f_s) = (r, s) \tag{13}$$

dargestellt werden, und da die Koordinaten ξ_r der Größe x zufolge (8) die Form

$$\xi_r = S(x f_r) \tag{14}$$

besitzen, so ist allgemein

$$x = \sum e_\iota S(x f_\iota). \tag{15}$$

Man erhält endlich, wenn man nach den Spezialwerten $x^{(s)}$ ordnet und die n Größen

$$c_r = \sum e_\iota f_\iota^{(r)} \tag{16}$$

einführt, die folgende Darstellung

$$x = \sum c_\iota x^{(\iota)}. \tag{17}$$

Die demselben Gebiete G angehörenden n Größen c_r bilden gewissermaßen eine Normalbasis desselben und sind durch

$$c_r^{(s)} = (r, s) \tag{18}$$

definiert. Die einzelnen n Bestandteile $c_s x^{(s)}$, welche den einzelnen Substitutionen entsprechen, kann man mit Herrn Weierstrass die Komponenten der Größe x nennen. Versteht man ferner unter einem Teiler der Null jede Größe x, von deren Spezialwerten $x^{(s)}$ mindestens einer verschwindet, so sind, falls $n > 1$ ist, die Größen c_r solche Teiler der Null.

Da nach dem Obigen alle Größen x des Gebietes G, d. h. alle ganzen rationalen Funktionen der n Größen e_r sich als homogene lineare Funktionen derselben darstellen lassen, so kann man jedes Produkt

$$e_r e_s = \sum e_\iota \eta_{\iota, rs} \tag{19}$$

setzen, wo die Koordinaten $\eta_{t,rs}$ notwendig den sämtlichen Bedingungen (1) und (2) genügen müssen, welche aus den Gleichungen $e_r e_s = e_s e_r$ und $(e_r e_s) e_t = (e_r e_t) e_s$ entspringen. In der Tat ergibt sich aus dem obigen allgemeinen Ausdruck (14) für die Koordinaten einer Größe x, daß

$$\eta_{t,rs} = S(e_r e_s f_t) \tag{20}$$

ist, und aus dieser Darstellung der Zahlen $\eta_{t,rs}$ durch das gegebene System E der Zahlen $e_r^{(s)}$ folgt sofort, daß alle jene Bedingungen identisch erfüllt sind, weil die Summe

$$\begin{aligned} &\sum \eta_{u,t\iota}\, \eta_{\iota,rs} = \sum e_t^{(\iota')} e_\iota^{(\iota')} f_u^{(\iota')} e_r^{(\iota'')} e_s^{(\iota'')} f_\iota^{(\iota'')} \\ &= \sum e_t^{(\iota')} f_u^{(\iota')} e_r^{(\iota'')} e_s^{(\iota'')} (\iota', \iota'') = \sum e_r^{(\iota')} e_s^{(\iota')} e_t^{(\iota')} f_u^{(\iota')} \\ &= S(e_r e_s e_t f_u), \end{aligned} \tag{21}$$

also symmetrisch in bezug auf die drei Indizes r, s, t ist.

Am einfachsten gestaltet sich natürlich die Multiplikation, wenn man alle Größen x des Gebietes G in der Form (17) durch die Normalbasis darstellt. Die Größen c_r haben nämlich, wie aus ihrer Definition (16) oder auch unmittelbar aus (18) hervorgeht, die Eigenschaften

$$c_r c_s = (r, s)\, c_r, \tag{22}$$

und hieraus folgt, wenn y ebenfalls eine beliebige Größe des Gebietes G bedeutet,

$$x\, y = \sum c_\iota\, x^{(\iota)}\, y^{(\iota)}, \tag{23}$$

was ohnehin wegen

$$(x\, y)^{(s)} = x^{(s)}\, y^{(s)} \tag{24}$$

selbstverständlich ist. Ebenso leuchtet ein, daß, falls $n > 1$, ein Produkt $x\, y$ von zwei von Null verschiedenen Größen x, y sehr wohl verschwinden kann; in der Tat bedeutet die Gleichung $x\, y = 0$ nichts anderes, als das gleichzeitige Bestehen der den n Substitutionen entsprechenden Gleichungen $x^{(s)} y^{(s)} = 0$, und diesen kann immer so genügt werden, daß einige Spezialwerte von jeder der Größen x, y verschwinden, aber mindestens einer derselben von Null verschieden ist. Ist x eine gegebene Größe, so ist die Mannigfaltigkeit der Wurzeln y der Gleichung $x\, y = 0$ hiernach sofort zu überblicken. Auf die Folgerungen, welche sich hieraus für die Division der Größen des Gebietes G und hinsichtlich der Mannigfaltigkeit der Wurzeln

von Gleichungen höheren Grades ergeben, will ich hier nicht mehr eingehen, weil sie von Herrn Weierstrass ausführlich besprochen sind. —

Ich gehe nun im zweiten Teil zu meiner Hauptaufgabe über, welche darin besteht, zu zeigen, daß umgekehrt jedes gegebene System von Zahlen $\eta_{t,rs}$, welches die Bedingungen (1) und (2) und eine sogleich aufzustellende Zusatzbedingung erfüllt, immer auf die im vorhergehenden beschriebene Weise (20) aus einem und nur einem System E von n^2 Zahlen $e_r^{(s)}$ mit nicht verschwindender Determinante e entspringt. Die erwähnte Zusatzbedingung besteht darin, daß, wenn man zur Abkürzung

(25) $$\sigma_r = \sum \eta_{\iota,r\iota}$$

und

(26) $$\tau_{rs} = \tau_{sr} = \sum \sigma_\iota \eta_{\iota,rs}$$

setzt, die Determinante

(27) $$\Delta = \sum \pm \tau_{11}\tau_{22}\dots\tau_{nn}$$

einen von Null verschiedenen Wert besitzt; es wird sich später, ohne daß ich besonders darauf zurückzukommen brauche, von selbst ergeben, daß diese einzige Bedingung vollständig äquivalent mit den drei Forderungen ist, auf welche Herr Weierstrass durch seine Untersuchung über die Zulässigkeit der überkomplexen Größen geführt wird (S. 403). Ihre Bedeutung für unsere Aufgabe ist leicht zu erkennen; ist nämlich das System der Zahlen $\eta_{t,rs}$ in der oben angegebenen Weise (20) wirklich aus einem System E entsprungen, so ist

(28) $$\sigma_r = \sum S(e_r e_\iota f_\iota) = \sum e_r^{(\iota')} e_\iota^{(\iota')} f_\iota^{(\iota')} = S(e_r)$$

und

(29) $$\tau_{rs} = \sum S(e_\iota)\, S(e_r e_s f_\iota) = \sum e_\iota^{(\iota')} e_r^{(\iota'')} e_s^{(\iota'')} f_\iota^{(\iota'')} = S(e_r e_s)$$

und folglich

(30) $$\Delta = e^2,$$

woraus die Notwendigkeit unserer Bedingung unmittelbar einleuchtet. Des leichteren Verständnisses wegen empfehle ich dem Leser, auch im folgenden immer die Bedeutung anzumerken, welche die einzuführenden Größen besitzen würden, falls die Abstammung der Zahlen $\eta_{t,rs}$ aus einem System E schon bewiesen wäre.

Die Bedingungen (1) und (2) lassen sich am einfachsten und mit dem besten Erfolge zusammenfassen, wenn man n unabhängige

Variable $\xi_1, \xi_2 \dots \xi_n$ und n homogene ganze Funktionen zweiten Grades $\eta_1, \eta_2 \dots \eta_n$ durch die Definition

$$2\eta_t = \sum \eta_{t,\iota\iota'} \xi_\iota \xi_{\iota'} \tag{31}$$

einführt. Die Bedingungen (1) sind dann durch

$$\eta_{t,rs} = \frac{\partial^2 \eta_t}{\partial \xi_r \partial \xi_s} \tag{32}$$

ausgedrückt. Setzt man ferner

$$\eta_{r,s} = \frac{\partial \eta_r}{\partial \xi_s} = \sum \eta_{r,s\iota} \xi_\iota, \tag{33}$$

so ist

$$2\eta_r = \sum \eta_{r,\iota} \xi_\iota \tag{34}$$

und, wenn d das Zeichen für eine Variation (d. h. eine totale Differentiation) bedeutet,

$$d\eta_r = \sum \eta_{r,\iota} d\xi_\iota = \sum \xi_\iota d\eta_{r,\iota}. \tag{35}$$

Die Bedingungen (2) werden ferner, wenn d' ebenfalls eine willkürliche Variation ist, zusammengefaßt in

$$\sum d\eta_{r,\iota} d'\eta_{\iota,s} = \sum d'\eta_{r,\iota} d\eta_{\iota,s}. \tag{36}$$

Alles Folgende beruht auf diesen Bedingungen und der freiesten Ausnutzung des Begriffes einer Variation. Man kann diesen Bedingungen noch verschiedene andere Formen geben, in denen sie ebenfalls zur Anwendung kommen werden. Multipliziert man mit ξ_s und summiert nach s, so folgt nach (35)

$$\sum d\eta_{r,\iota} d'\eta_\iota = \sum d'\eta_{r,\iota} d\eta_\iota. \tag{37}$$

Setzt man ferner $d'\xi_\iota = \xi_\iota$, so folgt aus (36)

$$\sum \eta_{\iota,s} d\eta_{r,\iota} = \sum \eta_{r,\iota} d\eta_{\iota,s}. \tag{38}$$

Wir führen noch folgende Funktionen ein, die lineare

$$\sigma = \sum \eta_{\iota,\iota} = \sum \sigma_\iota \xi_\iota, \tag{39}$$

die quadratische

$$2\tau = 2\sum \sigma_\iota \eta_\iota = \sum \tau_{\iota\iota'} \xi_\iota \xi_{\iota'}, \tag{40}$$

die linearen

$$\tau_r = \frac{\partial \tau}{\partial \xi_r} = \sum \sigma_\iota \eta_{\iota,r} = \sum \tau_{r\iota} \xi_\iota \tag{41}$$

und beginnen nun unsere Untersuchung.

Da die aus den Zahlen τ_{rs} gebildete Determinante (27) nach unserer Annahme nicht verschwindet, so kann man eine spezielle

Variation δ vollständig definieren durch die für alle n Indizes r geltende Forderung

$$\delta\tau_r = \sigma_r, \tag{42}$$

und zwar sind die hieraus folgenden Werte der Differentiale $\delta\xi_1$, $\delta\xi_2 \ldots \delta\xi_n$ bestimmte konstante Zahlen. Multipliziert man nun (36) mit σ_r und summiert nach r, so folgt mit Rücksicht auf (41)

$$\sum d\tau_\iota\, d'\eta_{\iota,s} = \sum d'\tau_\iota\, d\eta_{\iota,s}, \tag{43}$$

und wenn man hierin $d' = \delta$ setzt und (42) beachtet,

$$\sum d\tau_\iota \delta\eta_{\iota,s} = \sum \sigma_\iota d\eta_{\iota,s} = d\tau_s;$$

da nun, weil Δ nicht verschwindet, die n Differentiale $d\tau_1, d\tau_2 \ldots d\tau_n$ gänzlich unabhängig voneinander sind, so folgt hieraus offenbar

$$\delta\eta_{r,s} = (r,s), \quad \delta\eta_r = \xi_r, \quad \delta\tau = \sigma. \tag{44}$$

Hieraus ergibt sich die wichtige Folgerung, daß die Funktionaldeterminante

$$\varphi = \frac{d(\eta_1 \ldots \eta_n)}{d(\xi_1 \ldots \xi_n)} = \sum \pm \eta_{1,1}\, \eta_{2,2} \cdots \eta_{n,n} \tag{45}$$

nicht identisch verschwinden kann; legt man nämlich jeder Variablen ξ_r den entsprechenden Wert $\delta\xi_r$ bei, so geht $\eta_{r,s}$ in $\delta\eta_{r,s} = (r,s)$ über, und folglich nimmt die homogene ganze Funktion n-ten Grades φ den Wert

$$\frac{\delta^n \varphi}{\Pi(n)} = 1 \tag{46}$$

an (diese Determinante φ geht in die von Herrn Weierstrass auf S. 397 mit ε bezeichnete Größe über, wenn die $\xi_r = \beta_r$ gesetzt werden).

Hieraus folgt wieder, daß nicht bloß für jede positive, sondern auch für jede negative ganze Zahl p eine entsprechende Variation δ_p vollständig definiert werden kann durch die für alle n Indizes r geltende Rekursion

$$\delta_{p+1}\xi_r = \delta_p \eta_r, \tag{47}$$

mit der Anfangsbedingung $\delta_0 = \delta$. Die merkwürdigen Eigenschaften der hierdurch definierten Funktionen $\delta_p \xi_r$ (welche von Herrn Weierstrass mit $\xi_r^{(p)}$ bezeichnet sind) ergeben sich leicht aus unseren Grundbedingungen (37); setzt man $d' = \delta_p$, so erhält man zufolge (47)

$$\sum \delta_p \eta_{r,\iota}\, d\eta_\iota = \sum d\eta_{r,\iota}\, \delta_{p+1}\xi_\iota = \sum \delta_{p+1}\eta_{r,\iota}\, d\xi_\iota$$

und hieraus wegen der Willkürlichkeit von d,

$$\delta_{p+1}\eta_{r,s} = \sum \eta_{\iota,s}\delta_p\eta_{r,\iota} = \sum \eta_{r,\iota}\delta_p\eta_{\iota,s}. \tag{48}$$

Setzt man hierin $p = -1$, so folgt nach (44), daß

$$\sum \eta_{\iota,s}\delta_{-1}\eta_{r,\iota} = \sum \eta_{r,\iota}\delta_{-1}\eta_{\iota,s} = (r,s), \tag{49}$$

mithin das Produkt

$$\varphi\,\delta_{-1}\eta_{r,s} \tag{50}$$

der Koeffizient des Elementes $\eta_{s,r}$ in der Determinante φ ist.

Allgemeiner folgt aus (48) leicht durch den Schluß von q auf $q+1$, daß für je zwei ganze Zahlen p, q der Satz

$$\delta_{p+q}\eta_{r,s} = \sum \delta_p\eta_{r,\iota}\delta_q\eta_{\iota,s} \tag{51}$$

gilt, woraus man beiläufig schließt, daß

$$\begin{vmatrix} \delta_p\eta_{1,1} \dots \delta_p\eta_{1,n} \\ \dots\dots\dots\dots \\ \delta_p\eta_{n,1} \dots \delta_p\eta_{n,n} \end{vmatrix} = \varphi^p \tag{52}$$

ist, was aber auch schon aus (48) folgt.

Multipliziert man (51) mit ξ_s und summiert nach s, so folgt nach (35)

$$\delta_{p+q}\eta_r = \sum \delta_p\eta_{r,\iota}\delta_q\eta_\iota, \tag{53}$$

also zufolge (47) auch

$$\delta_{p+q}\xi_r = \sum \delta_p\eta_{r,\iota}\delta_q\xi_\iota. \tag{54}$$

Ebenso findet man aus (47) und (48) durch den Schluß von p auf $p\pm1$ die Allgemeingültigkeit des für $p = 0$ evidenten Satzes

$$d\,\delta_p\xi_r = p\sum \delta_{p-1}\eta_{r\iota}\,d\xi_\iota = p\sum d\,\eta_{r,\iota}\delta_{p-1}\xi_\iota \tag{55}$$

und hieraus die Funktionaldeterminante

$$\frac{d(\delta_p\xi_1 \dots \delta_p\xi_n)}{d(\xi_1 \dots \xi_n)} = p^n\varphi^{p-1}. \tag{56}$$

Setzt man $d = \delta_q$, so folgt aus (55), (54)

$$\delta_q\delta_p\xi_r = p\,\delta_{p+q-1}\xi_r, \tag{57}$$

also auch

$$\delta_q\delta_p\lambda = p\,\delta_{p+q-1}\lambda, \tag{58}$$

wenn λ eine willkürliche homogene lineare Funktion bedeutet. Setzt man $q = 0$, so folgt

$$\delta\,\delta_p\lambda = p\,\delta_{p-1}\lambda \tag{59}$$

und durch Wiederholung der Variation δ

$$\delta^m \delta_p \lambda = p(p-1) \dots (p-m+1)\, \delta_{p-m} \lambda, \tag{60}$$

speziell

$$\delta^m \delta_{-1} \lambda = (-1)^m \Pi(m)\, \delta_{-1-m} \lambda. \tag{61}$$

Ich wende mich jetzt zur näheren Betrachtung der Determinante φ. Zufolge der oben gefundenen Bedeutung des Produktes (50) ist nach einem bekannten Satz

$$d\varphi = \varphi \sum \delta_{-1} \eta_{\iota,\iota'}\, d\eta_{\iota',\iota} = \varphi \sum \delta_{-1} \eta_{\iota,\iota'}\, \eta_{\iota',\iota\iota''}\, d\xi_{\iota''};$$

aus den Grundbedingungen (36) folgt aber

$$\sum \delta_{-1} \eta_{r,\iota'}\, \eta_{\iota',rs} = \sum \eta_{r,r\iota'} \delta_{-1} \eta_{\iota',s},$$

und hierdurch vereinfacht sich mit Rücksicht auf (39), (41) das vorstehende Differential in folgender Weise

$$d\varphi = \varphi \sum \eta_{\iota,\iota\iota'} \delta_{-1} \eta_{\iota',\iota''} d\xi_{\iota''} = \varphi \sum \sigma_{\iota'} \delta_{-1} \eta_{\iota',\iota''} d\xi_{\iota''} = \varphi \sum \delta_{-1} \tau_{\iota''} d\xi_{\iota''}$$

oder also

$$d\varphi = \varphi \sum \delta_{-1} \tau_\iota\, d\xi_\iota = \varphi \sum d\tau_\iota\, \delta_{-1} \xi_\iota, \tag{62}$$

oder, wenn die n Differentiale $d\xi_r$ konstant sind, noch kürzer

$$d\varphi = \varphi\, \delta_{-1}\, d\tau, \tag{63}$$

wo nun $d\tau$ jede beliebige homogene lineare Funktion bedeutet, weil Δ von Null verschieden ist. Hieraus geht hervor, daß die n Funktionen $\delta_{-1} \xi_r$ sich durch die Derivierten von $\log \varphi$ ausdrücken lassen, und umgekehrt diese durch jene. Ferner ergibt sich, wenn man zur Abkürzung

$$\varphi_\mu = \frac{(-1)^\mu}{\Pi(\mu)} \delta^\mu \varphi \tag{64}$$

setzt, durch wiederholte Anwendung der Operation δ, unter Berücksichtigung von (61), der Satz

$$d\varphi_m = \sum_{\mu=0}^{\mu=m} \varphi_\mu \delta_{\mu-m-1}\, d\tau. \tag{65}$$

Bedenkt man, daß zufolge (46)

$$\varphi_n = (-1)^n, \tag{66}$$

und daß alle folgenden φ_{n+1}, $\varphi_{n+2} \dots$ verschwinden, so ergibt sich

$$\sum_{\mu=0}^{\mu=n} \varphi_\mu \delta_{\mu-m-1}\, d\tau = 0, \text{ wenn } m \geqq n,$$

und da $d\tau$, wie schon bemerkt, jede der n Variablen ξ_r bedeuten kann, so ergibt sich, wenn ψ eine willkürliche Funktion ist, immer

$$\sum_{\mu=0}^{\mu=n} \varphi_\mu \delta_{\mu-m-1}\psi = 0, \text{ wenn } m \geqq n;$$

nimmt man hierin, wenn p eine willkürliche ganze Zahl ist,

$$\psi = \delta_{p+m+2}\xi_r,$$

so folgt mit Rücksicht auf (57)

$$(p+m+2)\sum_{\mu=0}^{\mu=n} \varphi_\mu \delta_{\mu+p}\xi_r = 0, \text{ wenn } m \geqq n;$$

da nun für jede gegebene ganze Zahl p eine ganze Zahl $m \geqq n$ stets so gewählt werden kann, daß $(p+m+2)$ nicht verschwindet, so folgt, daß immer

$$\sum_{\mu=0}^{\mu=n} \varphi_\mu \delta_{\mu+p}\xi_r = 0, \tag{67}$$

also auch immer die Rekursion

$$\sum_{\mu=0}^{\mu=n} \varphi_\mu \delta_{\mu+p}\psi = 0 \tag{68}$$

gilt, wo ψ eine willkürliche Funktion.

Nehmen wir jetzt in (65) an, es sei $m < n$, so folgt mit Rücksicht auf (68)

$$d\varphi_m = -\sum_{\mu=m+1}^{\mu=n} \varphi_\mu \delta_{\mu-m-1}\, d\tau$$

oder auch

$$d\varphi_m = -\sum_{\mu=0}^{\mu=n-m-1} \varphi_{\mu+m+1}\delta_\mu\, \delta\tau.$$

Setzt man hierin $d = \delta$, und bedenkt, daß $\delta\tau = \sigma$ und $\delta\varphi_m = -(m+1)\varphi_{m+1}$ ist, so erhält man, wenn man noch m durch $m-1$ ersetzt,

$$m\varphi_m = \sum_{\mu=0}^{\mu=n-m} \varphi_{\mu+m}\delta_\mu \sigma. \tag{69}$$

Dieser Satz gilt für die Zahlen $m = 1, 2 \ldots n$ und offenbar auch für $m = 0$ zufolge (68); seine Bedeutung wird sich sogleich ergeben.

Wir führen jetzt eine Charakteristik ε ein, welche folgenden Sinn hat. Ist ψ eine beliebige Funktion der n Variablen ξ_r, so soll $\varepsilon(\psi)$ diejenige Funktion von den ξ_r und von einer neuen Variablen ξ bedeuten, welche aus ψ dadurch hervorgeht, daß jede Variable ξ_r durch die entsprechende Größe $(\xi_r - \xi\,\delta\xi_r)$ ersetzt wird. Da die $\delta\xi_r$ konstant

sind, so ist nach dem Taylorschen Satze, wenigstens für ganze Funktionen ψ,

$$\varepsilon(\psi) = \psi - \xi\frac{\delta\psi}{1} + \xi^2\frac{\delta^2\psi}{1.2} - \xi^3\frac{\delta^3\psi}{1.2.3} + \cdots \tag{70}$$

und allgemein, wenn die Differentiale $d\xi_r$ konstant sind,

$$d\,\varepsilon(\psi) = \varepsilon(d\psi) - \varepsilon(\delta\psi)\,d\xi. \tag{71}$$

Da φ eine ganze Funktion n-ten Grades ist, so ist mit Rücksicht auf (64)

$$\varepsilon(\varphi) = \varphi + \varphi_1\xi + \varphi_2\xi^2 + \cdots + \varphi_n\xi^n; \tag{72}$$

da ferner φ die Determinante der linearen Funktionen $\eta_{r,s}$, und zufolge (44)

$$\varepsilon(\eta_{r,s}) = \eta_{r,s} - (r,s)\,\xi \tag{73}$$

ist, so ergibt sich auch

$$\varepsilon(\varphi) = \begin{vmatrix} \eta_{1,1} - (1,1)\,\xi \ldots \eta_{1,n} - (1,n)\,\xi \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \eta_{n,1} - (n,1)\,\xi \ldots \eta_{n,n} - (n,n)\,\xi \end{vmatrix}. \tag{74}$$

Wir denken uns nun $\varepsilon(\varphi)$ als ganze Funktion n-ten Grades der Variablen ξ in n Faktoren ersten Grades zerlegt und setzen demgemäß, weil $\varphi_n = (-1)^n$ ist,

$$\varepsilon(\varphi) = \prod(x - \xi), \tag{75}$$

wo das Produktzeichen sich auf die n Wurzeln

$$x = x', x'' \ldots x^{(n)} \tag{76}$$

bezieht, welche Funktionen von den n Variablen ξ_r sind und nach dem Fundamentalsatze von Gauß im Körper der komplexen Zahlen stets existieren. Dann ergibt sich durch Vergleich von (68), (69), (72) mit den Newtonschen Formeln der Algebra, daß für jede ganze Zahl p

$$\delta_p\sigma = \delta_{p-1}\tau = S(x^p) \tag{77}$$

ist, wo die Summation S sich auf alle n Werte von x bezieht. Bezeichnet man ferner mit D die Diskriminante von $\varepsilon(\varphi)$, d. h. das Quadrat des Produktes aus allen Differenzen der n Größen x, so ist nach einem ebenfalls bekannten Satze

$$D = \begin{vmatrix} \delta\sigma, & \delta_1\sigma \ldots \delta_{n-1}\sigma \\ \delta_1\sigma, & \delta_2\sigma \ldots \delta_n\sigma \\ \cdots\cdots\cdots\cdots & \\ \delta_{n-1}\sigma, & \delta_n\sigma \ldots \delta_{2n-2}\sigma \end{vmatrix}, \tag{78}$$

welcher Ausdruck sich noch umformen läßt. Multipliziert man die Determinante

$$\varrho = \begin{vmatrix} \delta\xi_1 & \dots \delta\xi_n \\ \delta_1\xi_1 & \dots \delta_1\xi_n \\ \dots\dots\dots\dots \\ \delta_{n-1}\xi_1 \dots & \delta_{n-1}\xi_n \end{vmatrix} \tag{79}$$

mit der aus den Zahlen τ_{rs} gebildeten Determinante Δ, und bedenkt, daß

$$\sum \tau_{r\iota}\delta_p\xi_\iota = \delta_p\tau_r$$

ist, so erhält man das Produkt

$$\Delta\varrho = \begin{vmatrix} \delta\tau_1 & \dots \delta\tau_n \\ \delta_1\tau_1 & \dots \delta_1\tau_n \\ \dots\dots\dots\dots \\ \delta_{n-1}\tau_1 \dots & \delta_{n-1}\tau_n \end{vmatrix};$$

multipliziert man abermals mit ϱ, und bedenkt, daß mit Rücksicht auf (41) und (54)

$$\sum \delta_p\xi_\iota\delta_q\tau_\iota = \sum \delta_p\xi_\iota\sigma_{\iota'}\delta_q\eta_{\iota',\iota} = \sum \sigma_{\iota'}\delta_{p+q}\xi_{\iota'} = \delta_{p+q}\sigma$$

ist, so ergibt sich offenbar der Satz

$$D = \Delta\varrho^2. \tag{80}$$

Auf ähnliche Weise findet man leicht aus (74)

$$\varrho\,\varepsilon(\varphi) = \begin{vmatrix} 1, & \delta\xi_1 & \dots \delta\xi_n \\ \xi, & \delta_1\xi_1 & \dots \delta_1\xi_n \\ \dots\dots & \dots\dots & \dots\dots \\ \xi^n, & \delta_n\xi_1 & \dots \delta_n\xi_n \end{vmatrix}. \tag{81}$$

Aus unserer Annahme, daß die Determinante Δ von Null verschieden ist, läßt sich nun — worauf ich unten zurückkommen werde — in aller Strenge beweisen, daß die Determinante ϱ und folglich auch die Diskriminante D nicht identisch verschwindet. Man kann daher den n Variablen ξ_r solche bestimmte Zahlwerte beilegen, daß die n Wurzeln x sämtlich voneinander verschieden ausfallen. Nachdem dies geschehen, definieren wir für jede dieser n Wurzeln x ein entsprechendes System von n Zahlen $e_1, e_2 \dots e_n$ durch diejenigen n Gleichungen

$$x^p = \sum e_\iota\delta_p\xi_\iota, \tag{82}$$

welche den n Werten $p = 0, 1, 2 \dots (n-1)$ entsprechen; die n Größen e_r sind hierdurch in ihrer Abhängigkeit von der Wurzel x

vollständig bestimmt, weil die Determinante ϱ einen von Null verschiedenen Wert hat. Es ergibt sich zunächst, daß die Gleichung (82) nun für jede positive ganze Zahl p besteht (auch für jede negative, wenn φ von Null verschieden ist); in der Tat, da $\varepsilon(\varphi)$ für $\xi = x$ verschwindet, so genügt x^p zufolge (72) derselben Rekursion

$$\sum_{\mu=0}^{\mu=n} \varphi_\mu x^{\mu+p} = 0,$$

welche zufolge (67) für die Größen $\delta_p \xi_r$ gilt; nimmt man daher an, unser Satz (82) sei für n aufeinanderfolgende Werte

$$p = m,\ m+1 \ldots m+n-1$$

bewiesen, so ergibt sich aus dieser Übereinstimmung, und weil φ_n von Null verschieden ist, daß er auch für $p = m+n$ gilt, wodurch er offenbar allgemein bewiesen ist.

Hierauf führen wir für je zwei Indizes r, s aus der Reihe $1, 2 \ldots n$ eine entsprechende, ebenfalls von der Wahl der Wurzel x abhängende Zahl

$$e_{rs} = e_{sr} = \sum e_\iota \eta_{\iota, rs} \tag{83}$$

ein; multipliziert man mit $\delta_p \xi_r \delta_q \xi_s$ und summiert über alle Werte r, s, so folgt mit Rücksicht auf (54) und (82)

$$\sum e_{\iota\iota'} \delta_p \xi_\iota \delta_q \xi_{\iota'} = \sum e_\iota \eta_{\iota, \iota'\iota''} \delta_p \xi_{\iota'} \delta_q \xi_{\iota''} = \sum e_\iota \delta_p \xi_{\iota'} \delta_q \eta_{\iota, \iota'}$$
$$= \sum e_\iota \delta_{p+q} \xi_\iota = x^{p+q} = x^p x^q = \sum e_\iota \delta_p \xi_\iota e_{\iota'} \delta_q \xi_{\iota'},$$

also

$$\sum (e_{\iota\iota'} - e_\iota e_{\iota'}) \delta_p \xi_\iota \delta_q \xi_{\iota'} = 0;$$

setzt man hierin für p und q alle Werte aus der Reihe

$$0,\ 1,\ 2 \ldots (n-1),$$

und bedenkt, daß die Determinante ϱ von Null verschieden ist, so folgt leicht, daß immer $e_{rs} = e_r e_s$, also zufolge (83)

$$e_r e_s = \sum e_\iota \eta_{\iota rs} \tag{84}$$

ist, wodurch wir zu der Gleichung (19) unseres ersten Teiles zurückgekehrt sind.

Substituiert man endlich für x alle n verschiedenen Wurzeln und bezeichnet mit $e_r^{(s)}$ denjenigen Wert von e_r, welcher durch die Wurzel $x = x^{(s)}$ erzeugt wird, so erhält man, wenn man die Determinante der n^2 Zahlen (82) bildet, die den Werten

$$p = 0,\ 1,\ 2 \ldots (n-1)$$

entsprechen, das Resultat

$$\sqrt{D} = \varrho \sum \pm e_1' e_2'' \dots e_n^{(n)} = \varrho e$$

und hieraus mit Rücksicht auf (80)

(85) $$\Delta = e^2;$$

das auf diese Weise aus dem System der Zahlen $\eta_{t,rs}$ berechnete System E der Zahlen $e_r^{(s)}$ besitzt daher eine von Null verschiedene Determinante e.

Da die Gleichungen (84) für jede der n Substitutionen $x = x^{(s)}$ gelten, so ist hiermit aus den gegebenen Zahlen $\eta_{t,rs}$ ein n-wertiges System von n Größen $e_1, e_2 \dots e_n$ konstruiert, aus welchem umgekehrt auf die im ersten Teil angegebene Art unser jetzt gegebenes System von Zahlen $\eta_{t,rs}$ erzeugt wird. Hiermit ist der Beweis geliefert, daß jedes System von n Haupteinheiten, wie es in der Untersuchung des Herrn Weierstrass auftritt, stets aufgefaßt werden darf als ein n-wertiges System von n gewöhnlichen Zahlen, in der Weise, daß jede rationale Gleichung zwischen den n Haupteinheiten dann und nur dann wahr ist, wenn sie für jedes der von uns hergeleiteten Spezialsysteme $e_1^{(s)}, e_2^{(s)} \dots e_n^{(s)}$ gilt. Will man daher überhaupt noch von solchen überkomplexen Größen als von neuen Zahlen sprechen (was ich für unzweckmäßig halte, weil in unserer höheren Algebra beständig mehrwertige Größensysteme genau in der hier beschriebenen Weise auftreten), so kann dies doch nur in einem ganz anderen, und zwar unendlich viel schwächeren Sinne geschehen, als bei der gewaltigen Bereicherung des Körpers der reellen Zahlen durch die Hinzufügung der imaginären Zahlen, oder auch bei der Einführung der Hamiltonschen Quaternionen, die, wenn ihr Nutzen auch auf ein sehr kleines Feld beschränkt zu sein scheint, doch auf den Charakter der Neuheit gegenüber den anderen Zahlen unbedingten Anspruch erheben dürfen.

Es ist nun auch leicht zu zeigen, daß das gefundene System E der Zahlen $e_r^{(s)}$ — abgesehen von der Freiheit, die den einzelnen Substitutionen entsprechenden oberen Indizes nach Belieben mit einander zu vertauschen — ein einziges, vollständig bestimmtes, d. h. immer dasselbe ist, wie auch die numerischen Werte der Variablen ξ_r, denen ein von Null verschiedener Wert ϱ entspricht, sonst gewählt sein mögen. Denn wenn wir, nachdem wir ein bestimmtes solches System gefunden und uns dadurch auf die im ersten Teil unserer

Untersuchung angenommene Grundlage gestellt haben, den Größen ξ_r ihre volle Variabilität wiedergeben und, ohne Rücksicht auf die bisherige Bedeutung von x, diese Größe jetzt, wie im ersten Teil (6), als n-wertige lineare Funktion

$$x = \sum e_\iota \xi_\iota \tag{86}$$

definieren, so folgt aus (19) oder (84)

$$x\, e_r = \sum e_{\iota'}\, \eta_{\iota', r\iota}\, \xi_\iota = \sum e_\iota \eta_{\iota, r}, \tag{87}$$

und wenn ξ eine willkürliche einwertige Größe bedeutet,

$$(x - \xi)\, e_r = \sum e_\iota (\eta_{\iota, r} - (\iota, r)\, \xi); \tag{88}$$

wendet man hierauf alle n Substitutionen an, setzt für r alle n Indizes und bildet die Determinante, so erhält man nach Division durch die von Null verschiedene Determinante e und mit Rücksicht auf (74) das Resultat

$$\prod (x - \xi) = \varepsilon(\varphi); \tag{89}$$

da nun die Funktion $\varepsilon(\varphi)$ schon durch das System der Zahlen $\eta_{\iota, rs}$ vollständig bestimmt ist, so gilt dasselbe von der Gesamtheit der n linearen Funktionen x in (86), also auch von dem System E ihrer Koeffizienten $e_r^{(s)}$. Zugleich ergibt sich hierbei das Resultat, in welchem rückwärts alles übrige enthalten ist, daß $\varepsilon(\varphi)$ und also auch

$$\varphi = \prod x \tag{90}$$

ein Produkt von n linearen Faktoren ist. —

Bei dem vorstehenden Beweise der Existenz des erzeugenden Systems E und der Zerlegbarkeit der Funktion φ in lineare Faktoren habe ich denjenigen Weg gewählt, welcher die meisten Berührungspunkte mit den Entwicklungen des Herrn Weierstrass darbietet. Hierbei habe ich die besondere Voraussetzung machen müssen, daß die in (79) definierte Determinante ϱ nicht identisch verschwindet; in Wahrheit ist dies, wie ich schon oben bemerkt habe, eine notwendige Folge unserer Grundannahme, daß die Determinante Δ einen von Null verschiedenen Wert besitzt, aber es hat mir trotz mancher zeitraubenden Versuche nicht gelingen wollen, diesen nicht unwichtigen Satz kurz, und zwar lediglich mit denjenigen Hilfsmitteln zu beweisen, welche in der obigen Darstellung vor seiner Benutzung, also bis (81), entwickelt sind. Da die analoge Frage für die Funktion φ

oben in (46) auf die leichteste Weise erledigt ist, nämlich durch die wirkliche Angabe eines aus den Zahlen $\eta_{t,rs}$ rational abgeleiteten Wertsystems $\xi_r = \delta\xi_r$, für welches φ nicht verschwindet, so befremdet mich diese Schwierigkeit, und ich würde mich sehr freuen, wenn es einem anderen Mathematiker gelänge, sie zu überwinden.

Daß wirklich ϱ nicht identisch verschwindet, wenn Δ von Null verschieden ist, kann man nun — freilich post festum — auf einem ganz anderen Wege beweisen, nämlich so, daß man vorher die Zerlegbarkeit der Funktion φ in lineare Faktoren dartut. Der Kürze halber will ich mich aber hier darauf beschränken, nur die Hauptpunkte dieses Beweises anzugeben (vgl. den oben zitierten § 159 der zweiten Auflage von Dirichlets Zahlentheorie). Unter der im folgenden immer geltenden Annahme konstanter Differentiale $d\xi_r$, $d'\xi_r$ findet man aus (62) durch abermalige Differentiation unter Berücksichtigung von (55) und der aus (36) oder (43) leicht abzuleitenden Gleichung

$$\sum d\tau_\iota d'\eta_\iota = \sum \tau_\iota d d'\eta_\iota$$

das Resultat

$$dd' \log\varphi = -\delta_{-2}\sum \tau_\iota d d'\eta_\iota; \tag{91}$$

definiert man die von d und d' abhängige Variation d'' durch die ebenfalls konstanten Differentiale

$$d''\xi_r = d d'\eta_r, \tag{92}$$

so nimmt dasselbe die einfachere Form

$$dd' \log\varphi = -\delta_{-2} d''\tau \tag{93}$$

an, woraus leicht der Satz

$$dd' \log\varphi = d''\delta \log\varphi \tag{94}$$

folgt, welcher die Grundlage des Beweises bildet (beiläufig bemerkt, folgt hieraus schon, daß aus der Funktion φ und der Variation δ sich das ganze System der Zahlen $\eta_{t,rs}$ rückwärts ableiten läßt). Man zeigt zunächst leicht, daß jeder ganze rationale Faktor ψ der Funktion φ dieselbe Eigenschaft

$$dd' \log\psi = d''\delta \log\psi \tag{95}$$

besitzt. Da ferner

$$\delta\left(\frac{\psi^2 d''\delta\log\psi}{\delta\psi}\right) = \psi\,\delta\left(\frac{d''\delta\psi}{\delta\psi}\right) \tag{96}$$

ist, so ergibt sich, daß die ganze Funktion

$$\delta\psi^2 d^2\psi - 2\delta\psi d\psi \delta d\psi + d\psi^2 \delta^2\psi \tag{97}$$

durch ψ teilbar ist, und hieraus läßt sich, wenn man für ψ ein Produkt von lauter voneinander verschiedenen irreduktiblen oder Primfunktionen nimmt, auf verschiedene Art beweisen, daß $\varepsilon(\psi)$ und also auch ψ ein Produkt von lauter linearen Faktoren ist. Dasselbe gilt daher auch von $\varepsilon(\varphi)$ und φ. Ist endlich

$$x = \sum e_\iota \xi_\iota \tag{98}$$

irgendeiner dieser linearen Faktoren von φ, so kann man ihn immer so wählen, daß $\delta x = 1$ wird, und dann gibt der auch für ihn gültige obige Satz

$$dd' \log x = d''\delta \log x \tag{99}$$

unmittelbar das Resultat $dx\,d'x = d''x$, d. h.

$$e_r e_s = \sum e_\iota \eta_{\iota, rs}, \tag{100}$$

womit das erstrebte Ziel erreicht ist. Daß aber die Funktion ϱ nicht identisch verschwindet, daß also die n linearen Funktionen x voneinander verschieden sind, ergibt sich jetzt sofort daraus, daß, wie aus (77) oder auch auf andere Weise leicht folgt, $2\tau = S(x^2)$ ist, und daß die Diskriminante Δ dieser Funktion einen von Null verschiedenen Wert hat. —

Zum Schluß noch folgende Bemerkung. Ich habe der Untersuchung von vornherein den Körper der komplexen Zahlen zugrunde gelegt, weil hierdurch die Darstellung sehr erleichtert wird. Will man, wie es in der Abhandlung des Herrn Weierstrass geschieht, nur reelle Zahlen $\eta_{\iota, rs}$ und ξ_r zulassen, so hat dies auf das mehrwertige System $e_1, e_2 \ldots e_n$ lediglich den Einfluß, daß, wenn ein Spezialsystem (5) imaginäre Zahlen enthält, immer ein zweites Spezialsystem vorhanden ist, welches aus den mit ihnen konjugierten imaginären Zahlen besteht.

Braunschweig, 13. Februar 1885.

Erläuterungen zur vorstehenden Abhandlung. (Zugleich zu XXI.)

Diese Abhandlung bringt die Theorie der kommutativen hyperkomplexen Systeme ohne Radikal — hyperkomplex in bezug auf den Körper der komplexen Zahlen — auf der Grundlage der Zerlegung der Systemdeterminante (Gruppendeterminante) in Linearfaktoren (90), womit auch die Zerlegung der charakteristischen Gleichung des allgemeinen Elements gegeben ist (89). Daraus wird der Hauptsatz gefolgert, die Allgemeingültigkeit der im ersten Teil (bis 24) angegebenen Struktur: Die Darstellung als direkte Summe von n dem Körper der komplexen Zahlen isomorphen Körpern, wodurch die n verschiedenen Homomorphismen des Systems in den Körper der komplexen Zahlen vermittelt werden; die Komponenten der Einheit ergeben dabei in ihren Koeffizienten die n Homomorphismen der komplementären Basis.

Entsprechende Entwicklungen hatte Dedekind ursprünglich zur Begründung der Körpertheorie verwandt (§ 159 der 2. Auflage von Dirichlet-Dedekind; Bd. III dieser Werke), indem er einen Körper n-ten Grades als hyperkomplexes System über dem Körper der rationalen Zahlen auffaßte, aus dem Nichtauftreten von Nullteilern die Irreduzibilität der Systemdeterminante erschloß und deren Zerlegung in Linearfaktoren bei Erweiterung des Koeffizientenbereichs gab. Auf diese Begriffe geht er in XXI zurück; Restklassenringe nach zerlegbaren ganzzahligen Polynomen und Erweiterung des Koeffizientenbereichs bei einem als hyperkomplex aufgefaßten Kreiskörper geben Beispiele für das Auftreten von Nullteilern und sollen den Zusammenhang mit der üblichen Algebra illustrieren. Bemerkenswert ist auch die geometrische Deutung des dritten Beispiels, die darauf hinauskommt, das System als Restklassenring nach einem Polynomideal in mehreren Unbestimmten aufzufassen.

Wie aus dieser letzteren Auffassung das Dedekindsche Hauptresultat sich herleiten läßt, hat Hilbert (Gött. Nachr. 1896) vermöge seines Nullstellensatzes gezeigt. In der Sprache der Matrizen hat Frobenius eine neue Herleitung und Verallgemeinerung gegeben (Über vertauschbare Matrizen, Berl. Ber. 1896); der Zusammenhang besteht in der Tatsache, daß die irreduziblen Homomorphismen einer Matrix durch Zuordnung der Matrix zu ihren charakteristischen Wurzeln gegeben sind. Auch in den späteren hyperkomplexen Arbeiten von Frobenius — vor allem in seiner Theorie der nichtkommutativen „Dedekind-schen Systeme“ — zeigt sich Dedekindscher Einfluß; die hyperkomplexe Auffassung von Algebra und Galoisscher Theorie wirkt sich aber erst in den neuesten hyperkomplexen Arbeiten aus [vgl. etwa E. Noether, „Hyperkomplexe Größen und Darstellungstheorie“, Math. Zeitschr. **30** (1929), § 21 oder eine demnächst in der Math. Zeitschr. erscheinende Arbeit über hyperkomplexe Galoissche Theorie].

Noether.

XXI.

Erläuterungen zur Theorie der sogenannten allgemeinen komplexen Größen.

[Nachrichten von der Königlichen Gesellschaft der Wissenschaften zu Göttingen, Jahrgang 1887, S. 1—7.]

Seit dem Erscheinen der auf diese Theorie bezüglichen Abhandlung des Herrn Weierstrass (im Jahrgang 1884 dieser Nachrichten, S. 395) und der meinigen (1885, S. 141) habe ich bei mündlichen und brieflichen Unterhaltungen öfter die Erfahrung gemacht, daß die in beiden Schriften niedergelegten Auffassungen nicht mit hinreichender Deutlichkeit voneinander unterschieden werden. Da vielleicht meine Darstellung hieran die Schuld trägt, so erlaube ich mir noch einmal auf denselben Gegenstand zurückzukommen. Es handelt sich um die Auslegung des bekannten Ausspruches von Gauß:

„Der Verf. hat sich vorbehalten, den Gegenstand, welcher in der vorliegenden Abhandlung eigentlich nur gelegentlich berührt ist, künftig vollständiger zu bearbeiten, wo dann auch die Frage, warum die Relationen zwischen Dingen, die eine Mannigfaltigkeit von mehr als zwei Dimensionen darbieten, nicht noch andere in der allgemeinen Arithmetik zulässige Arten von Größen liefern können, ihre Beantwortung finden wird." (Gauß' Werke, Bd. II, S. 178.)

Herr Weierstrass faßt (S. 410—411 l. c.) seine Ansicht in folgende Worte:

„Wenn ich nun mit dem Ergebnis der vorstehenden Untersuchung die im Anfange angeführte Gaußische Bemerkung, daß komplexe Größen mit mehr als zwei Haupteinheiten in der allgemeinen Arithmetik unzulässig seien, zusammenhalte, so scheint es mir, daß Gauß diese Unzulässigkeit als dadurch begründet angesehen

habe, daß das Produkt zweier Größen, sobald $n > 2$, verschwinden kann, ohne daß einer seiner Faktoren den Wert Null hat. Denn hätte er diesen Umstand nicht als ein unübersteigliches Hindernis für die Einführung der allgemeinen komplexen Größen in die Arithmetik betrachtet, so würde es ihm schwerlich entgangen sein, daß sich eine Arithmetik dieser Größen begründen läßt, in welcher alle Sätze entweder mit denen der Arithmetik der gewöhnlichen komplexen Größen identisch sind oder doch in der letzteren ihr Analogon finden. Er würde dann auch ohne Zweifel seinen Ausspruch dahin modifiziert haben, daß die Einführung der allgemeinen komplexen Größen in die Arithmetik zwar nicht unstatthaft, wohl aber überflüssig sei. In der Tat geht aus dem oben (S. 407) ausgesprochenen Satze hervor, daß die Arithmetik der allgemeinen komplexen Größen zu keinem Resultat führen kann, das nicht aus Ergebnissen der Theorie der komplexen Größen mit einer oder mit zwei Haupteinheiten ohne weiteres ableitbar wäre."

Von dieser Auffassung weicht die meinige (vgl. S. 142, 147, 156 l. c.) erheblich, nämlich in dem Hauptpunkte ab, daß ich den Größen, welche im vorstehenden allgemeine komplexe Größen genannt werden, den Charakter der Neuheit gänzlich versage; es handelt sich in unserem Jahrhundert nicht mehr um ihre Zulassung, sie sind vielmehr schon lange und mit großem Erfolge in die allgemeine Arithmetik zugelassen; sie bilden, wie gesagt, keine neue oder — um buchstäblich genau mit Gauß zu reden — keine andere Art von Größen, sondern sie sind geradezu identisch mit den überall in der Algebra eingebürgerten mehrwertigen gewöhnlichen Zahlen; es ist unmöglich, jene von diesen zu unterscheiden, und die letzteren bieten bei folgerichtiger Ausbildung ihres Begriffes auch schon die erwähnte Erscheinung dar, daß ein Produkt aus nicht verschwindenden Faktoren sehr wohl verschwinden kann. In allem Diesen glaube ich die Bedeutung und die volle Bestätigung des Ausspruches von Gauß zu erkennen.

Da ich den in meiner Schrift gegebenen allgemeinen Beweisen, auf welche ich diese meine Auffassung gründe, und welche, wie ich gern hinzufüge, dem Wesen nach auch in den analytischen Entwicklungen des Herrn Weierstrass enthalten sind, nichts hinzuzufügen habe, so begnüge ich mich, die beiden verschiedenen Auf-

fassungen durch einige Beispiele zu erläutern, weil diese oft eine weit größere überzeugende Kraft besitzen, als eine allgemeine Theorie.

Jedes Beispiel für unsere Untersuchung ist dann ein vollkommen bestimmtes, sobald die Produkte von je zwei der Haupteinheiten linear durch die letzteren dargestellt sind. Ich wähle zunächst ein System von drei Haupteinheiten e_1, e_2, e_3 mit folgenden Grundformeln:

$$\begin{aligned}
e_1^2 &= -2e_1 - e_2 - 2e_3 \\
e_2^2 &= -2e_2 - 2e_2 - e_3 \\
e_3^2 &= -e_1 - 2e_2 - 2e_3 \\
e_2e_3 &= e_1 + e_2 \\
e_3e_1 &= e_2 + e_3 \\
e_1e_2 &= e_1 + e_3.
\end{aligned}$$

Dieselben erfüllen, wie man sich leicht überzeugt, alle die Bedingungen, welche sich aus dem sogenannten assoziativen Gesetz der Multiplikation ergeben. Behält man ferner die von mir (l. c. S. 147) gewählten Bezeichnungen bei, so findet man

$$\begin{aligned}
\sigma_1 &= \sigma_2 = \sigma_3 = -1 \\
\tau_{11} &= \tau_{22} = \tau_{33} = 5 \\
\tau_{23} &= \tau_{31} = \tau_{12} = -2 \\
\Delta &= 49,
\end{aligned}$$

und weil die Determinante Δ nicht verschwindet, so sind auch die von Herrn Weierstrass aufgestellten Zulässigkeits-Bedingungen erfüllt; mithin würden die Größen e_1, e_2, e_3 wirklich die Haupteinheiten eines zulässigen Systems komplexer Größen von der Form

$$\xi_1 e_1 + \xi_2 e_2 + \xi_3 e_3$$

bilden, wo die Koordinaten ξ_1, ξ_2, ξ_3 alle reellen Werte durchlaufen. Allein ich kann nicht glauben, daß Gauß hierin eine neue (andere) Art von Größen erblickt haben würde. In der Tat, es ist unmöglich, irgendeine Eigenschaft, eine Tatsache anzugeben, durch welche diese Größen e_1, e_2, e_3 sich von den dreiwertigen Kreisteilungs-Perioden

$$e_1 = r + r^{-1},\ e_2 = r^2 + r^{-2},\ e_3 = r^3 + r^{-3}$$

unterscheiden, wo r unbestimmt jede Wurzel der Gleichung

$$r^6 + r^5 + r^4 + r^3 + r^2 + r + 1 = 0$$

bedeutet.

Genau so verhält es sich, wie ich gezeigt habe, in jedem anderen Beispiele. Ich führe noch die beiden folgenden an:

$$e_1^2 = e_1 + e_2 + e_3,\ e_2^2 = e_3,\ e_3^2 = e_3,$$
$$e_2 e_3 = e_2,\ e_3 e_1 = e_2 + e_3,\ e_1 e_2 = e_2 + e_3$$

und

$$e_1^2 = e_1 + e_2 + e_3,\ e_2^2 = e_3,\ e_3^2 = -e_3,$$
$$e_2 e_3 = -e_2,\ e_3 e_1 = -e_2 + e_3,\ e_1 e_2 = e_2 + e_3.$$

Alle Bedingungen der Weierstrassschen Theorie sind erfüllt, aber ich kann die Haupteinheiten e_1, e_2, e_3 nicht für eine neue Art von Größen ansehen, weil sie schlechterdings nicht zu unterscheiden sind von den gewöhnlichen mehrwertigen Größen

$$e_1 = 1 + r,\ e_2 = r,\ e_3 = r^2,$$

wo r jede Wurzel der kubischen Gleichung

$$r^3 - r = 0$$

im ersten Falle, im zweiten der Gleichung

$$r^3 + r = 0$$

bedeutet.

Um die Erscheinung des Verschwindens von Produkten aus nicht verschwindenden Faktoren im Reiche der gewöhnlichen, aber mehrwertigen Zahlen zu erläutern, schicke ich folgende Bemerkung voraus. Ist r eine n-wertige*) Zahl, d. h. bedeutet r unterschiedslos jeden der n voneinander verschiedenen bestimmten Zahlwerte

$$r',\ r'' \ldots r^{(n)},$$

so wird folgerichtig, wenn $\varphi(t)$, $\psi(t)$ ganze Funktionen einer Veränderlichen t mit bestimmten (d. h. einwertigen) Koeffizienten sind, die Behauptung

$$\varphi(r) = \psi(r)$$

stets und nur dann für wahr gelten, wenn die n-Bedingungen

$$\varphi(r') = \psi(r'),\ \varphi(r'') = \psi(r'') \ldots \varphi(r^{(n)}) = \psi(r^{(n)})$$

sämtlich erfüllt sind, d. h. wenn die ganze Funktion $\varphi(t) - \psi(t)$ durch die ganze Funktion

$$f(t) = (t - r')(t - r'') \ldots (t - r^{(n)})$$

teilbar ist.

---

*) Wenn man lieber will, so mag man r eine veränderliche Größe nennen, deren Gebiet auf n bestimmte, voneinander verschiedene Werte r', $r'' \ldots r^{(n)}$ beschränkt ist.

Ist daher z. B. r eine zweiwertige Größe, welche unterschiedslos jeden der beiden Werte ± 1 bedeutet, so verschwindet weder die Größe $r + 1$ noch $r - 1$, aber ihr Produkt $r^2 - 1$ verschwindet.

Man sage nicht, dies sei nur künstlich herbeigezogen, um den bisher in die allgemeine Arithmetik eingeführten Größen eine Eigenschaft zuzusprechen, die eigentlich nur einer ganz neuen Art von Größen beigelegt werden dürfte. Dem ist keineswegs so. Daß diese Eigenschaft der gewöhnlichen mehrwertigen Größen selten oder vielleicht niemals ausdrücklich erwähnt ist, findet seinen Grund darin, daß sie bei den meisten Beispielen wegen der besonderen Beschaffenheit derselben gar nicht zum Vorschein kommt, während sie bei allgemein gehaltenen Untersuchungen selbstverständlich ist und gerade deshalb kaum Erwähnung verdient. In der Tat, eins der bekanntesten Beispiele mehrwertiger Zahlen wird von der Theorie derjenigen Zahlengebiete geliefert, die ich endliche Körper genannt habe; hier liegt die Sache so, daß r jede Wurzel einer sogenannten irreduzibelen Gleichung $f(r) = 0$ bedeutet, deren Koeffizienten rationale Zahlen sind, und außerdem werden auch nur rationale Koeffizienten in den aus r gebildeten Größen $\varphi(r)$ geduldet; es ist lediglich eine Folge dieser besonderen Beschränkungen, daß ein Produkt aus zwei nicht verschwindenden Faktoren $\varphi(r)$ ebenfalls niemals verschwinden kann. Der bekannteste spezielle Fall ist wohl der der Kreisteilung, welchen Gauß in der siebenten Sektion der Disquisitiones Arithmeticae behandelt hat; im Artikel 339 wird, wenn n eine Primzahl bedeutet, unter r jede Wurzel der Gleichung $R = 0$ verstanden, wo

$$R = r^{n-1} + r^{n-2} + \text{etc.} + r + 1,$$

und im Artikel 341 wird bewiesen, daß diese Gleichung irreduzibel ist; solange r diese Bedeutung einer $(n - 1)$-wertigen Größe behält, gilt der Satz, daß ein Produkt aus zwei nicht verschwindenden, rational gebildeten Faktoren $\varphi(r)$ ebenfalls nicht verschwindet, und bei Umformungen von Zahlen $\varphi(r)$ in $\psi(r)$ dürfen alle und nur solche Glieder weggelassen werden, die den Faktor R enthalten. Aber aus naheliegenden Gründen führt Gauß, was bemerkt zu werden verdient, die meisten (doch nicht alle) solchen Umformungen so aus, daß sie auch noch für $r = 1$ gültig bleiben, wodurch der Grad der Mehrwertigkeit erhöht wird; in allen diesen Fällen ist daher weder der Faktor R noch der Faktor $r - 1$ als verschwindend anzusehen,

wohl aber ihr Produkt $r^n - 1$. Dies wird freilich nirgends ausdrücklich erwähnt, aber tatsächlich verhält es sich so.

Auch die Geometrie kann leicht Veranlassung zur Betrachtung mehrwertiger Größen geben, bei welchen dieselbe Erscheinung auftritt. Sind z. B. drei Punkte M', M'', M''' durch ihre Cartesischen Koordinaten gegeben,

$$\begin{array}{lll} M' & \text{durch} & 1,\quad 0,\ 0 \\ M'' & \text{„} & 2,\quad 1,\ 1 \\ M''' & \text{„} & 0,\ -1,\ 1 \end{array}$$

und es handelt sich darum, alle algebraischen Flächen zu bestimmen, welche durch alle drei Punkte gehen, so läuft dies darauf hinaus, alle die rationalen Gleichungen zwischen drei Größen e_1, e_2, e_3 aufzustellen, welche durch jedes der drei obigen Systeme von je drei Koordinaten befriedigt werden. Diese Größen e_1, e_2, e_3 bilden daher ein solches mehrwertiges System, wie ich es im ersten Teile meiner Abhandlung (S. 143—147) betrachtet habe, und zwar sind die Grundformeln für die Multiplikation diejenigen, welche sich oben im zweiten meiner drei Beispiele finden. Die einzige für e_1, e_2, e_3 geltende lineare Gleichung

$$e_1 - e_2 = 1$$

entspricht der durch die drei Punkte M', M'', M''' gelegten Ebene; von den drei linearen Größen

$$e_1 - e_2 - e_3,\ e_2 + e_3,\ e_2 - e_3,$$

welche den durch den Nullpunkt und je zwei der Punkte M', M'', M'' gelegten Ebenen entsprechen und nach Herrn Weierstrass zweckmäßig Teiler der Null genannt werden können, verschwindet keine, wohl aber verschwinden die Produkte aus je zwei verschiedenen von ihnen, was sich geometrisch von selbst versteht.

Nachdem ich versucht habe, meine Deutung des Ausspruches von Gauß durch die vorstehenden Beispiele zu erläutern, glaube ich zugunsten derselben noch folgendes anführen zu dürfen. Die Grundlage für die Untersuchungen des Herrn Weierstrass (und ebenso der meinigen) über die Zulässigkeit allgemeiner komplexer Zahlen, welche linear aus n Haupteinheiten gebildet sind, besteht in der Forderung, daß die (von der Ordnung der Faktoren unabhängigen) Produkte aus je zwei Haupteinheiten sich wieder linear durch die Haupteinheiten darstellen lassen, und es darf wohl als sicher ange-

nommen werden, daß Gauß von derselben Grundlage ausgegangen ist. Vergleicht man nun hiermit den Artikel 345 der Disquisitiones Arithmeticae, in welchem Gauß den für die Kreisteilung äußerst wichtigen Satz aufstellt, daß die Produkte aus je zwei sogenannten Perioden sich linear durch die Perioden darstellen lassen, so springt die Ähnlichkeit jener arithmetischen Untersuchung über allgemeine komplexe Größen mit dieser, freilich sehr speziellen algebraischen Untersuchung über mehrwertige Größen der Kreisteilung so in die Augen, daß ich glauben möchte, Gauß müßte dieselbe sofort bemerkt haben und dadurch auf den Gedanken gekommen sein, daß jene hypothetischen komplexen Größen auch nichts anderes sind als gewöhnliche, aber mehrwertige Größen. Doch sind dies natürlich nur Wahrscheinlichkeitsgründe, welche die Streitfrage nicht entscheiden können, und darüber wird man vermutlich auch nicht mehr hinauskommen, weil jeder weitere Anhalt zu fehlen scheint.

XXII.

Über einen arithmetischen Satz von Gauß.

[Mitteilungen der Deutschen mathematischen Gesellschaft in Prag, Jahrgang 1892, S. 1—11.]

§ 1.

Die folgenden Betrachtungen beziehen sich auf den im Art. 42 der Disquisitiones Arithmeticae enthaltenen Satz:

I. Wenn die Koeffizienten der beiden ganzen Funktionen

$$P = x^m + p_1 x^{m-1} + p_2 x^{m-2} + \cdots + p_m,$$
$$Q = x^n + q_1 x^{n-1} + q_2 x^{n-2} + \cdots + q_n$$

der Variablen x rationale, aber nicht sämtlich ganze Zahlen sind, so können auch die Koeffizienten ihres Produkts

$$PQ = x^{m+n} + r_1 x^{m+n-1} + \cdots + r_{m+n}$$

nicht sämtlich ganze Zahlen sein.

Derselbe kommt meines Wissens nur ein einziges Mal, nämlich im Art. 341 zur Anwendung, und für diese Anwendung reicht die obige Fassung auch vollständig aus. Aber bei näherer Prüfung erkennt man leicht, daß der im Art. 42 enthaltene Beweis eine viel größere Tragweite besitzt, als diese Fassung des Satzes erkennen läßt. Um dies ganz deutlich zu machen, wollen wir mit p', q', r' bzw. die Nenner der in den Funktionen P, Q, PQ auftretenden, in den kleinsten Zahlen ausgedrückten Koeffizienten p, q, r und mit h irgendeine Primzahl bezeichnen; ist nun unter den Nennern p' mindestens einer durch die Potenz h^μ, aber keiner durch $h^{\mu+1}$ teilbar, und ist ebenso mindestens einer der Nenner q' durch h^ν, aber keiner durch $h^{\nu+1}$ teilbar, so zeigt Gauß, daß mindestens einer der Nenner r' durch die Potenz $h^{\mu+\nu}$ teilbar ist, und hiermit ist der obige Satz bewiesen, weil es (nach Annahme) mindestens eine Primzahl h gibt, für welche $\mu + \nu > 0$ ist. Um aber von dem, was Gauß bewiesen hat, nichts zu opfern, wollen wir mit a_0 das kleinste gemeinsame

Vielfache der Nenner p', mit b_0 dasjenige der Nenner q', mit c_0 dasjenige der Nenner r' bezeichnen; nach der bekannten Regel für die Bildung des kleinsten gemeinsamen Vielfachen von gegebenen Zahlen sind dann h^μ, h^ν und (weil offenbar keiner der Nenner r' durch $h^{\mu+\nu+1}$ teilbar sein kann) $h^{\mu+\nu}$ die höchsten Potenzen von h, welche bzw. in a_0, b_0 und c_0 aufgehen; und weil Ähnliches für jede Primzahl gilt, so folgt hieraus offenbar

$$a_0 b_0 = c_0,$$

während im obigen Satze nur behauptet wird, daß c_0 gewiß nicht $= 1$ sein kann, wenn mindestens eine der beiden Zahlen a_0, $b_0 > 1$ ist.

Multipliziert man nun eine Funktion P, deren höchster Koeffizient $= 1$ ist, mit dem Generalnenner a_0 der übrigen (oder auch aller) Koeffizienten, so entsteht immer eine sogenannte ursprüngliche (primitive) Funktion, d. h. eine Funktion

$$A = a_0 x^m + a_1 x^{m-1} + a_2 x^{m-2} + \cdots + a_m,$$

deren Koeffizienten ganze Zahlen ohne gemeinsamen Teiler sind; und umgekehrt, dividiert man eine ursprüngliche Funktion A durch ihren höchsten Koeffizienten a_0, so entsteht eine Funktion P, deren höchster Koeffizient $= 1$ und deren übrige Koeffizienten den Generalnenner a_0 haben. Aus dieser Bemerkung ergibt sich sofort, daß der von Gauß bewiesene Satz $a_0 b_0 = c_0$ auch in folgender Form ausgesprochen werden kann:

II. Das Produkt von zwei ursprünglichen Funktionen ist wieder eine ursprüngliche Funktion.

Versteht man ferner unter dem Teiler einer mit beliebigen ganzen rationalen Koeffizienten behafteten Funktion den größten gemeinsamen Teiler dieser Koeffizienten, so ist jede solche Funktion offenbar das Produkt aus ihrem Teiler und aus einer ursprünglichen Funktion, und der vorstehende Satz nimmt folgende Form an, in welcher ich ihn gelegentlich*) in Dirichlets Vorlesungen über Zahlentheorie (S. 466 der zweiten, S. 545 der dritten Auflage) erwähnt habe:

III. Der Teiler eines Produktes von zwei Funktionen ist das Produkt aus den Teilern der beiden Faktoren.

*) Daß dieser naheliegende und so leicht zu beweisende Satz schon vor mir von anderen ausgesprochen sein mag, ist zwar sehr wahrscheinlich, aber ich habe keine solche Stelle finden können.

Offenbar gilt derselbe Satz auch für Funktionen mit gebrochenen rationalen Koeffizienten, wenn man unter dem Teiler einer solchen Funktion F diejenige vollständig bestimmte (positive) Zahl t versteht, für welche der Quotient $F:t$ eine ursprüngliche Funktion wird; dann sind z. B. die Teiler der oben mit P, Q, PQ bezeichneten Funktionen die umgekehrten Werte von a_0, b_0, c_0, und der Satz besteht wieder in der Gleichung $c_0 = a_0 b_0$. Man findet ferner leicht, daß der Satz für Produkte von beliebig vielen Faktoren und für Funktionen von beliebig vielen unabhängigen Variablen gilt. Statt aber auf solche Verallgemeinerungen einzugehen, ziehe ich es vor, dem Satze noch eine andere gleichwertige Form zu geben, welche insofern einfacher und deshalb leichter auf höhere Zahlengebiete zu übertragen ist, als in ihr der Begriff des Teilers gar nicht mehr auftritt:

IV. Sind alle Koeffizienten a der Funktion A und alle Koeffizienten b der Funktion B rationale Zahlen, und sind alle Koeffizienten c des Produktes AB ganze Zahlen, so sind auch alle Produkte ab ganze Zahlen.

Um dies zu beweisen, bezeichne ich mit α, β die Teiler der Funktionen $A = \alpha A'$, $B = \beta B'$ und mit a', b' alle Koeffizienten der ursprünglichen Funktionen A', B'; jedes Produkt ab ist dann von der Form $(\alpha a')(\beta b')$, und weil $\alpha\beta$ (nach II oder III) der Teiler der Funktion AB ist, diese aber (nach Annahme) lauter ganze Koeffizienten c hat, so ist $\alpha\beta$ und folglich auch jedes Produkt ab eine ganze Zahl, w. z. b. w.

Ebenso leicht ist es, aus diesem Satze IV umgekehrt den Satz II oder III abzuleiten, ohne nochmals auf den Nerv des Beweises von Gauß, also auf die Bildung der Koeffizienten eines Produktes aus denen der Faktoren zurückzugehen. Wäre nämlich ein Produkt aus zwei ursprünglichen Funktionen A, B, deren Koeffizienten mit a, b bezeichnet werden mögen, keine ursprüngliche Funktion, wären also alle (offenbar ganzen) Koeffizienten von AB durch eine Primzahl h teilbar, so müßten, weil dann das Produkt $\frac{A}{h} \cdot B$ lauter ganze Koeffizienten hätte, alle Produkte $\frac{a}{h} \cdot b$ (nach IV) ganze Zahlen sein, was offenbar nicht der Fall ist, weil sowohl in A als auch in B sich mindestens ein durch h nicht teilbarer Koeffizient a, b findet.

Der Satz IV ist daher vollkommen gleichwertig mit dem Satze II oder III; aber jeder dieser Sätze ist schärfer als der Satz I.

§ 2.

Ich gehe nun dazu über, den Satz in der Weise zu verallgemeinern, daß die Koeffizienten, welche bisher als rational angenommen waren, beliebige algebraische Zahlen sein dürfen. Unter einer algebraischen Zahl verstehe ich jede Wurzel einer Gleichung mit rationalen Koeffizienten, und ich nenne sie eine ganze algebraische Zahl oder kürzer eine ganze Zahl, wenn unter den unendlich vielen Gleichungen, deren Wurzel sie ist, es auch eine solche gibt, deren höchster Koeffizient $= 1$ und deren übrige Koeffizienten ganze rationale Zahlen sind (Dirichlets Zahlentheorie, Aufl. 2 und 3, § 160). Hieraus ergeben sich sofort die a. a. O. bewiesenen Sätze:

1. Die Summen, Differenzen, Produkte von je zwei ganzen Zahlen sind ganze Zahlen.

2. Jede Wurzel einer Gleichung, deren höchster Koeffizient $= 1$ und deren übrige Koeffizienten ganze Zahlen sind, ist eine ganze Zahl.

Aus diesen beiden Sätzen leiten wir leicht noch den folgenden ab:

3. Eine Zahl α ist gewiß eine ganze Zahl, wenn es ein endliches System von Zahlen $\mu_1, \mu_2 \dots \mu_n$ gibt, die nicht sämtlich verschwinden und deren jede (μ_r) durch Multiplikation mit α ein Produkt von der Form

$$\alpha\mu_r = z_1^{(r)}\mu_1 + z_2^{(r)}\mu_2 + \cdots + z_n^{(r)}\mu_n$$

gibt, wo alle mit z bezeichneten Koeffizienten ganze Zahlen sind.

Denn durch Elimination der n Größen μ_r aus diesen n homogenen linearen Gleichungen ergibt sich bekanntlich die Gleichung

$$\begin{vmatrix} z_1' - \alpha, & z_2' & \dots & z_n' \\ z_1'' & , z_2'' - \alpha & \dots & z_n'' \\ \cdots & \cdots & \cdots & \cdots \\ z_1^{(n)} & , z_2^{(n)} & \dots & z_n^{(n)} - \alpha \end{vmatrix} = 0;$$

entwickelt man die Determinante nach Potenzen von α, so erhält man eine Gleichung von der Form

$$\alpha^n + y_1\alpha^{n-1} + y_2\alpha^{n-2} + \cdots + y_n = 0,$$

deren Koeffizienten $y_1, y_2 \dots y_n$ durch Addition, Subtraktion, Multiplikation aus den ganzen Zahlen z entstehen und folglich (nach 1.) ebenfalls ganze Zahlen sind, und hieraus folgt (nach 2.), daß auch α eine ganze Zahl ist, w. z. b. w.

Mit Hilfe der in dem genannten Werke begründeten allgemeinen Zahlentheorie, die sich auf die Begriffe des endlichen Zahlenkörpers und der ihm angehörenden Ideale stützt, ist es nun leicht, den obigen Satz III auf Funktionen mit beliebigen algebraischen Koeffizienten zu übertragen. Sind nämlich die Koeffizienten der beiden Funktionen

$$A = a_0 x^m + a_1 x^{m-1} + \cdots + a_m,$$
$$B = b_0 x^n + b_1 x^{n-1} + \cdots + b_n$$

und folglich auch diejenigen ihres Produktes

$$AB = c_0 x^{m+n} + c_1 x^{m+n-1} + \cdots + c_{m+n}$$

ganze Zahlen eines endlichen Körpers Ω, und bedeutet $\mathfrak{p}$ irgendein Primideal in Ω, so ergibt sich in ganz ähnlicher Art wie bei dem Beweise von Gauß, daß die höchste in allen Koeffizienten c aufgehende Potenz von $\mathfrak{p}$ gleich $\mathfrak{p}^{\mu+\nu}$ ist, wo $\mathfrak{p}^\mu$ die höchste in allen Zahlen a, und $\mathfrak{p}^\nu$ die höchste in allen Zahlen b enthaltene Potenz ist; sind nämlich r, s die kleinsten Indizes, für welche a_r nicht durch $\mathfrak{p}^{\mu+1}$ und b_s nicht durch $\mathfrak{p}^{\nu+1}$ teilbar ist, so kann der Koeffizient c_{r+s} gewiß nicht durch $\mathfrak{p}^{\mu+\nu+1}$ teilbar sein, weil er ein Aggregat von Produkten ab ist, die alle, mit Ausnahme des einzigen Gliedes $a_r b_s$, durch $\mathfrak{p}^{\mu+\nu+1}$ teilbar sind. Hiermit ist aber nach den Prinzipien der Idealtheorie wirklich bewiesen, daß der Teiler des Produktes AB d. h. der größte gemeinsame Idealteiler aller Koeffizienten c, das Produkt aus den Teilern von A und B ist.

Aber welche weit ausgedehnte Theorie gehört dazu, um diesen Satz beweisen, ja um ihn nur mit Verständnis aussprechen zu können! Ganz anders verhält es sich mit der folgenden Verallgemeinerung des Satzes IV, die nur den obigen einfachen Begriff der ganzen Zahl aber gar nichts von Körpern oder Idealen voraussetzt:

V. Wenn das Produkt aus zwei Funktionen A, B lauter ganze Koeffizienten besitzt, so ist jedes aus einem Koeffizienten von A und einem Koeffizienten von B gebildete Produkt eine ganze Zahl.

Dieser Satz ist zwar für den Kenner der Idealtheorie wieder gleichwertig mit der eben besprochenen Verallgemeinerung des Satzes III, aber seine viel einfachere Form läßt auch die Möglichkeit eines einfacheren Beweises vermuten. Die Herstellung eines solchen

Beweises bildet den eigentlichen Gegenstand der vorliegenden Abhandlung, und dies wird wohl im Hinblick auf die zahlreichen Anwendungen, welche der Satz V gestattet, hinreichend gerechtfertigt erscheinen.

§ 3.

Am kürzesten gelangt man zu dem gewünschten Ziele, indem man sich auf den folgenden speziellen Fall stützt:

VI. Wenn die ganze Funktion $f(x)$ lauter ganze Koeffizienten hat, und wenn ω irgendeine Wurzel der Gleichung $f(\omega) = 0$ bedeutet, so hat auch die ganze Funktion

$$f_1(x) = \frac{f(x)}{x - \omega}$$

lauter ganze Koeffizienten.

Um dies zu beweisen, setzen wir

$$f(x) = c_0 x^k + c_1 x^{k-1} + \cdots + c_k,$$
$$f_1(x) = a_0 x^{k-1} + a_1 x^{k-2} + \cdots + a_{k-1},$$

woraus

$$a_r = c_0 \omega^r + c_1 \omega^{r-1} + \cdots + c_r$$

folgt. Multipliziert man nun einen bestimmten solchen Koeffizienten a_r mit jeder der k Potenzen $1, \omega, \omega^2 \ldots \omega^{k-1}$, so erhält man

$$a_r \omega^s = c_0 \omega^{r+s} + c_1 \omega^{r+s-1} + \cdots + c_r \omega^s;$$

ist der Exponent s eine der $k - r$ Zahlen $0, 1, 2 \ldots k - r - 1$, also $r + s < k$, so behalten wir diese Form des Produktes bei; ist aber der Exponent s eine der r Zahlen $k - r$, $k - r + 1 \ldots k - 1$, so multiplizieren wir die Gleichung

$$f(\omega) = c_0 \omega^k + c_1 \omega^{k-1} + \cdots + c_k = 0$$

mit ω^{r+s-k}, wodurch sich die andere Form

$$a_r \omega^s = -c_{r+1} \omega^{s-1} - c_{r+2} \omega^{s-2} - \cdots - c_k \omega^{s+r-k}$$

ergibt; da mithin alle diese Produkte $a_r \omega^s$ in der Form

$$z_1 \omega^{k-1} + z_2 \omega^{k-2} + \cdots + z_k$$

darstellbar sind, wo die Koeffizienten z ganze Zahlen bedeuten, so ist (nach 3. in § 2) auch jeder Koeffizient a_r eine ganze Zahl, w. z. b. w.

Durch wiederholte Anwendung dieses Satzes ergibt sich offenbar folgendes. Wenn die Funktion

$$f(x) = c_0 (x - \omega_1)(x - \omega_2) \ldots (x - \omega_k)$$

lauter ganze Koeffizienten hat, so behält sie diese Eigenschaft nach Division durch beliebig viele der Faktoren ersten Grades $(x - \omega)$; der letzte Koeffizient einer so erhaltenen Funktion ist (abgesehen vom Vorzeichen) immer von der Form $c_0 \omega' = c_0 \omega_r \omega_s \omega_t \ldots$, wo $r, s, t \ldots$ irgendwelche voneinander verschiedene Indizes aus der Reihe $1, 2 \ldots k$ bedeuten, also ω' jedes beliebige Glied des entwickelten Produktes

$$(1 + \omega_1)(1 + \omega_2) \ldots (1 + \omega_k)$$

sein kann. Alle Produkte von der Form $c_0 \omega'$ sind also ganze Zahlen.

Und hieraus folgt leicht der zu beweisende Satz V. Denken wir uns nämlich die Funktion $f(x)$ auf irgendeine Weise in zwei Faktoren A, B zerlegt, und setzen

$$A = a_0(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_m),$$
$$B = b_0(x - \beta_1)(x - \beta_2) \ldots (x - \beta_n),$$

so ist $a_0 b_0 = c_0$, $m + n = k$, und der Komplex der $m + n$ Zahlen α, β ist identisch mit dem Komplex der k Zahlen ω. Bezeichnen wir daher mit α' jedes Glied des entwickelten Produktes

$$(1 + \alpha_1)(1 + \alpha_2) \ldots (1 + \alpha_m),$$

ebenso mit β' jedes Glied des entwickelten Produktes

$$(1 + \beta_1)(1 + \beta_2) \ldots (1 + \beta_n),$$

so sind die Produkte $\alpha' \beta'$ identisch mit den Zahlen ω', und folglich ist jedes Produkt $a_0 \alpha' . b_0 \beta' = c_0 \omega'$, also eine ganze Zahl. Da nun jeder Koeffizient a der Funktion A (abgesehen vom Vorzeichen) ein Aggregat von Produkten $a_0 \alpha'$ und ebenso jeder Koeffizient b der Funktion B ein Aggregat von Produkten $b_0 \beta'$ ist, so ist jedes Produkt ab auch ein Aggregat von Produkten $a_0 \alpha' . b_0 \beta'$, also eine Summe von ganzen Zahlen und folglich (nach 1. in § 2) ebenfalls eine ganze Zahl, w. z. b. w.

Man sieht leicht, daß der nunmehr bewiesene Satz V auch für Produkte von beliebig vielen Faktoren gilt. Sind a, b, c die Koeffizienten der drei Funktionen A, B, C, so wird, wenn das Produkt $ABC = (AB)C$ lauter ganze Koeffizienten hat, nach V auch jede Funktion $(AB)c$, also auch jedes Produkt $A(Bc)$ ganze Koeffizienten haben, woraus nach V wieder folgt, daß die Produkte $a(bc)$ ganze Zahlen sind; und so kann man offenbar fortfahren. Übrigens leuchtet

ein, daß man den obigen Beweis auch ohne weiteres für Produkte von beliebig vielen Faktoren hätte führen können.

Ebenso würde die Übertragung des Satzes auf den Fall, wo die Koeffizienten nicht Zahlen, sondern algebraische Funktionen von veränderlichen Größen sind, keine neue Schwierigkeit darbieten, und in dieser Allgemeinheit kann der Satz sehr wohl dazu dienen, die Betrachtungen, welche Kronecker in § 14 seiner „Grundzüge einer arithmetischen Theorie der algebraischen Größen“ (1882) entwickelt hat, zu vereinfachen und zu vervollständigen. Der in dieser gedankenreichen Abhandlung herrschenden Auffassung der arithmetisch-algebraischen Probleme würde freilich der obige Beweis des Satzes V insofern wohl nicht vollkommen entsprechen, als in ihm die Zerlegbarkeit der Funktion $f(x)$ in Faktoren ersten Grades vorausgesetzt wird. Aus diesem Grunde will ich zum Schluß noch einen ganz anderen Beweis des Satzes V mitteilen, in welchem diese Zerlegbarkeit durchaus nicht benutzt wird.

§ 4.

Der Gang des neuen Beweises läßt sich am einfachsten darstellen, wenn man einige wenige Begriffe aus der Theorie der Moduln entlehnt. Ein System $\mathfrak{a}$ von Zahlen α nenne ich einen Modul*), wenn die Summen und Differenzen von je zwei solchen Zahlen α wieder demselben System $\mathfrak{a}$ angehören. Sind alle diese Zahlen α auch in dem Modul $\mathfrak{b}$ enthalten, so heißt $\mathfrak{a}$ teilbar durch $\mathfrak{b}$; sind zwei Moduln $\mathfrak{a}$, $\mathfrak{b}$ gegenseitig durch einander teilbar, so sind sie identisch, was durch $\mathfrak{a} = \mathfrak{b}$ bezeichnet wird. Bedeutet α jede Zahl des Moduls $\mathfrak{a}$, ebenso β jede Zahl des Moduls $\mathfrak{b}$, so bilden alle Produkte $\alpha\beta$ und alle Summen solcher Produkte wieder einen Modul, welcher das Produkt von $\mathfrak{a}$ und $\mathfrak{b}$ heißt und mit $\mathfrak{ab}$ bezeichnet wird. Ist $\mathfrak{a}$ teilbar durch $\mathfrak{b}$, so ist offenbar $\mathfrak{ab}$ teilbar durch $\mathfrak{bb}$ Ebenso kann man Produkte von beliebig vielen Moduln und Potenzen von Moduln bilden, und es gelten hierbei dieselben Multiplikationsgesetze wie bei Produkten von Zahlen.

Wir brauchen uns hier nur mit sogenannten endlichen Moduln zu beschäftigen. Sind $a_0, a_1, a_2 \ldots a_m$ irgendwelche bestimmte Zahlen,

*) Dirichlets Zahlentheorie, Aufl. 2, § 161.

während $x_0, x_1, x_2 \ldots x_m$ willkürliche rationale ganze Zahlen bedeuten, so bilden alle in der Form

$$\alpha = a_0 x_0 + a_1 x_1 + a_2 x_2 + \cdots + a_m x_m \tag{1}$$

darstellbaren Zahlen α einen solchen endlichen Modul $\mathfrak{a}$, der durch das Symbol

$$\mathfrak{a} = [a_0, a_1, a_2 \ldots a_m] \tag{2}$$

bezeichnet wird; das System der Zahlen $a_0, a_1 \ldots a_m$ heißt eine Basis von $\mathfrak{a}$, und diese Zahlen selbst heißen die Glieder oder Elemente dieser Basis. Offenbar kann die Basis eines endlichen Moduls $\mathfrak{a}$ in unendlich viele, äußerlich verschiedene Formen gebracht werden, ohne die geringste Änderung des gesamten Zahleninhalts von $\mathfrak{a}$; z. B. darf man das erste Glied a_0, indem man alle anderen beibehält, durch jede Zahl von der Form (1) ersetzen, in welcher $x_0 = \pm 1$ ist. Wenn nun

$$\mathfrak{b} = [b_0, b_1 \ldots b_n] \tag{3}$$

ebenfalls ein endlicher Modul ist, so gilt dasselbe offenbar auch von dem Produkt $\mathfrak{a}\,\mathfrak{b}$, und zwar ist

$$\mathfrak{a}\,\mathfrak{b} = [p_0, p_1 \ldots], \tag{4}$$

wo die Zahlen $p_0, p_1 \ldots$ alle Produkte von der Form $a_r b_s$ bedeuten.

Ebenso leuchtet ein, daß auch jede Potenz des endlichen Moduls (2) wieder ein endlicher Modul ist; die Basis einer solchen Potenz

$$\mathfrak{a}^{n+1} = [\alpha_0, \alpha_1, \alpha_2 \ldots]$$

besteht aus allen Produkten α von $n+1$ gleichen oder verschiedenen Faktoren aus der Reihe $a_0, a_1 \ldots a_m$; die Anzahl dieser Produkte α ist bekanntlich

$$\frac{\Pi(m+n+1)}{\Pi(m)\,\Pi(n+1)}.$$

Für unseren Zweck ist aber eine Transformation dieser Basis in eine andere erforderlich, deren Glieder gewisse aus den Größen $a_0, a_1 \ldots a_m$ gebildete Determinanten sind. Der Kürze halber wollen wir mit r irgendeine Kombination von $n+1$ verschiedenen, der Größe nach geordneten Indizes

$$r_0 < r_1 < r_2 \cdots < r_n \tag{r}$$

bezeichnen, welche der Reihe der $m+n+1$ Zahlen

$$0, 1, 2 \ldots (m+n)$$

angehören; dann ist zugleich

$$r_0 \leqq r_1 - 1 \leqq r_2 - 2 \cdots \leqq r_n - n,$$

und diese $n + 1$ Zahlen $r_\nu - \nu$ gehören alle der Reihe der $m + 1$ Zahlen

$$0,\ 1,\ 2 \ldots m$$

an; jeder Kombination r entspricht daher ein bestimmtes Produkt

$$\alpha_r = a_{r_0} a_{r_1 - 1} a_{r_2 - 2} \cdots a_{r_n - n},$$

und umgekehrt leuchtet ein, daß jedes Produkt α, also jedes Glied der Basis von $\mathfrak{a}^{n+1}$, aus einer und nur aus einer einzigen Kombination r entspringt. Ist ferner s eine von r verschiedene Kombination

$$s_0 < s_1 < s_2 \cdots < s_n, \qquad (s)$$

so können die Differenzen $r_0 - s_0$, $r_1 - s_1 \ldots r_n - s_n$ nicht alle verschwinden, und wir wollen von den beiden entsprechenden Gliedern α_r, α_s das erste als das höhere, das zweite als das niedrigere ansehen, wenn die erste nicht verschwindende dieser Differenzen positiv ausfällt; offenbar ordnen sich dann alle Glieder α ihrer Höhe nach in eine bestimmte Folge der Art, daß, wenn von drei Gliedern $\alpha_r, \alpha_s, \alpha$ das erste höher als das zweite und dieses höher als das dritte ist, gewiß das erste auch höher als das letzte ist; von allen Gliedern α ist a_m^{n+1} das höchste, a_0^{n+1} das niedrigste.

Indem wir ferner festsetzen, daß $a_i = 0$ sein soll, so oft der Index i nicht in der Reihe der $m + 1$ Zahlen 0, 1, 2 ... m enthalten ist, lassen wir jeder Kombination r, also jedem Produkte α_r eine bestimmte Determinante

$$\alpha_r' = \begin{vmatrix} a_{r_0} & a_{r_0 - 1} & \cdots & a_{r_0 - n} \\ a_{r_1} & a_{r_1 - 1} & \cdots & a_{r_1 - n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{r_n} & a_{r_n - 1} & \cdots & a_{r_n - n} \end{vmatrix}$$

entsprechen. Dieselbe ist ein Aggregat von lauter Produkten α, unter denen sich das Hauptglied α_r befindet, und man kann beweisen — was wir der Kürze halber dem Leser überlassen müssen — daß alle anderen Glieder niedriger als α_r sind. Hieraus folgt mit Rücksicht auf eine frühere Bemerkung, daß man die aus den Produkten $\alpha_0, \alpha_1 \ldots$ bestehende Basis des Moduls $\mathfrak{a}^{n+1}$ schrittweise, indem man immer α_r durch α_r' ersetzt, in eine neue Basis transformieren kann, welche aus den sämtlichen Determinanten α_r' besteht, daß also

$$\mathfrak{a}^{n+1} = [\alpha_0', \alpha_1' \ldots]$$

ist. Mit Hilfe dieser Transformation kann man leicht den folgenden Satz beweisen:

VII. Bildet man aus den Koeffizienten der drei ganzen Funktionen

$$\begin{aligned} A &= a_0 x^m + a_1 x^{m-1} + \cdots + a_m, \\ B &= b_0 x^n + b_1 x^{n-1} + \cdots + b_n, \\ AB &= c_0 x^{m+n} + c_1 x^{m+n-1} + \cdots + c_{m+n} \end{aligned}$$

die drei endlichen Moduln

$$\begin{aligned} \mathfrak{a} &= [a_0, a_1 \ldots a_m], \\ \mathfrak{b} &= [b_0, b_1 \ldots b_n], \\ \mathfrak{c} &= [c_0, c_1 \ldots c_{m+n}], \end{aligned}$$

so ist

$$\mathfrak{a}^{n+1}\mathfrak{b} = \mathfrak{a}^n \mathfrak{c}, \quad \mathfrak{a}\mathfrak{b}^{m+1} = \mathfrak{b}^m \mathfrak{c}.$$

Beweis. Aus der Bildungsweise der Koeffizienten

$$c_i = a_i b_0 + a_{i-1} b_1 + \cdots + a_{i-n} b_n$$

geht zunächst hervor, daß der Modul $\mathfrak{c}$ durch $\mathfrak{a}\mathfrak{b}$ und folglich $\mathfrak{a}^n \mathfrak{c}$ durch $\mathfrak{a}^{n+1}\mathfrak{b}$ teilbar ist. Setzt man ferner für i die in einer bestimmten Kombination r enthaltenen Indizes $r_0, r_1 \ldots r_n$, so ergibt sich, daß alle Produkte $\alpha'_r b_\nu$ in der Form

$$\alpha'_{r,0} c_{r_0} + \alpha'_{r,1} c_{r_1} \cdots + \alpha'_{r,n} c_{r_n}$$

darstellbar sind, wo $\alpha'_{r,0}, \alpha'_{r,1} \ldots \alpha'_{r,n}$ gewisse Unterdeterminanten n^{ten} Grades von α'_r bedeuten und folglich in dem Modul $\mathfrak{a}^n$ enthalten sind. Mithin ist jedes Produkt $\alpha'_r b_\nu$ in $\mathfrak{a}^n \mathfrak{c}$ enthalten, und da die Determinanten α'_r eine Basis von $\mathfrak{a}^{n+1}$ und die Zahlen b_ν eine Basis von $\mathfrak{b}$ bilden, so ist das Produkt $\mathfrak{a}^{n+1}\mathfrak{b}$ teilbar durch $\mathfrak{a}^n \mathfrak{c}$ und folglich $\mathfrak{a}^{n+1}\mathfrak{b} = \mathfrak{a}^n \mathfrak{c}$, w. z. b. w.

Aus diesem ganz allgemeinen Satze, in welchem über die Beschaffenheit der Koeffizienten a, b, c gar nichts vorausgesetzt wird, ergibt sich nun unmittelbar unser Satz V. Bilden nämlich die Zahlen $\mu_1, \mu_2 \ldots \mu_k$ eine Basis des Moduls $\mathfrak{a}^n$, so sind alle Produkte

$$a b \mu_1, \; a b \mu_2 \ldots a b \mu_k$$

in $(\mathfrak{a}\mathfrak{b})\mathfrak{a}^n$, d. h. in $\mathfrak{a}^n \mathfrak{c}$ enthalten, also von der Form

$$z_1 \mu_1 + z_2 \mu_2 + \cdots + z_k \mu_k,$$

wo $z_1, z_2 \ldots z_k$ Zahlen des Moduls $\mathfrak{c}$ bedeuten. Setzen wir also jetzt (wie in V) voraus, daß alle Koeffizienten c ganze Zahlen sind, so gilt dasselbe (nach 1. in § 2) auch von diesen Zahlen $z_1, z_2 \ldots z_k$ und folglich (nach 3. in § 2) auch von jedem Produkt ab, w. z. b. w.

Erläuterungen zur vorstehenden Abhandlung.

In der Abhandlung Nr. XXV: Über die Begründung der Idealtheorie, bemerkt Dedekind, daß er den Beweis des Satzes V, des Hauptsatzes der vorstehenden Abhandlung, schon am 15. Februar 1887 gefunden und am 20. Februar d. J. an H. Weber mitgeteilt hat. Etwas später, aber unabhängig von Dedekind, ist der Satz von A. Hurwitz (Über die Theorie der Ideale, Göttinger Nachrichten 1894, Math.-phys. Kl., S. 291—298, vgl. Fußnote S. 292) in einer äquivalenten Form ausgesprochen worden. Aus Satz V folgt bekanntlich einfach, daß man zu einem beliebigen Ideale ein zweites so bestimmen kann, daß das Produkt ein Hauptideal wird, und diese Tatsache ist sowohl von Hurwitz als auch gelegentlich von Dedekind zum Aufbau der Idealtheorie benutzt worden. Eine eingehende Diskussion dieser Probleme gibt Dedekind in der Abhandlung Nr. XXV; man vergleiche auch die Besprechung dieser Abhandlung im Vorwort zur vierten Auflage von Dirichlets Zahlentheorie, ebenso die weiteren Literaturangaben (Kronecker, Mertens) bei A. Hurwitz: „Über einen Fundamentalsatz der arithmetischen Theorie der algebraischen Größen“, Göttinger Nachrichten 1895, S. 230—240.

Ore.

XXIII.

Über Gleichungen mit rationalen Koeffizienten.

[Jahresbericht der Deutschen Mathematikervereinigung, Bd. I, S. 33—35 (1892).]

Daß solche Sätze über Gleichungen, die für jeden endlichen Grad gelten, nicht ohne weiteres für Gleichungen von unendlich hohem Grade in Anspruch zu nehmen sind, wird zu unserer Zeit wohl von fast allen Mathematikern anerkannt. Da aber die Entscheidung über eine solche Frage bisweilen nicht leicht zu finden ist, so erlaube ich mir im folgenden einen besonderen, nicht unwichtigen Fall zu behandeln. In der Lehre von denjenigen Gleichungen, welche einen endlichen Grad und lauter rationale Koeffizienten haben, wird der bekannte Satz bewiesen:

1. Hat die irreduzible Gleichung $\varphi(x) = 0$ eine Wurzel gemein mit der Gleichung $\psi(x) = 0$, so ist jede Wurzel der ersteren Gleichung auch eine Wurzel der letzteren.

Dieser Satz verliert aber, wenn die Gleichung $\psi(x) = 0$ von unendlich hohem Grade ist, seine allgemeine Gültigkeit, und zwar selbst für solche Gleichungen, deren linke Seite $\psi(x)$ eine für alle Werte von x konvergierende Potenzenreihe mit rationalen Koeffizienten ist. Dies ergibt sich unmittelbar aus dem Satze:

2. Ist α irgendeine reelle Zahl, so gibt es eine solche Gleichung $\psi(x) = 0$ von unendlich hohem oder auch endlichem Grade, welche α als einzige reelle Wurzel besitzt.

Ist nämlich dies bewiesen, so folgt daraus jedesmal ein offenbarer Widerspruch mit dem Satze 1., wenn man für α eine Wurzel einer irreduziblen Gleichung $\varphi(x) = 0$ (z. B. $x^2 - 2 = 0$) wählt, die mindestens zwei reelle Wurzeln α, β hat. Es kommt also nur noch darauf an, den Satz 2. zu beweisen, und hierbei darf man sich auf den Fall einer positiven Zahl α beschränken, weil auf diesen der entgegengesetzte Fall durch Verwandlung von x in $-x$ zurückgeführt wird; im Falle $\alpha = 0$ kann man natürlich $\psi(x) = x$ nehmen.

Aus jeder positiven Zahl α entsteht — in ähnlicher Weise und mit derselben Bestimmtheit, wie bei der Entwicklung in einen gemeinen Kettenbruch — immer eine Reihe von ganzen Zahlen $a_1, a_2, a_3, \ldots$ und eine Reihe von zugehörigen Resten, d. h. solchen Zahlen $\varepsilon_1, \varepsilon_2, \varepsilon_3, \ldots$, welche alle der Bedingung

$$0 \leqq \varepsilon < 1$$

genügen, nach folgender Regel: Zunächst setze man

$$\frac{1}{\alpha} = a_1 + \varepsilon_1,$$

wodurch a_1 als die größte in $\frac{1}{\alpha}$ enthaltene ganze Zahl, also auch ε_1 als Rest bestimmt ist; für jeden größeren Index n aber setze man

$$\frac{2\varepsilon_1}{\alpha^2} = a_2 + \varepsilon_2, \quad \frac{3\varepsilon_2}{\alpha^2} = a_3 + \varepsilon_3, \quad \ldots, \quad \frac{n\varepsilon_{n-1}}{\alpha^2} = a_n + \varepsilon_n, \quad \ldots,$$

wodurch auch alle folgenden Zahlen a als größte Ganze und alle Reste ε vollständig bestimmt sind; zugleich leuchtet ein, daß von den Zahlen a keine negativ ist. Dann besitzt die vollkommen definierte Funktion

$$\psi(x) = -1 + a_1 \frac{x}{1} + a_2 \frac{x^3}{1.2} + a_3 \frac{x^5}{1.2.3} + \cdots + a_n \frac{x^{2n-1}}{\Pi(n)} + \cdots$$

alle im Satze 2. angegebenen Eigenschaften. In der Tat:

1. Die Koeffizienten von $\psi(x)$ sind sämtlich rationale Zahlen.

2. Da $\varepsilon_{n-1} < 1$, also $a_n < \frac{n}{\alpha^2}$, so ist das allgemeine Glied der Reihe $\psi(x)$ absolut kleiner als

$$\frac{x}{\alpha^2} \cdot \frac{(x^2)^{n-1}}{\Pi(n-1)},$$

woraus bekanntlich folgt, daß die Reihe $\psi(x)$ (wie die Exponentialreihe) für jeden Wert von x konvergiert.

3. Aus den Definitionen der Zahlen a und ε folgt, daß die aus $(n+1)$ Gliedern bestehende Summe

$$-1 + a_1 \frac{\alpha}{1} + a_2 \frac{\alpha^3}{1.2} + a_3 \frac{\alpha^5}{1.2.3} + \cdots + a_n \frac{\alpha^{2n-1}}{\Pi(n)} = -\varepsilon_n \frac{\alpha^{2n-1}}{\Pi(n)}$$

ist, und da die rechte Seite mit unendlich wachsendem n unendlich klein wird, so folgt $\psi(\alpha) = 0$, d. h. α ist eine Wurzel der Gleichung $\psi(x) = 0$.

4. Da von den Zahlen α keine negativ, wohl aber mindestens eine positiv ist (wie aus $\psi(\alpha) = 0$ hervorgeht), da ferner, abgesehen von dem konstanten Gliede -1, die Variable x in der Reihe $\psi(x)$ nur in Potenzen mit ungeraden Exponenten auftritt, so wird gleichzeitig mit x auch $\psi(x)$ das ganze reelle Gebiet von $-\infty$ bis $+\infty$ stets wachsend durchlaufen und folglich auch nur für den einzigen Wert $x = \alpha$ den Wert Null erhalten; d. h. die Gleichung $\psi(x) = 0$ hat außer α keine reelle Wurzel, w. z. b. w.

Hiermit ist die Unzuverlässigkeit des Satzes 1. für Gleichungen $\psi(x) = 0$ von unendlich hohem Grade erwiesen. Dieser Nachweis ist wohl nicht ganz wertlos, weil verschiedene Mathematiker auf den Gedanken gekommen sind, durch Anwendung dieses unzuverlässigen Satzes auf das Beispiel $\psi(x) = \sin x$ einen Beweis für die Transzendenz der Zahl π zu gewinnen, der offenbar nur wenige Zeilen erfordern würde.

Der Beweis des Satzes 2. läßt sich, wie man leicht sieht, in der mannigfaltigsten Weise abändern; zugleich leuchtet ein, daß dieser Satz auch für jede endliche Anzahl von vorgeschriebenen reellen Wurzeln α gilt.

Erläuterungen zur vorstehenden Abhandlung.

Eine französische Übersetzung dieser Abhandlung erschien unter dem Titel „Sur les équations à coefficients rationels“ in den Nouvelles Annales de mathématiques, 3. Ser., Bd. 17, S. 201—204 (1898). (Übersetzung von L. Laugel.) Der Übersetzer fügt am Ende der Abhandlung die folgende Note hinzu: M. Dedekind me prie de mentionner ici un mémoire de M. A. Hurwitz (Acta Math., t. 14, 1889) où la même question a été traitée d'une manière beaucoup plus générale.

In der erwähnten Abhandlung von Hurwitz „Über beständig konvergierende Potenzreihen mit rationalen Zahlenkoeffizienten und vorgeschriebenen Nullstellen“ wird das Dedekindsche Resultat aus dem folgenden allgemeineren Satz abgeleitet: Zu einer beliebig gegebenen Potenzreihe $A(x)$ kann man eine ganze transzendente Funktion $B(x)$ so bestimmen, daß die Koeffizienten in der Reihenentwicklung von $A(x)\, e^{B(x)}$ sämtlich rational sind.

Mit derselben Frage beschäftigte sich schon E. Strauss, Acta Mathematica **11** (1887), S. 13—18; vgl. auch O. Perron, Math. Ann. **104** (1930), S. 139—142.

Ore.

XXIV.

Zur Theorie der Ideale.

[Nachrichten von der Königlichen Gesellschaft der Wissenschaften zu Göttingen, Mathem.-phys. Klasse, Jahrgang 1894, S. 272—277.]

Nachdem es mir in den Jahren 1869 und 1870 endlich gelungen war, durch Einführung neuer Begriffe die letzten Schwierigkeiten zu überwinden, welche sich meinen früheren Versuchen, eine strenge und ausnahmelose Theorie der Ideale zu begründen, entgegengestellt hatten, diente mir die hiermit gewonnene Grundlage in den nächstfolgenden Jahren teils zur Untersuchung spezieller, insbesondere der kubischen Körper, teils zur Erforschung der allgemeinen Gesetze, welche die Beziehungen zwischen den Idealen verschiedener Körper beherrschen. Die letztere Frage, welche im wesentlichen auf die Betrachtung derjenigen Körper zurückkommt, die ich Galoissche Körper oder Normalkörper genannt habe, bot keine erheblichen Schwierigkeiten dar und konnte daher bald zu einem vollständigen Abschluß gebracht werden. Von der Veröffentlichung dieser Untersuchung bin ich immer durch andere Beschäftigungen abgezogen, und nur gelegentlich habe ich ihrer Erwähnung getan, z. B. im § 27 meiner Schrift Sur la théorie des nombres entiers algébriques (1877), wo ich den Satz ausgesprochen habe, daß aus den Idealen eines Normalkörpers die Ideale eines jeden in ihm als Divisor enthaltenen Körpers nach bestimmten Gesetzen abgeleitet werden können, und wo auch an einem sehr einfachen Beispiel die Kraft dieser von mir gefundenen Gesetze dargelegt ist*). Dies hat Herrn Frobenius, wie er mir in einem Schreiben vom 3. Juni 1882 aus Zürich mitteilte, zur selbständigen Durchforschung des Gegenstandes angeregt, durch welche er, wie sich bald herausstellte, zu einer

*) Vgl. auch Compte rendu der Pariser Akademie vom 24. Mai 1880, und die Anmerkung auf S. 618 der vierten Auflage von Dirichlets Vorlesungen über Zahlentheorie (1894).

nahezu vollständigen Übereinstimmung mit mir gelangt war; da er zugleich wegen einer Nebenfrage eine Mitteilung meiner Resultate wünschte, so verfaßte ich in der Eile eine kurze Übersicht derselben und fügte sie am 8. Juni meiner Antwort bei. Obgleich nun vor kurzem Herr Hilbert seine auf denselben Gegenstand bezügliche Untersuchung in diesen Nachrichten (7. Juli 1894) veröffentlicht hat, so erlaube ich mir doch, die eben erwähnte Übersicht, weil in ihr die Zerlegungen der Ideale noch allgemeiner ausgeführt sind*), ohne jeden Zusatz, nur mit Auslassung einiger unwesentlicher Worte jetzt mitzuteilen.

Einige Sätze aus der Untersuchung der Beziehungen zwischen den Idealen in verschiedenen Körpern.

I. Ideale in Normalkörpern.

Bezeichnungen:

Ω ein Normalkörper vom Grade n.

Φ die Gruppe aller n Permutationen φ, durch welche Ω in sich selbst übergeht. — Bedeutet z irgendein System von Zahlen des Körpers Ω oder auch eine einzelne solche Zahl, so bezeichne ich durch das Symbol $z\varphi$ das durch die Permutation φ aus z hervorgehende System**).

$\mathfrak{o}$ das Gebiet aller ganzen Zahlen ω des Körpers Ω. — Wenn ich in einer Gleichung oder Kongruenz den Buchstaben ω benutze, so will ich damit sagen, daß sie für jede in $\mathfrak{o}$ enthaltene Zahl ω, also gewissermaßen identisch gilt.

$\mathfrak{p}$ ein Primideal des Körpers Ω.

p die durch $\mathfrak{p}$ teilbare positive rationale Primzahl.

---

*) Auch die auf S. 235 von Herrn Hilbert aufgestellten Sätze über Partialdiskriminanten — von welchen die folgende Übersicht unmittelbar gar nicht handelt — scheinen die Allgemeinheit derjenigen Resultate nicht ganz zu erreichen, zu welchen ich durch die am Schlusse der Einleitung zu meiner Abhandlung Über die Diskriminanten endlicher Körper (1882) erwähnte Untersuchung gelangt war; auf diese gedenke ich später einzugehen. Dagegen ist mir die von Herrn Hilbert ausgeführte weitere Zerlegung der von ihm mit g_t, von mir mit X bezeichneten Gruppe neu gewesen.

**) Die im Originale benutzte Bezeichnung $z|\varphi$ ersetze ich hier durch die einfachere, welche ich in § 161 der vierten Auflage von Dirichlets Vorlesungen über Zahlentheorie (1894) eingeführt habe.

X die Gruppe aller derjenigen g Permutationen χ, für welche (identisch)

$$\omega\chi \equiv \omega \pmod{\mathfrak{p}}.$$

Dann gibt es eine Permutation

ψ_0 (oder vielmehr genau g solche Permutationen $\chi\psi_0$), für welche

$$\omega^p \equiv \omega\psi_0 \pmod{\mathfrak{p}}.$$

Daraus folgen die Eigenschaften:

$$\psi_0^{-1} X \psi_0 = X, \text{ d. h. } X\psi_0 = \psi_0 X,$$

und der Grad von $\mathfrak{p}$ ist der kleinste positive Exponent

f, für welchen

$$X\psi_0^f = X, \text{ d. h. } \psi_0^f \text{ in } X \text{ enthalten.}$$

Also

$$N(\mathfrak{p}) = p^f.$$

Ferner ist die Gruppe (Bezeichnungsweise von Galois)

$$\Psi = X + X\psi_0 + X\psi_0^2 + \cdots + X\psi_0^{f-1} \text{ (vom Grade } fg)$$

der Inbegriff aller derjenigen Permutationen ψ, welche der Bedingung

$$\mathfrak{p}\psi = \mathfrak{p}$$

genügen (d. h. die Gruppe, zu welcher $\mathfrak{p}$ gehört). Setzt man endlich

$$\Phi = \Psi\varphi_1 + \Psi\varphi_2 + \cdots + \Psi\varphi_e, \text{ also } n = efg,$$

so entspricht jedem dieser e Komplexe $\Psi\varphi_s$ ein mit $\mathfrak{p}$ konjugiertes Primideal

$$\mathfrak{p}_s = \mathfrak{p}\varphi_s;$$

diese e Primideale

$$\mathfrak{p}_1, \mathfrak{p}_2 \cdots \mathfrak{p}_e$$

sind verschieden voneinander, und es ist

$$\mathfrak{o}\mathfrak{p} = (\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_e)^g$$

$$N(\mathfrak{p}_s) = p^f \text{ (unabhängig von } s).$$

Wird $\mathfrak{p}$ durch $\mathfrak{p}_s$ ersetzt, so ist X, ψ_0, Ψ zu ersetzen durch $X_s = \varphi_s^{-1} X \varphi_s$, $\psi_{s,0} = \varphi_s^{-1}\psi_0\varphi_s$, $\Psi_s = \varphi_s^{-1}\Psi\varphi_s$.

II. Ideale in den Divisoren eines Normalkörpers Ω.

Kennt man die (in I erörterte) Konstitution aller Primideale $\mathfrak{p}$ des Normalkörpers Ω, so folgt daraus für jeden in Ω als Divisor enthaltenen Körper

Ω' durch alleinige Anwendung von Gruppen-Zerlegungen (also gewissermaßen aus rein algebraischen Prinzipien) die vollständige Kenntnis aller Primideale

$\mathfrak{p}'$ in Ω'. Die Bezeichnungen in I werden beibehalten. Bekannt ist:

Ω' gehört zu einer Permutations-Gruppe

Φ', bestehend aus allen denjenigen m (in Φ enthaltenen) Permutationen φ', die jede in Ω' enthaltene Zahl ungeändert lassen; dann ist

$$n = mn',$$

und n' ist der Grad von Ω' (umgekehrt, wenn Φ' eine in Φ enthaltene Gruppe ist, so gibt es immer einen, und nur einen zugehörigen Körper Ω'). Es wird daher das erstrebte Ziel lediglich durch Vergleichung von Φ' mit den in I betrachteten Permutationen und Gruppen erreicht. Dazu dient zunächst folgendes, was weniger oder zum Teil gar nicht bekannt scheint.

Bedeutet φ_r eine bestimmte Permutation, so bezeichne ich mit $\Psi\varphi_r\Phi'$ den Komplex aller voneinander verschiedenen Permutationen von der Form $\psi\varphi_r\varphi'$, wo ψ, φ' resp. alle in den Gruppen Ψ, Φ' enthaltenen Permutationen durchlaufen; ist h_r der Grad des größten gemeinschaftlichen Teilers Ψ'_r der Gruppen $\varphi_r^{-1}\Psi\varphi_r = \Psi_r$ und Φ' (d. h. besteht Ψ'_r aus h_r Permutationen), so werden immer je h_r Produkte $\psi\varphi_r\varphi'$ identisch, und das Produkt aus den Graden der Gruppen Ψ, Φ' (hier fg und m) ist daher das h_r-fache von der Anzahl der in $\Psi\varphi_r\Phi'$ enthaltenen Permutationen. Da ferner zwei solche Komplexe $\Psi\varphi_r\Phi'$, $\Psi\varphi_s\Phi'$ entweder ganz identisch sind, oder keine einzige gemeinschaftliche Permutation haben, so kann man setzen:

$$\Phi = \Psi\varphi_1\Phi' + \Psi\varphi_2\Phi' + \cdots + \Psi\varphi_{e'}\Phi'.$$

Dies ist, beiläufig gesagt, die Grundlage für die Untersuchung der algebraischen Reziprozität zwischen zwei beliebigen endlichen Körpern, nämlich denen, welche zu den Gruppen Ψ und Φ' gehören (Einwirkung zweier beliebigen irreduziblen Gleichungen aufeinander, Zerlegung jeder in e' Faktoren). Zugleich ist

$$\Phi = \Phi'\varphi_1^{-1}\Psi + \cdots + \Phi'\varphi_{e'}^{-1}\Psi.$$

Diese allgemeine Zerlegung einer Gruppe Φ nach zwei in ihr enthaltenen Gruppen Ψ, Φ' gibt für unseren Fall alles, was wir wünschen, durch folgende Bestimmungen.

Es sei φ_r eine bestimmte der in der obigen Zerlegung benutzten e' Permutationen $\varphi_1, \varphi_2 \cdots \varphi_{e'}$, und

$\mathfrak{p}_r = \mathfrak{p}\varphi_r$,

$\mathfrak{p}'_r$ das durch $\mathfrak{p}_r$ teilbare Primideal in Ω',

g_r der Grad des größten gemeinsamen Teilers

X'_r von $X_r = \varphi_r^{-1} X \varphi_r$ und Φ', daher

a_r definiert durch $g = a_r g_r$, so ist

$$\mathfrak{o}' p = \mathfrak{p}_1'^{a_1} \mathfrak{p}_2'^{a_2} \cdots \mathfrak{p}_{e'}'^{a_{e'}}, \quad \text{wo}$$

$\mathfrak{o}'$ das System aller ganzen Zahlen des Körpers Ω'.

Die Anzahl e' der Komplexe $\Psi \varphi_r \Phi'$, aus denen Φ besteht, ist daher zugleich die Anzahl aller voneinander verschiedenen, in p aufgehenden Primideale $\mathfrak{p}'_1, \mathfrak{p}'_2 \cdots \mathfrak{p}'_{e'}$ des Körpers Ω', und die Zerlegung von p in diesem Körper ist gefunden; die Bestimmung der Normen dieser Primideale $\mathfrak{p}'$ und ihre Zerlegung in Ω folgt jetzt. Es sei, wie oben,

Ψ'_r der größte gemeinsame Teiler der Gruppen

$\Psi_r = \varphi_r^{-1} \Psi \varphi_r$ und Φ',

h_r der Grad von Ψ'_r, folglich

$$\Phi' = \Psi'_r \varphi'_{r,1} + \Psi'_r \varphi'_{r,2} + \cdots + \Psi'_r \varphi'_{r,e_r}; \quad m = h_r e_r,$$

$\mathfrak{p}_{r,s} = \mathfrak{p}_r \varphi'_{r,s}$, so ist

$$\mathfrak{o}\mathfrak{p}'_r = (\mathfrak{p}_{r,1}\mathfrak{p}_{r,2} \cdots \mathfrak{p}_{r,e_r})^{g_r}$$

$$e_1 + e_2 + \cdots + e_{e'} = e.$$

Hiermit ist die Zerlegung erledigt (die letzte Gleichung folgt daraus, daß $e_r f g$ die Anzahl der in $\Psi \varphi_r \Phi'$ enthaltenen Permutationen ist). Endlich: da X'_r auch der größte gemeinsame Teiler von X_r und Ψ'_r ist (weil X_r Divisor von Ψ_r), so ist h_r teilbar durch g_r, also

f_r definiert durch $h_r = f_r g_r$,

und nach der obigen Regel besteht der Komplex $X_r \Psi'_r$ aus $f_r g$ Permutationen, welche alle in Ψ_r enthalten sind (weil X_r und Ψ'_r Divisoren von Ψ_r), und da dieser Komplex $X_r \Psi'_r$ zugleich eine Gruppe ist (weil $X_r \psi_r = \psi_r X_r$), so ist fg (als Grad von Ψ_r) teilbar durch $f_r g$ (als Grad von $X_r \Psi'_r$), mithin

f'_r definiert durch $f = f_r f'_r$. Dann ist

$$N'(\mathfrak{p}'_r) = (\mathfrak{o}', \mathfrak{p}'_r) = p^{f'_r}$$

und

$$\mathfrak{N}(\mathfrak{p}_{r,s}) = \mathfrak{p}_r'^{f_r} \quad \text{(unabhängig von } s\text{)},$$

wo $\mathfrak{N}$ das Symbol für die in bezug auf Ω' genommene Partialnorm von Zahlen oder Idealen des Körpers Ω bedeutet. — Sind Ω, Ω' zwei beliebige endliche Körper, so gehört zu jedem Ideal $\mathfrak{a}$ des Körpers Ω ein bestimmtes Ideal $\mathfrak{a}' = \mathfrak{N}(\mathfrak{a})$ des Körpers Ω', die Partialnorm von $\mathfrak{a}$ nach Ω', und es ist $\mathfrak{N}(\mathfrak{a}\mathfrak{b}) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b})$.

III. Verallgemeinerung.

Dieselben Sätze gelten ohne nennenswerte Wortänderung, wenn man an Stelle des Körpers R der rationalen Zahlen einen beliebigen endlichen Körper P setzt, und unter Ω einen endlichen Körper versteht, welcher P als einen Divisor enthält, und zwar ein Normalkörper in bezug auf P ist (d. h. daß Ω durch alle diejenigen Permutationen, welche jede Zahl in P ungeändert lassen, in sich selbst übergeht). Für die Zerlegung der Primideale p des Körpers P in Primideale $\mathfrak{p}$ des Körpers Ω gelten genau dieselben Gesetze wie in I. Sind ferner alle diese Zerlegungen bekannt, so erhält man daraus nach den in II angegebenen Gesetzen sowohl die Zerlegung jedes Primideals p in Primideale $\mathfrak{p}'$ eines Körpers Ω', welcher Multiplum von P und Divisor von Ω ist, als auch die Zerlegung dieser Primideale $\mathfrak{p}'$ in Primideale $\mathfrak{p}$ des Körpers Ω Und diese Verallgemeinerung kann noch weiter getrieben werden.

8. Juni 1882.

Erläuterungen zur vorstehenden Abhandlung.

Durch die Hilbertsche Abhandlung: Grundzüge einer Theorie des Galoisschen Zahlkörpers, Göttinger Nachrichten 1894, S. 224—236, veranlaßt, publizierte Dedekind seine früheren Untersuchungen über denselben Gegenstand. Während er die von Hilbert eingeführten Verzweigungsgruppen nicht studiert hat, gehen seine Resultate über die Primidealzerlegung in beliebigen Unterkörpern wesentlich über Hilbert hinaus. Ausführlichere Darstellungen dieser Theorie findet man bei P. Bachmann, Allgemeine Arithmetik der Zahlenkörper, Kap. 12, Leipzig 1905; H. Hasse, Jahresbericht der Deutschen Mathematikervereinigung **36** (1927), S. 233—311; man vgl. auch den Hilbertschen Bericht, Jahresbericht der Deutschen Mathematikervereinigung **4** (1897), S. 247—263.

Die weiteren Untersuchungen über den Zusammenhang zwischen Idealen und Gruppeneigenschaften behandeln meistens die Struktur der Verzweigungsgruppen. Zu erwähnen sind: F. Hüttig, Arithmetische Theorie eines Galoisschen Körpers, Diss. Marburg 1907; R. Fueter, Vierteljahrsschrift d. Naturf. Ges. in Zürich 1917, S. 67—72; A. Speiser, Journ. f. Math. **149** (1919), S. 174—188; T. Rella, Journ. f. Math. **150** (1920), S. 157—174; Ö. Ore, Math. Ann. **100** (1928), S. 650—673; **102** (1929), S. 283—304; Am. Math. Soc. **30** (1928), S. 610—620. Die in der Einleitung erwähnten Untersuchungen von Frobenius sind in den Sitzungsber. d. Berl. Akad. von 1896, erster Teilband, S. 689—703 erschienen.

Eine Untersuchung der gegenseitigen Reduktion zweier Polynome in dem von Dedekind auf S. 46 angedeuteten Sinne ist von Landsberg, Loewy, Takagi und M. Bauer durchgeführt; man vgl. die Darstellung in O. Haupt, Einführung in die Algebra, Leipzig 1929, S. 540—545.

Ore.

XXV.

Über die Begründung der Idealtheorie.

[Nachrichten von der Königlichen Gesellschaft der Wissenschaften zu Göttingen, Mathem.-phys. Klasse, Jahrgang 1895, S. 106—113.]

Von mehreren Seiten bin ich aufgefordert, meine Ansicht zu äußern über die kürzlich in diesen Nachrichten (1894, Nr. 4) von Herrn Hurwitz veröffentlichte Begründung der Idealtheorie und über deren Beziehungen zu der in der vierten Auflage von Dirichlets Zahlentheorie (welche ich im folgenden mit D. bezeichnen will) enthaltenen Darstellung desselben Gegenstandes. Wenn ich nun hierauf erkläre, daß ich der letzteren, also der meinigen den Vorzug gebe, so glaube ich diese Meinung ganz unbefangen aussprechen zu dürfen, weil ich schon im Februar 1887 denselben Weg wie Herr Hurwitz mit demselben Erfolge eingeschlagen habe, und weil ich erst von hieraus im November 1888 mit Hilfe neuer Beweismittel zu derjenigen Darstellung gelangt bin, welche ich später (1893) in das Werk von Dirichlet aufgenommen habe. Ich erlaube mir, im folgenden diesen Hergang etwas genauer zu beschreiben, weil die hierbei auftretende Einkleidung ein und desselben Grundgedankens in äußerlich verschiedene Formen wohl von allgemeinerem Interesse ist.

In § 172 der dritten Auflage der Zahlentheorie und ebenso in § 23 meiner Schrift Sur la théorie des nombres entiers algébriques habe ich hervorgehoben, daß die größte Schwierigkeit, welche bei der Begründung der Idealtheorie zu überwinden war, in dem Beweise des folgenden Satzes bestand:

1. Ist das Ideal $\mathfrak{c}$ teilbar*) durch das Ideal $\mathfrak{a}$, so gibt es ein Ideal $\mathfrak{b}$, welches der Bedingung $\mathfrak{a}\mathfrak{b} = \mathfrak{c}$ genügt (vgl. D. S. 553, VII).

*) Dieses Wort gebrauche ich, wie bisher immer, in dem Sinne, daß jede Zahl des Ideals $\mathfrak{c}$ auch in $\mathfrak{a}$ enthalten ist; ich muß, um Verwirrung zu vermeiden, hierauf aufmerksam machen, weil Herr Hurwitz in seinem Aufsatz (II, 5) mit demselben Worte gerade die im Nachsatz ausgesprochene Beziehung zwischen $\mathfrak{c}$ und $\mathfrak{a}$ bezeichnet.

Daß dieser Satz, durch welchen der Zusammenhang zwischen der Teilbarkeit und der Multiplikation der Ideale festgestellt wird, bei der damaligen Darstellung erst nahezu am Schlusse der Theorie beweisbar wurde, machte sich in der drückendsten Weise fühlbar, besonders dadurch, daß einige der wichtigsten Sätze nur allmählich durch schrittweise Befreiung von beschränkenden Voraussetzungen zu der ihnen zukommenden Allgemeinheit erhoben werden konnten. Ich bin daher im Laufe der Jahre öfter auf diesen Kardinalpunkt mit der Absicht zurückgekommen, einen einfachen, unmittelbar an den Begriff der ganzen Zahl anknüpfenden Beweis des Satzes 1 oder eines der drei folgenden Sätze zu gewinnen, welche, wie man leicht erkennt, von gleicher Bedeutung für die Begründung der Theorie sind:

2. Jedes Ideal $\mathfrak{m}$ kann durch Multiplikation mit einem Ideal $\mathfrak{n}$ in ein Hauptideal verwandelt werden (vgl. D. S. 554, IX).

3. Jeder endliche, von Null verschiedene Modul $\mathfrak{m}$, der aus ganzen oder gebrochenen algebraischen Zahlen besteht, kann durch Multiplikation mit einem Modul $\mathfrak{n}$, dessen Zahlen aus denen von $\mathfrak{m}$ auf rationale Weise gebildet sind, in einen Modul $\mathfrak{mn}$ verwandelt werden, welcher die Zahl 1 enthält und aus lauter ganzen Zahlen besteht (vgl. D. S. 528, VI).

4. Aus je m algebraischen Zahlen μ_r, die nicht alle verschwinden, kann man auf rationale Weise m Zahlen ν_s, ableiten, welche der Gleichung

$$\mu_1\nu_1 + \mu_2\nu_2 + \cdots + \mu_m\nu_m = 1$$

und außerdem der Bedingung genügen, daß alle m^2 Produkte $\mu_r\nu_s$ ganze Zahlen sind (vgl. D. S. 530, VII).

Wenn nun auch diese vier Sätze insofern vollständig gleichwertig sind, als jeder von ihnen ohne jede Schwierigkeit aus jedem der drei übrigen abgeleitet werden kann*), so geschieht es doch in solchen Fällen nicht selten, daß der eine Satz durch seine einfachere Fassung einem direkten Beweise leichter zugänglich wird als die anderen. In dem vorliegenden Beispiel zeichnet sich offen-

*) Um dies einzusehen, braucht man nur die hinter den Sätzen bemerkten Zitate zu verfolgen und zu bedenken, daß jeder endliche algebraische Modul $\mathfrak{m}$ durch Multiplikation mit einer geeigneten, von Null verschiedenen Zahl in einen ganzen Modul, und jeder von Null verschiedene ganze Modul eines endlichen Körpers durch Multiplikation mit jedem Ideal in ein Ideal verwandelt wird.

bar der Satz 4 oder auch der Satz 3, welcher sich von jenem nur äußerlich durch die Benutzung des Modulbegriffs unterscheidet, an Einfachheit vor den Sätzen 1 und 2 aus, in welchen der kompliziertere Begriff des Ideals auftritt. Es ist mir dann auch bald gelungen, den Satz 3 wenigstens für zweigliedrige Moduln $\mathfrak{m}$, also den Satz 4 für den Fall $m = 2$ zu beweisen, und zwar stimmt dieser Beweis, auf welchen ich unten zurückkommen werde, wesentlich mit demjenigen überein, welchen ich später in das Werk von Dirichlet (D. S. 529) aufgenommen habe. Aber es gelang mir damals nicht, diese Methode auf drei- und mehrgliedrige Moduln $\mathfrak{m}$ auszudehnen.

Eine neue Anregung zur Beschäftigung mit diesem Gegenstande empfing ich im Frühjahr 1882 durch die große Abhandlung „Grundzüge einer arithmetischen Theorie der algebraischen Größen“ von Leopold Kronecker. Das Studium derselben veranlaßte mich, eine Reihe von „bunten Bemerkungen“ aufzuschreiben, von denen Nr. 20 sich auf den für mich wichtigsten § 14, also auf die Begründung der Idealtheorie bezieht. Obgleich ich mich mit dem hier auftretenden „methodischen Hilfsmittel der unbestimmten Koeffizienten“ nicht befreunden konnte, so suchte ich doch in das Wesen der Methode einzudringen, um womöglich daraus einen Nutzen für meine Auffassung der Theorie zu ziehen, weil in dem hier gewonnenen Resultate auch der obige Satz 3 oder 4 offenbar enthalten ist. Nun schien und scheint mir noch heute in der Beweisführung Kroneckers eine Lücke oder wenigstens eine zweifelhafte Stelle zu sein; setzt man unter sonstiger Beibehaltung der dortigen Bezeichnungen der Kürze wegen

(1) $$(x + u'x' + u''x'' + \cdots)G = F$$

und

(2) $$(x + v'x' + v''x'' + \cdots)G = Q,$$

so ist G eine ganze Funktion der unbestimmten Größen u, während Q außerdem von den unbestimmten Größen v abhängt, und wenn ich die etwas dunkle Stelle richtig verstehe, so soll bewiesen werden, daß alle Koeffizienten dieser Funktion Q ganze Größen des hier betrachteten Bereichs ($\mathfrak{R}$) sind. Nun wird zwar gezeigt, daß Q einer Gleichung von der Form

(3) $$Q^n + C_1Q^{n-1} + \cdots + C_{n-1}Q + C_n = 0$$

genügt, wo C_1, $C_2 \cdots C_n$ ebenfalls ganze, und zwar solche ganze Funktionen der Variablen u, v bedeuten, deren Koeffizienten ganze Größen in $(\mathfrak{R})$ sind; aber es bedarf meiner Ansicht nach doch noch eines besonderen Beweises, daß sich hieraus die oben bezeichnete Eigenschaft der Koeffizienten von Q als notwendige Folge ergibt; ich habe wenigstens in den vorausgehenden §§ 1 bis 13 keine Stelle gefunden, aus welcher dies hervorgeht. Für den vorzugsweise mich interessierenden Fall, wo der Bereich $(\mathfrak{R})$ der Körper aller algebraischen Zahlen ist, also keine Variablen enthält, gelang es mir auch, einen solchen Beweis zu finden, den ich hier aber nur andeuten will, weil er in der Folge nicht weiter verwendet wird. Man sieht leicht ein, daß der fragliche Satz zufolge (3) auf den folgenden zurückkommt: „Wenn eine ganze rationale Funktion Q von Variablen stets eine ganze (algebraische) Zahl wird, sobald diese Variablen ganze Zahlen werden, so ist auch jeder Koeffizient der Funktion Q eine ganze Zahl.“ Und diesen Satz bewies ich, freilich auf eine ziemlich künstliche Weise, indem ich für die Variablen beliebige Wurzeln der Einheit einsetzte. Durch diese Vervollständigung der Beweisführung von Kronecker war nun, wie schon oben bemerkt, auch zugleich für den Satz 3 ein Beweis gewonnen, welcher von meiner bisherigen Idealtheorie unabhängig war und folglich zu einer neuen Begründung derselben dienen konnte. Aber dieser Weg entspricht durchaus nicht meinen Wünschen, teils weil die Benutzung der Funktionen von Variablen mir immer als ein der Sache fremdes Hilfsmittel erscheint, teils weil die Durchführung aller Beweise ohne Zweifel einen größeren Raum erfordert als in meiner damaligen Theorie.

So ruhte diese Frage mehrere Jahre ohne jeden Fortschritt, und sie kam erst aufs neue in Bewegung, als mein Freund H. Weber mir am 10. Februar 1887 von Marburg aus eine von ihm ausgearbeitete „Theorie der algebraischen Zahlen nach Kronecker“ zuschickte, in welcher die Hauptsätze ausführlich und vollständig bewiesen wurden. Bei angestrengtem Nachdenken über diese Darstellung fand ich nun am 15. Februar den folgenden Satz, durch welchen nach meiner Ansicht die Theorie von Kronecker noch eine wesentliche Vereinfachung gewinnt:

5. Wenn das Produkt GH aus zwei ganzen rationalen Funktionen G, H von beliebig vielen unabhängigen Variablen u lauter

ganze Koeffizienten hat, so ist auch jedes Einzelprodukt aus jedem Koeffizienten von G und jedem Koeffizienten von H eine ganze Größe.

Um nämlich zu beweisen, daß die oben mit Q bezeichnete Funktion lauter ganze Koeffizienten hat, braucht man nicht mehr, wie es bei Kronecker geschieht, die Gleichung (3) zu bilden, welcher Q genügt, sondern dies folgt jetzt unmittelbar daraus, daß das Produkt F in (1) lauter ganze Koeffizienten hat, also auch jedes Produkt aus jeder Größe x, x', $x''\cdots$ und aus jedem Koeffizienten der Funktion G ganz ist.

Diese Bemerkung und ein vollständiger Beweis des Satzes 5 bildeten den Hauptinhalt meiner am 20. Februar 1887 abgesendeten Antwort an H. Weber; dieser Beweis ist später in § 3 meiner Abhandlung „Über einen arithmetischen Satz von Gauß“ veröffentlicht, welche sich in den Mitteilungen der Deutschen mathematischen Gesellschaft in Prag (1892) findet, und auf S. 7 daselbst, ebenso auch in der Vorrede zur vierten Auflage von Dirichlets Zahlentheorie, habe ich auch die Wichtigkeit des Satzes 5 für die Theorie von Kronecker besonders betont. Herr Hurwitz, dem diese Abhandlung erst nach Abschluß seiner Arbeit bekannt geworden ist, knüpft an denselben Satz 5 an, für welchen er einen andern Beweis gibt, und leitet daraus den Satz 2 ab. Ebenso weise ich in meinem Briefe vom 20. Februar 1887 wieder darauf hin, daß der zur Abkürzung meiner Idealtheorie brauchbare Satz 3 eine unmittelbare Folge des Satzes 5 ist, aber dies geschieht mit dem ausdrücklichen Zusatz, ich würde mir zehnmal überlegen, wie eine solche Abkürzung durchzuführen sei, ohne den einheitlichen Charakter der Theorie zu stören!

Hiermit komme ich zum letzten Teile meiner Erzählung. Ich erinnere zunächst an eine schöne Stelle der Disquisitiones Arithmeticae, die schon in meiner Jugend den tiefsten Eindruck auf mich gemacht hat. Im Art. 76 berichtet Gauß, daß der Wilsonsche Satz zuerst von Waring bekanntgemacht ist, und fährt fort: Sed neuter demonstrare potuit, et cel. Waring fatetur demonstrationem eo difficiliorem videri, quod nulla notatio fingi possit, quae numerum primum exprimat. — At nostro quidem judicio hujusmodi veritates ex notionibus potius quam ex notationibus hauriri debebant. — In diesen letzten Worten liegt, wenn sie im allgemeinsten Sinne genommen werden, der Ausspruch eines

großen wissenschaftlichen Gedankens. die Entscheidung für das Innerliche im Gegensatz zu dem Äußerlichen. Dieser Gegensatz wiederholt sich auch in der Mathematik auf fast allen Gebieten; man denke nur an die Funktionentheorie, an Riemanns Definition der Funktionen durch innerliche charakteristische Eigenschaften, aus welchen die äußerlichen Darstellungsformen mit Notwendigkeit entspringen. Aber auch auf dem bei weitem enger begrenzten und einfacheren Gebiete der Idealtheorie kommen beide Richtungen zur Geltung, und ich habe mich an verschiedenen Stellen meiner oben erwähnten Schrift Sur la théorie des nombres entiers algébriques (am Schluß von § 12 und namentlich in der Einleitung) so ausführlich über die Anforderungen ausgesprochen, die ich mir damals wie heute bei dem Aufbau der Theorie stellte, daß ich nicht mehr darauf zurückzukommen brauche. Hiernach wird man es auch erklärlich finden, daß ich meiner Definition des Ideals durch eine charakteristische innerliche Eigenschaft den Vorzug gebe vor derjenigen durch eine äußerliche Darstellungsform, von welcher Herr Hurwitz in seiner Abhandlung (II, 1) ausgeht. Aus denselben Gründen konnte der oben erwähnte Beweis des Satzes 3, welcher sich auf den Satz 5 stützt, mich noch nicht völlig befriedigen, weil durch die Einmischung der Funktionen von Variablen die Reinheit der Theorie nach meiner Ansicht getrübt wird, und ich will jetzt berichten, auf welchem Wege es mir gelungen ist, das erstrebte Ziel zu erreichen.

Der am 15. Februar 1887 von mir gefundene Beweis des Satzes 5 geht so zu Werke (vgl. § 3 der Prager Abhandlung), daß zunächst der folgende sehr spezielle Fall bewiesen wird, in welchem der eine Faktor eine lineare Funktion ist:

6. Hat die ganze Funktion

$$f(x) = c_0 x^n + c_1 x^{n-1} + \cdots + c_n$$

lauter ganze Koeffizienten, so gilt dasselbe von der ganzen Funktion

$$\frac{f(x)}{x - \omega} = a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n,$$

wo ω eine Wurzel der Gleichung $f(\omega) = 0$ bedeutet.

Vergleicht man aber den Beweis dieses speziellen Satzes mit dem zu Anfang erwähnten, viel früher gefundenen Beweise (D. S. 529) des speziellen Falles des Satzes 3, in welchem m ein zwei-

gliedriger Modul $[\alpha, \beta]$ ist, so erkennt man leicht ihre vollständige Identität; denn wenn man $\alpha = \beta\omega$ setzt, so stimmt die Reihe der n Produkte $\beta\nu_r$, welche in dem letzteren auftreten, mit den obigen Koeffizienten a_r überein*). Da nun der vollständige Beweis des Satzes 5 (für Funktionen von einer Variablen, deren Betrachtung hier genügt) sich lediglich durch eine wiederholte Anwendung des speziellen Satzes 6 ergibt, so lag die Vermutung nahe, daß auch der allgemeine Satz 3 oder 4 durch wiederholte Anwendung des speziellen Falles, wo $\mathfrak{m}$ ein zweigliedriger Modul, oder $m = 2$ ist, sich würde ableiten lassen. Bei erneuter Beschäftigung mit dieser Frage ergab sich dies in der Tat am 22. Oktober 1888, und zwar auf folgende unerwartet einfache Weise durch die vollständige Induktion.

Ist n eine natürliche Zahl, und nimmt man an, der Satz 4 sei schon für alle Fälle bewiesen, wo $m < n + 2$, so kann man aus $n + 2$ gegebenen algebraischen Zahlen

$$\alpha,\ \beta,\ \mu_1,\ \mu_2 \cdots \mu_n$$

auf rationale Weise $2n + 4$ Zahlen

$$\begin{gathered} \alpha',\ \beta', \\ \alpha'',\ \nu_1,\ \nu_2 \cdots \nu_n, \\ \beta'',\ \varrho_1,\ \varrho_2 \cdots \varrho_n \end{gathered}$$

ableiten, welche den drei Gleichungen

$$\begin{aligned} &\alpha\alpha' + \beta\beta' = 1, \\ &\alpha\alpha'' + \mu_1\nu_1 + \cdots + \mu_n\nu_n = 1, \\ &\beta\beta'' + \mu_1\varrho_1 + \cdots + \mu_n\varrho_n = 1 \end{aligned} \tag{4}$$

und zugleich den Bedingungen genügen, daß alle Produkte

$$\begin{gathered} \alpha\alpha',\ \alpha\beta',\quad \beta\alpha',\ \beta\beta', \\ \alpha\alpha'',\ \alpha\nu_r,\ \mu_r\alpha'',\ \mu_r\nu_s, \\ \beta\beta'',\ \beta\varrho_r,\ \mu_r\beta'',\ \mu_r\varrho_s \end{gathered} \tag{5}$$

ganze Zahlen werden, wo r, s beliebige Zahlen aus der Reihe $1, 2 \cdots n$ bedeuten. Setzt man nun

$$\alpha''' = \alpha\alpha'\alpha'',\ \beta''' = \beta\beta'\beta'',\ \sigma_r = \alpha\alpha'\nu_r + \beta\beta'\varrho_r,$$

*) Es ist dies dieselbe Zahlenreihe, welche mir schon früher bei verschiedenen Gelegenheiten gute Dienste geleistet hatte (vgl. z. B. den Schluß von § 8 meiner Abhandlung Über die Diskriminanten endlicher Körper oder D. § 167).

so sind auch diese $n + 2$ Zahlen aus den gegebenen auf rationale Weise gebildet; zufolge (4) befriedigen sie die Gleichung

$$\alpha\alpha''' + \beta\beta''' + \mu_1\sigma_1 + \cdots + \mu_n\sigma_n = 1,$$

und zufolge (5) sind alle Produkte

$$\begin{array}{lll} \alpha\alpha''', & \alpha\beta''', & \alpha\sigma_r, \\ \beta\alpha''', & \beta\beta''', & \beta\sigma_r, \\ \mu_r\alpha''', & \mu_r\beta''', & \mu_r\sigma_s \end{array}$$

ganze Zahlen, weil sie in der Form

$$\begin{array}{ll} \alpha\alpha'\cdot\alpha\alpha'', & \alpha\beta'\cdot\beta\beta'', \quad \alpha\alpha'\cdot\alpha\nu_r + \alpha\beta'\cdot\beta\varrho_r, \\ \alpha\alpha''\cdot\beta\alpha', & \beta\beta'\cdot\beta\beta'', \quad \alpha\nu_r\cdot\beta\alpha' + \beta\beta'\cdot\beta\varrho_r, \\ \alpha\alpha'\cdot\mu_r\alpha'', & \beta\beta'\cdot\mu_r\beta'', \quad \alpha\alpha'\cdot\mu_r\nu_s + \beta\beta'\cdot\mu_r\varrho_s \end{array}$$

darstellbar sind, w. z. b. w.

Hiermit war endlich das, was ich so lange gesucht hatte, ein wirklich sachgemäßer Beweis der Sätze 3 und 4, also auch die Grundlage für die Neugestaltung meiner Idealtheorie gefunden. Indessen war ich auch mit diesem Induktionsbeweise noch nicht ganz zufrieden, weil in ihm die mechanische Rechnung vorherrscht, und bei längerem Nachdenken über den eigentlichen Grund seines Erfolges entdeckte ich am 9. November 1888 den allgemeinen Modulsatz

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

woraus die schließliche Form des Beweises entsprang (D. S. 530). Ich bemerke beiläufig, daß statt des dortigen Moduls

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

auch der Modul

$$\mathfrak{n} = \mathfrak{a}\mathfrak{b}'\mathfrak{c}' + \mathfrak{b}\mathfrak{c}'\mathfrak{a}' + \mathfrak{c}\mathfrak{a}'\mathfrak{b}'$$

hätte gewählt werden können, dessen Bau wohl etwas einfacher ist und sich genauer an den vorstehenden Induktionsbeweis anschließt; doch ziehe ich die erstere Wahl vor, weil bei der letzteren der Beweis, daß der Modul $\mathfrak{z} = [1]$ durch $\mathfrak{m}$ teilbar ist, sich weniger einfach gestaltet.

Bedenkt man nun, mit wie wenigen Schritten man jetzt (D. § 173) von dem Begriffe der ganzen Zahl zu dem Satze 3 und hiermit zur vollen Beherrschung der Idealtheorie gelangt, so kann, wie ich meine, gar kein Zweifel darüber bestehen, daß dieser Weg

vor allen Dingen sachgemäßer, aber zugleich auch einfacher und bei weitem kürzer ist als der im Februar 1887 gefundene, welcher zunächst zu dem Funktionensatz 5 und erst von diesem zu dem Zahlensatz 3 oder (wie in der Abhandlung des Herrn Hurwitz) zu dem gleichwertigen Satze 2 führt. Hierin bestehen die Gründe, auf denen mein im Eingang dieser Mitteilung ausgesprochenes Urteil beruht.

Braunschweig, am 14. Januar 1895.

Erläuterungen zur vorstehenden Abhandlung.

Die neuere Entwicklung hat den hier vertretenen Ansichten Dedekinds voll und ganz recht gegeben, in der Definition von Ideal und Teilbarkeit wie in der Begründung des Zerlegungssatzes. Um nur ein Beispiel zu nennen: bei Beibehaltung der einem kommutativen Bereich angepaßten Funktionen von Unbestimmten — also des verallgemeinerten Gaußschen Satzes — hätte sich der Zerlegungssatz nicht auf maximale Ordnungen hyperkomplexer Systeme übertragen lassen, wie dies tatsächlich durch Speiser und Artin geschehen ist (Züricher Vierteljahrsschrift 1926 und Hamburger Abhandlungen, Bd. V, 1927).

An Stelle der von Dedekind vorstehend angegebenen vier gleichwertigen Sätze als Grundlage ist in der neueren Behandlung die „ganze Abgeschlossenheit" getreten, die zusammen mit gewissen Endlichkeitsvoraussetzungen (eingeschränkter Doppelkettensatz) dem Zerlegungssatz gleichwertig ist (E. Noether, Math. Ann. **96**, 1926). Auf dieser Grundlage ergibt sich nach Krull (Math. Ann. **99**, 1928) direkt die auch von Dedekind (in der vierten Auflage von Dirichlet-Dedekind) in den Vordergrund gestellte Tatsache, daß die Ideale umkehrbare (eigentliche) Moduln sind, daß also die ganzen und gebrochenen Ideale eine Abelsche Gruppe gegenüber der Multiplikation bilden, woraus der Zerlegungssatz unmittelbar folgt. Während Krull zu dem Gruppennachweis noch den Weg über die Primideale nimmt, hat Artin diese Tatsache direkt bewiesen, und zwar allgemein für ganzabgeschlossene Bereiche, die keiner Endlichkeitsbedingung zu genügen brauchen. Die Gleichheit wird dabei durch einen passenden Äquivalenzbegriff ersetzt — auf dem Dedekindschen Begriff des Modulquotienten beruhend —, den in speziellerer Fassung schon v. d. Waerden zugrunde gelegt hatte (Math. Ann. **101**, 1929).

Der Artinsche Beweis wird in der, in der Sammlung Grundlehren der Math. Wissenschaften erscheinenden, „Modernen Algebra" von v. d. Waerden gebracht werden. Damit ist dann auch in die Lehrbuch-Literatur, wo bis jetzt der Hurwitzsche Beweis vorherrschte, die Dedekindsche Auffassung eingedrungen; ebenso wie dies für die modernen Vorlesungen gilt, wo E. Landau noch 1917, im Nachruf auf Dedekind (Gött. Nachr. 1917), das Gegenteil konstatieren konnte.

Noether.

XXVI.

Über eine Erweiterung des Symbols (a, b) in der Theorie der Moduln.

[Nachrichten von der Königlichen Gesellschaft der Wissenschaften zu Göttingen, Mathem.-phys. Klasse, Jahrgang 1895, S. 183—188.]

Am Schlusse des Vorwortes zu meiner Abhandlung Über die Diskriminanten endlicher Körper, welche der Königl. Gesellschaft am 5. August 1882 vorgelegt und in den Bd. 29 der Abhandlungen aufgenommen ist, habe ich hervorgehoben, daß alle in ihr gewonnenen Resultate einer wichtigen Verallgemeinerung fähig sind, zu welcher man dadurch gelangt, daß man den endlichen Körper Ω nicht nur auf den Körper der rationalen Zahlen, sondern auch auf jeden in Ω als Divisor enthaltenen Körper bezieht, wobei neben den gewöhnlichen Normen, Diskriminanten, Spuren auch partielle oder relative, auf diesen Körper bezügliche Normen usw. einzuführen und gewisse rationale Zahlen durch Ideale dieses Körpers zu ersetzen sind. Die Durchführung dieser Verallgemeinerung erfordert, wie ich damals bemerkt habe, einige vorbereitende Untersuchungen, welche aber auch ein selbständiges Interesse darbieten, und unter diesen befindet sich die in der Überschrift genannte Erweiterung des in der Modultheorie auftretenden Symbols $(\mathfrak{a}, \mathfrak{b})$, welche den Hauptgegenstand der folgenden Mitteilung bildet. Hierbei muß ich die Kenntnis des letzten Supplements der vierten Auflage (1894) von Dirichlets Vorlesungen über Zahlentheorie voraussetzen, welche ich kurz mit D. zitieren werde.

§ 1.

Der Grundgedanke unserer Untersuchung ist der folgende. Aus dem Begriff eines Moduls (D. § 168) ergibt sich eine unmittelbare Beziehung desselben zu dem Körper R der rationalen Zahlen, welche darin besteht, daß jede Zahl α eines Moduls $\mathfrak{a}$ durch Multiplikation mit jeder ganzen rationalen Zahl a immer in eine Zahl $a\alpha$ desselben

Moduls $\mathfrak{a}$ verwandelt wird; bezeichnet man mit $\mathfrak{z}$ den Inbegriff [1] aller ganzen Zahlen des Körpers R, so kann man diese Eigenschaft auch so aussprechen (D. S. 500), daß das Produkt $\mathfrak{z}\mathfrak{a}$ stets teilbar durch $\mathfrak{a}$ ist. Auf dieser Eigenschaft beruht ein großer Teil der allgemeinen Modultheorie. Ersetzen wir nun den Körper R durch einen beliebig gewählten endlichen Körper Z, der aber ungeändert beibehalten wird, und bezeichnen wir mit z den Inbegriff aller in ihm enthaltenen ganzen Zahlen, so soll im folgenden die Theorie aller derjenigen Moduln $\mathfrak{a}$ entwickelt werden, welche die Eigenschaft besitzen, daß $z\mathfrak{a}$ durch $\mathfrak{a}$ teilbar ist. In unseren Zeichen wird dies durch

$$z\mathfrak{a} > \mathfrak{a} \quad \text{oder} \quad z > \mathfrak{a}^0 \tag{1}$$

ausgedrückt, wo $\mathfrak{a}^0$ die Ordnung des Moduls $\mathfrak{a}$ bedeutet (D. S. 505). Da in z auch die Zahl 1 enthalten, also immer $\mathfrak{a} > z\mathfrak{a}$ ist, so ist diese Eigenschaft auch gleichbedeutend mit

$$z\mathfrak{a} = \mathfrak{a}. \tag{2}$$

Man kann sie auch so aussprechen, daß jede auf den Modul $\mathfrak{a}$ bezügliche Kongruenz mit jeder ganzen Zahl des Körpers Z multipliziert werden darf (D. S. 508). Wenn nun der Modul $\mathfrak{b}$ dieselbe Eigenschaft besitzt, so ergibt sich aus den allgemeinen Sätzen (D. S. 502, 500, 504)

$$z(\mathfrak{a}+\mathfrak{b}) = z\mathfrak{a} + z\mathfrak{b}, \quad z(\mathfrak{a}-\mathfrak{b}) > z\mathfrak{a} - z\mathfrak{b}, \tag{3}$$

$$z(\mathfrak{a}\mathfrak{b}) = (z\mathfrak{a})\mathfrak{b}, \quad z\left(\frac{\mathfrak{b}}{\mathfrak{a}}\right) > \frac{z\mathfrak{b}}{\mathfrak{a}}, \tag{4}$$

daß auch die vier Moduln $\mathfrak{a}+\mathfrak{b}$, $\mathfrak{a}-\mathfrak{b}$, $\mathfrak{a}\mathfrak{b}$ und $\mathfrak{b}:\mathfrak{a}$ von derselben Beschaffenheit sind. Mit Rücksicht auf diese Reproduktion durch alle Modul-Operationen wollen wir der Kürze wegen ein für allemal festsetzen, daß unter einem Modul schlechthin, falls nicht das Gegenteil ausdrücklich bemerkt wird, im folgenden stets ein solcher Modul $\mathfrak{a}$ verstanden werden soll, welcher die durch (1) oder (2) ausgedrückte Eigenschaft besitzt. —

Wir betrachten zunächst alle diejenigen endlichen, von Null verschiedenen Moduln, deren Zahlen dem Körper Z angehören. Zu der Bezeichnung dieser Moduln soll in der Regel die zweite Hälfte des lateinischen Alphabetes dienen, während die Buchstaben der ersten Hälfte meistens Zahlen des Körpers Z bedeuten.

Da die Ordnung x^0 eines solchen Moduls x aus lauter ganzen Zahlen besteht (D. S. 527), welche offenbar in Z, also auch in z enthalten sind, so ist $x^0 > z$, und da zufolge (1) auch $z > x^0$ ist, so folgt $x^0 = z$, mithin ist jeder solche Modul x ein Idealbruch (D. S. 560 Anm.). Dieser Fall ist so wichtig für unsere Untersuchung, daß ich noch einige Worte zur Erläuterung hinzufügen will. Wenn x ein ganzer Modul, also $x > z$ ist, so ist er offenbar ein Ideal (D. S. 551); hierbei bemerke ich ein für allemal, daß immer nur von solchen Idealen und Idealbrüchen die Rede sein wird, welche im Körper Z enthalten sind, was also künftig stets hinzuzudenken ist. Wenn aber der endliche Modul x auch gebrochene Zahlen enthält, so kann man eine von Null verschiedene ganze Zahl a des Körpers Z so wählen, daß alle Basiszahlen von x durch Multiplikation mit a in ganze Zahlen verwandelt werden, und folglich xa ein Ideal y wird; allgemeiner, es gibt unendlich viele Paare von Idealen u, v (z. B. $u = za$, $v = y$), welche der Bedingung $xu = v$ genügen, woraus $x = v:u = vu^{-1}$, also auch $x^{-1} = z:x = uv^{-1} = u:v$ und $xx^{-1} = z$ folgt (D. S. 553, 506, 507). Unter allen diesen Paaren u, v gibt es ein einziges, welches aus zwei relativen Primidealen u_0, v_0 besteht (D. S. 556), und jedes Paar ist von der Form $u = wu_0$, $v = wv_0$, wo $w = u + v$ ein willkürliches Ideal bedeutet; zugleich leuchtet ein, daß $u_0 = z - x^{-1}$ der Inbegriff aller oben mit a bezeichneten Zahlen (einschließlich $a = 0$) und ebenso $v_0 = z - x$, ferner $u_0^{-1} = z + x$, $v_0^{-1} = z + x^{-1}$ ist.

Aus den soeben betrachteten Moduln x bilden wir jetzt alle Moduln $\mathfrak{p}$ von der allgemeineren Form

$$\mathfrak{p} = x\alpha, \tag{5}$$

wo α jede beliebige, von Null verschiedene Zahl innerhalb oder außerhalb Z bedeutet. Diese Moduln $\mathfrak{p}$ wollen wir kurz einfache Moduln nennen, weil sie für unsere Untersuchung genau dieselbe Bedeutung besitzen wie die von Null verschiedenen eingliedrigen Moduln für die allgemeine Modultheorie (D. S. 494), und weil sie mit diesen letzteren zusammenfallen, wenn Z der Körper R der rationalen Zahlen ist*). Jeder einfache Modul $\mathfrak{p}$ ist offenbar ein endlicher, von Null verschiedener Modul, in welchem jedes Zahlenpaar ein nach Z reduzibles System bildet (D. S. 466), und man

*) Die Wahl des Buchstaben $\mathfrak{p}$ soll also keineswegs an Primideale erinnern.

überzeugt sich leicht, daß hierdurch umgekehrt der gemeinsame Charakter aller einfachen Moduln auf invariante Weise bestimmt ist. Offenbar läßt sich aber jeder einfache Modul $\mathfrak{p}$ auf unendlich viele verschiedene Arten in der Form (5) darstellen; ist nämlich y irgendein mit x äquivalenter Idealbruch (D. S. 579), also $x = yc$, wo c irgendeine von Null verschiedene Zahl in Z bedeutet, so wird $\mathfrak{p} = y\beta$, wo $\beta = c\alpha$; man darf daher bei der Darstellung (5) auch immer annehmen, daß x ein ganzer Idealbruch, d. h. ein Ideal ist.

Zugleich leuchtet ein, daß jeder einfache Modul $\mathfrak{p}$ ein eigentlicher Modul (D. S. 506), daß nämlich

$$\mathfrak{p}^0 = z = \mathfrak{p}\mathfrak{p}^{-1}, \quad \mathfrak{p}^{-1} = x^{-1}\alpha^{-1} \tag{6}$$

ist, und ebenso, daß Produkte und Quotienten von einfachen Moduln wieder einfache Moduln sind. Hieraus folgt auch leicht, daß immer

$$(\mathfrak{a} - \mathfrak{b})\mathfrak{p} = \mathfrak{a}\mathfrak{p} - \mathfrak{b}\mathfrak{p} \tag{7}$$

ist; denn nach der allgemeinen Modultheorie (D. S. 502) ist die linke Seite teilbar durch die rechte, und ebenso ist $(\mathfrak{a}\mathfrak{p} - \mathfrak{b}\mathfrak{p})\mathfrak{p}^{-1}$ teilbar durch den Modul $\mathfrak{a}\mathfrak{p}\mathfrak{p}^{-1} - \mathfrak{b}\mathfrak{p}\mathfrak{p}^{-1}$, d. h. durch $\mathfrak{a} - \mathfrak{b}$, woraus durch Multiplikation mit $\mathfrak{p}$ folgt, daß auch die rechte Seite unserer Gleichung (7) durch die linke teilbar ist, w. z. b. w. Auf dieselbe Weise ergibt sich, daß aus $\mathfrak{a}\mathfrak{p} > \mathfrak{b}\mathfrak{p}$ stets $\mathfrak{a} > \mathfrak{b}$ und aus $\mathfrak{a}\mathfrak{p} = \mathfrak{b}\mathfrak{p}$ stets $\mathfrak{a} = \mathfrak{b}$ folgt.

§ 2.

Wir wenden uns jetzt zum Beweise von Sätzen, auf denen die Einführung eines neuen Symbols beruht, und bei welchen die Analogie zwischen unseren einfachen Moduln und den eingliedrigen Moduln der allgemeinen Theorie noch deutlicher hervortritt (vgl. D. S. 514).

I. Jedes von Null verschiedene Vielfache $\mathfrak{q}$ eines einfachen Moduls $\mathfrak{p}$ ist ein einfacher Modul von der Form

$$\mathfrak{q} = u\mathfrak{p}, \tag{8}$$

wo u ein Ideal bedeutet, dessen Norm

$$(z, u) = N(u) = (\mathfrak{p}, \mathfrak{q}) \tag{9}$$

ist.

Denn aus der Teilbarkeit von $\mathfrak{q}$ durch $\mathfrak{p}$ folgt durch Multiplikation mit $\mathfrak{p}^{-1}$, daß der von Null verschiedene Modul $\mathfrak{q}\mathfrak{p}^{-1}$ durch z teilbar, also ein Ideal u ist, woraus sich (8) ergibt; da ferner $\mathfrak{p}$ von der Form (5) ist, wo x als ein Ideal angenommen werden darf,

so ergibt sich nach bekannten Sätzen (D. S. 510, 564)

$$(\mathfrak{p}, \mathfrak{q}) = (x\alpha, u\,x\alpha) = (x, u\,x) = N(u),$$

w. z. b. w.

Wir bemerken zunächst, daß das in (8) auftretende Ideal u durch $\mathfrak{p}$ und $\mathfrak{q}$ vollständig bestimmt ist, weil aus (8) durch Multiplikation mit $\mathfrak{p}^{-1}$ wieder $u = \mathfrak{q}\mathfrak{p}^{-1}$ folgt. Bedeutet ferner π irgendeine von Null verschiedene Zahl in $\mathfrak{p}$, so ist $z\pi > \mathfrak{p}$, also $z\pi = u\mathfrak{p}$, wo $u = \pi\mathfrak{p}^{-1}$ ein Ideal; offenbar entsprechen allen Zahlen π lauter äquivalente Ideale u (D. S. 573), und umgekehrt, wenn das Ideal u' mit u äquivalent, also $u' = cu$ ist, wo c eine Zahl des Körpers Z bedeutet, so ist die Zahl $\pi' = c\pi$ in $\mathfrak{p}$ enthalten und $u' = \pi'\mathfrak{p}^{-1}$; man kann daher (D. S. 579) die Zahl π aus $\mathfrak{p}$ auch immer so auswählen, daß $\pi\mathfrak{p}^{-1}$ relatives Primideal zu irgendeinem gegebenen Ideal wird.

Sodann benutzen wir den vorstehenden Satz, um für einen beliebigen Modul $\mathfrak{m}$ und einen einfachen Modul $\mathfrak{p}$ ein neues Symbol $(\mathfrak{p}; \mathfrak{m})$ zu erklären, in welchem wir die beiden Moduln nicht durch ein Komma, sondern durch ein Semikolon voneinander trennen. Hierbei sind zwei Fälle zu unterscheiden, je nachdem $(\mathfrak{p}, \mathfrak{m}) > 0$ oder $= 0$ ist (D. S. 509). Da immer $(\mathfrak{p}, \mathfrak{m})\mathfrak{p}$ durch $\mathfrak{p} - \mathfrak{m}$ teilbar ist (D. S. 511), so ist im ersten Falle auch $\mathfrak{p} - \mathfrak{m}$ ein von Null verschiedenes Vielfache $\mathfrak{q}$ von $\mathfrak{p}$, und wir definieren $(\mathfrak{p}; \mathfrak{m})$ gemäß (8) als das durch die Gleichung

$$\mathfrak{p} - \mathfrak{m} = (\mathfrak{p}; \mathfrak{m})\mathfrak{p} \tag{10}$$

vollständig bestimmte Ideal*)

$$(\mathfrak{p}; \mathfrak{m}) = (\mathfrak{p} - \mathfrak{m})\mathfrak{p}^{-1}, \tag{11}$$

und da immer $(\mathfrak{p}, \mathfrak{m}) = (\mathfrak{p}, \mathfrak{p} - \mathfrak{m})$ ist (D. S. 510), so folgt aus (9) auch

$$(\mathfrak{p}, \mathfrak{m}) = N(\mathfrak{p}; \mathfrak{m}). \tag{12}$$

Da umgekehrt, wenn $\mathfrak{p} - \mathfrak{m}$ von Null verschieden ist, zufolge (8) und (9) dasselbe auch von $(\mathfrak{p}, \mathfrak{m})$ gilt, so tritt der zweite Fall $(\mathfrak{p}, \mathfrak{m}) = 0$ stets und nur dann ein, wenn $\mathfrak{p} - \mathfrak{m} = 0$ ist, und dann wollen wir auch

$$(\mathfrak{p}; \mathfrak{m}) = 0 \tag{13}$$

*) Ist x ein Idealbruch, so ist z. B. $(z; x) = v_0$, $(x; z) = u_0$, wo u_0 und v_0 dieselbe Bedeutung für x haben wie in § 1.

setzen, weil hierdurch die Gleichungen (10), (11), (12) erhalten bleiben. In allen Fällen ist offenbar

$$(\mathfrak{p}; \mathfrak{m}) = (\mathfrak{p}; \mathfrak{p} - \mathfrak{m}). \tag{14}$$

Ebenso geht aus (10) hervor, daß die Gleichung

$$(\mathfrak{p}; \mathfrak{m}) = z \text{ gleichbedeutend mit } \mathfrak{p} > \mathfrak{m} \tag{15}$$

ist. Multipliziert man ferner (10) mit einem beliebigen einfachen Modul $\mathfrak{p}'$, so folgt mit Rücksicht auf (7) der in allen Fällen geltende Satz

$$(\mathfrak{p}\mathfrak{p}'; \mathfrak{m}\mathfrak{p}') = (\mathfrak{p}; \mathfrak{m}). \tag{16}$$

Durch wiederholte Anwendung des Satzes I und der daraus gezogenen Folgerungen ergibt sich der Satz

II. Sind $\mathfrak{a}, \mathfrak{b}$ beliebige Moduln, so ist $(\mathfrak{a}, \mathfrak{b})$ entweder $= 0$ oder die Norm eines Ideals u.

Ist nämlich $(\mathfrak{a}, \mathfrak{b}) = 1$, also $\mathfrak{a} > \mathfrak{b}$, so wird dem Satze durch $u = z$ genügt. Ist aber $(\mathfrak{a}, \mathfrak{b}) > 1$, so kann man aus $\mathfrak{a}$ immer ein System $\mathfrak{P}$ von einfachen Moduln $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_n$ in endlicher Anzahl n so auswählen, daß

$$\mathfrak{a} = (\mathfrak{a} - \mathfrak{b}) + \mathfrak{p}_1 + \mathfrak{p}_2 + \cdots + \mathfrak{p}_n \tag{17}$$

wird; denn wenn z. B. die Zahlen $\alpha_1, \alpha_2, \cdots, \alpha_s$, wo $s = (\mathfrak{a}, \mathfrak{b})$, ein Restsystem von $\mathfrak{a}$ nach $\mathfrak{b}$ bilden (D. S. 509), so ist offenbar auch $\mathfrak{a} = (\mathfrak{a} - \mathfrak{b}) + z\alpha_1 + z\alpha_2 + \cdots + z\alpha_s$; und dies ist nur ein spezieller Fall der allgemeinen Darstellung (17). Setzt man nun, wenn ν irgendeine der Zahlen $1, 2, \cdots, n$ bedeutet,

$$\mathfrak{a}_{\nu-1} = (\mathfrak{a} - \mathfrak{b}) + \mathfrak{p}_\nu + \mathfrak{p}_{\nu+1} + \cdots + \mathfrak{p}_n \tag{18}$$

und außerdem $\mathfrak{a}_n = \mathfrak{a} - \mathfrak{b}$, so ist $\mathfrak{a}_0 = \mathfrak{a}$ und

$$\mathfrak{a}_{\nu-1} = \mathfrak{p}_\nu + \mathfrak{a}_\nu < \mathfrak{a}_\nu, \tag{19}$$

also nach bekannten Sätzen (D. S. 510)

$$(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{a}_0, \mathfrak{a}_n) = (\mathfrak{a}_0, \mathfrak{a}_1)(\mathfrak{a}_1, \mathfrak{a}_2) \cdots (\mathfrak{a}_{n-1}, \mathfrak{a}_n)$$

und mit Rücksicht auf (12)

$$(\mathfrak{a}_{\nu-1}, \mathfrak{a}_\nu) = (\mathfrak{p}_\nu + \mathfrak{a}_\nu, \mathfrak{a}_\nu) = (\mathfrak{p}_\nu, \mathfrak{a}_\nu) = N(\mathfrak{p}_\nu; \mathfrak{a}_\nu).$$

Setzt man daher das Idealprodukt

$$(\mathfrak{p}_1; \mathfrak{a}_1)(\mathfrak{p}_2; \mathfrak{a}_2) \cdots (\mathfrak{p}_n; \mathfrak{a}_n) = u, \tag{20}$$

so folgt aus dem bekannten Satze über die Norm eines Produktes (D. S. 564) das Resultat

$$(a, b) = N(u), \tag{21}$$

w. z. b. w.

Es liegt nun die Vermutung sehr nahe, daß das in (20) gebildete Idealprodukt u, dessen Norm $= (a, b)$, sowohl von der Reihenfolge der in der Darstellung (17) des Moduls a auftretenden einfachen Moduln $\mathfrak{p}_r$ als auch von der Auswahl des Systems $\mathfrak{P}$ dieser Moduln gänzlich unabhängig, also invariant durch a und b bestimmt ist. Um dies zu beweisen, schicken wir folgenden Hilfssatz voraus:

III. Sind $\mathfrak{p}$, $\mathfrak{q}$ einfache Moduln, und setzt man zur Abkürzung

$$\mathfrak{p}' = \mathfrak{p} - (\mathfrak{q} + \mathfrak{m}),\ \mathfrak{q}' = \mathfrak{q} - (\mathfrak{p} + \mathfrak{m}), \tag{22}$$

wo $\mathfrak{m}$ ein beliebiger Modul, so ist

$$\mathfrak{q}'(\mathfrak{p} - \mathfrak{m}) = \mathfrak{p}'(\mathfrak{q} - \mathfrak{m}). \tag{23}$$

Dies ergibt sich ziemlich leicht aus dem in der allgemeinen Modultheorie (D. S. 499) bewiesenen, für je drei Moduln $\mathfrak{m}$, $\mathfrak{p}$, $\mathfrak{q}$ gültigen Satze

$$(\mathfrak{p} + \mathfrak{m}) - (\mathfrak{q} + \mathfrak{m}) = \mathfrak{p}' + \mathfrak{m} = \mathfrak{q}' + \mathfrak{m}, \tag{24}$$

woraus wir die für unseren Zweck hinreichenden Folgerungen

$$\mathfrak{p}' > \mathfrak{q}' + \mathfrak{m},\ \mathfrak{q}' > \mathfrak{p}' + \mathfrak{m} \tag{25}$$

ziehen. Nehmen wir nun zunächst an, die Moduln $\mathfrak{p} - \mathfrak{m}$ und $\mathfrak{q} - \mathfrak{m}$ seien beide von Null verschieden, so gilt dasselbe auch von $\mathfrak{p}'$ und $\mathfrak{q}'$, weil zufolge (22) offenbar $\mathfrak{p} - \mathfrak{m} > \mathfrak{p}'$ und $\mathfrak{q} - \mathfrak{m} > \mathfrak{q}'$ ist; da ferner $\mathfrak{p}' > \mathfrak{p}$ und $\mathfrak{q}' > \mathfrak{q}$, so sind (nach dem Satze I) auch $\mathfrak{p}'$, $\mathfrak{q}'$, $\mathfrak{p} - \mathfrak{m}$, $\mathfrak{q} - \mathfrak{m}$ einfache Moduln, und man kann daher

$$\mathfrak{p} - \mathfrak{m} = p\mathfrak{p}',\ \mathfrak{q} - \mathfrak{m} = q\mathfrak{q}' \tag{26}$$

setzen, wo p, q Ideale bedeuten, deren Identität wir jetzt beweisen wollen. Aus der ersten der durch (25) ausgedrückten Teilbarkeiten ergibt sich durch Multiplikation mit q zunächst $q\mathfrak{p}' > q\mathfrak{q}' + q\mathfrak{m}$; beide Moduln $q\mathfrak{q}'$, $q\mathfrak{m}$ sind aber durch $\mathfrak{m}$ teilbar, der erstere zufolge (26), und der letztere, weil $q > z$ ist; mithin ist auch $q\mathfrak{p}' > \mathfrak{m}$, und da ferner $q\mathfrak{p}' > \mathfrak{p}' > \mathfrak{p}$, so ist $q\mathfrak{p}'$ ein gemeinsames Vielfaches von $\mathfrak{m}$ und $\mathfrak{p}$, also auch teilbar durch $\mathfrak{p} - \mathfrak{m}$, d. h. $q\mathfrak{p}' > p\mathfrak{p}'$, und

hieraus ergibt sich $q > p$, weil $\mathfrak{p}'$ ein einfacher Modul ist. Zufolge der Symmetrie ist ebenso $p > q$, also wirklich

$$p = q, \tag{27}$$

und der Satz (23) ist daher eine unmittelbare Folge von (26), w. z. b. w. Dieser Satz gilt aber auch dann, wenn man die obige Annahme fallen läßt, daß $\mathfrak{p} - \mathfrak{m}$ und $\mathfrak{q} - \mathfrak{m}$ beide von Null verschieden sind. Dies leuchtet unmittelbar ein, wenn beide Moduln $= 0$ sind. Wenn ferner $\mathfrak{p} - \mathfrak{m} = 0$, aber $\mathfrak{q} - \mathfrak{m}$, also auch $\mathfrak{q}'$ von Null verschieden ist, so behält das Ideal q seine Bedeutung, und der obige Beweis für die Teilbarkeit von $q\mathfrak{p}'$ durch $\mathfrak{p} - \mathfrak{m}$ bleibt bestehen, mithin ist $\mathfrak{p}' = 0$ und der Satz (23) auch jetzt richtig, w. z. b. w.

Drückt man die in (23) auftretenden Moduln gemäß (10) aus, so nimmt unser Satz folgende Form an:

IV. Sind $\mathfrak{p}$, $\mathfrak{q}$ einfache Moduln, während $\mathfrak{m}$ einen beliebigen Modul bedeutet, so ist

$$(\mathfrak{q}; \mathfrak{p} + \mathfrak{m})(\mathfrak{p}; \mathfrak{m}) = (\mathfrak{p}; \mathfrak{q} + \mathfrak{m})(\mathfrak{q}; \mathfrak{m}). \tag{28}$$

Mit Hilfe desselben beweisen wir leicht, daß die Reihenfolge, nach welcher aus den in (17) auftretenden einfachen Moduln $\mathfrak{p}_\nu$ die Moduln $\mathfrak{a}_\nu$ in (18), (19) und die Ideale $(\mathfrak{p}_\nu; \mathfrak{a}_\nu)$ gebildet werden, keinen Einfluß auf deren Produkt u in (20) ausübt. In der Tat, ändert man diese Reihenfolge nur so weit ab, daß zwei Nachbarn $\mathfrak{p}_{\mu-1}$ und $\mathfrak{p}_\mu$ ihre Plätze miteinander vertauschen, alle übrigen $\mathfrak{p}_\nu$ ihren Platz behaupten, so bleiben auch alle Moduln $\mathfrak{a}_\nu$ mit einziger Ausnahme von $\mathfrak{a}_{\mu-1}$ ungeändert, welcher in

$$(\mathfrak{a} - \mathfrak{b}) + \mathfrak{p}_{\mu-1} + \mathfrak{p}_{\mu+1} + \cdots + \mathfrak{p}_n = \mathfrak{p}_{\mu-1} + \mathfrak{a}_\mu$$

übergeht; zugleich bleiben alle Faktoren des Produktes u in (20) ungeändert mit Ausnahme von

$$(\mathfrak{p}_{\mu-1}; \mathfrak{a}_{\mu-1}) \text{ und } (\mathfrak{p}_\mu; \mathfrak{a}_\mu),$$

welche bzw. in

$$(\mathfrak{p}_\mu; \mathfrak{p}_{\mu-1} + \mathfrak{a}_\mu) \text{ und } (\mathfrak{p}_{\mu-1}; \mathfrak{a}_\mu)$$

übergehen; da aber $\mathfrak{a}_{\mu-1} = \mathfrak{p}_\mu + \mathfrak{a}_\mu$ ist, so folgt aus (28), wenn man $\mathfrak{q} = \mathfrak{p}_{\mu-1}$, $\mathfrak{p} = \mathfrak{p}_\mu$, $\mathfrak{m} = \mathfrak{a}_\mu$ setzt, daß das Produkt der beiden ersteren Moduln mit dem der beiden letzteren identisch ist, also das Produkt u ungeändert bleibt. Dasselbe gilt daher auch für

jede Abänderung der Reihenfolge, weil eine solche bekanntlich immer durch fortgesetzte Vertauschung von zwei Nachbarn hervorgebracht werden kann, und wir dürfen daher sagen, das Idealprodukt u entspreche dem System $\mathfrak{P}$ der n einfachen Moduln $\mathfrak{p}_\nu$, welche in der Darstellung (17) des Moduls $\mathfrak{a}$ auftreten.

Noch leichter läßt sich nun zeigen, daß das Ideal u auch von der Auswahl des Systems $\mathfrak{P}$ unabhängig ist. Nehmen wir nämlich einmal an, es reiche schon das System $\mathfrak{P}_1$ der $n-1$ einfachen Moduln $\mathfrak{p}_2, \mathfrak{p}_3, \cdots, \mathfrak{p}_n$ zu einer solchen Darstellung von $\mathfrak{a}$ aus, es sei also

$$\mathfrak{a} = (\mathfrak{a} - \mathfrak{b}) + \mathfrak{p}_2 + \mathfrak{p}_3 + \cdots + \mathfrak{p}_n, \tag{29}$$

so wird, wenn man zu $\mathfrak{P}_1$ einen beliebigen, durch $\mathfrak{a}$ teilbaren einfachen Modul $\mathfrak{p}_1$ hinzufügt, ein System $\mathfrak{P}$ von n einfachen Moduln $\mathfrak{p}_\nu$ entstehen, welches der Bedingung (17) genügt, weil $\mathfrak{a} + \mathfrak{p}_1 = \mathfrak{a}$ ist. Behält man nun die früheren Bezeichnungen bei, so entspricht dem System $\mathfrak{P}_1$ das Idealprodukt

$$u_1 = (\mathfrak{p}_2; \mathfrak{a}_2)\,(\mathfrak{p}_3; \mathfrak{a}_3) \cdots (\mathfrak{p}_n; \mathfrak{a}_n),$$

und folglich ist $u = (\mathfrak{p}_1; \mathfrak{a}_1)\, u_1$; da aber zufolge (29) schon $\mathfrak{a}_1 = \mathfrak{a}$, also auch $\mathfrak{p}_1 > \mathfrak{a}_1$ ist, so folgt aus (15), daß $(\mathfrak{p}_1; \mathfrak{a}_1) = z$, mithin $u_1 = u$ ist. Dasselbe ergibt sich auch daraus, daß zufolge (21) gewiß $N(u) = N(u_1)$, also $N(\mathfrak{p}_1; \mathfrak{a}_1) = 1$ ist. Nennen wir der Kürze halber, indem wir die beiden Moduln $\mathfrak{a}, \mathfrak{b}$ festhalten, jedes System $\mathfrak{P}$ von n einfachen Moduln $\mathfrak{p}_\nu$, welches der Bedingung (17) genügt, ein vollständiges System, so können wir das eben gewonnene Resultat offenbar so aussprechen, daß ein solches System $\mathfrak{P}$ durch Aufnahme von beliebig vielen einfachen, durch $\mathfrak{a}$ teilbaren Moduln in ein ebenfalls vollständiges System $\mathfrak{R}$ übergeht, und daß beiden Systemen $\mathfrak{P}$ und $\mathfrak{R}$ ein und dasselbe Idealprodukt u entspricht. Ist nun $\mathfrak{Q}$ ebenfalls ein vollständiges System, und bezeichnet man mit $\mathfrak{R}$ das aus $\mathfrak{P}$ und $\mathfrak{Q}$ zusammengesetzte System, welches aus $\mathfrak{P}$ durch Hinzufügung von $\mathfrak{Q}$, aus $\mathfrak{Q}$ durch Hinzufügung von $\mathfrak{P}$ entsteht, so leuchtet ein, daß auch den beiden Systemen $\mathfrak{P}$, $\mathfrak{Q}$ ein und dasselbe Idealprodukt u entspricht, w. z. b. w.

Ist $\mathfrak{a}$ selbst ein einfacher Modul, so wird die Darstellung (17) durch $n = 1$, $\mathfrak{p}_1 = \mathfrak{a}$ erfüllt, d. h. $\mathfrak{a}$ selbst bildet ein vollständiges System, und das ihm entsprechende Idealprodukt u reduziert sich

auf den einzigen Faktor $(\mathfrak{a}; \mathfrak{a} - \mathfrak{b})$, welcher nach (14) mit $(\mathfrak{a}; \mathfrak{b})$ identisch ist. Wir wollen daher, wenn $\mathfrak{a}$ und $\mathfrak{b}$ wieder beliebige Moduln bedeuten, welche der Bedingung $(\mathfrak{a}, \mathfrak{b}) > 1$ genügen, das invariante, von der Darstellung (17) gänzlich unabhängige Idealprodukt u in (20) auch mit dem Symbol $(\mathfrak{a}; \mathfrak{b})$ bezeichnen; es wird daher

$$(30) \qquad (\mathfrak{a}; \mathfrak{b}) = (\mathfrak{p}_1; \mathfrak{a}_1)\,(\mathfrak{p}_2; \mathfrak{a}_2) \cdots (\mathfrak{p}_n; \mathfrak{a}_n),$$

wo $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_n$ einfache Moduln bedeuten, welche der Bedingung (17) genügen, während $\mathfrak{a}_1, \mathfrak{a}_2, \cdots, \mathfrak{a}_n$ durch (18) oder (19) bestimmt sind; die Bedeutung jedes Faktors von $(\mathfrak{a}; \mathfrak{b})$ ist früher in (11) erklärt. Zufolge (21) ist zugleich

$$(31) \qquad (\mathfrak{a}, \mathfrak{b}) = N(\mathfrak{a}; \mathfrak{b}).$$

Wir betrachten nun noch die beiden, bis jetzt ausgeschlossenen Fälle, wo $(\mathfrak{a}, \mathfrak{b}) = 1$ oder $= 0$ ist. Der erstere Fall tritt dann, und nur dann ein, wenn $\mathfrak{a} > \mathfrak{b}$ ist (also immer für $\mathfrak{a} = 0$); soll nun das Gesetz (31) bestehen bleiben, so müssen wir definieren

$$(32) \qquad (\mathfrak{a}; \mathfrak{b}) = z, \text{ wenn } (\mathfrak{a}, \mathfrak{b}) = 1.$$

Aber man kann auch (mit einziger Ausnahme des Falles $\mathfrak{a} = 0$) die Definition (30) anwenden; denn jedes beliebig ausgewählte System $\mathfrak{P}$ von einfachen, durch $\mathfrak{a}$ teilbaren Moduln $\mathfrak{p}_\nu$ ist im obigen Sinne ein vollständiges System, und da nach (15) jeder Faktor $(\mathfrak{p}_\nu; \mathfrak{a}_\nu) = z$ wird, weil $\mathfrak{a}_\nu = \mathfrak{a}$ ist, so folgt aus (30) auch (32). Soll endlich das Gesetz (31) auch im zweiten Falle erhalten bleiben, so müssen wir definieren

$$(33) \qquad (\mathfrak{a}; \mathfrak{b}) = 0, \text{ wenn } (\mathfrak{a}, \mathfrak{b}) = 0.$$

und man überzeugt sich leicht, daß dies mit (13) und auch mit (30) verträglich ist, wenn in diesem Falle überhaupt eine Darstellung von der Form (17) existiert.

Die Wahl der Bezeichnung $(\mathfrak{a}; \mathfrak{b})$, in welche freilich die notwendige Beziehung auf den Körper Z oder das Ideal z nicht aufgenommen ist, rechtfertigt sich zunächst dadurch, daß $(\mathfrak{a}; \mathfrak{b})$, wenn Z der Körper R der rationalen Zahlen, also z das System $\mathfrak{z}$ aller ganzen rationalen Zahlen ist, mit $(\mathfrak{a}, \mathfrak{b})$ oder vielmehr mit dem eingliedrigen Modul $\mathfrak{z}(\mathfrak{a}, \mathfrak{b})$ zusammenfällt; dies folgt unmittelbar aus (31) oder auch aus (11) und (30). Außerdem gelten aber für das

neue Symbol $(\mathfrak{a}; \mathfrak{b})$, wie wir jetzt beweisen wollen, auch dieselben Hauptsätze (D. S. 510, 511) wie für das alte Symbol $(\mathfrak{a}, \mathfrak{b})$*),

§ 3.

Die Darstellung (17) und das daraus abgeleitete Idealprodukt in (20) oder (30) bleibt offenbar ungeändert, wenn $\mathfrak{a}$ festgehalten, aber $\mathfrak{b}$ durch $\mathfrak{a} - \mathfrak{b}$ ersetzt wird; hieraus folgt unmittelbar der Satz

(34) $$(\mathfrak{a}; \mathfrak{b}) = (\mathfrak{a}; \mathfrak{a} - \mathfrak{b}).$$

Aus der Darstellung (17) folgt ferner durch Addition von $\mathfrak{b}$, weil $(\mathfrak{a} - \mathfrak{b}) + \mathfrak{b} = \mathfrak{b} = (\mathfrak{a} + \mathfrak{b}) - \mathfrak{b}$ ist, die Darstellung

$$\mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{p}_1 + \mathfrak{p}_2 + \cdots + \mathfrak{p}_n,$$

welche für die beiden Moduln $\mathfrak{a} + \mathfrak{b}, \mathfrak{b}$ dieselbe Bedeutung hat wie (17) für $\mathfrak{a}, \mathfrak{b}$; wir bilden daher, wie in (18), die entsprechende Kette der Moduln

$$\mathfrak{a}'_{\nu-1} = \mathfrak{b} + \mathfrak{p}_\nu + \mathfrak{p}_{\nu+1} + \cdots + \mathfrak{p}_n, \quad \mathfrak{a}'_n = \mathfrak{b}$$

und erhalten nach (30) zunächst

$$(\mathfrak{a} + \mathfrak{b}; \mathfrak{b}) = (\mathfrak{p}_1; \mathfrak{a}'_1)\,(\mathfrak{p}_2; \mathfrak{a}'_2) \cdots (\mathfrak{p}_n; \mathfrak{a}'_n).$$

Zwischen den beiden Ketten der Moduln $\mathfrak{a}_\nu$ und $\mathfrak{a}'_\nu$ besteht nun die durch die beiden Gleichungen

$$\mathfrak{a}'_\nu = \mathfrak{b} + \mathfrak{a}_\nu, \quad \mathfrak{a}_\nu = \mathfrak{a} - \mathfrak{a}'_\nu$$

ausgedrückte Korrespondenz (vgl. D. S. 499 Anm.); die erste ergibt sich unmittelbar aus (18) durch Addition von $\mathfrak{b}$, und aus ihr folgt die zweite; da nämlich $\mathfrak{a}_\nu > \mathfrak{a}$ ist, so gilt nach einem Satze der allgemeinen Modultheorie (D. S. 498) die Gleichung

$$(\mathfrak{a} - \mathfrak{b}) + \mathfrak{a}_\nu = \mathfrak{a} - (\mathfrak{b} + \mathfrak{a}_\nu),$$

welche mit der zu beweisenden zusammenfällt, weil $\mathfrak{a} - \mathfrak{b} > \mathfrak{a}_\nu$ ist. Da ferner $\mathfrak{p}_\nu > \mathfrak{a}$ ist, so folgt hieraus weiter

$$\mathfrak{p}_\nu - \mathfrak{a}_\nu = \mathfrak{p}_\nu - \mathfrak{a} - \mathfrak{a}'_\nu = \mathfrak{p}_\nu - \mathfrak{a}'_\nu,$$

also nach (14) oder (34) auch

$$(\mathfrak{p}_\nu; \mathfrak{a}_\nu) = (\mathfrak{p}_\nu; \mathfrak{a}'_\nu),$$

und wir erhalten den Satz

(35) $$(\mathfrak{a}; \mathfrak{b}) = (\mathfrak{a} + \mathfrak{b}; \mathfrak{b}).$$

*) Vgl. auch § 6 der von H. Weber und mir verfaßten Abhandlung Theorie der algebraischen Funktionen einer Veränderlichen (Crelles Journal, Bd. 92).

Aus der Darstellung (17) folgt ferner durch Multiplikation mit einem beliebigen einfachen Modul $\mathfrak{p}$ und mit Rücksicht auf (7) die Darstellung

$$\mathfrak{a}\mathfrak{p} = (\mathfrak{a}\mathfrak{p} - \mathfrak{b}\mathfrak{p}) + \mathfrak{p}\mathfrak{p}_1 + \mathfrak{p}\mathfrak{p}_2 + \cdots + \mathfrak{p}\mathfrak{p}_n;$$

der Kette der Moduln $\mathfrak{a}_\nu$ entspricht jetzt die Kette der Moduln $\mathfrak{a}_\nu\mathfrak{p}$, und hieraus ergibt sich mit Rücksicht auf (16) der Satz

$$(\mathfrak{a}\mathfrak{p};\ \mathfrak{b}\mathfrak{p}) = (\mathfrak{a};\ \mathfrak{b}). \tag{36}$$

Da ferner $(\mathfrak{p}_\nu;\ \mathfrak{a}_\nu)\,\mathfrak{p}_\nu = \mathfrak{p}_\nu - \mathfrak{a}_\nu > \mathfrak{a}_\nu$, und auch $(\mathfrak{p}_\nu;\ \mathfrak{a}_\nu)\,\mathfrak{a}_\nu > \mathfrak{a}_\nu$ ist, weil $(\mathfrak{p}_\nu;\ \mathfrak{a}_\nu) > z$, so folgt aus (19) durch Multiplikation mit $(\mathfrak{p}_\nu;\ \mathfrak{a}_\nu)$, daß auch $(\mathfrak{p}_\nu;\ \mathfrak{a}_\nu)\,\mathfrak{a}_{\nu-1} > \mathfrak{a}_\nu$, und da $\mathfrak{a}_0 = \mathfrak{a}$ und $\mathfrak{a}_n = \mathfrak{a} - \mathfrak{b}$, so ergibt sich aus (30) der Satz

$$(\mathfrak{a};\ \mathfrak{b})\,\mathfrak{a} > \mathfrak{a} - \mathfrak{b}. \tag{37}$$

Ist endlich $\mathfrak{a} < \mathfrak{b}$, und $\mathfrak{b} < \mathfrak{c}$, so ergibt sich auch leicht der Satz

$$(\mathfrak{a};\ \mathfrak{c}) = (\mathfrak{a};\ \mathfrak{b})\,(\mathfrak{b};\ \mathfrak{c}), \tag{38}$$

wenn man die Darstellung (17), in welcher $\mathfrak{a} - \mathfrak{b} = \mathfrak{b}$ ist, mit einer Darstellung von der Form

$$\mathfrak{b} = \mathfrak{c} + \mathfrak{q}_1 + \mathfrak{q}_2 + \cdots + \mathfrak{q}_s$$

verbindet, wo $\mathfrak{q}_1, \mathfrak{q}_2, \cdots, \mathfrak{q}_s$ einfache Moduln bedeuten.

Die Beweise aller vorstehenden Sätze (34) bis (38) stützen sich auf die Annahme der Existenz von solchen Darstellungen (17); aber man überzeugt sich mit Rücksicht auf (32) und (33) leicht, daß die Sätze auch dann gültig bleiben, wenn diese Annahme nicht erfüllt ist.

§ 4.

Wir wenden uns nun zu der Untersuchung der Beziehungen, welche zwischen unserem Symbol $(\mathfrak{a};\ \mathfrak{b})$ und gewissen Determinanten bestehen und denjenigen ganz ähnlich sind, welche für das alte Symbol $(\mathfrak{a};\ \mathfrak{b})$ gelten (D. S. 521—523).

Hierbei gehen wir, indem wir $(\mathfrak{a},\ \mathfrak{b}) > 0$ voraussetzen, wieder von der Darstellung (17) des Moduls $\mathfrak{a}$ aus und betrachten jedes System L von n Zahlen $\pi_1, \pi_2, \cdots, \pi_n$, welche bzw. in $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_n$, also auch in $\mathfrak{a}$ enthalten sind und zugleich der Kongruenz

$$\pi_1 + \pi_2 + \cdots + \pi_n \equiv 0 \pmod{\mathfrak{b}} \tag{39}$$

genügen. Aus je n solchen Lösungen $L', L'', \cdots, L^{(n)}$ dieser Kongruenz bilden wir, indem wir die in ihnen auftretenden Zahlen π_ν mit entsprechenden Akzenten versehen, die Determinante

$$\lambda = \sum \pm \pi_1' \pi_2'' \cdots \pi_n^{(n)}, \tag{40}$$

welche offenbar, wie jedes ihrer Glieder, in dem einfachen Modul

$$\mathfrak{p} = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_n \tag{41}$$

enthalten ist. Da $(\mathfrak{a}, \mathfrak{b})\,\mathfrak{a} > \mathfrak{b}$ ist (D. S. 511), und folglich, wenn α_ν eine willkürliche Zahl in $\mathfrak{p}_\nu$ bedeutet, die Zahl $\pi_\nu = (\mathfrak{a}, \mathfrak{b})\,\alpha_\nu$ für sich allein eine Lösung $L^{(\nu)}$ der Kongruenz (39) bildet, während die übrigen Glieder verschwinden, so leuchtet ein, daß unter den Determinanten λ sich auch solche befinden, welche von Null verschieden sind. Da außerdem $z\lambda > \mathfrak{p}$ ist, so erzeugt (nach § 2, I) jede von Null verschiedene Determinante λ ein Ideal $\lambda\mathfrak{p}^{-1}$, und wir wollen beweisen, daß das Ideal $(\mathfrak{a}; \mathfrak{b})$ der größte gemeinsame Teiler aller dieser Ideale $\lambda\mathfrak{p}^{-1}$ ist, was wir in unseren Zeichen (D. S. 496) durch

$$(\mathfrak{a}; \mathfrak{b}) = \sum \lambda \mathfrak{p}^{-1} \text{ oder } (\mathfrak{a}; \mathfrak{b})\,\mathfrak{p} = \sum z\lambda \tag{42}$$

ausdrücken können.

Hierzu wenden wir die vollständige Induktion an, indem wir die Darstellung (17) in die beiden folgenden

$$\mathfrak{a} = \mathfrak{a}_1 + \mathfrak{p}_1, \tag{43}$$

$$\mathfrak{a}_1 = (\mathfrak{a} - \mathfrak{b}) + \mathfrak{p}_2 + \mathfrak{p}_3 + \cdots + \mathfrak{p}_n \tag{44}$$

zerlegen, welche, weil $\mathfrak{a} - \mathfrak{a}_1 = \mathfrak{a}_1$ und $\mathfrak{a}_1 - \mathfrak{b} = \mathfrak{a} - \mathfrak{b}$ ist, für die Modulpaare $\mathfrak{a}, \mathfrak{a}_1$ und $\mathfrak{a}_1, \mathfrak{b}$ dieselbe Bedeutung haben wie die Darstellung (17) für das Modulpaar $\mathfrak{a}, \mathfrak{b}$; aus (30) folgt zugleich

$$(\mathfrak{a}; \mathfrak{b}) = (\mathfrak{p}_1; \mathfrak{a}_1)\,(\mathfrak{a}_1; \mathfrak{b}). \tag{45}$$

Unser Beweis setzt sich nun aus den folgenden fünf Hauptpunkten zusammen.

1. Betrachten wir zunächst, um den Fall $n = 1$ zu erledigen, nur das Modulpaar $\mathfrak{a}, \mathfrak{a}_1$, also die Darstellung (43), so sind nach (39) alle diejenigen in $\mathfrak{p}_1$ enthaltenen Zahlen π_1 zu bilden, welche der Kongruenz $\pi_1 \equiv 0 \pmod{\mathfrak{a}_1}$ genügen, d. h. alle Zahlen π_1 des einfachen Moduls

$$\mathfrak{n} = \mathfrak{p}_1 - \mathfrak{a}_1 = (\mathfrak{p}_1; \mathfrak{a}_1)\,\mathfrak{p}_1 = (\mathfrak{a}; \mathfrak{a}_1)\,\mathfrak{p}_1; \tag{46}$$

da nun jede aus einem einzigen Element π_1 gebildete Determinante ersten Grades $= \pi_1$ ist, und außerdem zufolge der Eigenschaft (2) jeder Modul

$$\mathfrak{n} = \sum z\,\pi_1 \tag{47}$$

ist, wo π_1 alle Zahlen in $\mathfrak{n}$ durchläuft, so leuchtet für diesen Fall $n = 1$ die Richtigkeit des Satzes (42) ein.

2. Dem Verfahren des Induktionsbeweises gemäß nehmen wir jetzt an, unser Satz sei für das in der Darstellung (44) auftretende Modulpaar $\mathfrak{a}_1, \mathfrak{b}$ bewiesen, und wir haben zu zeigen, daß hieraus seine Richtigkeit auch für das Modulpaar $\mathfrak{a}, \mathfrak{b}$ folgt. Nach der obigen Vorschrift besteht diese Annahme im folgenden. Man betrachte jedes System M von $(n-1)$ Zahlen $\varrho_2, \varrho_3, \cdots, \varrho_n$, welche bzw. in $\mathfrak{p}_2, \mathfrak{p}_3, \cdots, \mathfrak{p}_n$ enthalten sind und zugleich der Kongruenz

$$\varrho_2 + \varrho_3 + \cdots + \varrho_n \equiv 0 \pmod{\mathfrak{b}} \tag{48}$$

genügen; aus je $(n-1)$ solchen Lösungen $M', M'', \cdots, M^{(n)}$ bilde man die Determinante

$$\mu = \sum \pm \varrho_2' \varrho_3'' \cdots \varrho_n^{(n)}, \tag{49}$$

so wird

$$(\mathfrak{a}_1; \mathfrak{b}) = \sum \mu\,\mathfrak{q}^{-1} \text{ oder } (\mathfrak{a}_1; \mathfrak{b})\,\mathfrak{q} = \sum z\,\mu, \tag{50}$$

wo zur Abkürzung

$$\mathfrak{q} = \mathfrak{p}_2 \mathfrak{p}_3 \cdots \mathfrak{p}_n, \text{ also } \mathfrak{p} = \mathfrak{q}\,\mathfrak{p}_1 \tag{51}$$

gesetzt ist.

3. Wenden wir uns nun zu dem Modulpaare $\mathfrak{a}, \mathfrak{b}$, also zu der aus (43) und (44) zusammengesetzten Darstellung (17) und zu der ihr entsprechenden Kongruenz (39), so bemerken wir vor allen Dingen, daß der Inbegriff aller in der letzteren auftretenden Zahlen π_1 identisch ist mit dem obigen Modul $\mathfrak{n}$ in (46). Da nämlich die Zahlen π_ν in $\mathfrak{p}_\nu$, also auch in $\mathfrak{a}$ enthalten sind, so gilt die auf den Modul $\mathfrak{b}$ bezügliche Kongruenz (39) von selbst auch für den Modul $\mathfrak{a} - \mathfrak{b}$ und ist daher gleichbedeutend mit einer Gleichung von der Form

$$\pi_1 = \sigma - \pi_2 - \pi_3 - \cdots - \pi_n,$$

wo σ eine Zahl des Moduls $\mathfrak{a} - \mathfrak{b}$ bedeutet; hieraus geht aber mit Rücksicht auf (44) hervor, daß die in $\mathfrak{p}_1$ enthaltene Zahl π_1 auch

in $\mathfrak{a}_1$, also auch in $\mathfrak{n} = \mathfrak{p}_1 - \mathfrak{a}_1$ enthalten ist; und da umgekehrt jede in $\mathfrak{n}$, also gleichzeitig in $\mathfrak{p}_1$ und $\mathfrak{a}_1$ enthaltene Zahl π_1 gewiß von der vorstehenden Form ist, aus welcher wieder die Kongruenz (39) folgt, so ergibt sich hieraus die oben behauptete Identität aller in der Kongruenz (39) auftretenden Zahlen π_1 mit allen in 1. betrachteten Zahlen π_1 des Moduls $\mathfrak{n}$, und folglich gilt für diese Zahlen π_1 auch wieder die Gleichung (47).

4. Nun leuchtet ein, daß jede Lösung M der Kongruenz (48) auch als eine Lösung L der Kongruenz (39) aufgefaßt werden kann, in welcher $\pi_1 = 0$ ist. Kombiniert man daher je $(n-1)$ Lösungen der Kongruenz (48), denen die Determinante μ in (49) entspricht, mit jeder Lösung L der Kongruenz (39), so entspricht diesem System von n Lösungen zufolge (40) eine Determinante $\lambda = \pi_1 \mu$. Unter den sämtlichen Moduln $z\lambda$ befinden sich daher auch alle Moduln von der Form $z\pi_1 \cdot z\mu$, und folglich ist der größte gemeinsame Teiler $\sum z\lambda$ der ersteren auch ein Teiler der letzteren, also auch ihres größten gemeinsamen Teilers, und da der letztere, weil die Faktoren π_1, μ gänzlich unabhängig voneinander sind, von der Form

$$\sum z\pi_1 \cdot z\mu = \sum z\pi_1 \cdot \sum z\mu$$

ist, so ergibt sich zufolge (47) das Resultat

$$\sum z\lambda < \mathfrak{n} \sum z\mu,$$

welches mit Rücksicht auf (45), (46), (50), (51) die Form

$$\sum \lambda \mathfrak{p}^{-1} < (\mathfrak{a}; \mathfrak{b}) \tag{52}$$

annimmt.

5. Schwieriger ist der Beweis, daß das Ideal linker Hand auch durch das zur rechten teilbar ist. Nach einer früheren Bemerkung (§ 2, I) kann man aus dem einfachen Modul $\mathfrak{n}$ eine Zahl ω_1 so auswählen, daß $u = \omega_1 \mathfrak{n}^{-1}$ relatives Primideal zu $(\mathfrak{a}; \mathfrak{b})$ wird, und hierauf kann man aus u eine Zahl a wählen, welche relative Primzahl zu $(\mathfrak{a}; \mathfrak{b})$ ist, weil jedes Ideal u sich durch Multiplikation mit einem Ideal v, welches relatives Primideal zu $(\mathfrak{a}; \mathfrak{b})$ ist, in ein Hauptideal $za = uv$ verwandeln läßt (D. S. 559); zugleich wird $a\mathfrak{n} = v\omega_1 > z\omega_1$, und folglich wird jede Zahl π_1 des Moduls $\mathfrak{n}$ durch Multiplikation mit a in eine Zahl

$$a\pi_1 = c\omega_1 \tag{53}$$

verwandelt, wo c ebenso wie a in z enthalten ist. Da ferner ω_1 eine Zahl in $\mathfrak{n}$ ist, so gibt es zufolge 3. in den Moduln $\mathfrak{p}_2, \mathfrak{p}_3, \cdots, \mathfrak{p}_n$ bzw. Zahlen $\omega_2, \omega_3, \cdots, \omega_n$, welche die Kongruenz

$$\omega_1 + \omega_2 + \omega_3 + \cdots + \omega_n \equiv 0 \pmod{\mathfrak{b}} \tag{54}$$

erfüllen, also mit ω_1 eine partikuläre Lösung der Kongruenz (39) bilden. Betrachtet man nun jede Lösung L der letzteren, bestimmt aus der in ihr enthaltenen Zahl π_1 gemäß (53) die zugehörige ganze Zahl c und setzt

$$\varrho_\nu = a\pi_\nu - c\omega_\nu, \tag{55}$$

so ist $\varrho_1 = 0$, und die $n-1$ Zahlen $\varrho_2, \varrho_3, \cdots, \varrho_n$, welche bzw. in $\mathfrak{p}_2, \mathfrak{p}_3, \cdots, \mathfrak{p}_n$ enthalten sind, bilden, wie sich durch Multiplikation der Kongruenzen (39), (54) mit den ganzen Zahlen a, c und Subtraktion ergibt, eine Lösung M der Kongruenz (48). Betrachtet man nun wieder je n Lösungen $L', L'', \cdots, L^{(n)}$ der Kongruenz (39), welche die Determinante λ in (40) erzeugen, und versieht die nach (53) und (55) daraus abgeleiteten Zahlen c und Lösungen M mit entsprechenden Akzenten, so ist nach bekannten Sätzen

$$a^n\lambda = \begin{vmatrix} c'\omega_1, & a\pi_2', & \cdots, & a\pi_n' \\ c''\omega_1, & a\pi_2'', & \cdots, & a\pi_n'' \\ \cdots & \cdots & \cdots & \cdots \\ c^{(n)}\omega_1, & a\pi_2^{(n)}, & \cdots, & a\pi_n^{(n)} \end{vmatrix} = \begin{vmatrix} a\pi_1', & \varrho_2', & \cdots, & \varrho_n' \\ a\pi_1'', & \varrho_2'', & \cdots, & \varrho_n'' \\ \cdots & \cdots & \cdots & \cdots \\ a\pi_1^{(n)}, & \varrho_2^{(n)}, & \cdots, & \varrho_n^{(n)} \end{vmatrix}$$
$$= a(\pi_1'\mu' + \pi_1''\mu'' + \cdots + \pi_1^{(n)}\mu^{(n)}),$$

wo $\mu', \mu'', \cdots, \mu^{(n)}$ Determinanten μ von der Form (49) bedeuten, also zufolge (50) in $(\mathfrak{a}_1; \mathfrak{b})\,\mathfrak{q}$ enthalten sind; da ferner die Faktoren π_1 in $\mathfrak{n} = (\mathfrak{p}_1; \mathfrak{a}_1)\,\mathfrak{p}_1$, also die Produkte $\pi_1\mu$ und $a\pi_1\mu$ zufolge (45), (51) in $(\mathfrak{a}; \mathfrak{b})\,\mathfrak{p}$ enthalten sind, so ergibt sich aus der vorstehenden Gleichung zunächst $a^n\lambda\mathfrak{p}^{-1} > (\mathfrak{a}; \mathfrak{b})$ und folglich, weil a^n wie a relative Primzahl zu $(\mathfrak{a}; \mathfrak{b})$ ist, auch $\lambda\mathfrak{p}^{-1} > (\mathfrak{a}; \mathfrak{b})$, mithin auch

$$\sum \lambda\mathfrak{p}^{-1} > (\mathfrak{a}; \mathfrak{b}), \tag{56}$$

woraus mit Rücksicht auf (52) der Satz (42) folgt, w. z. b. w.

Dieser Satz kommt nun meistens in der Weise zur Anwendung, daß die in der Darstellung (17) auftretenden einfachen Moduln $\mathfrak{p}_\nu$ gemäß (5) in der Form

$$\mathfrak{p}_\nu = x_\nu\alpha_\nu \tag{57}$$

ausgedrückt sind, wo x_ν einen Idealbruch, α_ν eine von Null ver-

schiedene Zahl bedeutet, und hiermit nimmt die Darstellung (17) folgende Form an:

$$\mathfrak{a} = (\mathfrak{a} - \mathfrak{b}) + x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n. \tag{58}$$

Zugleich geht die Kongruenz (39), wenn man $\pi_\nu = a_\nu\alpha_\nu$ setzt, in

$$a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n \equiv 0 \pmod{\mathfrak{b}} \tag{59}$$

über, wo $a_1, a_2, \cdots, a_n$ Zahlen bedeuten, welche bzw. in den Idealbrüchen $x_1, x_2, \cdots, x_n$ enthalten sind. Bildet man nun aus je n solchen, durch Akzente unterschiedenen Lösungen der Kongruenz (59) die Determinante

$$A = \sum \pm a_1' a_2'' \cdots a_n^{(n)} \tag{60}$$

und setzt zur Abkürzung

$$X = x_1 x_2 \cdots x_n, \tag{61}$$

so nimmt unser Satz (42) mit Rücksicht auf (40) und (41) die Form

$$(\mathfrak{a}; \mathfrak{b})\, X = \sum z A \tag{62}$$

an, in welcher nur Zahlen und Idealbrüche des Körpers Z auftreten. —

Bevor wir weitergehen, wollen wir bemerken, daß der Satz (42) offenbar auch als Definition des Symbols $(\mathfrak{a}; \mathfrak{b})$ dienen könnte. Da die Ideale $\lambda\mathfrak{p}^{-1}$ von der Reihenfolge der einfachen Moduln $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_n$ im System $\mathfrak{P}$ gänzlich unabhängig sind, so besitzt diese Definition vor der früheren (in § 2) den Vorzug, daß die Invarianz leichter nachweisbar ist; denn durch Betrachtungen, welche den bei dem obigen Beweis angewendeten ganz ähnlich sind, ergibt sich sofort, daß der größte gemeinsame Teiler aller dem System $\mathfrak{P}$ entsprechenden Ideale $\lambda\mathfrak{p}^{-1}$ sich nicht ändert, wenn zu $\mathfrak{P}$ noch irgendein durch $\mathfrak{a}$ teilbarer einfacher Modul hinzugefügt wird, und hieraus folgt wie früher (§ 2), daß dieser größte gemeinsame Teiler auch von der Auswahl des vollständigen Systems $\mathfrak{P}$ unabhängig ist. Auch kann man offenbar der Definition schon vor diesem Nachweis die völlige Invarianz verleihen, wenn man $(\mathfrak{a}; \mathfrak{b})$ als den größten gemeinsamen Teiler aller Ideale $\lambda\mathfrak{p}^{-1}$ erklärt, welche allen vollständigen Systemen $\mathfrak{P}$ entsprechen.

Unsere frühere Definition von $(\mathfrak{a}; \mathfrak{b})$ hat dagegen den Vorzug, daß sie der Determinanten λ gar nicht bedarf und sich nur auf

die Bildung von Moduln stützt; will man ihr ferner von vornherein den Charakter der Invarianz verleihen, so wird man wieder $(\mathfrak{a}; \mathfrak{b})$ als den größten gemeinsamen Teiler aller Produkte

$$\frac{\mathfrak{p}_1 - \mathfrak{a}_1}{\mathfrak{p}_1} \cdot \frac{\mathfrak{p}_2 - \mathfrak{a}_2}{\mathfrak{p}_2} \cdots \frac{\mathfrak{p}_n - \mathfrak{a}_n}{\mathfrak{p}_n}$$

erklären, die allen zur Darstellung (17) tauglichen Folgen von einfachen Moduln $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_n$ entsprechen. Immerhin bleibt die eine wie die andere Definition von $(\mathfrak{a}; \mathfrak{b})$ hinsichtlich ihrer Einfachheit außerordentlich weit zurück hinter der Definition des alten Symbols $(\mathfrak{a}, \mathfrak{b})$, welche sich unmittelbar auf die Betrachtung der in den Moduln $\mathfrak{a}, \mathfrak{b}$ enthaltenen Zahlen stützt (D. S. 509). Nachdem ich seit vielen Jahren eine ähnliche Vereinfachung vergeblich gesucht habe, kann ich nur noch den Wunsch aussprechen, daß es einem anderen gelingen möge, eine solche zu finden.

§ 5.

Wir wenden uns jetzt zu denjenigen Sätzen, welche vorzugsweise von endlichen Moduln handeln. Hierbei werden wir öfter den der allgemeinen Modultheorie angehörenden Satz

$$(63) \qquad (\varrho + \sigma)\,\mathfrak{m} > \varrho\,\mathfrak{m} + \sigma\,\mathfrak{m}$$

anzuwenden haben, welcher offenbar für je zwei Zahlen ϱ, σ und jeden Modul $\mathfrak{m}$ gilt; denn wenn μ jede Zahl des Moduls $\mathfrak{m}$ bedeutet, so ist jede Zahl des Moduls linker Hand von der Form $(\varrho + \sigma)\,\mu = \varrho\,\mu + \sigma\,\mu$, also auch in dem Modul rechter Hand enthalten*); auch leuchtet ein, daß derselbe Satz für Summen von beliebig vielen Gliedern gilt. Nach dieser Vorbemerkung stellen wir den folgenden Satz auf, welcher die Grundlage für unsere Untersuchung bildet (vgl. D. S. 516):

I. Ist der letzte der drei Moduln $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ einfach, so kann man

$$(64) \qquad (\mathfrak{c} + \mathfrak{a}) - \mathfrak{b} = \mathfrak{q} + (\mathfrak{a} - \mathfrak{b})$$

setzen, wo $\mathfrak{q}$ ein einfacher Modul oder $= 0$ ist.

*) Vgl. D. S. 501, wo dieser fast selbstverständliche Satz doch hätte erwähnt werden sollen.

Um dies zu beweisen, setzen wir zur Abkürzung *)

$$\mathfrak{a}'' = (\mathfrak{c} + \mathfrak{a}) - (\mathfrak{a} + \mathfrak{b}), \tag{65}$$

$$\mathfrak{b}_1 = \mathfrak{a}'' - \mathfrak{b} = (\mathfrak{c} + \mathfrak{a}) - \mathfrak{b}, \tag{66}$$

$$\mathfrak{c}_1 = \mathfrak{a}'' - \mathfrak{c} = \mathfrak{c} - (\mathfrak{a} + \mathfrak{b}). \tag{67}$$

Nach einem Satze der allgemeinen Modultheorie (D. S. 499) ist dann

$$\mathfrak{a}'' = \mathfrak{c}_1 + \mathfrak{a} = \mathfrak{b}_1 + \mathfrak{a}, \tag{68}$$

und die zu beweisende Gleichung (64) lautet

$$\mathfrak{b}_1 = \mathfrak{q} + (\mathfrak{a} - \mathfrak{b}). \tag{69}$$

Wir bemerken nun zunächst, daß es immer zwei Zahlen ϱ, σ gibt, welche den drei Bedingungen

$$\varrho + \sigma = 1,\ \varrho\,\mathfrak{c}_1 > \mathfrak{b}_1,\ \sigma\,\mathfrak{c}_1 > \mathfrak{a} \tag{70}$$

genügen; dies leuchtet unmittelbar ein, falls $\mathfrak{c}_1 = 0$ ist, weil dann die beiden letzten Bedingungen von selbst erfüllt sind; im entgegengesetzten Falle ist $\mathfrak{c}_1$ (nach § 2, I) als Vielfaches von $\mathfrak{c}$ ebenfalls einfach, und da aus (68) sich $\mathfrak{c}_1 > \mathfrak{b}_1 + \mathfrak{a}$, also $z > \mathfrak{b}_1\mathfrak{c}_1^{-1} + \mathfrak{a}\mathfrak{c}_1^{-1}$ ergibt, so kann man die in z enthaltene Zahl $1 = \varrho + \sigma$ setzen, wo die Zahlen ϱ, σ bzw. in $\mathfrak{b}_1\mathfrak{c}_1^{-1}$, $\mathfrak{a}\mathfrak{c}_1^{-1}$ enthalten sind und folglich den Bedingungen (70) genügen. Wie nun auch diese Zahlen übrigens gewählt sein mögen, so ergibt sich leicht, daß der Modul

$$\mathfrak{q} = \varrho\,\mathfrak{c}_1, \tag{71}$$

welcher offenbar einfach oder $= 0$ ist, unserem Satze (69) genügt. Wendet man nämlich den Hilfssatz (63) auf den Fall $\mathfrak{m} = \mathfrak{c}_1$ an mit Rücksicht auf (70), so folgt $\mathfrak{c}_1 > \mathfrak{q} + \mathfrak{a}$, und da zufolge (70) auch $\mathfrak{q} > \mathfrak{b}_1$ ist, so ergibt sich aus (68), daß

$$\mathfrak{a}'' = \mathfrak{c}_1 + \mathfrak{a} > \mathfrak{q} + \mathfrak{a} > \mathfrak{b}_1 + \mathfrak{a} = \mathfrak{a}'',$$

also

$$\mathfrak{a}'' = \mathfrak{q} + \mathfrak{a}$$

und folglich nach (66)

$$\mathfrak{b}_1 = \mathfrak{a}'' - \mathfrak{b} = (\mathfrak{q} + \mathfrak{a}) - \mathfrak{b}$$

ist; bedenkt man aber, daß $\mathfrak{q} > \mathfrak{b}_1 > \mathfrak{b}$ ist, so folgt hieraus nach einem Satze der allgemeinen Modultheorie (D. S. 498) auch die Gleichung (69), w. z. b. w. Hieraus folgt unmittelbar der Satz

*) Diese Bezeichnung der Moduln durch Akzente und Indizes entnehme ich einer noch nicht veröffentlichten Arbeit über die aus drei beliebigen Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ entspringende Gruppe von 28 Moduln, welche sich in neun verschiedene Stufen verteilen (vgl. D. Anm. auf S. 499, 510).

II. Jedes Vielfache einer Summe von n einfachen Moduln ist darstellbar als Summe von höchstens n einfachen Moduln.

Dies ist nämlich für den Fall $n = 1$ schon früher (§ 2, I) bewiesen, und wenn der Satz für jedes Vielfache $\mathfrak{a} - \mathfrak{b}$ einer Summe $\mathfrak{a}$ von n einfachen Moduln gilt, so gilt er nach dem vorhergehenden Satze auch für jedes Vielfache $(\mathfrak{c} + \mathfrak{a}) - \mathfrak{b}$ einer Summe $\mathfrak{c} + \mathfrak{a}$ von $(n + 1)$ einfachen Moduln, also allgemein, w. z. b. w.

Es verlohnt sich aber der Mühe, nach den Vorschriften des vorhergehenden Satzes die Form irgendeines Vielfachen $\mathfrak{a} - \mathfrak{b}$ einer Summe

$$\mathfrak{a} = \mathfrak{p}_1 + \mathfrak{p}_2 + \cdots + \mathfrak{p}_n \tag{72}$$

von n einfachen Moduln $\mathfrak{p}_\nu$ wirklich herzustellen. Da immer $\mathfrak{a} = \mathfrak{a} + (\mathfrak{a} - \mathfrak{b})$ ist, so können wir die in unserer früheren Untersuchung (§ 2) benutzten Bezeichnungen (17), (18) auch auf unseren Fall anwenden; setzen wir außerdem zur Abkürzung

$$\mathfrak{a}'_{\nu-1} = \mathfrak{p}_\nu + \mathfrak{p}_{\nu+1} + \cdots + \mathfrak{p}_n = \mathfrak{p}_\nu + \mathfrak{a}'_\nu,\ \mathfrak{a}'_0 = \mathfrak{a},\ \mathfrak{a}'_n = 0, \tag{73}$$

so wird (zufolge D. S. 498), weil $\mathfrak{a}'_\nu > \mathfrak{a}$ ist,

$$\mathfrak{a}_\nu = (\mathfrak{a} - \mathfrak{b}) + \mathfrak{a}'_\nu = \mathfrak{a} - (\mathfrak{b} + \mathfrak{a}'_\nu),\ \mathfrak{a}_\nu + \mathfrak{b} = \mathfrak{b} + \mathfrak{a}'_\nu,$$

also, weil $\mathfrak{p}_\nu > \mathfrak{a}$ ist,

$$\mathfrak{p}_\nu - \mathfrak{a}_\nu = \mathfrak{p}_\nu - (\mathfrak{b} + \mathfrak{a}'_\nu) = \mathfrak{p}_\nu - (\mathfrak{a}_\nu + \mathfrak{b}).$$

Ersetzen wir daher die in dem vorhergehenden Satz I und seinem Beweis auftretenden Moduln und Zahlen $\mathfrak{a}$, $\mathfrak{c}$, $\mathfrak{q}$, ϱ, σ bzw. durch $\mathfrak{a}'_\nu$, $\mathfrak{p}_\nu$, $\mathfrak{q}_\nu$, ϱ_ν, σ_ν, so wird zufolge (66), (67), (70)

$$\mathfrak{b}_1 = \mathfrak{a}'_{\nu-1} - \mathfrak{b},\ \mathfrak{c}_1 = \mathfrak{p}_\nu - \mathfrak{a}_\nu = (\mathfrak{p}_\nu; \mathfrak{a}_\nu)\,\mathfrak{p}_\nu, \tag{74}$$

$$\varrho_\nu + \sigma_\nu = 1,\ \mathfrak{q}_\nu = \varrho_\nu \mathfrak{c}_1 > \mathfrak{b}_1,\ \sigma_\nu \mathfrak{c}_1 > \mathfrak{a}'_\nu, \tag{75}$$

und zufolge (69) erhält man

$$\mathfrak{a}'_{\nu-1} - \mathfrak{b} = \mathfrak{q}_\nu + (\mathfrak{a}'_\nu - \mathfrak{b}),$$

woraus, weil $\mathfrak{a}'_n - \mathfrak{b} = 0$ ist, die Darstellung

$$\mathfrak{a} - \mathfrak{b} = \mathfrak{q}_1 + \mathfrak{q}_2 + \cdots + \mathfrak{q}_n \tag{76}$$

folgt.

Nehmen wir ferner an, die einfachen Moduln $\mathfrak{p}_\nu$ seien nach (5) in der Form

$$\mathfrak{p}_\nu = x_\nu \alpha_\nu \tag{77}$$

gegeben, wo x_ν einen Idealbruch und α_ν eine von Null verschiedene Zahl bedeutet, so kann man immer eine Zahl $c_\nu^{(\nu)}$ des Körpers Z und einen Idealbruch y_ν so wählen, daß

$$y_\nu c_\nu^{(\nu)} = (\mathfrak{p}_\nu; \mathfrak{a}_\nu)\, x_\nu, \tag{78}$$

also zufolge (74), (77)

$$\mathfrak{c}_1 = y_\nu c_\nu^{(\nu)} \alpha_\nu \tag{79}$$

wird; ist nämlich $(\mathfrak{p}_\nu; \mathfrak{a}_\nu)$ von Null verschieden, so kann man z. B. $c_\nu^{(\nu)} = 1$ setzen, während im Falle $(\mathfrak{p}_\nu; \mathfrak{a}_\nu) = 0$ auch $c_\nu^{(\nu)} = 0$ wird, y_ν aber willkürlich, z. B. $= z$ gewählt werden kann. Ist nun irgendeine Wahl von $c_\nu^{(\nu)}$ und y_ν getroffen, und setzt man mit Rücksicht auf (75)

$$\beta_\nu = c_\nu^{(\nu)} \alpha_\nu \varrho_\nu = c_\nu^{(\nu)} \alpha_\nu - c_\nu^{(\nu)} \alpha_\nu \sigma, \tag{80}$$

so wird

$$\mathfrak{q}_\nu = \varrho_\nu \mathfrak{c}_1 = y_\nu \beta_\nu. \tag{81}$$

Da nach (75) ferner $\sigma_\nu \mathfrak{c}_1 > \mathfrak{a}'_\nu$, also nach (79), (73), (77)

$$y_\nu c_\nu^{(\nu)} \alpha_\nu \sigma_\nu > x_{\nu+1} \alpha_{\nu+1} + \cdots + x_n \alpha_n,$$

mithin

$$z\, c_\nu^{(\nu)} \alpha_\nu \sigma_\nu > y_\nu^{-1} x_{\nu+1} \alpha_{\nu+1} + \cdots + y_\nu^{-1} x_n \alpha_n$$

ist, so kann man die Zahl

$$-c_\nu^{(\nu)} \alpha_\nu \sigma_\nu = c_{\nu+1}^{(\nu)} \alpha_{\nu+1} + \cdots + c_n^{(\nu)} \alpha_n$$

und folglich nach (80)

$$\beta_\nu = c_\nu^{(\nu)} \alpha_\nu + c_{\nu+1}^{(\nu)} \alpha_{\nu+1} + \cdots + c_n^{(\nu)} \alpha_n \tag{82}$$

setzen, wo die Zahlen $c_\mu^{(\nu)}$ in $y_\nu^{-1} x_\mu$ enthalten sind, also den Bedingungen

$$y_\nu c_\mu^{(\nu)} > x_\mu \tag{83}$$

genügen, was zufolge (78) auch für den Fall $\mu = \nu$ gilt. Bildet man endlich das Produkt der n Gleichungen (78) und setzt zur Abkürzung

$$X = x_1 x_2 \cdots x_n, \quad Y = y_1 y_2 \cdots y_n, \tag{84}$$

$$C = c_1' c_2'' \cdots c_n^{(n)}, \tag{85}$$

so ergibt sich zufolge (30) der in allen Fällen gültige Satz

$$(\mathfrak{a}; \mathfrak{b})\, X = Y C, \tag{86}$$

und die Gleichungen (72), (76) gehen zufolge (77), (81) in

$$\mathfrak{a} = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n, \tag{87}$$

$$\mathfrak{a} - \mathfrak{b} = y_1\beta_1 + y_2\beta_2 + \cdots + y_n\beta_n \tag{88}$$

über.

Zur Erläuterung bemerken wir noch, daß die in den Gleichungen (81), (82), (83) enthaltene Darstellung von $\mathfrak{q}_\nu$ sich zwar einfacher schon aus der einen Bedingung $\mathfrak{q}_\nu > \mathfrak{b}_1 = \mathfrak{a}'_{\nu-1} - \mathfrak{b}$ in (75) ergibt; aber hieraus würde auch mit Zuziehung der beiden anderen Bedingungen (75) die wichtige Beziehung (78), also auch der Satz (86) nicht nachträglich gefolgert werden können, wenigstens nicht ohne die neu hinzutretende Voraussetzung, daß das System der n Zahlen α_ν in bezug auf den Körper Z irreduzibel ist (D. S. 466). Diese Bemerkung möge zugleich den Übergang bilden zu dem folgenden Fundamentalsatz (vgl. D. S. 518):

III. Wenn aus dem endlichen Modul $\mathfrak{a}$ sich n und nicht mehr Zahlen so auswählen lassen, daß sie ein nach Z irreduzibles System bilden, so ist $\mathfrak{a}$ darstellbar als Summe von n einfachen Moduln.

Um dies zu beweisen, wählen wir aus $\mathfrak{a}$ ein nach Z irreduzibles System von n Zahlen $\alpha_1, \alpha_2, \cdots, \alpha_n$; dann ist jede beliebige Zahl α in $\mathfrak{a}$ von der Form

$$\alpha = h_1\alpha_1 + h_2\alpha_2 + \cdots + h_n\alpha_n,$$

wo die Koeffizienten h_ν Zahlen des Körpers Z bedeuten (D. S. 467). Da ferner $\mathfrak{a}$ ein endlicher Modul, also von der Form

$$\mathfrak{a} = [\alpha'_1, \alpha'_2, \cdots, \alpha'_m]$$

ist (D. S. 494), so kann man, nachdem jede der m Basiszahlen α'_μ in der eben angegebenen Form

$$\alpha'_\mu = h_1^{(\mu)}\alpha_1 + h_2^{(\mu)}\alpha_2 + \cdots + h_n^{(\mu)}\alpha_n$$

dargestellt ist, bekanntlich eine von Null verschiedene Zahl a so wählen, daß alle mn Produkte $a h_\nu^{(\mu)}$ ganze Zahlen des Körpers Z, also in z enthalten sind. Setzt man nun $\alpha_\nu = a\omega_\nu$ und

$$\mathfrak{o} = z\omega_1 + z\omega_2 + \cdots + z\omega_n,$$

so leuchtet ein, daß die m Basiszahlen α'_μ in $\mathfrak{o}$ enthalten sind; mithin ist $\mathfrak{a}$ teilbar durch $\mathfrak{o}$, und da $\mathfrak{o}$ eine Summe von n einfachen Moduln ist, so gilt (nach dem vorhergehenden Satze II) dasselbe auch von $\mathfrak{a}$, w. z. b. w.

Es braucht kaum bemerkt zu werden, daß $\mathfrak{a}$ auch nicht als Summe von weniger als n einfachen Moduln darstellbar ist, weil sonst je n Zahlen in $\mathfrak{a}$ ein nach Z reduzibles System bilden würden (D. S. 468). Wir schließen unsere Untersuchung mit dem Beweis des folgenden Satzes (vgl. D. S. 521—523):

IV. Sind die beiden endlichen Moduln $\mathfrak{a}$, $\mathfrak{b}$ als Summen von einfachen Moduln in der Form

$$\mathfrak{a} = \sum^{\nu} x_\nu \alpha_\nu = x_1 \alpha_1 + \cdots + x_n \alpha_n, \tag{89}$$

$$\mathfrak{b} = \sum^{\mu} y_\mu \beta_\mu = y_1 \beta_1 + \cdots + y_m \beta_m \tag{90}$$

dargestellt, wo x_ν, y_μ Idealbrüche, α_ν, β_μ von Null verschiedene Zahlen bedeuten, so bestehen die erforderlichen und hinreichenden Bedingungen für die Teilbarkeit

$$\mathfrak{b} > \mathfrak{a} \tag{91}$$

in m Gleichungen von der Form

$$\beta_\mu = \sum^{\nu} c_{\mu,\nu}\, \alpha_\nu = c_{\mu,1} \alpha_1 + \cdots + c_{\mu,n} \alpha_n, \tag{92}$$

wo die mn Zahlen $c_{\mu,\nu}$ den Bedingungen

$$y_\mu c_{\mu,\nu} > x_\nu \tag{93}$$

genügen. Ist ferner das System der n Zahlen α_ν irreduzibel nach Z, und setzt man

$$X = x_1 x_2 \cdots x_n, \tag{94}$$

so wird

$$(\mathfrak{a};\, \mathfrak{b})\, X = \sum Y_\sigma\, C_\sigma, \tag{95}$$

wo die Modulsumme auf alle Kombinationen σ von je n Zahlen $\mu = 1', 2', \cdots, n'$ aus der Reihe $1, 2, \cdots, m$ zu erstrecken und entsprechend

$$Y_\sigma = y_{1'} y_{2'} \cdots y_{n'}, \tag{96}$$

$$C_\sigma = \sum \pm c_{1',1}\, c_{2',2} \cdots c_{n',n} \tag{97}$$

gesetzt ist.

Der erste Teil dieses Satzes ist leicht zu beweisen. Soll nämlich die Teilbarkeit (91) gelten, so muß auch $y_\mu \beta_\mu > \mathfrak{a}$, also

$$z \beta_\mu > \mathfrak{a}\, y_\mu^{-1} = \sum^{\nu} y_\mu^{-1} x_\nu \alpha_\nu$$

sein, und hieraus folgt die Existenz von Zahlen $c_{\mu,\nu}$, welche den Bedingungen (92), (93) genügen; und umgekehrt, wenn dieselben erfüllt sind, so folgt aus dem Hilfssatz (63), daß

$$y_\mu \beta_\mu = y_\mu \sum^{\nu} c_{\mu,\nu} \alpha_\nu > \sum^{\nu} y_\mu c_{\mu,\nu} \alpha_\nu > \sum^{\nu} x_\nu \alpha_\nu = \mathfrak{a},$$

also auch $\mathfrak{b} > \mathfrak{a}$ ist, was zu zeigen war. Den Beweis des zweiten Teiles kann man auf verschiedene Art führen; entweder transformiert man (nach II) den Modul $\mathfrak{b}$ in eine Summe von höchstens n einfachen Moduln und benutzt den dort bewiesenen Satz (86), oder man stützt sich unmittelbar auf den in § 4 enthaltenen Determinantensatz (62). Indem wir die Durchführung der ersteren Beweisart dem Leser überlassen (vgl. D. S. 519—523), wenden wir uns sofort zu der letzteren und betrachten alle Lösungen L der mit (59) übereinstimmenden Kongruenz

$$a_1 \alpha_1 + a_2 \alpha_2 + \cdots + a_n \alpha_n \equiv 0 \pmod{\mathfrak{b}} \tag{98}$$

durch n Zahlen a_ν, welche bzw. den Idealbrüchen x_ν angehören. Nun ist zufolge (90) diese Kongruenz gleichbedeutend mit der Existenz von m Zahlen b_μ, welche bzw. in den Idealbrüchen y_μ enthalten sind und der Gleichung

$$\sum^{\nu} a_\nu \alpha_\nu = \sum^{\mu} b_\mu \beta_\mu \tag{99}$$

genügen, und diese zerfällt zufolge (92) und vermöge der Irreduzibilität des Systems der n Zahlen α_ν in n Gleichungen von der Form

$$a_\nu = \sum^{\mu} b_\mu c_{\mu,\nu}; \tag{100}$$

und umgekehrt folgt aus (92), (93), (90), daß jedes beliebige System von m aus den Idealbrüchen y_μ gewählten Zahlen b_μ vermöge (100) ein System von n Zahlen a_ν erzeugt, welche bzw. den Idealbrüchen x_ν angehören und zugleich eine Lösung L der Kongruenz (98) bilden. Betrachtet man nun (wie in § 4) irgendein System von n solchen Lösungen $L', L'', \cdots, L^{(n)}$, die wir ebenso wie die zugehörigen Zahlen a_ν, b_μ durch Akzente unterscheiden, so folgt aus (100), daß die aus den n^2 Zahlen $a_\nu^{(\nu')}$ gebildete Determinante

$$A = \sum^{\sigma} B_\sigma C_\sigma \tag{101}$$

ist, wo die Summe sich über alle im Satze genannten Kombinationen σ erstreckt und jede Determinante B_σ auf dieselbe Weise aus den

Zahlen $b_\mu^{(\nu)}$ gebildet ist wie C_σ aus den Zahlen $c_{\mu,\nu}$ in (97). Da nun jede Zahl $b_\mu^{(\nu)}$ in y_μ enthalten ist, so ist jedes Glied der Determinante B_σ und folglich diese selbst in dem Produkte Y_σ enthalten, welches in (96) erklärt ist, also $z B_\sigma > Y_\sigma$, mithin ergibt sich aus (101) mit Rücksicht auf den Hilfssatz (63)

$$z A > \sum^{\sigma} z B_\sigma C_\sigma > \sum^{\sigma} Y_\sigma C_\sigma, \tag{102}$$

also zufolge (62) auch

$$(\mathfrak{a}; \mathfrak{b})\, X > \sum^{\sigma} Y_\sigma C_\sigma. \tag{103}$$

Wenn alle Determinanten C_σ verschwinden (wohin auch der Fall $m < n$ gehört), so bilden bekanntlich (D. S. 469) je n der m Zahlen β_μ in (92) und folglich auch je n Zahlen des Moduls $\mathfrak{b}$ in (90) ein nach Z reduzibles System; da aber allgemein $(\mathfrak{a}, \mathfrak{b})\, \mathfrak{a} > \mathfrak{b}$ ist (D. S. 511), so muß in diesem Falle gewiß $(\mathfrak{a}, \mathfrak{b}) = 0$ sein, weil sonst irgendein in $\mathfrak{a}$ enthaltenes irreduzibles System von n Zahlen α_ν', wie es zufolge (89) gewiß existiert, durch Multiplikation mit $(\mathfrak{a}, \mathfrak{b})$ in ein ebenfalls irreduzibles System von n Zahlen in $\mathfrak{b}$ verwandelt würde; mithin ist zufolge (33) auch $(\mathfrak{a}; \mathfrak{b}) = 0$. Dies folgt aber auch unmittelbar aus (103), und unser Satz (95) ist also in diesem Falle richtig.

Wenn aber die Determinanten C_σ nicht alle verschwinden, so ist die in Z enthaltene Modulsumme

$$e = \sum^{\sigma} Y_\sigma C_\sigma \tag{104}$$

auch von Null verschieden, also (nach § 1) ein Idealbruch, und zufolge (102) ist $A e^{-1}$ stets (falls A nicht verschwindet) ein Ideal. Bedeutet nun p irgendein gegebenes Primideal, so folgt aus

$$\sum^{\sigma} Y_\sigma C_\sigma e^{-1} = z,$$

daß es mindestens eine Kombination σ gibt — sie mag aus den n ersten Indizes $\nu = 1, 2, \cdots, n$ bestehen —, für welche das zugehörige Ideal $Y_\sigma C_\sigma e^{-1}$ nicht durch p teilbar ist. Für jeden solchen Index ν bilden wir nun nach (100) eine Lösung $L^{(\nu)}$ der Kongruenz (98), indem wir die sämtlichen m Zahlen $b_\mu = 0$ setzen mit einziger Ausnahme der Zahl b_ν, für welche wir eine noch näher

zu bestimmende Zahl $b_\nu^{(\nu)}$ des Idealbruchs y_ν wählen; dieses System von m Zahlen b_μ erzeugt nach (100) eine aus den n Zahlen

$$a_1^{(\nu)} = b_\nu^{(\nu)} c_{\nu,1}, \quad a_2^{(\nu)} = b_\nu^{(\nu)} c_{\nu,2}, \cdots, a_n^{(\nu)} = b_\nu^{(\nu)} c_{\nu,n}$$

bestehende Lösung $L^{(\nu)}$ der Kongruenz (98), und wenn man ebenso mit jedem der n Indizes $1, 2, \cdots, n$ der Kombination σ verfährt, so erhält man n Lösungen $L', L'', \cdots, L^{(n)}$ der Kongruenz (98), denen nach (101) die aus einem einzigen Gliede bestehende Determinante

$$A = B_\sigma C_\sigma$$

entspricht, wo

$$B_\sigma = b_1' b_2'' \cdots b_n^{(n)}, \quad C_\sigma = \sum \pm c_{1,1} c_{2,2} \cdots c_{n,n}.$$

Nun kann man aber (nach § 2, I) jede Zahl $b_\nu^{(\nu)}$ aus dem entsprechenden einfachen Modul oder Idealbruch y_ν so auswählen, daß das Ideal $b_\nu^{(\nu)} y_\nu^{-1}$ und folglich auch das Produkt $B_\sigma Y_\sigma^{-1}$ dieser n Ideale nicht durch p teilbar wird; bezeichnet man dasselbe mit q, so wird $B_\sigma = q Y_\sigma$, also

$$A e^{-1} = B_\sigma C_\sigma e^{-1} = q \cdot Y_\sigma C_\sigma e^{-1},$$

und folglich ist auch das Ideal $A e^{-1}$ nicht teilbar durch das Primideal p. Hiermit ist offenbar bewiesen, daß $z = \sum A e^{-1}$ der größte gemeinsame Teiler aller Ideale $A e^{-1}$, also auch

$$\sum z A = e$$

ist, und dies ist zufolge (62) und (104) nur eine andere Form für unseren Satz (95), w. z. b. w.

In dem Falle $m = n$, welcher in den Anwendungen am häufigsten auftritt, nimmt unser Satz (95) offenbar die Form

(105) $$(\mathfrak{a}; \mathfrak{b})\, X = Y C$$

an, wo

(106) $$Y = y_1 y_2 \cdots y_n$$

und

(107) $$C = \sum \pm c_{1,1} c_{2,2} \cdots c_{n,n}$$

ist (vgl. D. S. 523).

Nachdem hiermit die wichtigsten der auf das neue Symbol $(\mathfrak{a}; \mathfrak{b})$ bezüglichen Sätze bewiesen sind, bemerken wir endlich noch folgendes. Es ist schon oben (am Schlusse von § 2) erwähnt, daß in dieses Symbol eigentlich die Beziehung der Moduln $\mathfrak{a}, \mathfrak{b}$ auf den Körper Z

oder auf das System z aller in Z enthaltenen ganzen Zahlen aufgenommen werden müßte; am einfachsten würde man zu diesem Zwecke das Zeichen $(\mathfrak{a}; \mathfrak{b})$ etwa durch $(\mathfrak{a}, \mathfrak{b}, z)$ ersetzen, wo $\mathfrak{a}, \mathfrak{b}$ immer solche Moduln bedeuten, welche die Eigenschaft (2) besitzen. In der gegenwärtigen Abhandlung konnte dies der Kürze halber unterbleiben, weil alle Moduln $\mathfrak{a}, \mathfrak{b}$ ausschließlich auf diesen einzigen Körper Z bezogen wurden. Die genauere Bezeichnung $(\mathfrak{a}, \mathfrak{b}, z)$ wird aber notwendig, wenn mehrere solche Körper betrachtet werden. Nehmen wir z. B. an, es sei Z Divisor eines endlichen Körpers Ω und $\mathfrak{o}$ das System aller in Ω enthaltenen ganzen Zahlen, so wird jeder Modul $\mathfrak{a}$, welcher der Bedingung $\mathfrak{o}\,\mathfrak{a} = \mathfrak{a}$ genügt, auch die Eigenschaft (2) besitzen, weil $z > \mathfrak{o}$ ist. Zwei solche Moduln $\mathfrak{a}, \mathfrak{b}$ erzeugen also ein Ideal $(\mathfrak{a}, \mathfrak{b}, \mathfrak{o})$ des Körpers Ω und zugleich ein Ideal $(\mathfrak{a}, \mathfrak{b}, z)$ des Körpers Z, und unser Satz (31) ist nur ein spezieller Fall des allgemeinen Satzes

$$(108) \qquad (\mathfrak{a}, \mathfrak{b}, z) = \mathfrak{N}(\mathfrak{a}, \mathfrak{b}, \mathfrak{o}),$$

wo $\mathfrak{N}$ das Zeichen für die in bezug auf Z genommene Partialnorm von Zahlen oder Idealen des Körpers Ω bedeutet. Die ausführliche Darstellung dieser ebenfalls in der Einleitung erwähnten Untersuchungen muß aber einer besonderen Abhandlung vorbehalten bleiben.

Braunschweig, 4. Februar 1895.

Erläuterungen zur vorstehenden Abhandlung.

In der vorliegenden Arbeit wird die Normentheorie derjenigen endlichen Moduln entwickelt, deren Multiplikatorenbereich die Hauptordnung eines endlichen Zahlkörpers Z ist, insbesondere also die Theorie der „Relativnormen“ von Idealen. Und zwar beruhen die Entwicklungen wesentlich auf der Tatsache, daß ein großer Teil der üblichen Schlüsse erhalten bleibt, wenn statt der Gruppe der von Null verschiedenen rationalen Zahlen diejenige der ganzen und gebrochenen Ideale aus Z genommen wird. An Stelle der eingliedrigen Moduln treten dabei die „einfachen“, die den Idealen einer Klasse operatorisomorph sind; die Norm ist definiert vermöge einer (verallgemeinerten) Kompositionsreihe, deren Kompositionsfaktoren einfache Moduln sind. Daraus folgt insbesondere ohne jede Rechnung die wichtige Tatsache (31), die Formel für die Zwischennormen. Aber auch die Sätze über die Untermoduln n-gliedriger Moduln übertragen sich vollständig (§ 5, II, III); insbesondere wird ein Modul vom Rang n direkte Summe von n einfachen.

Kompliziert wird nur der — bei dem hier gegebenen Aufbau ganz unwesentliche — Zusammenhang mit Determinantendarstellung (§ 4). Der am Schluß dieses Paragraphen ausgesprochene Wunsch nach einem einfacheren Aufbau ist unterdes erfüllt: durch Übergang zum Quotientenring nach geeigneten Idealen — also Übergang zu den einzelnen Stellen, zur „Modultheorie im Kleinen“ — wird der Multiplikatorenbereich ein Hauptidealring, und alles läuft wie bei den Moduln in bezug auf ganze rationale Zahlen (H. Grell, Zur Theorie der Ordnungen, Math. Ann. **96**, 1927). Nicht erfaßt werden aber dabei, wegen des Hineinspielens der Idealklassen, die oben erwähnten Sätze II, III aus § 5, die somit als „Modultheorie im Großen“ anzusehen sind. Unter spezielleren Voraussetzungen — Linearformenmoduln — und dadurch mit im Spezialfall etwas weitergehenden Resultaten ist, auf weniger abstrakter Basis und scheinbar ganz unabhängig, diese „Modultheorie im Großen“ von E. Steinitz wieder entwickelt worden (Math. Ann. **71** und **72**, 1912), und von J. Schur zu Folgerungen für Gruppen linearer Substitutionen verwandt (Math. Ann. **71**). Die Dedekindsche Modultheorie im Großen ist auf arithmetische Fragen noch nicht angewandt worden; es scheint nicht ausgeschlossen, daß sie für die Theorie der Relativkörper noch von Bedeutung wird.

Noether.

XXVII.

Über Gruppen, deren sämtliche Teiler Normalteiler sind.

[Mathematische Annalen, Bd. 48, S. 548—561 (1897).]

Die vorliegende Untersuchung, welche ich in den ersten Herbstwochen des Jahres 1895 begonnen und beendet habe, ist durch die Frage nach allen denjenigen endlichen Zahlenkörpern veranlaßt, deren sämtliche Divisoren Normalkörper sind. Ist R die Gruppe aller Permutationen φ eines Normalkörpers Ω, so gehört bekanntlich zu jeder Gruppe S, welche ein Teiler von R ist, ein bestimmter Körper Ω', nämlich der Inbegriff aller derjenigen Zahlen in Ω, welche durch jede Permutation der Gruppe S in sich selbst übergehen, und umgekehrt gehört jeder Divisor von Ω, d. h. jeder in Ω enthaltene Körper Ω' zu einer bestimmten in R als Teiler enthaltenen Gruppe S; die Bedingung aber, daß Ω' wieder ein Normalkörper ist, besteht darin, daß S ein Normalteiler*) von R, also immer

$$\varphi^{-1} S \varphi = S, \qquad S\varphi = \varphi S \tag{1}$$

ist, wo φ jedes beliebige Element der Gruppe R bedeutet. Der auf die Gruppentheorie bezügliche Teil der obigen Frage kommt daher auf die Aufgabe zurück, die allgemeinste Form einer Gruppe R zu finden, deren sämtliche Teiler S Normalteiler von R sind.

Zu diesen Gruppen R gehören offenbar alle Abelschen, d. h. diejenigen Gruppen, deren Elemente sämtlich miteinander permutabel

*) Diese Benennung, welche H. Weber in seinem Lehrbuch der Algebra (Bd. I, 1895, S. 511) eingeführt hat, scheint mir aus mehreren Gründen zweckmäßiger als die sonst gebräuchlichen eines ausgezeichneten oder invarianten oder eigentlichen Teilers, welche letztere Bezeichnung ich in meinen Göttinger Vorlesungen (1857—1858) im Anschluß an eine Ausdrucksweise von Galois benutzt habe. Sind R, S irgend zwei verwandte, d. h. solche Gruppen, die ein gemeinsames Multiplum besitzen, und bedeutet φ jedes Element von R, so empfiehlt es sich aus algebraischen Gründen, den größten gemeinsamen Teiler aller Gruppen $\varphi^{-1} S \varphi$ die Norm von S in bezug auf R zu nennen.

sind; ihr Bau darf als hinreichend bekannt vorausgesetzt werden, und es handelt sich daher nur noch um die Form der nicht Abelschen Gruppen R, welche ich im folgenden Hamiltonsche Gruppen nennen werde. Die einfachste oder kleinste solche Gruppe R ist nämlich diejenige Gruppe achten Grades, welche sechs verschiedene Elemente vierten Grades enthält und welche wegen ihrer innigen Beziehungen zu Hamiltons berühmter Zahlenschöpfung die Quaternionengruppe Q heißen mag. Sodann ergibt sich das durch seine enge Umgrenzung überraschende Resultat, daß die allgemeinste Hamiltonsche Gruppe die Form

$$R = PQ \tag{2}$$

besitzt, wo P die Abelsche Gruppe aller derjenigen Elemente in R bedeutet, welche mit jedem Element von R permutabel sind; diese Gruppe P unterliegt nur den beiden Bedingungen, daß sie kein einziges Element vierten Grades, wohl aber das in der Quaternionengruppe Q befindliche Element zweiten Grades enthält.

§ 1.

Die Quaterniongruppe Q.

Man kann dieselbe (wie in der Einleitung) als Gruppe achten Grades definieren, welche sechs verschiedene Elemente vierten Grades enthält; die letzteren bilden offenbar drei Paare von je zwei reziproken Elementen und mögen mit $\alpha, \alpha^{-1}, \beta, \beta^{-1}, \gamma, \gamma^{-1}$ bezeichnet werden; außer dem Hauptelemente 1 muß Q endlich noch ein Element ε vom zweiten Grade enthalten. Es ist also

$$\varepsilon^2 = 1, \tag{3}$$

$$\alpha^2 = \alpha^{-2} = \beta^2 = \beta^{-2} = \gamma^2 = \gamma^{-2} = \varepsilon, \tag{4}$$

$$\varepsilon\alpha = \alpha\varepsilon = \alpha^{-1}, \quad \varepsilon\beta = \beta\varepsilon = \beta^{-1}, \quad \varepsilon\gamma = \gamma\varepsilon = \gamma^{-1}, \tag{5}$$

$$\varepsilon\alpha^{-1} = \alpha^{-1}\varepsilon = \alpha, \quad \varepsilon\beta^{-1} = \beta^{-1}\varepsilon = \beta, \quad \varepsilon\gamma^{-1} = \gamma^{-1}\varepsilon = \gamma. \tag{6}$$

Da nun das Produkt $\beta\gamma$ keine Potenz von β oder γ sein kann (weil sonst $\gamma = \beta^{\pm 1}$ wäre), so muß es mit einem der beiden übrigen Elemente $\alpha^{\pm 1}$ identisch sein. Offenbar dürfen wir die Bezeichnung der Elemente von Q so wählen, daß $\beta\gamma = \alpha$ wird; da hieraus $\beta\gamma\alpha = \alpha^2 = \beta^2$ und $\alpha\beta\gamma = \alpha^2 = \gamma^2$ folgt, so ergibt sich

$$\beta\gamma = \alpha, \qquad \gamma\alpha = \beta, \qquad \alpha\beta = \gamma. \tag{7}$$

Aus $(\beta\gamma)(\gamma\beta) = \beta(\gamma^2)\beta = \beta(\beta^2)\beta = \beta^4 = 1$ folgt ferner, daß $\beta\gamma$ und $\gamma\beta$ reziproke Elemente sind; aus (7) ergibt sich daher

(8) $$\gamma\beta = \alpha^{-1}, \quad \alpha\gamma = \beta^{-1}, \quad \beta\alpha = \gamma^{-1}.$$

Aus (7) und (8) folgen auch die Produkte der reziproken Elemente

(9) $$\gamma^{-1}\beta^{-1} = \alpha^{-1}, \quad \alpha^{-1}\gamma^{-1} = \beta^{-1}, \quad \beta^{-1}\alpha^{-1} = \gamma^{-1},$$

(10) $$\beta^{-1}\gamma^{-1} = \alpha, \quad \gamma^{-1}\alpha^{-1} = \beta, \quad \alpha^{-1}\beta^{-1} = \gamma.$$

Da ferner

(11) $$\alpha\alpha^{-1} = \alpha^{-1}\alpha = \beta\beta^{-1} = \beta^{-1}\beta = \gamma\gamma^{-1} = \gamma^{-1}\gamma = 1,$$

so ergeben sich aus den vorhergehenden Gleichungen auch die Produkte

(12) $$\gamma\beta^{-1} = \gamma^{-1}\beta = \alpha, \quad \beta\gamma^{-1} = \beta^{-1}\gamma = \alpha^{-1},$$

(13) $$\alpha\gamma^{-1} = \alpha^{-1}\gamma = \beta, \quad \gamma\alpha^{-1} = \gamma^{-1}\alpha = \beta^{-1},$$

(14) $$\beta\alpha^{-1} = \beta^{-1}\alpha = \gamma, \quad \alpha\beta^{-1} = \alpha^{-1}\beta = \gamma^{-1}.$$

Die Kompositionstabelle der Quaterniongruppe ist daher die folgende:

	1	ε	α^{-1}	α	β^{-1}	β	γ^{-1}	γ
1	1	ε	α^{-1}	α	β^{-1}	β	γ^{-1}	γ
ε	ε	1	α	α^{-1}	β	β^{-1}	γ	γ^{-1}
α	α	α^{-1}	1	ε	γ^{-1}	γ	β	β^{-1}
α^{-1}	α^{-1}	α	ε	1	γ	γ^{-1}	β^{-1}	β
β	β	β^{-1}	γ	γ^{-1}	1	ε	α^{-1}	α
β^{-1}	β^{-1}	β	γ^{-1}	γ	ε	1	α	α^{-1}
γ	γ	γ^{-1}	β^{-1}	β	α	α^{-1}	1	ε
γ^{-1}	γ^{-1}	γ	β	β^{-1}	α^{-1}	α	ε	1

wo das durch die Zeile φ und Spalte ψ bestimmte Feld das Produkt $\varphi\psi$ enthält.

Statt von der obigen Definition der Quaterniongruppe Q kann man auch von der folgenden ausgehen: die Gruppe Q wird durch zwei nicht permutable Elemente α, β erzeugt, welche den Bedingungen

(15) $$\beta\alpha\beta = \alpha, \quad \alpha\beta\alpha = \beta$$

genügen. Führt man nämlich das dritte Element $\gamma = \alpha\beta$ ein, so nehmen diese Bedingungen die Form (7) an, woraus alle anderen

Relationen leicht folgen. Durch Multiplikation der ersten Gleichung (7) mit α ergibt sich zunächst $\alpha^2 = \beta\gamma\alpha = \alpha\beta\gamma$; mit Rücksicht auf die zweite und dritte Gleichung (7) kann man daher das vierte Element ε durch

$$\varepsilon = \alpha^2 = \beta^2 = \gamma^2$$

einführen, welches folglich mit α, β, γ permutabel ist; die aus (7) folgende Gleichung

$$(\beta\gamma)\,(\gamma\alpha)\,(\alpha\beta) = \alpha\beta\gamma$$

ist daher identisch mit $\varepsilon^3 = \varepsilon$, also mit (3), und hieraus folgen offenbar die übrigen Gleichungen, also alle Kompositionen der Tabelle. Da wir ferner angenommen haben, daß die beiden erzeugenden Elemente α, β nicht permutabel sind, so ist $\gamma = \alpha\beta$ verschieden von $\gamma^{-1} = \beta\alpha$, mithin $\varepsilon = \gamma^2$ verschieden von 1, d. h. ε ist vom zweiten, und α, β, γ, α^{-1}, β^{-1}, γ^{-1} sind vom vierten Grade; man überzeugt sich auch leicht, daß alle diese Elemente voneinander verschieden sind.

Mag man aber von der einen oder der anderen Definition ausgehen und so zu der obigen Tabelle gelangen, so ist hiermit die Existenz der Gruppe Q noch nicht vollständig erwiesen; es muß bekanntlich noch gezeigt werden, daß sowohl aus $\varphi\psi = \varphi\chi$ wie aus $\psi\varphi = \chi\varphi$ immer $\psi = \chi$ folgt, und daß außerdem das Assoziationsgesetz $(\varphi\psi)\chi = \varphi(\psi\chi)$ gilt. Die erstere Eigenschaft ergibt sich zwar leicht aus dem Anblick der Tabelle, welche in jeder Zeile wie in jeder Spalte lauter verschiedene Elemente enthält; aber die Verifikation des Assoziationsgesetzes, wenn sie sich auch auf manche Art abkürzen läßt, würde doch schon ziemlich lästig sein. In solchen Fällen pflegt das einfachste Verfahren, um die Existenz einer durch erzeugende Elemente definierten Gruppe nachzuweisen, darin zu bestehen, daß man dieselbe als Teiler einer schon bekannten Gruppe G darstellt, weil dann die beiden obigen Gesetze von selbst erfüllt sind. Für unser Beispiel genügt es, die symmetrische Gruppe G aller $\Pi(8)$ Versetzungen von acht verschiedenen Dingen a, b, c, d, a', b', c', d' zu betrachten; benutzt man die bekannte Bezeichnung der Zyklen und setzt

$$(16)\qquad \begin{cases} \alpha = (d\,a\,d'\,a')(c\,b\,c'\,b'), \\ \beta = (d\,b\,d'\,b')(a\,c\,a'\,c'), \\ \gamma = (d\,c\,d'\,c')(b\,a\,b'\,a'), \\ \varepsilon = (a\,a')(b\,b')(c\,c')(d\,d'), \end{cases}$$

so erfüllen die beiden nicht permutablen Elemente α, β der Gruppe G wirklich die beiden Bedingungen (15), und folglich muß die von ihnen erzeugte Gruppe, welche ein Teiler von G ist, mit unserem System Q der acht verschiedenen Elemente $1, \varepsilon, \alpha, \beta, \gamma, \alpha^{-1}, \beta^{-1}, \gamma^{-1}$ identisch sein.

Diese Gruppe Q, deren Existenz hiermit gesichert ist, verdient den Namen der Quaterniongruppe zunächst wegen der augenscheinlichen Analogie zwischen der Komposition der drei Elemente vierten Grades α, β, γ und der Multiplikation der drei Hamiltonschen imaginären Einheiten i, j, k; es findet aber, wie ich schon im Februar 1886 erkannt habe, eine noch tiefer liegende Beziehung zwischen der Gruppe Q und Hamiltons Quaternionen statt, von welcher demnächst an einem anderen Orte gehandelt werden soll. Damals habe ich auch schon Normalkörper gebildet, deren Permutationsgruppe mit Q identisch ist; ein einfaches Beispiel, welches unendlich viele Spezialfälle umfaßt, liefert die Gleichung

$$\omega^2 = r(2 + \sqrt{2})(3 + \sqrt{6}),$$

wo r irgendeine von Null verschiedene rationale Zahl bedeutet; jede Wurzel ω einer solchen Gleichung erzeugt einen Quaternionkörper, d. h. einen Normalkörper achten Grades mit der Gruppe Q, und man kann beweisen, daß auf diese Weise jeder Quaternionkörper entsteht, der die Quadratwurzeln aus 2 und 3 enthält.

Daß aber diese Gruppe Q, welche außerdem schon in ganz anderen Untersuchungen aufgetreten ist, die in der Einleitung angegebene wichtige Bedeutung für alle Hamiltonschen Gruppen besitzt, habe ich erst im Herbste 1895 erkannt, und die Darlegung dieser Bedeutung bildet den ausschließlichen Gegenstand der vorliegenden Abhandlung.

Man überzeugt sich zunächst leicht, daß Q keine anderen Teiler als Normalteiler besitzt. Bezeichnet man der Kürze halber die durch irgendwelche Elemente $\varphi, \psi, \chi \cdots$ erzeugte Gruppe mit dem Symbol $[\varphi, \psi, \chi, \cdots]$, so daß z. B. $[\varphi]$ die aus allen Potenzen von φ bestehende zyklische oder reguläre Gruppe oder Periode bedeutet, so hat Q offenbar nur die folgenden sechs Teiler

$$(17) \qquad [1],\ [\varepsilon],\ [\alpha],\ [\beta],\ [\gamma],\ [\alpha, \beta] = Q;$$

daß $[1]$ und Q Normalteiler von Q sind, ist eine allgemeine Eigenschaft aller Gruppen; dasselbe gilt von $[\varepsilon]$, weil ε mit allen Elementen von Q permutabel ist, und auch z. B. von $[\alpha]$, weil

$$Q = [\alpha] + [\alpha]\beta \tag{18}$$

und

$$\beta^{-1}[\alpha]\beta = [\alpha^{-1}] = [\alpha] \tag{19}$$

ist. Also ist Q im Sinne der Einleitung wirklich eine Hamiltonsche Gruppe.

§ 2.

Kennzeichen der Hamiltonschen Gruppen.

Um die allgemeine Form aller Hamiltonschen Gruppen zu finden, ist es zweckmäßig, aus ihrer Definition, wie sie in der Einleitung gegeben ist, einfachere charakteristische Kennzeichen abzuleiten, welche in den folgenden Sätzen enthalten sind; daß dieselben auch für die Abelschen Gruppen gelten, welche also, wenn auch nur vorläufig, als ein spezieller Fall der Hamiltonschen Gruppen anzusehen sind, braucht kaum bemerkt zu werden*).

I. Die erforderliche und hinreichende Bedingung dafür, daß R eine Hamiltonsche Gruppe ist, besteht darin, daß, wenn φ, ψ irgendwelche Elemente von R bedeuten, das Element $\varphi^{-1}\psi\varphi$ eine Potenz von ψ, also in der Periode $[\psi]$ enthalten ist.

Denn wenn R eine Hamiltonsche (oder Abelsche) Gruppe ist, so muß $\varphi^{-1}[\psi]\varphi = [\psi]$, also $\varphi^{-1}\psi\varphi$ eine Potenz von ψ sein. Umgekehrt, wenn diese Bedingung durch alle Elemente φ, ψ einer Gruppe R erfüllt wird, und S irgendeine in R enthaltene Gruppe bedeutet, so wird, wenn ψ alle Elemente von S durchläuft, $\varphi^{-1}\psi\varphi$ als Potenz von ψ ebenfalls in S enthalten sein; mithin ist die aus den Elementen $\varphi^{-1}\psi\varphi$ bestehende Gruppe $\varphi^{-1}S\varphi$ ein Teiler von S und folglich $= S$, w. z. b. w.

Dieses Kennzeichen läßt sich in einer für unseren Zweck noch bequemeren Form ausdrücken, wenn man das durch die Bedingung

$$\psi\varphi = \varphi\psi\varepsilon \tag{20}$$

definierte Element

$$\varepsilon = (\psi^{-1}\varphi^{-1}\psi)\varphi = \psi^{-1}(\varphi^{-1}\psi\varphi) \tag{21}$$

*) Man könnte vielleicht beide Arten von Gruppen unter dem gemeinsamen Namen von Normalgruppen zusammenfassen.

einführt, welches wir der Kürze halber den Kommutator der Elemente φ, ψ nennen wollen*); der vorige Satz geht dann, weil

$$[\varphi^{-1}]\varphi = [\varphi]\varphi = [\varphi] \quad \text{und} \quad \psi^{-1}[\psi] = [\psi]$$

ist, offenbar in den folgenden über:

II. Die erforderliche und hinreichende Bedingung dafür, daß R eine Hamiltonsche Gruppe ist, besteht darin, daß der Kommutator ε von je zwei in R enthaltenen Elementen φ, ψ ein gemeinsames Element ihrer Perioden $[\varphi]$, $[\psi]$ und folglich auch mit allen Elementen der durch φ und ψ erzeugten Gruppe $[\varphi, \psi]$ permutabel ist.

Die nächsten Folgerungen, welche sich hieraus mit Zuziehung der bekannten, für je zwei Elemente ϱ, σ einer beliebigen Gruppe und für jede ganze rationale Zahl s gültigen Identität

$$\varrho^{-1}\sigma^s\varrho = (\varrho^{-1}\sigma\varrho)^s \tag{22}$$

ergeben, bilden den folgenden Satz:

III. Ist ε der Kommutator der Elemente φ, ψ einer Hamiltonschen Gruppe, so ist

$$\psi^n\varphi^m = \varphi^m\psi^n\varepsilon^{mn}, \tag{23}$$

$$(\varphi^m\psi^n)^t = \varphi^{mt}\psi^{nt}\varepsilon^{\frac{1}{2}mnt(t-1)}, \tag{24}$$

und die durch φ und ψ erzeugte Gruppe ist

$$[\varphi, \psi] = [\varphi][\psi] = [\psi][\varphi]. \tag{25}$$

Setzt man ferner

$$\varphi_1 = \varphi^m\psi^n, \qquad \psi_1 = \varphi^r\psi^s, \tag{26}$$

so ist

$$\varepsilon_1 = \varepsilon^{ms-nr} \tag{27}$$

der Kommutator der Elemente φ_1, ψ_1.

Wendet man nämlich die Identität (22) auf das Beispiel $\varrho = \varphi$, $\sigma = \psi$, $s = n$ an, so wird $\varrho^{-1}\sigma\varrho = \varphi^{-1}\psi\varphi = \psi\varepsilon$, und weil ψ zufolge II mit ε permutabel ist, so erhält man

$$\varphi^{-1}\psi^n\varphi = (\psi\varepsilon)^n = \psi^n\varepsilon^n,$$

also

$$\psi^{-n}\varphi^{-1}\psi^n = \varepsilon^n\varphi^{-1};$$

*) Ohne auf die Bedeutung dieses Begriffes für die allgemeine Gruppentheorie näher einzugehen, will ich nur den Satz erwähnen, daß der größte in einem Normalkörper von der Gruppe G enthaltene Abelsche Körper zu derjenigen Gruppe gehört, welche durch alle in G enthaltenen Kommutatoren erzeugt wird.

setzt man daher in (22) jetzt $\varrho = \psi^n$, $\sigma = \varphi^{-1}$, $s = m$, so wird $\varrho^{-1}\sigma\varrho = \varepsilon^n\varphi^{-1}$, und weil ε^n mit φ^{-1} permutabel ist, so erhält man

$$\psi^{-n}\varphi^{-m}\psi^n = (\varepsilon^n\varphi^{-1})^m = \varepsilon^{mn}\varphi^{-m},$$

also die Gleichung (23), und hieraus folgt leicht durch vollständige Induktion der Satz (24); denn wenn derselbe für eine bestimmte ganze rationale Zahl t gilt (wie z. B. für $t = 0$), so folgt durch Multiplikation mit $\varphi^m\psi^n$ oder mit dem reziproken Element $\psi^{-n}\varphi^{-m}$ unter Zuziehung von (23), daß er auch für die beiden benachbarten Zahlen $t \pm 1$ gilt. Aus (23) und (26) folgt ferner

$$\varphi_1\psi_1 = \varphi^m(\psi^n\varphi^r)\psi^s = \varphi^{m+r}\psi^{n+s}\varepsilon^{nr},$$
$$\psi_1\varphi_1 = \varphi^r(\psi^s\varphi^m)\psi^n = \varphi^{m+r}\psi^{n+s}\varepsilon^{ms},$$

und da ε Potenz von ψ ist, so sind alle Produkte $\varphi_1\psi_1$ von je zwei in dem Komplex $[\varphi][\psi]$ enthaltenen Elementen φ_1, ψ_1 in demselben Komplex enthalten, woraus (25) folgt; zugleich ergibt sich aus den beiden vorstehenden Gleichungen auch der Kommutator ε_1 in der Form (27), w. z. b. w.

§ 3.

Eigenschaften zweier nicht permutablen Elemente einer Hamiltonschen Gruppe.

Die zuletzt erhaltenen Resultate sind offenbar nur dann von Interesse, wenn die beiden Elemente φ, ψ nicht permutabel sind, was wir im folgenden annehmen; ihr Kommutator ε ist dann verschieden von dem Hauptelement 1 der Hamiltonschen Gruppe R; bedeutet daher e den Grad des Elementes ε und der Periode $[\varepsilon]$, so ist

$$e > 1, \quad \varepsilon^e = 1. \tag{28}$$

Wählt man nun die Exponenten m, n des Elementes φ_1 in (26) so, daß m, n, e keinen gemeinsamen Teiler haben, so kann man die Exponenten r, s des anderen Elementes ψ_1 so bestimmen, daß $ms - nr \equiv 1 \pmod{e}$ wird; nach (27) folgt hieraus $\varepsilon_1 = \varepsilon$, und da der Kommutator ε_1 der Elemente φ_1, ψ_1 nach Satz II eine Potenz von φ_1 ist, so ergibt sich nach (24) die Existenz einer ganzen Zahl t, welche der Bedingung

$$\varphi^{mt}\psi^{nt}\varepsilon^{\frac{1}{2}mnt(t-1)} = \varepsilon \tag{29}$$

genügt.

Um diesen Existenzsatz für unseren Zweck zu verwerten, wird es nötig, die Perioden $[\varphi]$, $[\psi]$ und deren größten gemeinsamen Teiler D, welcher bekanntlich selbst eine Periode ist, genauer zu betrachten. Da die Periode $[\varepsilon]$ nach Satz II ein gemeinsamer Teiler von $[\varphi]$, $[\psi]$, also auch ein Teiler von D ist, so ist der Grad von D teilbar durch e, also von der Form de. Da ferner jedes Element in D von der Form φ^m und zugleich eine Potenz von ψ, also auch mit ψ permutabel ist, so folgt aus (23), wenn man dort $n = 1$ setzt, daß $\varepsilon^m = 1$, also m durch e teilbar sein muß; alle Elemente von D sind daher Potenzen von φ^e, und da offenbar auf dieselbe Weise folgt, daß sie auch Potenzen von ψ^e sein müssen, so ist der größte gemeinsame Teiler D der Perioden $[\varphi]$, $[\psi]$ zugleich derjenige der Perioden $[\varphi^e]$, $[\psi^e]$; bezeichnet man daher die Grade der letzteren, weil sie durch den von D teilbar sein müssen, mit ade, bde, so sind ade^2, bde^2 die Grade von $[\varphi]$, $[\psi]$, und zufolge (25) ist nach einem bekannten Satze $abde^3$ der Grad von $[\varphi, \psi]$, woraus beiläufig folgt, daß der Grad einer Hamiltonschen Gruppe nicht kleiner als acht sein kann. Zugleich ergeben sich folgende Darstellungen unserer Gruppen:

$$[\varepsilon] = [\varphi^{ade}] = [\psi^{bde}], \tag{30}$$

$$\begin{aligned} D &= [\varphi^{ae}] = [\psi^{be}] \\ &= [\varepsilon](1 + \varphi^{ae} + \varphi^{2ae} + \cdots + \varphi^{(d-1)ae}) \\ &= [\varepsilon](1 + \psi^{be} + \psi^{2be} + \cdots + \psi^{(d-1)be}), \end{aligned} \tag{31}$$

$$[\varphi] = D(1 + \varphi + \varphi^2 + \cdots + \varphi^{ae-1}), \tag{32}$$

$$[\psi] = D(1 + \psi + \psi^2 + \cdots + \psi^{be-1}), \tag{33}$$

$$\begin{aligned} [\varphi, \psi] &= [\varphi][\psi] = [\psi][\varphi] \\ &= [\varphi](1 + \psi + \psi^2 + \cdots + \psi^{be-1}) \\ &= [\psi](1 + \varphi + \varphi^2 + \cdots + \varphi^{ae-1}) \end{aligned} \tag{34}$$

und aus den beiden ersten Darstellungen von D folgt die Existenz von zwei ganzen Zahlen h, k, welche den Bedingungen

$$\varphi^{ae} = \psi^{bek}, \quad \psi^{be} = \varphi^{aeh}, \quad hk \equiv 1 \pmod{de} \tag{35}$$

genügen.

Wir wenden uns nun dazu, den Existenzsatz (29) zur Geltung zu bringen; statt dies in voller Allgemeinheit durchzuführen, ziehen wir es vor, ihn auf zwei spezielle Beispiele von Zahlenpaaren m, n anzuwenden, was bequemer und ebenso erfolgreich ist.

Erstes Beispiel. Bedeutet c den größten gemeinsamen Teiler der beiden Zahlen

(36) $$a = ca', \qquad b = cb',$$

so setzen wir

$$m = -ha', \qquad n = b';$$

dann haben die Zahlen m, n, e zufolge (35), (36) keinen gemeinsamen Teiler, und es gibt daher zufolge (29) eine ganze Zahl t, welche der Bedingung

$$\varphi^{-ha't}\,\psi^{b't}\,\varepsilon^{-\frac{1}{2}ha'b't(t-1)} = \varepsilon$$

genügt. Da ε Potenz von φ ist, so muß $\psi^{b't}$ in D enthalten, also $b't$ zufolge (31) teilbar sein durch $be = b'ce$; mithin wird $t = ceu$, wo u eine ganze Zahl bedeutet, und da nach (35), (36) hieraus

$$\psi^{b't} = \psi^{beu} = \varphi^{aehu} = \varphi^{ha't}$$

folgt, so geht die obige Bedingung für t in

$$\varepsilon^{-\frac{1}{2}ha'b'ceu\,(ceu-1)} = \varepsilon,$$

also in die Kongruenz

$$-\tfrac{1}{2}ha'b'ceu(ceu-1) \equiv 1 \,(\text{mod. } e)$$

über. Da unter den Faktoren der linken Seite sich auch die Zahl e befindet, so ergibt sich durch Multiplikation mit 2 das Resultat

$$2 \equiv 0 \,(\text{mod. } e),$$

also zufolge (28)

(37) $$e = 2, \quad \varepsilon^2 = 1,$$

und hierdurch geht die vorstehende Kongruenz in

$$ha'b'cu \equiv 1 \,(\text{mod. } 2)$$

über, woraus mit Rücksicht auf (36) auch

(38) $$1 \equiv h \equiv a' \equiv b' \equiv c \equiv a \equiv b \,(\text{mod. } 2)$$

folgt. Die Grade von $[\varphi]$, $[\psi]$ sind $4ad$, $4bd$, und zufolge (30) ist

(39) $$\varepsilon = \varphi^{2ad} = \psi^{2bd}.$$

Der Grad der Gruppe $[\varphi, \psi]$ ist $= 8abd$.

Zweites Beispiel. Setzen wir

$$m = a(d-h), \qquad n = b,$$

so haben die Zahlen m, n, e zufolge (37), (38) keinen gemeinsamen Teiler, und außerdem ist zufolge (38) das Produkt

$$mn \equiv d-1 \,(\text{mod. } 2);$$

es gibt daher zufolge (29) eine ganze Zahl t, welche der Bedingung

$$\varphi^{a(d-h)t}\psi^{bt}\varepsilon^{\frac{1}{2}(d-1)t(t-1)} = \varepsilon$$

genügt. Da ε Potenz von φ ist, so muß ψ^{bt} in D enthalten, also bt zufolge (31) teilbar sein durch $be = 2b$; mithin wird $t = 2u$, wo u wieder eine ganze Zahl bedeutet, also $\frac{1}{2}t(t-1) \equiv u \pmod 2$; mit Rücksicht auf (35), (39) wird zugleich

$$\psi^{bt} = \psi^{2bu} = \varphi^{2ahu} = \varphi^{aht},$$
$$\varphi^{a(d-h)t}\psi^{bt} = \varphi^{adt} = \varphi^{2adu} = \varepsilon^{u},$$

mithin kommt die obige Bedingung für t auf

$$\varepsilon^{du} = \varepsilon$$

zurück, woraus

(40) $$d \equiv 1 \pmod 2$$

folgt.

Die in (37), (38), (39), (40) gewonnenen fundamentalen Resultate fassen wir zusammen in den folgenden Satz:

IV. Die Grade von je zwei nicht permutablen Elementen φ, ψ einer Hamiltonschen Gruppe sind $\equiv 4 \pmod 8$; bezeichnet man dieselben bzw. mit $8r+4$, $8s+4$, so ist der durch $\psi\varphi = \varphi\psi\varepsilon$ definierte Kommutator

(41) $$\varepsilon = \varphi^{4r+2} = \psi^{4s+2},$$

also vom Grade zwei.

§ 4.

Allgemeine Form der Hamiltonschen Gruppen.

Mit Hilfe der eben gewonnenen Grundlage gelingt es nun ohne Schwierigkeit, die allgemeine Form aller Hamiltonschen (nicht Abelschen) Gruppen R zu finden.

Diejenigen Elemente π einer solchen (oder auch jeder anderen) Gruppe R, welche mit jedem Element ω von R permutabel sind, bilden bekanntlich eine Gruppe, weil aus $\pi'\omega = \omega\pi'$ und $\pi''\omega = \omega\pi''$ auch $(\pi'\pi'')\omega = \omega(\pi'\pi'')$ folgt; diese, offenbar Abelsche Gruppe soll im folgenden durchweg mit P bezeichnet werden. Da R eine Hamiltonsche, also nicht Abelsche Gruppe ist, so muß P ein echter Teiler von R, d. h. verschieden von R sein, und es gibt mindestens zwei Elemente φ, ψ, welche nicht miteinander permutabel

und folglich auch nicht in P enthalten sind. Behalten wir für diese Elemente die Bezeichnungen unseres letzten Satzes IV bei, und setzen wir

$$\alpha = \varphi^{2r+1}, \quad \beta = \psi^{2s+1},$$

so ist

$$\alpha^4 = \beta^4 = 1,$$

und für den Kommutator ε der Elemente φ, ψ, welcher vom zweiten Grade ist, ergibt sich

$$\varepsilon = \alpha^2 = \beta^2, \quad \varepsilon^2 = 1;$$

wendet man ferner den Satz (23) auf das Beispiel $m = 2r + 1$, $n = 2s + 1$ an, so folgt

$$\beta\alpha = \alpha\beta\varepsilon,$$

d. h. ε ist auch der Kommutator der Elemente α, β, welche folglich nicht miteinander, wohl aber mit ε permutabel sind. Da nun aus der letzten Gleichung auch

$$\begin{aligned} \beta\alpha\beta &= \alpha\beta\varepsilon\beta = \alpha\beta^2\varepsilon = \alpha\varepsilon^2 = \alpha, \\ \alpha\beta\alpha &= \alpha^2\beta\varepsilon = \varepsilon\beta\varepsilon = \beta\varepsilon^2 = \beta \end{aligned}$$

folgt, so ergibt sich aus dem Vergleiche mit (15) in § 1, daß α, β die erzeugenden Elemente einer Quaterniongruppe Q sind. Es gilt daher der folgende Satz:

V. In jeder Hamiltonschen Gruppe R ist mindestens eine Quaterniongruppe Q als Teiler enthalten.

Wir untersuchen nun im folgenden die Beziehungen zwischen den beiden in R enthaltenen Gruppen P, Q, wobei wir für die letztere alle in § 1 benutzten Bezeichnungen beibehalten, und gelangen so zu der folgenden Reihe von Sätzen.

VI. Der Grad jedes nicht in P enthaltenen Elementes φ von R ist $\equiv 4 \pmod 8$.

Dies folgt unmittelbar aus IV, weil es mindestens ein mit φ nicht permutables Element ψ in R gibt.

VII. Das Quadrat jedes Elementes ω von R ist in P enthalten.

Denn wenn ω in P enthalten ist, so gilt dasselbe auch von ω^2, weil P eine Gruppe ist. Wenn aber das Element ω nicht in P enthalten ist, so ist nach VI sein Grad $\equiv 4 \pmod 8$, also der seines Quadrates $\equiv 2 \pmod 4$, woraus nach VI folgt, daß ω^2 in P enthalten ist, w. z. b. w.

VIII. Jedes Element ω der Gruppe R ist permutabel mit wenigstens einem der drei Elemente α, β, γ der Gruppe Q, und zwar entweder nur mit einem einzigen oder mit allen dreien.

Ist nämlich ω nicht permutabel mit α, so muß das von α verschiedene Element $\omega^{-1}\alpha\omega = \alpha^{-1}$ sein, weil es bekanntlich denselben Grad 4 wie α hat und außerdem nach Satz I (in § 2) eine Potenz von α ist; ebenso muß, wenn dasselbe Element ω auch mit β nicht permutabel ist, $\omega^{-1}\beta\omega = \beta^{-1}$ sein; da nun $\gamma = \alpha\beta$ ist, so folgt hieraus

$$\omega^{-1}\gamma\omega = \omega^{-1}\alpha\beta\omega = \omega^{-1}\alpha\omega\cdot\omega^{-1}\beta\omega = \alpha^{-1}\beta^{-1} = \gamma,$$

also $\gamma\omega = \omega\gamma$, d. h. ω ist mit wenigstens einem der drei Elemente α, β, γ permutabel. Ist aber ω mit zweien von ihnen, z. B. mit α und mit β permutabel, so ist es auch mit deren Produkt γ, also mit allen dreien permutabel, w. z. b. w.

IX. Der Grad eines mit α, β, γ permutablen Elementes ω kann nicht durch vier teilbar sein, und der Inbegriff aller dieser Elemente ω ist die Gruppe P.

Den ersten Teil dieses Satzes beweisen wir auf indirektem Wege, indem wir annehmen, der Grad eines mit α, β (also auch mit γ) permutablen Elementes ω sei teilbar durch vier. Dann gibt es unter den Potenzen von ω, welche alle ebenfalls mit α, β permutabel sind, auch zwei Elemente vierten Grades ϱ (und ϱ^{-1}); nach der Fundamentaleigenschaft I der Hamiltonschen Gruppe R ist nun $\beta^{-1}(\varrho\alpha)\beta$ eine Potenz $(\varrho\alpha)^n$ von $\varrho\alpha$; weil aber ϱ permutabel mit β ist, so folgt $\beta^{-1}(\varrho\alpha)\beta = \varrho\beta^{-1}\alpha\beta = \varrho\alpha^{-1}$, und weil ϱ permutabel mit α ist, so folgt $(\varrho\alpha)^n = \varrho^n\alpha^n$; mithin ist $\varrho\alpha^{-1} = \varrho^n\alpha^n$, also $\varrho^{1-n} = \alpha^{1+n}$. Daß dies aber unmöglich ist, ergibt sich, wenn man die vier Fälle $n \equiv 0, 1, 2, 3 \pmod 4$ durchgeht; im ersten und dritten Falle wäre nämlich $\varrho = \alpha$, was dem Umstande widerspricht, daß β mit ϱ, aber nicht mit α permutabel ist; im zweiten oder vierten Fall wäre $1 = \alpha^2$ oder $\varrho^2 = 1$, während doch α und ϱ vom vierten Grade sind. Unsere obige Annahme führt daher zu einem Widerspruch, und folglich ist der erste Teil des Satzes bewiesen. Es muß daher jedes mit α, β, γ permutable Element ω in der Gruppe P enthalten sein, weil nach Satz VI der Grad eines jeden, in P nicht enthaltenen Elementes durch vier teilbar ist, und da

umgekehrt jedes Element der Gruppe P zufolge ihrer Definition mit α, β, γ permutabel ist, so ergibt sich auch der zweite Teil des Satzes, w. z. b. w.

X. Der Inbegriff aller derjenigen Elemente ω, welche nur mit α, nicht mit β, γ permutabel sind, ist der Komplex $P\alpha$.

Der Grad eines solchen Elementes ω, welches nicht mit β permutabel, also auch nicht in der Gruppe P enthalten ist, hat nach Satz IV die Form $8p + 4$, und zufolge (41) wird der Kommutator der beiden Elemente ω, β durch die Potenzen

$$\omega^{4p+2} = \beta^2 = \varepsilon = \alpha^2$$

dargestellt; wenn ferner ω mit α, also auch mit α^{-1} permutabel ist, so folgt hieraus

$$(\omega\alpha^{-1})^{4p+2} = \omega^{4p+2}\alpha^{-(4p+2)} = \alpha^2\alpha^{-2} = 1;$$

mithin ist der Grad des Elementes $\omega\alpha^{-1}$ nicht teilbar durch vier, und hieraus folgt nach Satz VI, daß dieses Element in P, also ω in dem Komplex $P\alpha$ enthalten ist. Umgekehrt, wenn $\omega = \pi\alpha$ irgendein Element in $P\alpha$, also π mit allen Elementen permutabel ist, so ist $\omega\alpha = \pi\alpha^2 = \alpha\omega$, ferner $\omega\beta = \pi\alpha\beta$, und

$$\beta\omega = \beta\pi\alpha = \pi\beta\alpha = \pi\alpha\beta\varepsilon = \omega\beta\varepsilon;$$

mithin ist jedes Element ω in $P\alpha$ permutabel mit α, aber nicht permutabel mit β, w. z. b. w.

XI. Jede Hamiltonsche Gruppe R ist von der Form

$$R = PQ = P + P\alpha + P\beta + P\gamma, \tag{42}$$

wo Q eine in R enthaltene Quaterniongruppe

$$Q = (1 + \varepsilon)(1 + \alpha + \beta + \gamma), \tag{43}$$

und P die Abelsche Gruppe der mit allen Elementen von R permutablen Elemente bedeutet; diese Gruppe P enthält kein einziges Element vierten Grades, wohl aber das in Q befindliche Element zweiten Grades ε, welches zugleich der Kommutator von je zwei nicht permutablen Elementen der Gruppe R ist.

Denn aus den drei vorhergehenden Sätzen folgt, daß jedes Element ω der Gruppe R in einem, und nur in einem der vier Komplexe P, $P\alpha$, $P\beta$, $P\gamma$ enthalten ist; die Behauptungen über P folgen aus IX und VII, weil $\varepsilon = \alpha^2$ ist. Da endlich die Elemente

von P mit allen Elementen von R, ferner die Elemente von $P\alpha$ nach X mit α und folglich auch mit allen Elementen desselben Komplexes $P\alpha$ permutabel sind, so gehören zwei nicht permutable Elemente auch zwei verschiedenen der drei Komplexe $P\alpha$, $P\beta$, $P\gamma$ an; wählt man nun z. B. aus $P\alpha$, $P\beta$ nach Belieben die beiden Elemente $\varphi' = \pi'\alpha$, $\varphi'' = \pi''\beta$, wo also π', π'' in P enthalten sind, so ergibt sich

$$\varphi'\varphi'' = \pi'\pi''\alpha\beta, \quad \varphi''\varphi' = \pi'\pi''\beta\alpha = \pi'\pi''\alpha\beta\varepsilon = \varphi'\varphi''\varepsilon,$$

mithin sind diese Elemente φ', φ'' nicht permutabel, und ihr Kommutator ist $= \varepsilon$, w. z. b. w.

XII. Wenn in einer Gruppe G eine Quaterniongruppe Q und eine Abelsche Gruppe P enthalten ist, deren Elemente mit denen von Q permutabel sind, wenn ferner P das in Q befindliche Element zweiten Grades ε, aber kein einziges Element vierten Grades enthält, so ist das Produkt PQ eine Hamiltonsche Gruppe R.

Aus der Permutabilität der Elemente von P mit denen von Q folgt zunächst, daß PQ eine Gruppe R ist; wählt man für Q wieder die bisherige Bezeichnung (43), so ist R von der Form (42), weil die Periode $[\varepsilon] = 1 + \varepsilon$ der größte gemeinsame Teiler von P, Q ist. Daß R keine Abelsche Gruppe ist, folgt daraus, daß ihre Elemente α, β nicht permutabel sind. Um zu zeigen, daß R eine Hamiltonsche Gruppe ist, haben wir nach Satz I in § 2 für je zwei Elemente φ, ψ nachzuweisen, daß $\varphi^{-1}\psi\varphi$ eine Potenz von ψ ist. Wenn nun wenigstens eins dieser beiden Elemente in P enthalten ist, oder wenn sie beide demselben Komplex $P\alpha$ oder $P\beta$ oder $P\gamma$ angehören, so sind sie permutabel, und folglich ist $\varphi^{-1}\psi\varphi = \psi$. Wenn aber z. B. $\psi = \pi\alpha$ in $P\alpha$, und $\varphi = \pi'\beta$ in $P\beta$ enthalten ist, so wird

$$\varphi^{-1}\psi\varphi = \beta^{-1}\pi\alpha\beta = \pi\beta^{-1}\alpha\beta = \pi\alpha^{-1};$$

da nun der Grad von π nicht durch vier teilbar ist, weil sonst unter den (in P enthaltenen) Potenzen von π auch zwei Elemente vierten Grades wären, so ist der Grad von π^2 eine ungerade Zahl $2m+1$, also $\pi^{-(4m+1)} = \pi$, mithin $\varphi^{-1}\psi\varphi = \pi\alpha^{-1} = \psi^{-(4m+1)}$, w. z. b. w.

Hiermit ist das am Schlusse der Einleitung ausgesprochene Resultat der Untersuchung in allen Teilen begründet.

Braunschweig, 9. August 1896.

Erläuterungen zur vorstehenden Abhandlung.

Weitere Untersuchungen über die Struktur der Hamiltonschen Gruppen verdankt man G. A. Miller (Comptes rendus, Paris **126** (1898), S. 1406—1408; Bull. Amer. Math. Soc. **4** (1898), S. 510—515; **5** (1899), S. 292—296) und d'Alessandro (Giorn. di Matematica **37**). In anderer Weise hat E. Wendt einige der Millerschen Resultate abgeleitet (Math. Ann. **59** (1904), S. 187—192; **60** (1905), S. 319—320). Verallgemeinerungen der Hamiltonschen Gruppen studierten Miller (Math. Ann. **60** (1905), S. 597—606; Arch. d. Math. u. Phys. (3) **11** (1907), S. 76—79; Transactions Amer. Math. Soc. **8** (1907), S. 25—29) und Wendt (Math. Ann. **62** (1906), S. 381—400).

Die wichtigsten Eigenschaften der Kommutatoren und Kommutatorgruppen hat Dedekind schon 1880 erkannt und brieflich an Frobenius mitgeteilt. (Man vergleiche die Abhandlung von Frobenius, Sitzungsber. d. Berl. Akad. 1896, S. 1343—1382, § 2.) Publiziert ist aber der Satz in der Fußnote S. 93 zuerst von G. A. Miller (Quarterly Journ. of Math. **28** (1896), S. 232—284).

Über die auf S. 91 erwähnte Beziehung zwischen Quaternionen und Quaternionengruppen hat Dedekind nichts weiteres plubliziert. Die Bemerkung bezieht sich, wie aus den im Nachlaß veröffentlichten Briefen an Frobenius klar hervorgeht, auf die im Februar 1886 entdeckte Gruppendeterminante und ihre Zerlegung, die Dedekind im Quaternionenfall vollständig durchgeführt hatte. Auch die Konstruktion der Quaternionkörper wird im Nachlaß gebracht (XXXIX).

Die Bestimmung aller Gleichungen mit Quaternionengruppe ist von Mertens. und zwar für beliebige Grundkörper durchgeführt worden (Sitzungsber. d. Wien. Akad. **111** (1902), Abt. IIa, S. 17—37; **125** (1916), Abt. IIa, S. 735—740; **130** (1921), Abt. IIa, S. 69—90). Man vgl. auch die Abhandlung von G. Bucht (Ark. för Math. Astr. och Phys. **6** (1911), Nr. 30).

Ore.

XXVIII.

Über Zerlegungen von Zahlen durch ihre größten gemeinsamen Teiler.

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

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

§ 1.

Drei Zahlen.

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

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

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

$$a_1 = da', \quad b_1 = db', \quad c_1 = dc' \tag{2}$$

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

$$a = db'c'a'', \quad b = dc'a'b'', \quad c = da'b'c'', \tag{3}$$

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

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

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

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

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

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

so findet man

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

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

$$\left\{ \begin{array}{lll} & d = d, & \\ a' = \dfrac{a_1}{d}, & b' = \dfrac{b_1}{d}, & c' = \dfrac{c_1}{d}, \\ a'' = \dfrac{ad}{b_1 c_1}, & b'' = \dfrac{bd}{c_1 a_1}, & c'' = \dfrac{cd}{a_1 b_1}. \end{array} \right. \tag{4}$$

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

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

ganze Zahlen ohne gemeinsamen Teiler werden*).

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

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

so erhält man nach bekannten Regeln

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

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

$$(7) \qquad m = da'b'c'a''b''c'' = \frac{abcd}{a_1 b_1 c_1}.$$

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

**) Vgl. D. § 178, S. 555.

§ 2.

Vier Zahlen.

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

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

und man bezeichne den größten gemeinsamen Teiler

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

usw.,

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

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

setzen, wo die vier ganzen Zahlen

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

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

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

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

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

in welchen sechs neue ganze Zahlen

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

auftreten. Setzt man nun

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

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

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

also

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

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

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

in welchen abermals vier neue ganze Zahlen:

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

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

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

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

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

Fügen wir zu diesen Gleichungen noch die selbstverständliche

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

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

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

§ 3.

Kombinationen.

Um diese Betrachtungen auf ein beliebiges System von n gegebenen Zahlen

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

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

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

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

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

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

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

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

dann wird

$$\beta + \gamma = 123\,567, \quad \gamma + \alpha = 123\,467, \quad \alpha + \beta = 123\,457,$$
$$\beta - \gamma = 17, \qquad \gamma - \alpha = 27, \qquad \alpha - \beta = 37.$$

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

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

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

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

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

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

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

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

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

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

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

was zufolge A zunächst die Form

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

genügen.

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

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

und

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

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

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

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

Der Vollständigkeit wegen erwähnen wir ferner, daß offenbar immer

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

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

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

§ 4.

Bemerkungen über Dualgruppen.

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

**) Vgl. § 5 dieses Aufsatzes.

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

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

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

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

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

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

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

*) Dies folgt leicht aus D. § 178.

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

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

Jede Dualgruppe vom Idealtypus besitzt auch den Modultypus.

Hiernach entspringen naturgemäß die beiden Fragen:

Gibt es Dualgruppen, welche den Modultypus nicht besitzen?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

II. Das Ding α ist in α' enthalten.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

*) Vgl. D. § 169, S. 499, Anmerkung.

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

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

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

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

und

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

also auch die beiden folgenden**):

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

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

§ 5.

Abelsche Gruppe $\mathfrak{G}$.

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

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

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

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

$$ab = ba, \quad (ab)c = a(bc) \tag{1}$$

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

$$ao = a \tag{2}$$

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

$$aa^{-1} = o \tag{3}$$

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

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

$$a : b = \frac{a}{b} = ab^{-1}, \tag{4}$$

woraus

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

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

Es wird im folgenden oft von Produkten $\Pi\mathfrak{a}$ die Rede sein, wo das Produktzeichen Π sich auf alle m Elemente $\mathfrak{a} = \mathfrak{a}_1, \mathfrak{a}_2 \cdots \mathfrak{a}_m$ bezieht, welche unter einer gemeinsamen Form enthalten sind oder gewissen Bedingungen genügen; ein solches Produkt ist also erklärt durch

$$\Pi\mathfrak{a} = \mathfrak{a}_1 \mathfrak{a}_2 \cdots \mathfrak{a}_m. \tag{6}$$

Es kommt aber auch vor, daß die Anzahl m der fraglichen Elemente $\mathfrak{a}$ auf 1 oder 0 herabsinkt, und wir wollen festsetzen, daß unter $\Pi\mathfrak{a}$ im ersten Falle immer das einzige Element $\mathfrak{a}_1$ selbst, im letzteren Falle immer das Hauptelement $\mathfrak{o}$ der Gruppe zu verstehen ist.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

woraus durch Vergleichung mit (9) und mit

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

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

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

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

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

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

genügen.

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

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

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

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

woraus mit Rücksicht auf den vorhergehenden Satz (12) sich

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

ergibt, w. z. b. w.

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

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

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

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

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

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

also nach unserer Induktionsannahme

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

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

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

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

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

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

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

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

§ 6.

Ganze Elemente in $\mathfrak{G}$.

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

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

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

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

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

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

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

$$(5) \qquad (a+b+c)(bc+ca+ab) = (b+c)(c+a)(a+b),$$

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

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

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

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

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

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

also

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

mithin $a = o$, w. z. b. w.

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

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

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

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

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

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

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

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

$$\mathfrak{o} + \mathfrak{a} + \cdots + \mathfrak{a}^e = \mathfrak{a} + \cdots + \mathfrak{a}^e,$$

also

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

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

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

also zufolge (1) auch

$$\mathfrak{o} + \mathfrak{a}^m = \mathfrak{a}^m,$$

und hieraus ergibt sich das allgemeine Gesetz

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

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

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

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

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

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

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

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

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

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

$$a = da', \quad b = db', \quad ax + by = d \tag{10}$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$a - b = \frac{ab}{a + b} \tag{11}$$

oder, was dasselbe sagt, durch

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

und zugleich gilt der Satz

$$(a + b)(a - b) = ab. \tag{13}$$

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

$$a - a = a, \tag{1'}$$

$$a - b = b - a, \tag{2'}$$

$$(a - b) - c = a - (b - c), \tag{3'}$$

$$(a - b)c = ac - bc \tag{4'}$$

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

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

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

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

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

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

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

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

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

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

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

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

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

*) Vgl. D. § 178, S. 555.

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

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

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

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

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

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

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

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

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

§ 7.

Lösung der Aufgabe.

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

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

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

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

$$\begin{aligned} &\mathfrak{a}_1 + \mathfrak{a}_2, \quad \mathfrak{a}_1 + \mathfrak{a}_3 \cdots, \\ &\mathfrak{a}_1 + \mathfrak{a}_2 + \mathfrak{a}_3, \quad \mathfrak{a}_1 + \mathfrak{a}_2 + \mathfrak{a}_4 \cdots, \\ &\mathfrak{a}_1 + \mathfrak{a}_2 + \mathfrak{a}_3 + \mathfrak{a}_4 \cdots, \\ &\cdots\cdots\cdots\cdots\cdots \end{aligned}$$

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

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

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

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

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

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

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

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

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

$$(\alpha, \omega) + (\beta, \omega) = (\alpha + \beta, \omega). \tag{4}$$

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

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

so folgt aus unserer Induktionshypothese

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

und aus dem speziellen Produktsatz II in § 5 ergibt sich

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

Hieraus folgt weiter

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

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

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

so erhält man

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

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

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

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

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

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

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

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

wo zur Abkürzung

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Bezeichnet man nun das im Satze genannte kleinste gemeinsame Vielfache

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

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

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

also

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

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

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

w. z. b. w.

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

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

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

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

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

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

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

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

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

§ 8.

Endliche Dualgruppen in $\mathfrak{G}$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Die wichtigste Grundlage für unsere Untersuchung bildet aber der folgende

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

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

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

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

so wird

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

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

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

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

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

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

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

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

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

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

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

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

Erläuterungen zur vorstehenden Abhandlung.

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

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

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

Noether.

*) Vgl. D. § 170, S. 503, Anmerkung.

XXIX.

Über die Anzahl der Idealklassen in reinen kubischen Zahlkörpern.

[Journal für reine und angewandte Mathematik, Bd. 121, S. 40—123 (1900).]

Die vorliegende Abhandlung ist im Laufe des Winters 1897/98 durch Umarbeitung eines aus dem Jahre 1871 oder 1872 stammenden Entwurfes entstanden; ihr Hauptergebnis habe ich (Februar 1873) in meiner Anzeige*) der Vorlesungen über die Kreisteilung von P. Bachmann bei Besprechung des kubischen Reziprozitätsgesetzes mit den folgenden Worten kurz angedeutet: „Bedeutet k eine ganze rationale Zahl, deren Kubikwurzel irrational ist, so entspringt aus der Gleichung $x^3 = k$ ein reiner kubischer Körper, dessen Grundzahl die Form $D = -3g^2$ hat, wo g eine aus k leicht abzuleitende ganze Zahl ist. Fragt man nun nach allen in k nicht aufgehenden Primzahlen p von der Form $3n + 1$, von welchen die gegebene Zahl k kubischer Rest ist, so gelangt man mit Hilfe des Reziprozitätssatzes zu folgendem interessanten Resultat, welches im wesentlichen schon Gauß bekannt gewesen ist (und sich auf beliebige kubische Körper ausdehnen läßt): Die sämtlichen nicht äquivalenten, ursprünglichen positiven quadratischen Formen $ax^2 + bxy + cy^2$, in welchen $b^2 - 4ac = D$, zerfallen in drei Abteilungen von gleich vielen Individuen, deren erste eine Gruppe bildet, durch deren Formen alle und nur solche Primzahlen p dargestellt werden, von welchen k kubischer Rest ist. Mit Hilfe desselben wird die Bestimmung der Anzahl der Idealklassen des kubischen Körpers auf einen bekannten Teil der Theorie der Thetafunktionen zurückgeführt.“ Zur Vergleichung bemerke ich, daß die hier gebrauchten Zeichen k, x, g in der folgenden Abhandlung bzw. durch ∂, Θ, k ersetzt sind; der Satz über die für den kubischen Körper

*) Schlömilchs Zeitschrift für Mathematik und Physik, Jahrgang 18; 1873. Literaturzeitung S. 22, 43.

charakteristische Drittelung der Gruppe der quadratischen Formen von der Diskriminante D findet sich in § 11. Die eingeklammerten Worte, welche sich auf die Ausdehnung dieses Satzes auf alle kubischen Körper beziehen, habe ich damals, weil ich im Besitze des Beweises zu sein glaubte, dem Manuskripte der Anzeige gleich nachgeschickt, ihre Einfügung an der bezeichneten Stelle ist aber über dem großen Leipziger Setzerstrike versäumt, und sie sind erst im folgenden Hefte der Literaturzeitung (S. 43) abgedruckt. Durch Überhäufung mit Amtsgeschäften wurde ich in jener Zeit für mehrere Jahre an jeder wissenschaftlichen Tätigkeit gehindert, und erst später habe ich erkannt, daß die mir zu Gebote stehenden Mittel zum Beweise der Allgemeingültigkeit des Satzes nicht ausreichten. Seitdem bin ich nur vorübergehend und ohne den gewünschten Erfolg zu dieser Untersuchung zurückgekehrt; doch zweifle ich auch heute nicht an der Wahrheit des Satzes, den ich in allen Beispielen bestätigt gefunden habe, und ich glaube auch, daß für Körper von negativer Grundzahl die jetzt mehr ausgebildete Theorie der komplexen Multiplikation der elliptischen Funktionen zum Beweise wohl ausreichen wird; vielleicht wird, wenn dies gelingt, hierdurch auch ein Weg zur Lösung des großen Rätsels gebahnt, welche algebraische Zahlkörper den Klassen der binären quadratischen Formen (oder Moduln) von positiver Diskriminante entsprechen. Meine bisherigen auf diese Fragen bezüglichen Versuche gedenke ich in einer Abhandlung über die Invarianten beliebiger kubischer Körper mitzuteilen. Die gegenwärtige Abhandlung, welche sich ausschließlich mit den reinen kubischen Körpern beschäftigt, verfolgt lediglich das in der oben erwähnten Anzeige vom Jahre 1873 angedeutete Ziel und endigt mit der Einmündung der Untersuchung in die Theorie der komplexen Multiplikation. Ich erwähne schließlich, daß die Theorie der reinen kubischen Körper meines Wissens bisher nur von A. Markoff behandelt ist; seine Abhandlung*) „Sur les nombres entiers dépendants d'une racine cubique d'un nombre entier ordinaire“ beschränkt sich im wesentlichen auf die (von mir in §§ 1—5 behandelte) Bestimmung der in dem Körper vorhandenen Ideale, wobei die Auffassung von Zolotareff zugrunde gelegt ist; außerdem gibt sie am Schlusse eine sehr wertvolle Tabelle von Einheiten (vgl. unten § 13).

*) Mémoires de l'Académie impériale des sciences de St.-Pétersbourg, VII^{e} série, tome 38.

§ 1.

Reine kubische Zahlkörper.

Ist die rationale Zahl ∂ nicht die dritte Potenz einer rationalen Zahl, so sind die drei Kubikwurzeln $\Theta = \sqrt[3]{\partial}$ irrational, und es kann auch keine von ihnen die Wurzel einer quadratischen Gleichung $\Theta^2 + m\Theta + n = 0$ mit rationalen Koeffizienten m, n sein; multipliziert man nämlich mit Θ, so würde hieraus $(n - m^2)\Theta + (\partial - mn) = 0$, also, weil Θ irrational ist, $n = m^2$ und $\partial = mn = m^3$ folgen, was im Widerspruch mit unserer Annahme über ∂ steht. Mithin ist jede der drei Wurzeln Θ eine algebraische Zahl dritten Grades (vgl. § 167, S. 492 der vierten Auflage von Dirichlets Zahlentheorie, die ich mit D. zitieren werde). Im folgenden bezeichnen wir mit Θ die reelle Kubikwurzel aus ∂, mit Θ', Θ'' die beiden imaginären Wurzeln

$$\Theta' = \Theta\varrho, \quad \Theta'' = \Theta\varrho^2,$$

wo ϱ eine imaginäre dritte Einheitswurzel, also

$$\varrho^2 + \varrho + 1 = 0$$

ist.

Aus dem Körper R der rationalen Zahlen entsteht durch Adjunktion der Zahl Θ der reine kubische Zahlkörper $K = R(\Theta)$ vom Grade $(K, R) = 3$; er besteht aus allen Zahlen von der Form

$$\varkappa = x_1\Theta^2 + x_2\Theta + x_3,$$

wo x_1, x_2, x_3 beliebige Zahlen in R bedeuten, und jede Zahl $\varkappa$ kann auch nur auf eine einzige Art in dieser Form dargestellt werden, weil die drei Potenzen Θ^2, Θ, 1 eine irreduzible Basis von K bilden (D. § 164, S. 472). Die beiden Körper R und K sind die einzigen Divisoren von K; denn wenn der Körper L in K enthalten ist, so folgt (nach D. § 164, S. 473), daß $(K, L)(L, R) = (K, R) = 3$, also entweder $(K, L) = 3$, $(L, R) = 1$, $L = R$ oder $(K, L) = 1$, $(L, R) = 3$, $L = K$ ist. Betrachtet man nun irgend eine in K enthaltene Zahl $\varkappa$ von der obigen Form, so ist der von ihr erzeugte Körper $R(\varkappa)$ jedenfalls Divisor von K, und zwar tritt der Fall $R(\varkappa) = R$ immer und nur dann ein, wenn $\varkappa$ rational, also $x_1 = x_2 = 0$ ist; jede irrationale Zahl $\varkappa$ des Körpers K erzeugt daher stets denselben Körper $R(\varkappa) = K$ und ist folglich eine algebraische Zahl dritten Grades.

Diese Schlüsse sind offenbar unabhängig von der Voraussetzung, daß Θ reell ist, und gelten daher ebenso für die beiden reinen kubischen Körper $K' = R(\Theta')$ und $K'' = R(\Theta'')$. Bedeutet z. B. $\varkappa'$ eine irrationale Zahl des Körpers K', so ist $R(\varkappa') = K'$, und folglich kann $\varkappa'$ nicht reell sein, weil sonst K' aus lauter reellen Zahlen bestehen würde, während doch die imaginäre Zahl $\Theta' = \Theta\varrho$ in K' enthalten ist; mithin enthalten die Körper K', K'' außer den rationalen nur imaginäre Zahlen, während K nur aus reellen Zahlen besteht. Die beiden Körper K', K'' sind aber nicht allein von K, sondern auch voneinander verschieden; denn wäre $K' = K''$, so müßte die Zahl $\Theta'' = \Theta'\varrho$, also auch die Zahl $\varrho = \Theta'' : \Theta'$ in K' enthalten sein, was nach dem Obigen nicht angeht, weil ϱ eine algebraische Zahl zweiten Grades ist.

Der Körper K besitzt drei Permutationen (D. § 165), durch welche er in die drei konjugierten Körper K, K', K'' übergeht; jede in K enthaltene Zahl $\varkappa$ von der obigen Form

$$\varkappa = x_1\Theta^2 + x_2\Theta + x_3$$

geht durch die erste, die identische Permutation in sich selbst, durch die zweite und dritte in die konjugierten Zahlen $\varkappa' = x_1\Theta'^2 + x_2\Theta' + x_3$ und $\varkappa'' = x_1\Theta''^2 + x_2\Theta'' + x_3$ über; ist $\varkappa' = u + vi$, wo u, v reelle Zahlen bedeuten, während $i = \sqrt{-1}$ ist, so ist $\varkappa'' = u - vi$.

§ 2.

Invarianten des Körpers K.

Jede von Null verschiedene rationale Zahl ∂ kann offenbar immer und nur auf eine einzige Weise in der Form

$$\partial = a\,b^2\,c^3$$

dargestellt werden, wo c rational ist, und a, b natürliche Zahlen bedeuten, deren Produkt ab durch kein Primzahlquadrat teilbar ist; da in unserem Falle ∂ nicht die dritte Potenz einer rationalen Zahl ist, so ist außerdem

$$ab > 1.$$

Setzt man nun $\Theta = c\alpha$, so wird die positive Zahl $\alpha = \sqrt[3]{ab^2}$, und da α irrational und in K enthalten ist, so ist auch $K = R(\alpha)$; da ferner $\alpha^2 = \sqrt[3]{a^2b^4} = b\sqrt[3]{a^2b}$ ist, so wird, wenn man $\sqrt[3]{a^2b} = \beta$ setzt,

$$\alpha^2 = b\beta, \quad \beta^2 = a\alpha, \quad \alpha\beta = ab;$$
$$\alpha^3 = ab^2, \quad \beta^3 = a^2b,$$

und die allgemeine Form aller in K enthaltenen Zahlen $\varkappa$ ist:

$$\varkappa = z + x\alpha + y\beta,$$

wo z, x, y beliebige Zahlen in R bedeuten.

Die mit α und die mit β konjugierten Zahlen α', α'' und β', β'' ergeben sich aus

$$c\alpha = \Theta, \quad c\alpha' = \Theta' = \Theta\varrho = c\alpha\varrho, \quad c\alpha'' = \Theta'' = \Theta\varrho^2 = c\alpha\varrho^2$$

und aus

$$ab = \alpha\beta = \alpha'\beta' = \alpha''\beta'',$$

nämlich

$$\alpha' = \alpha\varrho, \quad \alpha'' = \alpha\varrho^2, \quad \beta' = \beta\varrho^2, \quad \beta'' = \beta\varrho,$$

und hieraus folgt allgemein

$$\varkappa' = z + x\alpha\varrho + y\beta\varrho^2, \quad \varkappa'' = z + x\alpha\varrho^2 + y\beta\varrho$$

oder

$$\varkappa' = (x\alpha - z)\varrho + (y\beta - z)\varrho^2; \quad \varkappa'' = (x\alpha - z)\varrho^2 + (y\beta - z)\varrho.$$

Für das Supplement und die Norm der Zahl $\varkappa$ erhält man daher (nach D. § 176, S. 542 und § 167, S. 486) die Darstellungen

$$\begin{aligned}\varkappa'\varkappa'' &= (x\alpha - z)^2 - (x\alpha - z)(y\beta - z) + (y\beta - z)^2 \\ &= (z^2 - ab\,x\,y) + (ay^2 - zx)\alpha + (bx^2 - zy)\beta\end{aligned}$$

und

$$N(\varkappa) = \varkappa\varkappa'\varkappa'' = z^3 - 3abzxy + ab^2x^3 + a^2by^3.$$

Wir stellen uns jetzt die Aufgabe, alle diejenigen Zahlen $\varkappa$ in K zu finden, deren dritte Potenz rational ist. Nehmen wir an, es sei $\varkappa^3 = e$, wo e eine rationale Zahl bedeutet, so folgt auch $\varkappa'^3 = e$, also muß

$$\varkappa' = \varkappa \quad \text{oder} \quad \varkappa' = \varkappa\varrho \quad \text{oder} \quad \varkappa' = \varkappa\varrho^2$$

sein; da aber allgemein

$$\begin{aligned}\varkappa' - \varkappa &= (1 - \varrho^2)(x\alpha\varrho - y\beta), \\ \varkappa' - \varkappa\varrho &= (1 - \varrho)(z - y\beta\varrho), \\ \varkappa' - \varkappa\varrho^2 &= (\varrho^2 - \varrho)(z\varrho - x\alpha),\end{aligned}$$

und außerdem die Zahl ϱ nicht in K enthalten ist, so muß im ersten, zweiten, dritten Falle entsprechend

$$\begin{aligned}x = y = 0, &\quad \varkappa = z, &\quad e = z^3, \\ z = y = 0, &\quad \varkappa = x\alpha, &\quad e = ab^2x^3, \\ z = x = 0, &\quad \varkappa = y\beta, &\quad e = a^2by^3\end{aligned}$$

sein. Im ersten Falle ist $\varkappa$ rational, also $R(\varkappa) = R$, und dasselbe gilt auch für den zweiten und dritten Fall, wenn x bzw. $y = 0$ ist;

in allen diesen Fällen ist e die dritte Potenz einer rationalen Zahl. Soll also die Zahl $\varkappa$ (ebenso wie Θ) die Kubikwurzel aus einer rationalen Zahl e sein, welche (wie ∂) nicht die dritte Potenz einer rationalen Zahl ist, so geschieht dies nur im zweiten oder dritten Falle, wenn x bzw. y von Null verschieden gewählt wird, und gleichzeitig wird $R(\varkappa) = K$; vergleicht man ferner die Formen $e = a\,b^2\,x^3$, $e = b\,a^2\,y^3$ der Zahl e mit der Form $\partial = a\,b^2\,c^3$, so ergibt sich, daß alle diese irrationalen Zahlen $\varkappa$ des Körpers K, deren dritte Potenz e rational ist, auf dasselbe Paar a, b oder b, a führen. Wir nennen daher diese beiden natürlichen Zahlen a, b, durch welche der reine kubische Körper K vollständig bestimmt ist, die Invarianten des Körpers K.

Nr.	ab	a	b	ab^2	a^2b	k	k''	h
1	2	2	1	2	4	6	1	1
2	3	3	1	3	9	9	1	1
3	5	5	1	5	25	15	2	1
4	6	6	1	6	36	18	3	1
5	6	3	2	12	18	18	3	1
6	7	7	1	7	49	21	2	3
(7)	10	10	1	10	100	10	2	1
8	10	5	2	20	50	30	6	3
9	11	11	1	11	121	33	4	2
10	13	13	1	13	169	39	4	3
11	14	14	1	14	196	42	6	3
(12)	14	7	2	28	98	14	2	3
13	15	15	1	15	225	45	6	2
14	15	5	3	45	75	45	6	1
(15)	17	17	1	17	289	17	2	1
(16)	19	19	1	19	361	19	2	3
17	21	21	1	21	441	63	6	3
18	21	7	3	63	147	63	6	6
19	22	22	1	22	484	66	12	3
(20)	22	11	2	44	242	22	4	1
21	23	23	1	23	529	69	8	1

Da der Körper K durch Vertauschung von a mit b nicht geändert wird, so kann man, um alle reinen kubischen Körper K und jeden nur einmal zu erhalten, so verfahren: man betrachte alle natürlichen Zahlen, welche > 1 und durch kein Primzahlquadrat teilbar sind, und zerlege jede auf alle Arten in zwei Faktoren a, b, von denen a der größere ist; bezeichnet man dann mit α und β die positiven Kubikwurzeln aus ab^2 und a^2b, so ist $R(\alpha) = R(\beta)$ ein reeller reiner kubischer Körper K, zu welchem jedesmal zwei konjugierte imaginäre reine kubische Körper K', K'' gehören. Hier folgt

der Anfang einer solchen Tabelle (siehe S. 153) aller reinen kubischen Körper K; die in ihr auftretenden Spalten k und k'' werden später (§§ 3, 4, 9) erklärt werden, und h bedeutet die Anzahl der Idealklassen des Körpers.

§ 3.

Die in $3ab$ aufgehenden Primideale.

Es sei $\mathfrak{o}$ die Hauptordnung des Körpers K, d. h. der Inbegriff aller in ihm enthaltenen ganzen algebraischen Zahlen, und

$$\Delta(\mathfrak{o}) = D$$

die Diskriminante oder Grundzahl von K (D. § 175, S. 538). Um $\mathfrak{o}$ und D zu bestimmen, betrachten wir zunächst den Modul

$$\mathfrak{n} = [1, \alpha, \beta],$$

d. h. den Inbegriff aller derjenigen Zahlen $\varkappa = z + x\alpha + y\beta$, welche durch beliebige ganze rationale Zahlen z, x, y erzeugt werden; da die Basiszahlen 1, α, β ganze (algebraische) Zahlen sind, so gilt dasselbe von allen diesen Zahlen $\varkappa$, d. h. der Modul $\mathfrak{n}$ ist teilbar durch den Modul $\mathfrak{o}$, was in Zeichen durch $\mathfrak{n} > \mathfrak{o}$ oder $(\mathfrak{n}, \mathfrak{o}) = 1$ ausgedrückt wird (D. § 171, S. 510); zugleich ist

$$\Delta(\mathfrak{n}) = D(\mathfrak{o}, \mathfrak{n})^2,$$

wo $(\mathfrak{o}, \mathfrak{n})$ die Anzahl der nach dem Modul $\mathfrak{n}$ inkongruenten Zahlen in $\mathfrak{o}$ bedeutet (D. § 175, S. 539). Zufolge der Definition der Diskriminante eines Moduls (D. § 175, S. 536) ist nun $\Delta(\mathfrak{n})$ das Quadrat der Determinante

$$\begin{vmatrix} 1, & \alpha, & \beta \\ 1, & \alpha', & \beta' \\ 1, & \alpha'', & \beta'' \end{vmatrix} = \begin{vmatrix} 1, & \alpha, & \beta \\ 1, & \alpha\varrho, & \beta\varrho^2 \\ 1, & \alpha\varrho^2, & \beta\varrho \end{vmatrix} = 3\alpha\beta(\varrho^2 - \varrho),$$

und da $\alpha\beta = ab$, und $(\varrho^2 - \varrho)^2 = -3$ ist, so ergibt sich

$$\Delta(\mathfrak{n}) = -3(3ab)^2;$$

aus der Vergleichung mit der obigen Form von $\Delta(\mathfrak{n})$ folgt, daß die Anzahl $(\mathfrak{o}, \mathfrak{n})$ ein Divisor von $3ab$, also

$$3ab = k(\mathfrak{o}, \mathfrak{n}), \quad D = -3k^2$$

ist, wo k eine natürliche Zahl bedeutet. Die Bestimmung dieser für alles Folgende sehr wichtigen Zahl k wird erleichtert, wenn wir vorher alle in $3ab$ aufgehenden Primideale des Körpers K aufsuchen, unter welchen sich jedenfalls auch alle in der Grundzahl D aufgehenden

Primideale befinden; mit dieser ohnehin unerläßlichen Aufgabe wollen wir uns daher jetzt beschäftigen.

Betrachten wir zunächst ein in a aufgehendes Primideal $\mathfrak{p}$, so muß die durch $\mathfrak{p}$ teilbare natürliche Primzahl p, welche zugleich die kleinste in $\mathfrak{p}$ enthaltene natürliche Zahl ist (D. § 179, S. 563), ebenfalls in a aufgehen, und da ab nicht durch p^2 teilbar ist, so wird

$$\alpha^3 = ab^2 = pq,$$

wo q nicht durch p, also auch nicht durch $\mathfrak{p}$ teilbar ist; da nun $\mathfrak{p}$ in p, pq, α^3, also auch in α aufgeht, so muß $\mathfrak{p}^3$ in pq, also auch in p aufgehen; nach einem allgemeinen, aus der Betrachtung der Normen folgenden Satze kann aber die Anzahl der (gleichen oder verschiedenen) Primideale, deren Produkt $= \mathfrak{o}p$ ist, nicht größer als der Grad des Körpers, in unserem Falle also nicht größer als 3 sein; mithin ist

$$\mathfrak{o}p = \mathfrak{p}^3, \quad N(\mathfrak{p}) = (\mathfrak{o}, \mathfrak{p}) = p,$$

d. h. $\mathfrak{o}p$ ist die dritte Potenz eines Primideals $\mathfrak{p}$ vom ersten Grade (D. § 180, S. 565). Ganz dasselbe gilt offenbar für alle in b aufgehenden natürlichen Primzahlen p und Primideale $\mathfrak{p}$.

Ein anderer Weg, um zu dem vorstehenden Resultate zu gelangen, stützt sich auf die Multiplikation und Reduktion der endlichen Moduln (D. § 170, S. 502 und § 172, S. 519); wir wollen ihn kurz andeuten, seine nähere Ausführung aber, weil sie keine Schwierigkeit darbietet, dem Leser überlassen. Jeder natürliche Divisor m von ab hat die Form $m = a_1 b_1$, wo a_1 Divisor von a, b_1 Divisor von b ist; betrachtet man nun den Modul

$$\mathfrak{m} = [m, \alpha, \beta],$$

so findet man leicht

$$\mathfrak{m}^2 = [m, a_1\alpha, b_1\beta], \quad \mathfrak{m}^3 = m\mathfrak{n};$$

da nun $\mathfrak{o}\mathfrak{n} = \mathfrak{o}$ ist, weil $\mathfrak{n}$ die Zahl 1 enthält, so ergibt sich

$$\mathfrak{o}m = (\mathfrak{o}\mathfrak{m})^3,$$

wo $\mathfrak{o}\mathfrak{m}$ offenbar ein Ideal ist. Als spezieller Fall entspringt hieraus für das oben mit $\mathfrak{p}$ bezeichnete Primideal die Darstellung

$$\mathfrak{p} = \mathfrak{o}[p, \alpha, \beta].$$

Unsere Aufgabe, alle in $3ab$ aufgehenden Primideale zu finden, ist durch das Vorstehende offenbar erledigt, wenn ab durch 3 teilbar ist; im entgegengesetzten Falle, wo

$$a^2 \equiv b^2 \equiv 1 \pmod{3},$$

kommt es aber noch darauf an, die Zerlegung von $\mathfrak{o}\,3$ in Primideale zu finden, und hierbei werden wir auf eine wichtige Einteilung aller reinen kubischen Körper K in zwei verschiedene Arten geführt werden. Hierzu betrachten wir die irrationale ganze Zahl

$$\mu = \alpha - a,$$

welche zufolge $\alpha^3 = a\,b^2$ der irreduziblen Gleichung

$$\mu^3 + 3\,a\,\mu^2 + 3\,a^2\,\mu + a\,(a^2 - b^2) = 0$$

genügt. Da der Koeffizient $3\,a^2$ von μ im dritten Gliede nicht durch 9 teilbar ist, so kann μ nicht durch 3 teilbar sein (D. § 173, S. 531), aber das erste Glied μ^3 ist durch 3 teilbar, weil dies von allen folgenden Gliedern gilt. Aus der Existenz einer durch 3 nicht teilbaren Zahl μ, deren dritte Potenz durch 3 teilbar ist, folgt bekanntlich, daß $\mathfrak{o}\,3$ nicht ein Produkt von lauter verschiedenen Primidealen, sondern durch das Quadrat eines Primideals $\mathfrak{p}$ teilbar ist; setzt man demgemäß

$$\mathfrak{o}\,3 = \mathfrak{p}^2\,\mathfrak{p}_1,$$

so folgt aus der Betrachtung der Normen leicht, daß $\mathfrak{p}$ und $\mathfrak{p}_1$ Primideale ersten Grades sind; denn wenn man $N(\mathfrak{p}) = 3^m$, $N(\mathfrak{p}_1) = 3^n$ setzt, wo $m \geqq 1$, $n \geqq 0$, so folgt $N(\mathfrak{o}\,3) = 3^3 = 3^{2m+n}$, also $3 = 2\,m + n$, mithin $m = n = 1$; es ist daher

$$N(\mathfrak{p}) = N(\mathfrak{p}_1) = 3,$$

und folglich ist auch $\mathfrak{p}_1$ ein Primideal. Aber nun entsteht die Frage, ob $\mathfrak{p}_1$ identisch mit $\mathfrak{p}$ ist oder nicht; hierauf antwortet der folgende

Satz: Die in der Zerlegung $\mathfrak{o}\,3 = \mathfrak{p}^2\,\mathfrak{p}_1$ auftretenden Primideale ersten Grades $\mathfrak{p}$, $\mathfrak{p}_1$ sind gleich oder verschieden, je nachdem $a^2 - b^2$ unteilbar oder teilbar durch 9 ist.

Zum Beweise benutzen wir die obige kubische Gleichung, welche zufolge $\mu + a = \alpha$ die Form

$$\mu^3 + 3\,a\,\alpha\,\mu + a\,(a^2 - b^2) = 0$$

annimmt, und bezeichnen mit r den Exponenten der höchsten in $(a^2 - b^2)$ aufgehenden Potenz von 3, welcher jedenfalls $\geqq 1$ ist, während a und α relative Primzahlen zu 3 sind. Ist nun erstens $\mathfrak{p} = \mathfrak{p}_1$, also $\mathfrak{o}\,3 = \mathfrak{p}^3$, und $\mathfrak{p}^s$ die höchste in μ aufgehende Potenz von $\mathfrak{p}$, so ist $1 \leqq s \leqq 2$, weil μ durch $\mathfrak{p}$, aber nicht durch 3 teilbar ist, und die Exponenten der höchsten in μ^3, $3\,a\,\alpha\,\mu$, $a\,(a^2 - b^2)$ aufgehenden Potenzen von $\mathfrak{p}$ sind der Reihe nach $3\,s$, $3 + s$, $3\,r$. Die beiden

ersteren sind voneinander verschieden, weil $3+s$ nicht durch 3 teilbar ist, und da der kleinere von ihnen zufolge der obigen Gleichung mit dem dritten $3r$ übereinstimmen muß, so ergibt sich $3r = 3s < 3+s \leqq 5$, also $r = s = 1$, mithin ist $(a^2 - b^2)$ nicht durch 9, und μ nicht durch $\mathfrak{p}^2$ teilbar. Ist aber zweitens $\mathfrak{p}$ verschieden von $\mathfrak{p}_1$, also $\mathfrak{o}\,3 = \mathfrak{p}^2\mathfrak{p}_1$ nicht teilbar durch $\mathfrak{p}_1^2$, so ist $\mathfrak{p}_1^r$ die höchste in $(a^2 - b^2)$ aufgehende Potenz von $\mathfrak{p}_1$; da nun μ^3 durch 3, also μ gewiß durch $\mathfrak{p}_1$ teilbar ist, so sind die Zahlen μ^3, $3\,\alpha\,\alpha\,\mu$ mindestens durch $\mathfrak{p}_1^2$ teilbar; zufolge der obigen Gleichung muß daher auch $(a^2 - b^2)$ durch $\mathfrak{p}_1^2$ teilbar sein, mithin ist $r \geqq 2$, also $(a^2 - b^2)$ teilbar durch 9. — Die beiden einander ausschließenden Annahmen über $\mathfrak{p}$ und $\mathfrak{p}_1$, welche alle Fälle erschöpfen, führen also zu zwei Folgerungen über die Zahl $(a^2 - b^2)$, welche ebenfalls einander ausschließen und alle Fälle erschöpfen; mithin muß umgekehrt $\mathfrak{p} = \mathfrak{p}_1$ oder $\mathfrak{p}$ von $\mathfrak{p}_1$ verschieden sein, je nachdem $(a^2 - b^2)$ unteilbar oder teilbar durch 9 ist, w. z. b. w.

An den vorstehenden Satz knüpfen wir noch die folgenden Bemerkungen. Obgleich derselbe nur für den Fall ausgesprochen und bewiesen ist, wo $a\,b$ nicht durch 3 teilbar ist, so umfaßt er doch offenbar auch den schon vorher erledigten Fall, wo $a\,b$ durch 3 teilbar ist, weil dann ebenfalls $\mathfrak{o}\,3 = \mathfrak{p}^3$, und $a^2 - b^2$ nicht einmal durch 3, geschweige durch 9 teilbar ist. Wir teilen daher alle reinen kubischen Körper K nach dem Verhalten der Zahl 3 in zwei Arten ein und nennen K einen Körper erster oder zweiter Art, je nachdem $a^2 - b^2$ unteilbar oder teilbar durch 9 ist, oder — was nach dem Vorstehenden hiermit gleichbedeutend ist — je nachdem die in der Zerlegung $\mathfrak{o}\,3 = \mathfrak{p}^2\mathfrak{p}_1$ auftretenden Primideale $\mathfrak{p}$, $\mathfrak{p}_1$ gleich oder verschieden sind.

Hierauf wollen wir den Fall eines Körpers K von zweiter Art noch etwas näher betrachten; dann kann man

$$a^2 \equiv b^2 \equiv 1 - 3\,c \pmod 9$$

setzen, wo c eine nach dem Modul 3 bestimmte ganze rationale Zahl bedeutet. Da das Produkt $a^2 - b^2$ der beiden Faktoren $a \pm b$ durch 9 teilbar, ihre Summe $2\,a$ aber unteilbar durch 3 ist, so können sie nicht beide durch 3 teilbar sein, und folglich muß einer von ihnen durch 9 teilbar sein; mithin ist

$$a \equiv \pm b \pmod 9,$$

und umgekehrt folgt hieraus, daß K ein Körper zweiter Art ist. Unter den 21 Körpern der Tabelle am Schlusse von § 2 sind daher die 5 durch Einklammerung ihrer Nummern (7), (12), (15), (16), (20) kenntlich gemachten Körper von zweiter, die übrigen 16 von erster Art. Wir wollen nun darauf ausgehen, die beiden in 3 aufgehenden Primideale $\mathfrak{p}$, $\mathfrak{p}_1$ deutlich zu unterscheiden. Da die dritte Potenz der Zahl $\mu = \alpha - a$ durch 3 teilbar ist, so muß μ durch $\mathfrak{p}\mathfrak{p}_1$, also μ^2 durch $\mathfrak{p}^2\mathfrak{p}_1^2 = 3\mathfrak{p}_1$, mithin auch durch 3 teilbar sein; nun ist aber

$$\begin{aligned}\mu^2 &= (\alpha - a)^2 = \alpha^2 - 2a\alpha + a^2 = b\beta - 2a\alpha + a^2 \\ &= (1 + a\alpha + b\beta) + (a^2 - 1 - 3a\alpha),\end{aligned}$$

und da der zweite eingeklammerte Bestandteil offenbar durch 3 teilbar ist, so gilt dasselbe auch von dem ersten; setzen wir daher

$$\gamma = \frac{1 + a\alpha + b\beta}{3},$$

so ist γ eine ganze Zahl; durch Einführung derselben geht die obige Gleichung, weil $a^2 - 1 \equiv -3c \pmod 9$ ist, in die Kongruenz

$$\mu^2 \equiv 3(\gamma - c - a\alpha) \pmod 9$$

über, und da die Zahlen μ^2 und 9 durch $3\mathfrak{p}_1$ teilbar sind, so folgt $\gamma \equiv c + a\alpha \pmod{\mathfrak{p}_1}$; da ferner $\mu = \alpha - a$ durch $\mathfrak{p}_1$ teilbar, also $\alpha \equiv a$, $a\alpha \equiv a^2 \equiv 1 \pmod{\mathfrak{p}_1}$ ist, so ergibt sich

$$\gamma \equiv c + 1 \pmod{\mathfrak{p}_1}.$$

Um eine ähnliche Kongruenz für das andere Primideal $\mathfrak{p}$ zu erhalten, setze man die kubische Gleichung, deren Wurzel μ ist, in die Form

$$\mu(\mu^2 + 3a\alpha) + a(a^2 - b^2) = 0;$$

da $a^2 - b^2$ durch 9, also durch $\mathfrak{p}^4$ teilbar ist, so folgt hieraus die Kongruenz

$$\mu(\mu^2 + 3a\alpha) \equiv 0 \pmod{\mathfrak{p}^4};$$

nun ist μ zwar durch $\mathfrak{p}\mathfrak{p}_1$, aber nicht durch $\mathfrak{p}^2$ teilbar (weil sonst μ durch $\mathfrak{p}^2\mathfrak{p}_1$, also durch 3 teilbar wäre), mithin

$$\mu^2 + 3a\alpha \equiv 0 \pmod{\mathfrak{p}^3};$$

vergleicht man dies mit der obigen Kongruenz

$$\mu^2 + 3a\alpha \equiv 3(\gamma - c) \pmod 9,$$

welche, weil 9 durch $\mathfrak{p}^4$ teilbar ist, auch für den Modul $\mathfrak{p}^3$ gilt, so folgt, daß $3(\gamma - c)$ durch $\mathfrak{p}^3$ teilbar ist, und da 3 zwar durch $\mathfrak{p}^2$, aber nicht durch $\mathfrak{p}^3$ teilbar ist, so ergibt sich die gesuchte Kongruenz

$$\gamma \equiv c \pmod{\mathfrak{p}}.$$

Besonders hervorzuheben ist aber noch das obige Resultat, daß es in jedem Körper zweiter Art eine ganze Zahl γ gibt, welche nicht in dem Modul $\mathfrak{n}$ enthalten ist; hieraus folgt, daß die Hauptordnung $\mathfrak{o}$ ein echter Teiler von $\mathfrak{n}$, also $(\mathfrak{o}, \mathfrak{n}) > 1$ ist.

§ 4.

Die Grundzahl D.

Mit Hilfe der eben geführten Untersuchung über die in $3ab$ aufgehenden Primideale gelingt es nun ohne Schwierigkeit, die Hauptordnung $\mathfrak{o}$ jedes reinen kubischen Körpers K und hiermit seine Grundzahl D sowie die in den Gleichungen

$$3ab = k(\mathfrak{o}, \mathfrak{n}), \quad D = -3k^2$$

auftretenden natürlichen Zahlen k und $(\mathfrak{o}, \mathfrak{n})$ zu bestimmen. Nach einem allgemeinen Satze der Modultheorie (D. § 171, I., S. 511) ist $\mathfrak{o}(\mathfrak{o}, \mathfrak{n}) > \mathfrak{n}$, d. h. jede Zahl des Moduls $\mathfrak{o}$ wird durch Multiplikation mit $(\mathfrak{o}, \mathfrak{n})$ in eine Zahl des Moduls $\mathfrak{n}$ verwandelt. Bedeutet daher ω jede beliebige ganze Zahl des Körpers K, d. h. jede in $\mathfrak{o}$ enthaltene Zahl, so wird $(\mathfrak{o}, \mathfrak{n})\omega$, also auch $k(\mathfrak{o}, \mathfrak{n})\omega = 3ab\omega$ in dem Modul $\mathfrak{n}$ enthalten sein, und folglich ist

$$3ab\omega = z + x\alpha + y\beta,$$

wo z, x, y ganze rationale Zahlen bedeuten; um daher alle Zahlen ω zu finden, haben wir alle Systeme z, x, y zu suchen, für welche

$$z + x\alpha + y\beta \equiv 0 \pmod{3ab}$$

wird. Bedeutet nun zunächst p eine in a aufgehende natürliche Primzahl, so ist, wie in § 3 gezeigt ist, $\mathfrak{o}p = \mathfrak{p}^3$, und da $\alpha^3 = ab^2$, $\beta^3 = a^2b$ ist, so leuchtet ein, daß $\mathfrak{p}$ die höchste in α, und $\mathfrak{p}^2$ die höchste in β aufgehende Potenz des Primideals $\mathfrak{p}$ ist. Aus der Kongruenz

$$z + x\alpha + y\beta \equiv 0 \pmod{\mathfrak{p}^3}$$

folgt daher zunächst $z \equiv 0 \pmod{\mathfrak{p}}$, mithin muß z als rationale Zahl auch durch p, also durch $\mathfrak{p}^3$ teilbar sein (D. § 179, S. 563), und hierdurch kommt die vorstehende Kongruenz auf

$$x\alpha + y\beta \equiv 0 \pmod{\mathfrak{p}^3}$$

zurück. Aus dieser Kongruenz folgt wieder $x\alpha \equiv 0 \pmod{\mathfrak{p}^2}$, und da α nicht durch $\mathfrak{p}^2$ teilbar ist, so muß die rationale Zahl x durch $\mathfrak{p}$, also auch durch p teilbar sein. Hierdurch reduziert sich unsere Kongruenz auf $y\beta \equiv 0 \pmod{\mathfrak{p}^3}$, und da β nicht durch $\mathfrak{p}^3$ teilbar ist, so muß auch die rationale Zahl y durch $\mathfrak{p}$, also auch durch p teilbar sein. Mithin sind alle drei Zahlen z, x, y durch p teilbar.

Offenbar gilt ganz dasselbe für jede in b, also für jede in ab aufgehende natürliche Primzahl p, und da ab ein Produkt von lauter verschiedenen Primzahlen p ist, so müssen die ganzen rationalen Zahlen z, x, y alle durch ab teilbar, also von der Form

$$z = abw, \quad x = abu, \quad y = abv$$

sein, wo w, u, v wieder ganze rationale Zahlen bedeuten; zugleich wird

$$3\omega = w + u\alpha + v\beta,$$

mithin ist $\mathfrak{o}\,3 > \mathfrak{n}$, d. h. jede ganze Zahl ω wird schon durch Multiplikation mit 3 in eine Zahl des Moduls $\mathfrak{n}$ verwandelt.

Ist nun ab teilbar durch 3, gehört also die Zahl 3 zu den eben betrachteten Primzahlen p, so müssen auch die Zahlen w, u, v durch 3 teilbar sein, mithin ist jede Zahl ω auch in $\mathfrak{n}$ enthalten, d. h. es ist $\mathfrak{o} = \mathfrak{n}$, $(\mathfrak{o}, \mathfrak{n}) = 1$, $k = 3ab$. Betrachten wir ferner den anderen Fall, in welchem K ebenfalls ein Körper erster Art, also $a^2 \equiv b^2 \equiv 1 \pmod{3}$, aber $a^2 - b^2$ nicht durch 9 teilbar ist, so ist (nach § 3) auch jetzt $\mathfrak{o}\,3 = \mathfrak{p}^3$, und die Zahl $\mu = \alpha - a$ ist durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbar. Multipliziert man nun mit b und bedenkt, daß $b\beta = \alpha^2 = (\mu + a)^2$ ist, so wird

$$\begin{aligned} 3b\omega &= bw + bu(\mu + a) + v(\mu + a)^2 \\ &= x_0 + x_1\mu + x_2\mu^2, \end{aligned}$$

wo die Zahlen

$$x_0 = bw + abu + a^2v, \quad x_1 = bu + 2av, \quad x_2 = v$$

ebenfalls ganze rationale Zahlen sind und der Kongruenz

$$x_0 + x_1\mu + x_2\mu^2 \equiv 0 \pmod{\mathfrak{p}^3}$$

genügen; da aber $\mathfrak{p}$ und $\mathfrak{p}^2$ die höchsten bzw. in μ und μ^2 aufgehenden Potenzen von $\mathfrak{p}$ sind, so ergibt sich ebenso wie oben, daß die Zahlen x_0, x_1, x_2 der Reihe nach durch $\mathfrak{p}$, also auch durch 3 teilbar sind, und hieraus folgt offenbar, daß auch die Zahlen v, u, w der Reihe nach durch 3 teilbar sind; mithin ist auch in diesem Falle jede Zahl ω in dem Modul $\mathfrak{n}$ enthalten, und es gilt folglich der

Satz. Ist K ein Körper erster Art, so ist

$$\mathfrak{o} = \mathfrak{n} = [1, \alpha, \beta],$$
$$k = 3ab, \quad D = -3k^2.$$

Zugleich ergibt sich für diesen Fall, wie der Leser aus § 3 leicht ableiten wird, die folgende Darstellung aller in der Grundzahl D aufgehenden Primideale $\mathfrak{p}$. Geht $\mathfrak{p}$ in ab auf, so ist

$$\mathfrak{p} = [p, \alpha, \beta],$$

wo p wieder die durch $\mathfrak{p}$ teilbare natürliche Primzahl bedeutet; geht aber $\mathfrak{p}$ nicht in ab auf, ist also $p = 3$, und ab nicht teilbar durch 3, so ist

$$\mathfrak{p} = [3, \alpha - a, \beta - b].$$

Hierauf wenden wir uns zu den Körpern K von zweiter Art, also zu den Körpern K, welche durch die Kongruenz $a \equiv \pm b \pmod 9$ charakterisiert sind, woraus zugleich folgt, daß ab nicht durch 3 teilbar ist. Wir haben schon am Schlusse von § 3 hervorgehoben, daß in diesem Falle die Hauptordnung $\mathfrak{o}$ ein echter Teiler des Moduls $\mathfrak{n}$, also $(\mathfrak{o}, \mathfrak{n}) > 1$ ist; da ferner in dem gegenwärtigen § 4 bewiesen ist, daß der Modul $\mathfrak{n}$ immer ein Teiler des Hauptideals $\mathfrak{o}3$ ist, so ist nach zwei allgemeinen Sätzen der Modul- und Idealtheorie (D. § 171, S. 510 und § 180, S. 564)

$$(\mathfrak{o}, \mathfrak{n})(\mathfrak{n}, \mathfrak{o}3) = (\mathfrak{o}, \mathfrak{o}3) = N(\mathfrak{o}3) = N(3) = 3^3,$$

also ist $(\mathfrak{o}, \mathfrak{n})$ eine der Potenzen $3, 3^2, 3^3$; zufolge § 3 ist aber auch $3ab = k(\mathfrak{o}, \mathfrak{n})$, und da ab nicht durch 3 teilbar ist, so ergibt sich $(\mathfrak{o}, \mathfrak{n}) = 3$, $k = ab$. Es ist nun auch leicht, die Hauptordnung $\mathfrak{o}$ als endlichen Modul darzustellen. Zu diesem Zwecke erinnern wir an das in § 3 gewonnene Resultat, daß die in $\mathfrak{n}$ nicht enthaltene Zahl

$$\gamma = \frac{1 + a\alpha + b\beta}{3}$$

eine ganze Zahl, also in $\mathfrak{o}$ enthalten ist; setzen wir daher

$$\mathfrak{o}_1 = \mathfrak{n} + [\gamma] = [1, \alpha, \beta, \gamma],$$

so ist der Modul $\mathfrak{o}_1$ ein Vielfaches von $\mathfrak{o}$ und zugleich ein Teiler von $\mathfrak{n}$ (nämlich der größte gemeinsame Teiler von $\mathfrak{n}$ und $[\gamma]$), und hieraus folgt nach dem schon vorher benutzten Modulsatze

$$(\mathfrak{o}, \mathfrak{o}_1)(\mathfrak{o}_1, \mathfrak{n}) = (\mathfrak{o}, \mathfrak{n}) = 3;$$

da endlich die in $\mathfrak{o}_1$ enthaltene Zahl γ nicht in $\mathfrak{n}$ enthalten, also $\mathfrak{o}_1$ ein echter Teiler von $\mathfrak{n}$, mithin $(\mathfrak{o}_1, \mathfrak{n}) > 1$ ist, so folgt*), daß $(\mathfrak{o}_1, \mathfrak{n}) = 3$, $(\mathfrak{o}, \mathfrak{o}_1) = 1$, also $\mathfrak{o} = \mathfrak{o}_1$ sein muß, womit die gesuchte Darstellung von $\mathfrak{o}$ gefunden ist. Bedenkt man noch, daß $1 = 3\gamma - a\alpha - b\beta$ ist, so leuchtet ein, daß $\mathfrak{o}$ auch als dreigliedriger Modul $[\gamma, \alpha, \beta]$ darstellbar ist. Das Resultat unserer Untersuchung besteht daher in dem folgenden

Satz. Ist K ein Körper zweiter Art, so ist

$$\mathfrak{o} = \mathfrak{n} + [\gamma] = [1, \alpha, \beta, \gamma] = [\gamma, \alpha, \beta],$$
$$k = ab, \quad D = -3k^2.$$

Auch für diesen Fall läßt sich die Darstellung der in D aufgehenden Primideale $\mathfrak{p}$ in Form von endlichen Moduln leicht aus § 3 ableiten; da sie aber für den weiteren Verlauf unserer Untersuchung nicht erforderlich ist, so begnügen wir uns, die Resultate kurz anzugeben. Geht die durch $\mathfrak{p}$ teilbare natürliche Primzahl p in ab auf, so ist

$$\mathfrak{p} = [p\gamma, \alpha, \beta] = \mathfrak{o}[p, \alpha, \beta];$$

ist aber $p = 3$, so findet man für die in der Zerlegung $\mathfrak{o}\,3 = \mathfrak{p}^2\mathfrak{p}_1$ auftretenden Primideale $\mathfrak{p}$, $\mathfrak{p}_1$ und deren Produkt die Darstellungen

$$\mathfrak{p}\mathfrak{p}_1 = [3, \alpha - a, \beta - b],$$
$$\mathfrak{p} = \mathfrak{p}\mathfrak{p}_1 + [\gamma - c] = [3, \gamma - c, \alpha - a, \beta - b],$$
$$\mathfrak{p}_1 = \mathfrak{p}\mathfrak{p}_1 + [\gamma - c - 1] = [3, \gamma - c - 1, \alpha - a, \beta - b],$$

und das Produkt $\mathfrak{p}\,\mathfrak{p}_1$ ist zugleich der Führer der Ordnung $\mathfrak{n}$, d. h. der Quotient $\mathfrak{n} : \mathfrak{o}$ oder auch der größte gemeinsame Teiler aller in der Ordnung $\mathfrak{n}$ enthaltenen Ideale (D. § 180, S. 572).

Nachdem in allen Fällen gezeigt ist, wie die Grundzahl $D = -3k^2$ von den beiden Invarianten a, b abhängt, bemerken wir zum Schluß, daß — im Gegensatz zu der Theorie der quadratischen Körper — der reine kubische Körper K oder vielmehr das System der drei konjugierten Körper K, K', K'' offenbar durch die gemeinsame Grundzahl D im allgemeinen noch nicht vollständig bestimmt ist; so z. B. tritt in den beiden Zeilen 4 und 5 der Tabelle (§ 2) derselbe Wert $k = 18$ auf, mithin haben die beiden gänzlich ver-

*) Diese Folgerung $(\mathfrak{o}_1, \mathfrak{n}) = 3$ bestätigt sich leicht durch die Bemerkung, daß die drei Zahlen 0, γ, 2γ offenbar ein Restsystem von $\mathfrak{o}_1$ nach $\mathfrak{n}$ bilden (D. § 171, S. 509).

schiedenen Körpersysteme K, K', K'', von denen das eine durch $\sqrt[3]{6}$, das andere durch $\sqrt[3]{12}$ erzeugt wird, dieselbe Grundzahl $D = -2^2 \cdot 3^5$, und ähnliches wiederholt sich in den Zeilen 13, 14 und in den Zeilen 17, 18 der Tabelle. Daß dieselbe Erscheinung auch bei Körpern zweiter Art auftritt, zeigt die Vergleichung des Invariantenpaars $a = 34 = 2 \cdot 17$, $b = 7$ mit dem Invariantenpaar $a = 119 = 7 \cdot 17$, $b = 2$, denen derselbe Wert $k = ab = 2 \cdot 7 \cdot 17$, also dieselbe Grundzahl $D = -3 \cdot 2^2 \cdot 7^2 \cdot 17^2$ entspricht, weil in beiden Fällen $a \equiv b \pmod 9$ ist.

§ 5.

Die in der Grundzahl nicht aufgehenden Primideale.

Wir wenden uns jetzt zu der Aufgabe, auch alle diejenigen natürlichen Primzahlen p, welche nicht in der Grundzahl D aufgehen, in ihre idealen Primfaktoren $\mathfrak{p}$ zu zerlegen. Um die Körper von erster und zweiter Art gemeinsam zu behandeln, erinnern wir daran, daß (nach § 4) jede ganze Zahl ω in K durch Multiplikation mit 3 jedenfalls in eine Zahl des Moduls $\mathfrak{n} = [1, \alpha, \beta]$ verwandelt wird; da $p \equiv \pm 1 \pmod 3$, so ist also auch das Produkt $(1 \mp p)\omega$, welches $\equiv \omega \pmod p$ ist, in $\mathfrak{n}$ enthalten, und man kann daher immer

$$\omega \equiv z + x\alpha + y\beta \pmod p$$

setzen, wo z, x, y ganze rationale Zahlen bedeuten. Durchläuft jede von ihnen ein bestimmtes System von p inkongruenten Zahlen (mod. p), so nimmt der Ausdruck rechter Hand p^3 verschiedene Werte ν an, und jede in $\mathfrak{n}$ enthaltene Zahl ist wenigstens einer dieser Zahlen ν kongruent (mod. p); zufolge der vorstehenden Kongruenz ist aber auch jede ganze, d. h. jede in $\mathfrak{o}$ enthaltene Zahl ω mit einer Zahl ν kongruent, und da die Anzahl $(\mathfrak{o}, \mathfrak{o}p)$ aller nach p inkongruenten Zahlen ω ebenfalls $= N(\mathfrak{o}p) = N(p) = p^3$ ist, so ergibt sich, daß die genannten Zahlen ν sämtlich inkongruent (mod. p) sind und folglich ein Restsystem von $\mathfrak{o}$ nach $\mathfrak{o}p$ bilden (D. § 180, S. 564); es kann daher auch nur dann $\omega \equiv 0 \pmod p$ werden, wenn $z \equiv x \equiv y \equiv 0 \pmod p$ ist*).

*) In der Zeichensprache der Modul- und Idealtheorie (D. § 169, S. 496, 498 und § 171, S. 510 und § 180, S. 564) drücken sich diese Beziehungen zwischen $\mathfrak{o}$, $\mathfrak{n}$ und p auf folgende Weise aus: $\mathfrak{n} + \mathfrak{o}p = \mathfrak{o}$, $\mathfrak{n} - \mathfrak{o}p = \mathfrak{n}p$, also $(\mathfrak{n}, \mathfrak{o}p) = (\mathfrak{n}, \mathfrak{n}p) = (\mathfrak{o}, \mathfrak{o}p) = N(p) = p^3$.

Benutzt man nun den für alle ganzen algebraischen Zahlen $\xi, \eta, \zeta \cdots$ geltenden Satz (D. § 185, S. 617)

$$(\xi + \eta + \zeta + \cdots)^p \equiv \xi^p + \eta^p + \zeta^p + \cdots \pmod{p}$$

und bedenkt, daß nach Fermat für jede ganze rationale Zahl z immer $z^p \equiv z \pmod{p}$ ist, so ergibt sich

$$\omega^p \equiv z + x\alpha^p + y\beta^p \pmod{p}$$

und durch Wiederholung dieses Verfahrens allgemein

$$\omega^{p^n} \equiv z + x\alpha^{p^n} + y\beta^{p^n} \pmod{p},$$

wo n jede natürliche Zahl bedeutet. Das Verhalten der Primzahl p ist nun ganz verschieden, je nachdem $p \equiv +1$ oder $p \equiv -1 \pmod 3$ ist; wir trennen daher unsere Untersuchung in zwei Hauptteile und betrachten zuerst den einfacheren Fall

I. $$p = 3m - 1 \equiv -1 \pmod 3.$$

Dann ist $p^2 - 1 = (p+1)(p-1) = 3m(p-1)$, und da ab nicht durch p teilbar ist, so folgt aus dem Satze von Fermat

$$\alpha^{p^2-1} = (ab^2)^{m(p-1)} \equiv 1 \pmod{p}$$

$$\beta^{p^2-1} = (a^2b)^{m(p-1)} \equiv 1 \pmod{p},$$

also

$$\alpha^{p^2} \equiv \alpha, \quad \beta^{p^2} \equiv \beta \pmod{p},$$

und folglich genügt jede ganze Zahl ω des Körpers K der Kongruenz

$$\omega^{p^2} \equiv \omega \pmod{p}.$$

Hieraus folgt erstens, daß p durch kein Primidealquadrat teilbar sein kann; denn wenn in irgendeinem endlichen Körper jede ganze Zahl ω einer Kongruenz von der Form

$$\omega \equiv \lambda\omega^2 + \mu\omega^3 + \nu\omega^4 + \cdots \pmod{\mathfrak{a}}$$

genügt, wo $\mathfrak{a}$ ein bestimmtes Ideal und $\lambda, \mu, \nu \cdots$ bestimmte ganze Zahlen dieses Körpers sind, so müßte, wenn $\mathfrak{a}$ durch das Quadrat eines Primideals $\mathfrak{p}$ teilbar wäre, jede durch $\mathfrak{p}$ teilbare Zahl ω auch durch $\mathfrak{p}^2$ teilbar, d. h. es müßte $\mathfrak{p}$ selbst durch $\mathfrak{p}^2$ teilbar sein, was unmöglich ist.

Da ferner die Anzahl der inkongruenten Wurzeln ω der obigen Kongruenz $= (\mathfrak{o}, \mathfrak{o}p) = p^3$, also größer als ihr Grad p^2 ist, so folgt zweitens (D. § 180, S. 570), daß $\mathfrak{o}p$ selbst kein Primideal, also ein Produkt von zwei oder drei verschiedenen Primidealen ist. Im letzteren Falle müßten diese drei Primideale, weil das Produkt ihrer Normen $= N(\mathfrak{o}p) = p^3$ ist (D. § 180, S. 564), alle vom ersten Grade

sein, es müßte daher (D. § 180, V, S. 570), wenn ω jede ganze Zahl bedeutet, $\omega^p - \omega$ durch jedes dieser Primideale, also auch durch ihr Produkt $\mathfrak{o}\,p$ teilbar sein; nun ist aber z. B. $\alpha^{p-2} = \alpha^{3(m-1)} = (a\,b^2)^{m-1}$ und $\alpha^2 = b\,\beta$, also $\alpha^p = g\,\beta$, wo g eine ganze rationale Zahl bedeutet, mithin ist die in $\mathfrak{n}$ enthaltene Zahl $\alpha - \alpha^p = \alpha - g\,\beta$ nicht durch p teilbar, und folglich unsere Annahme unzulässig. Das Resultat unserer Untersuchung besteht also darin, daß $\mathfrak{o}\,p$ ein Produkt von zwei verschiedenen Primidealen $\mathfrak{p}$, $\mathfrak{p}_1$ ist; offenbar muß das eine vom ersten, das andere vom zweiten Grade sein, und wir können daher

$$\mathfrak{o}\,p = \mathfrak{p}\,\mathfrak{p}_1, \quad N(\mathfrak{p}) = p, \quad N(\mathfrak{p}_1) = p^2$$

setzen. — Hierauf wenden wir uns zu dem Fall

II. $$p = 3\,m + 1 \equiv +1 \pmod 3.$$

Dann hat bekanntlich (D. § 31, S. 73) die Kongruenz $u^3 \equiv 1 \pmod p$ drei inkongruente rationale Wurzeln $u \equiv 1,\ r,\ r^2$, wo

$$r^2 + r + 1 \equiv 0 \pmod p$$

ist; bedeutet ferner c irgendeine durch p nicht teilbare ganze rationale Zahl, so ist $c^{p-1} = c^{3m} \equiv 1 \pmod p$ und folglich $c^m \equiv r^e \pmod p$, wo der Exponent e nach dem Modul 3 bestimmt ist; je nachdem e durch 3 teilbar oder unteilbar ist, ist die Zahl c kubischer Rest oder Nichtrest von p, d. h. die Kongruenz $w^3 \equiv c \pmod p$ hat im ersten Fall drei inkongruente Wurzeln w, im letzteren gar keine.

Wendet man dies auf die Zahl $c = a\,b^2$ an und bedenkt, daß $(a\,b^2)(a^2\,b) = (a\,b)^3$ ist, so kann man gleichzeitig

$$(a\,b^2)^m \equiv r^e, \quad (a^2\,b)^m \equiv r^{2e} \pmod p$$

setzen, und hieraus folgt

$$\left.\begin{aligned} \alpha^p &\equiv \alpha\,r^e, & \alpha^{p^2} &\equiv \alpha\,r^{2e}, & \alpha^{p^3} &\equiv \alpha \\ \beta^p &\equiv \beta\,r^{2e}, & \beta^{p^2} &\equiv \beta\,r^e, & \beta^{p^3} &\equiv \beta \end{aligned}\right\} \pmod p,$$

mithin genügt jede ganze Zahl ω der Kongruenz

$$\omega^{p^3} \equiv \omega \pmod p.$$

Hieraus folgt wieder erstens, daß p durch kein Primidealquadrat teilbar ist. Wir wollen zweitens beweisen, daß p durch kein Primideal zweiten Grades $\mathfrak{p}$ teilbar sein kann; wäre dies nämlich der Fall, so müßte (D. § 180, V, S. 570) jede ganze Zahl ω außer der vorstehenden auch den Kongruenzen $\omega^{p^2} \equiv \omega \pmod{\mathfrak{p}}$, $\omega^{p^3} \equiv \omega^p \pmod{\mathfrak{p}}$, mithin auch der Kongruenz $\omega^p \equiv \omega \pmod{\mathfrak{p}}$ genügen; dann wäre aber die Anzahl $(\mathfrak{o}, \mathfrak{p}) = N(\mathfrak{p}) = p^2$ der inkongruenten

Wurzeln ω dieser letzten Kongruenz größer als ihr Grad p, was unmöglich ist (D. § 180, S. 570), und folglich ist unsere Annahme p sei durch ein Primideal zweiten Grades teilbar, unzulässig.

Es bleiben daher nur zwei Fälle übrig: entweder ist $\mathfrak{o}p$ ein Produkt von drei verschiedenen Primidealen ersten Grades $\mathfrak{p}$, $\mathfrak{p}_1$, $\mathfrak{p}_2$, oder $\mathfrak{o}p$ ist selbst ein Primideal dritten Grades. Im ersteren Fall ist $\omega^p - \omega$ für jede ganze Zahl ω durch jedes der drei Primideale $\mathfrak{p}$, $\mathfrak{p}_1$, $\mathfrak{p}_2$, also auch durch ihr Produkt $\mathfrak{o}p$ teilbar; wendet man dies auf die Zahl $\omega = \alpha$ an, so folgt, daß $\alpha(1 - r^e)$ durch p teilbar ist, und da α relative Primzahl zu p ist, so ergibt sich $r^e \equiv 1 \pmod{p}$, also $e \equiv 0 \pmod{3}$, d. h. die Zahl ab^2 (und ebenso a^2b) ist kubischer Rest von p. Umgekehrt, wenn dies der Fall, also e durch 3 teilbar ist, so folgt $\alpha^p \equiv \alpha$, $\beta^p \equiv \beta \pmod{p}$, also auch allgemein $\omega^p \equiv \omega \pmod{p}$, und es kann daher $\mathfrak{o}p$ kein Primideal sein, weil sonst die Anzahl $(\mathfrak{o}, \mathfrak{o}p) = p^3$ der inkongruenten Wurzeln ω dieser Kongruenz größer als ihr Grad p wäre. Das Resultat unserer Untersuchung besteht also hierin: Es ist

$$\mathfrak{o}p = \mathfrak{p}\mathfrak{p}_1\mathfrak{p}_2, \quad N(\mathfrak{p}) = N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p,$$

wo $\mathfrak{p}$, $\mathfrak{p}_1$, $\mathfrak{p}_2$ drei verschiedene Primideale bedeuten, oder es ist $\mathfrak{o}p$ selbst ein Primideal dritten Grades, je nachdem die Zahl ab^2 kubischer Rest oder Nichtrest von p ist.

§ 6.

Die Dirichletsche Idealfunktion.

Das Ziel, welches wir in der gegenwärtigen Abhandlung zu erreichen suchen, besteht in der Bestimmung der Anzahl h der Idealklassen im Körper K. Die hierzu führende, von Dirichlet vorgezeichnete Methode stützt sich bekanntlich (D. § 184, S. 609—611) auf die Betrachtung der Funktion

$$J = \sum \frac{1}{N(\mathfrak{a})^s} = \Pi \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}},$$

wo $\mathfrak{a}$ in der Summe alle Ideale und $\mathfrak{p}$ in dem Produkte alle Primideale des Körpers durchläuft, und zwar kommt alles darauf an zu untersuchen, wie sich diese Funktion J der Variablen s für unendlich kleine positive Werte von $s - 1$ verhält. Bezieht sich nämlich

das Grenzzeichen lim auf diese Annäherung der Variablen s an die Zahl 1, so wird

$$\lim (s-1)J = gh,$$

wo h die Klassenanzahl der Ideale und g eine wesentlich von der Grundzahl D und von den Einheiten des Körpers abhängende Konstante bedeutet, deren allgemeiner Ausdruck

$$g = \frac{2^v \pi^{n-v} E}{\sqrt{(D)}}$$

jetzt für unseren Fall eines reinen kubischen Körpers K zu spezialisieren ist. Der Nenner $\sqrt{(D)}$ ist die positive Quadratwurzel aus dem absoluten Werte (D) der Grundzahl $D = -3k^2$, also $\sqrt{(D)} = k\sqrt{3}$, wo $\sqrt{3}$ positiv und $k = 3ab$ oder $= ab$ ist, je nachdem K ein Körper erster oder zweiter Art ist. Das Zeichen π hat die gewöhnliche Bedeutung der Ludolfschen Zahl 3,14159 ..., und n ist der Grad des Körpers K, also $n = 3$. Die Zahl v ist dadurch bestimmt, daß $(2v-n)$ die Anzahl der reellen, also $2(n-v)$ die Anzahl der imaginären unter den mit K konjugierten Körpern K, K', K'' ist; mithin ist $v = 2$. Die Konstante E bestimmt sich durch $rE = S'$, wo r die Anzahl 2 aller in dem (reellen) Körper K enthaltenen Einheitswurzeln ± 1 und S' den Regulator eines Fundamentalsystems S von $(v-1)$ Einheiten in K bedeutet (D. § 183, S. 597, 602); da $v = 2$ ist, so besteht S aus einer einzigen Einheit $\varepsilon > 1$, und der Regulator S' ist $= log\,\varepsilon$, mithin $E = \frac{1}{2} log\,\varepsilon$ (und alle Einheiten in K haben die Form $\pm \varepsilon^m$, wo m alle ganzen rationalen Zahlen durchläuft). Durch das Eintragen aller dieser Werte in den obigen Ausdruck erhalten wir

$$g = \frac{2\pi\, log\,\varepsilon}{k\sqrt{3}},$$

mithin

$$\lim (s-1)J = h\,\frac{2\pi\, log\,\varepsilon}{k\sqrt{3}}.$$

Für die Bildung der Funktion J, zu welcher wir jetzt übergehen, legen wir die Produktform zu Grunde; durchläuft p alle natürlichen Primzahlen, und bezeichnen wir mit $F(p)$ denjenigen Faktor von J, welcher von allen verschiedenen in p aufgehenden Primidealen $\mathfrak{p}$ herrührt, so wird

$$J = \Pi F(p);$$

setzen wir ferner zur Abkürzung

$$P_n = \frac{1}{1 - \frac{1}{p^{ns}}},$$

wo n irgendeine natürliche Zahl bedeutet, so ergeben sich (nach §§ 3, 5) die folgenden Regeln zur Bestimmung des Faktors $F(p)$.

1. Geht p in k auf, so ist $\mathfrak{o}p = \mathfrak{p}^3$, wo $\mathfrak{p}$ ein Primideal ersten Grades, also $N(\mathfrak{p}) = p$, mithin $F(p) = P_1$.

2. Geht p nicht in k, aber in D auf, so ist $p = 3$ und K ein Körper zweiter Art; dann ist $\mathfrak{o}p = \mathfrak{o}3 = \mathfrak{p}^2\mathfrak{p}_1$, wo $\mathfrak{p}$ und $\mathfrak{p}_1$ zwei verschiedene Primideale ersten Grades bedeuten, also $N(\mathfrak{p}) = N(\mathfrak{p}_1) = 3 = p$, mithin $F(p) = P_1^2$.

3. Geht p nicht in D auf, und ist $p \equiv -1 \pmod 3$, so ist $\mathfrak{o}p = \mathfrak{p}\mathfrak{p}_1$, $N(\mathfrak{p}) = p$, $N(\mathfrak{p}_1) = p^2$, mithin $F(p) = P_1 P_2$.

4. Geht p nicht in D auf, ist ferner $p \equiv +1 \pmod 3$ und ab^2 kubischer Rest von p, so ist $\mathfrak{o}p = \mathfrak{p}\mathfrak{p}_1\mathfrak{p}_2$, $N(\mathfrak{p}) = N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$, mithin $F(p) = P_1^3$.

5. Geht p nicht in D auf, ist ferner $p \equiv +1 \pmod 3$ und ab^2 kubischer Nichtrest von p, so ist $\mathfrak{o}p$ ein Primideal dritten Grades, mithin $F(p) = P_3$.

§ 7.

Der quadratische Körper von der Grundzahl -3.

Aus der Vergleichung der beiden letzten Regeln für die Primzahlen p, welche $\equiv +1 \pmod 3$ sind und nicht in D aufgehen, leuchtet ein, daß zur Bildung unserer Funktion J die Theorie der kubischen Reste durchaus erforderlich ist. Gauß hat sich seit dem Jahre 1805 mit dieser Theorie und derjenigen der biquadratischen Reste beschäftigt*) und hierbei bald die überaus folgenreiche Entdeckung gemacht, daß, um dieselben auf einen gleichen Grad von Vollkommenheit zu erheben wie die Lehre von den quadratischen Resten, das Gebiet der höheren Arithmetik, in welcher bis dahin nur rationale ganze Zahlen betrachtet waren, durch die Einführung von neuen ganzen Zahlen erweitert werden muß, welche aus dritten oder vierten Wurzeln der Einheit gebildet sind, und hiermit war zugleich der Grund für die allgemeine Theorie der ganzen algebraischen

*) Vgl. Bd. II seiner Werke, S. 50, 67, 102, 161, 165, 166, 171.

Zahlen gelegt. Gauß hat aber von seinen Untersuchungen nur die auf die biquadratischen Reste bezüglichen teilweise veröffentlicht, und die in seinem Nachlaß vorgefundenen Aufzeichnungen über die aus dritten Wurzeln der Einheit gebildeten Zahlen sind wegen ihrer Unvollständigkeit nicht in die Herausgabe seiner Werke aufgenommen*) [1)]. Den in diesem Zahlengebiete Q (dem quadratischen Körper von der Grundzahl -3) geltenden Reziprozitätssatz für die kubischen Reste hat zuerst Jacobi**) bekanntgemacht und in seinen Vorlesungen bewiesen; derselbe aus der Theorie der Kreisteilung gezogene Beweis ist später von Eisenstein***), der ihn ohne Zweifel unabhängig von Jacobi gefunden hat, zuerst veröffentlicht. Da dieser Gegenstand seitdem von mehreren Autoren†) behandelt und als hinreichend bekannt anzusehen ist, so begnügen wir uns, die wichtigsten, für unsere Untersuchung notwendigen Tatsachen kurz in Erinnerung zu bringen.

Der durch die imaginäre dritte Einheitswurzel ϱ erzeugte quadratische Körper Q von der Grundzahl -3 besteht aus allen Zahlen ω von der Form $x + y\varrho$, wo x, y rationale Zahlen bedeuten, und jede solche Zahl ω geht durch die nicht identische Permutation des Körpers in die konjugierte Zahl $\omega' = x + y\varrho^2 = x - y - y\varrho$ über. Da von den Zahlen des reinen kubischen Körpers K im folgenden gar nicht mehr die Rede sein wird, so bezeichnen wir die Norm $\omega\omega' = x^2 - xy + y^2$ unbedenklich mit $N(\omega)$, und ebenso setzen wir die aus allen ganzen Zahlen ω bestehende Hauptordnung $[1, \varrho] = o$. Die sechs Einheiten des Körpers sind die Zahlen ± 1, $\pm\varrho$, $\pm\varrho^2$, die wir gemeinsam immer mit σ bezeichnen. Alle Ideale des Körpers sind Hauptideale, d. h. jede von 0 und den Einheiten σ verschiedene

---

*) Vgl. unten § 11.

**) Über die Kreisteilung und ihre Anwendung auf die Zahlentheorie (Monatsberichte der Berliner Akademie vom Jahre 1837, wieder abgedruckt in Crelles Journal, Bd. 30, 1846).

***) Beweis des Reziprozitätssatzes für die kubischen Reste in der Theorie der aus dritten Wurzeln der Einheit zusammengesetzten komplexen Zahlen (Crelles Journal, Bd. 27, 1844). — Nachtrag zum kubischen Reziprozitätssatz für die aus dritten Wurzeln der Einheit zusammengesetzten komplexen Zahlen. Kriterien des kubischen Charakters der Zahl 3 und ihrer Teiler (Crelles Journal, Bd. 28, 1844).

†) Vgl. namentlich Bachmann: Die Lehre von der Kreisteilung und ihre Beziehungen zur Zahlentheorie. Leipzig 1872 (Vorlesungen 14 und 15).

[1)] Man vgl. C. F. Gauß, Werke Bd. VIII, S. 5—20 und die dazu gehörigen Bemerkungen von Fricke.]

ganze Zahl ist entweder eine Primzahl π des Körpers, oder sie ist zusammengesetzt, und im letzteren Falle kann sie stets und wesentlich nur auf eine einzige Art als Produkt von lauter Primzahlen π dargestellt werden, wobei die sechs mit einer Zahl ω assoziierten Zahlen $\sigma\omega$ als nicht wesentlich verschieden angesehen werden. Das System aller Primzahlen π ergibt sich in folgender Weise aus der Betrachtung der durch sie teilbaren natürlichen Primzahlen p. Die Zahl $p = 3 = (1-\varrho)(1-\varrho^2) = -\varrho^2(1-\varrho)^2$ ist wesentlich das Quadrat der Primzahl ersten Grades $\pi = 1-\varrho$; ist $p \equiv +1 \pmod 3$, so ist $p = \pi\pi' = N(\pi) = N(\pi')$ das Produkt von zwei konjugierten, wesentlich verschiedenen Primzahlen ersten Grades π und π'; ist $p \equiv -1 \pmod 3$, so ist p selbst eine Primzahl zweiten Grades π in Q, also $N(\pi) = p^2$. Mit Ausnahme des ersten dieser drei Fälle ist daher immer $N(\pi) \equiv +1 \pmod 3$.

Ist μ irgendeine von 0 verschiedene Zahl in $\mathfrak{o}$, so ist $N(\mu)$ die Anzahl $(\mathfrak{o}, \mathfrak{o}\mu)$ aller nach μ inkongruenten Zahlen in $\mathfrak{o}$; bezeichnen wir ferner mit $\varphi'(\mu)$ die Anzahl derjenigen inkongruenten Zahlen ω, welche relative Primzahlen zu μ sind, so ist $\varphi'(\sigma) = 1$ und, wenn μ keine Einheit ist,

$$\varphi'(\mu) = N(\mu)\,\Pi\left(1 - \frac{1}{N(\pi)}\right),$$

wo π alle wesentlich verschiedenen, in μ aufgehenden Primzahlen durchläuft; zugleich ist

$$\omega^{\varphi'(\mu)} \equiv 1 \pmod{\mu}.$$

Ist π eine von $(1-\varrho)$ verschiedene Primzahl, also $N(\pi) = 3m + 1$, $\varphi'(\pi) = 3m$, so genügt jede durch π nicht teilbare Zahl ω der Kongruenz

$$\omega^{3m} - 1 = (\omega^m - 1)(\omega^m - \varrho)(\omega^m - \varrho^2) \equiv 0 \pmod{\pi},$$

und da bekanntlich keine der drei Kongruenzen

$$\omega^m \equiv \varrho^e \pmod{\pi},$$

wo $e \equiv 0, 1, 2 \pmod 3$ zu setzen ist, mehr als m inkongruente Wurzeln ω haben kann, so muß jede von ihnen genau m solche Wurzeln haben. Diejenigen m Zahlen ω, für welche $e \equiv 0 \pmod 3$ wird, sind die kubischen Reste der Primzahl π, d. h. für jede dieser Zahlen ω (und nur für diese) gibt es eine oder vielmehr drei inkongruente Wurzeln ξ der Kongruenz $\xi^3 \equiv \omega \pmod{\pi}$. Die übrigen $2m$ Zahlen ω sind die kubischen Nichtreste von π, und sie ver-

teilen sich in gleicher Anzahl m auf die beiden Fälle $e \equiv 1, 2 \pmod 3$. In allen Fällen nennen wir die durch ω vollständig bestimmte Einheitswurzel ϱ^e den kubischen Charakter oder kurz den Charakter der Zahl ω in bezug auf die Primzahl π und setzen nach Jacobi

$$\left(\frac{\omega}{\pi}\right) = \varrho^e,$$

weil hier und in der Folge eine Verwechselung mit dem Symbol von Legendre in der Theorie der quadratischen Reste nicht zu befürchten ist*). Unser Symbol wird also vollständig erklärt durch

$$\left(\frac{\omega}{\pi}\right)^3 = 1, \quad \left(\frac{\omega}{\pi}\right) \equiv \omega^m \pmod \pi,$$

wo m die obige Bedeutung hat. Hieraus folgt zunächst, daß der Wert des Symbols ungeändert bleibt, wenn die Primzahl π durch eine assoziierte Zahl $\sigma\pi$, oder wenn ω durch eine nach π kongruente Zahl ersetzt wird, und da für je zwei durch π nicht teilbare Zahlen ω_1, ω_2 offenbar das Gesetz

$$\left(\frac{\omega_1 \omega_2}{\pi}\right) = \left(\frac{\omega_1}{\pi}\right)\left(\frac{\omega_2}{\pi}\right)$$

gilt, so fällt das Symbol, als Funktion aller durch π nicht teilbaren Zahlen ω angesehen, unter den allgemeinen Begriff eines Charakters einer Abelschen Gruppe, welche letztere hier von den $3m$ Zahlklassen $\omega \pmod \pi$ gebildet wird (D. § 184, S. 612); diejenigen m Zahlklassen, welche aus den kubischen Resten von π, also aus den Zahlen ω bestehen, deren Charakter $= 1$ ist, bilden ebenfalls eine Gruppe, d. h. sie reproduzieren sich durch Multiplikation. Da $\pm 1 = (\pm 1)^3$, so ist stets

$$\left(\frac{\pm 1}{\pi}\right) = 1.$$

Bedenkt man ferner, daß jede Potenz ϱ^e durch die nicht identische Permutation des Körpers in ϱ^{2e}, also die obige Kongruenz $\omega^m \equiv \varrho^e \pmod \pi$ in die Kongruenz $\omega'^m \equiv \varrho^{2e} \pmod{\pi'}$ übergeht, so ergibt sich aus der Definition des Symbols das Gesetz

$$\left(\frac{\omega'}{\pi'}\right) = \left(\frac{\omega}{\pi}\right)^2.$$

*) Von dieser Ausdrucks- und Bezeichnungsweise weicht die von Eisenstein benutzte ein wenig ab.

Wenden wir dies auf den Fall an, wo ω eine rationale Zahl c, also $c' = c$ ist, so ergibt sich

$$\left(\frac{c}{\pi'}\right) = \left(\frac{c}{\pi}\right)^2.$$

Ist nun erstens die durch π teilbare natürliche Primzahl $p \equiv -1 \pmod 3$, so sind π und π' assoziiert mit $p = p'$, mithin

$$\left(\frac{c}{p}\right) = 1, \quad \text{wenn } p \equiv -1 \pmod 3;$$

dasselbe ergibt sich auch daraus, daß in diesem Falle $3m = (p+1)(p-1)$, also m teilbar durch $p-1$, und folglich $c^m \equiv 1 \pmod p$ ist. Wenn aber zweitens $p = 3m+1 \equiv +1 \pmod 3$ ist, so sind π, π' zwei wesentlich verschiedene Primzahlen ersten Grades, und es ist entweder

$$\left(\frac{c}{\pi}\right) = \left(\frac{c}{\pi'}\right) = 1$$

oder

$$\left(\frac{c}{\pi}\right) = \varrho, \quad \left(\frac{c}{\pi'}\right) = \varrho^2$$

oder

$$\left(\frac{c}{\pi}\right) = \varrho^2, \quad \left(\frac{c}{\pi'}\right) = \varrho.$$

Im ersten dieser drei Fälle, und nur in diesem, ist c kubischer Rest von π, also $c^m \equiv 1 \pmod \pi$, und da hieraus offenbar auch $c^m \equiv 1 \pmod p$ folgt, so ist (nach § 5, II) die Zahl c auch kubischer Rest von p im Körper der rationalen Zahlen; und umgekehrt, wenn letzteres der Fall ist, so leuchtet unmittelbar ein, daß c auch im Körper Q kubischer Rest von π (und π') ist; mithin tritt der erste der drei obigen Fälle dann und nur dann ein, wenn c im Körper der rationalen Zahlen kubischer Rest von p ist.

An dieser Stelle brechen wir die Aufzählung der für uns wichtigen Eigenschaften des Körpers Q vorläufig ab, um sie später wieder aufzunehmen. Das Vorstehende reicht nämlich schon aus, um die in § 6 begonnene Darstellung der Idealfunktion J des reinen kubischen Körpers K wesentlich zu vereinfachen. Zu diesem Zweck führen wir, wenn die Invarianten a, b des Körpers K und die daraus abgeleiteten Zahlen k und $D = -3k^2$ ihre frühere Bedeutung (§§ 3, 4) behalten, für jede Primzahl π des quadratischen Körpers Q eine Funktion $\psi(\pi)$ ein, welche für alles Folgende von der größten

Wichtigkeit ist; bedeutet p wieder die durch π teilbare natürliche Primzahl, so definieren*) wir auf folgende Weise:

I. Geht π, also auch p in k auf, so setzen wir

$$\psi(\pi) = 0.$$

II. Geht π, also auch p nicht in k, wohl aber in D auf, so ist $p = 3$, also π assoziiert mit $(1-\varrho)$, und der Körper K ist von zweiter Art; in diesem Fall setzen wir

$$\psi(\pi) = 1.$$

III. In den übrigen, also in allen denjenigen Fällen, wo π, also auch p nicht in D aufgeht, setzen wir

$$\psi(\pi) = \left(\frac{ab^2}{\pi}\right),$$

wo das Symbol rechter Hand die oben angegebene Bedeutung hat, also eine Potenz von ϱ ist.

Aus dieser Definition folgen offenbar für alle Primzahlen π zunächst die beiden Sätze

IV. $$\psi(\sigma\pi) = \psi(\pi), \quad \psi(\pi') = \psi(\pi)^2.$$

Man überzeugt sich ferner leicht, daß in allen fünf Fällen, welche am Schlusse von § 6 aufgezählt sind, die dort erklärte Funktion $F(p)$ durch den Ausdruck

$$F(p) = \frac{1}{1-\frac{1}{p^s}} \cdot \Pi \frac{1}{1-\frac{\psi(\pi)}{N(\pi)^s}}$$

dargestellt wird, wo das Produktzeichen Π sich auf alle wesentlich verschiedenen, in p aufgehenden Primzahlen π bezieht. Um dies zu beweisen, bezeichnen wir den Ausdruck rechter Hand vorläufig mit $F_1(p)$; gehen wir die fünf Fälle am Schlusse von § 6 unter Beibehaltung der dortigen Bedeutung von P_n einzeln durch, so ergibt sich folgendes:

1. Zufolge der Definition I ist $\psi(\pi) = 0$ für jede in p aufgehende Primzahl, mithin $F_1(p) = P_1$.

*) Die hier für die Primzahlen π, später für alle ganzen Zahlen ω des Körpers Q erklärte Funktion ψ hängt offenbar unsymmetrisch, aber so von den Invarianten a, b des Körpers K ab, daß sie durch deren Vertauschung in ihr Quadrat übergeht.

2. Zufolge der Definition II ist $\psi(\pi) = 1$ für die wesentlich einzige in p aufgehende Primzahl $\pi = \sigma(1 - \varrho)$, und da $N(\pi) = 3 = p$ ist, so wird $F_1(p) = P_1^2$.

3. Die wesentlich einzige in p aufgehende Primzahl π ist p selbst; zufolge der Definition III und weil $p \equiv -1 \pmod 3$ ist, wird daher

$$\psi(\pi) = \left(\frac{ab^2}{p}\right) = 1,$$

und da $N(\pi) = p^2$ ist, so wird $F_1(p) = P_1 P_2$.

4. In diesem (wie in dem folgenden) Falle ist p durch zwei wesentlich verschiedene Primzahlen π, π' teilbar, deren Normen $N(\pi) = N(\pi') = p$ sind; da ferner ab^2 kubischer Rest von p, also auch von π und π' ist, so ist zufolge der Definition III:

$$\psi(\pi) = \left(\frac{ab^2}{\pi}\right) = 1, \quad \psi(\pi') = \left(\frac{ab^2}{\pi'}\right) = 1,$$

mithin wird $F_1(p) = P_1^3$.

5. Da in diesem Falle ab^2 kubischer Nichtrest von p, also auch von π, π' ist, so folgt aus der Definition III entweder

$$\psi(\pi) = \left(\frac{ab^2}{\pi}\right) = \varrho, \quad \psi(\pi') = \left(\frac{ab^2}{\pi'}\right) = \varrho^2$$

oder

$$\psi(\pi) = \left(\frac{ab^2}{\pi}\right) = \varrho^2, \quad \psi(\pi') = \left(\frac{ab^2}{\pi'}\right) = \varrho,$$

mithin wird in beiden Fällen

$$F_1(p) = \frac{1}{1 - \frac{1}{p^s}} \cdot \frac{1}{1 - \frac{\varrho}{p^s}} \cdot \frac{1}{1 - \frac{\varrho^2}{p^s}} = P_3.$$

Nachdem hiermit für alle Fälle die Identität $F(p) = F_1(p)$ bewiesen ist, ergibt sich für die Idealfunktion $J = \Pi F(p)$, wo p alle natürlichen Primzahlen durchläuft, die folgende Zerlegung

$$J = GH;$$

hier ist

$$G = \Pi \frac{1}{1 - \frac{1}{p^s}} = \sum \frac{1}{n^s},$$

wo sich das Produktzeichen Π auf alle natürlichen Primzahlen p, das Summenzeichen Σ auf alle natürlichen Zahlen n bezieht, während

$$H = \Pi \frac{1}{1 - \frac{\psi(\pi)}{N(\pi)^s}}$$

ist, wo das Produktzeichen Π sich auf alle wesentlich verschiedenen Primzahlen π des Körpers Q bezieht. Wir wollen nun dieses unendliche Produkt H ebenfalls in Form einer unendlichen Reihe darstellen.

Sobald eine Funktion $\psi(\pi)$ für alle Primzahlen π in Q, und zwar so definiert ist, daß für alle sechs mit π assoziierten Primzahlen $\sigma\pi$ immer $\psi(\sigma\pi) = \psi(\pi)$ wird, so läßt sich die Funktion ψ stets zu einer Funktion $\psi(\omega)$ jeder ganzen Zahl ω in Q so erweitern, daß für je zwei solche Zahlen ω_1, ω_2 das Gesetz

V. $$\psi(\omega_1\omega_2) = \psi(\omega_1)\psi(\omega_2)$$

gilt; schließt man noch die beiden leicht zu behandelnden, für uns aber gänzlich interesselosen singulären Fälle aus, wo die gegebenen Zahlen $\psi(\pi)$ alle $= 1$ oder alle $= 0$ sind, so kann eine solche Erweiterung der Funktion ψ auch nur auf eine einzige Weise ausgeführt werden. Soll nämlich das Gesetz V bestehen, so muß zunächst $\psi(0) = \psi(0)\psi(\pi)$, mithin

VI. $$\psi(0) = 0$$

sein; da ferner nach unserer Voraussetzung $\psi(\sigma\pi) = \psi(\pi)$ ist, so muß $\psi(\sigma)\psi(\pi) = \psi(\pi)$, also

VII. $$\psi(\sigma) = 1$$

und folglich auch immer

VIII. $$\psi(\sigma\omega) = \psi(\omega)$$

sein. Wählt man nun aus jedem System von sechs assoziierten Primzahlen eine bestimmte nach Belieben aus und nennt dieselbe etwa eine primäre Primzahl, so ist jede zusammengesetzte Zahl ω von der Form

$$\omega = \sigma\pi_1\pi_2\pi_3\cdots,$$

wo σ eine bestimmte Einheit und wo das System der primären Primzahlen π_1, π_2, π_3 $\cdots$ ebenfalls vollständig bestimmt ist; nach dem obigen Gesetze, welches offenbar für eine beliebige Anzahl von Faktoren gelten muß, ist dann

IX. $$\psi(\omega) = \psi(\pi_1)\psi(\pi_2)\psi(\pi_3)\cdots,$$

und folglich ist die geforderte Erweiterung der Funktion ψ nur auf eine einzige Weise möglich. Daß aber umgekehrt die durch die vorstehenden Bestimmungen VI, VII, IX erhaltene Funktion ψ auch dem obigen Multiplikationsgesetz V genügt, leuchtet unmittelbar ein. Zugleich ergibt sich aus IV für unsere Funktion ψ der Satz

X. $$\psi(\omega') = \psi(\omega)^2.$$

Entwickelt man nun jeden Faktor des unendlichen Produktes H, in welchem π ausschließlich alle primären Primzahlen durchläuft, in eine geometrische Reihe

$$\frac{1}{1 - \frac{\psi(\pi)}{N(\pi)^s}} = 1 + \frac{\psi(\pi)}{N(\pi)^s} + \frac{\psi(\pi)^2}{N(\pi)^{2s}} + \frac{\psi(\pi)^3}{N(\pi)^{3s}} + \cdots,$$

so nimmt die letztere zufolge der Erweiterung unserer Funktion ψ die Form

$$1 + \frac{\psi(\pi)}{N(\pi)^s} + \frac{\psi(\pi^2)}{N(\pi^2)^s} + \frac{\psi(\pi^3)}{N(\pi^3)^s} + \cdots = \sum \frac{\psi(\pi^n)}{N(\pi^n)^s}$$

an, wo n den Wert 0 und alle natürlichen Zahlen durchläuft. Multipliziert man ferner alle diese den primären Primzahlen π entsprechenden Reihen, so erhält man

$$H = \sum \frac{\psi(\omega)}{N(\omega)^s},$$

wo ω jede Zahl von der Form

$$\omega = \pi_1^{n_1} \pi_2^{n_2} \pi_3^{n_3} \cdots$$

einmal durchläuft, in welcher $\pi_1, \pi_2, \pi_3 \cdots$ voneinander verschiedene primäre Primzahlen und $n_1, n_2, n_3 \cdots$ ganze, nicht negative Zahlen bedeuten. Bedenkt man endlich, daß je zwei verschiedene solche Zahlen ω auch nicht assoziiert sind, und daß zu jeder Zahl ω sechs assoziierte Zahlen $\mu = \sigma\omega$ gehören, denen dieselbe Norm $N(\mu) = N(\omega)$ und derselbe Wert $\psi(\mu) = \psi(\omega)$ zukommt, so erhält man das Resultat

$$6H = \sum \frac{\psi(\mu)}{N(\mu)^s},$$

wo das Summenzeichen sich auf alle von Null verschiedenen ganzen Zahlen μ des Körpers Q bezieht.

Aus der Definition der Funktion ψ geht hervor, daß $\psi(\mu)$ immer und nur dann $= 0$ ist, wenn μ durch eine in der Zahl k aufgehende Primzahl π teilbar ist; läßt man alle diese verschwindenden Glieder weg, so ist die obige Summe nur noch auf alle diejenigen Zahlen μ

auszudehnen, welche relative Primzahlen zu der Zahl k sind, und $\psi(\mu)$ ist immer eine Potenz von ϱ. Um aber die allgemeine Form aller Zahlen μ zu finden, für welche $\psi(\mu)$ einen vorgeschriebenen Wert 1 oder ϱ oder ϱ^2 besitzt, bedürfen wir des kubischen Reziprozitätssatzes.

§ 8.

Der kubische Reziprozitätssatz.

Indem wir die in § 7 begonnene Aufzählung der für unsere Untersuchung wichtigen Eigenschaften des Körpers Q wieder aufnehmen, schreiten wir zunächst zu einer schon von Jacobi empfohlenen und auch von Eisenstein benutzten Erweiterung des Symbols

$$\left(\frac{\omega}{\mu}\right)$$

für alle Fälle, wo μ relative Primzahl zu 3ω ist, während bisher μ als Primzahl π vorausgesetzt war; diese Erweiterung ist genau auf dieselbe Weise durchzuführen wie diejenige der Funktion ψ in § 7. Wir setzen daher

$$\left(\frac{\omega}{\sigma}\right) = 1,$$

wo σ wieder jede Einheit bedeutet; ist ferner die zusammengesetzte Zahl

$$\mu = \pi_1 \pi_2 \pi_3 \cdots$$

als Produkt von lauter Primzahlen $\pi_1, \pi_2, \pi_3 \cdots$ dargestellt, so setzen wir

$$\left(\frac{\omega}{\mu}\right) = \left(\frac{\omega}{\pi_1}\right)\left(\frac{\omega}{\pi_2}\right)\left(\frac{\omega}{\pi_3}\right)\cdots,$$

und diese Definition ist eine durchaus eindeutige, weil das vorstehende Produkt ungeändert bleibt, wenn die Primzahlen π durch assoziierte Primzahlen $\sigma\pi$ ersetzt werden. Aus den früher erwähnten Eigenschaften des einfachen Symbols ergeben sich offenbar für das neue Symbol die Gesetze

$$\left(\frac{\omega}{\mu}\right)^3 = 1, \quad \left(\frac{\omega}{\sigma\mu}\right) = \left(\frac{\omega}{\mu}\right), \quad \left(\frac{\pm 1}{\mu}\right) = 1, \quad \left(\frac{\omega'}{\mu'}\right) = \left(\frac{\omega}{\mu}\right)^2,$$

$$\left(\frac{\omega_1\omega_2}{\mu}\right) = \left(\frac{\omega_1}{\mu}\right)\left(\frac{\omega_2}{\mu}\right), \quad \left(\frac{\omega}{\mu_1\mu_2}\right) = \left(\frac{\omega}{\mu_1}\right)\left(\frac{\omega}{\mu_2}\right),$$

und wenn μ_0 das Produkt aller wesentlich verschiedenen, in μ aufgehenden Primzahlen π oder auch irgendeine durch dieses Produkt teilbare Zahl (z. B. μ) bedeutet, so folgt aus

$$\omega_1 \equiv \omega_2 \pmod{\mu_0} \text{ auch } \left(\frac{\omega_1}{\mu}\right) = \left(\frac{\omega_2}{\mu}\right).$$

Unser Symbol ist daher, als Funktion des Zählers ω angesehen, auch jetzt ein Charakter der Abelschen Gruppe, welche von den $\varphi'(\mu)$ Zahlklassen $\omega \pmod{\mu}$ gebildet wird.

Ist nun der Nenner μ des Symbols assoziiert mit der dritten Potenz einer Zahl ν (in Q), so leuchtet ein, daß für alle $\varphi'(\mu)$ Zahlklassen ω das Symbol den Wert 1 hat, weil aus $\mu = \sigma\nu^3$ auch

$$\left(\frac{\omega}{\mu}\right) = \left(\frac{\omega}{\sigma\nu^3}\right) = \left(\frac{\omega}{\nu^3}\right) = \left(\frac{\omega}{\nu}\right)^3 = 1$$

folgt. In jedem anderen Falle gibt es aber unter den höchsten in μ aufgehenden Primzahlpotenzen π^e mindestens eine, deren Exponent e nicht durch 3 teilbar ist, und man kann nach § 7 einen kubischen Nichtrest λ der Primzahl π so wählen, daß

$$\left(\frac{\lambda}{\pi}\right) = \varrho^e$$

wird; setzt man nun $\mu = \nu\pi^e$, so ist ν relative Primzahl zu π^e, und man kann bekanntlich eine Zahl $\omega_1 \pmod{\mu}$ durch die Kongruenzen

$$\omega_1 \equiv 1 \pmod{\nu}, \quad \omega_1 \equiv \lambda \pmod{\pi^e}$$

bestimmen; dann ist ω_1 relative Primzahl zu μ, und aus den obigen Sätzen ergibt sich

$$\left(\frac{\omega_1}{\mu}\right) = \left(\frac{\omega_1}{\nu}\right)\left(\frac{\omega_1}{\pi}\right)^e = \left(\frac{1}{\nu}\right)\left(\frac{\lambda}{\pi}\right)^e = \varrho^{e^2} = \varrho;$$

bezeichnet man nun mit ω_0 alle diejenigen nach μ inkongruenten Zahlen, welche der Bedingung

$$\left(\frac{\omega_0}{\mu}\right) = 1$$

genügen und offenbar für sich eine Gruppe bilden, so folgt leicht, daß

$$\left(\frac{\omega}{\mu}\right) = 1 \text{ oder } \varrho \text{ oder } \varrho^2$$

wird, je nachdem

$$\omega \equiv \omega_0 \text{ oder } \omega_0\omega_1 \text{ oder } \omega_0\omega_1^2 \pmod{\mu}$$

ist, und jede dieser drei Arten von Zahlen besteht aus $\frac{1}{3}\varphi'(\mu)$ Zahlklassen ω (mod. μ).

Die durch die Primzahl $(1-\varrho)$ nicht teilbaren Zahlen μ zerfallen in bezug auf die vier Moduln $1-\varrho$, $(1-\varrho)^2$, $(1-\varrho)^3$, $(1-\varrho)^4$ bzw. in 2, 6, 18, 54 Zahlklassen, welche auf folgende Weise dargestellt werden können:

$$\mu \equiv \pm 1 \pmod{1-\varrho}, \quad \mu \equiv \sigma \pmod 3,$$
$$\mu \equiv \sigma \cdot 4^m \pmod{3-3\varrho}, \quad \mu \equiv \sigma \cdot 4^m \cdot (4-3\varrho)^n \pmod 9,$$

wo σ jede Einheit und jeder der Exponenten m, n die Zahlen 0, 1, 2 durchläuft; aus der letzten Darstellung gehen die anderen sukzessive hervor, weil $4-3\varrho \equiv 1 \pmod{3-3\varrho}$, $4 \equiv 1 \pmod 3$, $\sigma \equiv \pm 1 \pmod{1-\varrho}$ ist; zugleich wird

$$N(\mu) = \mu\mu' \equiv 4^{2m} \equiv 1 + 6m \pmod 9.$$

Legen wir diese Darstellung der Zahlen μ zugrunde, so nehmen die zuerst von Eisenstein aufgestellten und bewiesenen sogenannten Ergänzungssätze folgende Formen an:

$$\left(\frac{\varrho}{\mu}\right) = \varrho^{\frac{N(\mu)-1}{3}} = \varrho^{2m}, \quad \left(\frac{1-\varrho}{\mu}\right) = \varrho^{m+n},$$
$$\left(\frac{\varrho-\varrho^2}{\mu}\right) = \varrho^n, \quad \left(\frac{3}{\mu}\right) = \varrho^{2n};$$

der erste dieser vier Sätze folgt sehr leicht aus der ursprünglichen Definition des kubischen Charakters in bezug auf eine Primzahl π, während der zweite eine tiefer liegende Begründung erfordert, die man am angegebenen Orte findet; durch Multiplikation ergibt sich hieraus der dritte und endlich durch Quadrieren der vierte Satz, weil $(\varrho-\varrho^2)^2 = -3$ ist. Aus diesen Sätzen folgt, daß die vier vorstehenden Symbole ungeändert bleiben, wenn die Zahl μ durch irgendeine nach dem Modul 9 kongruente Zahl ersetzt wird; für das erste Symbol gilt dies sogar schon dann, wenn diese Kongruenz in bezug auf den Modul $(3-3\varrho)$ stattfindet.

Wir wenden uns endlich zu dem von Eisenstein bewiesenen allgemeinen Reziprozitätssatze. Da jede durch $(1-\varrho)$ unteilbare Zahl mit einer, und nur einer der sechs Einheiten σ nach dem Modul 3 kongruent ist, so finden sich unter den sechs mit ihr assoziierten Zahlen immer zwei Zahlen μ, welche der Bedingung $\mu \equiv \pm 1$ (mod. 3) oder, was dasselbe sagt, der Bedingung $\mu^2 \equiv 1$ (mod. 3)

genügen; für je zwei relative Primzahlen μ, ν, welche zugleich diese Bedingung $\mu^2 \equiv \nu^2 \equiv 1 \pmod 3$ erfüllen, gilt dann das Gesetz

$$\left(\frac{\mu}{\nu}\right) = \left(\frac{\nu}{\mu}\right);$$

falls aber die Zahlen μ, ν die genannte Bedingung nicht erfüllen, so findet zwischen den beiden vorstehenden Symbolen eine Beziehung statt, welche mit Hilfe des ersten der obigen vier Ergänzungssätze immer leicht abzuleiten ist.

Wir benutzen jetzt die vorstehenden Sätze zu einer wesentlichen Umformung unserer in § 7 erklärten Funktion $\psi(\mu)$ unter der Voraussetzung, daß μ relative Primzahl zu k ist. Hierbei müssen wir die beiden Fälle unterscheiden, wo der reine kubische Körper K von erster oder zweiter Art ist (§ 3).

Im ersten Falle ist $k = 3ab$, und da ab durch 3, aber nicht durch 9 teilbar sein kann, so bezeichnen wir mit 3^u, 3^v die höchsten in a, b aufgehenden Potenzen von 3 und setzen

$$a = 3^u \cdot a_1, \quad b = 3^v \cdot b_1,$$

wo entweder $u = v = 0$, oder $u = 1$, $v = 0$ oder $u = 0$, $v = 1$ ist, während a_1 und b_1 nicht durch 3 teilbar sind. Ist nun μ relative Primzahl zu k, und stellen wir dieselbe in der Form $\mu = \pi_1 \pi_2 \pi_3 \cdots$ als Produkt von lauter Primzahlen π dar (von denen keine in $D = -3k^2$ aufgehen kann), so folgt aus den Definitionen III und IX in § 7 zunächst

$$\psi(\mu) = \left(\frac{ab^2}{\pi_1}\right)\left(\frac{ab^2}{\pi_2}\right)\left(\frac{ab^2}{\pi_3}\right)\cdots = \left(\frac{ab^2}{\mu}\right) = \left(\frac{3}{\mu}\right)^{u+2v}\left(\frac{a_1 b_1^2}{\mu}\right);$$

wählt man nun eine Einheit σ so, daß $\sigma\mu \equiv \pm 1 \pmod 3$ wird, und bedenkt, daß auch $a_1 b_1^2 \equiv \pm 1 \pmod 3$ ist, so folgt aus dem allgemeinen Reziprozitätssatze

$$\left(\frac{a_1 b_1^2}{\mu}\right) = \left(\frac{a_1 b_1^2}{\sigma\mu}\right) = \left(\frac{\sigma\mu}{a_1 b_1^2}\right),$$

und wir erhalten das Resultat

XI. $$\psi(\mu) = \left(\frac{3}{\mu}\right)^{u+2v}\left(\frac{\sigma\mu}{a_1 b_1^2}\right),$$

$$\sigma\mu \equiv \pm 1 \pmod 3, \quad k = 3ab = 3^{1+u+v} \cdot a_1 b_1.$$

Im zweiten Falle, wo K von zweiter Art, also $k = ab \equiv \pm 1 \pmod 3$, und $a^2 \equiv b^2 \pmod 9$, also auch $ab^2 \equiv a^3 \equiv \pm 1 \pmod 9$

ist, ergibt sich aus den obigen Ergänzungssätzen (wo μ, σ, m, n bzw. durch ab^2, ± 1, 0, 0 zu ersetzen sind)

$$\left(\frac{\varrho}{ab^2}\right) = 1, \quad \left(\frac{1-\varrho}{ab^2}\right) = 1$$

und, weil jede Einheit $\sigma = \pm \varrho^r$ ist, auch

$$\left(\frac{\sigma}{ab^2}\right) = 1.$$

Ist nun μ relative Primzahl zu k, so kann man stets

$$\mu = \sigma(1-\varrho)^r \nu$$

setzen, wo σ eine Einheit, und $\nu \equiv 1 \pmod 3$, also ν relative Primzahl zu $3k$, mithin auch zu D ist; aus den vorstehenden Gleichungen ergibt sich mit Hilfe des Reziprozitätssatzes

$$\left(\frac{\mu}{ab^2}\right) = \left(\frac{\sigma}{ab^2}\right)\left(\frac{1-\varrho}{ab^2}\right)^r \left(\frac{\nu}{ab^2}\right) = \left(\frac{\nu}{ab^2}\right) = \left(\frac{ab^2}{\nu}\right).$$

Gehen wir jetzt zur Bestimmung von $\psi(\mu)$ über, so folgt aus der obigen Darstellung von μ mit Rücksicht auf V, VII, II in § 7 zunächst $\psi(\mu) = \psi(\nu)$; stellt man ferner die Zahl ν als Produkt $\pi_1 \pi_2 \pi_3 \cdots$ von lauter Primzahlen dar, von denen keine in D aufgehen kann, so folgt aus III und IX in § 7

$$\psi(\nu) = \left(\frac{ab^2}{\pi_1}\right)\left(\frac{ab^2}{\pi_2}\right)\left(\frac{ab^2}{\pi_3}\right)\cdots = \left(\frac{ab^2}{\nu}\right),$$

und wir erhalten daher das einfache Resultat

XII. $$\psi(\mu) = \left(\frac{\mu}{ab^2}\right), \text{ wenn } k = ab.$$

Aus diesen Darstellungen XI und XII der Funktion $\psi(\mu)$ ergeben sich die folgenden wichtigen Sätze.

XIII. Die Funktion $\psi(\mu)$ hat für alle Zahlen μ, welche derselben Zahlklasse in bezug auf den Modul k angehören, einen und denselben Wert.

Dies leuchtet für den zweiten Fall unmittelbar aus XII ein, weil k durch jede in ab^2 aufgehende Primzahl π teilbar ist, mithin aus $\mu_1 \equiv \mu \pmod k$ auch

$$\left(\frac{\mu_1}{ab^2}\right) = \left(\frac{\mu}{ab^2}\right),$$

also $\psi(\mu_1) = \psi(\mu)$ folgt. Dasselbe ergibt sich für den ersten Fall auf folgende Weise aus XI. Da $k = 3ab$ ist, so folgt aus $\mu_1 \equiv \mu \pmod{k}$ auch $\mu_1 \equiv \mu \pmod{3}$; ist daher die Einheit σ so gewählt, daß $\sigma\mu \equiv \pm 1 \pmod{3}$ wird, so ist auch $\sigma\mu_1 \equiv \pm 1 \pmod{3}$, also

$$\psi(\mu_1) = \left(\frac{3}{\mu_1}\right)^{u+2v}\left(\frac{\sigma\mu_1}{a_1 b_1^2}\right);$$

da nun $\sigma\mu_1 \equiv \sigma\mu \pmod{k}$, und k durch jede in $a_1 b_1^2$ aufgehende Primzahl π teilbar ist, so folgt

$$\left(\frac{\sigma\mu_1}{a_1 b_1^2}\right) = \left(\frac{\sigma\mu}{a_1 b_1^2}\right)$$

und hieraus, falls $u + 2v = 0$ ist, $\psi(\mu_1) = \psi(\mu)$; wenn aber $u + 2v > 0$, also k durch 9 teilbar ist, so ist auch $\mu_1 \equiv \mu \pmod{9}$, also

$$\left(\frac{3}{\mu_1}\right) = \left(\frac{3}{\mu}\right),$$

mithin ist auch in diesem Falle $\psi(\mu_1) = \psi(\mu)$, w. z. b. w.

XIV. Ist $\mu \equiv r \pmod{k}$, wo r eine rationale relative Primzahl zu k bedeutet, so ist $\psi(\mu) = 1$.

Bedeutet μ' wie früher die mit μ konjugierte Zahl, so folgt aus unserer Annahme auch $\mu' \equiv r$, also*) $\mu \equiv \mu' \pmod{k}$, mithin zufolge XIII auch $\psi(\mu) = \psi(\mu')$; da ferner nach X in § 7 stets $\psi(\mu') = \psi(\mu)^2$ ist, so folgt $\psi(\mu) = 1$, w. z. b. w.

XV. Ist p eine in k aufgehende natürliche Primzahl, und $k = pq$, so gibt es immer eine relative Primzahl μ zu k, welche den beiden Bedingungen

$$\mu \equiv 1 \pmod{q}, \qquad \psi(\mu) = \varrho$$

genügt.

Bei dem Beweise haben wir eine Reihe von Fällen zu unterscheiden, und wir wollen zunächst den Fall $p = 3$ betrachten, welcher nur dann eintreten kann, wenn der kubische Körper K von erster Art ist; wir haben für den Beweis also die Darstellung XI der Funktion ψ zu benutzen und dabei zu berücksichtigen, daß $q = ab = 3^{u+v} \cdot a_1 b_1$ ist; sodann müssen wir die drei Fälle trennen, welche die beiden dort mit u, v bezeichneten Zahlen darbieten können.

---

*) Aus $\mu \equiv \mu' \pmod{k}$ folgt umgekehrt, daß μ einer rationalen Zahl kongruent ist (mod. k).

Ist erstens $u = v = 0$, also $a_1 = a$, $b_1 = b$, so ist $ab \equiv \pm 1$ (mod. 3), aber es kann nicht $ab^2 \equiv \pm 1$ (mod. 9) sein, weil hieraus $a^2 b^4 \equiv 1$, also auch $a^2 \equiv b^2$ (mod. 9) folgen würde, was unmöglich ist, weil der Körper K von erster, nicht von zweiter Art ist. Man kann daher

$$ab^2 \equiv \pm 4^m \pmod 9$$

setzen, wo m nicht durch 3 teilbar ist, und nach dem ersten Ergänzungssatze ist zugleich

$$\left(\frac{\varrho}{ab^2}\right) = \varrho^{2m}.$$

Da nun $q = ab$ relative Primzahl zu 3 ist, so gibt es bekanntlich immer Zahlen μ, welche den beiden Kongruenzen

$$\mu \equiv 1 \pmod q, \qquad \mu \equiv \varrho^m \pmod 3$$

genügen, und jede solche Zahl μ ist offenbar relative Primzahl zu $k = 3q$. Zufolge der ersten dieser beiden Kongruenzen ist die erste, im Satze an die Zahl μ gestellte Forderung erfüllt, und da $q = ab$ durch jede in ab^2 aufgehende Primzahl π teilbar ist, so folgt zugleich

$$\left(\frac{\mu}{ab^2}\right) = \left(\frac{1}{ab^2}\right) = 1.$$

Aus der zweiten der vorstehenden Kongruenzen folgt ferner, daß die Einheit $\sigma = \varrho^{2m}$ die in XI geforderte Bedingung $\sigma\mu \equiv 1$ (mod. 3) erfüllt, mithin wird

$$\psi(\mu) = \left(\frac{\sigma\mu}{ab^2}\right) = \left(\frac{\sigma}{ab^2}\right)\left(\frac{\mu}{ab^2}\right) = \left(\frac{\varrho^{2m}}{ab^2}\right) = \varrho^{4m^2} = \varrho,$$

d. h. die Zahl μ genügt auch der zweiten, im Satze an sie gestellten Forderung, w. z. b. w.

Ist zweitens $u = 1$, $v = 0$, also $a = 3a_1$, $b = b_1$, $k = 9a_1 b$, $q = 3a_1 b$, so gibt es, weil $a_1 b$ relative Primzahl zu 9 ist, Zahlen μ, welche den beiden Kongruenzen

$$\mu \equiv 1 \pmod{a_1 b}, \qquad \mu \equiv (4 - 3\varrho)^2 \pmod 9$$

genügen, und jede solche Zahl μ ist relative Primzahl zu k. Aus der zweiten Kongruenz folgt $\mu \equiv 1$ (mod. 3), und hieraus in Verbindung mit der ersten Kongruenz auch $\mu \equiv 1$ (mod. q), also ist die erste, im Satze an μ gestellte Forderung erfüllt. Zugleich er-

gibt sich, daß die in XI auftretende Einheit $\sigma = 1$ gewählt werden kann, und es wird folglich

$$\psi(\mu) = \left(\frac{3}{\mu}\right)\left(\frac{\mu}{a_1 b^2}\right).$$

Da jede in $a_1 b^2$ aufgehende Primzahl π auch in dem Modul $a_1 b$ der ersten Kongruenz aufgeht, so ist

$$\left(\frac{\mu}{a_1 b^2}\right) = \left(\frac{1}{a_1 b^2}\right) = 1,$$

und da aus der zweiten Kongruenz in Verbindung mit dem vierten Ergänzungssatze (wo $n = 2$ zu setzen ist)

$$\left(\frac{3}{\mu}\right) = \varrho^4 = \varrho$$

folgt, so wird auch $\psi(\mu) = \varrho$, wie gefordert war.

Ist drittens $u = 0$, $v = 1$, also $a = a_1$, $b = 3b_1$, $k = 9ab_1$, $q = 3ab_1$, so werden die Forderungen des Satzes erfüllt, wenn man μ durch die beiden Kongruenzen

$$\mu \equiv 1 \pmod{ab_1}, \qquad \mu \equiv 4 - 3\varrho \pmod{9}$$

bestimmt. Den Beweis, welcher auf dieselbe Weise wie im vorigen Falle zu führen ist, dürfen wir dem Leser überlassen.

Nachdem hiermit der Fall $p = 3$ erledigt ist, nehmen wir jetzt an, es sei p verschieden von 3. Um die hierbei auftretenden Unterfälle so viel wie möglich zusammenzufassen, setzen wir $e = 1$ oder $= 2$, je nachdem p in a oder in b aufgeht; dann ist p^e die höchste in ab^2 aufgehende Potenz von p. Da p im Körper Q entweder eine Primzahl oder ein Produkt von zwei verschiedenen Primzahlen ist, so kann es in Q keine Zahl geben, deren dritte Potenz mit p assoziiert wäre, und hieraus folgt nach einer früheren Bemerkung (S. 178) die Existenz einer relativen Primzahl ω zu p, welche der Bedingung

$$\left(\frac{\omega}{p}\right) = \varrho$$

genügt. Mag nun der kubische Körper K von erster oder zweiter Art, mag also k durch 3 teilbar sein oder nicht, immer sind die beiden Faktoren p, q der Zahl $k = pq$ relative Primzahlen, mithin gibt es immer Zahlen μ, welche den beiden Kongruenzen

$$\mu \equiv 1 \pmod{q}, \qquad \mu \equiv \omega^e \pmod{p}$$

genügen, und jede solche Zahl μ ist relative Primzahl zu k. Durch die erste Kongruenz ist die erste, im Satze an μ gestellte Forderung erfüllt, wir haben daher nur noch zu zeigen, daß $\psi(\mu) = \varrho$ ist, und hierzu müssen wir die beiden Hauptfälle voneinander trennen.

Ist $k = 3ab$, so haben wir die Darstellung XI zu Grunde zu legen. Da q durch 3, im Falle $u + 2v > 0$ sogar durch 9 teilbar ist, so folgt aus der ersten Kongruenz und aus dem vierten Ergänzungssatz zunächst

$$\left(\frac{3}{\mu}\right)^{u+2v} = 1,$$

und da außerdem die Einheit $\sigma = 1$ der Bedingung $\sigma\mu \equiv 1 \pmod 3$ genügt, so wird

$$\psi(\mu) = \left(\frac{\mu}{a_1 b_1^2}\right) = \left(\frac{\mu}{c}\right)\left(\frac{\mu}{p}\right)^e,$$

wo $a_1 b_1^2 = c p^e$ gesetzt, also c nicht durch p teilbar ist. Jede in c aufgehende Primzahl π geht daher auch in q auf, und da $\mu \equiv 1 \pmod q$ ist, so folgt

$$\left(\frac{\mu}{c}\right) = \left(\frac{1}{c}\right) = 1.$$

Aus der zweiten, bisher nicht benutzten Kongruenz $\mu \equiv \omega^e \pmod p$ folgt ferner

$$\left(\frac{\mu}{p}\right) = \left(\frac{\omega^e}{p}\right) = \left(\frac{\omega}{p}\right)^e = \varrho^e, \quad \left(\frac{\mu}{p}\right)^e = \varrho,$$

mithin ist auch $\psi(\mu) = \varrho$, w. z. b. w.

Ist aber $k = ab$, so haben wir die Darstellung XII anzuwenden. Setzen wir jetzt $ab^2 = cp^e$, so ist c nicht teilbar durch p, und es wird wie in dem vorigen Fall

$$\psi(\mu) = \left(\frac{\mu}{a b^2}\right) = \left(\frac{\mu}{c}\right)\left(\frac{\mu}{p}\right)^e = \left(\frac{1}{c}\right)\left(\frac{\omega}{p}\right)^{e^2} = \varrho.$$

Der hiermit vollständig bewiesene Satz läßt sich allgemeiner in folgender Weise aussprechen.

XVI. Ist $k = mn$, wo m, n natürliche Zahlen bedeuten, deren erstere $m < k$ ist, so gibt es relative Primzahlen μ zu k, welche den Bedingungen

$$\mu \equiv 1 \pmod m, \qquad \psi(\mu) = \varrho$$

genügen.

Da nämlich $n > 1$ ist, so gibt es mindestens eine in n, also auch in k aufgehende natürliche Primzahl p, und wenn man $k = pq$ setzt, so ist q teilbar durch m; nach dem vorigen Satze gibt es aber Zahlen μ, welche den Bedingungen $\mu \equiv 1 \pmod{q}$, $\psi(\mu) = \varrho$ genügen, und da aus der ersteren auch $\mu \equiv 1 \pmod{m}$ folgt, so ist unser Satz bewiesen.

§ 9.

Die Funktion ψ als Gruppencharakter.

Mit Hilfe der im vorstehenden bewiesenen Eigenschaften der Funktion ψ wird es gelingen, die am Schlusse von § 7 betrachtete Summe H so umzuformen, daß die Bestimmung der Anzahl h der Idealklassen im Körper K auf die Theorie der komplexen Multiplikation der elliptischen Funktionen zurückgeführt wird. Hierbei werde ich öfter ein Symbol benutzen, welches mir seit Jahren bei meinen Studien in der Gruppen- und Körpertheorie nützliche Dienste geleistet hat. Sind $\mathfrak{A}$, $\mathfrak{B}$ Komplexe von Elementen einer Gruppe $\mathfrak{R}$ (in welcher die Gruppenoperation wie eine Multiplikation bezeichnet wird), so soll das Zeichen $\mathfrak{A}\mathfrak{B}$ den Inbegriff aller verschiedenen Elemente bedeuten, welche in der Form $\alpha\beta$ darstellbar sind, wo α jedes Element von $\mathfrak{A}$, ebenso β jedes Element von $\mathfrak{B}$ durchläuft. Sind $\mathfrak{A}$, $\mathfrak{B}$ selbst Gruppen, also Teiler von $\mathfrak{R}$ (was durch $\mathfrak{A}\mathfrak{A} = \mathfrak{A}$, $\mathfrak{B}\mathfrak{B} = \mathfrak{B}$ ausgedrückt wird), so soll das Symbol $(\mathfrak{A}, \mathfrak{B})$ die Anzahl der voneinander verschiedenen Komplexe $\mathfrak{A}\beta$ bedeuten, welche allen Elementen β der Gruppe $\mathfrak{B}$ entsprechen, und aus welchen der Komplex $\mathfrak{A}\mathfrak{B}$ besteht*). Dann ist immer $(\mathfrak{A}, \mathfrak{B}) = (\mathfrak{D}, \mathfrak{B})$, wo $\mathfrak{D}$ den größten gemeinsamen Teiler der beiden Gruppen $\mathfrak{A}$, $\mathfrak{B}$ bedeutet. Wenn ferner der Komplex $\mathfrak{A}\mathfrak{B}$ selbst eine Gruppe ist (was durch $\mathfrak{A}\mathfrak{B} = \mathfrak{B}\mathfrak{A}$ ausgedrückt wird und immer dann eintritt, wenn $\mathfrak{R}$ eine Abelsche Gruppe ist), so ist zugleich $(\mathfrak{A}, \mathfrak{B}) = (\mathfrak{A}, \mathfrak{A}\mathfrak{B})$. Endlich erwähne ich noch den Satz $(\mathfrak{E}, \mathfrak{G}) = (\mathfrak{E}, \mathfrak{F})(\mathfrak{F}, \mathfrak{G})$, welcher immer gilt, wenn die Gruppe $\mathfrak{E}$ ein Teiler der Gruppe $\mathfrak{F}$, und diese ein Teiler der Gruppe $\mathfrak{G}$ ist.

---

*) Ist $\mathfrak{R}$ die Gruppe aller Permutationen eines Normalkörpers C, und sind A, B die zu den Gruppen $\mathfrak{A}$, $\mathfrak{B}$ gehörigen Körper (so daß z. B. A der Inbegriff aller derjenigen Zahlen in C ist, welche durch jede Permutation der Gruppe $\mathfrak{A}$ in sich selbst übergehen), so ist das Gruppensymbol $(\mathfrak{A}, \mathfrak{B})$ identisch mit dem Symbol (A, B), welches ich in der Körpertheorie gebrauche (D. § 164, S. 471).

Nachdem dies vorausgeschickt ist, beschäftigen wir uns mit der Abelschen Gruppe $\mathfrak{R}$, deren Elemente diejenigen $\varphi'(k)$ Zahlklassen (mod. k) sind, in welche die sämtlichen, im Körper Q enthaltenen, relativen Primzahlen zu k zerfallen. Bezeichnen wir mit o wieder den Inbegriff aller ganzen Zahlen ω, während μ eine bestimmte relative Primzahl zu k bedeutet, so wollen wir die aus allen Zahlen von der Form $\mu + \omega k$ bestehende Zahlklasse kurz die Klasse μ nennen, wobei der Repräsentant μ durch jede andere Zahl derselben Klasse ersetzt werden darf. Die Gruppenoperation besteht in der Multiplikation dieser Klassen: multipliziert man jede Zahl der Klasse μ_1 mit jeder Zahl der Klasse μ_2, so sind alle Produkte in derselben Klasse $\mu_1\mu_2$ enthalten, welche deshalb auch das Produkt jener beiden Klassen μ_1 und μ_2 heißen mag. Die Klasse 1 ist das Hauptelement unserer Gruppe $\mathfrak{R}$ und bildet für sich allein eine Gruppe; mit Benutzung des oben erklärten Symbols wird daher $(1, \mathfrak{R}) = \varphi'(k)$. Um diese Zahl (den Grad der Gruppe $\mathfrak{R}$) zu bestimmen, haben wir den in § 7 angegebenen Satz anzuwenden; da k rational, also $N(k) = k^2$ ist, so erhalten wir

$$\varphi'(k) = k^2 \Pi\left(1 - \frac{1}{N(\pi)}\right),$$

wo π alle wesentlich verschiedenen, in k aufgehenden Primzahlen π des Körpers Q durchläuft. Bedeutet nun p jede in k aufgehende natürliche Primzahl, und bezeichnet man zur Abkürzung mit p_0 diejenige der drei Zahlen $0, \pm 1$, welche der Bedingung $p_0 \equiv p \pmod 3$ genügt*), so liefern die in p aufgehenden Primzahlen π zu dem vorstehenden Produkte den Beitrag

$$\left(1 - \frac{1}{p}\right)\left(1 - \frac{p_0}{p}\right),$$

und folglich wird

$$\varphi'(k) = \varphi(k)\varphi''(k),$$

wo

$$\varphi(k) = k\Pi\left(1 - \frac{1}{p}\right), \qquad \varphi''(k) = k\Pi\left(1 - \frac{p_0}{p}\right)$$

gesetzt ist.

Hier bedeutet $\varphi(k)$ wie üblich die Anzahl derjenigen nach k inkongruenten rationalen Zahlen, welche relative Primzahlen zu k

*) Offenbar ist p_0 identisch mit dem hier zu vermeidenden Symbol $\left(\frac{p}{3}\right)$ von Legendre und mit meinem Symbol $(-3, p)$ (D. S. 637, 655).

sind, also die Anzahl derjenigen Zahlklassen unserer Gruppe $\mathfrak{K}$, in welchen sich auch rationale Zahlen r befinden; dieselben bilden offenbar für sich eine Gruppe, einen Teiler von $\mathfrak{K}$, den wir mit $\mathfrak{R}$ bezeichnen wollen, und die Bedeutung der obigen Zerlegung von $\varphi'(k)$ kann durch

$$(1, \mathfrak{R}) = \varphi(k), \quad (\mathfrak{R}, \mathfrak{K}) = \varphi''(k)$$

ausgedrückt werden, weil $(1, \mathfrak{K}) = (1, \mathfrak{R})(\mathfrak{R}, \mathfrak{K})$ ist. Wir wollen schon jetzt bemerken, daß für alle hier in Betracht kommenden Zahlen k, die nach § 4 aus den Invarianten a, b des kubischen Körpers K abzuleiten sind, $\varphi''(k)$ durch 9 teilbar ist. Da nämlich $k = 3ab$ oder $= ab$ ist, je nachdem K von erster oder zweiter Art ist, und da ab durch kein Primzahlquadrat p^2 teilbar ist, so wird $k = c\Pi p$, wo $c = 3$ oder $= 1$ ist, je nachdem ab durch 3 teilbar ist oder nicht, mithin

$$\varphi''(k) = c\Pi(p - p_0).$$

Da nun jeder Faktor $(p - p_0)$ durch 3 teilbar ist, so leuchtet unsere Behauptung für alle die Fälle ein, wo k durch mindestens zwei verschiedene Primzahlen p teilbar ist. Wenn aber k nur durch eine einzige Primzahl p teilbar, also $\varphi''(k) = c(p - p_0)$ ist, so sind zwei Fälle zu unterscheiden. Ist K von erster Art, also $k = 3ab$, so ist $p = 3$, $p_0 = 0$, und da $ab > 1$ ist, so muß $ab = 3$, $k = 9$, $c = 3$, also $\varphi''(k) = 3 \cdot 3 = 9$ sein. Ist aber K von zweiter Art, also $a^2 \equiv b^2 \pmod 9$, so ist $k = ab = p$ verschieden von 3, also $p_0^2 = 1$, $c = 1$, und der Symmetrie halber dürfen wir annehmen, es sei $a = p$, $b = 1$; hieraus folgt $a^2 - b^2 = (p - p_0)(p + p_0) \equiv 0 \pmod 9$, und da von den beiden Faktoren $(p - p_0)$, $(p + p_0)$ nur der erste durch 3 teilbar ist, so folgt $\varphi''(k) = p - p_0 \equiv 0 \pmod 9$. Nachdem hiermit unsere Behauptung für alle Fälle erwiesen ist, wollen wir, wo es bequem erscheint,

$$\varphi''(k) = 9k''$$

setzen; die Werte der hierdurch erklärten natürlichen Zahl k'' sind für die ersten 21 Körper K in der vorletzten Spalte der Tabelle am Schlusse von § 2 angegeben.

Wir kehren nun zur Betrachtung der Funktion $\psi(\mu)$ zurück, wo μ jede in Q enthaltene relative Primzahl zu k bedeutet. Da $\psi(\mu)$ nach Satz XIII in § 8 für alle Zahlen μ, welche derselben Klasse (mod. k) angehören, einen und denselben Wert hat, so können wir

die Funktion ψ von den Zahlen μ auf die Klassen μ übertragen, welche die Elemente der Gruppe $\mathfrak{K}$ bilden, und da (nach V in § 7) für je zwei solche Klassen μ_1, μ_2 und deren Produkt $\mu_1\mu_2$ das Gesetz $\psi(\mu_1\mu_2) = \psi(\mu_1)\psi(\mu_2)$ gilt, so ist ψ ein Charakter der Gruppe $\mathfrak{K}$ (D. § 184, S. 612). Außerdem wissen wir (vgl. den Schluß von § 7), daß $\psi(\mu)$ immer eine Potenz von ϱ ist, also keine anderen Werte als 1, ϱ, ϱ^2 annehmen kann; zufolge VII in § 7 ist nun gewiß $\psi(1) = 1$, und da aus dem Satze XV oder XVI in § 8 (weil immer $k > 1$ ist) beiläufig folgt, daß es eine Zahl τ gibt, für welche $\psi(\tau) = \varrho$, also auch $\psi(\tau^2) = \varrho^2$ wird, so nimmt $\psi(\mu)$ wirklich alle drei Werte 1, ϱ, ϱ^2 an. Bezeichnen wir nun mit μ_0 alle diejenigen Klassen, welche der Bedingung $\psi(\mu_0) = 1$ genügen, so folgt aus dem Multiplikationsgesetz des Charakters ψ, daß diese Klassen eine Gruppe*) bilden, welche wir im folgenden stets mit ψ_0 bezeichnen wollen. Behält ferner τ die eben festgesetzte Bedeutung, so leuchtet ein, daß alle in dem Komplex $\psi_0\tau$ enthaltenen Klassen $\mu_1 = \mu_0\tau$ der Bedingung $\psi(\mu_1) = \varrho$ genügen; umgekehrt, wenn μ_1 der Repräsentant einer solchen Klasse ist, für welche $\psi(\mu_1) = \varrho$ wird, so kann man immer, weil τ relative Primzahl zu k ist, eine Zahl μ so bestimmen, daß $\mu\tau \equiv \mu_1 \pmod{k}$ wird, und da hieraus $\psi(\mu_1) = \psi(\mu\tau) = \psi(\mu)\psi(\tau)$, also $\psi(\mu) = 1$ folgt, so ist die Klasse μ in der Gruppe ψ_0 der Klassen μ_0 enthalten, mithin ist der Komplex $\psi_0\tau$ der Inbegriff aller verschiedenen Klassen μ_1, welche der Bedingung $\psi(\mu_1) = \varrho$ genügen. Genau ebenso ergibt sich, daß der Komplex $\psi_0\tau^2$ der Inbegriff aller verschiedenen Klassen μ_2 ist, für welche $\psi(\mu_2) = \varrho^2$ wird, und da jeder der drei Komplexe ψ_0, $\psi_0\tau$, $\psi_0\tau^2$ aus gleich vielen verschiedenen Klassen besteht, so ist

$$(1, \psi_0) = \tfrac{1}{3}\varphi'(k) = 3k''\varphi(k), \qquad (\psi_0, \mathfrak{K}) = 3,$$

weil jede Klasse der Gruppe $\mathfrak{K}$ einem und nur einem dieser drei Komplexe angehören muß**).

---

*) Vertauscht man die beiden Invarianten a, b des Körpers K miteinander, wodurch die Funktion ψ in ihr Quadrat übergeht (§ 7, Anm. auf S. 173), so bleibt diese Gruppe ψ_0 ungeändert, d. h. sie ist ebenfalls eine Invariante des Körpers K.

**) Ist ψ ein beliebiger Charakter einer beliebigen Abelschen Gruppe $\mathfrak{K}$, bedeutet ferner ψ_0 die Gruppe aller derjenigen Elemente von $\mathfrak{K}$, für welche $\psi = 1$ wird, und setzt man $(\psi_0, \mathfrak{K}) = n$, so ist n zugleich die Anzahl aller verschiedenen Werte von ψ, und diese Werte ψ sind die sämtlichen Wurzeln der Gleichung $\psi^n = 1$; zugleich ist $\mathfrak{K} = \psi_0\mathfrak{P}$, wo $\mathfrak{P}$ eine Periode, d. h. eine Gruppe bedeutet, welche aus den Potenzen eines einzigen Elementes τ besteht. Umgekehrt,

Nach dem Satze XIV in § 8 ist nun gewiß $\psi(\mu) = 1$, wenn μ einer rationalen Zahl r kongruent ist (mod. k), d. h. wenn μ einer der $\varphi(k)$ Zahlklassen der oben mit $\mathfrak{R}$ bezeichneten Gruppe angehört; mithin ist $\mathfrak{R}$ ein Teiler der Gruppe ψ_0, und für alle $\varphi(k)$ Klassen eines Komplexes $\mathfrak{R}\nu$ hat der Charakter ψ denselben Wert $\psi(\nu)$. Dies wollen wir jetzt auf die am Schlusse von § 7 betrachtete Summe

$$6H = \sum \frac{\psi(\mu)}{N(\mu)^s}$$

anwenden, wo μ alle relativen Primzahlen zu k durchläuft. Da die Gesamtgruppe $\mathfrak{R}$ aller $\varphi'(k)$ Zahlklassen μ aus $\varphi''(k)$ Komplexen von der Form $\mathfrak{R}\nu$ besteht, so wollen wir zur Abkürzung

$$S(\mathfrak{R}\nu) = \sum \frac{1}{N(\mu)^s}$$

setzen, wo μ alle Zahlen der in dem Komplex $\mathfrak{R}\nu$ enthaltenen $\varphi(k)$ Klassen durchläuft; dann wird offenbar

$$6H = \Sigma \psi(\nu) S(\mathfrak{R}\nu),$$

wo die Summe Σ auf ein System von $\varphi''(k)$ geeignet gewählten Zahlen ν auszudehnen ist, der Art, daß die entsprechenden Komplexe $\mathfrak{R}\nu$ alle Zahlklassen der Gruppe $\mathfrak{R}$ erschöpfen. Die weitere Umformung des vorstehenden Ausdrucks bildet den Hauptgegenstand unserer ferneren Untersuchungen.

§ 10.

Die Wurzeln der Ordnung $[1, k\varrho]$.

Betrachtet man einen bestimmten Klassenkomplex von der Form $\mathfrak{R}\nu$, so ist die eben definierte entsprechende Summe $S(\mathfrak{R}\nu)$ über alle und nur diejenigen Zahlen μ auszudehnen, welche $\equiv r\nu$ (mod. k) sind, wo r jede rationale Zahl bedeutet, welche relative Primzahl zu k ist. Das System aller dieser Zahlen μ bildet einen Teil des Systems aller derjenigen Zahlen λ, welche $\equiv x\nu$ (mod. k) sind, wo x jede ganze rationale Zahl bedeutet; jede solche Zahl λ ist also von der

---

wenn $\mathfrak{K} = \mathfrak{H}\mathfrak{P}$ ist, wo $\mathfrak{H}$ und $\mathfrak{P}$ Gruppen bedeuten, deren letztere $\mathfrak{P}$ eine Periode ist, so gibt es, wenn $(\mathfrak{H}, \mathfrak{K}) = (\mathfrak{H}, \mathfrak{P}) = n$ gesetzt wird, genau $\varphi(n)$ verschiedene Charaktere ψ der Gruppe $\mathfrak{K}$, welche der Bedingung $\psi_0 = \mathfrak{H}$ genügen. — Ist ferner $\mathfrak{A}$ eine in $\mathfrak{K}$ enthaltene Gruppe, so ist die über alle Elemente α von $\mathfrak{A}$ ausgedehnte Summe $\Sigma\psi(\alpha)$ immer und nur dann $= 0$, wenn $\mathfrak{A}$ kein Teiler von ψ_0 ist.

Form $\omega k + xv$, wo ω alle Zahlen in $\mathfrak{o}$ (d. h. alle ganzen Zahlen des Körpers Q), und x alle Zahlen des Moduls $[1]$ durchläuft, und umgekehrt ist jede in dieser Form darstellbare Zahl $\lambda \equiv xv \pmod{k}$. Das durch k und v vollständig bestimmte System dieser Zahlen λ, welches wir kurz mit k_v bezeichnen wollen, ist offenbar ein endlicher Modul, und wenn man die in der Modultheorie übliche (auch oben in §§ 3, 4 benutzte) Bezeichnung anwendet, so wird

$$k_v = [k, k\varrho, v] = \mathfrak{o}k + [v];$$

wir wollen vorläufig diese Form eines dreigliedrigen Moduls beibehalten und erst später die Zurückführung auf einen zweigliedrigen Modul mit irreduzibler Basis betrachten. Die Theorie dieser Moduln k_v, welche ich die Wurzeln der Ordnung $k_1 = \mathfrak{o}k + [1] = [1, k\varrho]$ genannt habe, ist in Dirichlets Vorlesungen über Zahlentheorie ausführlich dargestellt (§ 181, S. 622—627 der dritten, und § 187, S. 651—657 der vierten Auflage), und ich werde mich später auf diese Darstellung berufen; für unseren nächsten Schritt ist aber diese Theorie noch entbehrlich. Offenbar sind zwei solche Moduln k_μ, k_ν stets und nur dann identisch, wenn die beiden Zahlen μ, ν (die immer als relative Primzahlen zu k vorausgesetzt werden) denselben Klassenkomplex $\mathfrak{R}\mu = \mathfrak{R}\nu$ erzeugen, und folglich ist die Anzahl $\varphi''(k)$ aller verschiedenen, in $\mathfrak{K}$ enthaltenen Komplexe $\mathfrak{R}\nu$ zugleich die Anzahl aller verschiedenen Moduln k_ν. Setzen wir nun zur Abkürzung

$$S(k_\nu) = \sum \frac{1}{N(\lambda)^s},$$

wo λ alle Zahlen des Moduls k_ν mit einziger Ausnahme der Zahl Null, und zwar jede solche Zahl nur einmal durchläuft, so enthält diese Summe alle Glieder der in § 9 mit $S(\mathfrak{R}\nu)$ bezeichneten Summe und außerdem unendlich viele andere Glieder; aber wir wollen beweisen, daß trotzdem

$$6H = \Sigma\psi(\nu)S(\mathfrak{R}\nu) = \Sigma\psi(\nu)S(k_\nu)$$

ist, wo die zweite Summe Σ auf alle $\varphi''(k)$ verschiedenen Moduln k_ν auszudehnen ist.

Um den Gang des Beweises, welcher auf dem Satze XVI in § 8 beruht, nicht zu unterbrechen, schicken wir folgende Betrachtungen über gewisse Teiler der Gruppe $\mathfrak{K}$ voraus. Ist $k = mn$, wo m, n natürliche Zahlen bedeuten, so ist jede relative Primzahl μ zu k von selbst auch relative Primzahl zu m, und wir wollen den Inbegriff

aller derjenigen von diesen Zahlen μ, welche $\equiv 1 \pmod{m}$ sind, mit $\mathfrak{N}$ bezeichnen; derselbe besteht offenbar aus einer gewissen Anzahl von Zahlklassen (mod. k), welche eine Gruppe, einen Teiler der Gruppe $\mathfrak{K}$ bilden. Umgekehrt, wenn eine gegebene Zahl ω relative Primzahl zu m ist, so folgt hieraus im allgemeinen zwar noch nicht, daß ω auch zu k relative Primzahl ist, aber man überzeugt sich leicht*), daß es immer Zahlen gibt, welche $\equiv \omega \pmod{m}$ und zugleich relative Primzahlen zu k sind, und wenn ω_1 irgendeine bestimmte solche Zahl bedeutet, so wird ihre Gesamtheit durch den in der Gruppe $\mathfrak{K}$ enthaltenen Klassenkomplex $\mathfrak{N}\omega_1$ dargestellt; wendet man daher das in § 9 erklärte Gruppensymbol an, so wird

$$(1, \mathfrak{N}) = \frac{\varphi'(k)}{\varphi'(m)}, \quad (\mathfrak{N}, \mathfrak{K}) = \varphi'(m),$$

weil zu jeder der $\varphi'(m)$ Zahlklassen $\omega \pmod{m}$ ein und nur ein Komplex $\mathfrak{N}\omega_1$ gehört, und weil $(1, \mathfrak{N})(\mathfrak{N}, \mathfrak{K}) = (1, \mathfrak{K}) = \varphi'(k)$ ist**).

Bedeutet nun $\mathfrak{N}$ wie bisher die Gruppe aller derjenigen $\varphi(k)$ Klassen in $\mathfrak{K}$, in welchen sich auch rationale Zahlen r befinden, so leuchtet ein, daß die Gruppe $\mathfrak{N}\mathfrak{N}$ aus lauter solchen Klassen besteht, deren Zahlen nach dem Modul m mit rationalen Zahlen kongruent sind; umgekehrt, wenn μ relative Primzahl zu k und zugleich $\equiv z \pmod{m}$ ist, wo z rational, so ist z gewiß relative Primzahl zu m, man kann daher eine ebenfalls rationale Zahl r, welche zugleich relative Primzahl zu k ist, so wählen, daß $r \equiv z \pmod{m}$, also auch $\mu \equiv r \pmod{m}$ wird, und hieraus folgt nach dem Obigen, daß μ in einer Klasse des Komplexes $\mathfrak{N}r$, also auch in einer Klasse der Gruppe $\mathfrak{N}\mathfrak{N}$ enthalten ist. Mithin ist diese Gruppe $\mathfrak{N}\mathfrak{N}$ der Inbegriff aller derjenigen Klassen in $\mathfrak{K}$, deren Zahlen nach dem Modul m mit rationalen Zahlen kongruent sind, und es ist auch leicht, den Grad dieser Gruppe, d. h. die Anzahl $(1, \mathfrak{N}\mathfrak{N})$ der in ihr enthaltenen Klassen zu bestimmen. Da nämlich $\varphi(m)$ die Anzahl

---

*) Die Kongruenz $\omega_1 \equiv \omega \pmod{m}$ ist (nach D. § 180, II, S. 568) vereinbar mit $\omega_1 \equiv 1 \pmod{\varkappa}$, wo $\varkappa$ das Produkt aller Primzahlen π bedeutet, die in k, aber nicht in m aufgehen.

**) Dieselben Sätze wiederholen sich in der Zahlentheorie jedes endlichen Körpers Ω bei der Vergleichung der Zahlklassen, die sich auf irgend ein Ideal $\mathfrak{k}$ beziehen, mit den Zahlklassen, die sich auf ein in $\mathfrak{k}$ aufgehendes Ideal $\mathfrak{m}$ beziehen. Ist Ω der Körper der rationalen Zahlen, so bilden die entsprechenden Sätze eine wesentliche Grundlage für die gesamte Theorie der Kreisteilung.

derjenigen nach m inkongruenten rationalen Zahlen z ist, welche relative Primzahlen zu m sind, und da jeder dieser Zahlen z ein Komplex $\mathfrak{N}r$ von $(1, \mathfrak{N})$ Klassen in $\mathfrak{N}\mathfrak{N}$ entspricht, deren Zahlen $\mu \equiv z \pmod{m}$ sind, so ist

$$(1, \mathfrak{N}\mathfrak{N}) = \varphi(m)(1, \mathfrak{N}) = \varphi(m)\frac{\varphi'(k)}{\varphi'(m)} = \frac{\varphi'(k)}{\varphi''(m)}.$$

Da ferner $(1, \mathfrak{N})(\mathfrak{N}, \mathfrak{N}\mathfrak{N}) = (1, \mathfrak{N}\mathfrak{N})$, und $(1, \mathfrak{N}) = \varphi(k)$ ist, so ergibt sich zugleich

$$(\mathfrak{N}, \mathfrak{N}\mathfrak{N}) = \frac{\varphi'(k)}{\varphi(k)\varphi''(m)} = \frac{\varphi''(k)}{\varphi''(m)}.$$

Zu denselben Resultaten gelangt man auch, wenn man bedenkt, daß $(\mathfrak{N}, \mathfrak{N}\mathfrak{N}) = (\mathfrak{N}, \mathfrak{N}) = (\mathfrak{D}, \mathfrak{N})$ ist, wo $\mathfrak{D}$ den größten gemeinsamen Teiler der Gruppen $\mathfrak{N}, \mathfrak{N}$ bedeutet; denn jede in $\mathfrak{D}$ enthaltene Klasse wird durch eine rationale Zahl r repräsentiert, welche relative Primzahl zu k und zugleich $\equiv 1 \pmod{m}$ ist, mithin ist ihre Anzahl

$$(1, \mathfrak{D}) = \frac{\varphi(k)}{\varphi(m)},$$

und da

$$(1, \mathfrak{D})(\mathfrak{D}, \mathfrak{N}) = (1, \mathfrak{N}) = \frac{\varphi'(k)}{\varphi'(m)}$$

sein muß, so ergibt sich für $(\mathfrak{D}, \mathfrak{N})$, also für $(\mathfrak{N}, \mathfrak{N}\mathfrak{N})$ wieder der obige Ausdruck.

Aus der eben festgestellten Bedeutung der Gruppe $\mathfrak{N}\mathfrak{N}$ ziehen wir endlich noch folgenden Schluß. Ist ω wieder eine gegebene relative Primzahl zu m, und bedeutet ω_1 wie oben eine bestimmte relative Primzahl zu k, welche $\equiv \omega \pmod{m}$ ist, so war $\mathfrak{N}\omega_1$ der Komplex aller der Klassen in $\mathfrak{N}$, deren Zahlen ebenfalls $\equiv \omega \pmod{m}$ sind; ebenso leuchtet jetzt ein, daß $\mathfrak{N}\mathfrak{N}\omega_1$ der Komplex aller der Klassen in $\mathfrak{N}$ ist, deren Zahlen $\equiv z\omega \pmod{m}$ sind, wo z alle rationalen relativen Primzahlen zu m durchläuft.

Nach diesen Vorbereitungen wenden wir uns zum Beweise des oben ausgesprochenen Satzes über die Umformung der Summe $6H$. Wir heben zunächst die charakteristische Eigenschaft aller in den Moduln k_ν enthaltenen Zahlen λ hervor, welche darin besteht, daß der größte gemeinsame Teiler von k und λ immer eine natürliche Zahl ist. Da nämlich $\lambda \equiv x\nu \pmod{k}$, und x rational, ferner ν relative Primzahl zu k ist, so ist der rationale (positiv genommene) größte gemeinsame Teiler n der beiden rationalen Zahlen k, x

auch derjenige von k und xv, also (nach D. § 180, S. 566) auch derjenige von k und λ; setzt man daher $k = mn$, so wird $\lambda = \omega n$, wo ω relative Primzahl zu m ist.

Umgekehrt, wenn eine solche Zahl $\lambda = \omega n$ gegeben ist, so suchen wir alle Moduln k_ν, in denen λ enthalten ist. Die erforderliche und hinreichende Bedingung dafür, daß λ in k_ν enthalten sei, besteht in der Existenz einer rationalen Zahl x, welche der Kongruenz $xv \equiv \lambda = \omega n \pmod{k}$ genügt, und da $k = mn$, und v relative Primzahl zu k ist, so muß zunächst x durch n teilbar, also $x = ny$ sein; hieraus folgt $yv \equiv \omega \pmod{m}$, und weil ω relative Primzahl zu m ist, so gilt dasselbe auch von der rationalen Zahl y; es gibt daher rationale Zahlen z, welche der Kongruenz $yz \equiv 1 \pmod{m}$ genügen, und hieraus folgt $v \equiv z\omega \pmod{m}$; zufolge der obigen Bemerkung muß daher v einer Klasse des Komplexes $\mathfrak{N}\mathfrak{N}\omega_1$ angehören, wo ω_1 wieder eine relative Primzahl zu k bedeutet, welche $\equiv \omega \pmod{m}$ ist, und umgekehrt leuchtet ein, daß dann die Zahl λ wirklich in dem Modul k_v enthalten ist, weil aus $v \equiv z\omega \pmod{m}$ rückwärts $yv \equiv \omega \pmod{m}$, $xv \equiv \omega n = \lambda \pmod{k}$ folgt, wo $yz \equiv 1 \pmod{m}$ und $x = ny$ ist. Mithin ist der Komplex $\mathfrak{N}\mathfrak{N}\omega_1$ der Inbegriff aller derjenigen Zahlklassen v, welche die Eigenschaft haben, daß die gegebene Zahl $\lambda = \omega n$ in dem Modul k_v enthalten ist*), und die Anzahl dieser verschiedenen Moduln k_v, d. h. die Anzahl der in dem Komplexe $\mathfrak{N}\mathfrak{N}\omega_1$ enthaltenen verschiedenen Komplexe $\mathfrak{N}v$, ist $= (\mathfrak{N}, \mathfrak{N}\mathfrak{N}) = \varphi''(k) : \varphi''(m)$. Wir haben nun zwei wesentlich verschiedene Fälle zu betrachten.

Ist die gegebene Zahl λ selbst relative Primzahl zu k, so ist $n = 1$, $m = k$, $\mathfrak{N} = 1$; die Zahl λ tritt daher nur in einem einzigen Modul $k_v = k_\lambda$ auf und erzeugt nur ein einziges, mit dem Koeffizienten $\psi(\lambda)$ behaftetes Glied $N(\lambda)^{-s}$, und dieses Glied findet sich ebenso in der ersten wie in der zweiten Summe, deren Identität wir zu beweisen haben.

Ist aber λ nicht relative Primzahl zu k, ist also $n > 1$, $m < k$, so liefert λ gar keinen Beitrag zu der ersten Summe; da aber die Zahl λ in $(\mathfrak{N}, \mathfrak{N}\mathfrak{N})$ verschiedenen Moduln k_v enthalten ist, so liefert

*) Dasselbe ergibt sich auch aus dem leicht zu beweisenden Satze $\mathfrak{o}n - k_\nu = nm_\nu$, wo $\mathfrak{o}n - k_\nu$ das kleinste gemeinsame Vielfache der beiden Moduln $\mathfrak{o}n$, k_ν und $m_\nu = \mathfrak{o}m + [\nu] = k_\nu m_1$ ist.

sie zu der zweiten Summe ebensoviele Beiträge $\psi(\nu)N(\lambda)^{-s}$; um daher auch für diesen Fall die Identität der beiden Summen und hiermit unseren Satz zu beweisen, brauchen wir nur noch zu zeigen, daß die über alle diese Moduln k_ν erstreckte Summe $\sum\psi(\nu) = 0$ ist. Hierzu berufen wir uns auf den Satz XVI in § 8, den wir nach unserer jetzigen Bezeichnung offenbar so aussprechen können, daß es in der Gruppe $\mathfrak{N}$ eine Zahlklasse μ gibt, für welche $\psi(\mu) = \varrho$, also nicht $= 1$ wird. Die Gruppe $\mathfrak{N}$ ist daher kein Teiler*) der in § 9 definierten Gruppe ψ_0, und folglich ist der größte gemeinsame Teiler $\mathfrak{E}$ dieser beiden Gruppen ein echter Teiler von $\mathfrak{N}$, d. h. $\mathfrak{E}$ ist verschieden von $\mathfrak{N}$, mithin $(\mathfrak{E}, \mathfrak{N}) = (\psi_0, \mathfrak{N}) = (\psi_0, \psi_0\mathfrak{N}) > 1$, und da $(\psi_0, \psi_0\mathfrak{N})(\psi_0\mathfrak{N}, \mathfrak{K}) = (\psi_0, \mathfrak{K}) = 3$ sein muß, so folgt $(\mathfrak{E}, \mathfrak{N}) = 3$ (und $(\psi_0\mathfrak{N}, \mathfrak{K}) = 1$, also $\psi_0\mathfrak{N} = \mathfrak{K}$). Mithin besteht die Gruppe $\mathfrak{N}$ aus den drei verschiedenen Komplexen $\mathfrak{E}$, $\mathfrak{E}\mu$, $\mathfrak{E}\mu^2$, und für die in ihnen enthaltenen Klassen nimmt der Charakter ψ bzw. die Werte 1, ϱ, ϱ^2 an, während $\psi(\mu^3) = \psi(\mu)^3 = 1$, also $\mathfrak{E}\mu^3 = \mathfrak{E}$ ist. Bedenkt man ferner, daß die Gruppe $\mathfrak{N}$ (nach § 9) ein Teiler der Gruppe ψ_0, also die Gruppe $\mathfrak{N}\mathfrak{E}$ ein gemeinsamer Teiler der beiden Gruppen ψ_0, $\mathfrak{N}\mathfrak{N}$ ist**), so ergibt sich ebenso, daß die Gruppe $\mathfrak{N}\mathfrak{N}$ aus den drei verschiedenen Komplexen $\mathfrak{N}\mathfrak{E}$, $\mathfrak{N}\mathfrak{E}\mu$, $\mathfrak{N}\mathfrak{E}\mu^2$ und folglich der Komplex $\mathfrak{N}\mathfrak{N}\omega_1$ aus den drei verschiedenen Komplexen $\mathfrak{N}\mathfrak{E}\omega_1$, $\mathfrak{N}\mathfrak{E}\mu\omega_1$, $\mathfrak{N}\mathfrak{E}\mu^2\omega_1$ besteht. Zerlegt man nun die Gruppe $\mathfrak{N}\mathfrak{E}$ in lauter verschiedene Komplexe von der Form $\mathfrak{N}\varepsilon$ (deren Anzahl offenbar $= \varphi''(k) : 3\varphi''(m)$ ist), so ist hiermit auch der Komplex $\mathfrak{N}\mathfrak{N}\omega_1$ in lauter verschiedene Komplexe $\mathfrak{N}\nu$ zerlegt, und zwar hat ν alle Klassen $\varepsilon\omega_1$, $\varepsilon\mu\omega_1$, $\varepsilon\mu^2\omega_1$ zu durchlaufen, welche den verschiedenen Klassen ε entsprechen. Hiermit sind zugleich alle Moduln k_ν gefunden, in denen die Zahl λ enthalten ist; vereinigt man nun immer die drei Klassen ν, welche derselben Klasse ε entsprechen, und be-

*) Vgl. den Schluß der zweiten Anmerkung zu § 9 auf S. 189, worin das Wesen des obigen Beweises enthalten ist.

**) Offenbar ist $\mathfrak{N}\mathfrak{E}$ der größte gemeinsame Teiler von ψ_0, $\mathfrak{N}\mathfrak{N}$, und dieser Satz gilt allgemein für irgendwelche Teiler ψ_0, $\mathfrak{N}, \mathfrak{N}$ einer beliebigen Abelschen Gruppe $\mathfrak{K}$, wenn $\mathfrak{N}$ Teiler von ψ_0 und $\mathfrak{E}$ der größte gemeinsame Teiler von $\psi_0, \mathfrak{N}$ ist. Bedient man sich einer kürzlich von mir vorgeschlagenen Ausdrucksweise (§ 4 des Aufsatzes „Über Zerlegungen von Zahlen durch ihre größten gemeinsamen Teiler“ in der Festschrift zur Braunschweiger Naturforscher-Versammlung 1897), so ist diese Eigenschaft so auszusprechen, daß die sämtlichen Teiler einer beliebigen Abelschen Gruppe immer eine Dualgruppe vom Modultypus bilden.

denkt man, daß $\psi(\varepsilon\omega_1) = \psi(\omega_1)$, $\psi(\varepsilon\mu\omega_1) = \varrho\,\psi(\omega_1)$, $\psi(\varepsilon\mu^2\omega_1) = \varrho^2\psi(\omega_1)$ und folglich die Summe dieser drei Werte $= 0$ ist, so ergibt sich, daß auch die über alle Klassen ν erstreckte Summe $\Sigma\,\psi(\nu) = 0$ ist, und hiermit ist unser obiger Satz vollständig bewiesen.

§ 11.

Binäre quadratische Formen.

Die sämtlichen $\varphi''(k)$ verschiedenen Moduln $k_\nu = \mathfrak{o}k + [\nu]$ sind (nach D. § 187, S. 651—657) dadurch vollständig charakterisiert, daß sie die Ordnung $k_1 = [1, k\varrho]$ haben und der Bedingung $\mathfrak{o}k_\nu = \mathfrak{o}$ genügen, und da $k_\mu k_\nu = k_{\mu\nu}$ ist, so bilden sie hinsichtlich ihrer Multiplikation eine Abelsche Gruppe. Da ferner unsere Funktion ψ für alle diejenigen in einem solchen Modul k_ν enthaltenen Zahlen, welche relative Primzahlen zu k sind, denselben Wert besitzt, so kann man sie von den Zahlen oder Zahlklassen ν auf die Moduln k_ν eindeutig übertragen, indem man $\psi(k_\nu) = \psi(\nu)$ setzt; aus der Eigenschaft $\psi(\mu\nu) = \psi(\mu)\psi(\nu)$ folgt dann $\psi(k_\mu k_\nu) = \psi(k_{\mu\nu}) = \psi(\mu\nu) = \psi(k_\mu)\psi(k_\nu)$, mithin ist ψ jetzt auch ein Charakter der eben genannten Gruppe aller Moduln k_ν. Zugleich wird

$$6H = \Sigma\,\psi(k_\nu)\,S(k_\nu),$$

wo die Summe Σ über alle $\varphi''(k)$ Moduln k_ν auszudehnen ist, und hier ist

$$S(k_\nu) = \sum \frac{1}{N(\lambda)^s},$$

wo λ alle Zahlen des Moduls k_ν (mit Ausnahme der Null) zu durchlaufen hat.

Bezeichnet man nun die Moduln k_ν mit $\mathfrak{k}_0, \mathfrak{k}_1, \mathfrak{k}_2$, je nachdem $\psi(k_\nu) = \psi(\nu) = 1, \varrho, \varrho^2$ ist, so nimmt der obige Ausdruck die Form

$$6H = \Sigma S(\mathfrak{k}_0) + \varrho\,\Sigma S(\mathfrak{k}_1) + \varrho^2\,\Sigma S(\mathfrak{k}_2)$$

an, wo die erste, zweite, dritte Summe bzw. über alle Moduln $\mathfrak{k}_0, \mathfrak{k}_1, \mathfrak{k}_2$ auszudehnen ist. Die Moduln $\mathfrak{k}_0$ bilden für sich eine Gruppe, welche offenbar der Gruppe ψ_0 in § 9 entspricht, und wenn man wieder $\varphi''(k) = 9k''$ setzt (wie in § 9), so ist ihre Anzahl $= 3k''$, und ebenso groß ist die der Moduln $\mathfrak{k}_1$ wie die der Moduln $\mathfrak{k}_2$.

Da zwischen den in §§ 6, 7 erklärten Funktionen J, G, H der Variablen s die Relation $J = GH$ besteht, und da J und G durchaus

reell sind, so gilt dasselbe auch für H; hieraus folgt, daß in dem vorstehenden Ausdruck $\Sigma S(\mathfrak{k}_1) = \Sigma S(\mathfrak{k}_2)$ und folglich

$$6H = \Sigma S(\mathfrak{k}_0) - \Sigma S(\mathfrak{k}_1)$$

sein muß. Dasselbe bestätigt sich leicht auf folgende Weise. Ist ν relative Primzahl zu der rationalen Zahl k, so gilt dasselbe von der mit ν konjugierten Zahl ν', und die beiden Moduln $k_\nu = \mathfrak{o}k + [\nu]$, $k_{\nu'} = \mathfrak{o}k + [\nu']$ sind ebenfalls miteinander konjugiert, d. h. jede Zahl λ des Moduls k_ν ist konjugiert mit einer Zahl λ' des Moduls $k_{\nu'}$, und umgekehrt. Da nun $N(\lambda) = N(\lambda')$, so ist auch $S(k_\nu) = S(k_{\nu'})$; da ferner $\psi(\nu') = \psi(\nu)^2$ ist (nach § 7, X), so wird, je nachdem k_ν ein Modul $\mathfrak{k}_0, \mathfrak{k}_1, \mathfrak{k}_2$ ist, $k_{\nu'}$ ein Modul $\mathfrak{k}_0, \mathfrak{k}_2, \mathfrak{k}_1$ sein*); die Moduln $\mathfrak{k}_2$ sind daher die sämtlichen mit den Moduln $\mathfrak{k}_1$ konjugierten Moduln, und folglich ist $\Sigma S(\mathfrak{k}_1) = \Sigma S(\mathfrak{k}_2)$, w. z. b. w.

Eine zweite Vereinfachung ergibt sich aus der Betrachtung der äquivalenten Moduln k_ν. Die sämtlichen mit der Ordnung k_1 äquivalenten Moduln k_μ sind (nach D. S. 655) von der Form σk_1, wo σ alle Einheiten ± 1, $\pm\varrho$, $\pm\varrho^2$ durchläuft, und da jeder Modul durch Multiplikation mit (-1) in sich selbst übergeht, so sind nur die drei Moduln

$$k_1 = \mathfrak{o}k + [1], \quad \varrho k_1 = \mathfrak{o}k + [\varrho] = k_\varrho, \quad \varrho^2 k_1 = \mathfrak{o}k + [\varrho^2] = k_{\varrho^2}$$

zu betrachten; diese drei äquivalenten Moduln sind aber wirklich voneinander verschieden, weil $k > 1$ ist, und weil folglich die drei Klassenkomplexe $\mathfrak{R}$, $\mathfrak{R}\varrho$, $\mathfrak{R}\varrho^2$ verschieden sind. Bezeichnet man mit $\mathfrak{S}$ die Gruppe der durch die sechs Einheiten σ repräsentierten Klassen (welche alle verschieden sind, weil $k > 2$ ist), so haben $\mathfrak{R}$ und $\mathfrak{S}$ die beiden Klassen ± 1 gemein, und die Gruppe $\mathfrak{R}\mathfrak{S}$ besteht aus den drei Komplexen $\mathfrak{R}$, $\mathfrak{R}\varrho$, $\mathfrak{R}\varrho^2$; zugleich ist $(\mathfrak{R}\mathfrak{S}, \mathfrak{R}) = 3k''$, und man erkennt leicht, daß jedem Komplex $\mathfrak{R}\mathfrak{S}\nu$ ein Tripel von drei verschiedenen Moduln

$$k_\nu, \quad k_{\nu\varrho} = \varrho k_\nu, \quad k_{\nu\varrho^2} = \varrho^2 k_\nu$$

entspricht, welche miteinander, aber mit keinem anderen Modul äquivalent sind. Da nun, wenn λ alle Zahlen in k_ν durchläuft, $\varrho\lambda$ alle Zahlen in ϱk_ν und $\varrho^2\lambda$ alle Zahlen in $\varrho^2 k_\nu$ durchläuft, so folgt

*) Dasselbe ergibt sich auch aus dem Satze $k_\nu k_{\nu'} = k_{\nu\nu'} = k_1$, welcher daraus folgt, daß die Zahl $\nu\nu'$ rational ist, also einer Klasse der Gruppe $\mathfrak{R}$ angehört (vgl. D. S. 645, 653).

$S(k_\nu) = S(k_{\nu\varrho}) = S(k_{\nu\varrho^2})$, weil $N(\lambda) = N(\varrho\lambda) = N(\varrho^2\lambda)$ ist; da außerdem $\psi(\sigma) = 1$, also $\psi(k_\nu) = \psi(k_{\nu\varrho}) = \psi(k_{\nu\varrho^2})$ ist, so gehören je drei solche äquivalente Moduln entweder alle zu den Moduln $\mathfrak{k}_0$, oder alle zu den Moduln $\mathfrak{k}_1$, oder alle zu den Moduln $\mathfrak{k}_2$. Behält man daher von je drei Moduln $k_\nu, k_{\nu\varrho}, k_{\nu\varrho^2}$ immer nur einen bei, so geht unsere obige Gleichung in

$$2H = \Sigma' S(\mathfrak{k}_0) - \Sigma' S(\mathfrak{k}_1)$$

über, wo die Summationen Σ' auf alle nicht äquivalenten Moduln $\mathfrak{k}_0$, $\mathfrak{k}_1$ auszudehnen sind; jede dieser beiden Summen besteht daher aus k'' Gliedern.

Die Anzahl aller nicht äquivalenten Ordnungswurzeln k_ν ist daher $= 3k''$, und ebenso groß ist (nach D. S. 656) die Anzahl aller derjenigen nicht äquivalenten endlichen Moduln $\mathfrak{m}$ des Körpers Q, deren Ordnung $\mathfrak{m}^0 = k_1 = [1, k\varrho]$ ist. Dies beruht wesentlich darauf, daß alle Ideale (und Idealbrüche) des Körpers Q (d. h. alle Moduln von der Ordnung $\mathfrak{o}$) nur eine einzige Klasse bilden, also äquivalent sind, oder daß, was dasselbe sagt, je zwei Zahlen η, θ des Körpers Q stets (und zwar auf sechs verschiedene Arten) in die Form $\eta = \alpha\delta$, $\theta = \beta\delta$ gesetzt werden können, wo α, β ganze relative Primzahlen bedeuten*); ist nun $\mathfrak{m}$ irgendein endlicher Modul von der Ordnung $\mathfrak{m}^0 = k_1$, so enthält er gewiß zwei voneinander unabhängige Zahlen und ist folglich (nach D. § 172, VI) ein zweigliedriger Modul $\mathfrak{m} = [\eta, \theta] = \delta[\alpha, \beta] = \delta\mathfrak{k}$; der mit $\mathfrak{m}$ äquivalente Modul $\mathfrak{k} = [\alpha, \beta]$ hat (nach D. § 181, S. 579 oder § 187, S. 655) dieselbe Ordnung $\mathfrak{k}^0 = \mathfrak{m}^0 = k_1$, und da zugleich $\mathfrak{o}\mathfrak{k} = \mathfrak{o}\alpha + \mathfrak{o}\beta = \mathfrak{o}$ ist, so ist $\mathfrak{k}$ eine der Wurzeln k_ν der Ordnung k_1, w. z. b. w.

Um nun die dem Modul k_ν entsprechende Summe $S(k_\nu) = \Sigma N(\lambda)^{-s}$ zu bilden, wo λ alle Zahlen in k_ν (mit Ausnahme der Null) durchläuft, ist es zweckmäßig, die dreigliedrige Basis des Moduls

$$k_\nu = \mathfrak{o}k + [\nu] = [k, k\varrho, \nu]$$

durch eine irreduzible, also aus zwei Zahlen α, β bestehende Basis zu ersetzen, was bekanntlich auf unendlich viele Arten geschehen kann (D. § 172, S. 517—523). Wir bemerken zuvor, daß k_ν ein Teiler von $\mathfrak{o}k$ ist und, weil ν relative Primzahl zu k ist, aus k Zahl-

*) Daß α, β hier und im folgenden eine ganz andere Bedeutung haben wie in §§ 2—5, kann wohl keine Störung verursachen.

klassen (mod. k) besteht, deren Repräsentanten die Zahlen $0, \nu, 2\nu \cdots (k-1)\nu$ sind; nach der Bezeichnung der Modultheorie ist daher

$$(k_\nu, \mathfrak{o}k) = k,$$

und da $\mathfrak{o}$ ein Teiler von k_ν, also $(\mathfrak{o}, k_\nu)(k_\nu, \mathfrak{o}k) = (\mathfrak{o}, \mathfrak{o}k) = N(k) = k^2$ ist, so folgt auch

$$(\mathfrak{o}, k_\nu) = k.$$

Setzt man nun

$$k_\nu = [\alpha, \beta],$$

so folgt aus $\mathfrak{o}k_\nu = \mathfrak{o}$, daß α, β relative Primzahlen sind, und wenn man

$$\alpha = a_1 + a_2\varrho, \qquad \beta = b_1 + b_2\varrho$$

setzt, wo a_1, a_2, b_1, b_2 ganze rationale Zahlen bedeuten, so ist (nach D. § 172, VII, S. 523) die Determinante $a_1b_2 - b_1a_2 = \pm(\mathfrak{o}, k_\nu) = \pm k$. Da nun der Modul k_ν durch Vertauschung der beiden Basiszahlen α, β nicht geändert wird, so dürfen und wollen wir festsetzen, daß immer

$$a_1b_2 - b_1a_2 = +k$$

sein soll, und demgemäß soll α die erste, β die zweite Basiszahl von k_ν heißen; zufolge dieser Bezeichnung wird gleichzeitig

$$k_\nu = [\alpha, \beta] = [-\alpha, -\beta] = [\beta, -\alpha] = [-\beta, \alpha],$$

und die allgemeinste Darstellung ist

$$k_\nu = [\alpha_1, \beta_1], \qquad \alpha_1 = a\alpha + c\beta, \qquad \beta_1 = b\alpha + d\beta,$$

wo a, b, c, d vier ganze rationale Zahlen bedeuten, die der Bedingung

$$ad - bc = +1$$

genügen*). Führt man die mit α, β konjugierten Zahlen α', β' ein, so ist der mit k_ν konjugierte Modul

$$k_{\nu'} = [\alpha', -\beta'].$$

Benutzt man ferner die bekannte Bezeichnung für die Zusammensetzung der Substitutionen (D. § 55, S. 134), so wird

$$\begin{pmatrix} \alpha, & \beta \\ \alpha', & \beta' \end{pmatrix} = \begin{pmatrix} 1, & \varrho \\ 1, & \varrho^2 \end{pmatrix} \begin{pmatrix} a_1, & b_1 \\ a_2, & b_2 \end{pmatrix},$$

und wenn man die Determinanten nimmt, so drückt sich die obige Unterscheidung zwischen der ersten und zweiten Basiszahl durch die Gleichung

$$\alpha\beta' - \beta\alpha' = k(\varrho^2 - \varrho) = -k(1 + 2\varrho) = -k\sqrt{-3}$$

*) Die Zahlen a, b sind natürlich nicht zu verwechseln mit den Invarianten des kubischen Körpers K in §§ 2—9.

aus, welche zugleich lehrt, wie aus α, β rückwärts die Zahl k, also auch die Ordnung $k_1 = [1, k\varrho]$ des Moduls $[\alpha, \beta]$ zu bestimmen ist.

Zufolge dieser letzten Bemerkung gilt auch die folgende Umkehrung: wenn zwei relative Primzahlen α, β der vorstehenden Bedingung $\alpha\beta' - \beta\alpha' = k(\varrho^2 - \varrho)$ genügen, so ist der Modul $\mathfrak{k} = [\alpha, \beta]$ gewiß eine Wurzel der Ordnung $k_1 = [1, k\varrho]$. Da nämlich $\alpha\beta' - \beta\alpha'$ nicht verschwindet, so folgt zunächst, daß die Basis α, β irreduzibel ist, mithin besitzt $\mathfrak{k}$ (nach D. S. 642) eine Ordnung $\mathfrak{k}^0$ von der Form $[1, m\varrho]$, wo m eine natürliche Zahl ist; da ferner α, β relative Primzahlen sind, so folgt $o\mathfrak{k} = o$, mithin ist $\mathfrak{k}$ (nach D. S. 651—652) eine Wurzel der Ordnung $\mathfrak{k}^0$, und hieraus folgt nach der obigen Untersuchung, daß $\alpha\beta' - \beta\alpha' = m(\varrho^2 - \varrho)$, also $m = k$, $\mathfrak{k}^0 = [1, k\varrho]$, mithin $\mathfrak{k}$ einer der Moduln k_ν ist, w. z. b. w.

Hat man nun eine bestimmte Basis α, β des Moduls k_ν gewählt, so ist jede in k_ν enthaltene Zahl λ stets und nur auf eine einzige Weise in der Form

$$\lambda = \alpha x + \beta y$$

darstellbar, wo x als erste und y als zweite Variable unabhängig voneinander alle ganzen rationalen Zahlen durchlaufen; zugleich wird

$$N(\lambda) = \lambda\lambda' = (\alpha x + \beta y)(\alpha' x + \beta' y) = A x^2 + B x y + C y^2,$$

wo zur Abkürzung

$$A = \alpha\alpha', \quad B = \alpha\beta' + \beta\alpha', \quad C = \beta\beta'$$

gesetzt ist, und dem Modul k_ν entspricht die Summe

$$S(k_\nu) = \sum \frac{1}{(A x^2 + B x y + C y^2)^s},$$

welche über alle Paare x, y mit Ausnahme des Paares 0, 0 auszudehnen ist.

Offenbar sind A, C positive und, wie auch B, ganze rationale Zahlen, und da α relative Primzahl zu β, also auch α' relative Primzahl zu β' ist, so können A, B, C keinen gemeinsamen Teiler haben; denn wenn π eine in A und C aufgehende Primzahl des Körpers Q bedeutet, so sind von den vier Zahlen α, β', α', β entweder nur die beiden ersten oder nur die beiden letzten durch π teilbar, und in beiden Fällen kann π nicht in B aufgehen. Da ferner

$$B^2 - 4AC = (\alpha\beta' - \beta\alpha')^2 = -3k^2 = D$$

ist, so entspricht jeder Basis α, β des Moduls k_ν eine bestimmte positive, ursprüngliche, binäre quadratische Form $(A, \frac{1}{2}B, C)$, deren Diskriminante*) die Grundzahl D des kubischen Körpers K ist (§ 4). Ersetzt man aber α, β durch die oben angegebene allgemeinste Basis α_1, β_1, und bezeichnet man mit x_1, y_1 die zugehörigen Variablen, welche wieder alle ganzen rationalen Zahlen durchlaufen, so folgt aus der doppelten Darstellung

$$\lambda = \alpha x + \beta y = \alpha_1 x_1 + \beta_1 y_1,$$

daß die alten und neuen Variablen durch die Gleichungen

$$x = a x_1 + b y_1, \qquad y = c x_1 + d y_1$$

verbunden sind; mithin geht die Form $(A, \frac{1}{2}B, C)$ durch die Substitution $\begin{pmatrix} a, & b \\ c, & d \end{pmatrix}$ in diejenige Form über, welche der neuen Basis α_1, β_1 entspricht. Alle diese Formen sind daher eigentlich äquivalent (D. § 56, S. 136) und bilden die sämtlichen Individuen einer bestimmten Formenklasse $\mathfrak{F}_\nu$, welche dem Modul k_ν entspricht. Dieselbe Formenklasse entspricht aber auch den beiden anderen, mit k_ν äquivalenten Moduln

$$k_{\nu\varrho} = \varrho k_\nu = [\alpha\varrho, \beta\varrho], \qquad k_{\nu\varrho^2} = \varrho^2 k_\nu = [\alpha\varrho^2, \beta\varrho^2],$$

weil die Zahlen A, B, C offenbar ungeändert bleiben, wenn α, β bzw. durch $\alpha\varrho$, $\beta\varrho$ oder durch $\alpha\varrho^2$, $\beta\varrho^2$ ersetzt werden; es ist daher $\mathfrak{F}_\nu = \mathfrak{F}_{\nu\varrho} = \mathfrak{F}_{\nu\varrho^2}$.

Umgekehrt, wenn irgendeine positive ursprüngliche Form $(A, \frac{1}{2}B, C)$ von der Diskriminante

$$B^2 - 4AC = D = -3k^2$$

gegeben ist, so fragen wir, ob es eine Basis α, β eines Moduls $k_\nu = [\alpha, \beta]$ gibt, welcher diese Form im obigen Sinne entspricht. Um dies zu untersuchen, betrachten wir die beiden konjugierten, offenbar ganzen Zahlen

$$\Theta = \frac{B + k\sqrt{-3}}{2} = \frac{B+k}{2} + k\varrho,$$

$$\Theta' = \frac{B - k\sqrt{-3}}{2} = \frac{B-k}{2} - k\varrho,$$

welche mit A, B, C, k durch die Gleichungen

$$\Theta + \Theta' = B, \qquad \Theta\Theta' = AC, \qquad \Theta' - \Theta = -k(1 + 2\varrho)$$

*) Vgl. D. § 145. Anmerkung auf S. 388—389.

verbunden sind. Soll nun die gegebene Form der Basis α, β entsprechen, so ist erforderlich und hinreichend, daß α, β relative Primzahlen sind, welche den obigen Bedingungen $\alpha\beta' - \beta\alpha' = -k(1 + 2\varrho)$, $\alpha\alpha' = A$, $\alpha\beta' + \beta\alpha' = B$, $\beta\beta' = C$, also den Bedingungen

$$\alpha\alpha' = A, \quad \beta\alpha' = \Theta, \quad \alpha\beta' = \Theta', \quad \beta\beta' = C$$

genügen. Durch die beiden ersten und ebenso durch die beiden letzten dieser vier Bedingungen ist zunächst das Verhältnis der beiden gesuchten relativen Primzahlen α, β aus den gegebenen Zahlen A, Θ, Θ', C vollständig zu bestimmen in den beiden Formen

$$\frac{\beta}{\alpha} = \frac{\Theta}{A} = \frac{C}{\Theta'},$$

welche vermöge der Relation $AC = \Theta\Theta'$ miteinander übereinstimmen. Offenbar gibt es immer nur sechs verschiedene solche Paare von relativen Primzahlen α, β; denn die beiden gegebenen Zahlen A, Θ besitzen im Körper Q sechs verschiedene assoziierte größte gemeinsame Teiler γ, und jeder von ihnen liefert ein entsprechendes Zahlenpaar

$$\alpha = \frac{A}{\gamma}, \quad \beta = \frac{\Theta}{\gamma}.$$

Hat man nun eine bestimmte Wahl über γ, also auch über α, β getroffen, so folgt aus $C\alpha = \Theta'\beta$, daß C durch β, ebenso Θ' durch α teilbar ist; wir haben daher eine Zerlegung von der Form

$$A = \alpha\gamma, \quad \Theta = \beta\gamma, \quad \Theta' = \alpha\delta, \quad C = \beta\delta,$$

wo δ ein durch die Wahl von γ bestimmter, größter gemeinsamer Teiler von Θ', C ist. Durch den Übergang zu den konjugierten Zahlen ergibt sich hieraus die zweite Zerlegung

$$A = \alpha'\gamma', \quad \Theta = \alpha'\delta', \quad \Theta' = \beta'\gamma', \quad C = \beta'\delta',$$

mithin muß α' als gemeinsamer Teiler von A, Θ ein Teiler von γ sein, und wenn man $\gamma = \alpha'\varepsilon$ setzt, so folgt aus $A = \alpha\alpha'\varepsilon$, daß $\varepsilon = \varepsilon'$ eine natürliche Zahl ist, weil dasselbe von $\alpha\alpha'$ und von dem ersten Koeffizienten A der positiven Form $(A, \frac{1}{2}B, C)$ gilt; aus der doppelten Darstellung von Θ folgt ferner $\beta\gamma = \beta\alpha'\varepsilon = \alpha'\delta'$, also $\delta' = \beta\varepsilon$, $\delta = \beta'\varepsilon$, und die beiden obigen Zerlegungen fließen zusammen in die folgende:

$$A = \alpha\alpha'\varepsilon, \quad \Theta = \beta\alpha'\varepsilon, \quad \Theta' = \alpha\beta'\varepsilon, \quad C = \beta\beta'\varepsilon.$$

Die natürliche Zahl ε ist daher gemeinsamer Teiler von A, C, Θ, Θ', also auch von $B = \Theta + \Theta'$, und da $(A, \frac{1}{2}B, C)$ eine ursprüngliche Form ist, so folgt $\varepsilon = 1$, also

$$A = \alpha\alpha', \quad \Theta = \beta\alpha', \quad \Theta' = \alpha\beta', \quad C = \beta\beta'.$$

Jedes der auf die obige Weise aus den gegebenen Zahlen A, Θ abgeleiteten sechs Paare von relativen Primzahlen α, β ist daher wirklich eine Basis eines Moduls k_ν, der die gegebene Form $(A, \frac{1}{2}B, C)$ entspricht, und außer diesen Basen gibt es keine andere. Bezeichnet man eine bestimmte von ihnen mit α, β, so haben sie die gemeinsame Form $\alpha\sigma$, $\beta\sigma$, wo σ alle sechs Einheiten ± 1, $\pm\varrho$, $\pm\varrho^2$ durchläuft, und sie liefern immer drei verschiedene, aber äquivalente Moduln

$$k_\nu = [\alpha, \beta], \quad k_{\nu\varrho} = [\alpha\varrho, \beta\varrho], \quad k_{\nu\varrho^2} = [\alpha\varrho^2, \beta\varrho^2].$$

Das hiermit gewonnene Resultat können wir so aussprechen:

Jedem Tripel von äquivalenten Moduln k_ν, $k_{\nu\varrho}$, $k_{\nu\varrho^2}$ entspricht eine bestimmte Klasse $\mathfrak{F}_\nu$ von eigentlich äquivalenten quadratischen Formen der Diskriminante $D = -3k^2$, und umgekehrt entspricht jede solche Formenklasse immer einem, und nur einem solchen Tripel von Moduln. Die gemeinsame Anzahl der Modultripel und Formenklassen ist $= 3k''$.

Jeder Basis α, β des Moduls k_ν entspricht, wie oben bemerkt, eine Basis α', $-\beta'$ des mit k_ν konjugierten Moduls $k_{\nu'}$; ersetzt man aber α, β bzw. durch α', $-\beta'$, so gehen die drei Zahlen A, B, C bzw. in A, $-B$, C über, also entsprechen diesen Basen der Moduln k_ν, $k_{\nu'}$ die beiden entgegengesetzten Formen $(A, \frac{1}{2}B, C)$ und $(A, -\frac{1}{2}B, C)$; zugleich ist $k_{\nu'\varrho^2}$ mit $k_{\nu'\varrho}$[1]], und ebenso $k_{\nu'\varrho}$ mit $k_{\nu\varrho^2}$ konjugiert, und zwei solchen konjugierten Tripeln entsprechen zwei entgegengesetzte Formenklassen $\mathfrak{F}_\nu$ und $\mathfrak{F}_{\nu'}$.

Hinsichtlich der Auswahl der Basen α, β und der entsprechenden Formen $(A, \frac{1}{2}B, C)$ erwähnen wir zwei verschiedene Regeln, deren jede sich durch besondere Vorzüge empfiehlt. Die eine besteht darin, daß man (nach D. § 187, S. 652—655) für die erste Basiszahl α eine natürliche Zahl m wählt; setzt man dann die zweite Basiszahl

[1]) Es muß offenbar $k_{\nu'\varrho}$ heißen.]

$\beta = t + n\varrho$, so wird immer $mn = k$, und die entsprechende Form hat die Koeffizienten

$$A = m^2, \quad B = m(2t - n), \quad C = t^2 - tn + n^2;$$

diese Formen bilden einen speziellen Fall derjenigen Formen, welche Gauß in den Artikeln 254, 255 der Disquisitiones Arithmeticae betrachtet (vgl. D. §§ 150, 151). Nach der zweiten Regel wählt man die Basis immer so, daß ihr eine sogenannte reduzierte Form $(A, \frac{1}{2}B, C)$ entspricht, in welcher absolut genommen $B \leqq A \leqq C$ und welche aus der ersten Form leicht abzuleiten ist (Art. 171 der Disqu. Arithm. oder D. § 164).

Wir erinnern noch daran, daß (nach D. § 187) der Multiplikation der Moduln, welche durch $k_\mu k_\nu = k_{\mu\nu}$ ausgedrückt wird, die Komposition der Formenklassen $\mathfrak{F}_\mu \mathfrak{F}_\nu = \mathfrak{F}_{\mu\nu}$ entspricht, und knüpfen hieran die folgende Betrachtung. Da jeder Formenklasse $\mathfrak{F}_\nu$ ein und nur ein Tripel von Moduln k_ν, $k_{\nu\varrho}$, $k_{\nu\varrho^2}$ entspricht, welche denselben Charakter $\psi(\nu)$ haben, so kann man diesen Charakter eindeutig auf die Formenklasse übertragen, indem man $\psi(\mathfrak{F}_\nu) = \psi(k_\nu) = \psi(\nu)$ setzt, und da hieraus $\psi(\mathfrak{F}_\mu \mathfrak{F}_\nu) = \psi(\mathfrak{F}_\mu)\psi(\mathfrak{F}_\nu)$ folgt, so ist jetzt ψ ein Charakter der Abelschen Gruppe $\mathfrak{H}$, welche aus den $3k''$ Formenklassen $\mathfrak{F}$ besteht. Wir haben oben mit $\mathfrak{k}_0$ alle diejenigen Moduln k_ν bezeichnet, deren Charakter $\psi(k_\nu) = 1$ ist; sie bilden eine aus k'' Tripeln bestehende Gruppe, und ebenso bilden die zugehörigen k'' Formenklassen eine Gruppe $\mathfrak{G}$, welche wieder der Gruppe ψ_0 in § 9 entspricht; zugleich ist $(\mathfrak{G}, \mathfrak{H}) = 3$, und wenn man mit $\mathfrak{F}_\tau$ eine bestimmt gewählte Formenklasse bezeichnet, deren Charakter $= \varrho$ ist, so besteht die Gesamtgruppe $\mathfrak{H}$ der $3k''$ Formenklassen aus den drei Komplexen $\mathfrak{G}$, $\mathfrak{G}\mathfrak{F}_\tau = \mathfrak{G}_1$, $\mathfrak{G}\mathfrak{F}_\tau^2 = \mathfrak{G}_2$, denen bzw. die Charaktere $1, \varrho, \varrho^2$ zukommen. In welcher Beziehung steht nun diese Gruppe $\mathfrak{G}$ zu unserem kubischen Körper K? Um diese Frage zu beantworten, betrachten wir alle diejenigen in D nicht aufgehenden natürlichen Primzahlen p, welche $\equiv 1 \pmod 3$ sind, von welchen also die Grundzahl D quadratischer Rest ist. Im quadratischen Körper Q ist daher $p = \pi\pi'$, wo π, π' zwei konjugierte, wesentlich verschiedene Primzahlen bedeuten, die nicht in $3k$ aufgehen; diese Primzahlen sind bzw. in den beiden konjugierten Moduln k_π, $k_{\pi'}$ enthalten, und da $p = N(\pi) = N(\pi')$ ist, so ist p darstellbar durch

jede in den beiden entgegengesetzten Formenklassen $\mathfrak{F}_\pi$, $\mathfrak{F}_{\pi'}$ enthaltene Form $(A, \frac{1}{2}B, C)$. Da umgekehrt (nach D. § 60) jede solche Form, durch welche p darstellbar ist, mit einer Form $(p, \frac{1}{2}r, q)$ äquivalent ist, wo $r^2 = D + 4pq \equiv D \pmod{4p}$, und da die letztere Form, wie oben gezeigt ist, immer nur drei äquivalenten Moduln k, $= [\alpha, \beta]$ entspricht, wo $\alpha\alpha' = p$, also α mit π oder π' assoziiert und folglich auch relative Primzahl zu k ist, so muß $k_\nu = k_{\sigma\pi}$ oder $= k_{\sigma\pi'}$ sein, mithin gehört die Form $(p, \frac{1}{2}r, q)$ einer der beiden Formenklassen $\mathfrak{F}_\pi$, $\mathfrak{F}_{\pi'}$ an, und die natürliche Primzahl p ist daher ausschließlich darstellbar durch die Formen dieser beiden Klassen (vgl. D. §§ 86, 87). Nun gehört die Formenklasse $\mathfrak{F}_\pi$ dem Komplexe $\mathfrak{G}$, $\mathfrak{G}_1$, $\mathfrak{G}_2$, und gleichzeitig gehört die Formenklasse $\mathfrak{F}_{\pi'}$ dem Komplexe $\mathfrak{G}$, $\mathfrak{G}_2$, $\mathfrak{G}_1$ an, je nachdem $\psi(\pi) = 1, \varrho, \varrho^2$ ist; nach der Definition der Funktion ψ in § 7 tritt aber der erste dieser drei Fälle dann, und nur dann ein, wenn ab^2 kubischer Rest der natürlichen Primzahl p ist, wo a, b die Invarianten des kubischen Körpers K bedeuten. Wollen wir diesen Körper K nicht ausdrücklich erwähnen, so besteht das hiermit gewonnene Resultat in dem folgenden

Satz. Ist mindestens eine der beiden natürlichen Zahlen $a, b > 1$ und ab durch kein Quadrat einer natürlichen Primzahl teilbar, setzt man ferner $k = 3ab$ oder $= ab$, je nachdem $(a^2 - b^2)$ durch 9 unteilbar oder teilbar ist, so ist die Anzahl aller nicht äquivalenten, positiven, ursprünglichen binären quadratischen Formen $(A, \frac{1}{2}B, C)$ von der Diskriminante $B^2 - 4AC = D = -3k^2$ immer ein Vielfaches $3k''$ von 3, und ein Drittel der durch diese Formen vertretenen Formenklassen bildet eine Kompositionsgruppe $\mathfrak{G}$, welche durch die folgende Eigenschaft charakterisiert ist: Bedeutet p jede natürliche Primzahl, welche $\equiv 1 \pmod 3$ ist und nicht in D aufgeht, so sind durch die k'' Formen der Gruppe $\mathfrak{G}$ alle und nur solche Primzahlen p darstellbar, von denen ab^2, also auch a^2b kubischer Rest ist, während durch die Formen der übrigen $2k''$ Klassen alle und nur solche Primzahlen p darstellbar sind, von denen ab^2 kubischer Nichtrest ist.

Wollen wir aber die Bedeutung der quadratischen Formen für den kubischen Körper K hervorheben, so erinnern wir uns daran,

daß (nach § 5) die natürliche Primzahl p, je nachdem ab^2 kubischer Rest oder Nichtrest von p ist, im Körper K durch drei verschiedene Primideale ersten Grades teilbar oder selbst eine Primzahl dritten Grades ist, und erhalten den folgenden*)

Satz. Bedeutet D die Grundzahl eines kubischen Körpers K, so ist die Anzahl der Klassen, in welche die ursprünglichen binären quadratischen Formen von der Diskriminante D zerfallen, ein Vielfaches von 3, und ein Drittel dieser Klassen bildet eine durch folgende Eigenschaft charakterisierte Kompositionsgruppe $\mathfrak{G}$: Bedeutet p jede, in D nicht aufgehende, natürliche Primzahl, von welcher D quadratischer Rest ist, so wird p im Körper K durch drei verschiedene Primideale teilbar oder selbst eine Primzahl sein, je nachdem p durch eine Form der Gruppe $\mathfrak{G}$ darstellbar ist oder nicht.

Auf einem der Papiere aus dem Nachlasse von Gauß, welche mir — wahrscheinlich im Jahre 1860 — zur Ansicht, aber nicht zur Herausgabe mitgeteilt wurden, befand sich eine Bemerkung über kubische Reste, welche nach meiner Abschrift folgendermaßen lautet [1]):

Observatio venustissima inductione facta.

2 est Residuum vel non Residuum cubicum numeri primi p formae $3n+1$, prout p repraesentabilis est per formam

$$xx + 27yy$$
$$\text{vel } 4xx + 2xy + 7yy.$$

3 est Residuum vel non Residuum, prout p repraesentabilis est per

$$xx + 243yy \text{ aut } 4xx + 2xy + 61yy$$
$$\text{vel } 7xx + 6xy + 36yy \text{ aut } 9xx + 6xy + 28yy.$$

---

*) Die Form, in welcher ich diesen Fundamentalsatz hier ausspreche, ist so gewählt, daß sie, wie ich glaube, für alle kubischen Körper ohne Ausnahme, selbst für die Kreiskörper gilt; den allgemeinen Beweis dieses Satzes zu finden, ist mir aber bisher nicht gelungen. Dagegen bietet die Zerlegung aller anderen Primzahlen p in Primideale keine erhebliche Schwierigkeit dar.

[1]) C. F. Gauß, Werke Bd. VIII, S. 5.]

5 est Residuum		Nonresiduum
(1, 0, 675)	si	(7, 2, 97)
(25, 0, 27)	p	(9, 3, 76)
(13, 1, 52)	repraesentatur per	(19, 3, 36)
(4, 1, 169)		(25, 5, 28)
		(25, 10, 31)
		(27, 9, 28)

In diesen Sätzen muß man ohne Zweifel die frühesten Entdeckungen erblicken, die Gauß auf dem Gebiete der kubischen (und biquadratischen) Reste gemacht hat, und durch welche er bald darauf zu der Erweiterung des Begriffs der ganzen Zahl geführt ist (vgl. § 7).

Noch bevor dieses merkwürdige Fragment mir bekannt geworden war, hatte ich den ersten dieser drei Sätze bei dem Versuche gefunden, die Methode, durch welche Gauß den biquadratischen Charakter der Zahl 2 bestimmt (Theoria residuorum biquadraticorum I, Art. 15—23), auf die Theorie der kubischen Reste zu übertragen. Der Beweis, den ich am 7. Januar 1858 in einer algebraischen Vorlesung zu Göttingen vorgetragen habe, ergibt sich in der Tat sehr einfach aus Art. 358 der Disquisitiones Arithmeticae; behält man nämlich die dortige Bezeichnung bei, bedeutet also n eine natürliche Primzahl, welche $\equiv 1 \pmod 3$ ist, so zeigt Gauß, daß immer

$$4n = MM + 27NN$$

und gleichzeitig, wenn $M \equiv 1 \pmod 3$ gewählt wird,

$$9a = n + 1 + M$$

ist, wo $a - 1 = (\mathfrak{R}\mathfrak{R})$ die Anzahl derjenigen inkongruenten kubischen Reste z von n bedeutet, welche die Eigenschaft besitzen, daß auch $(z + 1)$ kubischer Rest von n ist. Setzt man nun $z + 1 \equiv z_1 \pmod n$ und bedenkt, daß die Zahl (-1) immer kubischer Rest von n ist, so folgt aus $-z_1 + 1 \equiv -z \pmod n$, daß die Zahl $(-z_1)$ dieselbe Eigenschaft wie z besitzt. Man kann daher alle diese $(a - 1)$ Zahlklassen z in eine Reihe von Paaren z und $(-z - 1)$ ordnen, und folglich wird $a - 1$ eine gerade Zahl sein, wenn nicht etwa der Fall vorkommt, daß die beiden Zahlen derselben Klasse angehören, also $2z \equiv -1 \pmod n$ ist; dies geschieht immer und nur dann, wenn die Zahl 2 selbst ein kubischer Rest von n ist, und da es in diesem Falle auch nur für eine einzige Klasse z geschieht, so ergibt sich,

daß a gerade oder ungerade ist, je nachdem die Zahl 2 kubischer Rest oder Nichtrest von n ist*). Da ferner immer $a \equiv M \equiv N \pmod 2$ ist, so folgt, daß die Primzahl n im ersten Falle und nur in diesem durch die Hauptform $(1, 0, 27) = xx + 27yy$ darstellbar ist; wenn aber 2 kubischer Nichtrest von n ist, so muß n durch die beiden anderen reduzierten Formen $(4, \pm 1, 7) = 4xx \pm 2xy + 7yy$ der Determinante -27 oder der Diskriminante -108 darstellbar sein. Hiermit ist der obige Satz vollständig bewiesen, und man überzeugt sich leicht, daß er mit unserer allgemeinen Theorie übereinstimmt, weil die Invarianten des durch die Zahl $\sqrt[3]{2}$ erzeugten kubischen Körpers K_1 die Zahlen 2 und 1 sind, woraus $k = 6$, $k'' = 1$ folgt.

Unterhalb 100 gibt es nur zwei Primzahlen n oder p, von denen die Zahl 2 kubischer Rest ist, nämlich

$$31 = 2^2 + 27 \cdot 1^2, \qquad 43 = 4^2 + 27 \cdot 1^2,$$

und wenn t eine willkürliche Zahl bedeutet, so ist

$$t^3 - 2 \equiv (t-4)(t-7)(t+11) \pmod{31},$$
$$t^3 - 2 \equiv (t+9)(t+11)(t-20) \pmod{43},$$

wie man leicht mit Hilfe des Canon Arithmeticus von Jacobi findet.

Gehen wir jetzt zu den beiden anderen Sätzen über, um sie ebenfalls mit unserer Theorie zu vergleichen, so ist es auch hier zweckmäßig, zu jeder der von Gauß angegebenen reduzierten Formen, falls sie nicht eine zweiseitige (eine forma anceps) ist, die entgegengesetzte Form hinzuzufügen. In dem zweiten Satze, der von dem kubischen Charakter der Zahl 3 handelt, ist das Formensystem der Determinante -243 außerdem noch durch die beiden oben fehlenden Formen $(13, \pm 2, 19)$ zu ergänzen, und wir wollen (wie im folgenden § 12) zur Abkürzung

$$(1, 0, 243) = (00), \quad (7, -3, 36) = (10), \quad (7, 3, 36) = (20),$$
$$(4, 1, 61) = (01), \quad (9, 3, 28) = (11), \quad (13, -2, 19) = (21),$$
$$(4, -1, 61) = (02), \quad (13, 2, 19) = (12), \quad (9, -3, 28) = (22)$$

setzen. Die Bedeutung dieser Bezeichnung ist folgende. Jede Form (yz), wo die beiden Zahlen y, z durch beliebige nach dem Modul 3 kon-

*) Aus der Bedeutung der Gaußschen Zahlen $b = (\mathfrak{R}\mathfrak{R}')$, $c = (\mathfrak{R}\mathfrak{R}'')$, welche nicht beide ungerade sein können, ergibt sich allgemeiner, daß die Zahl 2 dem Komplex $\mathfrak{R}$ oder $\mathfrak{R}'$ oder $\mathfrak{R}''$ angehört, je nachdem $a \equiv b \equiv c \equiv 0$ oder $a+1 \equiv b+1 \equiv c \equiv 0$ oder $a+1 \equiv b \equiv c+1 \equiv 0 \pmod 2$ ist.

gruente Zahlen ersetzt werden dürfen, soll auch als Zeichen für die durch sie repräsentierte Formenklasse angesehen werden; dann ist die aus den Klassen $(y_1 z_1)$ und $(y_2 z_2)$ zusammengesetzte Klasse

$$(y_1 z_1)(y_2 z_2) = (yz), \quad \text{wo} \quad y \equiv y_1 + y_2, \quad z \equiv z_1 + z_2 \pmod 3,$$

also auch

$$(yz) = (10)^y (01)^z, \qquad (10)^3 = (01)^3 = (00),$$

und der Satz von Gauß besteht darin, daß die Zahl 3 kubischer Rest oder Nichtrest der natürlichen Primzahl p ist, je nachdem p durch eine der drei Formen (00), (01), (02) darstellbar ist oder nicht. Die kleinsten durch die Formen (00), (01) darstellbaren Primzahlen sind

$$307 = 8^2 + 243 \cdot 1^2, \qquad 61 = 4 \cdot 0^2 + 2 \cdot 0 \cdot 1 + 61 \cdot 1^2,$$

und es ist

$$t^3 - 3 \equiv (t + 79)(t + 113)(t + 115) \pmod{307},$$
$$t^3 - 3 \equiv (t - 4)(t - 5)(t + 9) \pmod{61}.$$

Vergleichen wir nun diesen zweiten Satz von Gauß mit unserer Theorie, so ergibt sich folgendes. Die Invarianten des durch die Zahl $\sqrt[3]{3}$ erzeugten Körpers K_3 sind die Zahlen 3, 1, und da folglich $k = 9$, $k'' = 1$ ist, so müssen schon die drei reduzierten Formen

$$(1, \tfrac{1}{2}, 61), \qquad (7, \pm\tfrac{3}{2}, 9)$$

der Diskriminante -243 die Entscheidung über den kubischen Charakter der Zahl 3 geben; die oben mit $\mathfrak{G}$ bezeichnete Gruppe besteht allein aus der Hauptklasse $(1, \frac{1}{2}, 61)$, und die Zahl 3 ist daher kubischer Rest von allen und nur von denjenigen Primzahlen p, welche durch diese Form darstellbar sind. In der Tat ist wieder

$$307 = 7^2 + 7 \cdot 2 + 61 \cdot 2^2, \qquad 61 = 0^2 + 0 \cdot 1 + 61 \cdot 1^2,$$

und man erkennt leicht, daß der Satz von Gauß vollständig mit dem unsrigen übereinstimmt. Dies beruht auf den allgemeinen Sätzen über den Zusammenhang zwischen den Formen verschiedener Ordnung; jede Gruppe $\mathfrak{G}$ innerhalb der Gesamtgruppe $\mathfrak{H}$ aller Formen der Diskriminante D liefert eine entsprechende Gruppe $\mathfrak{G}'$ innerhalb der Gesamtgruppe $\mathfrak{H}'$ aller Formen, deren Diskriminante D' irgend ein quadratisches Vielfaches De^2 von D ist, und zwar bleibt die Anzahl $(\mathfrak{G}', \mathfrak{H}')$ invariant $= (\mathfrak{G}, \mathfrak{H})$, weil jede Formenklasse der Diskriminante D sich in gleich viele Formenklassen der Diskriminante D' zerteilt*).

*) Vgl. D. §§ 150, 151, 187 und die obige Anmerkung zu § 10 auf S. 192.

Jede solche, aus einer Gruppe $\mathfrak{G}$ abgeleitete Gruppe $\mathfrak{G}'$ ist daran kenntlich, daß sie die Gruppe aller derjenigen Formenklassen der Diskriminante D' in sich enthält, welche durch Komposition mit der Hauptklasse der Diskriminante D diese selbe Hauptklasse erzeugen. In unserem Falle ist $e = 2$, $D = -3(9)^2$, $D' = -3(18)^2$, und je drei Formenklassen $(y\,z)$ der letzteren Diskriminante liefern durch Komposition mit der Klasse $(1, \frac{1}{2}, 61)$ eine Klasse der Diskriminante D, was in leicht verständlicher Weise durch

$$\begin{aligned}
\{(00), (01), (02)\}(1, \tfrac{1}{2}, 61) &= (1, \tfrac{1}{2}, 61)\\
\{(10), (11), (12)\}(1, \tfrac{1}{2}, 61) &= (7, -\tfrac{3}{2}, 9)\\
\{(20), (21), (22)\}(1, \tfrac{1}{2}, 61) &= (7, \tfrac{3}{2}, 9)
\end{aligned}$$

oder durch

$$(y\,z)(1, \tfrac{1}{2}, 61) = (7, -\tfrac{3}{2}, 9)^y$$

bezeichnet werden kann.

Aus demselben Grunde könnte man in umgekehrter Weise den ersten Satz von Gauß so umformen, daß zur Entscheidung über den kubischen Charakter der Zahl 2 die Formen der Diskriminante $D = -3(6)^2$ durch je drei Formen der Diskriminante $D' = -3(18)^2$ ersetzt werden; in der Tat ist

$$\begin{aligned}
\{(00), (11), (22)\}(1, 0, 27) &= (1, 0, 27)\\
\{(01), (12), (20)\}(1, 0, 27) &= (4, -1, 7)\\
\{(02), (10), (21)\}(1, 0, 27) &= (4, 1, 7)
\end{aligned}$$

oder

$$(y\,z)(1, 0, 27) = (4, -1, 7)^{2y+z},$$

und die Zahl 2 ist kubischer Rest oder Nichtrest einer Primzahl p, je nachdem letztere darstellbar oder nicht darstellbar durch eine der drei Formen (00), (11), (22) ist; so z. B. werden die beiden oben genannten Primzahlen 31 und 43, von denen 2 kubischer Rest ist, durch die Form $(11) = (9, 3, 28)$ dargestellt:

$$31 = 9\cdot 1^2 + 6\cdot 1\cdot(-1) + 28\cdot(-1)^2, \quad 43 = 9\cdot 1^2 + 6\cdot 1\cdot 1 + 28\cdot 1^2.$$

Ganz ähnlich verhält es sich mit dem dritten Satz von Gauß, wo zur Entscheidung über die Zahl 5 die 18 Formen der Diskriminante $D' = -3(30)^2$ benutzt werden, während nach unserer Theorie schon die 6 Formen der Diskriminante $D = -3(15)^2$ hierzu ausreichen. Um die Komposition der ersteren 18 Formen miteinander übersichtlich darzustellen (wie bei dem zweiten Satze), wollen wir sie gemeinsam

durch $(y\,z)$ bezeichnen, wo z wieder nach dem Modul 3, aber y jetzt nach dem Modul 6 zu nehmen ist; setzen wir

$$(10) = (7,\ 2,\ 97),\quad (01) = (4,\ 1,\ 169),\quad (y\,z) = (10)^y\,(01)^z,$$

so wird

$$(60) = (03) = (00),$$

ferner

$$\begin{array}{lll}
(00) = (1,\ 0,\ 675), & (01) = (4,\ 1,\ 169), & (02) = (4,\ -1,\ 169)\\
(10) = (7,\ 2,\ 97), & (11) = (27,\ -9,\ 28), & (12) = (25,\ 5,\ 28)\\
(20) = (19,\ 3,\ 36), & (21) = (25,\ 10,\ 31), & (22) = (9,\ -3,\ 76)\\
(30) = (25,\ 0,\ 27), & (31) = (13,\ 1,\ 52), & (32) = (13,\ -1,\ 52)\\
(40) = (19,\ -3,\ 36), & (41) = (9,\ 3,\ 76), & (42) = (25,\ -10,\ 31)\\
(50) = (7,\ -2,\ 97), & (51) = (25,\ -5,\ 28), & (52) = (27,\ 9,\ 28)
\end{array}$$

und die Komposition dieser Formenklassen mit der Hauptklasse $(1, \frac{1}{2}, 169)$ kann durch

$$\begin{array}{l}
\{(00),\ (01),\ (02)\}\,(1, \frac{1}{2}, 169) = (1, \frac{1}{2}, 169)\\
\{(10),\ (11),\ (12)\}\,(1, \frac{1}{2}, 169) = (7, -\frac{5}{2}, 25)\\
\{(20),\ (21),\ (22)\}\,(1, \frac{1}{2}, 169) = (9, -\frac{3}{2}, 19)\\
\{(30),\ (31),\ (32)\}\,(1, \frac{1}{2}, 169) = (13, \frac{1}{2}, 13)\\
\{(40),\ (41),\ (42)\}\,(1, \frac{1}{2}, 169) = (9, \frac{3}{2}, 19)\\
\{(50),\ (51),\ (52)\}\,(1, \frac{1}{2}, 169) = (7, \frac{5}{2}, 25)
\end{array}$$

oder kurz durch

$$(y\,z)\,(1, \tfrac{1}{2}, 169) = (7, -\tfrac{5}{2}, 25)^y$$

dargestellt werden. Die Zahl 5 ist dann und nur dann kubischer Rest der Primzahl p, wenn p durch eine der beiden zweiseitigen Formen

$$(1, \tfrac{1}{2}, 169),\qquad (13, \tfrac{1}{2}, 13)$$

darstellbar ist; offenbar ist 13 die kleinste solche Primzahl, und sie ist darstellbar durch die Formen (31), (32); zugleich ist

$$t^3 - 5 \equiv (t+2)\,(t+5)\,(t+6) \pmod{13}.$$

Die 18 Formen $(y\,z)$ der Diskriminante $D' = -3\,(30)^2$ geben, weil je sechs von ihnen aus einer Form der Diskriminante $D = -3\,(6)^2$ entstehen, auch wieder die Entscheidung über den kubischen Charakter der Zahl 2; aus

$$(10)(1,\ 0,\ 27) = (01)(1,\ 0,\ 27) = (4,\ 1,\ 7)$$

folgt

$$(y\,z)(1,\ 0,\ 27) = (4,\ 1,\ 7)^{y+z},$$

mithin entspricht der Hauptklasse (1, 0, 27) die Gruppe der sechs Klassen (00), (12), (21), (30), (42), (51), welche die Potenzen der

Klasse (12) oder (51) sind, und die Zahl 2 ist dann und nur dann kubischer Rest der Primzahl p, wenn p durch eine Form dieser Gruppe darstellbar ist; so z. B. wird die oben angeführte Primzahl 43 durch die beiden Formen (12), (51), und ebenso die Primzahl 31 durch die beiden Formen (21), (42) dargestellt.

Wir haben an den drei Sätzen von Gauß soeben gezeigt, wie der kubische Charakter einer Zahl ab^2, der nach unserer Theorie von den Formen der Diskriminante $D = -3k^2$ abhängt, auch durch die Formen jeder Diskriminante $D' = De^2 = -3(ke)^2$ bestimmt werden kann, welche ein quadratisches Vielfaches von D ist. Aus der Definition der Funktion ψ in § 7 und aus dem Satze XVI in § 8 folgt aber auch, wie der Leser leicht finden wird, daß die Grundzahl D des kubischen Körpers K wirklich die absolut kleinste Diskriminante ist, deren Formen die fragliche Entscheidung geben, und hierin liegt eine wesentliche Vervollständigung des oben in doppelter Form ausgesprochenen allgemeinen Satzes. Noch wichtiger ist aber der Umstand, daß die in § 10 bewiesene Umformung der Funktion H nicht mehr gelten würde, wenn man statt der Moduln k_ν, denen die Formenklassen $\mathfrak{F}_\nu$ von der Diskriminante D entsprechen, solche Moduln $(ke)_\nu$ einführen wollte, denen Formen von absolut größerer Diskriminante $D' = De^2$ entsprechen; auch dies beruht auf dem Satze XVI in § 8, doch wollen wir uns hier begnügen, die Tatsache an den folgenden Beispielen nachzuweisen.

§ 12.

Beispiele.

Wir haben schon am Schlusse von § 4 hervorgehoben, daß ein (reeller) reiner kubischer Körper K durch seine Grundzahl $D = -3k^2$ im allgemeinen noch nicht vollständig bestimmt ist, daß es also verschiedene Körper K geben kann, welche demselben Werte der natürlichen Zahl k entsprechen. Zu allen diesen Körpern K gehört dann auch dasselbe System von Moduln k_ν des quadratischen Körpers Q (in § 10) und dasselbe System $\mathfrak{H}$ von binären Formen (in § 11); aber diese Körper K werden sich immer voneinander unterscheiden durch die zugehörige Funktion ψ (in § 7) und folglich durch die Gruppe $\mathfrak{G}$ (in § 11), welche aus einem Drittel der Gruppe $\mathfrak{H}$ besteht. Zufolge der Tabelle in § 2 tritt dieser Fall zuerst für den Wert $k = 18$ ein, welchem die beiden durch die Zahlen $\sqrt[3]{6}$ und $\sqrt[3]{12}$ erzeugten Körper K_4

und K_5 entsprechen, und da die Zahl 18 durch die beiden ersten in der Tabelle auftretenden Werte 6 und 9 von k teilbar ist, so wird die Untersuchung des Falles $k = 18$ zugleich die Theorie der durch die Zahlen $\sqrt[3]{2}$ und $\sqrt[3]{3}$ erzeugten Körper K_1 und K_2 umfassen, mit welchen wir uns eben schon in § 11 beschäftigt haben; die Durchführung dieses Beispiels wird daher besonders lehrreich sein.

Zunächst kommt es nach § 9 darauf an, im quadratischen Körper Q alle ganzen Zahlen μ übersichtlich darzustellen, welche relative Primzahlen zum Modul $k = 18$ sind; da 2 und 3 die einzigen in 18 aufgehenden natürlichen Primzahlen sind, so erhalten wir

$$\varphi(k) = \varphi(18) = 18\left(1 - \tfrac{1}{2}\right)\left(1 - \tfrac{1}{3}\right) = 6,$$
$$\varphi''(k) = 9k'' = \varphi''(18) = 18\left(1 - \tfrac{-1}{2}\right)\left(1 - \tfrac{0}{3}\right) = 27.$$

also $k'' = 3$, und die Anzahl der inkongruenten Zahlen μ ist

$$\varphi'(k) = \varphi(k)\varphi''(k) = \varphi'(18) = 162 = 2 \cdot 3^4.$$

Die Gruppe $\mathfrak{R}$ dieser Zahlklassen μ läßt sich durch

$$\mu \equiv 5^w \varrho^x (4 - 3\varrho)^y (1 + 9\varrho)^z \pmod{18}$$

darstellen, wo der Exponent w nach dem Modul 6, die Exponenten x, y, z aber nach dem Modul 3 zu nehmen sind, weil

$$5^6 \equiv \varrho^3 \equiv (4 - 3\varrho)^3 \equiv (1 + 9\varrho)^3 \equiv 1 \pmod{18}$$

ist. Daß diese Darstellung vollständig und wesentlich nur auf eine einzige Weise möglich ist, erkennt man leicht daraus, daß sie aus den beiden folgenden Darstellungen

$$\mu \equiv (-1)^w \varrho^x \cdot 4^w (4 - 3\varrho)^y \pmod{9},$$
$$\mu \equiv \varrho^{x+y+2z} \pmod{2}$$

zusammengesetzt ist; die erstere stimmt mit der in § 8, S. 179 angegebenen überein und dient dazu, um aus der gegebenen Zahl μ die Exponenten w (mod. 6), x (mod. 3) und y (mod. 3) zu bestimmen, während aus der letzteren Darstellung sich die Zahl z (mod. 3) ergibt; zugleich folgt aus § 8, S. 179 die Bestimmung

$$\left(\frac{3}{\mu}\right) = \varrho^{2y}.$$

Setzen wir ferner

$$\sigma = \varrho^{2x},$$

so genügt diese Einheit der Bedingung $\sigma\mu \equiv \pm 1 \pmod{3}$, und zugleich wird

$$\sigma\mu \equiv \varrho^{y+2z} \pmod{2};$$

da nun die Zahl 2 auch im Körper Q eine Primzahl und $N(2) = 4 = 3 \cdot 1 + 1$ ist, so folgt aus der Definition des kubischen Charakters in § 7 auch

$$\left(\frac{\sigma\mu}{2}\right) = \varrho^{y+2z}.$$

Endlich bemerken wir, daß aus der obigen Darstellung der Zahlen μ (mod. 18) auch die Darstellung

$$\mu' \equiv 5^w \varrho^{2x}(4 - 3\varrho)^{2y}(1 + 9\varrho)^{2z} \pmod{18}$$

der konjugierten Zahlen μ' folgt, weil $4 - 3\varrho^2 \equiv (4 - 3\varrho)^2$ und $1 + 9\varrho^2 \equiv (1 + 9\varrho)^2 \pmod{18}$ ist.

Gehen wir nun dazu über, nach den Regeln in §§ 10, 11 die 27 Moduln k_μ zu bestimmen, so ist zunächst zu bemerken, daß die Gruppe $\mathfrak{R}$ derjenigen Klassen, welche auch rationale Zahlen enthalten, aus den 6 Klassen

$$5^w \equiv 1, 5, 7, 17, 13, 11 \pmod{18},$$

und die Gruppe $\mathfrak{R}\mathfrak{S}$ (in § 11, S. 197) aus den 18 Klassen $5^w\varrho^x$ besteht. Wir werden daher alle Moduln k_μ und jeden nur einmal erhalten, wenn wir in der obigen Darstellung immer $w = 0$ setzen, während jede der Zahlen x, y, z ihre drei Werte durchlaufen muß. Da ferner diese 27 Moduln in 9 Tripel von der Form k_μ, $k_{\mu\varrho}$, $k_{\mu\varrho^2}$ zerfallen, welche je einem Komplex $\mathfrak{R}\mathfrak{S}\mu$ entsprechen, und da für unseren Zweck von je drei solchen äquivalenten Moduln nur einer erforderlich ist, so dürfen wir auch $x = 0$ setzen und erhalten die folgende, sogleich zu erläuternde Tabelle:

y	z	μ	$(18)_\mu$	9_μ	6_μ	ψ_1	ψ_2	ψ_4	ψ_5
0	0	1	$1{,}18\,\varrho$	$1{,}9\,\varrho$	$1{,}6\,\varrho$	1	1	1	1
1	0	$4 + 15\varrho$	$6{,}2 + 3\,\varrho$	$3{,}2 + 3\,\varrho$	$2{,}3\,\varrho$	ϱ	ϱ^2	1	ϱ
2	0	$7 + 3\varrho$	$6{,}1 + 3\,\varrho$	$3{,}1 + 3\,\varrho$	$2{,}1 + 3\,\varrho$	ϱ^2	ϱ	1	ϱ^2
0	1	$1 + 9\varrho$	$2{,}1 + 9\,\varrho$	$1{,}9\,\varrho$	$2{,}1 + 3\,\varrho$	ϱ^2	1	ϱ^2	ϱ
1	1	$13 + 6\varrho$	$3{,}1 + 6\,\varrho$	$3{,}2 + 3\,\varrho$	$1{,}6\,\varrho$	1	ϱ^2	ϱ^2	ϱ^2
2	1	$16 + 3\varrho$	$6{,}4 + 3\,\varrho$	$3{,}1 + 3\,\varrho$	$2{,}3\,\varrho$	ϱ	ϱ	ϱ^2	1
0	2	$10 + 9\varrho$	$2{,}9\,\varrho$	$1{,}9\,\varrho$	$2{,}3\,\varrho$	ϱ	1	ϱ	ϱ^2
1	2	$13 + 15\varrho$	$6{,}5 + 3\,\varrho$	$3{,}2 + 3\,\varrho$	$2{,}1 + 3\,\varrho$	ϱ^2	ϱ^2	ϱ	1
2	2	$7 + 12\varrho$	$3{,}2 + 6\,\varrho$	$3{,}1 + 3\,\varrho$	$1{,}6\,\varrho$	1	ϱ	ϱ	ϱ

Die Zahlen y, z der beiden ersten Spalten bestimmen in Verbindung mit $w = x = 0$ die Zahlenklasse $\mu \pmod{18}$ der dritten Spalte, und in der folgenden Spalte ist für den zugehörigen Modul $(18)_\mu = [18, 18\varrho, \mu]$ eine zweigliedrige Basis angegeben, deren erstes Glied eine natürliche Zahl ist; diese Basis ist nach bekannten Regeln (D. § 172, S. 519—520) immer leicht zu finden. Die 9 Moduln $(18)_\mu$ bilden eine Gruppe, und das Gesetz ihrer Multiplikation ergibt sich aus ihrer Darstellung

$$(18)_\mu = [6, 2 + 3\varrho]^y [2, 1 + 9\varrho]^z.$$

Die binären quadratischen Formen $(A, \frac{1}{2}B, C)$ von der Diskriminante $-3(18)^2$, welche den hier angegebenen Modulbasen entsprechen (§ 11), sind nicht reduziert, aber es hat (nach D. § 64) keine Schwierigkeit, die ihnen äquivalenten reduzierten Formen herzustellen, und diese letzteren sind mit denjenigen identisch, welche wir in § 11 bei der Besprechung des zweiten Satzes von Gauß mit (yz) bezeichnet haben. In der fünften und sechsten Spalte findet man zweigliedrige Basen für die durch die Zahl μ bestimmten Moduln

$$9_\mu = [9, 9\varrho, \mu] = (18)_\mu [1, 9\varrho] = (18)_\mu 9_1,$$
$$6_\mu = [6, 6\varrho, \mu] = (18)_\mu [1, 6\varrho] = (18)_\mu 6_1,$$

und die ihnen entsprechenden Formenklassen von den Diskriminanten $-3 \cdot 9^2$ und $-3 \cdot 6^2$ ergeben sich durch Komposition der Formen (yz) mit den Formen $(1, \frac{1}{2}, 61)$ und $(1, 0, 27)$, wie ebenfalls schon in § 11 besprochen ist.

Die vier letzten Spalten enthalten endlich die Werte der Charaktere $\psi(\mu)$ für die durch $\sqrt[3]{2}, \sqrt[3]{3}, \sqrt[3]{6}, \sqrt[3]{12}$ erzeugten reinen kubischen Körper K_1, K_2, K_4, K_5, welche den Zeilen 1, 2, 4, 5 der Tabelle in § 2 entsprechen. Da alle vier Körper von erster Art sind, so ist die Formel XI in § 8 (S. 180) anzuwenden, also

$$\psi(\mu) = \left(\frac{3}{\mu}\right)^{u+2v} \left(\frac{\sigma\mu}{a_1 b_1^2}\right),$$

wo die Einheit σ der Bedingung $\sigma\mu \equiv \pm 1 \pmod{3}$ genügen muß, und wo die Zahlen u, v, a_1, b_1 aus den Invarianten a, b des Körpers K so zu bestimmen sind, daß

$$a = 3^u \cdot a_1, \qquad b = 3^v \cdot b_1,$$

und a_1, b_1 nicht durch 3 teilbar werden. Die Einheit σ ist oben schon für jede Zahl μ bestimmt, und zugleich ist

$$\left(\frac{3}{\mu}\right) = \varrho^{2y}, \qquad \left(\frac{\sigma\mu}{2}\right) = \varrho^{y+2z};$$

hieraus ergeben sich für unsere vier Körper die folgenden Bestimmungen:

Körper K_1; $k = 6$; $k'' = 1$.

$$a = 2,\ b = 1;\quad u = 0,\ v = 0;\quad a_1 = 2,\ b_1 = 1;$$

$$\psi_1(\mu) = \left(\frac{\sigma\mu}{2}\right) = \varrho^{y+2z}.$$

Körper K_2; $k = 9$; $k'' = 1$.

$$a = 3,\ b = 1;\quad u = 1,\ v = 0;\quad a_1 = 1,\ b_1 = 1;$$

$$\psi_2(\mu) = \left(\frac{3}{\mu}\right) = \varrho^{2y}.$$

Körper K_4; $k = 18$; $k'' = 3$.

$$a = 6,\ b = 1;\quad u = 1,\ v = 0;\ a_1 = 2,\ b_1 = 1;$$

$$\psi_4(\mu) = \left(\frac{3}{\mu}\right)\left(\frac{\sigma\mu}{2}\right) = \varrho^{2z}.$$

Körper K_5; $k = 18$; $k'' = 3$.

$$a = 3,\ b = 2;\quad u = 1,\ v = 0;\quad a_1 = 1,\ b_1 = 2;$$

$$\psi_5(\mu) = \left(\frac{3}{\mu}\right)\left(\frac{\sigma\mu}{4}\right) = \left(\frac{3}{\mu}\right)\left(\frac{\sigma\mu}{2}\right)^2 = \varrho^{y+z}.$$

Nachdem hiermit die vier letzten Spalten unserer Tabelle ausgefüllt sind, ergeben sich aus diesen Werten von ψ die (nicht äquivalenten) Moduln $\mathfrak{k}_0$, $\mathfrak{k}_1$, $\mathfrak{k}_2$, für welche $\psi(\mathfrak{k}_0) = 1$, $\psi(\mathfrak{k}_1) = \varrho$, $\psi(\mathfrak{k}_2) = \varrho^2$ und deren gemeinsame Anzahl $= k''$ ist:

Körper K_1.

$$\mathfrak{k}_0 = [1,\ 6\varrho],\ \mathfrak{k}_1 = [2,\ 3\varrho],\ \mathfrak{k}_2 = [2,\ 1 + 3\varrho].$$

Körper K_2.

$$\mathfrak{k}_0 = [1,\ 9\varrho],\ \mathfrak{k}_1 = [3,\ 1 + 3\varrho],\ \mathfrak{k}_2 = [3,\ 2 + 3\varrho].$$

Körper K_4.

$$\mathfrak{k}_0 = [1,\ 18\varrho],\ [6,\ 1 + 3\varrho],\ [6,\ 2 + 3\varrho],$$
$$\mathfrak{k}_1 = [2,\ 9\varrho],\ [3,\ 2 + 6\varrho],\ [6,\ 5 + 3\varrho],$$
$$\mathfrak{k}_2 = [2,\ 1 + 9\varrho],\ [3,\ 1 + 6\varrho],\ [6,\ 4 + 3\varrho].$$

Körper K_5.

$$\mathfrak{k}_0 = [1,\ 18\varrho],\ [6,\ 4+3\varrho],\ [6,\ 5+3\varrho],$$
$$\mathfrak{k}_1 = [2,\ 1+9\varrho],\ [3,\ 2+6\varrho],\ [6,\ 2+3\varrho],$$
$$\mathfrak{k}_2 = [2,\ 9\varrho],\ [3,\ 1+6\varrho],\ [6,\ 1+3\varrho].$$

Die zu diesen 15 Moduln gehörigen reduzierten quadratischen Formen sind schon früher angegeben, und hiermit sind zugleich die beiden ersten Sätze von Gauß in § 11 durch unsere allgemeine Theorie bestätigt. Um nun für die hier betrachteten vier Körper K_1, K_2, K_4, K_5 auch die entsprechenden Funktionen H_1, H_2, H_4, H_5 zu bestimmen, welche in § 11 (S. 198) in der Form

$$2H = \Sigma' S(\mathfrak{k}_0) - \Sigma' S(\mathfrak{k}_1)$$

dargestellt sind, setzen wir zur Abkürzung

$$U = S[1,\ 18\varrho] = \Sigma(x^2 + 243\,y^2)^{-s},$$
$$U_1 = S[3,\ 1+6\varrho] = S[3,\ 2+6\varrho] = \Sigma(9\,x^2 + 6\,xy + 28\,y^2)^{-s},$$
$$U_2 = S[2,\ 9\varrho] = S[2,\ 1+9\varrho] = \Sigma(4\,x^2 + 2\,xy + 61\,y^2)^{-s},$$
$$U_4 = S[6,\ 1+3\varrho] = S[6,\ 2+3\varrho] = \Sigma(7\,x^2 + 6\,xy + 36\,y^2)^{-s},$$
$$U_5 = S[6,\ 4+3\varrho] = S[6,\ 5+3\varrho] = \Sigma(13\,x^2 + 4\,xy + 19\,y^2)^{-s},$$

ferner

$$V_1 = S[1,\ 6\varrho] = \Sigma(x^2 + 27\,y^2)^{-s},$$
$$W_1 = S[2,\ 3\varrho] = S[2,\ 1+3\varrho] = \Sigma(4\,x^2 + 2\,xy + 7\,y^2)^{-s},$$
$$V_2 = S[1,\ 9\varrho] = \Sigma(x^2 + xy + 61\,y^2)^{-s},$$
$$W_2 = S[3,\ 1+3\varrho] = S[3,\ 2+3\varrho] = \Sigma(7\,x^2 + 3\,xy + 9\,y^2)^{-s}$$

und erhalten

$$2H_1 = V_1 - W_1,\quad 2H_2 = V_2 - W_2,$$
$$2H_4 = (U + 2U_4) - (U_1 + U_2 + U_5),$$
$$2H_5 = (U + 2U_5) - (U_1 + U_2 + U_4).$$

Wir wollen jetzt, wie wir schon am Schlusse von § 11 angekündigt haben, diese Beispiele benutzen, um noch einmal auf die in § 10 bewiesene Umformung der Funktion H zurückzukommen. Wir haben dort, wenn k_ν irgendeine Wurzel der Ordnung $k_1 = [1,\ k\varrho]$ bedeutet, mit $S(k_\nu)$ die Summe der Größen $N(\lambda)^{-s}$ bezeichnet, wo λ alle (von Null verschiedenen) Zahlen des Moduls k_ν durchläuft; wir wollen jetzt unter dem Zeichen k_ν^* den Inbegriff aller derjenigen von diesen Zahlen λ verstehen, welche relative Primzahlen zu k sind, und wollen den von diesen Zahlen herrührenden Teil der Summe $S(k_\nu)$ mit $S(k_\nu^*)$

bezeichnen; offenbar ist diese letztere Summe identisch mit der am Schlusse von § 9 erklärten Summe $S(\Re\nu)$, und der in § 10 bewiesene Satz lautet

$$6H = \Sigma\psi(\nu)S(k_\nu^*) = \Sigma\psi(\nu)S(k_\nu),$$

wo k_ν alle Wurzeln der Ordnung k_1 durchläuft. Wir haben dann in § 11 die zweite Summe durch die Betrachtung der Paare von konjugierten Moduln und der Tripel von äquivalenten Moduln vereinfacht, und da dieselbe Vereinfachung offenbar auch für die erste Summe gilt, so nimmt der vorstehende Satz die folgende Form an:

$$2H = \Sigma' S(\mathfrak{k}_0^*) - \Sigma' S(\mathfrak{k}_1^*) = \Sigma' S(\mathfrak{k}_0) - \Sigma' S(\mathfrak{k}_1),$$

wo die Summationen nur auf alle nicht äquivalenten Moduln $\mathfrak{k}_0$, $\mathfrak{k}_1$ auszudehnen sind. Diese beiden Ausdrücke für $2H$ unterscheiden sich dadurch voneinander, daß in beiden Bestandteilen des ersten Ausdrucks nur solche Glieder $N(\lambda)^{-s}$ auftreten, in welchen λ, also auch $N(\lambda)$ relative Primzahl zu k ist, während in beiden Bestandteilen des zweiten Ausdrucks auch solche Glieder $N(\lambda)^{-s}$ auftreten, in welchen $N(\lambda)$ nicht relative Primzahl zu k ist, und der Satz besteht also darin, daß diese letzteren Glieder sich gegenseitig aufheben. Dies wollen wir jetzt wenigstens an unseren Beispielen bestätigen.

Es ist in § 10 schon gezeigt, daß der größte gemeinsame Teiler von k und irgend einer in k_ν enthaltenen Zahl λ immer mit einer natürlichen Zahl n assoziiert ist, und wenn man $k = mn$ setzt, so überzeugt man sich leicht, daß der Inbegriff aller der in k_ν enthaltenen Zahlen λ, welchen dieselbe Zahl n entspricht, $= n \cdot m_\nu^*$, d. h. der Inbegriff aller mit n multiplizierten Zahlen des Systems m_ν^* ist, und hieraus ergibt sich offenbar der allgemeine Satz

$$S(k_\nu) = \Sigma\frac{S(m_\nu^*)}{n^{2s}},$$

wo das Summenzeichen sich auf alle Zerlegungen $k = mn$ bezieht; multipliziert man mit k^{2s}, so erhält man

$$k^{2s}S(k_\nu) = \Sigma m^{2s}S(m_\nu^*),$$

wo m alle natürlichen Divisoren von k durchläuft, und hieraus folgt nach bekannten Regeln (D. § 138, S. 362), wie umgekehrt die Summen von der Form $S(k_\nu^*)$ sich durch Summen von der Form $S(m_\nu)$ darstellen lassen.

Um diesen Satz auf unsere Beispiele anzuwenden, betrachten wir auch die Moduln 3_ν, 2_ν, welche je ein Tripel bilden, und den Modul $1_\nu = [1, \varrho]$ und setzen

$$X = S[1, 3\varrho] = \Sigma(x^2 + xy + 7y^2)^{-s},$$
$$Y = S[1, 2\varrho] = \Sigma(x^2 + 3y^2)^{-s},$$
$$Z = S[1, \varrho] = \Sigma(x^2 + xy + y^2)^{-s}.$$

Bezeichnen wir ferner, falls $S(m_\nu) = M$ gesetzt ist, mit M^* immer die Summe $S(m_\nu^*)$, so erhalten wir die Relationen

$$Z = Z^*,\ Y = Y^* + 2^{-2s}Z^*,\ X = X^* + 3^{-2s}Z^*,$$
$$V_1 - V_1^* = W_1 - W_1^* = 3^{2s}T,$$
$$V_2 - V_2^* = W_2 - W_2^* = 3^{-2s}X,$$
$$U - U^* = 3^{-2s}V_1^* + 2^{-2s}V_2^* + T,$$
$$U_1 - U_1^* = 3^{-2s}V_1^* + 2^{-2s}W_2^* + T,$$
$$U_2 - U_2^* = 3^{-2s}W_1^* + 2^{-2s}V_2^* + T,$$
$$U_4 - U_4^* = U_5 - U_5^* = 3^{-2s}W_1^* + 2^{-2s}W_2^* + T,$$

wo zur Abkürzung

$$T = 6^{-2s}X^* + 9^{-2s}Y^* + (18)^{-2s}Z^*$$

gesetzt ist, und hieraus folgt

$$2H_1 = V_1 - W_1 = V_1^* - W_1^*,$$
$$2H_2 = V_2 - W_2 = V_2^* - W_2^*,$$
$$2H_4 = (U + 2U_4) - (U_1 + U_2 + U_5)$$
$$= (U^* + 2U_4^*) - (U_1^* + U_2^* + U_5^*),$$
$$2H_5 = (U + 2U_5) - (U_1 + U_2 + U_4)$$
$$= (U^* + 2U_5^*) - (U_1^* + U_2^* + U_4^*),$$

wodurch die in § 10 bewiesene Umformung bestätigt wird.

Bei der Besprechung des zweiten Satzes von Gauß über den kubischen Charakter der Zahl 3 haben wir bemerkt, daß derselbe vollständig mit unserer Theorie übereinstimmt, obgleich Gauß die Darstellung der Primzahlen p durch quadratische Formen von der Diskriminante $-3\cdot(18)^2$ benutzt, während schon die Darstellung durch quadratische Formen von der Diskriminante $-3\cdot 9^2$ dieselbe Entscheidung liefert; jede der letzteren Formen löst sich gewissermaßen in drei Formen der höheren Diskriminante auf. Ganz dasselbe gilt von dem ersten Satze über den kubischen Charakter der Zahl 2; jede der von Gauß (in Übereinstimmung mit unserer Theorie) betrachteten Formen der Diskriminante $-3\cdot 6^2$ könnte durch drei

entsprechende Formen der höheren Diskriminante $-3\cdot(18)^2$ ersetzt werden. Aber um so wichtiger ist es hervorzuheben, daß die Wahl der einen oder der anderen Diskriminante durchaus nicht freisteht, wenn es sich um die Herstellung der Funktion

$$2H = \Sigma' S(\mathfrak{k}_0) - \Sigma' S(\mathfrak{k}_1)$$

handelt. In der Tat, wollte man (nach § 11) die Formen von den Diskriminanten $-3\cdot 6^2$ und $-3\cdot 9^2$ durch je drei entsprechende Formen der Diskriminante $-3\cdot(18)^2$ ersetzen, so würde man für $2H_1$ und $2H_2$ die beiden Ausdrücke

$$P_1 = (U + 2U_1) - (U_2 + U_4 + U_5),$$
$$P_2 = (U + 2U_2) - (U_1 + U_4 + U_5)$$

erhalten, die aber von den oben gefundenen Ausdrücken $(V_1 - W_1)$ und $(V_2 - W_2)$ wesentlich verschieden sind. Behält man von den Gliedern $N(\lambda)^{-s}$ dieser Summen nur diejenigen bei, in denen $N(\lambda)$ relative Primzahl zu 18 ist, so erhält man die beiden entsprechenden Ausdrücke

$$P_1^* = (U^* + 2U_1^*) - (U_2^* + U_4^* + U_5^*),$$
$$P_2^* = (U^* + 2U_2^*) - (U_1^* + U_4^* + U_5^*),$$

und aus den obigen Formeln ergibt sich

$$P_1 = P_1^* + 3\cdot 3^{-2s}(V_1^* - W_1^*),$$
$$P_2 = P_2^* + 3\cdot 2^{-2s}(V_2^* - W_2^*).$$

Hieraus folgt zunächst, daß P_1, P_2 bzw. verschieden sind von P_1^*, P_2^*; ferner leuchtet aus der ersten Gleichung ein, daß P_1 auch von $2H_1$, d. h. von $(V_1^* - W_1^*)$ verschieden ist, weil sonst das Aggregat P_1^* auch solche Glieder $N(\lambda)^{-s}$ enthalten müßte, in denen $N(\lambda)$ durch 3 teilbar ist, was nicht der Fall ist; daß aber auch P_2 verschieden von $2H_2$, d. h. von $(V_2^* - W_2^*)$ ist, folgt aus der zweiten Gleichung erst dann, wenn man aus §§ 6, 7 noch die Tatsache hinzuzieht, daß H_2 von der Form $(1 - 2^{-2s})^{-1}M$ ist, wo M nur solche Glieder $N(\lambda)^{-s}$ enthält, in denen $N(\lambda)$ relative Primzahl zu 2 ist.

Um nun den Zusammenhang zwischen den Funktionen H_1, P_1, P_1^* und den zwischen H_2, P_2, P_2^* vollständig aufzuklären, wollen wir bemerken, daß außer dem obigen Satze über die Zerlegung der Summe $k^{2s}S(k_\nu)$ in Summen von der Form $m^{2s}S(m_\nu^*)$ noch eine Reihe von Relationen zwischen unseren Summen $S(m_\nu)$ besteht, die mit der Transformation der elliptischen Funktionen nahe zusammenhängen, und denen ebenso viele Relationen zwischen den Summen $S(m_\nu^*)$ entsprechen.

Für unseren Zweck genügt es, den einfachsten Fall dieses allgemeinen Satzes zu betrachten, der sich in sehr verschiedenen Einkleidungen darstellen läßt; wir wählen die folgende. Sind α, β zwei Konstanten von irrationalem Verhältnis, und ist p eine natürliche Primzahl, so bilden wir zwei Systeme von je $(p+1)$ zweigliedrigen Moduln; das erste System $\mathfrak{M}_1$ soll aus den $(p+1)$ Moduln

$$[\alpha, \beta], \quad [p\alpha, p\beta], \quad [p\alpha, p\beta], \quad \cdots [p\alpha, p\beta]$$

bestehen, welche mit Ausnahme des ersten $[\alpha, \beta]$ sämtlich mit $[p\alpha, p\beta]$ identisch sind, während das zweite System $\mathfrak{M}_2$ aus den $(p+1)$ Moduln

$$[\alpha, p\beta], \quad [p\alpha, \beta], \quad [p\alpha, \alpha+\beta], \quad \cdots [p\alpha, (p-1)\alpha+\beta]$$

bestehen soll, welche mit Ausnahme des ersten $[\alpha, p\beta]$ von der Form $[p\alpha, c\alpha+\beta]$ sind, wo c die p Zahlen $0, 1, 2 \cdots (p-1)$ durchläuft. Alle in diesen $(2p+2)$ Moduln enthaltenen Zahlen λ sind von der Form $\lambda = x\alpha + y\beta$, wo x, y ganze rationale Zahlen bedeuten, und jede solche Zahl λ tritt, wie der Leser leicht finden wird, ebensooft in den Moduln des Systems $\mathfrak{M}_1$ wie in den Moduln des Systems $\mathfrak{M}_2$ auf; sind nämlich beide Zahlen x, y durch p teilbar, so ist λ in allen $(p+1)$ Moduln des Systems $\mathfrak{M}_1$ und in allen $(p+1)$ Moduln des Systems $\mathfrak{M}_2$ enthalten; ist aber mindestens eine der beiden Zahlen x, y unteilbar durch p, so ist λ in einem einzigen Modul des Systems $\mathfrak{M}_1$ und in einem einzigen Modul des Systems $\mathfrak{M}_2$ enthalten. Man kann daher sagen, daß $\mathfrak{M}_1$ und $\mathfrak{M}_2$ denselben Gehalt von Zahlen λ besitzen, wobei zugleich die Häufigkeit des Auftretens dieser Zahlen berücksichtigt werden soll. Wir nehmen jetzt ferner an, daß das Verhältnis der Konstanten α, β nicht reell ist, und setzen wie früher $N(\lambda) = \lambda\lambda' = (x\alpha + y\beta)(x\alpha' + y\beta')$, wo λ' die mit λ konjugierte komplexe Zahl bedeutet, und

$$S[\alpha, \beta] = \Sigma N(\lambda)^{-s},$$

wo λ alle von Null verschiedenen Zahlen des Moduls $[\alpha, \beta]$ einfach durchläuft, während die Konstante $s > 1$ ist; dann folgt aus der obigen Übereinstimmung der Systeme $\mathfrak{M}_1$, $\mathfrak{M}_2$ der Satz

$$S[\alpha, \beta] + pS[p\alpha, p\beta] = S[\alpha, p\beta] + \Sigma S[p\alpha, c\alpha+\beta],$$

wo das Summenzeichen Σ sich auf die p Zahlen c bezieht; die linke Seite dieser Gleichung läßt sich offenbar auch in der Form

$$(1 + p \cdot p^{-2s}) S[\alpha, \beta]$$

darstellen, und die Beispiele $p = 2$, $p = 3$ liefern die beiden folgenden Sätze

$$(1 + 2 \cdot 2^{-2s}) S[\alpha, \beta] = S[\alpha, 2\beta] + S[2\alpha, \beta] + S[2\alpha, \alpha + \beta],$$
$$(1 + 3 \cdot 3^{-2s}) S[\alpha, \beta] = S[\alpha, 3\beta] + S[3\alpha, \beta] + S[3\alpha, \alpha + \beta] + S[3\alpha, 2\alpha + \beta].$$

Wendet man den ersten Satz auf die vier Moduln

$$[\alpha, \beta] = [1, \varrho], \quad [1, 3\varrho], \quad [1, 9\varrho], \quad [3, 1 + 3\varrho],$$

den zweiten auf die fünf Moduln

$$[\alpha, \beta] = [1, \varrho], \quad [1, 2\varrho], \quad [1, 3\varrho], \quad [1, 6\varrho], \quad [2, 3\varrho]$$

an, und berücksichtigt die Identitäten

$$[2, \varrho] = \varrho[1, 2\varrho], \quad [2, 1 + \varrho] = \varrho^2[1, 2\varrho],$$
$$[3, \varrho] = \varrho[1, 3\varrho], \quad [3, 1 + \varrho] = \varrho^2[1, 3\varrho], \quad [3, 2 + \varrho] = (2 + \varrho)[1, \varrho],$$
$$[3, 2\varrho] = \varrho[2, 1 + 3\varrho], \quad [3, 2 + 2\varrho] = \varrho^2[2, 3\varrho], \quad [3, 1 + 2\varrho] = (1 + 2\varrho)[1, 2\varrho],$$
$$[3, 3\varrho] = 3[1, \varrho], \quad [3, 6\varrho] = 3[1, 2\varrho], \quad [6, 3\varrho] = 3\varrho[1, 2\varrho],$$

so erhält man die folgenden neun Relationen

$$(1 + 2 \cdot 2^{-2s}) Z = 3Y; \quad (1 + 3 \cdot 3^{-2s} - 3^{-s}) Z = 3X,$$
$$(1 + 3 \cdot 3^{-2s} - 3^{-s}) Y = (1 + 2 \cdot 2^{-2s}) X = V_1 + 2W_1,$$
$$(1 + 3 \cdot 3^{-2s}) X - 3^{-2s} Z = V_2 + 2W_2,$$
$$(1 + 3 \cdot 3^{-2s}) V_1 - 3^{-2s} Y = U + 2U_1,$$
$$(1 + 3 \cdot 3^{-2s}) W_1 - 3^{-2s} Y = U_2 + U_4 + U_5,$$
$$(1 + 2 \cdot 2^{-2s}) V_2 = U + 2U_2,$$
$$(1 + 2 \cdot 2^{-2s}) W_2 = U_1 + U_4 + U_5,$$

von denen aber nur acht voneinander unabhängig sind.

Drückt man nun jede Summe M nach den obigen Formeln durch Summen von der Form M^* aus, so ergeben sich für die letzteren die einfacheren Relationen

$$(1 - 2^{-2s}) Z^* = 3Y^*; \quad (1 - 3^{-s}) Z^* = 3X^*,$$
$$(1 - 3^{-s}) Y^* = (1 - 2^{-2s}) X^* = V_1^* + 2W_1^*; \quad X^* = V_2^* + 2W_2^*,$$
$$V_1^* = U^* + 2U_1^*; \quad W_1^* = U_2^* + U_4^* + U_5^*,$$
$$(1 - 2^{-2s}) V_2^* = U^* + 2U_2^*; \quad (1 - 2^{-2s}) W_2^* = U_1^* + U_4^* + U_5^*.$$

Wir wollen bemerken, daß man diese letzteren Relationen auch auf einem ganz anderen Wege ableiten kann, bei welchem der leicht zu beweisende Hilfssatz zur Anwendung kommt, daß, wenn μ (ebenso wie ν) relative Primzahl zu k ist, der Inbegriff der durch μ teilbaren Zahlen in k_ν identisch mit $\mu \cdot k_{\nu\mu'}$ ist, wo μ' wieder die mit μ konjugierte

Zahl bedeutet. Ist nun p eine natürliche Primzahl und ν relative Primzahl zu pk, so kann man jede der $\varphi(k)$ Zahlklassen (mod. k), aus welchen das System k_ν^* besteht, in p^2 Zahlklassen (mod. pk) zerlegen, welche sich, wenn p in k aufgeht, in Systeme von der Form $(pk)_\mu^*$ zusammenfassen lassen, während im entgegengesetzten Falle auch noch die Zahlen in k_ν^* zu gruppieren sind, welche nicht relative Primzahlen zu p sind. Für unseren Zweck genügt es, die Resultate für die beiden Primzahlen $p = 2$, $p = 3$ anzugeben. Ist k gerade, so besteht das System k_ν^* aus den beiden Systemen

$$(2k)_\nu^*, \quad (2k)_{\nu(1+k\varrho)}^*,$$

d. h. jede in k_ν^* enthaltene Zahl findet sich in einem und nur einem dieser beiden Systeme, und umgekehrt sind alle Zahlen dieser beiden Systeme auch in k_ν^* enthalten. Ist aber k ungerade, so besteht k_ν^* aus den vier Systemen

$$2 \cdot k_\nu^*, \quad (2k)_\nu^*, \quad (2k)_{\nu(1+k\varrho)}^*, \quad (2k)_{\nu(1+k\varrho^2)}^*,$$

deren erstes der Inbegriff aller mit 2 multiplizierten Zahlen des Systems k_ν^* ist. Wenn ferner k durch 3 teilbar ist, so besteht k_ν^* aus den drei Systemen

$$(3k)_\nu^*, \quad (3k)_{\nu(1+k\varrho)}^*, \quad (3k)_{\nu(1+k\varrho^2)}^*,$$

und wenn k nicht durch 3 teilbar ist, so besteht k_ν^* aus den vier Systemen

$$(1-\varrho) \cdot k_{\nu(2+\varrho)}^*, \quad (3k)_\nu^*, \quad (3k)_{\nu(3+k\varrho)}^*, \quad (3k)_{\nu(3+k\varrho^2)}^*.$$

Der erste dieser vier Sätze kann hier nicht zur Anwendung kommen, weil 18 nicht durch 4 teilbar ist; wendet man aber den zweiten, dritten, vierten Satz bzw. auf die Beispiele

$$\begin{aligned} k_\nu &= [1, \varrho], \quad [1, 3\varrho], \quad [1, 9\varrho], \quad [3, 1+3\varrho], \\ k_\nu &= [1, 3\varrho], \quad [1, 6\varrho], \quad [2, 3\varrho], \\ k_\nu &= [1, \varrho], \quad [1, 2\varrho] \end{aligned}$$

an und bildet die entsprechenden Summen $S(k_\nu^*)$, so erhält man die obigen neun Relationen zwischen den Funktionen M^*, von denen die eine aus den übrigen folgt.

Aus den letzten vier dieser Relationen ergeben sich nun für die oben mit P_1^*, P_2^* bezeichneten Aggregate die Ausdrücke

$$P_1^* = V_1^* - W_1^*, \quad P_2^* = (1 - 2^{-2s})(V_2^* - W_2^*),$$

deren Form sich dadurch erklärt, daß jede relative Primzahl zu 6 auch relative Primzahl zu 18 ist, während die relativen Primzahlen

zu 9 nicht alle auch relative Primzahlen zu 18 sind. Berücksichtigt man noch die oben gefundenen Beziehungen zwischen P_1^*, P_2^* und P_1, P_2, so vervollständigen sich unsere früheren Ausdrücke für die beiden Funktionen $2H_1$, $2H_2$ in folgender Weise:

$$2H_1 = V_1 - W_1 = V_1^* - W_1^* = P_1^* = \frac{P_1}{1 + 3 \cdot 3^{-2s}},$$

$$2H_2 = V_2 - W_2 = V_2^* - W_2^* = \frac{P_2^*}{1 - 2^{-2s}} = \frac{P_2}{1 + 2 \cdot 2^{-2s}},$$

und hiermit ist unsere Absicht, diese Funktionen durch die Formen der Diskriminante $-3(18)^2$ darzustellen, wirklich erreicht.

§ 13.

Der Grenzsatz von Kronecker.

Nachdem wir durch die vorhergehenden Beispiele die Bildung des Charakters ψ, der Moduln k_ν, und hiermit auch der Funktion

$$2H = \Sigma' S(\mathfrak{k}_0) - \Sigma' S(\mathfrak{k}_1)$$

hinreichend erläutert haben, wenden wir uns zur Lösung der Aufgabe, welche wir uns in § 6 gestellt haben. Es handelt sich darum, die Anzahl h der Idealklassen des reinen kubischen Körpers K durch die wirkliche Ausführung des in der Gleichung

$$h \frac{2\pi \log \varepsilon}{k\sqrt{3}} = \lim (s-1)J$$

angedeuteten Grenzprozesses zu bestimmen, welcher darin besteht, daß die positive Variable $(s-1)$ unendlich klein wird. In § 7 ist die Dirichletsche Idealfunktion J in die beiden Faktoren G, H zerlegt, von denen der erste die über alle natürlichen Zahlen n ausgedehnte Summe

$$G = \sum \frac{1}{n^s}$$

ist, während der zweite Faktor H nach manchen Umformungen in § 11 die obige Gestalt angenommen hat. Da nun bekanntlich

$$\lim (s-1)G = 1$$

ist, so wird

$$h \frac{2\pi \log \varepsilon}{k\sqrt{3}} = \lim H,$$

und dieser Grenzwert läßt sich mit Hilfe eines berühmten Satzes von Kronecker leicht bestimmen. Da die Anzahl k'' der nicht äquivalenten Moduln $\mathfrak{k}_0$ mit der der Moduln $\mathfrak{k}_1$ übereinstimmt, so genügt hierzu schon der Ausdruck für den Grenzwert der Differenz

$$\Sigma(A x^2 + B x y + C y^2)^{-s} - \Sigma(A_1 x^2 + B_1 x y + C_1 y^2)^{-s},$$

wo $(A, \frac{1}{2}B, C)$, $(A_1, \frac{1}{2}B_1, C_1)$ irgend zwei positive Formen von derselben negativen Diskriminante $D = B^2 - 4AC$ bedeuten. Die Darstellung dieses Grenzwertes durch Thetafunktionen hat Kronecker zuerst im Monatsbericht der Berliner Akademie vom 22. Januar 1863 ohne Beweis mitgeteilt. Es lag nun nahe, diesen ersten Satz als Ausfluß eines zweiten aufzufassen, durch welchen das Verhalten der von einer einzelnen Form $(A, \frac{1}{2}B, C)$ erzeugten Summe

$$\Sigma(A x^2 + B x y + C y^2)^{-s}$$

für unendlich kleine positive Werte von $(s - 1)$ genauer ermittelt wird. Bekanntlich hat Dirichlet zuerst bewiesen, daß diese Funktion unendlich groß wird wie

$$\frac{2\pi}{(s-1)\sqrt{-D}},$$

und hierin besteht eine wesentliche Grundlage seiner Methode, die Klassenanzahl der Formen von der negativen Diskriminante D zu bestimmen. Jetzt kam es darauf an, einen Schritt weiter zu gehen, nämlich den endlichen Grenzwert der Differenz

$$\Sigma(A x^2 + B x y + C y^2)^{-s} - \frac{2\pi}{(s-1)\sqrt{-D}}$$

zu ermitteln. Diese Aufgabe ist zuerst für beliebige reelle Koeffizienten A, B, C von H. Weber in einem an mich gerichteten Briefe vom 12. Oktober 1881 vollständig gelöst, dessen Inhalt er später veröffentlicht hat im Bd. 33 der Mathematischen Annalen (1889) und in § 113 seines Werkes „Elliptische Funktionen und Algebraische Zahlen“ (1891). Inzwischen ist aber auch Kronecker in zahlreichen Aufsätzen über die elliptischen Funktionen auf diesen Gegenstand zurückgekommen; schon im Sitzungsberichte der Berliner Akademie vom 30. Juli 1885 findet sich seine, von der Weberschen wesentlich verschiedene Ableitung des fraglichen Grenzwertes, zunächst für rationale Koeffizienten, und endlich hat er im Sitzungsberichte vom

21. Februar 1889 den Satz auch auf Formen mit komplexen Koeffizienten ausgedehnt. Wir beschränken uns hier auf Formen mit reellen Koeffizienten und stellen den Satz in der für unseren Zweck geeigneten Form folgendermaßen dar.

Es seien α und $\beta = \alpha\omega$ irgend zwei komplexe Konstanten von imaginärem Verhältnis ω, und zwar setzen wir fest, daß der reelle Teil von $i\omega$ negativ sei; bezeichnen wir immer mit α' die mit α konjugierte komplexe Zahl und mit $N(\alpha)$ das stets positive Produkt $\alpha\alpha'$, so können wir dies auch durch die Bedingung

$$\Delta = i(\alpha\beta' - \beta\alpha') = i(\omega' - \omega)N(\alpha) > 0$$

ausdrücken, und wir nennen zugleich α die erste, β die zweite Basiszahl des binären Moduls $\mathfrak{k} = [\alpha, \beta] = \alpha[1, \omega]$, dessen Zahlen von der Form $\lambda = \alpha x + \beta y$ sind, wo x, y alle ganzen rationalen Zahlen durchlaufen. Sind α_1 und $\beta_1 = \alpha_1\omega_1$ ebenfalls eine erste und zweite Basiszahl desselben Moduls $\mathfrak{k} = [\alpha, \beta] = [\alpha_1, \beta_1]$, so bestehen zwischen diesen beiden Basen Relationen von der Form

$$\alpha_1 = a\alpha + c\beta, \quad \beta_1 = b\alpha + d\beta,$$

wo a, b, c, d vier ganze rationale Zahlen bedeuten, die der Bedingung

$$ad - bc = +1$$

genügen (vgl. § 11). Hieraus geht hervor, daß die oben mit Δ bezeichnete positive Größe eine Invariante des Moduls $\mathfrak{k}$, d. h. unabhängig von der Wahl seiner Basis ist. Bedient man sich ferner einer in der Theorie der elliptischen Modulfunktionen üblichen Ausdrucksweise*), so gehören die durch die Gleichung

$$\omega_1 = \frac{b + d\omega}{a + c\omega}$$

verbundenen Zahlen ω, ω_1 derselben Klasse äquivalenter Zahlen an, und diese Klasse ist also ebenfalls eine Invariante des Moduls $\mathfrak{k}$, oder vielmehr eine Invariante der Modulklasse, welche aus allen mit $\mathfrak{k}$ äquivalenten Moduln besteht. Von hervorragender Wichtigkeit für die eben genannte Theorie ist die Funktion

$$\eta(\omega) = e^{\frac{\pi i\omega}{12}} \Pi(1 - e^{2\pi i\omega n}),$$

*) Vgl. meinen Aufsatz in diesem Journal, Bd. 83, und meine Erläuterungen zum Fragment XXVIII in der zweiten Auflage von Riemanns Werken (1892). Eine ausführliche Darstellung der ganzen Theorie findet man in dem oben zitierten Werke von H. Weber und in den Vorlesungen über die Theorie der elliptischen Modulfunktionen von F. Klein und R. Fricke (1890—1892).

wo n in dem Produkte Π alle natürlichen Zahlen durchläuft; das Gesetz ihrer linearen Transformation wird durch die Gleichung

$$\eta(\omega_1) = r(a + c\omega)^{1/2}\eta(\omega)$$

ausgedrückt, wo $r^{24} = 1$ und ω_1 die obige Bedeutung hat; berücksichtigt man noch, daß $\eta(-\omega')$ die mit $\eta(\omega)$ konjugierte Größe, und daß

$$\omega_1' - \omega_1 = \frac{\omega' - \omega}{(a + c\omega)(a + c\omega')}$$

ist, so ergibt sich hieraus leicht, daß die Größe

$$H(\omega) = H(-\omega') = \eta(\omega)\eta(-\omega')\sqrt{i(\omega' - \omega)},$$

wo die Quadratwurzel immer positiv genommen werden soll, für alle mit ω äquivalenten Zahlen einen und denselben positiven Wert besitzt, welcher mithin eine Invariante der aus allen diesen Zahlen bestehenden Klasse ist. Durchläuft nun λ alle von Null verschiedenen Zahlen des Moduls $\mathfrak{k}$, und bezeichnen wir (wie in §§ 10, 11, 12) mit $S(\mathfrak{k})$ die Summe aller entsprechenden Potenzen $N(\lambda)^{-s}$, so besteht der Satz von Kronecker darin, daß

$$S(\mathfrak{k}) = \frac{2\pi}{\Delta}\left\{\frac{1}{s-1} - 2\Gamma'(1) - \log\Delta - 2\log H(\omega)\right\} + (0)$$

ist, wo die Funktion (0) gleichzeitig mit $(s-1)$ unendlich klein wird, während $-\Gamma'(1) = 0{,}5772\cdots$ die bekannte Eulersche Konstante ist.

Um nun diesen Satz auf unsere Moduln $\mathfrak{k} = k_\nu$ anzuwenden, bemerken wir zunächst, daß die obige Unterscheidung zwischen der ersten und zweiten Basiszahl mit der in § 11 festgesetzten übereinstimmt, wenn wir jetzt noch annehmen, daß dort unter ϱ immer diejenige Kubikwurzel der Einheit verstanden wird, für welche

$$1 + 2\varrho = \sqrt{-3} = i\sqrt{3}$$

wird, wo $\sqrt{3}$ positiv zu nehmen ist; behält man die dortigen Bezeichnungen bei, so wird zugleich

$$\Delta = i(\alpha\beta' - \beta\alpha') = k\sqrt{3}$$

und

$$\omega = \frac{\beta}{\alpha} = \frac{b_1 + b_2\varrho}{a_1 + a_2\varrho} = \frac{B + ik\sqrt{3}}{2A},$$

wo $(A, \frac{1}{2}B, C)$ wieder die der Basis α, β entsprechende binäre quadratische Form bedeutet. Hat man nun für jeden der k'' Moduln $\mathfrak{k}_0$

und für jeden der k'' Moduln $\mathfrak{k}_1$ nach Belieben eine Basis α, β gewählt, und bezeichnet man mit ω_0, ω_1 die entsprechenden Werte von ω, so liefert der Satz von Kronecker das Resultat

$$\lim H = \frac{2\pi}{k\sqrt{3}}\left\{\Sigma' \log H(\omega_1) - \Sigma' \log H(\omega_0)\right\},$$

und hieraus ergibt sich die Bestimmung der Anzahl h der Idealklassen im Körper K durch die Gleichung

$$\varepsilon^h = \frac{\Pi H(\omega_1)}{\Pi H(\omega_0)},$$

wo ε die Fundamentaleinheit des Körpers K bedeutet, und wo die Produktzeichen Π im Nenner und Zähler sich auf alle nicht äquivalenten Zahlen ω_0, ω_1 beziehen.

Mit diesem Resultat, in welchem der Zusammenhang zwischen den reinen kubischen Körpern und den aus der komplexen Multiplikation der elliptischen Funktionen entspringenden algebraischen Zahlkörpern enthalten ist, brechen wir die gegenwärtige Abhandlung ab; doch fügen wir noch die folgenden Bemerkungen hinzu, die sich auf die wirkliche Berechnung der Klassenanzahl h beziehen. Für diesen Zweck ist, wie wir gestehen müssen, die Brauchbarkeit des gewonnenen Resultats noch an gewisse Bedingungen gebunden, die zurzeit keineswegs als allgemein erfüllt anzusehen sind. Vor allem ist zu bemerken, daß hierzu die Kenntnis der Fundamentaleinheit ε des Körpers K erforderlich ist; nun haben sich zwar verschiedene ausgezeichnete Mathematiker damit beschäftigt, die zuerst von Jacobi*) angegebene und an einigen Beispielen durchgeführte Methode zu vervollkommnen, aber ein einfacher und zugleich nachweislich unfehlbarer Weg zur Gewinnung von ε, der sich mit der Lösung der Pellschen Gleichung in der Theorie der quadratischen Körper vergleichen ließe, ist meines Wissens bisher noch immer nicht gefunden. Für die Beispiele der in § 2 aufgestellten Tabelle ist es freilich ohne große Mühe möglich, die Aufgabe zu lösen, und zwar gelingt dies meistens durch die Zerlegung einiger wenigen Zahlen des Körpers in ihre idealen Primfaktoren; für diejenigen, welche solche Berechnungen anstellen mögen, bemerke ich folgendes. Gibt man den Buchstaben

*) Allgemeine Theorie der kettenbruchähnlichen Algorithmen, in welchen jede Zahl aus drei vorhergehenden gebildet wird (Journal für reine und angewandte Mathematik, Bd. 69).

a, b, α, β wieder dieselbe Bedeutung wie in § 2, so findet man leicht, daß jede im Körper K enthaltene Zahl

$$\varkappa = z + x\alpha + y\beta,$$

von deren rationalen Koordinaten z, x, y höchstens eine verschwindet, auch als Quotient in den Formen

$$\varkappa = \frac{y_1\alpha - b x_1}{b x - y\alpha} = \frac{x_1\beta - a y_1}{a y - x\beta} = \frac{z_1 - y_1\beta}{z - x\alpha} = \frac{z_1 - x_1\alpha}{z - y\beta}$$

darstellbar ist, wo

$$z_1 = z^2 - ab\,x\,y, \quad x_1 = a y^2 - z\,x, \quad y_1 = b x^2 - z\,y$$

die Koordinaten ihres Supplements

$$\varkappa'\varkappa'' = z_1 + x_1\alpha + y_1\beta$$

bedeuten. Hierdurch wird man veranlaßt, nur solche Zahlen $\varkappa$ zu betrachten, in welchen eine der Koordinaten x, y verschwindet, während die beiden anderen ganze Zahlen ohne gemeinsamen Teiler sind; eine solche Zahl $\varkappa$ ist nur durch Primideale ersten Grades teilbar, und $\varkappa$ kann auch nicht durch zwei verschiedene, in derselben natürlichen Primzahl p aufgehende Primideale teilbar sein, ausgenommen den Fall $p = 3$ bei den Körpern zweiter Art, wo $\mathfrak{o}\,3 = \mathfrak{p}^2\mathfrak{p}_1$, und wo jede Zahl $\varkappa$ entweder relative Primzahl zu 3 oder teilbar durch $\mathfrak{p}\mathfrak{p}_1$, aber niemals teilbar durch $\mathfrak{p}^2$ ist. Auf Grund dieser Eigenschaften schließt man aus der Norm von $\varkappa$, welche die leicht zu berechnende Form $z^3 + ab^2x^3$ oder $z^3 + a^2by^3$ hat, sofort auf die Zerlegung des Ideals $\mathfrak{o}\varkappa$ in seine Primfaktoren. Um zu bewirken, daß eine solche Zahl $\varkappa$ durch ein in der natürlichen Primzahl p aufgehendes Primideal ersten Grades $\mathfrak{p}$ teilbar wird, braucht man nur mit Hilfe des Canon Arithmeticus die beiden rationalen Zahlen u, v zu bestimmen, für welche $\alpha \equiv u$, $\beta \equiv v \pmod{\mathfrak{p}}$, also $u^3 \equiv ab^2$, $v^3 \equiv a^2b$, $uv \equiv ab \pmod{p}$ wird; dann ist der Modul $[p, \alpha - u, \beta - v]$ das kleinste gemeinsame Vielfache $\mathfrak{p} - \mathfrak{n}$ von $\mathfrak{p}$ und der Ordnung $\mathfrak{n} = [1, \alpha, \beta]$, und unter den in ihm enthaltenen Zahlen $\varkappa$ wird man vorzugsweise diejenigen wählen, deren Koordinaten so klein wie möglich sind. In allen Beispielen der Tabelle in § 2 und einigen anderen, die ich untersucht habe, findet man bald, daß aus wenigen so zerlegten Zahlen $\varkappa$ sich zwei Produkte von verschiedenem Absolutwert bilden lassen, welche aus denselben Primidealen zusammengesetzt sind, deren Quotient folglich eine irrationale

Einheit ist. Die Aufsuchung der Fundamentaleinheit ε, welche hierdurch bekanntlich in endliche Grenzen eingeschlossen ist, kann freilich noch ziemlich mühselig sein, obgleich die Anzahl der anzustellenden Versuche durch Zuziehung gewisser Kongruenzen sich noch beschränken läßt.

Am Schlusse der in der Einleitung erwähnten Abhandlung gibt Herr Markoff eine wertvolle Tabelle von Einheiten für diejenigen 52 aus $\alpha = \sqrt[3]{ab^2}$ gebildeten Körper, in welchen $ab^2 \leqq 70$ ist (von den 54 in der Tabelle angegebenen Einheiten treten zwei je zweimal auf, die eine bei $ab^2 = 12$ und $ab^2 = 18$, die andere bei $ab^2 = 20$ und $ab^2 = 50$); daß der von ihm eingeschlagene Weg der Berechnung mit dem eben beschriebenen wesentlich übereinstimmt, geht teils aus der Darstellungsform dieser Einheiten hervor, teils aus der in § 5 (S. 20) enthaltenen Bemerkung: „Ne nous arrêtant pas aux méthodes sûres mais fatigantes pour déterminer l'unité complexe fondamentale nous remarquons, que pour les valeurs petites de a et b il est facile de trouver les unités complexes par le tâtonnement en considérant plusieurs nombres ξ composés des mêmes facteurs premiers". Unter diesen 52 Körpern befinden sich auch alle in meiner Tabelle (§ 2) angegebenen 21 Körper ($ab \leqq 23$), und die in diesem Umfange angestellte Vergleichung mit meinen Rechnungen hat ergeben, daß die von Herrn Markoff gefundenen Einheiten sämtlich fundamental sind mit einziger Ausnahme des Beispiels $ab^2 = 28$, in welchem die von ihm angegebene Einheit das Quadrat der Fundamentaleinheit ist.

Während die von Herrn Markoff und mir angewandte Methode auf der Zerlegung der Zahlen in ihre idealen Primfaktoren beruht, hat Herr Mehmke schon seit dem Jahre 1885 den zuerst von Jacobi angegebenen, später von Herrn Bachmann*) behandelten Algorithmus der Annäherung wieder aufgenommen und durch gewisse Modifikationen zu vervollkommnen gesucht, worüber er mir brieflich in den Jahren 1889 bis 1893 interessante Mitteilungen gemacht hat, die mir die Veröffentlichung seiner Methoden sehr wünschenswert erscheinen lassen; mit bestem Danke erwähne ich einer von ihm

*) Zur Theorie von Jacobis Kettenbruch-Algorithmen (dieses Journal Bd. 75, 1873). Vgl. Fr. Meyer, Über kettenbruchähnliche Algorithmen (Verhandlungen des Mathematikerkongresses in Zürich 1897).

berechneten Tabelle von 39 Einheiten, unter denen sich acht auf die Beispiele $ab^2 = 76, 124, 126, 140, 198, 207, 234, 350$ beziehen, also nicht in der Markoffschen Tabelle enthalten sind.

Die weiter unten zu benutzenden Fundamentaleinheiten ε der in § 12 mit K_1, K_2, K_4, K_5 bezeichneten Körper und ihre reziproken Werte ε^{-1} sind die folgenden:

$$\begin{aligned} \varepsilon_1 &= 1 + \alpha + \beta, & \varepsilon_1^{-1} &= -1 + \alpha, \\ \varepsilon_2 &= 4 + 3\alpha + 2\beta, & \varepsilon_2^{-1} &= -2 + \beta, \\ \varepsilon_4 &= 109 + 60\alpha + 33\beta, & \varepsilon_4^{-1} &= 1 - 6\alpha + 3\beta, \\ \varepsilon_5 &= 55 + 24\alpha + 21\beta, & \varepsilon_5^{-1} &= 1 + 3\alpha - 3\beta. \end{aligned}$$

Wenden wir uns jetzt zu der Berechnung der Funktion $H(\omega)$, welche für alle einander äquivalenten Zahlen ω denselben Wert besitzt, so ist es vorteilhaft, für den Repräsentanten einer solchen Klasse immer die in derselben enthaltene reduzierte Zahl ω zu wählen, welche den Bedingungen

$$-1 \leqq \omega + \omega' \leqq +1, \quad \omega\omega' \geqq 1$$

genügt, weil dann der analytische Modul (oder absolute Betrag) von $e^{2\pi i\omega}$ bekanntlich so klein wie möglich wird; da es ohnehin feststeht, daß h eine ganze Zahl ist, so genügt in der Regel die Annäherung

$$\eta(\omega) = e^{\frac{\pi i\omega}{12}}, \quad \eta(-\omega') = e^{-\frac{\pi i\omega'}{12}}.$$

$$H(\omega) = e^{-\frac{\pi i(\omega'-\omega)}{12}} \sqrt{i(\omega'-\omega)}.$$

Setzt man wie oben

$$\omega = \frac{B + ik\sqrt{3}}{2A}, \quad -\omega' = \frac{-B + ik\sqrt{3}}{2A}, \quad i(\omega'-\omega) = \frac{k\sqrt{3}}{A},$$

wo $(A, \frac{1}{2}B, C)$ die der reduzierten Zahl ω entsprechende reduzierte Form von der Diskriminante $B^2 - 4AC = D = -3k^2$ bedeutet, so wird

$$\log H(\omega) = -\frac{\pi k\sqrt{3}}{12A} - \tfrac{1}{2}\log A + \tfrac{1}{2}\log(k\sqrt{3});$$

setzt man hierin für ω die k'' Werte ω_0 und die k'' Werte ω_1 ein und bezeichnet die entsprechenden Werte von A mit A_0 und A_1, so ergibt sich

$$h\log\varepsilon = \frac{\pi k\sqrt{3}}{12}\left\{\sum\frac{1}{A_0} - \sum\frac{1}{A_1}\right\} + \tfrac{1}{2}\left\{\sum\log A_0 - \sum\log A_1\right\};$$

führt man endlich statt der natürlichen Logarithmen *log* die gemeinen Logarithmen *Log* ein und setzt zur Abkürzung

$$M = \frac{\pi\sqrt{3}}{12}\,Log\,e = 0{,}196\,930\,8\cdots, \quad Log\,M = 0{,}294\,313\,7\cdots - 1,$$

so erhält man die Annäherung

$$h\,Log\,\varepsilon = Mk\left\{\sum\frac{1}{A_0} - \sum\frac{1}{A_1}\right\} + \tfrac{1}{2}\left\{\sum Log\,A_0 - \sum Log\,A_1\right\},$$

welche, wie gesagt, zur Berechnung der ganzen Zahl h in der Regel vollständig ausreicht*). Um eine Probe für die Genauigkeit dieser Formel zu machen, deren rechte Seite mit $\mathfrak{M}$ bezeichnet werden möge, wollen wir sie auf die vier Körper K_1, K_2, K_4, K_5 anwenden, für welche die Werte der Zahlen A_0, A_1 in § 12 angegeben sind; die hiernach zu berechnenden Werte von $\mathfrak{M}$ sind dann mit den obigen Werten der Fundamentaleinheiten ε zu vergleichen.

Körper K_1.

$k = 6,\ k'' = 1;\ A_0 = 1;\ A_1 = 4;\ \mathfrak{M} = 0{,}585\,158\,6;$
$\varepsilon = 3{,}847\,322\,1,\ Log\,\varepsilon = 0{,}585\,158\,5.$

Körper K_2.

$k = 9,\ k'' = 1;\ A_0 = 1;\ A_1 = 7;\ \mathfrak{M} = 1{,}096\,631\,5;$
$\varepsilon = 12{,}486\,916\,4,\ Log\,\varepsilon = 1{,}096\,455\,0.$

Körper K_4.

$k = 18,\ k'' = 3;\ A_0 = 1,\ 7,\ 7;\ A_1 = 4,\ 9,\ 13;\ \mathfrak{M} = 2{,}514\,792\,9;$
$\varepsilon = 326{,}990\,833\,6,\ Log\,\varepsilon = 2{,}514\,535\,6.$

Körper K_5.

$k = 18,\ k'' = 3;\ A_0 = 1,\ 13,\ 13;\ A_1 = 4,\ 7,\ 9;\ \mathfrak{M} = 2{,}216\,900\,7;$
$\varepsilon = 164{,}981\,855\,8,\ Log\,\varepsilon = 2{,}217\,436\,2.$

In allen diesen Beispielen schließt man aus der obigen Näherungsformel $h\,Log\,\varepsilon = \mathfrak{M}$ mit Sicherheit, daß die Klassenanzahl $h = 1$ ist, weil $\mathfrak{M}$ nahezu mit $Log\,\varepsilon$ übereinstimmt.

Auf dieselbe Weise habe ich die Klassenanzahl h für alle Körper der Tabelle in § 2 und außerdem für die drei Beispiele $ab^2 = 35$, 53, 91 berechnet, denen die Werte $h = 3$, 1, 9 entsprechen.

*) Nach einer oberflächlichen Schätzung ist für jede reduzierte Zahl ω der absolute Betrag der Differenz $Log\,\eta(\omega) - \frac{\pi i\omega}{12}\,Log\,e$ immer $< 0{,}001\,894\,3$.

Bedenkt man, daß für diese Bestimmungsart der Klassenanzahl h außer der Kenntnis der Fundamentaleinheit ε auch die Aufstellung der Moduln $\mathfrak{k}$ und ihrer Charaktere ψ erforderlich ist, welche für größere Werte von ab immer zeitraubender wird, so kann man dem oben gewonnenen Resultate nur einen sehr geringen oder gar keinen praktischen Wert beilegen. Auf Grund des schönen Satzes von Herrn Minkowski*), daß es in jeder Idealklasse mindestens ein Ideal gibt, dessen Norm absolut kleiner ist als die Quadratwurzel aus der Grundzahl des Körpers, gestaltet sich die Berechnung von h viel kürzer; die oben beschriebene Zerlegung der Zahlen $\varkappa$ von der Form $z + x\alpha$ oder $z + y\beta$ in ihre idealen Primfaktoren liefert (in allen 24 von mir behandelten Beispielen) so viele Äquivalenzen zwischen den fraglichen Idealen, daß sie sich wirklich in h Klassen einordnen, und es kommt nur noch darauf an zu zeigen, daß diese Klassen auch voneinander verschieden sind, was meistens keine Schwierigkeit macht; in den Fällen, wo ab durch Primzahlen p von der Form $3m + 1$ teilbar ist, dient hierzu namentlich die Bemerkung, daß $N(z + x\alpha + y\beta) \equiv z^3 \pmod{ab}$, also die Norm jedes Hauptideals kubischer Rest von jeder solchen Primzahl p ist, worauf zugleich die Einteilung der Idealklassen in Geschlechter beruht. Ich bemerke schließlich, daß auch Herr Markoff in § 6 seiner Abhandlung für einige Beispiele die Klassenanzahl h auf ganz ähnliche Weise bestimmt hat.

Ich habe im Vorwort leider versäumt, die kürzlich in der Vierteljahrsschrift der Naturforschenden Gesellschaft in Zürich (1897, Jahrgang 42) veröffentlichte nachgelassene Abhandlung: „Zur Theorie der zerlegbaren Formen, insbesondere der kubischen“ von Arnold Meyer zu erwähnen; sie ist schon im Jahre 1870 verfaßt und bietet, abgesehen von der Ermittlung der Idealzahlen, nur wenige Berührungspunkte mit meiner Arbeit dar.

---

*) Théorèmes arithmétiques (Compte rendu der Pariser Akademie vom 26. Januar 1891).

Erläuterungen zur vorstehenden Abhandlung.

Dedekind verwendet in dieser Arbeit zum erstenmal die bekannte Dirichlet-Dedekindsche Grenzformel zur Bestimmung der Klassenanzahl in Körpern, welche nicht Unterkörper eines Kreisteilungskörpers sind, und zwar mit Methoden, die auch für allgemeinere Untersuchungen bedeutungsvoll sind. Die in der Einleitung und früher in der Anzeige der Bachmannschen Vorlesungen ausgesprochene Vermutung, daß die Resultate über den Zusammenhang zwischen kubischen Resten und Klassen der quadratischen Formen auch für beliebige kubische Körper richtig bleiben, ist von Takagi [Comptes rendus **171** (1920), S. 1202—1205] bewiesen. Der Satz folgt als Spezialfall eines allgemeineren Satzes über auflösbare Körper vom Primzahlgrad, und der Beweis beruht auf den allgemeinen Zerlegungsgesetzen in relativ-Abelschen Körpern, entspricht also der Dedekindschen Vermutung, daß das Problem bei beliebigen kubischen Körpern unter Anwendung der Theorie der komplexen Multiplikation behandelt werden könnte. Die Klassenzahl der Körper der komplexen Multiplikation hat zuerst Fueter [Gött. Nachr. **1907**, S. 288—298, Rendiconti di Palermo **29** (1910), S. 380—395] bestimmt.

Zu §§ 1—5. Die in diesen Paragraphen enthaltenen Resultate über Diskriminante und Primidealzerlegung bei reinen kubischen Körpern hätte man auch einfach aus den allgemeineren Abhandlungen XV und XIV, Bd. I folgern können. Die Abhandlung über die Invarianten beliebiger kubischer Körper, die Dedekind in der Einleitung in Aussicht stellt, hat er leider nicht publiziert.

Für allgemeine kubische Körper hat eine Reihe von Autoren sich mit der Aufstellung einer Basis, Bestimmung der Körperdiskriminante und Primidealzerlegung und mit der damit eng verbundenen Berechnung der Klassenzahl beschäftigt. Es sollen hier nur einige der wichtigsten Arbeiten erwähnt werden: G. Woronoj, Diss. St. Petersburg 1894; L. W. Reid, Amer. Journ. of Math. **23** (1901), S. 68—84; L. Sapolsky, Diss. Göttingen 1902; W. E. Berwick, Proc. London Math. Soc. (2) **12** (1913), S. 393—429; (2) **23** (1925), S. 359—378; G. E. Wahlin, Amer. Journ. of Math. **44** (1922), S. 191—203. Eine vollständige Untersuchung der kubischen Körper und ihrer Invarianten mittels der Theorie der Klassenkörper gab H. Hasse [Math. Zeitschr. **31** (1930), S. 565—582].

§§ 7—8. Die neuere Literatur über Reziprozitätsgesetze findet man bei Hasse: Bericht usw. Teil II: Reziprozitätsgesetze. Ergänzungsband VI, Jahresbericht d. Deutschen Math.-Ver. 1930.

Den Quotienten aus der Zetafunktion eines Körpers und der Zetafunktion eines Unterkörpers (wie speziell die Dedekindsche Funktion H, S. 174—175) hat Artin [Math. Ann. **89** (1923), S. 147—156] für metazyklische und andere Körper untersucht, ganz allgemein in der Arbeit über die L-Reihen [Hamburg. Abhandl. **3** (1924), S. 89—108].

Für beliebige kubische Körper hat C. G. Jaeger [Amer. Journ. of Math. **52** (1930), S. 85—96] ein Charaktersymbol ψ eingeführt, das ähnliche Eigenschaften wie das Dedekindsche besitzt.

§ 11. Das auf S. 206—207 erwähnte Fragment von Gauß ist in Bd. VIII, S. 5 seiner Werke mit verschiedenen anderen, teilweise weitergehenden Notizen über kubische und biquadratische Reste abgedruckt. Nach den Erläuterungen von Fricke war die Notiz auf dem Vorsatzblatt des Einbandes von Gauß' Handexemplar der Disquisitiones geschrieben und stammt wahrscheinlicherweise aus der Zeit 1804—1805.

§ 13. Ein einfacher Beweis des Kroneckerschen Grenzsatzes findet sich z. B. in H. Weber, Lehrbuch der Algebra, Bd. III, § 141 (2. Auflage). Neuere Untersuchungen über den Kroneckerschen Grenzsatz findet man bei Fueter [Rendiconti di Palermo **29** (1910), S. 380—395] und Herglotz [Leipziger Berichte **75** (1923), S. 3—14, 31—37]; vgl. auch L. J. Mordell, Proc. Roy. Soc. London **125** (1929), S. 262—276.

Hinsichtlich der notwendigen Berechnung der Fundamentaleinheit soll bemerkt werden, daß die oben erwähnte, in russischer Sprache verfaßte Arbeit von G. Woronoj angeblich eine Methode zur Bestimmung der Fundamentaleinheit in beliebigen kubischen Körpern mit negativer Diskriminante enthalten soll.

Es ist hier nicht möglich, auf die reichhaltige Literatur über die Dedekindsche Zetafunktion näher einzugehen; es muß nur auf die fundamentalen Arbeiten von Hecke, Landau, Artin u. a. verwiesen werden. Unter Benutzung der Dedekindschen Vorarbeiten studierte Landau die Eigenschaften der Zetafunktionen reiner kubischer Körper (Festschrift zu H. A. Schwarz, 1914, S. 244—273).

Ore.

XXX.

Über die von drei Moduln erzeugte Dualgruppe.

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

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

§ 1.

Allgemeine Eigenschaften der Dualgruppen.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 Teiler von $\mathfrak{b}$ heißen.

Ist endlich keines der beiden Elemente $\mathfrak{a}$, $\mathfrak{b}$ durch das andere teilbar, 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) charakterisierte Teilbarkeit 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 teilbar 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 Teiler $\mathfrak{a}$ von $\mathfrak{b}$, $\mathfrak{b}'$ ist Teiler 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 Teiler von $\mathfrak{b}$, $\mathfrak{b}'$. Diese Ausdrucksweise dehnen wir auch auf mehr als zwei Elemente aus, und durch wiederholte Anwendung des Vorhergehenden ergibt sich der Satz: ist jedes der Elemente $\mathfrak{a}'$, $\mathfrak{a}''$, $\mathfrak{a}'''$ $\cdots$ ein Teiler 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 Teiler des größten gemeinsamen Teilers 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 $\mathfrak{b}$ ein Teiler von $\mathfrak{m}$, also $\mathfrak{b} < \mathfrak{m}$, und $\mathfrak{p}$ ein beliebiges Element, so ist

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

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

§ 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 $\pm$ 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 $\mathfrak{b}$ ein Teiler des Moduls $\mathfrak{m}$, also $\mathfrak{b} < \mathfrak{m}$, und $\mathfrak{p}$ ein beliebiger Modul, so ist

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

so wird

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

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

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

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

so wird

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

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

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

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

und

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

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

wo

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

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

§ 3.

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

Ist die Anzahl der nach dem Modul $\mathfrak{n}$ inkongruenten 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) $$(\mathfrak{m}, \mathfrak{n}) = (\mathfrak{m} + \mathfrak{n}, \mathfrak{n}),$$

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

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

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

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

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

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

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

hierauf aus (20) und (25)

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

hierauf aus (21) und (24)

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

endlich aus (23)

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

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

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

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

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

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

und aus (22)

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

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

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

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

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

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

folgt.

Wir begnügen uns, das hiernach einzuschlagende Verfahren an denjenigen Symbolen $(\mathfrak{m}, \mathfrak{n})$ der dritten Klasse 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 ergibt sich durch zweimalige Anwendung von (32)

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

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

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

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

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

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

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

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

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

oder die Form

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

geben kann, fließt auch der Satz

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

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

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

§ 4.

Idealgruppen.

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

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

jedes der drei Paare von Produkten

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

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

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

über.

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

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

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

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

§ 5.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§ 6.

Beziehung zwischen dem Modul- und dem Kettengesetz.

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

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

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

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

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

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

definieren. Zunächst ergeben sich die folgenden 11 ursprünglichen Teilbarkeiten

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

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

rationen $\pm$ die oben definierten Elemente $\mathfrak{b}_3$, $\mathfrak{b}'''$, $\mathfrak{c}'''$, $\mathfrak{c}_3$; für die übrigen vier Paare ergibt 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 Konstitution, 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 $\mathfrak{m} = \mathfrak{n} = \mathfrak{m} \pm \mathfrak{n}$ entsprechen, sind zur Erleichterung des Überblicks leer gelassen.

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

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

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

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

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

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

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

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

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

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

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

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

und behaupten zunächst, daß

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

wäre nun $\mathfrak{a} - \mathfrak{b}$ verschieden von $\mathfrak{m}$, so müßte, weil $\mathfrak{a}$ und $\mathfrak{b}$ nächste Teiler 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 Teiler 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 Teilbarkeiten in (15) bis (18) zu vergleichen; so erhält man

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

Wir wollen ferner bemerken, daß die im ersten Teile des Satzes aufgestellte Behauptung $\mathfrak{a} + \mathfrak{b} = \mathfrak{b}$ 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 Teiler von $\mathfrak{c}_3 = \mathfrak{a} - \mathfrak{b}_1$. Ebenso gilt im zweiten Teile 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 gibt es in $\mathfrak{M}$ mindestens eine mit $\mathfrak{K}$ äquivalente Kette $\mathfrak{P}$, in welcher das Glied $\mathfrak{p}$ auftritt.

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

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

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

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

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

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

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

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

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

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

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

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

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

und die Kette $\mathfrak{P}$ wird

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

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

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

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

und die Kette $\mathfrak{P}$ wird

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

zugleich ist $p = q = 4$.

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

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

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

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

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

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

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

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

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

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

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 Modulgesetz und dem Kettengesetz nachgewiesen ist, fügen wir noch einige Bemerkungen über endliche Modulgruppen hinzu, deren Beweise der Leser leicht finden wird. Unter den Elementen $\mathfrak{m}$

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

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

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

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

Alles dies bestätigt sich an dem früher behandelten Beispiele der aus 28 verschiedenen Moduln bestehenden Gruppe $\mathfrak{D}$; hier ist $\mathfrak{p} = \mathfrak{d}''''$, $\mathfrak{q} = \mathfrak{d}_4$, $k = 8$, 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 $\mathfrak{d}_1$, $\mathfrak{d}_2$, $\mathfrak{c}_2$, $\mathfrak{a}_3$, $\mathfrak{d}_4$ für sich eine Modulgruppe mit vier Stufen S', von denen

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

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 Teilbarkeit $\mathfrak{m} > \mathfrak{d}$ 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 Teilbarkeit $\mathfrak{m} > \mathfrak{d}$ folgt, daß also die beiden Aussagen

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

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

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

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

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

also

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

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

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

also auch

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

Braunschweig, den 8. Januar 1900.

Erläuterungen zur vorstehenden Abhandlung.

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

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

Noether.

XXXI.

Über die Permutationen des Körpers aller algebraischen Zahlen.

[Festschrift zur Feier des hundertfünfzigjährigen Bestehens der Königlichen Gesellschaft der Wissenschaften zu Göttingen. Abhandlungen der mathematisch-physikalischen Klasse, S. 1—17 (1901).]

Die vorliegende, rein algebraische Untersuchung verfolgt das Ziel, gewisse Sätze, die sich auf endliche Körper beziehen, auf unendliche Körper auszudehnen; um aber ihren Gegenstand genauer zu bezeichnen, ist es nötig, an die Bedeutung der in der Überschrift gewählten Ausdrücke und an einige Sätze zu erinnern, welche sich auf dieselben beziehen. Eine ausführliche Entwicklung dieser Begriffe und der Beweise findet man in der vierten Auflage (1894) von Dirichlets Vorlesungen über Zahlentheorie (Supplement XI), die ich im folgenden mit D. zitieren werde; hier beschränke ich mich in den beiden ersten Paragraphen darauf, aus dieser Darstellung mit Übergehung der Beweise nur das zu entlehnen, was für unseren Zweck unerläßlich ist.

§ 1.

Körper und irreduzibele Systeme.

Ein System A von reellen oder komplexen Zahlen heißt ein Körper (D. § 160), wenn die Summen, Differenzen, Produkte und Quotienten von je zwei dieser Zahlen demselben System A angehören. Der kleinste Körper R besteht aus allen rationalen, der größte Körper Z aus allen komplexen Zahlen. Ein Körper A heißt Divisor eines Körpers B, und zugleich heißt B ein Multiplum von A, wenn jede in A enthaltene Zahl auch dem Körper B angehört; der Körper R ist ein gemeinsamer Divisor, der Körper Z ein gemeinsames Multiplum aller Körper A. Ist B Multiplum von A und Divisor von C, so ist A Divisor von C. Jedes bestimmte System von Körpern A, mag ihre Anzahl endlich oder unendlich sein, besitzt einen

bestimmten größten gemeinsamen Divisor D; dieser Körper besteht aus denjenigen Zahlen, welche allen diesen Körpern A gemeinsam angehören, und jeder gemeinsame Divisor dieser Körper A ist Divisor von D. Dasselbe Körpersystem besitzt ein bestimmtes kleinstes gemeinsames Multiplum M; dieser Körper M ist der größte gemeinsame Divisor aller derjenigen Körper, welche (wie z. B. Z) gemeinsame Multipla der Körper A sind.

Ein endliches System T von m Zahlen $t_1, t_2 \cdots t_m$ heißt reduzibel in bezug auf den Körper A, wenn es m Zahlen $a_1, a_2 \cdots a_m$ in A gibt, welche der Bedingung

$$a_1 t_1 + a_2 t_2 + \cdots + a_m t_m = 0$$

genügen und nicht alle verschwinden; im entgegengesetzten Falle heißt das System T irreduzibel nach A (D. § 164).

Eine Zahl t heißt algebraisch in bezug auf den Körper A, wenn es eine natürliche Zahl n gibt, für welche die $n+1$ Potenzen

$$1, t, t^2 \cdots t^{n-1}, t^n$$

ein nach A reduzibeles System bilden; die kleinste Zahl n, für welche dies eintritt, heißt der Grad von t, und wir sagen, t sei eine algebraische Zahl n^{ten} Grades in bezug auf A. Offenbar ist eine solche Zahl t die Wurzel einer (irreduzibelen) Gleichung

$$t^n + a_1 t^{n-1} + \cdots + a_{n-1} t + a_n = 0,$$

deren Koeffizienten $a_1, a_2 \cdots a_n$ Zahlen des Körpers A sind, während die n Potenzen

$$1, t, t^2 \cdots t^{n-1}$$

ein nach A irreduzibeles System bilden. Man überzeugt sich leicht (D. § 164, IX), daß der Inbegriff U aller Zahlen u von der Form

$$u = x_1 t^{n-1} + x_2 t^{n-2} + \cdots + x_{n-1} t + x_n,$$

wo $x_1, x_2 \cdots x_{n-1}, x_n$ willkürliche Zahlen in A bedeuten, wieder ein Körper, und zwar ein Multiplum von A ist; diesen Körper U bezeichnen wir mit $A(t)$, und wir sagen, er entstehe aus A durch Adjunktion von t. Je $n+1$ Zahlen dieses Körpers $A(t)$ bilden ein nach A reduzibeles System, mithin ist jede Zahl u algebraisch in bezug auf A, und ihr Grad nicht größer als n; ist dieser Grad $= n$, so ist $A(u)$ identisch mit $A(t)$.

Ein Körper B heißt endlich in bezug auf den Körper A und vom Grade n, wenn es in B ein aus n Zahlen bestehendes, nach A irreduzibeles System gibt, während je $n+1$ Zahlen des Körpers B

ein nach A reduzibeles System bilden; diesen Grad n, welcher immer eine natürliche Zahl ist, bezeichnen wir durch das Symbol (B, A). Dann sind alle Zahlen in B algebraisch in bezug auf A, darunter gibt es auch (unendlich viele) Zahlen t, deren Grad $= n$ ist (D. § 165, VI), und der durch Adjunktion einer solchen Zahl t aus A entstehende Körper $A(t)$ ist das kleinste gemeinsame Multiplum M der beiden Körper A, B; mithin besteht der Satz

$$(1) \qquad (B, A) = (M, A).$$

Wenn B selbst ein Multiplum von A, also $M = B$ ist, so heißt B ein endliches Multiplum von A; ist zugleich der Körper C ein endliches Multiplum von B, so ist C auch ein endliches Multiplum von A, und es gilt der Satz (D. § 164, X)

$$(2) \qquad (C, A) = (C, B)\,(B, A).$$

Daß ein Körper D Divisor eines Körpers M ist, wird durch $(D, M) = 1$ vollständig ausgedrückt.

Ist aber B nicht endlich in bezug auf A, gibt es also in B, wie groß auch die natürliche Zahl m gewählt sein mag, immer m Zahlen, die ein nach A irreduzibeles System bilden, so wollen wir $(B, A) = \infty$ setzen*), wodurch wir erreichen, daß die beiden Sätze (1) und (2) allgemein gelten, der letztere natürlich unter der früheren Annahme, daß B Multiplum von A und Divisor von C ist.

§ 2.

Permutationen eines Körpers.

Eine Abbildung φ des Körpers A, durch welche jede in A enthaltene Zahl a in eine entsprechende Zahl $a\varphi$ übergeht, heißt eine Permutation von A, wenn sie den vier Gesetzen

$$(u+v)\varphi = u\varphi + v\varphi, \quad (u-v)\varphi = u\varphi - v\varphi,$$
$$(uv)\varphi = (u\varphi)\,(v\varphi), \quad \left(\frac{u}{v}\right)\varphi = \frac{u\varphi}{v\varphi}$$

gehorcht, wo u, v willkürliche Zahlen in A bedeuten (D. § 161); wir sagen auch, die Permutation φ beziehe sich auf den Körper A, und nennen den letzteren kurz den Körper von φ, um hierdurch auszudrücken, daß die Abbildung φ auf keine außerhalb A liegende Zahl wirken soll. Ist ferner T irgendein Teil von A, d. h. ein

*) Vgl. den Schluß von D. § 164, wo für diesen Fall $(B, A) = 0$ gesetzt wird, was aber für die jetzige Untersuchung weniger vorteilhaft ist.

System von Zahlen t, die alle in A enthalten sind, so bezeichnen wir mit $T\varphi$ den Inbegriff aller Bilder $t\varphi$ dieser Zahlen t. Die Zahl $t\varphi$ heißt konjugiert mit t.

Aus dieser Definition folgt leicht, daß das Zahlensystem $A\varphi$ wieder ein Körper ist, und daß je zwei verschiedene Zahlen des Körpers A durch φ in zwei verschiedene Zahlen des konjugierten Körpers $A\varphi$ übergehen; aus diesem Grunde läßt sich die Permutation φ eindeutig umkehren, und wenn man mit φ^{-1} diejenige Abbildung des Körpers $A\varphi$ bezeichnet, durch welche jede in $A\varphi$ enthaltene Zahl $a\varphi$ in a übergeht, so leuchtet ein, daß diese Umkehrung φ^{-1} eine Permutation von $A\varphi$, und $(A\varphi)\varphi^{-1} = A$ ist.

Jeder Körper A besitzt mindestens eine, nämlich die sogenannte identische Permutation, durch welche jede seiner Zahlen in sich selbst übergeht; wir wollen sie im folgenden mit A_0 bezeichnen. Ist φ eine beliebige Permutation von A, und r eine rationale, also auch in A enthaltene Zahl, so ist $r\varphi = r$, woraus zugleich folgt, daß der Körper R der rationalen Zahlen nur eine einzige, die identische Permutation R_0 besitzt.

Ist der Körper A ein Divisor des Körpers B, so ist in jeder Permutation ψ von B eine entsprechende Permutation φ von A enthalten, welche für jede Zahl a des Körpers A durch $a\varphi = a\psi$ definiert wird, woraus zugleich folgt, daß der Körper $A\varphi = A\psi$, also ein Divisor des Körpers $B\psi$ ist. Diese Permutation φ heißt der auf A bezügliche Divisor von ψ, und umgekehrt heißt ψ ein auf B bezügliches Multiplum von φ (D. § 163). Im Falle $A = B$ ist offenbar $\varphi = \psi$; ist aber A verschieden von B, also ein sogenannter echter Divisor von B, so ist auch φ wesentlich verschieden von ψ, weil die Wirkungsgebiete beider Permutationen verschieden sind. Die einzige Permutation R_0 des Körpers R der rationalen Zahlen ist gemeinsamer Divisor aller Körperpermutationen, und jeder Divisor einer identischen Permutation ist ebenfalls eine identische Permutation. Ist die Permutation φ des Körpers A ein Divisor der Permutation ψ, und letztere ein Divisor der Permutation χ, so ist φ zugleich der auf A bezügliche Divisor von χ.

Aus der unendlichen Menge von Sätzen, zu welchen diese Begriffe führen, wollen wir hier nur zwei besonders wichtige hervorheben; um sie bequem aussprechen zu können, schicken wir noch folgende Erklärung voraus (D. § 161). Ist $\mathfrak{P}$ ein (endliches oder unendliches)

System von Permutationen ψ beliebiger Körper B, so geht eine in dem größten gemeinsamen Divisor dieser Körper B enthaltene Zahl t durch jede Permutation ψ in eine entsprechende Zahl $t\psi$ über, und sie heißt n-wertig zu $\mathfrak{P}$, wenn n die Anzahl der voneinander verschiedenen Werte ist, welche sich unter diesen Zahlen $t\psi$ finden; offenbar ist jede rationale Zahl einwertig zu $\mathfrak{P}$. Hiernach lautet unser erster, leicht zu beweisender Satz (D. § 163) so:

I. Ist $\mathfrak{P}$ ein System von Körper-Permutationen ψ, so bildet die Gesamtheit aller zu $\mathfrak{P}$ einwertigen Zahlen einen Körper A; die Permutationen ψ haben alle einen und denselben auf A bezüglichen Divisor φ, und jeder gemeinsame Divisor der Permutationen ψ ist Divisor dieser Permutation φ.

Diesen Körper A, welcher durch das System $\mathfrak{P}$ vollständig bestimmt ist, wollen wir kurz den Körper von $\mathfrak{P}$ nennen, und seine Permutation φ soll der größte gemeinsame Divisor der Permutationen ψ oder kürzer der Rest von $\mathfrak{P}$ heißen; besteht das System $\mathfrak{P}$ nur aus einer einzigen Permutation ψ, so ist offenbar auch im früheren Sinne A der Körper von ψ, und $\varphi = \psi$.

Während die Existenz der Divisoren einer gegebenen Körper-Permutation unmittelbar einleuchtet, so liegt die umgekehrte Frage viel tiefer; sie wird wenigstens teilweise durch den folgenden zweiten Satz (D. § 165, III) beantwortet:

II. Ist der Körper B ein endliches Multiplum des Körpers A, und φ eine Permutation von A, so ist der Grad (B, A) auch die Anzahl aller verschiedenen Permutationen ψ von B, welche Multipla von φ sind; zugleich ist A der Körper, und φ der Rest des Systems $\mathfrak{P}$ dieser Permutationen ψ.

Das bekannteste Beispiel zu diesem Satze ergibt sich aus der Betrachtung des Körpers Z aller Zahlen und des Körpers X aller reellen Zahlen. Offenbar ist $Z = X(i)$, wo i eine Wurzel der quadratischen Gleichung $i^2 + 1 = 0$ bedeutet; die beiden Zahlen 1, i bilden ein nach X irreduzibeles System, jede Zahl in Z ist auf eine einzige Weise in der Form $x_1 + i x_2$ darstellbar, wo x_1, x_2 in X enthalten sind, und folglich ist $(Z, X) = 2$. Bedeutet nun φ die identische Permutation von X, so gibt es wirklich zwei und nur zwei verschiedene Permutationen ψ von Z, die Multipla von φ sind; die eine ist die identische Permutation von Z, während die andere durch $(x_1 + i x_2)\psi = x_1 - i x_2$ definiert ist.

§ 3.

Permutationen des Körpers aller algebraischen Zahlen.

Der zuletzt hervorgehobene Hauptsatz II setzt voraus, daß der Körper B ein endliches Multiplum des Körpers A ist; läßt man diese Voraussetzung fallen, so scheint mir die Beantwortung der Frage, ob jede Permutation φ von A mindestens ein auf B bezügliches Multiplum ψ besitzt, auf die größten Schwierigkeiten zu stoßen. Nehmen wir z. B. den reellen quadratischen Körper $A = R(\sqrt{2})$, welcher aus dem rationalen Körper R durch Adjunktion von $\sqrt{2}$ entsteht, so besitzt A eine nicht identische Permutation φ, durch welche $\sqrt{2}$ in $-\sqrt{2}$ übergeht, und da A ein Divisor des Körpers X aller reellen Zahlen ist, so entsteht die Frage: gibt es ein auf X bezügliches Multiplum von φ? Ich weiß es nicht, doch glaube ich, daß diese Frage zu verneinen ist; die Zahlen des reellen Körpers X scheinen mir durch die Stetigkeit so unlöslich miteinander verbunden zu sein, daß ich vermute, er könne außer der identischen gar keine andere Permutation besitzen, und hieraus würde folgen, daß der Körper Z aller Zahlen nur die beiden, am Schlusse von § 2 genannten Permutationen besitzt. Nach einigen vergeblichen Versuchen, hierüber Gewißheit zu erlangen, habe ich diese Untersuchung aufgegeben; um so mehr würde es mich erfreuen, wenn ein anderer Mathematiker mir eine entscheidende Antwort auf diese Frage mitteilen wollte.

Dieselbe Frage kann aber vollständig beantwortet werden, wenn man sich auf das unstetige Gebiet H aller algebraischen Zahlen beschränkt. Unter einer algebraischen Zahl schlechthin wird hier jede Zahl t verstanden, welche algebraisch in bezug auf den rationalen Körper R, also die Wurzel einer Gleichung

$$t^n + a_1 t^{n-1} + a_2 t^{n-2} + \cdots + a_{n-1} t + a_n = 0$$

mit rationalen Koeffizienten $a_1, a_2 \cdots a_{n-1}, a_n$ ist. Der Inbegriff H aller dieser Zahlen t ist bekanntlich ein Körper, und unter einem algebraischen Körper schlechthin verstehen wir jeden Divisor von H; offenbar ist H kein endliches Multiplum von R, also $(H, R) = \infty$. Wir erwähnen ferner, daß jede mit einer algebraischen Zahl t konjugierte Zahl $t\psi$ (§ 2) ebenfalls algebraisch ist; denn weil die rationalen Koeffizienten $a_1, a_2 \cdots a_n$ durch jede Permutation ψ in sich selbst übergehen, so muß $t\psi$ derselben Gleichung genügen, deren Wurzel t ist. Hierauf schreiten wir zum Beweis des folgenden Existenzsatzes:

III. Ist φ eine Permutation eines algebraischen Körpers A, so besitzt der Körper H aller algebraischen Zahlen mindestens eine Permutation ω, welche Multiplum von φ ist.

Ist H ein endliches Multiplum von A, so ist unser Satz eine unmittelbare Folge des oben (in § 2) erwähnten Hauptsatzes II; wir beschränken uns daher im folgenden auf den entgegengesetzten Fall $(H, A) = \infty$, während (A, R) endlich oder auch unendlich sein kann. Der Beweis beruht dann hauptsächlich auf einer wichtigen Eigenschaft des Körpers H, welche zuerst von G. Cantor*) hervorgehoben ist und darin besteht, daß alle Zahlen dieses Körpers H sich in eine einfach unendliche Reihe

$$h_1, h_2, h_3 \cdots h_r, h_{r+1} \cdots \qquad (h)$$

anordnen lassen, in der Art, daß jeder natürlichen Zahl r eine bestimmte algebraische Zahl h_r, und daß umgekehrt jeder algebraischen Zahl t eine (und nur eine) natürliche Zahl r entspricht, für welche $h_r = t$ wird. Eine solche Anordnung (Abbildung des Körpers H durch die Reihe der natürlichen Zahlen r) läßt sich auf unendlich viele verschiedene Arten herstellen; unserem Beweis legen wir eine bestimmte solche Anordnung (h), gleichgültig welche, zugrunde, und wir nennen die natürliche Zahl r den Index der algebraischen Zahl h_r.

Da nun $(H, A) = \infty$ vorausgesetzt wird, so ist A ein echter Divisor von H, d. h. es gibt in H, also in der Reihe (h) Zahlen, welche nicht in A enthalten sind; unter allen diesen Zahlen gibt es eine völlig bestimmte Zahl $t = h_r$, welche den kleinsten Index r hat, und wir wollen diese Zahl r auch den Index des Körpers A nennen; ist $r > 1$, so sind die der Zahl t vorausgehenden $r - 1$ Zahlen $h_1, h_2 \cdots h_{r-1}$ alle in A enthalten. Da nun die Zahl t auch algebraisch in bezug auf A ist, so entsteht (nach § 1) aus A durch Adjunktion von t ein Körper

$$A_1 = A(t),$$

welcher ein endliches Multiplum von A und zugleich ein Divisor von H ist. Der Kürze halber wollen wir diesen Körper A_1, welcher

*) Über eine Eigenschaft des Inbegriffs aller reellen algebraischen Zahlen (Crelles Journal, Bd. 77). Diesen, auf den Körper H ausgedehnten Satz hatte ich ebenfalls gefunden, aber ich zweifelte an seiner Fruchtbarkeit, bis ich durch den schönen Beweis der Existenz von transzendenten Zahlen, den Cantor in § 2 seiner Abhandlung geführt hat, eines Besseren belehrt wurde.

durch A und die zugrunde gelegte Anordnung (h) völlig bestimmt ist, das nächste Multiplum von A nennen. Der Körper H kann aber kein endliches Multiplum von A_1 sein, weil sonst [nach (2) in § 1] H auch ein endliches Multiplum von A wäre, mithin ist $(H, A_1) = \infty$; man kann daher auf A_1 dieselbe Betrachtung anwenden wie eben auf A, und so entspringt, indem man auf dieselbe Weise fortfährt, aus dem Körper A eine offenbar unendliche Kette (A) von Körpern

$$A,\ A_1,\ A_2 \cdots A_s,\ A_{s+1} \cdots, \qquad (A)$$

in der jedes folgende Glied A_{s+1} das nächste Multiplum des vorhergehenden A_s ist, während sie alle zugleich Divisoren von H sind. Da ferner der Körper $A_1 = A(t)$ außer den schon in A enthaltenen Zahlen $h_1, h_2 \cdots h_{r-1}$ auch noch die neue Zahl $t = h_r$ enthält, so ist sein Index $\geqq r + 1$, und durch Wiederholung desselben Schlusses ergibt sich, daß der Körper A_s gewiß alle diejenigen Zahlen der Reihe (h) enthält, deren Index $< r + s$ ist. Da nun jede algebraische Zahl einen bestimmten endlichen Index hat, so kann man, wenn eine oder mehrere solche Zahlen $u, v \cdots$ in endlicher Anzahl gegeben sind, die natürliche Zahl s immer so groß wählen, daß alle diese Zahlen in dem Körper A_s, mithin auch in allen folgenden Körpern A_{s+1}, $A_{s+2} \cdots$ enthalten sind.

Wir nehmen jetzt an, es sei irgendeine Permutation φ des Körpers A gegeben. Da die Zahl $t = h_r$ nicht in A enthalten, also der endliche Grad $(A_1, A) \geqq 2$ ist, so gibt es nach dem für endliche Multipla geltenden Hauptsatz II (in § 2) immer mehrere verschiedene Permutationen ψ des Körpers $A_1 = A(t)$, welche Multipla von φ sind, und jede dieser Permutationen ψ ist vollständig bestimmt durch die konjugierte Zahl $t\psi$, in welche die Zahl t durch ψ übergeht. An sich wäre es für unseren Beweis ganz gleichgültig, welche von diesen Permutationen ψ, deren Anzahl $= (A_1, A)$ ist, wir auswählen wollen; um aber alles auf völlig bestimmte Regeln zu bringen, verfahren wir folgendermaßen. Da die Zahlen $t\psi$ (wie oben erwähnt ist) ebenfalls algebraisch, also in der Reihe (h) enthalten und außerdem alle voneinander verschieden sind, so setzen wir fest, daß von den Permutationen ψ immer diejenige gewählt werden soll, für welche der Index von $t\psi$ so klein wie möglich ausfällt; diese Permutation von A_1, welche durch φ und die Anordnung (h) völlig bestimmt ist, wollen wir mit φ_1 bezeichnen und das nächste Multiplum der ge-

gebenen Permutation φ nennen. Offenbar kann man nun mit dieser Permutation φ_1 des Körpers A_1 genau so verfahren, wie eben mit der Permutation φ des Körpers A, und durch beständige Fortsetzung dieser Bildung entspringt aus der gegebenen Permutation φ eine unendliche Kette

$$\varphi,\ \varphi_1,\ \varphi_2 \cdots \varphi_s,\ \varphi_{s+1} \cdots, \qquad (\varphi)$$

in der allgemein φ_s eine Permutation von A_s, und φ_{s+1} das nächste Multiplum von φ_s ist.

Nachdem die beiden Ketten (A) und (φ) der Körper A_s und ihrer Permutationen φ_s gebildet sind, gestaltet sich der Beweis unseres Satzes III sehr einfach. Wir definieren eine Abbildung ω des Körpers H auf folgende Weise. Ist u irgendeine algebraische Zahl, so gibt es nach einer früheren Bemerkung in der Kette (A) auch solche Körper A_s, in denen die Zahl u enthalten ist, und wenn n die kleinste Zahl s bedeutet, für welche dies eintritt, so setzen wir fest, daß u durch die Abbildung ω in das Bild

$$u\omega = u\varphi_n$$

übergehen soll; hierdurch ist die Abbildung ω des Körpers H vollständig bestimmt, und wir wollen jetzt beweisen, daß sie eine Permutation von H und zugleich ein Multiplum von φ ist. Zunächst bemerken wir, daß die Zahl u des Körpers A_n auch in allen folgenden Körpern A_{n+1}, $A_{n+2} \cdots$ der Kette (A), also allgemein in A_s enthalten ist, wenn $s \geqq n$ genommen wird, und da φ_s zugleich ein Multiplum von φ_n ist, so folgt aus der Definition von ω auch

$$u\omega = u\varphi_s.$$

Bedeutet nun v ebenfalls eine algebraische Zahl, so kann man s so groß wählen, daß beide Zahlen u, v und folglich auch deren Summe, Differenz, Produkt und Quotient demselben Körper A_s angehören, und hieraus folgt, wie eben bemerkt ist, auch

$$u\omega = u\varphi_s, \quad v\omega = v\varphi_s,$$
$$(u+v)\omega = (u+v)\varphi_s, \quad (u-v)\omega = (u-v)\varphi_s,$$
$$(uv)\omega = (uv)\varphi_s, \quad \left(\frac{u}{v}\right)\omega = \left(\frac{u}{v}\right)\varphi_s;$$

da nun φ_s eine Permutation des Körpers A_s ist, also den in § 2 angegebenen Grundgesetzen gehorcht, so ergibt sich unmittelbar, daß die Abbildung ω des Körpers H denselben Grundgesetzen gehorcht,

also eine Permutation von H ist. Bedeutet ferner a irgendeine Zahl des Körpers A, so ist zufolge der Definition von ω auch $a\omega = a\varphi$, also ist ω ein Multiplum von φ, w. z. b. w.

§ 4.

Verallgemeinerung.

Wir wollen nun den eben bewiesenen Satz III durch die folgenden Bemerkungen vervollständigen und verallgemeinern, wobei wir unter H immer den aus allen algebraischen Zahlen bestehenden Körper verstehen. Zunächst erkennt man leicht, daß der Satz bestehen bleibt, wenn der Körper H durch irgendeinen algebraischen Körper B ersetzt wird, der ein Multiplum des Körpers A ist. Wenn nämlich φ wieder eine Permutation von A ist, so gibt es, wie wir jetzt wissen, mindestens eine Permutation ω von H, welche Multiplum von φ ist; bedeutet nun ψ den auf B bezüglichen Divisor von ω, so ist φ nach einer früheren Bemerkung (§ 2) zugleich der auf A bezügliche Divisor von ψ. Es gilt daher der folgende Satz:

IV. Ist der Körper A ein Divisor des algebraischen Körpers B, so besitzt jede Permutation φ von A mindestens ein auf B bezügliches Multiplum.

Dies ist, falls B ein endliches Multiplum von A ist, offenbar nur ein spezieller Fall des Satzes II (in § 2), welcher zugleich die schärfere Bestimmung enthält, daß der Grad (B, A) die genaue Anzahl aller verschiedenen Permutationen ψ ist. Wir können nun auch leicht beweisen, daß im entgegengesetzten Falle, wenn B kein endliches Multiplum von A ist, die Anzahl der Permutationen ψ von B, welche Multipla derselben Permutation φ von A sind, unendlich groß, also wieder $= (B, A)$ ist, wenn wir die am Schlusse von § 1 festgesetzte Bedeutung des Symbols beibehalten. Hierzu führt die Betrachtung derjenigen Körper A', welche (wie z. B. A selbst) endliche Multipla von A und zugleich Divisoren von B sind. Da jeder solche Körper A' verschieden von B, also ein echter Divisor von B ist, so gibt es in B gewiß solche Zahlen t, die nicht in A' enthalten sind, und folglich entsteht aus A' durch Adjunktion einer solchen algebraischen Zahl t ein Körper $A'' = A'(t)$, der ein endliches Multiplum von A', also auch von A, und zugleich wieder ein Divisor von B ist; da ferner $(A'', A') \geqq 2$, also $(A'', A) = (A'', A')\,(A', A) \geqq 2(A', A)$

ist, so leuchtet ein, daß, wenn m eine gegebene, beliebig große natürliche Zahl bedeutet, unter allen Körpern A' es auch solche gibt, für welche $(A', A) \geqq m$ ist. Nach dem Satze II (in § 2) besitzt ein solcher Körper A' gewiß mindestens m verschiedene Permutationen

$$\varphi'_1, \varphi'_2 \cdots \varphi'_m,$$

welche Multipla der gegebenen Permutation φ von A sind, und da A' ein Divisor von B ist, so besitzt nach dem eben bewiesenen Satze IV jede dieser m Permutationen φ' mindestens ein auf B bezügliches Multiplum ψ; die so erhaltenen m Permutationen

$$\psi_1, \psi_2 \cdots \psi_m$$

sind folglich auch Multipla von φ, und sie sind alle voneinander verschieden, weil jede Permutation ψ von B nur einen einzigen, völlig bestimmten, auf A' bezüglichen Divisor φ' besitzt. Da m beliebig groß genommen werden kann, so ergibt sich, daß die Anzahl aller verschiedenen Permutationen ψ von B, welche Multipla derselben Permutation φ von A sind, unendlich groß, also $= (B, A)$ ist, w. z. b. w.

Unter derselben Voraussetzung wollen wir endlich noch zeigen, daß auch der letzte Teil des Satzes II (in § 2) bestehen bleibt. Das System $\mathfrak{P}$ aller Permutationen ψ von B, welche Multipla der Permutation φ von A sind, besitzt (nach dem Satze I in § 2) einen bestimmten größten gemeinsamen Divisor oder Rest χ, und da φ ein gemeinsamer Divisor aller Permutationen ψ, also auch Divisor von χ ist, so ist der Körper C dieser Permutation χ ein Multiplum von A und zugleich Divisor von B. Machen wir nun die Annahme, C sei verschieden von A, also $(C, A) \geqq 2$, so besitzt C, wie eben bewiesen ist, mindestens eine von χ verschiedene Permutation χ', welche ebenfalls Multiplum von φ ist; da ferner C Divisor von B ist, so hat B mindestens eine Permutation ψ', welche Multiplum von χ', also auch von φ ist und folglich auch dem System $\mathfrak{P}$ angehört; mithin muß χ als Rest von $\mathfrak{P}$ auch Divisor von ψ' sein; es besäße daher ψ' zwei verschiedene, auf denselben Körper C bezügliche Divisoren χ, χ', was unmöglich ist. Unsere obige Annahme, die Körper A, C seien verschieden, ist daher unzulässig, und hieraus folgt offenbar, daß $\chi = \varphi$ ist. Hiernach können wir den obigen Satz IV in folgender Weise vervollständigen:

V. Ist der Körper A ein Divisor des algebraischen Körpers B, und φ eine Permutation von A, so ist der Grad (B, A), mag er

endlich oder unendlich sein, die Anzahl aller verschiedenen Permutationen ψ von B, welche Multipla von φ sind; zugleich ist A der Körper, und φ der Rest des Systems $\mathfrak{P}$ dieser Permutationen ψ.

§ 5.

Gruppen von Permutationen.

Aus dem Vorhergehenden folgt unmittelbar, daß der Körper H, welcher aus allen algebraischen Zahlen besteht, unendlich viele verschiedene Permutationen ω besitzt. Da nun jede in H enthaltene Zahl t durch eine Permutation ω wieder in eine algebraische Zahl $t\omega$ übergeht, so ist der mit H konjugierte Körper $H\omega$ gewiß ein Divisor von H, aber wir können leicht zeigen, daß immer $H\omega = H$ ist. Denn betrachtet man wieder irgendeine mit rationalen Koeffizienten behaftete Gleichung, deren Wurzel eine gegebene algebraische Zahl t ist, und bezeichnet mit $t_1, t_2 \cdots t_m$ alle diejenigen m Wurzeln dieser Gleichung, die voneinander verschieden sind, so gehören dieselben auch dem Körper H an, und sie gehen (wie in § 2 erwähnt ist) durch ω in ebenso viele verschiedene Zahlen $t_1\omega, t_2\omega \cdots t_m\omega$ über; da die letzteren aber derselben Gleichung genügen, so muß eine von ihnen mit der gegebenen Zahl t übereinstimmen, mithin ist jede Zahl t des Körpers H auch in $H\omega$ enthalten, woraus offenbar die obige Behauptung $H\omega = H$ folgt. Diese Eigenschaft des Körpers H, durch jede seiner Permutationen in sich selbst überzugehen, bezeichnen wir dadurch, daß wir ihn einen Normalkörper nennen (vgl. D. § 166). Eine unmittelbare Folge, oder vielmehr nur eine andere Ausdrucksform dieser Eigenschaft besteht darin, daß die Umkehrung ω^{-1} einer jeden Permutation ω von H ebenfalls eine Permutation von H ist (§ 2).

Es ist nun an der Zeit, noch einen Begriff aus der allgemeinen Theorie der Körper-Permutationen in Erinnerung zu bringen, nämlich den ihrer Zusammensetzung (D. § 162). Hierbei beschränken wir uns der Kürze halber auf den folgenden speziellen Fall*). Es sei M

*) Ich will hier beiläufig bemerken, daß man die Resultante $\varphi\psi$ auch ganz allgemein erklären kann, wenn φ, ψ Permutationen von zwei beliebigen Körpern A, B sind; es gibt einen und nur einen Divisor A' von A, welcher durch φ in den größten gemeinsamen Divisor von $A\varphi$ und B übergeht, und die Resultante $\varphi\psi$ wird als Permutation dieses Körpers A' durch $x(\varphi\psi) = (x\varphi)\psi$ definiert, wo x jede Zahl in A' bedeutet. Die beiden Sätze $(\varphi\psi)^{-1} = \psi^{-1}\varphi^{-1}$ und $(\varphi\psi)\chi = \varphi(\psi\chi)$ behalten ihre Gültigkeit, während andere Sätze gewisse Modifikationen erfordern.

ein beliebiger Körper, und $\mathfrak{E}$ der Inbegriff aller derjenigen Permutationen ε von M, durch welche M in sich selbst übergeht, welche also der Bedingung $M\varepsilon = M$ genügen; es gibt immer wenigstens eine solche, nämlich die identische Permutation M_0 von M, und jede Umkehrung ε^{-1} ist ebenfalls in $\mathfrak{E}$ enthalten. Je zwei (gleiche oder verschiedene) solche Permutationen φ, ψ erzeugen eine Resultante $\varphi\psi$, welche für jede in M enthaltene Zahl x durch

$$x(\varphi\psi) = (x\varphi)\psi$$

definiert wird und ebenfalls eine in $\mathfrak{E}$ enthaltene Permutation von M ist. Hieraus folgen die beiden Sätze

$$(\varphi\psi)^{-1} = \psi^{-1}\varphi^{-1},\ (\varphi\psi)\chi = \varphi(\psi\chi),$$

wo χ ebenfalls jede in $\mathfrak{E}$ enthaltene Permutation bedeutet, und die Resultante $\varphi\varphi^{-1}$ ist die identische Permutation M_0. Ein in $\mathfrak{E}$ enthaltenes System $\mathfrak{A}$ von Permutationen α heißt eine Gruppe, wenn 1. die Resultanten von je zwei Permutationen α und 2. alle Umkehrungen α^{-1} demselben System $\mathfrak{A}$ angehören, und sie heißt endlich oder unendlich, je nachdem die Anzahl der Permutationen α endlich oder unendlich ist; im ersteren Falle findet man leicht, daß die Bedingung 2. schon eine notwendige Folge der Bedingung 1. ist. Der Inbegriff $\mathfrak{E}$ ist selbst eine Gruppe, und ebenso bildet die identische Permutation M_0 für sich allein eine Gruppe, welche in jeder Gruppe $\mathfrak{A}$ enthalten ist. Für endliche Gruppen gilt nun der folgende Fundamentalsatz (D. § 166, I):

VI. Besteht eine endliche Gruppe $\mathfrak{A}$ aus n Permutationen des Körpers M, und ist A der Körper von $\mathfrak{A}$, so ist $(M, A) = n$, also M ein endliches Multiplum von A, und der Rest von $\mathfrak{A}$ ist die identische Permutation A_0 von A. Zugleich folgt aus dem Satze II (in § 2), daß die Gruppe $\mathfrak{A}$ auch der Inbegriff aller auf M bezüglichen Multipla von A_0 ist.

Man überzeugt sich leicht, daß dieser Satz VI in Verbindung mit dem Satze II (in § 2) die Theorie von Galois vollständig in sich schließt. Um dies etwas näher auszuführen, nehmen wir an, die obige Gruppe $\mathfrak{E}$ sei endlich, woraus natürlich auch die Endlichkeit jeder in $\mathfrak{E}$ enthaltenen Gruppe $\mathfrak{A}$ folgt. Bedeutet E den Körper der Gruppe $\mathfrak{E}$, und E_0 seine identische Permutation, so ist M nach VI

ein endliches Multiplum von E, der Rest von $\mathfrak{E}$ ist E_0, und umgekehrt ist $\mathfrak{E}$ der Inbegriff aller auf M bezüglichen Multipla von E_0. Der Kern der Theorie von Galois besteht nun darin, daß einerseits die Körper A, welche Divisoren von M und zugleich Multipla von E sind, und andererseits die in $\mathfrak{E}$ enthaltenen Gruppen $\mathfrak{A}$ sich gegenseitig eindeutig entsprechen. Erstens besitzt jede solche Gruppe $\mathfrak{A}$ einen bestimmten Körper A, welcher aus allen zu $\mathfrak{A}$ einwertigen Zahlen des Körpers M besteht, also ein Divisor von M ist, und da jede in E enthaltene, also zu $\mathfrak{E}$ einwertige Zahl auch einwertig zu $\mathfrak{A}$ ist, so ist A auch Multiplum von E. Da ferner $\mathfrak{A}$ nach VI der Inbegriff aller auf M bezüglichen Multipla der identischen Permutation A_0 von A ist, so haben zwei verschiedene Gruppen $\mathfrak{A}$ auch zwei verschiedene Körper A. Wir haben daher zweitens nur noch zu zeigen, daß umgekehrt jeder Körper A, welcher Divisor von M und Multiplum von E ist, auch wirklich der Körper einer in $\mathfrak{E}$ enthaltenen Gruppe $\mathfrak{A}$ ist. Zunächst folgt aus dem in § 1 erwähnten Satze $(M, E) = (M, A)(A, E)$, daß M ein endliches Multiplum von A ist; mithin ist der Grad (M, A) nach dem Satze II (in § 2) auch die Anzahl aller derjenigen Permutationen α von M, welche Multipla der identischen Permutation A_0 von A sind, und zugleich ist A der Körper, A_0 der Rest des Systems $\mathfrak{A}$ dieser Permutationen α. Wir brauchen also nur noch zu beweisen, daß dieses System $\mathfrak{A}$ eine in $\mathfrak{E}$ enthaltene Gruppe ist. Da A Multiplum von E, also E_0 der auf E bezügliche Divisor von A_0 ist, so ist jede Permutation α auch Multiplum von E_0 und folglich in der Gruppe $\mathfrak{E}$ enthalten. Bedeutet ferner x jede Zahl des Körpers A, so ist $x = xA_0 = x\alpha$, also auch $x\alpha^{-1} = x$, und wenn α_1, α_2 zwei solche Permutationen α sind, so folgt hieraus auch $x(\alpha_1\alpha_2) = (x\alpha_1)\alpha_2 = x\alpha_2 = x$, also gehört die Resultante $\alpha_1\alpha_2$ demselben System $\mathfrak{A}$ an, welches folglich eine Gruppe ist, w. z. b. w.

Aus der hiermit nachgewiesenen Korrespondenz zwischen den Körpern A und den Gruppen $\mathfrak{A}$ fließen unmittelbar die übrigen Sätze der Theorie von Galois, welche von den Beziehungen zwischen mehreren solchen Körpern A und von den entsprechenden Beziehungen zwischen den zugehörigen Gruppen $\mathfrak{A}$ handeln (D. § 166). Auf alles dies brauchen wir, weil es hinreichend bekannt ist, hier nicht einzugehen, und wir haben auch das Vorstehende nur deshalb wieder in Erinnerung gebracht, um jetzt auf das abweichende Verhalten unendlicher Permutationsgruppen aufmerksam zu machen.

§ 6.

Unendliche Gruppen von Permutationen.

Wir haben gesehen, daß der aus allen algebraischen Zahlen bestehende Körper H unendlich viele Permutationen ω besitzt, und daß er durch jede von ihnen in sich selbst übergeht; diese Permutationen ω bilden daher eine unendliche Gruppe, die wir mit $\mathfrak{G}$ bezeichnen wollen, und wir fragen, ob wohl auch hier eine gegenseitig eindeutige Korrespondenz zwischen den algebraischen Körpern A (den Divisoren von H) und den in $\mathfrak{G}$ enthaltenen Gruppen $\mathfrak{A}$ besteht.

Geht man von irgendeinem algebraischen Körper A aus, und bezeichnet mit A_0 dessen identische Permutation, so gibt es nach dem Satze V (in § 4), welcher hier den Satz II (in § 2) vollständig ersetzt, immer Permutationen α des Körpers H, welche Multipla von A_0 sind; mag ihre Anzahl (H, A) endlich oder unendlich sein, immer ist A der Körper, und A_0 der Rest des Systems $\mathfrak{A}$ dieser Permutationen α. Da ferner A_0 eine identische Permutation ist, so findet man leicht (wie zuletzt in § 5), daß dieses in $\mathfrak{G}$ enthaltene System $\mathfrak{A}$ eine Gruppe ist; wir wollen sie die Identitätsgruppe des Körpers A nennen. Da ferner, wie schon bemerkt, A der Körper von $\mathfrak{A}$ ist, so folgt, daß zwei verschiedene Körper A auch zwei verschiedene Identitätsgruppen $\mathfrak{A}$ haben. Die oben aufgeworfene Frage würde daher zu bejahen sein, wenn man beweisen könnte, daß jede in $\mathfrak{G}$ enthaltene Gruppe $\mathfrak{A}$ die Identitätsgruppe eines Körpers A ist, was ja für endliche Gruppen $\mathfrak{A}$ nach dem Satze VI (in § 5) wirklich der Fall ist. Nun hat zwar auch jede unendliche Gruppe $\mathfrak{A}$ einen bestimmten Körper A, der Divisor von H, also algebraisch ist, und da in $\mathfrak{A}$ immer die identische Permutation von H enthalten ist, so ist der Rest von $\mathfrak{A}$ gewiß die identische Permutation A_0 dieses Körpers A, also enthält $\mathfrak{A}$ nur solche Permutationen α von H, welche auch in der Identitätsgruppe $\mathfrak{A}'$ des Körpers A enthalten sind; aber es fehlt der Nachweis, daß umgekehrt jede in $\mathfrak{A}'$ enthaltene Permutation α', d. h. jedes auf H bezügliche Multiplum von A_0 auch in der gegebenen Gruppe $\mathfrak{A}$ enthalten ist, oder anders ausgedrückt, daß die Körper zweier verschiedener Gruppen auch verschieden sind. Dies habe ich anfangs für sehr wahrscheinlich gehalten, und erst nach mehreren vergeblichen Versuchen, es zu beweisen, ist es mir gelungen, mich von der Unrichtigkeit dieser Vermutung durch ein Beispiel zu

überzeugen, welches ich zum Schluß dieser Arbeit jetzt noch mitteilen will.

Dieses Beispiel bezieht sich nicht auf den vollen Körper H, sondern auf die einfachste Klasse unendlicher Kreiskörper. Ist p eine bestimmte natürliche Primzahl, so entspricht jeder natürlichen Zahl n eine bestimmte Einheitswurzel

$$u_n = \cos\frac{2\pi}{p^n} + i\sin\frac{2\pi}{p^n}, \tag{1}$$

und wir wollen mit P_n den durch sie erzeugten Kreiskörper $R(u_n)$ vom Grade $\varphi(p^n) = (p-1)p^{n-1}$ bezeichnen, während P_0 der Körper R der rationalen Zahlen ist. Aus

$$u_n = u_{n+1}^p \tag{2}$$

folgt, daß in der unendlichen Kette von Körpern

$$P_0,\ P_1,\ P_2,\ P_3 \cdots$$

jedes Glied P_n Divisor des nächstfolgenden P_{n+1}, also auch jedes folgenden Gliedes P_{n+s} ist.

Wenn irgendeine Kette von Körpern P_n vorliegt, welche diese letztere Eigenschaft besitzt, so kann ihr kleinstes gemeinsames Multiplum M keine anderen als solche Zahlen t enthalten, die schon mindestens einem Körper P_n und also auch allen folgenden Körpern P_{n+s} angehören; denn der Inbegriff aller dieser Zahlen t bildet, wie man leicht findet, wirklich einen Körper, welcher offenbar ein Divisor von M, zugleich aber auch Multiplum aller P_n, also auch Multiplum von M, mithin $= M$ ist; man kann daher dieses Multiplum M zweckmäßig auch mit P_∞ bezeichnen. Ist nun ε irgendeine Permutation von M und ε_n der auf P_n bezügliche Divisor von ε, so entsteht eine unendliche Kette von Permutationen

$$\varepsilon_0,\ \varepsilon_1,\ \varepsilon_2,\ \varepsilon_3 \cdots,$$

in der jedes Glied ε_n Divisor aller folgenden Glieder ε_{n+s} ist. Umgekehrt, wenn eine bestimmte Kette von Permutationen ε_n der Körper P_n vorliegt, welche diese letztere Eigenschaft besitzt, so folgt aus der oben besprochenen Konstitution des Körpers M leicht (wie in § 3), daß es eine und nur eine Permutation ε von M gibt, welche Multiplum aller dieser Permutationen ε_n ist.

Wenden wir dies auf unseren Fall der Kreiskörper $P_n = R(u_n)$ an, und bezeichnen mit $\mathfrak{E}$ den Inbegriff aller Permutationen ε ihres

kleinsten Multiplums $M = P_\infty$, so ist der auf P_n bezügliche Divisor ε_n von ε völlig bestimmt durch die mit u_n konjugierte Zahl $u_n \varepsilon_n = u_n \varepsilon$, und diese ist bekanntlich immer eine Potenz von u_n, deren Exponent eine durch p nicht teilbare Zahl ist und durch jede nach dem Modul p^n kongruente Zahl ersetzt werden darf; bezeichnen wir diese Zahl mit (n, ε), so wird daher

$$u_n \varepsilon_n = u_n \varepsilon = u_n^{(n, \varepsilon)}, \tag{3}$$

und da aus (2) auch

$$u_n \varepsilon = (u_{n+1} \varepsilon)^p,$$

also

$$u_n^{(n, \varepsilon)} = u_{n+1}^{p(n+1, \varepsilon)} = u_n^{(n+1, \varepsilon)}$$

folgt, so ist

$$(n, \varepsilon) \equiv (n + 1, \varepsilon) \pmod{p^n}, \tag{4}$$

und diese Kongruenz drückt aus, daß ε_n Divisor von ε_{n+1} ist. Umgekehrt, wenn eine Kette von solchen, durch p nicht teilbaren Zahlen (n, ε) vorliegt, welche den Bedingungen (4) genügen, so folgt aus den obigen allgemeinen Bemerkungen, daß ihr eine und nur eine Permutation ε von M entspricht, welche durch (3) bestimmt ist. Hierbei darf man festsetzen, daß (n, ε) positiv und kleiner als p^n sein soll, und wenn man $(n + 1, \varepsilon) = (n, \varepsilon) + c_n p^n$ setzt, so wird $0 \leqq c_n < p$; jede willkürlich gewählte unendliche Reihe von solchen Zahlen $c_1, c_2, c_3 \cdots$ liefert in Verbindung mit jeder der $p - 1$ Zahlen $(1, \varepsilon)$ eine bestimmte Permutation ε, und hieraus folgt, daß der Inbegriff $\mathfrak{E}$ aller ε in gewissem Sinne eine stetige Mannigfaltigkeit bildet, worauf wir hier nicht weiter eingehen.

Bekanntlich geht der Körper P_n durch jede Permutation in sich selbst über, es ist also $P_n \varepsilon = P_n \varepsilon_n = P_n$, und hieraus folgt offenbar auch $M \varepsilon = M$, mithin bildet der Inbegriff $\mathfrak{E}$ (nach § 5) eine Gruppe. Sind ε, ε', also auch $\varepsilon\varepsilon'$ in $\mathfrak{E}$ enthalten, so folgt aus (3)

$$u_n(\varepsilon\varepsilon') = (u_n \varepsilon)\varepsilon' = (u_n \varepsilon')^{(n, \varepsilon)} = u_n^{(n, \varepsilon)(n, \varepsilon')},$$

also

$$(n, \varepsilon\varepsilon') \equiv (n, \varepsilon)(n, \varepsilon') \pmod{p^n}, \tag{5}$$

und da die rechte Seite sich durch Vertauschung von ε, ε' nicht ändert, so folgt, daß

$$\varepsilon\varepsilon' = \varepsilon'\varepsilon, \tag{6}$$

also $\mathfrak{E}$ eine Abelsche Gruppe ist.

Jede Permutation ε erzeugt durch wiederholte Zusammensetzung mit sich selbst und ihrer Umkehrung ε^{-1} die Reihe aller Potenzen ε^r,

welche eine Gruppe bilden, die wir mit $[\varepsilon]$ bezeichnen wollen. Von einigem Interesse ist nun die Frage, ob es außer der identischen Permutation M_0 von M, welche für sich allein eine Gruppe bildet, noch andere endliche, d. h. solche Permutationen α gibt, die eine endliche Gruppe $[\alpha]$ erzeugen. Bedeutet m die Anzahl der in einer solchen Gruppe $[\alpha]$ enthaltenen verschiedenen Permutationen α^r, so ist bekanntlich $\alpha^m = M_0$, und umgekehrt, wenn eine natürliche Zahl m diese Bedingung erfüllt, so folgt hieraus, daß α endlich ist. Diese Forderung drückt sich nach (3), (4), (5) dadurch aus, daß α für jede natürliche Zahl n den Bedingungen

$$(7) \qquad (n, \alpha)^m \equiv 1, \ (n, \alpha) \equiv (n+1, \alpha) \ (\text{mod. } p^n)$$

genügen muß. Schließt man den Fall $p = 2$ aus, so ergibt die genaue Untersuchung, welche keine erheblichen Schwierigkeiten darbietet, daß es nur $p-1$ endliche Permutationen α gibt; diese sind durch

$$(8) \qquad (n, \alpha) \equiv (1, \alpha)^{p^{n-1}} \ (\text{mod. } p^n)$$

bestimmt, und man erhält sie alle, wenn man $(1, \alpha)$ irgendein vollständiges System nach p inkongruenter Zahlen durchlaufen läßt, welche nicht durch p teilbar sind; die entsprechenden Zahlen (n, α) bilden alle $p-1$ Wurzeln x_n der Kongruenz

$$(9) \qquad x_n^{p-1} \equiv 1 \ (\text{mod. } p^n),$$

und hieraus folgt, daß diese $p-1$ Permutationen α die Bedingung

$$(10) \qquad \alpha^{p-1} = M_0$$

erfüllen. Sie bilden eine Gruppe $\mathfrak{A}$, und wenn man für $(1, \alpha)$ eine primitive Wurzel der Primzahl p wählt, so ist diese Gruppe $\mathfrak{A} = [\alpha]$. Bedeutet ferner A den Körper von $\mathfrak{A}$, so folgt aus dem Satze VI (in § 5), daß $(M, A) = p-1$, also M ein endliches Multiplum von A ist*).

Es ist nun auch nicht schwer, alle endlichen und unendlichen Divisoren des Körpers M aufzufinden und die zugehörigen, in $\mathfrak{E}$ enthaltenen Identitätsgruppen zu bestimmen. Der Kürze wegen verzichten wir hierauf, und wir wollen nur noch zum Schluß an einem Beispiel den oben versprochenen Nachweis liefern, daß nicht jede in $\mathfrak{E}$

*) In dem oben ausgeschlossenen Falle $p = 2$ findet man leicht, daß es zwei endliche Permutationen von M gibt, nämlich die identische und eine andere, durch welche jede Einheitswurzel u_n in u_n^{-1} übergeht.

enthaltene Gruppe eine Identitätsgruppe ist, oder anders ausgedrückt, daß zwei verschiedene Gruppen denselben Körper haben können.

Wir bezeichnen mit g eine bestimmt gewählte primitive Wurzel aller Potenzen der (ungeraden) Primzahl p und definieren eine Permutation β unseres Körpers M durch die für jede natürliche Zahl n geltende Kongruenz

$$(n, \beta) \equiv g \pmod{p^n},$$

wodurch die Existenz-Bedingung (4) erfüllt ist. Bedeutet β_n wieder den auf P_n bezüglichen Divisor von β, so ist also

$$u_n \beta_n = u_n^g, \; u_n \beta_n^r = u_n^{g^r},$$

und da die Potenzen

$$g, g^2, g^3 \cdots g^{\Phi(p^n)}$$

nach dem Modul p^n ein vollständiges System inkongruenter, durch p nicht teilbarer Zahlen bilden, so erschöpfen die Potenzen

$$\beta_n, \beta_n^2, \beta_n^3 \cdots \beta_n^{\Phi(p^n)}$$

alle Permutationen des endlichen Körpers P_n; mithin muß nach einem bekannten Satze (oder nach II in § 2) jede in P_n enthaltene Zahl t, welche der Bedingung $t\beta = t$, also auch den Bedingungen $t\beta^r = t$ genügt, rational sein, also dem Körper R angehören. Wir kehren nun zu der Permutation β des Körpers M zurück, betrachten die aus allen Potenzen von β bestehende Gruppe $\mathfrak{B} = [\beta]$ und suchen deren Körper, d. h. den Inbegriff B aller zu $\mathfrak{B}$ einwertigen Zahlen t des Körpers M; diese Einwertigkeit wird schon vollständig durch die Forderung $t\beta = t$ ausgedrückt, weil hieraus auch $t\beta^{-1} = t$ und allgemein $t\beta^r = t$ folgt. Da nun, wie früher bemerkt, jede Zahl t des unendlichen Körpers M gewiß auch einem endlichen Körper P_n angehört, woraus $t\beta = t\beta_n$ folgt, so muß t auch der Bedingung $t\beta_n = t$ genügen und folglich rational sein, mithin ist $B = R$. Andererseits leuchtet aber ein, daß die Identitätsgruppe von R, d. h. der Inbegriff aller auf M bezüglichen Multipla der identischen Permutation R_0 die volle Gruppe $\mathfrak{E}$ aller Permutationen ε von M, und daß R der Körper dieser Gruppe $\mathfrak{E}$ ist, weil jede zu $\mathfrak{E}$ einwertige Zahl auch einwertig zu $\mathfrak{B}$ sein muß. Daß endlich die in $\mathfrak{E}$ enthaltene Gruppe $\mathfrak{B}$ verschieden von $\mathfrak{E}$ ist, ergibt sich schon daraus, daß von den oben gefundenen $p - 1$ endlichen Permutationen α nur eine einzige, nämlich die identische Permutation M_0 in $\mathfrak{B}$ enthalten ist. Also haben die beiden verschiedenen Gruppen $\mathfrak{B}$ und $\mathfrak{E}$ denselben Körper R, w. z. b. w.

Zusatz aus dem Nachlaß:

Bestimmung der Divisoren von M und ihrer Identitätsgruppen.

Wir suchen jetzt alle Divisoren D von M. Enthält D eine Zahl μ vom Exponenten p^s (wo $s \geqq 1$)*), so ist D als Multiplum von $R(\mu) = A_s \cdot Q_e$**) auch Multiplum von A_s. Gibt es daher in D Zahlen μ, deren Exponent p^s jeden gegebenen Wert übertrifft, so ist D gemeinsames Multiplum aller A_s und folglich auch ein Multiplum von A, mithin

$$(M, A) = (M, D) \cdot (D, A) = p - 1,$$
$$(D, A) = e, \quad (M, D) = f; \quad p - 1 = e \cdot f$$

und folglich (leicht)

$$D = A \cdot Q_e.$$

Im entgegengesetzten Fall ist D kein Multiplum von A; dann gibt es eine Zahl s von der Art, daß A_s Divisor von D, aber A_{s+1} nicht Divisor von D ist; mithin sind die Exponenten aller in D enthaltenen Zahlen $\leqq p^s$, d. h. D ist Divisor von $P_s = A_s \cdot P_1$, also D ein endlicher Körper,

$$D = A_s \cdot Q_e. \quad [\text{Im Falle } s = 0 \text{ ist } D = R.]$$

Identitätsgruppen der Unterkörper von M.

Körper $M_{s,e} = A_s \cdot Q_e$; $p - 1 = e \cdot f$.

Identitätsgruppe $\mathfrak{E}_{s,e}$: Alle Permutationen ε von M, die Multipla der identischen Permutation von $A_s \cdot Q_e$ sind.

$$u_n \varepsilon = u_n^{(n,\varepsilon)}; \quad (n, \varepsilon) \equiv (1, \varepsilon)^{p^n - 1} \pmod{p^n},$$
$$(s, \varepsilon)^f \equiv 1 \pmod{p^s}.$$

Körper $A \cdot Q_e$; Identitätsgruppe $\mathfrak{E}_{\infty,e}$:

$$u_n \varepsilon = u_n^{(n,\varepsilon)}; \quad (n, \varepsilon) \equiv (1, \varepsilon)^{p^n - 1} \pmod{p^n},$$
$$(1, \varepsilon)^f \equiv 1 \pmod{p}.$$

*) Jede Zahl μ in M hat einen bestimmten Exponenten p^s, d. h. sie ist in P_s, aber nicht in P_{s-1} enthalten.

**) Bezeichnet man, wenn e jeden Divisor von $p - 1 = e \cdot f$ bedeutet, mit Q_e den in P_1 enthaltenen Körper vom Grade e, so sind alle endlichen Körper, die in M enthalten sind, von der Form

$$A_s \cdot Q_e \quad [s = 1, 2, \cdots],$$

wo A_s der Durchschnitt des Körpers A mit P_s ist.

Erläuterungen zur vorstehenden Abhandlung.

In einem Brief an Frobenius (18. April 1897) schreibt Dedekind, nachdem er einen kurzen Überblick über den Inhalt der Arbeit gegeben hatte: „Für die unendlichen Körper hat bisher ein Noli me tangere gegolten; nur deshalb möchte ich gern einmal von ihnen sprechen."

Seitdem hat die Entwicklung der Algebra dieses „Noli me tangere" überwunden: Auf Grund der Steinitzschen Theorie der Körper konnte für beliebige unendliche Körper die volle Automorphismengruppe aufgestellt werden, im wesentlichen nach der Dedekindschen Methode; nur daß eine beliebige Wohlordnung zugrunde gelegt werden muß, und neben der algebraischen noch eine vorher abzuspaltende rein transzendente Erweiterung zu berücksichtigen ist. Dabei treten im Fall der komplexen Zahlen neben dem Übergang zum konjugiert Komplexen noch beliebig viele, allerdings „extrem unstetige" Abbildungen auf, entgegen der von Dedekind am Anfang von § 3 ausgesprochenen Vermutung [vgl. dazu A. Ostrowski, Journ. f. Math. **143** (1913); E. Noether, Math. Ann. **77** (1916); in geometrischer Einkleidung der Fragestellung: H. Lebesgue, Atti Torino **42** (1907); E. Kamke, Jahresber. d. d. Math.-Ver. **36** (1927)].

Die Galoissche Theorie der unendlichen Körper ist von W. Krull im engen Anschluß an Dedekind entwickelt [Math. Ann. **100** (1928)]. Bei geeigneter Topologisierung — die sich im abzählbaren Fall direkt aus den Dedekindschen Fundamentalfolgen ergibt — zeigt sich, daß alle und nur die abgeschlossenen Untergruppen „Identitätsgruppen" sind, und daß bei jedem unendlichen Körper (erster Art) auch Nicht-Identitätsgruppen auftreten, entsprechend dem Dedekindschen Beispiel. Auch der Zusammenhang mit den p-adischen Zahlen, der sich schon deutlich bei Dedekind zeigt, kehrt allgemein bei allen „idealzyklischen" Gruppen wieder.

Die von Dedekind selbst noch nicht betrachtete Idealtheorie der unendlichen Körper ist seither ebenfalls entwickelt: in den Grundzügen durch E. Stiemke [Math. Zeitschr. **25** (1926)], unter ausdrücklicher Berufung auf die Methoden der vorliegenden Abhandlung, und weitergehend durch W. Krull [Math. Zeitschr. **29** (1928) und **31** (1930)].

Noether.

XXXII.

Gauß in seiner Vorlesung über die Methode der kleinsten Quadrate.

[Festschrift zur Feier des hundertfünfzigjährigen Bestehens der Königlichen Gesellschaft der Wissenschaften zu Göttingen. Beiträge zur Gelehrtengeschichte Göttingens. S. 45—59 (1901).]

Als geborener Braunschweiger habe ich schon früh von Gauß sprechen hören, und ich glaubte gern an seine Größe, ohne zu wissen, worin sie bestand. Um so tieferen Eindruck machte es auf mich, als ich zuerst von seiner geometrischen Darstellung der imaginären oder, wie man zu jener Zeit wohl noch sagte, der unmöglichen Größen hörte. Ich war damals als Student auf dem Collegium Carolinum (der heutigen Technischen Hochschule) ein wenig in die höhere Mathematik eingedrungen, und bald darauf, als Gauß im Juli 1849 sein 50jähriges Doktor-Jubiläum feierte, sandte unser Lehrkörper einen von dem geistreichen Philologen Petri verfaßten Glückwunsch an ihn, worin mir der Passus, er habe das Unmögliche möglich gemacht, ganz besonders gefiel. Zu Ostern 1850 kam ich nach Göttingen, und hier wuchs mein Verständnis schon etwas mehr, als ich im Seminar durch eine kurze, aber sehr interessante Vorlesung von Stern in die Elemente der Zahlentheorie eingeführt wurde und den Reziprozitätssatz kennen lernte. Auf meinen Wegen nach oder von der Sternwarte, wo ich eine Vorlesung des trefflichen Professors Goldschmidt über populäre Astronomie hörte, begegnete ich zuweilen Gauß und erfreute mich des Anblicks seiner stattlichen, Ehrfurcht gebietenden Erscheinung, und sehr oft sah ich ihn in größter Nähe auf seinem festen Platze im Literarischen Museum, das er regelmäßig besuchte, um Zeitungen zu lesen.

Zu Anfang des folgenden Wintersemesters hielt ich mich für reif, seine Vorlesung über die Methode der kleinsten Quadrate zu hören, und so betrat ich, mit dem Testierbuch ausgerüstet und nicht ohne

Herzklopfen, zum ersten Male sein Wohnzimmer, wo ich ihn an seinem Schreibtisch sitzend fand. Meine Meldung schien ihn wenig zu erfreuen, ich hatte auch wohl gehört, daß er sich ungern entschloß, Vorlesungen zu halten; nachdem er seinen Namen in das Buch eingetragen hatte, sagte er nach kurzem Schweigen: „Sie wissen vielleicht, daß es immer sehr zweifelhaft ist, ob meine Vorlesungen zustande kommen; wo wohnen Sie? bei dem Barbier Vogel? Nun, das trifft sich ja glücklich, denn der ist auch mein Barbier, durch ihn werde ich Sie benachrichtigen."

Einige Tage darauf trat dann Vogel, eine stadtbekannte Persönlichkeit, ganz erfüllt von der Wichtigkeit seiner Mission, bei mir ein, um zu bestellen, daß sich noch mehrere Zuhörer gemeldet hätten, und daß Herr Geh. Hofrat Gauß die Vorlesung halten würde.

Wir waren neun Studenten, von denen ich A. Ritter (später Professor der Mechanik in Hannover und Aachen) und Moritz Cantor (später Professor in Heidelberg) nach und nach näher kennen lernte; wir alle kamen sehr regelmäßig, es hat wohl selten einer von uns gefehlt, obgleich der Weg nach der Sternwarte im Winter bisweilen nicht angenehm war. Das Auditorium war durch ein Vorzimmer von Gauß' Arbeitszimmer getrennt und ziemlich klein. Wir saßen an einem Tisch, dessen Längsseiten für je drei, aber nicht für vier Personen bequemen Platz darboten. Der Tür gegenüber am oberen Ende saß Gauß in mäßiger Entfernung vom Tische, und wenn wir vollzählig waren, so mußten zwei von uns, die zuletzt kamen, ganz in seine Nähe rücken und ihr Heft auf den Schoß nehmen. Gauß trug ein leichtes schwarzes Käppchen, einen ziemlich langen braunen Gehrock, graue Beinkleider; er saß meist in bequemer Haltung, etwas gebeugt vor sich niedersehend, mit über dem Leib gefalteten Händen. Er sprach ganz frei, sehr deutlich, einfach und schlicht; wenn er aber einen neuen Gesichtspunkt hervorheben wollte, wobei er ein besonders charakteristisches Wort gebrauchte, so erhob er wohl plötzlich den Kopf, wandte sich zu einem seiner Nachbarn und blickte ihn während der nachdrücklichen Rede ernst mit seinen schönen, durchdringenden blauen Augen an. Das war unvergeßlich. Seine Sprache war fast ganz dialektfrei, nur bisweilen kamen Anklänge an unsere stadt-braunschweigische Mundart; beim Zählen z. B., wobei er auch den Gebrauch der Finger nicht verschmähte, sagte er nicht eins, zwei, drei, sondern eine, zweie, dreie usf., wie man es

noch jetzt bei uns auf dem Markte hören kann. Ging er von einer prinzipiellen Erörterung zur Entwicklung mathematischer Formeln über, so erhob er sich, und in stattlicher, ganz aufrechter Haltung schrieb er an einer neben ihm stehenden Tafel mit der ihm eigenen schönen Handschrift, wobei es ihm immer durch Sparsamkeit und zweckmäßige Anordnung gelang, mit dem ziemlich kleinen Raume auszukommen. Für die Zahlenbeispiele, auf deren sorgfältige Durchführung er besonderen Wert legte, brachte er die erforderlichen Data auf kleinen Zetteln mit.

Indem ich nun zu dem Inhalt der (wöchentlich dreistündigen) Vorlesung übergehe, beziehe ich mich auf einen Brief von Gauß an Schumacher aus dem Jahre 1844, welcher im Band VIII von Gauß' Werken (S. 147—148) abgedruckt ist; er berichtet dort, daß seine Vorlesung aus drei Teilen besteht, von denen der erste eine nur auf Prinzipien der Zweckmäßigkeit basierte Begründungsart und die eigentliche praktische Anwendung der Methode der kleinsten Quadrate gibt, während der zweite und dritte Teil die beiden wesentlich verschiedenen Begründungsarten der Methode durch die Wahrscheinlichkeitsrechnung behandelt, wie sie in der Theoria motus corporum coelestium und in der Theoria combinationis observationum dargestellt sind. Denselben Weg schlug Gauß auch zu meiner Zeit ein, und ich möchte hier einiges aus dem ersten Teile mitteilen, was, wie ich glaube, weniger bekannt ist als der Inhalt der anderen Teile; freilich kann ich es auch hierbei nicht vermeiden, sehr bekannte Dinge mit einzuflechten. Den Zweck der Methode der kleinsten Quadrate und ihre elementare Begründung stellte Gauß ungefähr so dar:

Es liegt eine Reihe von Beobachtungen (Messungen) vor, die dazu dienen sollen, gewisse unbekannte Größen $x, y, z \cdots$ zahlenmäßig zu bestimmen; die unmittelbaren Gegenstände dieser Beobachtungen können diese Unbekannten selbst, allgemeiner aber gewisse Funktionen von ihnen sein, d. h. Größen $V, V', V'' \cdots$, welche sich streng berechnen lassen würden, wenn die Werte von $x, y, z \cdots$ schon bekannt wären. Werden nun für diese Funktionen durch unmittelbare Beobachtungen die Werte $M, M', M'' \cdots$ gefunden, so erhält man ein entsprechendes System von sogenannten Beobachtungsgleichungen $V = M, V' = M', V'' = M'' \cdots$, aus denen die unbekannten Elemente $x, y, z \cdots$ ermittelt werden sollen; dies ist natürlich nur dann möglich, wenn die Anzahl der Beobachtungen mindestens ebenso

groß ist, wie die der unbekannten Elemente. Da aber alle unsere Messungen nur einen begrenzten Genauigkeitsgrad besitzen, also Fehlern unterworfen sind, so sucht man deren schädlichen Einfluß durch Vermehrung der Anzahl der Beobachtungen zu bekämpfen, und dann fragt sich, wie soll man ein solches, mit unbekannten Fehlern $M - V$, $M' - V'$, $M'' - V'' \cdots$ behaftetes, überzähliges System von Beobachtungsgleichungen $V = M$, $V' = M'$, $V'' = M'' \cdots$ behandeln, um die unvermeidlichen Widersprüche zwischen ihnen auszugleichen und so die plausibelsten Werte der unbekannten Elemente $x, y, z \cdots$ zu finden? Hierbei wird vorausgesetzt, daß diese Beobachtungen gleiche Zuverlässigkeit besitzen, d. h., daß wir keinen Grund haben, einer von ihnen größeres Zutrauen zu schenken als den übrigen. Macht man eine bestimmte Hypothese über die Werte $x, y, z \cdots$ und berechnet daraus die entsprechenden Werte der Funktionen $V, V', V'' \cdots$, so erhält man ein entsprechendes System von Fehlern $M - V$, $M' - V'$, $M'' - V'' \cdots$, aber es fragt sich, welchen Maßstab soll man zugrunde legen, um nach Beschaffenheit dieser Fehler einer solchen Hypothese den Vorzug vor einer anderen zuzuerkennen?

Hier könnte man, da die Beobachtungen wegen ihrer gleichen Zuverlässigkeit eine gleichmäßige Behandlung verdienen, zunächst an die algebraische Summe der Fehler denken, um nach ihrer Kleinheit die Brauchbarkeit einer Hypothese zu beurteilen, und dies würde geradezu dahin führen, die Hypothese für die beste zu erklären, für welche diese Summe gleich Null wird. Allein man sieht sofort, daß dies nicht als allgemeines Prinzip gelten kann, weil, sobald die Anzahl der unbekannten Elemente mindestens gleich zwei ist, unendlich viele verschiedene Hypothesen dieser Forderung genügen würden, und außerdem würde eine Hypothese, bei welcher große Fehler durch die entgegengesetzten Vorzeichen sich in der Summe aufheben, für ebenso gut gelten, als eine andere, in welcher die einzelnen Fehler absolut genommen kleiner sind.

Dies kann uns veranlassen, nur die absoluten Werte der Fehler zu betrachten und die Hypothese für die beste zu erklären, für welche deren Summe so klein wie möglich ausfällt. Allein auch gegen dieses Prinzip lassen sich mehrere triftige Einwände erheben, nämlich:

a) Es verstößt gegen den mathematischen Sinn, daß hierbei die negativen Fehler auf andere Weise in die Rechnung eintreten sollen als die positiven.

b) Die Behandlung wird bei einer größeren Anzahl unbekannter Elemente $x, y, z \cdots$ bald sehr verwickelt.

c) Selbst im einfachsten Falle, wo nur eine einzige unbekannte Größe auftritt, und diese zugleich der unmittelbare Gegenstand der sämtlichen Beobachtungen ist, führt dieses Prinzip zu Resultaten, denen wir unseren Beifall nicht schenken können. Hätte man z. B. vier Beobachtungen $x = 900$, $x = 903$, $x = 917$, $x = 921$ gemacht, so würde jeder zwischen 903 und 917 liegende Wert x für gleich brauchbar gelten müssen, weil für alle diese Werte x die Summe der absoluten Fehler denselben kleinsten Wert $(x - 900) + (x - 903) + (917 - x) + (921 - x) = 35$ erhalten würde; dieselbe Erscheinung tritt immer auf, wenn die Anzahl der Beobachtungen gerade ist, während bei einer ungeraden Anzahl immer der in der Mitte liegende Wert x für den besten gelten müßte, so daß die übrigen Beobachtungen auch hier gar keinen Einfluß auf die Bestimmung von x ausüben würden.

d) Von besonderem Gewicht ist endlich der Einwand, daß nach diesem Prinzip bei einer größeren Anzahl von Beobachtungen ein großer Fehler keinen stärkeren Einfluß auf das Resultat ausüben würde, als eine Reihe kleiner Fehler, deren absolute Werte dieselbe Summe besitzen, während doch die Hypothese, welcher die letztere Erscheinung entspricht, nach unserem Gefühl gewiß den Vorzug vor der ersteren verdient.

Aus allen diesen Gründen ist dieses Prinzip zu verwerfen, und wir müssen einen anderen Maßstab suchen, durch welchen diese Mängel beseitigt werden, zumal die Wahl dieses Maßstabes ganz unserer Willkür überlassen ist. Hierzu führt uns von selbst der letztgenannte Einwand; die Rücksicht darauf, daß ein Fehler, welcher a-mal so groß ist als ein Fehler, der a-mal vorkommt, stärker ins Gewicht fallen muß, als diese a einzelnen Fehler, veranlaßt uns, statt der Fehler selbst ihre Quadrate zu nehmen und die Brauchbarkeit einer Hypothese nach der Kleinheit der ihr entsprechenden Summe der Fehlerquadrate zu schätzen. So gewinnen wir den Grundsatz der sogenannten Methode der kleinsten Quadrate, nach welchem diejenige Hypothese über die Werte der unbekannten Größen $x, y, z \cdots$ als die beste gelten soll, für welche die Summe der Fehlerquadrate so klein wie möglich wird. Durch die Wahl dieses Maßstabes weichen wir den obigen Einwänden a) und d) aus, ebenso gestaltet sich der unter b) erwähnte Übelstand weit besser, und die

unter c) bemerkte Erscheinung wird ganz unmöglich. Wollte man, um den Einwand d) zu beseitigen, eine noch höhere Potenz der Fehler einführen, so müßte dieselbe jedenfalls eine paare sein, um dem ersten Vorwurf zu begegnen; aber dann werden die Rechnungen so außerordentlich verwickelt, daß diese Behandlung die Mühe nicht lohnen würde.

Nach dieser sehr einleuchtenden, nur auf Prinzipien der Zweckmäßigkeit beruhenden Begründung der Methode ging Gauß sofort zur Bildung der sogenannten Normalgleichungen über, die durch partielle Differentiation der Summe

$$\Omega = (V - M)^2 + (V' - M')^2 + (V'' - M'')^2 + \cdots$$

der Fehlerquadrate in bezug auf jede der unbekannten Größen x, $y, z \cdots$ gewonnen werden. Der Kürze wegen will ich hier

$$d\Omega = 2(X\,dx + Y\,dy + Z\,dz + \cdots)$$

setzen, dann gibt die Forderung des Minimums von Ω die auf x, $y, z \cdots$ bezüglichen Normalgleichungen

$$X = 0, \quad Y = 0, \quad Z = 0 \cdots,$$

die von Gauß vollständig entwickelt dargestellt wurden.

Der zunächst behandelte und wichtigste Hauptfall ist der, wo die Größen V, V', $V'' \cdots$, also auch X, Y, $Z \cdots$ lineare Funktionen von $x, y, z \cdots$ sind. Zuerst wurde natürlich der spezielle Fall vorgeführt, wo eine einzige unbekannte Größe x durch wiederholte unmittelbare Messungen bestimmt werden soll, und wo die entsprechende Normalgleichung zu der altbekannten Regel des arithmetischen Mittels führt. Ein dazugehöriges Zahlenbeispiel — Bestimmung der Polhöhe von Lauenburg aus 11 Beobachtungen — benutzte Gauß, um uns auf gewisse Rechnungsvorteile aufmerksam zu machen. Da alle beobachteten Werte natürlich dieselbe Anzahl 53 der Grade aufwiesen und erst in den Minuten zwischen 21 und 22 schwankten, so wäre es ja töricht, bei der Bildung des arithmetischen Mittels diese so weit miteinander übereinstimmenden Werte wirklich zu addieren und ihre Summe nachher durch ihre Anzahl zu dividieren; statt dessen ist es offenbar vorteilhafter, etwa $53^0\,21'$ oder $53^0\,22'$ als genäherten Wert von x anzusehen, also $x = 53^0\,21' + t''$ oder $x = 53^0\,22' + u''$ zu setzen, und nur das arithmetische Mittel dieser Korrektionen t oder u

in Sekunden zu berechnen. Das war freilich sehr einleuchtend, aber Gauß verschmähte es nicht, eine solche scheinbare Kleinigkeit hervorzuheben, weil in ihr der Keim eines allgemeinen Prinzips enthalten war, und ebenso verfuhr er in den folgenden Aufgaben mit einer oder mehreren Unbekannten; immer wurde die allgemeine Regel an bestimmten Zahlenbeispielen durchgeführt, die zu ähnlichen Bemerkungen Veranlassung gaben. Von allen diesen Aufgaben glaube ich hier die letzte (fünfte) mitteilen zu dürfen, weil sie wohl auch heute noch einiges Interesse darbietet.

Es handelt sich um die als nahezu gleich zuverlässig anzusehenden Messungen der Höhendifferenzen (in Metern) von den folgenden fünf Punkten: P (Boden der Göttinger Sternwarte), Q (Meridianzeichen der Wehnder Papiermühle), R (Fläche des Postamentes auf dem Hohenhagen), S (östlicher Abhang des Hils, eine Viertelstunde von Ammensen), T (Brocken, Marmorplatte des vormaligen, im Hause gelegenen Turms). Bedeuten diese Zeichen zugleich die Höhen der entsprechenden Punkte, so liegen folgende sieben Beobachtungen vor:

$$\begin{aligned} Q &= P + 64{,}334 \\ R &= P + 349{,}366 \\ R &= Q + 283{,}596 \\ S &= Q + 206{,}580 \\ S &= R - 76{,}108 \\ T &= R + 648{,}427 \\ T &= S + 719{,}612 \end{aligned}$$

In diesen Gleichungen treten tatsächlich nur vier Unbekannte auf, nämlich die relativen Höhen $Q-P$, $R-P$, $S-P$, $T-P$ über Göttingen; denn absolute Höhen können natürlich hieraus nicht gefunden werden. Nun wird man sich zunächst durch geschickte Kombinationen genäherte Werte für diese Unbekannten verschaffen und hierauf

$$\begin{aligned} Q &= P + 64{,}334 + q \\ R &= P + 348{,}648 + r \\ S &= P + 271{,}727 + s \\ T &= P + 994{,}207 + t \end{aligned}$$

setzen, wo q, r, s, t die Korrektionen dieser Näherungswerte bedeuten. Führt man sie als neue Unbekannte ein und drückt sie in Millimetern

aus, so nehmen die obigen sieben Beobachtungsgleichungen folgende Form an:

$$\begin{aligned}
0 + q &= 0\\
-\ 718 + r &= 0\\
+\ 718 - q + r &= 0\\
+\ 813 - q + s &= 0\\
-\ 813 - r + s &= 0\\
-\ 2868 - r + t &= 0\\
+\ 2868 - s + t &= 0
\end{aligned}$$

und die vier Normalgleichungen lauten:

$$\begin{aligned}
0 &= -\ 1531 + 3q - r - s\\
0 &= +\ 3681 - q + 4r - s - t\\
0 &= -\ 2868 - q - r + 3s - t\\
0 &= \quad\quad - r - s + 2t
\end{aligned}$$

Nach einigen Bemerkungen über die direkte Auflösung dieser Gleichungen durch zweckmäßige Anordnung der sukzessiven Eliminationen teilte uns Gauß eine indirekte Auflösungsmethode mit, einen Kunstgriff, durch den man sich die beschwerliche Eliminationsarbeit, wie er sagte, oft erleichtern könne. Derselbe besteht wesentlich darin, die konstanten Glieder durch fortgesetzte Substitutionen auf immer kleinere absolute Werte herabzudrücken, und dieser Prozeß beginnt in unserem Beispiel auf folgende Weise. Ignoriert man in der zweiten Gleichung, welche das größte konstante Glied (3681) enthält, die Unbekannten q, s, t neben dem Gliede $4r$, welches den größten Koeffizienten (4) hat, und vernachlässigt Bruchteile, so erhält man für r den Wert -920; man betrachtet ihn als eine Annäherung und führt eine Korrektion r' als neue Unbekannte ein, indem man $r = -920 + r'$ setzt; die unbekannten Glieder werden hierdurch nur insofern berührt, daß r' an Stelle von r tritt, während die konstanten Glieder in -611, $+1$, -1948, $+920$ übergehen. Indem man nach derselben Regel fortfährt, wird man in der dritten Gleichung die Unbekannten q, r', t ignorieren und $s = +649 + s'$ setzen, wodurch die konstanten Glieder in -1260, -648, -1, $+271$ übergehen. Offenbar kommt es immer nur darauf an, die neue Substitution zu notieren, wobei man die Akzente der neuen Unbekannten füglich unterdrücken darf, und die neuen Werte der konstanten Glieder zu berechnen; den ganzen

Mechanismus kann man in leicht verständlicher Weise durch eine Tabelle darstellen, deren Anfang hier folgen mag:

	r	s	q	r	s
	-920	$+649$	$+420$	$+267$	$+229$
-1531	-611	-1260	0	-267	-496
$+3681$	$+1$	-648	-1068	0	-229
-2868	-1948	-1	-421	-688	-1
0	$+920$	$+271$	$+221$	$+4$	-225

Hat man 73 solche Operationen gemacht, so sind die konstanten Teile so klein geworden, daß sie durch eine neue Substitution nicht mehr vermindert werden können, und es genügt dann, jede der ursprünglichen Unbekannten durch Addition ihrer sukzessiven Näherungswerte zu berechnen:

$$\begin{aligned} q &= +420\cdots \\ r &= -920+267\cdots \\ s &= +649+229\cdots \\ t &= \cdots \end{aligned}$$

Noch viel kürzer wird die Arbeit, wenn man mit diesem Kunstgriff einen zweiten verbindet, welcher im folgenden besteht. Man führt noch eine neue Unbekannte p ein, indem man den Anfangspunkt verlegt und q, r, s, t durch $q-p$, $r-p$, $s-p$, $t-p$ ersetzt; behandelt man die hierdurch umgeformten Beobachtungsgleichungen wieder nach der Methode der kleinsten Quadrate, so erhält man die folgenden fünf Normalgleichungen:

$$\begin{aligned} 0 &= +718+2p-q-r \\ 0 &= -1531-p+3q-r-s \\ 0 &= +3681-p-q+4r-s-t \\ 0 &= -2868-q-r+3s-t \\ 0 &= -r-s+2t, \end{aligned}$$

von denen die vier letzten in die früheren übergehen, wenn $p=0$ gesetzt wird. Sie haben zwei merkwürdige Eigenschaften, deren Grund man leicht erkennt: erstens ist die Summe der konstanten Glieder, und

ebenso die Summe der Koeffizienten jeder einzelnen Unbekannten gleich Null, und zweitens ist auch die Summe der Koeffizienten aller Unbekannten in jeder einzelnen Gleichung gleich Null. Zufolge der ersten Eigenschaft ist jede Gleichung eine identische Folge der vier anderen, und es ist daher unmöglich, bestimmte Werte der fünf Unbekannten aus ihnen abzuleiten. Wendet man aber die oben beschriebene indirekte Auflösungsmethode an, so wird man finden, daß dieselbe jetzt viel schneller zum Abschluß kommt, und außerdem ergibt sich aus dem Umstande, daß die Summe der konstanten Glieder stets gleich Null bleiben muß, eine überaus angenehme Kontrolle der fortlaufenden Rechnung, deren Anfang wieder durch die folgende Tabelle dargestellt werden mag:

	r	s	p	q
	− 920	+ 649	− 819	+ 147
+ 718	+ 1638	+ 1638	0	− 147
− 1531	− 611	− 1260	− 441	0
+ 3681	+ 1	− 648	+ 171	+ 24
− 2868	− 1948	− 1	− 1	− 148
0	+ 920	+ 271	+ 271	+ 271

Nach etwa 20 Operationen schließt diese Rechnung ab und liefert bestimmte Werte der fünf Unbekannten, aus denen sich schließlich die eigentlichen Unbekannten $q - p$, $r - p$, $s - p$, $t - p$ ergeben. In der Vorlesung wurden natürlich nur die ersten Schritte dieses wie des früheren Prozesses wirklich ausgeführt. Über die Vorzüge und Nachteile dieser indirekten Auflösungsmethode gegenüber der gewöhnlichen durch sukzessive Elimination der Unbekannten muß ich mich jeder Bemerkung enthalten; es genügt mir, durch die Mitteilung dieses Beispiels wieder darauf hinzuweisen, wie unablässig Gauß bemüht war, auch bei dem praktischen Rechnen sinnreiche Kunstgriffe zu erfinden.

Hierauf folgte die Behandlung des Falles, wo die Beobachtungsgleichungen $V = M \cdots$ die Unbekannten nicht mehr, wie bisher, in linearer Form enthalten. Die Einführung genäherter Werte, welche früher nur als ein die Zahlenrechnungen vereinfachender Kunstgriff

auftrat, wird hier zu dem Prinzip ausgebildet, durch welches dieser Fall auf den früheren der linearen Gleichungen zurückzuführen ist, indem man die kleinen Korrektionen als neue Unbekannte behandelt und deren Produkte bei der Entwicklung nach dem Satze von Taylor vernachlässigt. Als Beispiel diente die Pothenot'sche Aufgabe in der praktischen Geometrie, speziell die Ortsbestimmung von Rosdorf bei Göttingen aus sechs Einschnitten.

Nun ging Gauß zu einer ebenfalls elementar gehaltenen Entwicklung des Begriffs der Präzision einer Beobachtungsmethode über. Wenn die vorliegenden Beobachtungen $V = M$, $V' = M' \cdots$ nicht mehr, wie bisher vorausgesetzt wurde, gleiche Zuverlässigkeit besitzen, so muß man sie als auf verschiedene Maßstäbe bezogen ansehen und jede Gleichung mit einem entsprechenden, die gleiche Zuverlässigkeit wiederherstellenden Koeffizienten k multiplizieren. Die hieraus nach der Methode der kleinsten Quadrate abgeleiteten Normalgleichungen enthalten diese (relativen) Präzisionen k nur in ihren Quadraten, und diese heißen die entsprechenden Gewichte p der Beobachtungen.

Diese Betrachtung gibt zugleich ein Mittel an die Hand, die Zuverlässigkeit der durch die Methode der kleinsten Quadrate gewonnenen Resultate im Vergleich mit der Zuverlässigkeit der gegebenen Beobachtungen zu bestimmen. Das Prinzip, auf welches sich diese Ableitung gründet, ist das der Konsequenz. Man denkt sich zu der ursprünglich vorhandenen Gruppe von Beobachtungen, die wieder als gleich zuverlässig vorausgesetzt werden, und deren Präzision $= 1$ angenommen wird, eine beliebige Anzahl anderer Beobachtungen von derselben Präzision hinzu, wodurch die zuerst gefundenen plausibelsten Werte der Unbekannten x, y, $z \cdots$ in andere Werte übergehen werden. Um diese zu finden, kann man nun zwei verschiedene Wege einschlagen, welche aber notwendig zu denselben Resultaten führen müssen. Der erste Weg besteht darin, daß man nach der Methode der kleinsten Quadrate sämtliche Beobachtungsgleichungen beider Gruppen gleichzeitig behandelt, der zweite darin, daß man die allein aus der ersten Gruppe (der wirklich gegebenen Beobachtungen) abgeleiteten Resultate mit gewissen, noch unbestimmt gelassenen Präzisions-Koeffizienten k multipliziert und hierauf mit der zweiten, hinzugedachten Gruppe von Beobachtungen kombiniert. Durch die Forderung, daß die auf diesen beiden verschiedenen Wegen er-

haltenen Schlußresultate miteinander übereinstimmen müssen, ergeben sich dann die Werte der Präzisionen k und ihrer Quadrate, der Gewichte p.

Diese allgemeine Anleitung zur Gewichtsbestimmung der durch die Methode der kleinsten Quadrate gewonnenen Resultate wurde zunächst an den einfachsten Fällen durchgeführt, wo die (immer als linear vorausgesetzten) Beobachtungsgleichungen nur eine Unbekannte enthalten. Um aber für eine beliebige Anzahl n von Unbekannten $x, y \cdots$, deren letzte z sein möge, die Regel allgemein auszudrücken (wobei die uns damals noch wenig geläufige Sprache der Determinanten-Theorie gänzlich vermieden wurde), beschrieb Gauß zunächst ein Verfahren zur Auflösung der auf $x, y \cdots z$ bezüglichen Normalgleichungen $X = 0$, $Y = 0 \cdots Z = 0$, welches er mit dem Namen der rechten Elimination belegte (vgl. Disquisitiones circa elementa elliptica Palladis). Man eliminiere die erste Unbekannte x aus allen n Gleichungen, indem man nur die erste, auf x bezügliche Normalgleichung $X = 0$ mit geeigneten Koeffizienten multipliziert und von den folgenden, unveränderten Normalgleichungen abzieht, welche dadurch in $Y' = 0 \cdots Z' = 0$ übergehen und frei von x sind; nun eliminiere man ebenso die zweite Unbekannte y aus allen diesen $(n-1)$ Gleichungen, indem man nur die erste Gleichung $Y' = 0$ mit geeigneten Koeffizienten multipliziert und von allen folgenden abzieht; fährt man so fort, so gelangt man schließlich zu einer Gleichung von der Form $H(z - C) = 0$, in welcher nur noch die letzte Unbekannte z auftritt, und wo H, C bekannte Werte bedeuten, die sich aus dem Verlauf dieser rechten Elimination mit Bestimmtheit ergeben. Die Auflösung der Normalgleichungen liefert also für z den plausibelsten Wert C, und die Regel von Gauß besteht darin, daß der Koeffizient H zugleich das Gewicht dieses Resultats $z = C$ darstellt, d. h. also: In der Methode der kleinsten Quadrate wird das Gewicht jedes einzelnen Resultats für eine Unbekannte durch den Koeffizienten dargestellt, welchen diese Unbekannte bei rechter Elimination in der letzten Gleichung erhält.

Bei dem Beweise dieses Satzes, den ich hier des Raumes wegen mit einer kleinen Änderung der Bezeichnung wiedergebe, beschränkte sich Gauß auf den Fall von drei Unbekannten x, y, z. Durch die rechte Elimination von x, y werden offenbar zwei Koeffizienten α, β gewonnen, welche bewirken, daß identisch

$$\alpha X + \beta Y + Z = H\,(z - C)$$

wird. Denkt man sich nun zu den wirklich vorhandenen m Beobachtungsgleichungen, denen die Normalgleichungen $X = 0$, $Y = 0$, $Z = 0$ mit dem Resultat $z = C$ entsprechen, noch eine Beobachtung $z = D$ von derselben Präzision hinzu und schlägt den oben beschriebenen ersten Weg ein, bei welchem alle $(m + 1)$ Beobachtungen gleichzeitig behandelt werden, so bleiben offenbar die auf x, y bezüglichen Normalgleichungen $X = 0$, $Y = 0$ ungeändert bestehen, während die dritte $Z = 0$ in $Z + (z - D) = 0$ übergeht; zufolge der obigen Identität ergibt sich daher z jetzt aus der Gleichung

$$H(z - C) + (z - D) = 0.$$

Schlägt man aber den zweiten Weg ein, indem man das aus den m wirklich vorhandenen Beobachtungen durch die Methode der kleinsten Quadrate gewonnene Resultat $z = C$ mit einer noch unbestimmten Präzision k multipliziert und nun nach derselben Methode mit der hinzugedachten Beobachtung $z = D$ kombiniert, so erhält man, wenn das unbekannte Gewicht $kk = p$ gesetzt wird, die einzige Normalgleichung

$$p(z - C) + (z - D) = 0,$$

und durch den Vergleich mit dem Resultate des ersten Weges folgt $p = H$, w. z. b. w.

In nahem Zusammenhang mit der eben beschriebenen rechten Elimination steht die sukzessive identische Umformung der Summe Ω der Fehlerquadrate in eine Reihe von Quadraten linearer Funktionen $A, B, C \cdots$, die so gewählt werden, daß x nur in A, y nur in A und B, z nur in A, B, C usf. auftritt. Der zuletzt verbleibende konstante Bestandteil stellt dann das Minimum von Ω dar, und die plausibelsten Werte der Unbekannten x, y, $z \cdots$ ergeben sich aus den Gleichungen $A = 0$, $B = 0$, $C = 0 \cdots$ in umgekehrter Folge.

Mit dieser Darstellung schloß Gauß am 24. Januar 1851 den ersten Teil seiner Vorlesung, durch den er uns mit dem Wesen der Methode der kleinsten Quadrate vollkommen vertraut gemacht hatte. Es folgte nun eine überaus klare und durch originelle Beispiele erläuterte Entwicklung der Grundbegriffe und der Hauptsätze der Wahrscheinlichkeitsrechnung, die als Einleitung zu der zweiten und dritten Begründungsart der Methode diente, worauf ich hier nicht mehr eingehen darf. Ich kann nur sagen, daß wir diesem ausgezeichneten Vortrage, in welchem auch einige Beispiele aus der Theorie der be-

stimmten Integrale behandelt wurden, mit immer steigendem Interesse gefolgt sind. Aber es schien uns auch, als ob Gauß selbst, der vorher wenig Neigung gezeigt hatte, die Vorlesung zu halten, im Laufe derselben doch einige Freude an seiner Lehrtätigkeit empfand. So kam es am 13. März zum Schluß, Gauß erhob sich, wir alle mit ihm, und er entließ uns mit den freundlichen Abschiedsworten: „Es bleibt mir nur noch übrig, Ihnen zu danken für die große Regelmäßigkeit und Aufmerksamkeit, mit der Sie meinem, doch wohl recht trocken zu nennenden Vortrage gefolgt sind.“ Seitdem ist nun ein halbes Jahrhundert verflossen, aber dieser angeblich trockene Vortrag steht mir unvergeßlich in der Erinnerung als einer der schönsten, die ich je gehört habe.

XXXIII.

Über binäre trilineare Formen und die Komposition der binären quadratischen Formen.

[Journal für reine und angewandte Mathematik, Bd. 129, S. 1—34 (1905).]

Bei der Besprechung der in lineare Faktoren zerlegbaren Formen, welche zu einem endlichen algebraischen Zahlkörper gehören, habe ich bemerkt, daß die drei Formen, deren eine durch eine bilineare Substitution in das Produkt der beiden anderen übergeht, im wesentlichen, d. h. abgesehen von konstanten Faktoren, umgekehrt durch diese Substitution bestimmt sind*). In dem einfachsten Falle der binären quadratischen Formen ist diese Tatsache zwar nicht ausdrücklich von Gauß ausgesprochen, aber sie ist vollständig in der Schlußbemerkung des Art. 235 der Disquisitiones Arithmeticae enthalten, in welchem die Transformation einer Form in ein Produkt aus zwei Formen durch eine bilineare Substitution in der allgemeinsten Weise behandelt wird. Bei meinem ersten Studium dieser Untersuchung erregte die genannte Tatsache meine besondere Aufmerksamkeit, und ich erkannte bald, daß mit einer solchen gegebenen Substitution immer zwei andere Substitutionen und drei quadratische Formen von der Art verbunden sind, daß jede der drei Formen durch eine ihr entsprechende Substitution in das Produkt der beiden anderen Formen übergeht. Hat man sich hiervon überzeugt, was bei zweckmäßiger Wahl der Bezeichnung keine Schwierigkeit darbietet, so wird die Lösung des allgemeinen von Gauß behandelten Problems in hohem Grade vereinfacht. Da dies noch nicht bekannt zu sein scheint, so wage ich es, meine Untersuchung zu veröffentlichen und dem Andenken an meinen großen Lehrer Dirichlet zu widmen, der selbst eine Ehre darein gesetzt hat, durch eine Reihe von Abhandlungen das Verständnis des von ihm am höchsten bewunderten Werkes von Gauß zu erleichtern.

*) Dirichlets Vorlesungen über Zahlentheorie, vierte Auflage, § 182, S. 586.

§ 1.

Wir betrachten im folgenden drei Paare von unabhängigen Variabeln

$$(x_1, y_1), (x_2, y_2), (x_3, y_3)$$

und zwei Reihen von je vier willkürlichen Konstanten

$$\alpha = \alpha_0, \alpha_1, \alpha_2, \alpha_3,$$
$$\beta = \beta_0, \beta_1, \beta_2, \beta_3.$$

Bedeutet r, s, t, wie immer im folgenden, irgend eine Permutation der drei Indizes 1, 2, 3 (während der Index 0 ungeändert bleibt), so dürfen wir jeden aus den Variabeln und Konstanten gebildeten Ausdruck, der in bezug auf die beiden Indizes s, t symmetrisch ist, als eine durch den Index r bestimmte Größe ansehen und demgemäß bezeichnen. In diesem Sinne bilden wir drei binäre quadratische Formen F_1, F_2, F_3 durch die gemeinsame Definition

$$(1)\quad \begin{cases} F_r = F_r(x_r, y_r) = A_r x_r^2 + B_r x_r y_r + C_r y_r^2 \\ = (\beta_s x_r + \alpha_t y_r)(\beta_t x_r + \alpha_s y_r) - (\alpha_r x_r + \beta_0 y_r)(\alpha_0 x_r + \beta_r y_r), \end{cases}$$

wo also

$$(2)\quad \begin{cases} A_r = \beta_s\beta_t - \alpha_0\alpha_r, \quad C_r = \alpha_s\alpha_t - \beta_0\beta_r, \\ B_r = \alpha_s\beta_s + \alpha_t\beta_t - \alpha_r\beta_r - \alpha_0\beta_0. \end{cases}$$

Wir wollen beweisen, daß diese drei Formen ein und dieselbe Diskriminante

$$(3)\qquad D = B_1^2 - 4A_1C_1 = B_2^2 - 4A_2C_2 = B_3^2 - 4A_3C_3$$

haben, und daß jede von ihnen durch eine entsprechende bilineare Substitution in das Produkt der beiden anderen Formen übergeht.

Das erstere folgt leicht aus einem bekannten Satz über partiale Determinanten. Bildet man aus zwei Reihen von je vier Größen

$$p, p', p'', p''',$$
$$q, q', q'', q'''$$

die sechs Determinanten

$$(4)\quad \begin{cases} P = pq' - qp', \quad Q = pq'' - qp'', \quad R = pq''' - qp''', \\ U = p''q''' - q''p''', \quad T = p'q''' - q'p''', \quad S = p'q'' - q'p'', \end{cases}$$

so genügen die drei letzteren den beiden Gleichungen

$$Up' - Tp'' + Sp''' = 0, \quad Uq' - Tq'' + Sq''' = 0;$$

multipliziert man die erste mit $-q$, die zweite mit p und addiert, so erhält man den in Rede stehenden Satz

$$PU - QT + RS = 0. \tag{5}$$

Wenden wir ihn auf das Beispiel

$$\begin{cases} p = \beta_r, & p' = \alpha_s, & p'' = \alpha_t, & p''' = \beta_0, \\ q = -\alpha_0, & q' = -\beta_t, & q'' = -\beta_s, & q''' = -\alpha_r \end{cases} \tag{6}$$

an, so wird zufolge (2):

$$\begin{cases} P = -A_s, \quad Q = -A_t, \quad R = -\frac{1}{2}(B_t + B_s), \\ U = -C_s, \quad T = -C_t, \quad S = -\frac{1}{2}(B_t - B_s), \end{cases} \tag{7}$$

also

$$A_s C_s - A_t C_t + \tfrac{1}{4}(B_t + B_s)(B_t - B_s) = 0$$

oder

$$B_s^2 - 4 A_s C_s = B_t^2 - 4 A_t C_t,$$

womit unsere Behauptung über die Diskriminanten der drei Formen bewiesen ist. Wir bemerken zugleich, daß diese gemeinsame Diskriminante D, die eine homogene Funktion vierten Grades von den acht Konstanten α, β ist, nicht identisch verschwindet; denn wenn man z. B. $\alpha_0 = \beta_0 = 0$, alle anderen sechs Konstanten $\alpha, \beta = 1$ setzt, so werden alle neun Koeffizienten A_r, B_r, C_r gleich 1, also $D = -3$.

Um auch die zweite Behauptung zu beweisen, setzen wir zur Abkürzung

$$\frac{\partial F_r}{\partial x_r} = 2 A_r x_r + B_r y_r = 2 u_r, \quad \frac{\partial F_r}{\partial y_r} = B_r x_r + 2 C_r y_r = 2 v_r, \tag{8}$$

woraus

$$u_r x_r + v_r y_r = F_r \tag{9}$$

folgt, und nehmen die Konstanten (6) zu Koeffizienten der beiden bilinearen, in bezug auf s, t symmetrischen Funktionen

$$\begin{cases} X_r = \quad \beta_r x_s x_t + \alpha_s x_s y_t + \alpha_t y_s x_t + \beta_0 y_s y_t, \\ Y_r = -\alpha_0 x_s x_t - \beta_t x_s y_t - \beta_s y_s x_t - \alpha_r y_s y_t. \end{cases} \tag{10}$$

Eliminiert man der Reihe nach jedes der vier Produkte $x_s x_t$, $x_s y_t$, $y_s x_t$, $y_s y_t$, so erhält man mit Rücksicht auf (4), (7), (8) die Gleichungen

$$\begin{aligned}
&\alpha_0 X_r + \beta_r Y_r \\
&= -A_s x_s y_t - A_t y_s x_t - \frac{1}{2}(B_t + B_s) y_s y_t = -y_s u_t - u_s y_t, \\
&\beta_t X_r + \alpha_s Y_r \\
&= \quad A_s x_s x_t - \frac{1}{2}(B_t - B_s) y_s x_t - C_t y_s y_t = -y_s v_t + u_s x_t, \\
&\beta_s X_r + \alpha_t Y_r \\
&= \quad A_t x_s x_t + \frac{1}{2}(B_t - B_s) x_s y_t - C_s y_s y_t = \quad x_s u_t - v_s y_t, \\
&\alpha_r X_r + \beta_0 Y_r \\
&= \frac{1}{2}(B_t + B_s) x_s x_t + C_t x_s y_t + \quad C_s y_s x_t = \quad x_s v_t + v_s x_t,
\end{aligned}$$

die man mit Benutzung der bekannten Bezeichnung für die Multiplikation von zwei binären Substitutionen auch in der Form

$$\begin{pmatrix} \beta_s X_r + \alpha_t Y_r, & \alpha_r X_r + \beta_0 Y_r \\ \alpha_0 X_r + \beta_r Y_r, & \beta_t X_r + \alpha_s Y_r \end{pmatrix} = \begin{pmatrix} x_s, & v_s \\ -y_s, & u_s \end{pmatrix} \begin{pmatrix} u_t, & v_t \\ -y_t, & x_t \end{pmatrix}$$

darstellen kann, und da bekanntlich die Determinante des Produkts von zwei Substitutionen das Produkt aus deren Determinanten ist, so ergibt sich aus der Definition (1) der Formen $F_r = F_r(x_r, y_r)$ und aus (9) das Resultat

$$F_r(X_r, Y_r) = F_s F_t, \tag{11}$$

womit auch unsere zweite Behauptung bewiesen ist.

Man erkennt übrigens leicht, daß dieser zweite Satz (11) den ersten (3) über die Diskriminanten in sich schließt. Sieht man nämlich x_s, y_s als Konstanten an, so nimmt die obige bilineare Substitution (10) die Form einer einfachen binären Substitution

$$\begin{aligned}
X_r &= \quad (\beta_r x_s + \alpha_t y_s) x_t + (\alpha_s x_s + \beta_0 y_s) y_t, \\
Y_r &= -(\alpha_0 x_s + \beta_s y_s) x_t - (\beta_t x_s + \alpha_r y_s) y_t
\end{aligned}$$

an, deren Determinante zufolge (1) gleich $-F_s$ ist, und durch diese Substitution geht die Form

$$F_r(X_r, Y_r) = A_r X_r^2 + B_r X_r Y_r + C_r Y_r^2$$

nach dem Satz (11) in die Form

$$F_s F_t(x_t, y_t) = F_s A_t x_t^2 + F_s B_t x_t y_t + F_s C_t y_t^2$$

über. Nach dem bekannten Fundamentalsatz über die Transformation einer binären quadratischen Form durch eine einfache lineare Substitution ist aber die Diskriminante der neuen Form gleich der der alten, multipliziert mit dem Quadrat der Substitutionsdeterminante. Bezeichnet man nun mit D_1, D_2, D_3 die Diskriminanten der Formen F_1, F_2, F_3, so ist in unserem Falle die Diskriminante der neuen Form

$$(F_s B_t)^2 - 4(F_s A_t)(F_s C_t) = D_t F_s^2,$$

und da D_r die Diskriminante der alten Form, und $-F_s$ die Substitutionsdeterminante ist, so folgt $D_t F_s^2 = D_r(-F_s)^2$, also $D_t = D_r$, was zu beweisen war.

Die acht Konstanten α, β bilden daher immer die Koeffizienten von drei verwandten binären bilinearen Substitutionen, deren Zusammenhang wesentlich in der Identität

(12) $$y_1 X_1 - x_1 Y_1 = y_2 X_2 - x_2 Y_2 = y_3 X_3 - x_3 Y_3$$

besteht, und erzeugen zugleich drei quadratische Formen, deren jede durch eine dieser Substitutionen in das Produkt der beiden anderen übergeht.

Indem wir uns vorbehalten, auf diese Identität später (in § 4) zurückzukommen, beschließen wir diese Betrachtungen mit einer Bemerkung, die sich auf den Fall bezieht, wo die bisher willkürlichen acht Konstanten α, β ganze rationale Zahlen sind. Dann sind auch die Koeffizienten der drei Formen F_1, F_2, F_3 und deren Diskriminante D ganze Zahlen; wir wollen annehmen, daß keine dieser Formen identisch verschwindet, und wollen mit M_r den Teiler der Form F_r, d. h. den positiven größten gemeinsamen Teiler ihrer Koeffizienten A_r, B_r, C_r bezeichnen. Bedeutet ferner K_r den größten gemeinsamen Teiler von M_s, M_t, also auch den der sechs Koeffizienten A_s, B_s, C_s, A_t, B_t, C_t, so folgt aus (3) auch $B_s \equiv B_t \pmod{2K_r}$, mithin ist K_r auch gemeinsamer Teiler der sechs partialen Determinanten (7), und zwar der größte, weil umgekehrt jeder gemeinsame Teiler dieser Determinanten offenbar auch in B_s, B_t, also in M_s, M_t, K_r aufgeht.

Entwickelt man nun beide Seiten der in bezug auf die vier Variabeln x_s, y_s, x_t, y_t identischen Gleichung (11) durch Auflösung aller die Variabeln einschließenden Klammern, so leuchtet ein, daß alle Koeffizienten der linken Seite durch M_r teilbar sind, während offenbar das Produkt $M_s M_t$ der größte gemeinsame Teiler der neun

Koeffizienten der rechten Seite ist; mithin ist $M_s M_t$ teilbar durch M_r, also

(13) $M_2 M_3 = M_1 N_1, \quad M_3 M_1 = M_2 N_2, \quad M_1 M_2 = M_3 N_3,$

wo N_1, N_2, N_3 ebenfalls natürliche Zahlen bedeuten; dann ist zugleich

(14) $M_1^2 = N_2 N_3, \quad M_2^2 = N_3 N_1, \quad M_3^2 = N_1 N_2,$

und wenn z. B. M_2, M_3 relative Primzahlen sind, also $K_1 = 1$, so folgt

(15) $M_1 = M_2 M_3, \quad N_1 = 1, \quad N_2 = M_3^2, \quad N_3 = M_2^2.$

§ 2.

Nach dieser Vorbereitung wenden wir uns zu der Aufgabe, welche Gauß im Art. 235 der Disquisitiones Arithmeticae behandelt hat. Ich will aber vorher bemerken, daß ich hier wie schon früher*) statt der von Gauß zugrunde gelegten Formen $ax^2 + 2bxy + cy^2$, deren zweiter Koeffizient den Faktor 2 enthält, immer Formen $f(x, y) = ax^2 + bxy + cy^2$ betrachte, wo a, b, c beliebige Konstanten bedeuten, die nur der Beschränkung unterliegen sollen, daß die aus ihnen gebildete Diskriminante $\partial = b^2 - 4ac$ der Form $f = f(x, y)$ von Null verschieden ist.

Sind nun $f_1 = f_1(x_1, y_1)$, $f_2 = f_2(x_2, y_2)$, $f_3 = f_3(x_3, y_3)$ drei solche Formen mit den Diskriminanten $\partial_1, \partial_2, \partial_3$, so besteht die Untersuchung darin, alle Folgerungen aus der Annahme zu ziehen, daß die erste Form f_1 durch eine bilineare Substitution in das Produkt $f_2 f_3$ der beiden anderen Formen übergeht; bezeichnet man daher mit X_1, Y_1 zwei bilineare Funktionen der beiden Paare (x_2, y_2), (x_3, y_3), so wird diese Annahme durch die Identität

$$f_1(X_1, Y_1) = f_2 f_3$$

ausgedrückt; um aber die Symmetrie so viel wie möglich zu bewahren, fügen wir dem Produkt noch einen von Null verschiedenen konstanten Faktor k_1 hinzu und setzen also

(16) $$f_1(X_1, Y_1) = k_1 f_2 f_3.$$

Aus den acht Koeffizienten α, β der bilinearen Funktionen, die wir (gemäß (10) in § 1) in die Form

(17) $$\begin{cases} X_1 = \beta_1 x_2 x_3 + \alpha_2 x_2 y_3 + \alpha_3 y_2 x_3 + \beta_0 y_2 y_3, \\ Y_1 = -\alpha_0 x_2 x_3 - \beta_3 x_2 y_3 - \beta_2 y_2 x_3 - \alpha_1 y_2 y_3 \end{cases}$$

*) Zuerst in §§ 169, 170 der zweiten Auflage (1871) von Dirichlets Vorlesungen über Zahlentheorie.

setzen, bilden wir nach § 1 die drei Formen F_1, F_2, F_3; dann besteht das Endresultat der Untersuchung wesentlich darin, daß diese Formen sich beziehungsweise von den Formen f_1, f_2, f_3 nur um konstante, von Null verschiedene Faktoren n_1, n_2, n_3 unterscheiden, daß also identisch

$$F_1 = n_1 f_1, \quad F_2 = n_2 f_2, \quad F_3 = n_3 f_3 \tag{18}$$

ist.

Um dies in aller Kürze zu beweisen, verfahre man ebenso wie bei dem zweiten Beweise des Diskriminantensatzes (3) in § 1. Sieht man in den Gleichungen (17) erst x_2, y_2, dann x_3, y_3 als Konstanten an, so nehmen sie die Gestalt von einfachen linearen Substitutionen an, deren Determinanten bzw. $-F_2, -F_3$ sind, und der Fundamentalsatz über solche Transformationen einer Form f_1 ergibt zufolge der Annahme (16) die beiden Gleichungen

$$\partial_1(-F_2)^2 = \partial_3(k_1 f_2)^2, \quad \partial_1(-F_3)^2 = \partial_2(k_1 f_3)^2,$$

und da $k_1, \partial_1, \partial_2, \partial_3$ nach unserer Annahme von Null verschieden sind, so folgen hieraus die beiden letzten Gleichungen (18), wo n_2, n_3 von Null verschiedene Konstanten bedeuten. Multipliziert man diese beiden Gleichungen miteinander, so geht die Annahme (16) mit Rücksicht auf den Satz (11) in § 1 in die Gleichung

$$k_1 F_1(X_1, Y_1) = n_2 n_3 f_1(X_1, Y_1)$$

über, welche identisch in bezug auf die vier Variabeln x_2, y_2, x_3, y_3 bestehen muß. Da nun ∂_2 nicht Null ist, also auch die Form f_2 nicht identisch verschwindet, so gilt dasselbe auch von der Form $F_2 = n_2 f_2$; man kann daher den Variabeln x_2, y_2 in (17) solche Werte beilegen, daß F_2 einen von Null verschiedenen Wert erhält, und folglich kann man hierauf x_3, y_3 immer so wählen, daß X_1, Y_1 beliebig vorgeschriebene Werte x_1, y_1 annehmen; man darf daher in der vorstehenden Gleichung X_1, Y_1 durch die unabhängigen Variabeln x_1, y_1 ersetzen, und folglich gilt auch die erste der Identitäten (18), was zu beweisen war.

Umgekehrt, wenn zwischen drei Formen f_1, f_2, f_3 und den in § 1 definierten Formen F_1, F_2, F_3 die drei Identitäten (18) bestehen, wo n_1, n_2, n_3 von Null verschiedene Konstanten bedeuten, so folgen aus dem Satze (11) in § 1 die drei Identitäten

$$f_r(X_r, Y_r) = k_r f_s f_t, \tag{19}$$

wo

$$k_r = \frac{n_s n_t}{n_r}, \tag{20}$$

d. h. jede der drei Formen f_1, f_2, f_3 geht durch eine bilineare Substitution in das mit einer Konstanten multiplizierte Produkt der beiden anderen Formen über.

Die drei Gleichungen (18), aus denen unmittelbar die Relationen

$$D = \partial_1 n_1^2 = \partial_2 n_2^2 = \partial_3 n_3^2 \tag{21}$$

zwischen den Diskriminanten der sechs Formen F_r, f_r folgen, schließen diejenigen neun Gleichungen in sich, welche Gauß in der Schlußbemerkung des Art. 235 mit Ω bezeichnet, und die als Grundlage für die in den Artikeln 236—241 folgenden Untersuchungen dienen. Die Gleichungen (18), bei deren Ableitung wir gar keine Voraussetzung über die besondere Natur der Koeffizienten der Formen f_1, f_2, f_3 und der bilinearen Funktionen X_1, Y_1 gemacht haben, enthalten den algebraischen Teil der Untersuchung; wir wollen jetzt annehmen, alle diese Koeffizienten seien ganze rationale Zahlen, und wollen die zahlentheoretischen Folgerungen aus der Annahme (16) ziehen, die bei Gauß schon im Laufe seiner Untersuchung auftreten.

Aus (18) folgt zunächst, daß n_1, n_2, n_3 ganze oder gebrochene rationale Zahlen sind, mithin haben zufolge (21) die Diskriminanten D, ∂_1, ∂_2, ∂_3 dasselbe Vorzeichen, und sie verhalten sich wie Quadrate von ganzen Zahlen (Conclusio prima bei Gauß). Bezeichnen wir ferner mit m_r den Teiler der Form f_r und (wie in § 1) mit M_r den der Form F_r, so ist zufolge (18)

$$M_1 = \varepsilon_1 m_1 n_1, \quad M_2 = \varepsilon_2 m_2 n_2, \quad M_3 = \varepsilon_3 m_3 n_3, \tag{22}$$

wo

$$\varepsilon_1^2 = \varepsilon_2^2 = \varepsilon_3^2 = 1, \tag{23}$$

also $\varepsilon_1 n_1$, $\varepsilon_2 n_2$, $\varepsilon_3 n_3$ positiv sind.

Jetzt kehren wir, indem wir die Symmetrie aufgeben, zu der eigentlichen Annahme von Gauß zurück, daß nämlich f_1 durch die bilineare Substitution (17) in das Produkt $f_2 f_3$ selbst übergeht, daß also

$$f_1(X_1, Y_1) = f_2 f_3, \tag{24}$$

mithin

$$k_1 = 1, \quad n_1 = n_2 n_3, \quad \varepsilon_1 = \varepsilon_2 \varepsilon_3 \tag{25}$$

ist, woraus nach (21), (22) auch

$$\partial_2 = \partial_1 n_3^2, \quad \partial_3 = \partial_1 n_2^2, \tag{26}$$

$$\partial_2 m_3^2 = \partial_1 M_3^2, \quad \partial_3 m_2^2 = \partial_1 M_2^2 \tag{27}$$

folgt. Bedeutet daher K_1 wieder den größten gemeinsamen Teiler von M_2, M_3 (wie in § 1), so ist $\partial_1 K_1^2$ der größte gemeinsame Teiler der beiden Produkte $\partial_2 m_3^2$, $\partial_3 m_2^2$ (Conclusio secunda et quarta bei Gauß).

Nach der Definition von Gauß heißt nun die Form f_1 zusammengesetzt (composita) aus den beiden Formen f_2, f_3, wenn $K_1 = 1$ ist, also M_2, M_3 relative Primzahlen sind. Beschränken wir uns jetzt auf diesen Fall, so folgt aus (27), daß die Diskriminante ∂_1 der aus f_2, f_3 zusammengesetzten Form f_1 der größte gemeinsame Teiler von $\partial_2 m_3^2$, $\partial_3 m_2^2$ ist. Da ferner nach (15) in § 1 aus der jetzigen Annahme auch $M_1 = M_2 M_3$ folgt, so ergibt sich aus (22), (25) auch $m_1 = m_2 m_3$, d. h. der Teiler m_1 der zusammengesetzten Form f_1 ist das Produkt aus den Teilern m_2, m_3 der Formen f_2, f_3 (Conclusio quinta bei Gauß).

Hiermit ist der wesentliche Inhalt des Art. 235 der Disquisitiones Arithmeticae erschöpft. Die daselbst zum Ziele führenden Rechnungen, die zum großen Teil nur angedeutet sind, und deren wirkliche Ausführung dem Leser überlassen ist, glaube ich in der hier vorliegenden Darstellung erheblich vereinfacht zu haben. Da diese Vereinfachung hauptsächlich auf der in § 1 vorausgeschickten Einführung der mit einer jeden bilinearen Substitution verbundenen drei Formen F_1, F_2, F_3 und auf deren symmetrischer Behandlung beruht, welche mit geringer Rechnung zu dem Hauptsatz (11) führt, so war es eben wegen dieser Symmetrie nicht möglich, die Bezeichnungen von Gauß beizubehalten. Zur Erleichterung einer Vergleichung bemerke ich folgendes. Gauß untersucht die Transformation einer Form F in das Produkt von zwei Formen f, f', deren Variable entsprechend bezeichnet sind, durch die bilineare Substitution

$$X = pxx' + p'xy' + p''yx' + p'''yy',$$
$$Y = qxx' + q'xy' + q''yx' + q'''yy'$$

und gebraucht die Zeichen P, Q, R, S, T, U in derselben Bedeutung wie in Gleichung (4). Um daher von dieser Bezeichnung zu der meinigen in (24) überzugehen, hat man F, f, f' bzw. durch f_1, f_2, f_3

zu ersetzen, und die vorstehende bilineare Substitution geht in (17) über, wenn die Koeffizienten p, $p' \cdots q'''$ wie in (6) ausgedrückt werden, wobei die Indizes r, s, t bzw. durch 1, 2, 3 zu ersetzen sind. Beachtet man nun die Vorzeichen der hieraus entspringenden Ausdrücke (7), so erkennt man, daß man die in den neun Schlußgleichungen Ω bei Gauß auftretenden beiden Zahlen n, n' bzw. durch $-n_3$, $-n_2$ zu ersetzen hat, um diese Gleichungen Ω in Übereinstimmung mit unseren Gleichungen (18) zu bringen, in denen zufolge (25) $n_1 = n_2 n_3$ ist. Dies ist deshalb erwähnenswert, weil Gauß auf die Vorzeichen der Zahlen n, n' eine wichtige Unterscheidung hinsichtlich der Art gründet, wie die Formen f, f' in die Transformation oder Komposition $F = ff'$ eintreten, worauf wir hier aber nicht näher eingehen können.

§ 3.

Der Satz (11) in § 1, auf welchem alles andere beruht, ist dort wohl auf dem kürzesten Wege hergeleitet, nämlich durch unmittelbare Rechnung mit den acht Konstanten α, β, aus denen die Koeffizienten der sechs bilinearen Funktionen (10) und die der drei quadratischen Formen (1) gebildet sind. Man kann aber zu demselben Resultat und zu einem tieferen Einblick in den Gegenstand der Untersuchung auf einem ganz anderen Wege gelangen, wobei diese Konstanten α, β gar nicht explizite in die Rechnung eintreten, sondern die in (12) angeführte binäre trilineare Form als alleiniger Ausgangspunkt der Untersuchung dient. Der Weg, den ich hierbei einschlage, beruht auf der freiesten Ausnutzung der totalen Differentiation in der Auffassung, wie ich sie mir seit vielen Jahren gebildet und gelegentlich auch befreundeten Mathematikern mitgeteilt habe*). Da dieselbe nicht nur in der reinen Analysis, sondern auch in der Geometrie, Mechanik, in der mathematischen Physik nützlich verwendet werden kann und noch nicht so allgemein bekannt zu sein scheint, wie sie es wohl verdient, so will ich wenigstens das, was für unseren Zweck erforderlich ist, zunächst besprechen.

---

*) Vgl. § 159 der zweiten Auflage (1871) von Dirichlets Vorlesungen über Zahlentheorie und meinen Aufsatz: Zur Theorie der aus n Haupteinheiten gebildeten komplexen Größen (Göttinger Nachrichten 1885), wo von dieser Auffassung Gebrauch gemacht ist.

Ich betrachte einen analytischen Raum, in welchem jeder Punkt durch die Werte von n unabhängigen Variabeln (Koordinaten) x_1, $x_2, \cdots, x_n$ bestimmt ist, und bezeichne mit Φ den Inbegriff aller derjenigen Funktionen φ dieser Variabeln, welche partielle Derivierte von beliebig hoher Ordnung besitzen und zugleich der Bedingung

$$\frac{\partial}{\partial x_r}\left(\frac{\partial \varphi}{\partial x_s}\right) = \frac{\partial}{\partial x_s}\left(\frac{\partial \varphi}{\partial x_r}\right) \tag{28}$$

genügen. Dann soll das Zeichen d eine Operation bedeuten, welche aus jeder solchen Funktion φ eine entsprechende, ebenfalls in Φ enthaltene Funktion $d\varphi$ in der Weise erzeugt, daß das bekannte Grundgesetz der totalen Differentiation erfüllt wird, d. h. jede zwischen m solchen Funktionen $\varphi_1, \varphi_2, \cdots, \varphi_m$ bestehende Identität

$$F(\varphi_1, \varphi_2, \cdots, \varphi_m) = 0 \tag{29}$$

soll die Identität

$$\frac{\partial F}{\partial \varphi_1} d\varphi_1 + \frac{\partial F}{\partial \varphi_2} d\varphi_2 + \cdots + \frac{\partial F}{\partial \varphi_m} d\varphi_m = 0 \tag{30}$$

zur Folge haben.

Daß solche Operationen d überhaupt möglich sind, geht aus der gewöhnlichen Auffassung der Differentiale als unendlich kleiner Änderungen der Variablen hervor; wir müssen aber jetzt feststellen, in welchem Umfange solche Operationen d in der obigen allgemeinsten Auffassung existieren, und wodurch sie vollständig bestimmt werden. Die letztere Frage läßt sich sofort beantworten; denn wenn φ irgend eine in dem System Φ enthaltene Funktion ist, so besteht zwischen ihr und den n unabhängigen Variablen $x_1, x_2, \cdots, x_n$ eine Identität, die wir in der Form

$$\varphi = f(x_1, x_2, \cdots, x_n) \tag{31}$$

darstellen dürfen, und hieraus soll nach der obigen Definition der Operation d die Identität

$$d\varphi = \frac{\partial \varphi}{\partial x_1} dx_1 + \frac{\partial \varphi}{\partial x_2} dx_2 + \cdots + \frac{\partial \varphi}{\partial x_n} dx_n = \sum^{r} \frac{\partial \varphi}{\partial x_r} dx_r \tag{32}$$

folgen; mithin ist die Operation d vollständig bestimmt, sobald in jedem Punkte unseres Raumes die Werte der n Funktionen

$$dx_1, dx_2, \cdots, dx_n \tag{33}$$

gegeben sind. Umgekehrt, hat man diese n Funktionen willkürlich aus Φ gewählt, und bildet man daraus nach (32) für jede Funk-

tion φ eine zugehörige Funktion $d\varphi$ (welche für $\varphi = x_r$ offenbar mit der gewählten Funktion dx_r übereinstimmt), so ist leicht zu zeigen, daß die hierdurch bestimmte Operation d wirklich der obigen Grundforderung genügt. Denn durch partielle Derivation in bezug auf die Variable x_r ergibt sich aus der oben angenommenen Identität (29) bekanntlich

$$\frac{\partial F}{\partial \varphi_1}\frac{\partial \varphi_1}{\partial x_r} + \frac{\partial F}{\partial \varphi_2}\frac{\partial \varphi_2}{\partial x_r} + \cdots + \frac{\partial F}{\partial \varphi_m}\frac{\partial \varphi_m}{\partial x_r} = 0;$$

multipliziert man mit dx_r und summiert, indem man r die Indizes $1, 2, \cdots, n$ durchlaufen läßt, so ergibt sich mit Rücksicht auf (32) die zu beweisende Gleichung (30).

Aus dem in (29), (30) ausgedrückten Grundgesetz einer solchen Operation d leuchtet auch unmittelbar ihre Invarianz ein, d. h. sie bleibt dieselbe, wenn statt der Koordinaten x ein anderes System von n voneinander unabhängigen Funktionen y zur Ortsbestimmung gewählt wird, wobei die ihnen entsprechenden Funktionen dy gemäß (32) aus den Funktionen dx zu bestimmen sind. Auch versteht sich von selbst, daß zufolge desselben Gesetzes alle Regeln der gewöhnlichen Differentiation, wie

$$d(\varphi_1 \pm \varphi_2) = d\varphi_1 \pm d\varphi_2, \quad d(\varphi_1 \varphi_2) = \varphi_2 d\varphi_1 + \varphi_1 d\varphi_2$$

ihre volle Geltung behalten.

Unter den vielen verschiedenen Namen, welche man je nach der Beschaffenheit des Anwendungsgebietes einer solchen Operation d beilegen möchte*), will ich hier den in einem solchen Gebiet eingebürgerten, freilich in viel speziellerer Bedeutung gebrauchten Namen Vektor wählen, während die durch d erzeugten Funktionen $d\varphi$ unbedenklich Differentiale genannt werden können. Die partielle Derivation $\frac{\partial}{\partial x_r}$ in bezug auf die Variable x_r ist offenbar der spezielle Vektor d, für welchen die Differentiale (33) mit Ausnahme von dx_r, welches $= 1$ ist, identisch verschwinden. Es ist auch zweckmäßig, den Vektor Null einzuführen, und durch $d = 0$ anzudeuten, daß alle n Funktionen (33), also auch alle $d\varphi$ identisch verschwinden;

*) Immer von einer Differentiation erster Ordnung oder Variation erster Ordnung zu sprechen, ist zu unbequem. Sophus Lie gebraucht für seine Symbole $X(f)$, die mit den Vektoren identisch sind, den Namen infinitesimale Transformation (Theorie der Transformationsgruppen; Abschnitt 1, Kapitel 3, § 13, S. 54).

eine Verwirrung ist hierbei nicht zu befürchten, weil aus dem Zusammenhang sich immer ergeben wird, ob von der Zahl oder dem Vektor Null die Rede ist.

Da ein Vektor d aus jedem Element φ des Systems Φ ein ebenfalls in Φ enthaltenes Element $d\varphi$ erzeugt, so fällt diese Operation unter den viel allgemeineren Begriff einer Abbildung des Systems Φ in sich selbst. Solche Abbildungen, die im folgenden ausschließlich durch Buchstaben e (mit Akzenten oder Indizes) bezeichnet werden sollen, gestatten sehr mannigfaltige Verbindungen und symbolische Rechnungen, die ich jetzt erkläre, um sie später auf unsere Vektoren anzuwenden. Eine Abbildung e von Φ in sich selbst erzeugt aus jedem Element φ des Systems Φ ein mit $e\varphi$ zu bezeichnendes Bild, welches wieder eine in Φ enthaltene Funktion ist, und die Abbildungen e, e' gelten stets und nur dann für eine und dieselbe — was durch $e = e'$ ausgedrückt wird —, wenn für jede Funktion φ die Identität $e\varphi = e'\varphi$ besteht. Aus je zwei Abbildungen e_1, e_2 entspringt eine als Produkt $e_1 e_2$ zu bezeichnende Abbildung, welche durch die für jede Funktion φ geltende Identität $(e_1 e_2)\varphi = e_1(e_2\varphi) = e_1 e_2 \varphi$ erklärt wird und von dem Produkt $e_2 e_1$ wohl zu unterscheiden ist; ersetzt man aber in dieser Definition die willkürliche Funktion φ durch $e_3\varphi$, wo e_3 eine beliebige Abbildung bedeutet, so ergibt sich unmittelbar die Geltung des Assoziationsgesetzes

$$(e_1 e_2)e_3 = e_1(e_2 e_3) = e_1 e_2 e_3,$$

und hieraus folgt in bekannter Weise die bestimmte Bedeutung eines aus m Abbildungen in vorgeschriebener Folge gebildeten Produkts $e_1 e_2 \cdots e_m$. Zwei Abbildungen e_1, e_2 heißen permutabel, wenn $e_1 e_2 = e_2 e_1$ ist.

Ebenso sollen Summe und Differenz $(e_1 \pm e_2)$ und, wenn λ eine Funktion in Φ ist, das Produkt λe durch

$$(e_1 \pm e_2)\varphi = e_1\varphi \pm e_2\varphi \quad \text{und} \quad (\lambda e)\varphi = \lambda(e\varphi) = \lambda e\varphi$$

erklärt werden, und eine symbolische Gleichung von der Form

$$e = \lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_m e_m = \sum_{\iota}^{\iota} \lambda_\iota e_\iota, \tag{34}$$

wo die λ_ι Funktionen in Φ sind, soll bedeuten, daß für jede Funktion φ die Identität

$$e\varphi = \sum_{\iota}^{\iota} \lambda_\iota e_\iota \varphi \tag{35}$$

besteht. Ersetzt man φ durch $e'\varphi$, wo e' eine beliebige Abbildung bedeutet, so ergibt sich, daß die symbolische Gleichung

$$\lambda e e' = \sum^{\iota} \lambda \lambda_\iota e_\iota e', \tag{36}$$

wo λ eine Funktion bedeutet, eine notwendige Folge der Gleichung (34) ist, d. h. man darf eine solche Gleichung gliedweise von links mit einer Funktion λ, von rechts mit einer Funktion φ oder einer Abbildung e' multiplizieren; ebenso darf man solche Gleichungen addieren und subtrahieren, wie wenn die Abbildungen e Größen wären. Da ferner ein Vektor d alle Regeln der gewöhnlichen Differentiation befolgt, so ergibt sich aus (35) ebenso, daß auch die symbolische Gleichung

$$de = \sum^{\iota} \lambda_\iota de_\iota + \sum^{\iota} d\lambda_\iota e_\iota \tag{37}$$

eine Folge von (34) ist.

Wir betrachten im folgenden nur solche Abbildungen e, welche entweder selbst Vektoren oder Produkte von mehreren Vektoren sind. Hat man ein System von m Vektoren $d_1, d_2, \cdots, d_m$ und ebenso vielen Funktionen $\lambda_1, \lambda_2, \cdots, \lambda_m$, so ergibt sich aus der Gleichung (32), wenn man sie für jeden Vektor d_ι in Anspruch nimmt und von links mit λ_ι multipliziert, daß jede Abbildung von der Form

$$d = \lambda_1 d_1 + \lambda_2 d_2 + \cdots + \lambda_m d_m = \sum^{\iota} \lambda_\iota d_\iota \tag{38}$$

wieder ein Vektor ist; einen solchen Vektor d nennen wir abhängig von den m Vektoren d_ι, und ebenso sagen wir, daß diese m Vektoren d_ι voneinander abhängig seien oder ein reduzibles System bilden, falls es m Funktionen λ_ι gibt, die nicht alle identisch verschwinden, und für welche der vorstehende Vektor $d = 0$ wird. Offenbar tritt dieser Fall immer ein, wenn $m > n$ ist; ist aber $m \leqq n$, so wird er dadurch charakterisiert, daß alle Determinanten m-ten Grades, die man aus den m Zeilen und aus m Spalten des Systems

$$\begin{array}{cccc} d_1 x_1, & d_1 x_2, & \cdots, & d_1 x_n \\ d_2 x_1, & d_2 x_2, & \cdots, & d_2 x_n \\ \cdots & \cdots & \cdots & \cdots \\ d_m x_1, & d_m x_2, & \cdots, & d_m x_n \end{array}$$

bilden kann, identisch verschwinden. Wir sagen ferner, die m Vektoren d_ι in (38) seien voneinander unabhängig oder sie bilden ein irreduzibles System, wenn die Forderung $d = 0$ nur durch das identische Verschwinden aller m Funktionen λ_ι erfüllt wird. Bilden n Vektoren $d_1, d_2, \cdots, d_n$ ein solches irreduzibles System, so läßt sich jeder Vektor d in der Form

$$(39) \qquad d = \lambda_1 d_1 + \lambda_2 d_2 + \cdots + \lambda_n d_n = \sum^{r} \lambda_r d_r$$

darstellen, wo die n Funktionen λ_r durch d vollständig bestimmt sind. Ein solches System bilden offenbar die n partiellen Derivationen $\frac{\partial}{\partial x_r}$, und die vorstehende Gleichung geht dann in

$$d = \sum^{r} dx_r \frac{\partial}{\partial x_r}$$

über, die mit (32) übereinstimmt.

Wir wollen jetzt zwei beliebige Vektoren d_1, d_2 betrachten und die daraus entspringenden Produkte $d_1 d_2$ und $d_2 d_1$ miteinander vergleichen. Zufolge (32) ist

$$d_2 \varphi = \sum^{r} \frac{\partial \varphi}{\partial x_r} d_2 x_r, \qquad d_1 \frac{\partial \varphi}{\partial x_r} = \sum^{s} \frac{\partial}{\partial x_s}\left(\frac{\partial \varphi}{\partial x_r}\right) d_1 x_s,$$

wo r, s die Indizes 1, 2, $\cdots$, n durchlaufen, und da jeder Vektor die Regeln der totalen Differentiation befolgt, so wird

$$d_1 d_2 \varphi = \sum^{r} \frac{\partial \varphi}{\partial x_r} d_1 d_2 x_r + \sum^{r,s} \frac{\partial}{\partial x_s}\left(\frac{\partial \varphi}{\partial x_r}\right) d_1 x_s d_2 x_r$$

und ebenso durch Vertauschung von d_1, d_2

$$d_2 d_1 \varphi = \sum^{r} \frac{\partial \varphi}{\partial x_r} d_2 d_1 x_r + \sum^{r,s} \frac{\partial}{\partial x_s}\left(\frac{\partial \varphi}{\partial x_r}\right) d_2 x_s d_1 x_r;$$

vertauscht man in der letzten Doppelsumme die beiden voneinander unabhängigen Summationsbuchstaben r, s miteinander, so ergibt sich aus der Annahme (28) ihre Identität mit der Doppelsumme, welche in der Darstellung von $d_1 d_2 \varphi$ auftritt; durch Subtraktion erhält man daher die Gleichung

$$(d_1 d_2 - d_2 d_1)\varphi = \sum^{r} \frac{\partial \varphi}{\partial x_r} (d_1 d_2 - d_2 d_1) x_r,$$

in welcher nur die Derivierten erster Ordnung der willkürlichen Funktion φ auftreten. Definiert man daher eine neue Operation oder Abbildung (d_1, d_2) durch

$$(40) \qquad (d_1, d_2) = d_1 d_2 - d_2 d_1 = -(d_2, d_1),$$

so wird

$$(41) \qquad (d_1, d_2)\varphi = \sum^{r} \frac{\partial \varphi}{\partial x_r} (d_1, d_2) x_r,$$

und durch Vergleichung mit (32) ergibt sich der wichtige Satz, daß diese Abbildung (d_1, d_2) wieder ein Vektor ist. Dieser Satz ist meines Wissens zuerst von Jacobi gefunden (in § 23 der nachgelassenen Abhandlung Nova methodus, aequationes differentiales partiales primi ordinis inter numerum variabilium quemcunque propositas integrandi, dieses Journal Bd. 60) und bildet eine wesentliche Grundlage seiner Untersuchungen über die partiellen Differentialgleichungen. Ich bemerke ausdrücklich, daß die von ihm mit A, B bezeichneten Operationen vollständig identisch mit unseren Vektoren sind; daß aber diese Operationen nicht nur die Gesetze der totalen Differentiation befolgen, sondern daß gerade in dieser, alles andere einschließenden Eigenschaft ihr ganzes Wesen besteht, scheint nirgends deutlich erkannt und in aller Schärfe ausgesprochen zu sein.

Daß zwei Vektoren d_1, d_2 permutabel sind, daß also $d_1 d_2 = d_2 d_1$ ist, wird jetzt durch $(d_1, d_2) = 0$ ausgedrückt. Wir betrachten nun drei beliebige Vektoren d_1, d_2, d_3 und bilden daraus die Abbildung

$$(42) \qquad (d_1; d_2, d_3) = d_1(d_2, d_3) - (d_2, d_3) d_1 = -(d_1; d_3, d_2),$$

welche zufolge des eben erhaltenen Fundamentalsatzes ebenfalls ein Vektor ist; verfährt man nach den bei (34), (36), (37) angegebenen Regeln, so erhält man

$$(d_1; d_2, d_3) = (d_1 d_2 d_3 + d_3 d_2 d_1) - (d_2 d_3 d_1 + d_1 d_3 d_2),$$

und hieraus ergibt sich durch zyklische Vertauschung und Addition der Satz*)

$$(43) \qquad (d_1; d_2, d_3) + (d_2; d_3, d_1) + (d_3; d_1, d_2) = 0.$$

Wenden wir dieselben Regeln auf die Gleichung (38) an, die wir wieder in der Form

$$(44) \qquad d = \sum^{\iota} \lambda_\iota d_\iota$$

*) Derselbe Satz findet sich in dem angeführten Werke von Lie (Abschnitt 1, Kapitel 5, § 26).

darstellen, und bezeichnen wir mit d' einen beliebigen Vektor, so erhalten wir

$$dd' = \sum^{\iota} \lambda_\iota d_\iota d', \quad d'd = \sum \lambda_\iota d' d_\iota + \sum d' \lambda_\iota d_\iota;$$

subtrahiert man die erste Gleichung von der zweiten und wendet die Symbolik (40) an, so ergibt sich die Vektorgleichung

$$(45) \qquad (d', d) = \sum^{\iota} \lambda_\iota (d', d_\iota) + \sum^{\iota} d' \lambda_\iota d_\iota$$

als eine notwendige Folge von (44).

Bezeichnet man die aus einem Vektor d durch Wiederholung entspringenden Abbildungen dd, $ddd \cdots$ bzw. mit d^2, $d^3 \cdots$, so gelten auch für diese Operationen die gewöhnlichen Regeln der Differentiation, z. B.

$$d^2\varphi = \sum^{r} \frac{\partial \varphi}{\partial x_r} d^2 x_r + \sum^{r,s} \frac{\partial^2 \varphi}{\partial x_r \partial x_s} dx_r dx_s.$$

Genügen die n Differentiale dx_r den partiellen Differentialgleichungen $d^2 x_r = 0$ (was z. B. immer dann eintritt, wenn sie konstant sind), so folgt

$$d^2\varphi = \sum^{r,s} \frac{\partial^2 \varphi}{\partial x_r \partial x_s} dx_r dx_s,$$

und wenn man für φ eine ganze homogene Funktion zweiten Grades $F = F(x_1, x_2, \cdots, x_n)$ wählt, so wird

$$(46) \qquad d^2 F = 2F(dx_1, dx_2, \cdots, dx_n).$$

Im Falle $n = 2$ wollen wir mit x, y die unabhängigen Variabeln und mit d einen Vektor bezeichnen, der den Bedingungen $d^2 x = d^2 y = 0$ genügt. Betrachten wir nun eine binäre quadratische Form

$$(47) \qquad F = F(x, y) = Ax^2 + Bxy + Cy^2$$

und setzen deren Diskriminante

$$(48) \qquad B^2 - 4AC = D,$$

so wird

$$(49) \qquad \begin{cases} dF = (2Ax + By)dx + (Bx + 2Cy)dy \\ \qquad\quad = x(2Adx + Bdy) + y(Bdx + 2Cdy) \end{cases}$$

und

$$(50) \qquad \tfrac{1}{2} d^2 F = Adx^2 + Bdxdy + Cdy^2 = F(dx, dy).$$

Diese Gleichungen lassen sich, wenn man die Multiplikation der binären Substitutionen benutzt, auch in der Form

$$\begin{pmatrix} 2F, & dF \\ dF, & d^2F \end{pmatrix} = \begin{pmatrix} x, & y \\ dx, & dy \end{pmatrix} \begin{pmatrix} 2A, & B \\ B, & 2C \end{pmatrix} \begin{pmatrix} x, & dx \\ y, & dy \end{pmatrix} \tag{51}$$

darstellen, und aus dem Satze über die Determinante eines Produkts von Substitutionen ergibt sich

$$dF^2 - 2Fd^2F = D(xdy - ydx)^2. \tag{52}$$

Es braucht aber kaum gesagt zu werden, daß dies nichts anderes ist als der bekannte, auch in § 1 benutzte Fundamentalsatz für die Transformation einer binären quadratischen Form F von der Diskriminante D durch eine binäre Substitution $\begin{pmatrix} x, & dx \\ y, & dy \end{pmatrix}$, und daß der vorstehende Beweis ganz unabhängig von der hier vorgetragenen Theorie der Vektoren ist; der Satz sollte nur im Anschluß an diese Theorie in einer solchen Form dargestellt werden, wie wir ihn demnächst gebrauchen werden.

§ 4.

Wir kehren jetzt zu der in § 1 geführten Untersuchung zurück, um sie in anderer Form zu wiederholen und fortzusetzen. Wir betrachten, wie dort, drei Paare von unabhängigen Variabeln (x_1, y_1), (x_2, y_2), (x_3, y_3), die wir kurz die Paare z_1, z_2, z_3 nennen, und wollen in diesem sechsfach ausgedehnten analytischen Raume die Eigenschaften einer binären trilinearen Form H untersuchen, d. h. einer ganzen Funktion, welche in bezug auf jedes der drei Paare homogen vom ersten Grade ist. Hieraus folgt zunächst

$$H = x_1 \frac{\partial H}{\partial x_1} + y_1 \frac{\partial H}{\partial y_1} = x_2 \frac{\partial H}{\partial x_2} + y_2 \frac{\partial H}{\partial y_2} = x_3 \frac{\partial H}{\partial x_3} + y_3 \frac{\partial H}{\partial y_3}. \tag{53}$$

Bezeichnen wir (wie in § 1) mit r, s, t irgendeine Permutation der drei Indizes 1, 2, 3, so können wir drei Vektoren d_1, d_2, d_3 durch die gemeinsame Definition

$$d_r\varphi = \frac{\partial \varphi}{\partial x_r}\frac{\partial H}{\partial y_r} - \frac{\partial \varphi}{\partial y_r}\frac{\partial H}{\partial x_r} \tag{54}$$

einführen, wo φ, wie immer im folgenden, jede willkürliche Funktion der sechs Variabeln bedeuten soll. Zufolge (32) ist daher

$$d_r x_r = \frac{\partial H}{\partial y_r}, \quad d_r y_r = -\frac{\partial H}{\partial x_r} \tag{55}$$

und

$$d_r x_s = d_r y_s = d_r x_t = d_r y_t = 0; \tag{56}$$

für den Vektor d_r verhalten sich daher die Paare z_s, z_t wie Konstanten, während $d_r x_r$, $d_r y_r$ bilineare Funktionen dieser beiden Paare, also konstant in bezug auf das Paar z_r sind. Ist daher φ homogen in bezug auf jedes einzelne Paar, und zwar vom Grade m_r in bezug auf z_r, so ist $d_r\varphi$ homogen von den Graden $m_r - 1$, $m_s + 1$, $m_t + 1$ in bezug auf die Paare z_r, z_s, z_t. Aus (54) folgt zunächst

$$d_r H = 0, \tag{57}$$

und zufolge (55) nehmen die Gleichungen (53) die Form

$$H = y_s d_s x_s - x_s d_s y_s \tag{58}$$

an.

Um nun den in (40) erklärten Vektor $(d_r, d_s) = -(d_s, d_r)$ zu bilden, entwickeln wir die Gleichung (57), indem wir die Operation d_r an dem Ausdruck (58) mit Rücksicht auf (56) vollziehen, woraus $y_s d_r d_s x_s = x_s d_r d_s y_s$ folgt; setzt man diese durch x_s und y_s, also auch durch $x_s y_s$ teilbare ganze Funktion $= x_s y_s F_{r,s}$, so wird

$$d_r d_s x_s = x_s F_{r,s}, \quad d_r d_s y_s = y_s F_{r,s}. \tag{59}$$

Da nun $d_s x_s$, $d_s y_s$ bilineare Funktionen von z_r, z_t, also $d_r d_s x_s$ und $d_r d_s y_s$ homogen vom ersten Grade in bezug auf z_s, vom zweiten Grade in bezug auf z_t und frei von z_r sind, so ist $F_{r,s}$ eine binäre quadratische Form des Paares z_t mit konstanten Koeffizienten. Zufolge (56) ist nun

$$d_s d_r x_s = d_s d_r y_s = 0,$$

mithin können wir die Gleichungen (59) durch

$$(d_r, d_s) x_s = x_s F_{r,s}, \quad (d_r, d_s) y_s = y_s F_{r,s}$$

ersetzen; vertauscht man r mit s, wodurch (d_r, d_s) in $(d_s, d_r) = -(d_r, d_s)$ übergeht, so folgt hieraus

$$(d_r, d_s) x_r = -x_r F_{s,r}, \quad (d_r, d_s) y_r = -y_r F_{s,r},$$

wo $F_{s,r}$ ebenfalls eine quadratische Form des Paares z_t bedeutet. Da ferner die Variabeln x_t, y_t sich für beide Vektoren d_r, d_s wie Konstanten verhalten, so ist $(d_r, d_s) x_t = 0$, $(d_r, d_s) y_t = 0$.

Hiermit ist der Vektor (d_r, d_s) vollständig bestimmt, und zufolge (32) wird

$$(d_r, d_s)\varphi = F_{r,s}\left(x_s \frac{\partial \varphi}{\partial x_s} + y_s \frac{\partial \varphi}{\partial y_s}\right) - F_{s,r}\left(x_r \frac{\partial \varphi}{\partial x_r} + y_r \frac{\partial \varphi}{\partial y_r}\right). \tag{60}$$

Dies Resultat gibt Veranlassung, drei neue, von der Form H ganz unabhängige Vektoren e_1, e_2, e_3 durch die gemeinsame Erklärung

$$e_r\varphi = x_r\frac{\partial\varphi}{\partial x_r} + y_r\frac{\partial\varphi}{\partial y_r} \tag{61}$$

einzuführen, woraus

$$e_r x_r = x_r, \quad e_r y_r = y_r \tag{62}$$

und

$$e_r x_s = e_r y_s = e_r x_t = e_r y_t = 0 \tag{63}$$

folgt. Daß eine Funktion φ homogen in bezug auf das Paar z_r, und zwar vom Grade m_r ist, wird jetzt durch $e_r\varphi = m_r\varphi$ ausgedrückt; die Gleichungen (53) lauten daher

$$e_r H = H, \tag{64}$$

und die Gleichung (60) geht über in

$$(d_r, d_s)\varphi = F_{r,s}e_s\varphi - F_{s,r}e_r\varphi.$$

Setzt man nun $\varphi = H$ und bedenkt, daß zufolge (57) auch $(d_r, d_s)H = 0$ ist, so erhält man $(F_{r,s} - F_{s,r})H = 0$, und da wir annehmen, daß die Form H nicht identisch verschwindet, so ergibt sich $F_{r,s} = F_{s,r}$ (was übrigens auch in dem ausgeschlossenen Falle $H = 0$ gelten würde, weil zufolge (55), (59) dann beide Formen $F_{r,s}, F_{s,r}$ identisch verschwinden); wir dürfen daher diese quadratische Form des Paares z_t einfacher durch $F_t = F_t(x_t, y_t)$ bezeichnen, und zugleich nimmt die vorhergehende Gleichung die Form

$$(d_r, d_s)\varphi = F_t(e_s\varphi - e_r\varphi) \tag{65}$$

an, welche nach (34) symbolisch auch durch

$$(d_r, d_s) = F_t(e_s - e_r) \tag{66}$$

ausgedrückt werden kann, und die Gleichungen (59) lauten jetzt

$$d_r d_s x_s = x_s F_t, \quad d_r d_s y_s = y_s F_t. \tag{67}$$

Daß übrigens die durch die erste Gleichung (59) vollständig definierte Größe $F_{r,s}$ symmetrisch in bezug auf r, s ist, hätte man schon dort leicht zeigen können; denn setzt man in (54) die willkürliche Funktion

$$\varphi = d_s x_s = \frac{\partial H}{\partial y_s},$$

so erhält man

$$x_s F_{r,s} = \frac{\partial^2 H}{\partial x_r \partial y_s}\frac{\partial H}{\partial y_r} - \frac{\partial^2 H}{\partial y_r \partial y_s}\frac{\partial H}{\partial x_r},$$

und da die hier auftretenden Derivierten zweiter Ordnung ebenso wie $F_{r,s}$ nur noch die beiden Variabeln x_t, y_t enthalten, so ergibt sich die genannte Symmetrie durch partielle Derivation nach x_s, und wir erhalten für die Form $F_{r,s} = F_{s,r} = F_t$ den Ausdruck

$$F_t = \frac{\partial^2 H}{\partial x_r \partial y_s} \frac{\partial^2 H}{\partial y_r \partial x_s} - \frac{\partial^2 H}{\partial y_r \partial y_s} \frac{\partial^2 H}{\partial x_r \partial x_s}. \tag{68}$$

Um jetzt den Zusammenhang der gegenwärtigen Untersuchung mit der in § 1 deutlich zu machen, bemerke ich folgendes. Identifiziert man die Form H mit der dort in (12) dargestellten Funktion, so sind die Konstanten α_0, β_0, α_r, β_r bzw. die Koeffizienten von $x_1 x_2 x_3$, $y_1 y_2 y_3$, $x_r y_s y_t$, $y_r x_s x_t$; die in (55) erklärten Größen $d_r x_r$, $d_r y_r$ sind identisch mit den Funktionen X_r, Y_r in (10), und der vorstehende Ausdruck für F_t stimmt vollständig mit der dortigen Definition (1) der drei Formen F_1, F_2, F_3 überein.

Den Satz (65) wenden wir jetzt auf zwei Beispiele an. Setzt man zuerst $\varphi = F_s$, so folgt

$$d_r d_s F_s = 2 F_s F_t, \tag{69}$$

weil $d_r F_s = 0$, $e_s F_s = 2 F_s$, $e_r F_s = 0$ ist. Setzt man zweitens $\varphi = d_t x_t$ und bedenkt, daß diese Funktion bilinear in bezug auf die beiden Paare z_r, z_s, daß also

$$e_s d_t x_t = e_r d_t x_t = d_t x_t \tag{70}$$

ist, so erhält man $d_r d_s d_t x_t = d_s d_r d_t x_t$; zufolge (67) ist aber $d_s d_t x_t = x_t F_r$, und $d_r d_t x_t = x_t F_s$, mithin wird $d_r (x_t F_r) = d_s (x_t F_s)$, und da x_t für beide Vektoren d_r, d_s konstant ist, so folgt der wichtige Satz

$$d_r F_r = d_s F_s. \tag{71}$$

Diese Funktion ist also symmetrisch in bezug auf alle drei Indizes 1, 2, 3 und offenbar eine neue trilineare Form, die wir mit H' bezeichnen und die zu H adjungierte Form nennen wollen; es ist also

$$H' = d_1 F_1 = d_2 F_2 = d_3 F_3, \tag{72}$$

und der Satz (69) geht in

$$d_r H' = d_r^2 F_r = 2 F_s F_t \tag{73}$$

über. Da zufolge (55) der Vektor d_r den Bedingungen $d_r^2 x_r = d_r^2 y_r = 0$ genügt, so können wir hier die am Schlusse von § 3 bewiesenen Sätze

(50), (52) anwenden. Zufolge (50) läßt sich die Gleichung (73) auch in der Form

$$F_r(d_r x_r,\ d_r y_r) = F_s F_t \tag{74}$$

darstellen, und dies Resultat ist offenbar vollständig identisch mit dem Hauptsatz (11) in § 1, welcher dort auf ganz anderem Wege bewiesen ist. Bezeichnet man ferner mit D_r die Diskriminante der Form F_r, so folgt aus (52) die Gleichung

$$d_r F_r^2 - 2 F_r d_r^2 F_r = D_r (x_r d_r y_r - y_r d_r x_r)^2,$$

welche zufolge (72), (73), (58) die Form

$$H'^2 - 4 F_r F_s F_t = D_r H^2$$

annimmt; da $F_r F_s F_t = F_1 F_2 F_3$ und H, H' symmetrisch in bezug auf die Indizes 1, 2, 3 sind, so folgt hieraus, daß die Formen F_1, F_2, F_3 dieselbe Diskriminante

$$D = D_1 = D_2 = D_3 \tag{75}$$

besitzen, was mit dem Satze (3) in § 1 übereinstimmt, und zugleich ergibt sich, daß zwischen den beiden trilinearen Formen H, H' und den drei quadratischen Formen F_1, F_2, F_3 die Identität

$$H'^2 - DH^2 = 4 F_1 F_2 F_3 \tag{76}$$

besteht.

Der Satz (71), auf welchem die Einführung der zu H adjungierten Form H' beruht, läßt sich auf einem zwar nicht kürzeren, aber mehr symmetrischen Wege beweisen, den ich hier noch andeuten will. Aus den Definitionen (55), (56), (62), (63) ergibt sich leicht die Vektoridentität

$$(d_t,\ e_r) = -d_t; \tag{77}$$

vertauscht man r mit s und subtrahiert, so folgt $(d_t,\ e_s - e_r) = 0$, d. h. die beiden Vektoren d_t und $(e_s - e_r)$ sind permutabel. Unterwirft man daher die Gleichung (66) nach der in (45) angegebenen Regel dem Vektor d_t und benutzt das in (42) erklärte Symbol, so erhält man

$$(d_t;\ d_r,\ d_s) = d_t F_t (e_s - e_r), \tag{78}$$

und aus dem Satze (43) folgt

$$(d_2 F_2 - d_3 F_3) e_1 + (d_3 F_3 - d_1 F_1) e_2 + (d_1 F_1 - d_2 F_2) e_3 = 0;$$

da aber die drei Vektoren e_1, e_2, e_3 zufolge ihrer Definition (62), (63) offenbar ein irreduzibles System bilden, so müssen die drei Differenzen $(d_r F_r - d_s F_s)$ identisch verschwinden, wie zu beweisen war.

Ich bemerke endlich noch folgendes. Wenn für eine partikuläre Form H die Form F_1 identisch verschwindet, so muß zufolge (72), (74) auch H' und mindestens eine der beiden Formen F_2, F_3 identisch verschwinden. Man findet leicht, daß das Verschwinden der beiden Formen F_1, F_2 stets und nur dann eintritt, wenn $H = h_{1,2} h_3$ ist, wo $h_{1,2}$ eine bilineare Funktion der Paare z_1, z_2, und h_3 eine lineare Funktion des Paares z_3 bedeutet. Verschwinden alle drei Formen F_1, F_2, F_3, so ist $H = h_1 h_2 h_3$ ein Produkt von drei linearen Faktoren, und umgekehrt.

§ 5.

Es liegt nahe, die eben geführte Untersuchung von der Form H auf die zu ihr adjungierte Form H' zu übertragen. Bezeichnet man mit d_r', F_r' die Vektoren und quadratischen Formen, die hierbei aus den auf H bezüglichen Vektoren und Formen d_r, F_r hervorgehen, während die in (61) erklärten Vektoren e_r ihre von H gänzlich unabhängige Bedeutung behalten, so ist

$$d_r' \varphi = \frac{\partial \varphi}{\partial x_r} \frac{\partial H'}{\partial y_r} - \frac{\partial \varphi}{\partial y_r} \frac{\partial H'}{\partial x_r}; \tag{79}$$

hieraus folgt zunächst die mit (57) analoge Gleichung

$$d_r' H' = 0, \tag{80}$$

und durch den Vergleich mit (54), (73) ergibt sich

$$d_r' H = -d_r H' = -2 F_s F_t; \tag{81}$$

ebenso entspricht der Gleichung (64) die Gleichung

$$e_r H' = H'. \tag{82}$$

Sodann bemerken wir, daß die drei Vektoren d_r, e_r, d_r' gewiß ein reduzibles System bilden, weil die beiden Paare z_s, z_t sich gegen sie wie Konstanten verhalten; es muß also eine Identität von der Form

$$\lambda d_r + \lambda' d_r' + \mu e_r = 0$$

bestehen, wo λ, λ', μ Funktionen bedeuten, die nicht alle verschwinden; unterwirft man dieser Identität die beiden Formen H, H' und berücksichtigt (57), (64), (80), (81), (82), so folgt

$$\lambda'(-2 F_s F_t) + \mu H = 0, \quad \lambda(2 F_s F_t) + \mu H' = 0,$$

mithin wird

$$-H' d_r + H d_r' + 2 F_s F_t e_r = 0. \tag{83}$$

Wendet man dieses Resultat auf die Funktion F_r an und bedenkt, daß $d_r F_r = H'$, $e_r F_r = 2F_r$ ist, so folgt

$$-H'^2 + H d'_r F_r + 4 F_r F_s F_t = 0,$$

und zufolge (76) ergibt sich

$$d'_r F_r = DH. \tag{84}$$

Überträgt man jetzt den Satz (66) auf die Form H', so erhält man

$$(d'_r, d'_s) = F'_t(e_s - e_r),$$

was als Definition der quadratischen Form F'_t angesehen werden kann. Läßt man diesen Vektor auf die Form F_s wirken, so wird die rechte Seite $= 2F_s F'_t$; da ferner $d'_r F_s = 0$, $d'_s F_s = DH$, also $(d'_r, d'_s)F_s = d'_r d'_s F_s = D d'_r H = D(-2F_s F_t)$ ist, so folgt

$$F'_t = -DF_t; \tag{85}$$

die gemeinsame Diskriminante D' der drei Formen F'_1, F'_2, F'_3 ist daher

$$D' = D^3, \tag{86}$$

und die vorhergehende Vektoridentität wird

$$(d'_r, d'_s) = -DF_t(e_s - e_r) = -D(d_r, d_s). \tag{87}$$

Endlich folgt aus der Definition (72) der zu H adjungierten Form H', daß die zu H' adjungierte Form $= d'_t F'_t = -D d'_t F_t = -D^2 H$, also die mit $(-D^2)$ multiplizierte erste Form H ist, und hiermit leuchtet ein, daß die Identität (76) bei dem Übergang von H zu H' sich nur mit $(-D^3)$ multipliziert. —

Die Form H und ihre Adjungierte H' bilden die Basis einer Schar von unendlich vielen trilinearen Formen

$$H'' = Hp + H'q, \tag{88}$$

wo p, q zwei willkürliche Konstanten bedeuten. Behandelt man eine solche Form H'' ebenso wie H in § 4 und definiert drei ihr entsprechende Vektoren d''_r durch

$$d''_r \varphi = \frac{\partial \varphi}{\partial x_r}\frac{\partial H''}{\partial y_r} - \frac{\partial \varphi}{\partial y_r}\frac{\partial H''}{\partial x_r}, \tag{89}$$

so wird offenbar

$$d''_r H''_r = 0, \quad d''_r = p d_r + q d'_r, \tag{90}$$

und aus den für die Vektoren d_r, d'_r gefundenen Resultaten ergibt sich

$$d''_r H = -2F_s F_t q, \quad d''_r H' = +2F_s F_t p, \tag{91}$$

$$d''_r F_r = H'p + DHq, \tag{92}$$

also

$$(d_r'', d_s'')F_s = d_r'' d_s'' F_s = 2F_s F_t m, \tag{93}$$

wo

$$m = p^2 - Dq^2. \tag{94}$$

Die aus der Form H'' entspringenden quadratischen Formen F_1'', F_2'', F_3'' sind nach (66) durch die Vektoridentität

$$(d_r'', d_s'') = F_t''(e_s - e_r)$$

zu erklären, und aus (93) folgt

$$F_t'' = mF_t, \tag{95}$$

$$(d_r'', d_s'') = mF_t(e_s - e_r) = m(d_r, d_s). \tag{96}$$

Die Trias der zu den trilinearen Formen H'' der Schar (88) gehörenden quadratischen Formen ist daher invariant, wenn man von gemeinsamen konstanten Faktoren m absieht. Drei solche Formen (95) besitzen die gemeinsame Diskriminante

$$D'' = Dm^2,$$

und für die zu H'' adjungierte Form $H''' = d_r'' F_r''$ findet man nach (95), (92) den Ausdruck

$$H''' = m(H'p + DHq); \tag{97}$$

diese Form ist daher ebenfalls in der Schar (88) enthalten.

Um endlich die aus (76) hervorgehende Identität

$$H'''^2 - D''H''^2 = 4F_1''F_2''F_3'' \tag{98}$$

zu bestätigen, wollen wir die Quadratwurzeln aus den Diskriminanten D und $D'' = Dm^2$ einführen und ihren Zusammenhang immer so bestimmen, daß

$$\sqrt{D''} = m\sqrt{D} \tag{99}$$

wird; dann folgt aus (88), (97) die Gleichung

$$H''' + H''\sqrt{D''} = m(p + q\sqrt{D})(H' + H\sqrt{D}); \tag{100}$$

ersetzt man hierin $\sqrt{D}$ durch $-\sqrt{D}$, also auch $\sqrt{D''}$ durch $-\sqrt{D''}$, und multipliziert beide Gleichungen miteinander, so folgt

$$H'''^2 - D''H''^2 = m^3(H'^2 - DH^2),$$

was zufolge (76), (95) mit der zu beweisenden Gleichung (98) übereinstimmt. —

Der in (96) erhaltene Satz gibt noch zu folgenden Bemerkungen Veranlassung. Entwickelt man den Vektor (d_r'', d_s'') nach den in § 3 angegebenen Regeln aus der Definition (90), so wird

$$(d_r'', d_s'') = p^2(d_r, d_s) + pq\{(d_r, d_s') + (d_r', d_s)\} + q^2(d_r', d_s');$$

die Vergleichung mit (96), wo $m = p^2 - Dq^2$, ergibt daher wieder den Satz (87), und da der mit pq multiplizierte Vektor verschwinden muß, so erhält man den neuen Satz, daß der Vektor

$$(d_r, d_s') = (d_s, d_r'), \tag{101}$$

also symmetrisch in bezug auf die beiden Indizes r, s ist. Dasselbe Resultat ergibt sich auch, wenn man nach der in § 3 angegebenen Regel (45) die Identität (83) dem Vektor d_s unterwirft und hierbei die Sätze (66), (77) benutzt; auf diese Weise erhält man den symmetrischen Ausdruck

$$H(d_s, d_r') = F_t\{2F_r d_r - H' e_r + 2F_s d_s - H' e_s\}, \tag{102}$$

der sich aber noch einfacher darstellen läßt.

Führt man nämlich noch drei Vektoren δ_1, δ_2, δ_3 durch die gemeinsame Erklärung

$$\delta_r \varphi = \frac{\partial \varphi}{\partial x_r}\frac{\partial F_r}{\partial y_r} - \frac{\partial \varphi}{\partial y_r}\frac{\partial F_r}{\partial x_r} \tag{103}$$

ein*), so folgt unmittelbar

$$\delta_r F_r = 0; \tag{104}$$

vergleicht man ferner (103) mit den Definitionen (54), (79) und berücksichtigt (72), (84), so erhält man

$$\delta_r H = -d_r F_r = -H', \quad \delta_r H' = -d_r' F_r = -DH. \tag{105}$$

Die drei Vektoren δ_r, d_r, e_r bilden offenbar wieder ein reduzibles System, und wenn man ähnlich verfährt, wie bei der Herleitung des Satzes (83), indem man die beiden vorstehenden Ausdrücke für $\delta_r F_r$, $\delta_r H$ benutzt, so ergibt sich

$$H\delta_r = 2F_r d_r - H' e_r, \tag{106}$$

wodurch die Gleichung (102) in

$$(d_s, d_r') = F_t(\delta_r + \delta_s) = (d_r, d_s') \tag{107}$$

übergeht. Eliminiert man aus den beiden Gleichungen (83), (106) einmal d_r, dann e_r, mit Rücksicht auf (76), so erhält man noch zwei ähnliche Relationen, die sich aber auch aus (104), (105) ableiten

*) Ich bemerke beiläufig, daß hieraus $\delta_r^2 x_r = D x_r$, $\delta_r^2 y_r = D y_r$ folgt.

ließen; das System dieser vier Gleichungen, durch welche die Abhängigkeit von je drei der vier Vektoren e_r, d_r, d'_r, δ_r ausgedrückt wird, ist das folgende:

$$(108)\quad \begin{cases} * & DHd_r - H'd'_r + 2F_sF_t\delta_r = 0, \\ -DHe_r & * + 2F_rd'_r - H'\delta_r = 0, \\ H'e_r & -2F_rd_r * + H\delta_r = 0, \\ -2F_sF_te_r + & H'd_r - Hd'_r * = 0. \end{cases}$$

§ 6.

Da jede binäre quadratische Form ein Produkt von zwei linearen Faktoren ist, so folgt aus (76), daß jede der beiden konjugierten trilinearen Formen

$$(109)\qquad U = \tfrac{1}{2}(H' + H\sqrt{D}), \quad V = \tfrac{1}{2}(H' - H\sqrt{D}),$$

deren Produkt

$$(110)\qquad UV = F_1F_2F_3$$

ist, und welche als spezielle Fälle in der Schar der Formen (88) enthalten sind, ein Produkt von drei linearen Faktoren ist. Wir nehmen im folgenden an, daß H eine allgemeine Form ist, d. h. daß ihre acht Koeffizienten α, β willkürliche Konstanten sind, und bezeichnen mit

$$(111)\qquad \lambda_r = x_r + \omega_r y_r, \quad \mu_r = x_r + \omega'_r y_r$$

lineare Funktionen des Paares z_r, in denen die Variable x_r den Koeffizient 1 hat. Bezeichnet man ferner die Koeffizienten der Formen F_r wie in (1), so kann man zufolge (110) gleichzeitig

$$(112)\qquad U = L\lambda_1\lambda_2\lambda_3, \quad V = M\mu_1\mu_2\mu_3$$

und

$$(113)\qquad F_r = A_r\lambda_r\mu_r$$

setzen, wo L, M Konstanten sind, die der Bedingung

$$(114)\qquad LM = A_1A_2A_3$$

genügen*), und die Konstanten ω_r, ω'_r sind als Wurzeln einer quadratischen Gleichung in ihrem Komplex durch

$$(115)\qquad A_r(\omega_r + \omega'_r) = B_r, \quad A_r\omega_r\omega'_r = C_r$$

bestimmt; es kommt darauf an, sie genau voneinander zu unterscheiden.

*) Bezeichnet man die den Koeffizienten α, β der Form H entsprechenden Koeffizienten von H' mit α', β', so ist offenbar

$$2L = \alpha'_0 + \alpha_0\sqrt{D}, \quad 2M = \alpha'_0 - \alpha_0\sqrt{D}.$$

Läßt man die Form H'' in (88) mit der Form U in (109) zusammenfallen, indem man $2p = \sqrt{D}$, $2q = 1$ setzt, und behält für diese spezielle Form $H'' = U$ die Vektorbezeichnung d_r'' bei, so verschwindet die Konstante m in (94), mithin verschwinden zufolge (95) auch die drei quadratischen Formen F_r'' identisch, was mit den am Schluß von § 4 gemachten Bemerkungen vollständig übereinstimmt. Aus der Definition von d_r'' und aus (112) ergibt sich sodann

$$d_r'' x_r = \frac{\partial U}{\partial y_r} = L\lambda_s\lambda_t\omega_r, \quad d_r'' y_r = -\frac{\partial U}{\partial x_r} = -L\lambda_s\lambda_t,$$

und hieraus folgen die beiden Gleichungen

$$d_r''\lambda_r = 0, \quad d_r''\mu_r = L\lambda_s\lambda_t(\omega_r - \omega_r'),$$

deren erste auch eine unmittelbare Folge der Gleichung $d_r'' H'' = d_r'' U = 0$ ist. Zufolge (113) wird daher

$$d_r'' F_r = A_r\lambda_r d_r''\mu_r = A_r U(\omega_r - \omega_r'),$$

und da andererseits die Gleichung (92) in

$$d_r'' F_r = \tfrac{1}{2}(H'\sqrt{D} + DH) = U\sqrt{D}$$

übergeht, so ergibt die Vergleichung beider Ausdrücke das unterscheidende Resultat

$$A_r(\omega_r - \omega_r') = \sqrt{D}. \tag{116}$$

Verbindet man dasselbe mit (115), so folgt

$$\omega_r = \frac{B_r + \sqrt{D}}{2A_r}, \quad \omega_r' = \frac{B_r - \sqrt{D}}{2A_r}, \tag{117}$$

und hierdurch sind die sechs linearen Funktionen λ_r, μ_r vollständig bestimmt.

Wir kehren nun noch einmal zu den durch die Form H gegebenen Vektoren d_r zurück, um ihnen die Funktionen U, V, λ_r, μ_r zu unterwerfen. Da $d_r H = 0$ und $d_r H' = 2F_s F_t$ ist, so folgt aus den Definitionen (109)

$$d_r U = d_r V = F_s F_t;$$

andererseits ergibt sich aus den Darstellungen (112)

$$d_r U = L\lambda_s\lambda_t d_r\lambda_r, \quad d_r V = M\mu_s\mu_t d_r\mu_r;$$

vergleicht man diese Ausdrücke mit einander und berücksichtigt (113), (114), so folgt

$$A_r d_r\lambda_r = M\mu_s\mu_t, \quad A_r d_r\mu_r = L\lambda_s\lambda_t, \tag{118}$$

und die vorhergehenden Ausdrücke vereinigen sich in

$$d_r U = d_r V = F_s F_t = A_r d_r \lambda_r d_r \mu_r. \tag{119}$$

Bedenkt man nun, daß die homogenen linearen Funktionen λ_r, μ_r, wenn x_r, y_r durch $d_r x_r$, $d_r y_r$ ersetzt werden, in $d_r \lambda_r$, $d_r \mu_r$ übergehen, so läßt sich diese letzte Gleichung zufolge (113) auch in der Form

$$F_r(d_r x_r,\ d_r y_r) = F_s F_t$$

darstellen, die wir früher in (74) erhalten haben, und die, wie schon bemerkt, mit dem Hauptsatze (11) in § 1 übereinstimmt. Die Gleichungen (118) dagegen enthalten eine wichtige Ergänzung zu diesem Transformationssatz, weil sie lehren, in welcher Weise hierbei die beiden Linearfaktoren von F_r sich transformieren, und dies ist von Bedeutung für die Art, in welcher nach Gauß die Formen F_s, F_t in die Transformation eintreten (vgl. den Schluß von § 2).

In ähnlicher Weise folgt aus (105), wenn man den Vektor δ_r auf die Darstellungen (109), (112) wirken läßt,

$$\begin{cases} \delta_r U = -U\sqrt{D}, & \delta_r V = V\sqrt{D}, \\ \delta_r \lambda_r = -\lambda_r \sqrt{D}, & \delta_r \mu_r = \mu_r \sqrt{D}, \end{cases} \tag{120}$$

und hieraus nach (113) wieder die Gleichung (104).

§ 7.

Es ist schon in § 1 bemerkt, daß die Diskriminante D der drei Formen F_1, F_2, F_3 eine homogene Funktion vierten Grades von den acht Konstanten α, β ist, welche nach § 4 zugleich die Koeffizienten der Form H sind. Ich will jetzt zum Schluß noch auf die beherrschende Stellung aufmerksam machen, welche diese Funktion D einnimmt, indem ich nachweise, daß aus ihren partiellen Derivierten auch die Koeffizienten der zu H adjungierten Form H' und die der drei Formen F_1, F_2, F_3 sich bilden lassen.

Nach § 4 sind α_0, β_0, α_r, β_r bzw. die Koeffizienten der Produkte $x_1 x_2 x_3$, $y_1 y_2 y_3$, $x_r y_s y_t$, $y_r x_s x_t$ in H, d. h. es ist

$$\alpha_0 = \frac{\partial^3 H}{\partial x_1 \partial x_2 \partial x_3}, \quad \beta_0 = \frac{\partial^3 H}{\partial y_1 \partial y_2 \partial y_3},$$

$$\alpha_r = \frac{\partial^3 H}{\partial x_r \partial y_s \partial y_t}, \quad \beta_r = \frac{\partial^3 H}{\partial y_r \partial x_s \partial x_t},$$

und wir wollen mit α_0', β_0', α_r', β_r' die entsprechenden Koeffizienten in der adjungierten Form H' bezeichnen. Für die letztere ergibt sich aus ihrer Definition (72) der Ausdruck

$$H' = d_r F_r = \frac{\partial F_r}{\partial x_r}\frac{\partial H}{\partial y_r} - \frac{\partial F_r}{\partial y_r}\frac{\partial H}{\partial x_r}$$
$$= (2A_r x_r + B_r y_r)\frac{\partial H}{\partial y_r} - (B_r x_r + 2C_r y_r)\frac{\partial H}{\partial x_r},$$

mithin wird

$$\frac{\partial H'}{\partial x_r} = 2A_r\frac{\partial H}{\partial y_r} - B_r\frac{\partial H}{\partial x_r}, \quad \frac{\partial H'}{\partial y_r} = B_r\frac{\partial H}{\partial y_r} - 2C_r\frac{\partial H}{\partial x_r},$$

und durch fortgesetzte Derivationen erhält man daher

$$(121) \qquad \begin{cases} \alpha_0' = 2A_r\beta_r - B_r\alpha_0, & \beta_0' = B_r\beta_0 - 2C_r\alpha_r, \\ \alpha_r' = 2A_r\beta_0 - B_r\alpha_r, & \beta_r' = B_r\beta_r - 2C_r\alpha_0. \end{cases}$$

Aus den in (2) angegebenen Ausdrücken für die Koeffizienten A_r, B_r, C_r der Form F_r folgt nun

$$\frac{\partial C_r}{\partial \alpha_0} = \frac{\partial A_r}{\partial \beta_0} = \frac{\partial C_r}{\partial \alpha_r} = \frac{\partial A_r}{\partial \beta_r} = 0,$$
$$\frac{\partial B_r}{\partial \beta_0} = \frac{\partial A_r}{\partial \alpha_r} = -\alpha_0, \quad \frac{\partial B_r}{\partial \alpha_0} = \frac{\partial C_r}{\partial \beta_r} = -\beta_0,$$
$$\frac{\partial A_r}{\partial \alpha_0} = \frac{\partial B_r}{\partial \beta_r} = -\alpha_r, \quad \frac{\partial C_r}{\partial \beta_0} = \frac{\partial B_r}{\partial \alpha_r} = -\beta_r,$$

mithin erhält man mit Rücksicht auf $D = B_r^2 - 4A_rC_r$ für die Koeffizienten von H' die Formeln

$$\alpha_0' = -2A_r\frac{\partial C_r}{\partial \beta_0} + B_r\frac{\partial B_r}{\partial \beta_0} = \frac{1}{2}\frac{\partial D}{\partial \beta_0},$$
$$\beta_0' = -B_r\frac{\partial B_r}{\partial \alpha_0} + 2C_r\frac{\partial A_r}{\partial \alpha_0} = -\frac{1}{2}\frac{\partial D}{\partial \alpha_0},$$
$$\alpha_r' = -2A_r\frac{\partial C_r}{\partial \beta_r} + B_r\frac{\partial B_r}{\partial \beta_r} = \frac{1}{2}\frac{\partial D}{\partial \beta_r},$$
$$\beta_r' = -B_r\frac{\partial B_r}{\partial \alpha_r} + 2C_r\frac{\partial A_r}{\partial \alpha_r} = -\frac{1}{2}\frac{\partial D}{\partial \alpha_r}.$$

Bezeichnet man daher mit (α, β) jedes der vier Paare (α_0, β_0), (α_1, β_1), (α_2, β_2), (α_3, β_3) und mit (α', β') das entsprechende Paar für die Form H', so wird

$$(122) \qquad \alpha' = \frac{1}{2}\frac{\partial D}{\partial \beta}, \quad \beta' = -\frac{1}{2}\frac{\partial D}{\partial \alpha}.$$

Hieraus erhält man für die beiden Paare (α_s', β_s'), (α_t', β_t'), indem man den Ausdruck $D = B_r^2 - 4A_rC_r$ beibehält und die Derivierten von A_r, B_r, C_r gemäß (2) bildet, die Ausdrücke

$$(123)\qquad \begin{cases} \alpha_s' = B_r\alpha_s - 2C_r\beta_t, & \beta_s' = 2A_r\alpha_t - B_r\beta_s, \\ \alpha_t' = B_r\alpha_t - 2C_r\beta_s, & \beta_t' = 2A_r\alpha_s - B_r\beta_t. \end{cases}$$

Bedient man sich der Bezeichnung für die allgemeine Komposition von rechteckigen, nach Zeilen und Spalten geordneten Größensystemen (Matrizen), so kann man die acht Gleichungen (121), (123) in

$$(124)\qquad \begin{pmatrix} B_r, & -2C_r \\ 2A_r, & -B_r \end{pmatrix} \begin{pmatrix} \beta_r, & \alpha_s, & \alpha_t, & \beta_0 \\ \alpha_0, & \beta_t, & \beta_s, & \alpha_r \end{pmatrix} = \begin{pmatrix} \beta_r', & \alpha_s', & \alpha_t', & \beta_0' \\ \alpha_0', & \beta_t', & \beta_s', & \alpha_r' \end{pmatrix}$$

zusammenfassen; permutiert man die Indizes r, s, t, so erhält man für jeden der acht Koeffizienten α', β' drei äußerlich verschiedene Ausdrücke, die alle aus (122) entspringen, wenn man D wie in (3) durch die Koeffizienten der Formen F_1 oder F_2 oder F_3 darstellt.

Hiermit ist gezeigt, daß die Koeffizienten der zu H adjungierten Form H' durch Derivierte erster Ordnung von D dargestellt werden; durch fortgesetzte Derivation erhält man für die Koeffizienten der quadratischen Formen F_1, F_2, F_3 die folgenden Ausdrücke

$$(125)\qquad \begin{cases} 6A_r = \dfrac{\partial^2 D}{\partial\beta_0\partial\beta_r} - \dfrac{\partial^2 D}{\partial\alpha_s\partial\alpha_t}, & 6C_r = \dfrac{\partial^2 D}{\partial\alpha_0\partial\alpha_r} - \dfrac{\partial^2 D}{\partial\beta_s\partial\beta_t}, \\ 6B_r = \dfrac{\partial^2 D}{\partial\alpha_s\partial\beta_s} + \dfrac{\partial^2 D}{\partial\alpha_t\partial\beta_t} - \dfrac{\partial^2 D}{\partial\alpha_r\partial\beta_r} - \dfrac{\partial^2 D}{\partial\alpha_0\partial\beta_0}, \end{cases}$$

deren Analogie mit den Darstellungen (2) von $-C_r$, $-A_r$, $+B_r$ ersichtlich ist; die Ausführung der Rechnung mag aber dem Leser überlassen bleiben.

Das in (122) erhaltene Resultat reizt dazu, in dem von den sieben Paaren (α, β), (x_r, y_r) gebildeten, vierzehnfach ausgedehnten Raume einen Vektor δ einzuführen, welcher durch

$$(126)\qquad \delta\alpha = \alpha', \quad \delta\beta = \beta', \quad \delta x_r = \delta y_r = 0,$$

also durch

$$(127)\qquad \delta\varphi = \frac{1}{2}\sum^{(\alpha,\beta)}\left(\frac{\partial\varphi}{\partial\alpha}\frac{\partial D}{\partial\beta} - \frac{\partial\varphi}{\partial\beta}\frac{\partial D}{\partial\alpha}\right)$$

definiert wird, wo φ eine willkürliche Funktion bedeutet, und die Summe über alle vier Paare (α, β) auszudehnen ist. Da H eine homogene lineare Funktion der Größen α, β ist, so folgt aus (126) unmittelbar

$$(128)\qquad \delta H = H'.$$

Ersetzt man φ in (127) durch $\frac{\partial \varphi}{\partial x_r}$, $\frac{\partial \varphi}{\partial y_r}$, so folgt

$$\delta \frac{\partial \varphi}{\partial x_r} = \frac{\partial \delta \varphi}{\partial x_r}, \quad \delta \frac{\partial \varphi}{\partial y_r} = \frac{\partial \delta \varphi}{\partial y_r}, \tag{129}$$

d. h. der Vektor δ ist permutabel mit den Vektoren $\frac{\partial}{\partial x_r}$, $\frac{\partial}{\partial y_r}$; bedeutet daher ψ_r eine beliebige Funktion, welche frei von den beiden Variabeln x_r, y_r des Paares z_r ist, so hat $\delta \psi_r$ dieselbe Eigenschaft, und wenn ε_r irgend einen der vier in (54), (61), (79), (103) erklärten Vektoren d_r, e_r, d'_r, δ_r bedeutet, die alle nur auf das Paar z_r wirken, so folgt hieraus

$$(\delta, \varepsilon_r)\psi_r = \delta \varepsilon_r \psi_r - \varepsilon_r \delta \psi_r = 0,$$

weil $\varepsilon_r \psi_r = \varepsilon_r \delta \psi_r = 0$ ist. Um also einen solchen Vektor (δ, ε_r) vollständig zu bestimmen, braucht man nur noch die beiden Funktionen $(\delta, \varepsilon_r)x_r$ und $(\delta, \varepsilon_r)y_r$ zu ermitteln.

Beginnt man mit dem Vektor $\varepsilon_r = d_r$ und berücksichtigt (126), (128), (129), so erhält man

$$(\delta, d_r)x_r = \delta d_r x_r = \delta \frac{\partial H}{\partial y_r} = \frac{\partial \delta H}{\partial y_r} = \frac{\partial H'}{\partial y_r} = d'_r x_r,$$

$$(\delta, d_r)y_r = \delta d_r y_r = \delta\left(-\frac{\partial H}{\partial x_r}\right) = -\frac{\partial \delta H}{\partial x_r} = -\frac{\partial H'}{\partial x_r} = d'_r y_r,$$

und da zugleich $(\delta, d_r)\psi_r = 0 = d'_r \psi_r$ ist, so folgt

$$(\delta, d_r) = d'_r. \tag{130}$$

Verfährt man ähnlich mit dem Vektor $\varepsilon_r = e_r$, so ergibt sich, daß δ permutabel mit e_r, also auch mit $(e_s - e_r)$ ist, d. h. es ist

$$(\delta, e_r) = 0, \quad (\delta, e_s - e_r) = 0. \tag{131}$$

Wendet man nun den Satz (43) auf die drei Vektoren δ, d_r, d_s an und bedenkt, daß

$$(d_r, d_s) = F_t(e_s - e_r), \quad (d_s, \delta) = -d'_s, \quad (\delta, d_r) = d'_r$$

ist, so folgt zunächst

$$(\delta, F_t(e_s - e_r)) - (d_r, d'_s) + (d_s, d'_r) = 0;$$

zufolge (101) ist aber $(d_r, d'_s) = (d_s, d'_r)$, und da nach der in (45) angegebenen Regel

$$(\delta, F_t(e_s - e_r)) = F_t(\delta, e_s - e_r) + \delta F_t(e_s - e_r)$$

ist, wo das erste Glied rechts nach (131) verschwindet, so ist $\delta F_t(e_s - e_r) = 0$, und hieraus folgt

(132) $$\delta F_t = 0; \quad \delta A_t = \delta B_t = \delta C_t = 0,$$

also auch

(133) $$\delta D = 0,$$

was übrigens auch unmittelbar aus (127) folgt.

Läßt man jetzt den Vektor (130) auf F_r wirken, so wird

$\delta d_r F_r - d_r \delta F_r = d'_r F_r$, und da $d_r F_r = H'$, $\delta F_r = 0$, $d'_r F_r = DH$ ist, so folgt

(134) $$\delta^2 H = \delta H' = DH,$$

mithin

(135) $$\delta^2 \alpha = \delta \alpha' = D\alpha, \quad \delta^2 \beta = \delta \beta' = D\beta,$$

was sich auch aus (121) mit Rücksicht auf $\delta A_r = \delta B_r = \delta C_r = 0$ leicht ergeben würde.

Verfährt man endlich auf dieselbe Weise mit den Vektoren d'_r, δ_r, so erhält man, wie der Leser sofort finden wird,

(136) $$(\delta, d'_r) = D d_r, \quad (\delta, \delta_r) = 0.$$

Erläuterungen zur vorstehenden Abhandlung.

Dedekind behandelt hier wieder die Komposition der quadratischen Formen, ein Problem, das er schon wiederholt in den Supplementen zu Dirichlets Zahlentheorie studiert hat. Die Bemerkung Dedekinds, daß jede bilineare Form die entsprechenden komponierbaren Formen bestimmt, hat schon Cayley (Journ. f. Math. **39** (1850), S. 14—15) gemacht. Arndt (Arch. f. Math. u. Phys. **15** (1850), S. 429—480) hat sich auch mit ähnlichen Fragen beschäftigt. L. E. Dickson (History of the theory of numbers, Bd. 3, S. 75) bemerkt: „Dedekind war offenbar nicht mit den Resultaten von Arndt und Cayley bekannt, indem er das Problem von neuem angriff und eine einfache und symmetrische Behandlungsweise entwickelte."

Eine übersichtliche Darstellung der Geschichte der Theorie der Komposition der quadratischen Formen findet man in dem eben erwähnten Buch von L. E. Dickson, Bd. 3, Kap. 3. Unter den wichtigsten neueren Arbeiten über die Komposition quadratischer Formen sollen die folgenden erwähnt werden: H. Weber, Gött. Nachr. 1907, S. 86—100. A. Speiser, Festschrift zu H. Weber, 1912, S. 375—395. H. Brandt, Journ. f. Math. **143** (1913), S. 106—127; **150** (1920), S. 1—46. Math. Zeitschr. **17** (1923), S. 153—160; Math. Ann. **91** (1924), S. 300—315.

Ore.

XXXIV.

Über den Zellerschen Beweis des quadratischen Reziprozitätssatzes.

[Festschrift Heinrich Weber zu seinem siebzigsten Geburtstag am 5. März 1912 gewidmet von Freunden und Schülern. Leipzig und Berlin 1912, S. 23—36.]

Das Lemma, auf welches Gauß seinen dritten und fünften Beweis des Reziprozitätssatzes gegründet hat, ist später der Ausgangspunkt für viele andere Beweise desselben Satzes geworden[1]). Unter allen diesen Beweisen scheint mir der einfachste der zu sein, welchen Chr. Zeller[2]) mir in einem Briefe vom 8. Juli 1872 mitgeteilt hat; dieser Brief schließt mit den durchaus zutreffenden Worten: „Man braucht also jene Hilfsgrößen nicht, welche bisher bei dem Beweise unseres Satzes verwendet worden sind und denselben umständlich gemacht haben.“ In der Tat vermeidet Zeller gänzlich die in dem dritten Beweise von Gauß eingeführten größten Ganzen $[x]$ und gelangt zum Ziele, indem er zwei neue Betrachtungen mit dem Lemma von Gauß verbindet. Einige Monate später hat Zeller (in dem Sitzungsberichte der Berliner Akademie vom 16. Dezember 1872) einen sehr ähnlichen Beweis veröffentlichen lassen, in welchem an Stelle der zweiten Betrachtung eine dritte tritt, wodurch aber die Einfachheit nach meiner Ansicht ein wenig gelitten hat. Mag nun diese Abänderung noch so geringfügig scheinen, so glaube ich doch Zellers Verdienst in ein helleres Licht zu rücken, wenn ich den wesentlichen Inhalt des genannten Briefes in freier Umarbeitung und geänderter Bezeichnung jetzt bekannt mache.

Hierzu ist es freilich nötig, die bekannten Tatsachen, auf denen das Lemma von Gauß beruht, kurz in Erinnerung zu bringen, und

---

[1]) Eine sehr eingehende Darstellung dieser Beweise findet man bei P. Bachmann (Niedere Zahlentheorie, erster Teil, 1902, Seite 212—286).

[2]) Damals Pfarrer und Bezirks-Schulinspektor zu Weiler bei Schorndorf (Württemberg), später Seminarrektor in Markgröningen, wo er im Jahre 1899 als Oberschulrat verstorben ist.

zwar in der Form, daß unter dem Reste einer ganzen Zahl in bezug auf einen ungeraden Modulus $p > 1$ immer ihr absolut kleinster, also zwischen den Grenzen $\pm\frac{p}{2}$ gelegener Rest verstanden werden soll. Läßt man nun, wenn q relative Primzahl zu p ist, den Faktor h alle ganzen Zahlen

$$1, 2, \cdots, \frac{p-1}{2}$$

des Intervalles $0 < h < \frac{p}{2}$ durchlaufen, und bildet man die Reste a und die Quotienten y für die Produkte

$$hq = a + yp \equiv a \pmod{p}, \tag{1}$$

so sind diese Reste a alle von Null und auch voneinander verschieden, weil zwei verschiedene Faktoren h immer zwei inkongruente Produkte hq erzeugen; da ferner auch die Summe von zwei Produkten hq niemals durch p teilbar ist, so sind sogar die absoluten Werte aller Reste a verschieden und stimmen folglich in ihrem Komplex mit den Faktoren h völlig überein; jeder Faktor h ist auch der absolute Wert von einem und nur einem Reste a. Bedeutet daher P das Produkt aller Faktoren h, und m die Anzahl derjenigen Reste a, welche negativ sind, so ist $P(-1)^m$ das Produkt aller Reste a, und durch Multiplikation aller Kongruenzen (1) ergibt sich

$$Pq^{\frac{p-1}{2}} \equiv P(-1)^m \pmod{p}.$$

Wird jetzt angenommen, daß die ungerade Zahl p eine Primzahl ist, so ist das Produkt P nicht teilbar durch p, mithin

$$q^{\frac{p-1}{2}} \equiv (-1)^m \pmod{p}.$$

Das nach Euler benannte Kriterium besteht bekanntlich darin, daß die Potenz linker Hand $\equiv +1$ oder $\equiv -1 \pmod{p}$ ist, je nachdem q quadratischer Rest oder Nichtrest von p ist, und wenn man diese positive oder negative Einheit nach Legendre durch das Symbol $\left(\frac{q}{p}\right)$ bezeichnet, so kann das Resultat der vorhergehenden Betrachtung durch die Gleichung

$$\left(\frac{q}{p}\right) = (-1)^m$$

ausgedrückt werden[1]). Hierin besteht das obenerwähnte Lemma von Gauß.

Ist q ebenfalls eine ungerade positive Primzahl, so wird der zu beweisende Reziprozitätssatz bekanntlich durch die Gleichung

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}$$

ausgedrückt, welche jetzt mit Hilfe des Lemma von Gauß eine einfachere Gestalt annimmt. Durchläuft nämlich der Faktor k alle ganzen Zahlen

$$1, 2, \cdots, \frac{q-1}{2}$$

des Intervalls $0 < k < \frac{q}{2}$, und bildet man wie in (1) die Reste b und die Quotienten x für die Produkte

$$kp = b + xq \equiv b \pmod{q}, \tag{2}$$

so sind die absoluten Werte der Reste b wieder alle verschieden, und ebenso wird

$$\left(\frac{p}{q}\right) = (-1)^n,$$

wo n die Anzahl derjenigen Reste b bedeutet, die negativ sind; hierdurch verwandelt sich der zu beweisende Satz offenbar in die Kongruenz

$$m + n \equiv \frac{p-1}{2}\,\frac{q-1}{2} \pmod{2}, \tag{3}$$

welche auch so ausgesprochen werden kann: Die Summe $m + n$ ist stets und nur dann ungerade, wenn $p \equiv q \equiv -1 \pmod{4}$ ist.

Nachdem diese Umformung des Reziprozitätssatzes, welche die Grundlage für den dritten und fünften Beweis von Gauß bildet, in Erinnerung gebracht ist, will ich jetzt die beiden Hauptpunkte hervorheben, auf denen Zellers Beweis beruht. Hierbei setze ich lediglich voraus, es seien p, q relative[2]) Primzahlen, beide ungerade, positiv

---

[1]) E. Schering hat bemerkt, daß dieselbe auch für das von Jacobi verallgemeinerte Symbol von Legendre gilt (Monatsbericht der Berliner Akademie vom 22. Juni 1876).

[2]) Der folgende Beweis gilt daher zufolge der vorhergehenden Anmerkung auch für den verallgemeinerten Reziprozitätssatz.

und > 1; auch soll (wie in der Berliner Darstellung) p die kleinere dieser beiden Zahlen bedeuten.

Die erste Bemerkung Zellers geht aus einer Vergleichung der beiden Reihen (1) und (2) hervor und besteht darin, daß alle Gleichungen (1) aus ebenso vielen Gleichungen (2) nur durch Umsetzung ihrer Glieder entspringen. Ist z. B. $p = 11$, $q = 27$, so erhält man die Reihe (2) und daraus die Reihe (1) in der folgenden Tabelle:

$1 \cdot p = +11 + 0 \cdot q$	
$2 \cdot p = -5 + 1 \cdot q$	$1 \cdot q = +5 + 2 \cdot p$
$3 \cdot p = +6 + 1 \cdot q$	
$4 \cdot p = -10 + 2 \cdot q$	
$5 \cdot p = +1 + 2 \cdot q$	$2 \cdot q = -1 + 5 \cdot p$
$6 \cdot p = +12 + 2 \cdot q$	
$7 \cdot p = -4 + 3 \cdot q$	$3 \cdot q = +4 + 7 \cdot p$
$8 \cdot p = +7 + 3 \cdot q$	
$9 \cdot p = -9 + 4 \cdot q$	
$10 \cdot p = +2 + 4 \cdot q$	$4 \cdot q = -2 + 10 \cdot p$
$11 \cdot p = +13 + 4 \cdot q$	
$12 \cdot p = -3 + 5 \cdot q$	$5 \cdot q = +3 + 12 \cdot p$
$13 \cdot p = +8 + 5 \cdot q$	

Um diese Beziehung zwischen den beiden Reihen allgemein zu beweisen, setze man jede Gleichung (1) in die Form

$$yp = -a + hq;$$

aus der Definition der Zahlen a, h und aus unserer Annahme $p < q$ folgt

$$-\frac{p}{2} < -a < +\frac{p}{2}, \quad p < hq < \frac{p}{2}q,$$

hieraus durch Addition und Division durch p

$$+\frac{1}{2} < y < \frac{q+1}{2},$$

mithin auch $0 < y < \frac{q}{2}$. Also ist jeder in der Reihe (1) auftretende Quotient y auch einer der Faktoren k in der Reihe (2), und da jede Zahl $-a$ zwischen den Grenzen $\pm\frac{p}{2}$, also gewiß auch zwischen $\pm\frac{q}{2}$ liegt, so ist $-a$ der diesem Faktor $k = y$ entsprechende Rest b des Produktes kp in (2), und der Quotient $x = h$, w. z. b. w.

Mit diesen Resten $b = -a$, deren Anzahl $= \frac{p-1}{2}$ ist, sind aber alle zwischen den Grenzen $\pm\frac{p}{2}$ liegenden Reste b in (2) erschöpft, weil, wie oben bemerkt, die absoluten Werte aller Reste b voneinander verschieden sind. Die Anzahl m der negativen Reste a in (1) ist daher zugleich die Anzahl derjenigen positiven Reste b in (2), welche $< \frac{p}{2}$ sind; fügt man zu diesen m positiven Resten b noch alle n negativen Reste b hinzu, so ist die Summe $m + n$ die Anzahl aller Reste b in (2), welche in dem Intervalle

$$(4) \qquad -\frac{q}{2} < b < +\frac{p}{2}$$

liegen.

In dem obigen Beispiel $p = 11$, $q = 27$, wo $m = 2$, $n = 5$, liegen im Intervalle (4) die sieben Reste $b = -10, -9, -5, -4, -3, +1, +2$; die übrigen sechs Reste sind $b = 6, 7, 8, 11, 12, 13$.

Nachdem hiermit die Bedeutung der Summe $m + n$ für die Reihe (2) festgestellt ist, beantwortet Zeller die Hauptfrage nach ihrer Parität, ob sie gerade oder ungerade ist, durch eine zweite Betrachtung, deren einfacher Grundgedanke in Folgendem besteht. Wenn es in einem endlichen System von Elementen b ein Gesetz gibt, das jedem b ein bestimmtes Element b' desselben Systems zuordnet, und zwar so symmetrisch, daß umgekehrt $(b')' = b$ wird, so hat die Anzahl aller b offenbar dieselbe Parität wie die Anzahl der Fälle, in denen $b' = b$ ist. Für unsere Untersuchung, wo es sich um die Reste b in der Reihe (2) handelt, gewinnt Zeller eine solche Verteilung in symmetrische Paare b, b' auf folgende Weise.

Durchläuft der Faktor k alle seine Werte, und setzt man

$$(5) \qquad k + k' = \frac{q+1}{2},$$

so durchläuft k' offenbar dieselben Werte in umgekehrter Folge, und jedem solchen Faktorenpaar k, k' entspricht ein Restepaar

$$b \equiv kp, \quad b' \equiv k'p \pmod{q}.$$

Da jeder Rest b durch einen und nur einen Faktor k erzeugt wird, so ist durch b vermöge (5) auch der Faktor k', mithin auch der zugehörige Rest b' vollständig bestimmt, und aus der Symmetrie der Gleichung (5) in bezug auf k, k' folgt, daß umgekehrt $(b')' = b$ ist.

Durch Addition der beiden vorstehenden Kongruenzen mit Rücksicht auf (5) folgt die Kongruenz

$$b + b' \equiv \frac{q+1}{2} p \pmod{q},$$

welche die gegenseitige Abhängigkeit der beiden, ein symmetrisches Paar bildenden Reste b, b' vollständig ausdrückt. Dies läßt sich aber noch genauer verfolgen. Zufolge der Definition der Reste b, b' liegt einerseits ihre Summe $b + b'$ gewiß zwischen den Grenzen $\pm q$; andererseits ist das ihr kongruente Produkt

$$\frac{q+1}{2} p = \frac{p-q}{2} + \frac{p+1}{2} q = \frac{p+q}{2} + \frac{p-1}{2} q, \tag{6}$$

mithin

$$b + b' \equiv \frac{p-q}{2} \equiv \frac{p+q}{2} \pmod{q},$$

und da zufolge unserer Annahme $p < q$ die beiden Zahlen $\frac{p \mp q}{2}$ ebenfalls zwischen den Grenzen $\pm q$ liegen, so ist

$$\text{entweder } b + b' = \frac{p-q}{2}$$

$$\text{oder } b + b' = \frac{p+q}{2}.$$

Im ersten Fall sind beide Reste b, b' algebraisch $< \frac{p}{2}$; wäre nämlich einer derselben, z. B. $b' > \frac{p}{2}$, so wäre der andere $b < -\frac{q}{2}$, was der Definition von b widerspricht. Im zweiten Fall sind beide Reste $> \frac{p}{2}$; wäre nämlich z. B. $b' < \frac{p}{2}$, so wäre $b > \frac{q}{2}$, was abermals unmöglich ist. Mithin sondern sich die beiden Fälle in folgender Weise scharf voneinander:

$$\text{I.} \quad b + b' = \frac{p-q}{2}, \; -\frac{q}{2} < b, \; b' < +\frac{p}{2}, \tag{7}$$

$$\text{II.} \quad b + b' = \frac{p+q}{2}, \; +\frac{p}{2} < b, \; b' < +\frac{q}{2}, \tag{8}$$

und zugleich leuchtet ein, daß b' in jedem dieser beiden Intervalle dieselben Werte wie b, aber in umgekehrter Größenfolge durchläuft.

Wir betrachten jetzt nur noch das erste Intervall (7), welches identisch mit dem obigen in (4) ist und folglich genau $m + n$ Reste b enthält. Diese Summe $m + n$ wird daher immer gerade sein, wenn jedes symmetrische Restpaar in (7) aus zwei ungleichen Resten b, b' besteht. Da ferner der Fall $b = b'$ immer und nur dann eintrifft, wenn zugleich $k = k'$ ist, so geschieht dies in (7) gewiß und nur in dem einzigen Fall, wenn gleichzeitig

$$b = b' = \frac{p-q}{4},\ k = k' = \frac{q+1}{4},$$

also

$$p \equiv q \equiv -1 \pmod 4 \tag{9}$$

ist, und da alle anderen, etwa in (7) enthaltenen Restpaare aus zwei ungleichen Resten b, b' bestehen, so ist die Summe $m + n$ in diesem und nur in diesem Falle (9) ungerade.

Hiermit ist die Kongruenz (3), also auch der Reziprozitätssatz wirklich bewiesen.

Zur Erläuterung bemerke ich noch folgendes. Ist $q \equiv 1 \pmod 4$, so folgt aus (5), daß der Fall $k = k'$ niemals eintreten kann; es wird daher jedes Restpaar sowohl in (7) wie in (8) aus zwei ungleichen Resten b, b' bestehen, und folglich ist sowohl die Anzahl $m + n$ der Reste b in (7), wie die Anzahl $\frac{q-1}{2} - m - n$ der Reste b in (8) gerade. Ist dagegen $q \equiv -1 \pmod 4$, so tritt der Fall $k = k'$, also auch $b = b'$, gewiß einmal ein, nämlich in (7) oder (8), je nachdem $p \equiv -1$ oder $\equiv +1 \pmod 4$ ist.

In dem obigen Beispiel $p = 11$, $q = 27$, wo $m = 2$, $n = 5$, ordnen sich die sieben Reste des Intervalles (7) in die vier Paare

$$(b, b') = (-10, +2), (-9, +1), (-5, -3), (-4, -4)$$

mit der Summe $b + b' = -8$, und die sechs Reste des Intervalles (8) zerfallen in die drei Paare

$$(b, b') = (6, 13), (7, 12), (8, 11)$$

mit der Summe $b + b' = +19$. Da dieses Beispiel den Bedingungen (9) genügt, so entspricht dem Faktor $k = k' = 7$ das im Intervall (7) liegende, aus zwei gleichen Resten bestehende Paar $b = b' = -4$.

Im vorstehenden habe ich Zellers scharfsinnigen Beweis (auf Grund des Briefes vom 8. Juli 1872) etwas ausführlicher dargestellt, weil er mit geringstem Aufwande von Rechnung eine sehr deutliche

Einsicht in den Bau und den Zusammenhang der beiden Reihen (1), (2) gibt und deshalb besonders geeignet zum Vortrage vor Anfängern erscheint. Um ihn mit der sehr kurz gefaßten Berliner Darstellung (vom 16. Dezember 1872) bequem zu vergleichen, ändere ich die in der letzteren gewählte Bezeichnung so ab, daß sie mit unserer obigen übereinstimmt, und außerdem will ich zur Abkürzung die Anzahl der Reste b innerhalb des Intervalles

$$(10) \qquad -\frac{q}{2} < b < -\frac{p}{2}$$

mit t bezeichnen. Durch eine Betrachtung, die nahezu mit dem ersten Teile des obigen Beweises übereinstimmt, ergibt sich zunächst die Zerlegung

$$(11) \qquad m + n = \frac{p-1}{2} + t,$$

und handelt sich es daher jetzt noch um die Frage, wann die Anzahl t gerade oder ungerade ist. Dazu dient wieder eine Verteilung der Reste b in symmetrische Paare, die aber von der obigen, durch (5) bestimmten wesentlich abweicht und deshalb hier näher behandelt werden soll. Schließt man in (2) den größten Faktor $k = \frac{q-1}{2}$ aus, dem zufolge (6) nach Subtraktion von p der positive Rest $b = \frac{q-p}{2}$ entspricht, und setzt man

$$(12) \qquad k + k'' = \frac{q-1}{2},$$

so durchläuft k'' dieselben $\frac{q-3}{2}$ Faktoren wie k, und jedes Paar von Resten $b \equiv kp$, $b'' \equiv k''p \pmod{q}$ liefert eine zwischen den Grenzen $\pm q$ liegende Summe

$$b + b'' \equiv \frac{q-1}{2}\, p \equiv -\frac{p+q}{2} \equiv \frac{q-p}{2} \pmod{q}.$$

Verfährt man ähnlich wie oben, so erhält man wieder zwei scharf getrennte Intervalle

$$\text{III.} \quad b + b'' = -\frac{p+q}{2};\ -\frac{q}{2} < b,\ b'' < -\frac{p}{2}$$

$$\text{IV.} \quad b + b'' = +\frac{q-p}{2};\ -\frac{p}{2} < b,\ b'' < +\frac{q}{2},$$

in denen b'' immer dieselben Werte wie b durchläuft. Da das Intervall III mit dem in (10) identisch ist und folglich t Reste b enthält (weil der einzige ausgeschlossene Rest $b = \frac{q-p}{2}$ außerhalb dieses Intervalles liegt), so ergibt sich durch deren Verteilung in symmetrische Paare b, b'', daß diese Anzahl t stets und nur dann ungerade ist, wenn der Fall

$$k = k'' = \frac{q-1}{4},\ b = b'' = -\frac{p+q}{4}$$

eintritt, was immer und nur dann geschieht, wenn $q \equiv 1$, $p \equiv -1$ (mod. 4) ist. Durch Kombination dieses Resultates mit der obigen Zerlegung (11) gelangt schließlich die Berliner Darstellung, indem sie die einzelnen Fälle der Reste von p, q (mod. 4) durchgeht, ebenfalls zu dem Endergebnis, daß die Summe $m + n$ dann und nur dann ungerade ist, wenn $p \equiv q \equiv -1$ (mod. 4) ist, w. z. b. w.

Aus mehreren Gründen verdient wohl der frühere Beweis den Vorzug vor diesem zweiten. Da der Charakter der Summe $m + n$ (mod. 2) das einzige Ziel der Untersuchung bildet, so erscheint ihre Zerlegung (11) in zwei Bestandteile von vornherein als ein Umweg, der sich am Schluß nochmals fühlbar macht; außerdem ist die hier benutzte, durch (12) bestimmte Verteilung der Reste b in symmetrische Paare weniger einfach als die frühere, schon weil sie den Ausschluß eines Faktors k und des entsprechenden Restes b erfordert.

Als Zeller mir seinen Beweis mitteilte, kannte er den dritten Beweis von Gauß nur in der schon vereinfachten Darstellung, wie sie sich in §§ 43, 44 der Vorlesungen über Zahlentheorie von Dirichlet (zweite Auflage 1871) findet. In meiner Antwort (vom 13. Juli 1872) drückte ich ihm meine Freude über seinen Beweis aus, der so geradenwegs auf das Ziel zusteuert, und fügte eine kurze Darstellung des fünften Beweises von Gauß hinzu, der ihm augenscheinlich noch unbekannt war. Dies hat Zeller veranlaßt, mir noch einmal zu schreiben (am 7. Oktober 1872); auch in diesem Briefe findet sich noch keine Spur von der eben besprochenen zweiten Symmetrie der Reihe (2), die den Nerv des Beweises in der Berliner Darstellung bildet; er enthält aber noch zwölf Formeln, die von gewissen Summen der Reste a, b und der Quotienten x, y in den Reihen (1), (2) handeln und damals, wie ich glaube, noch unbekannt waren. Diese

Formeln, deren Beweise Zeller zum Teil andeutet, sind eigentlich nur Kombinationen von sechs verschiedenen Relationen, die ich jetzt im Anschluß an den ersten Beweis von Zeller noch ableiten will. Hierbei bezeichne ich die Reste a, b bzw. mit a_1, b_1 oder mit a_2, b_2, je nachdem sie negativ oder positiv sind, und die Summen der Zahlen

$$h,\ a,\ a_1,\ a_2,\ y;\ k,\ b,\ b_1,\ b_2,\ x$$

bzw. mit

$$H,\ A,\ A_1,\ A_2,\ Y;\ K,\ B,\ B_1,\ B_2,\ X.$$

Da die absoluten Werte $-a_1$, a_2 aller Reste a mit den Faktoren h, ebenso die absoluten Werte $-b_1$, b_2 aller Reste b mit den Faktoren k übereinstimmen, so erhält man zunächst

$$(13) \qquad -A_1 + A_2 = H = \frac{1}{2}\,\frac{p+1}{2}\,\frac{p-1}{2},$$

$$(14) \qquad -B_1 + B_2 = K = \frac{1}{2}\,\frac{q+1}{2}\,\frac{q-1}{2}.$$

Zwei neue Gleichungen folgen aus der Betrachtung der beiden Intervalle (7), (8). Während die $m+n$ Reste b in (7) aus den n negativen Resten b_1 und den m positiven Zahlen $-a_1$ bestehen, so verbleiben nach Entfernung der letzteren aus den Resten b_2 die $\frac{q-1}{2} - m - n$ Reste b in (8), und da b' in jedem der beiden Intervalle dieselben Werte wie b durchläuft, so folgt durch Summation

$$(15) \qquad 2\,(B_1 - A_1) = \frac{p-q}{2}\,(m+n),$$

$$(16) \qquad 2\,(B_2 + A_1) = \frac{p+q}{2}\left(\frac{q-1}{2} - m - n\right).$$

Durch Auflösung dieser vier Gleichungen ergibt sich

$$(17) \qquad -4\,A_1 = p\,(m+n) - \frac{p-1}{2}\,\frac{q-1}{2},$$

$$(18) \qquad -4\,B_1 = q\,(m+n) - \frac{p-1}{2}\,\frac{q-1}{2},$$

$$(19) \qquad +4\,A_2 = \frac{2p+q+1}{2}\,\frac{p-1}{2} - p\,(m+n),$$

$$(20) \qquad +4\,B_2 = \frac{2q+p+1}{2}\,\frac{q-1}{2} - q\,(m+n).$$

woraus auch noch

$$2A = 2(A_1 + A_2) = \frac{p+q}{2}\,\frac{p-1}{2} - p(m+n), \tag{21}$$

$$2B = 2(B_1 + B_2) = \frac{p+q}{2}\,\frac{q-1}{2} - q(m+n) \tag{22}$$

folgt.

Es leuchtet ein, daß aus jeder dieser Formeln auch die Kongruenz (3), also der Reziprozitätssatz folgt; außerdem will ich bemerken, daß diese Kongruenz durch die schärfere

$$m + n \equiv -\frac{p-1}{2}\,\frac{q-1}{2} \pmod 4 \tag{23}$$

ersetzt werden kann, die man leicht erhält, wenn man z. B. die Gleichung (17) mit p multipliziert und bedenkt, daß $p^2 \equiv 1$, also $p(p-1) \equiv -(p-1) \pmod 8$ ist.

Besonders hervorzuheben ist aber, daß alle diese Formeln, obwohl sie auf der ausdrücklichen Annahme $p < q$ beruhen, augenscheinlich auch für die entgegengesetzte Annahme $p > q$ gelten, weil die Ausdrücke für B_1, B_2 und B aus denen für A_1, A_2 und A durch gleichzeitige Vertauschung von p mit q (und von m mit n) hervorgehen.

Um endlich die Summen X, Y der Quotienten x, y ebenfalls durch p, q, m, n auszudrücken, kann man verschiedene Wege einschlagen. Da die Ausdrücke für H, A, K, B schon bekannt sind, so liegt es nahe, hierzu die beiden Gleichungen

$$Hq = A + Yp, \quad Kp = B + Xq \tag{24}$$

zu benutzen, die aus (1), (2) durch Summation entstehen, und zufolge der eben hervorgehobenen Bemerkung genügt es, nur eine der beiden Summen, z. B. X zu berechnen, weil hieraus die andere Y durch Vertauschung von p mit q hervorgehen muß. Aus (14) und (22) folgt nun

$$\begin{aligned} 2(Kp - B) &= \frac{q+1}{2}\,p\,\frac{q-1}{2} - \frac{p+q}{2}\,\frac{q-1}{2} + q(m+n) \\ &= \left(\frac{p-1}{2}\,\frac{q-1}{2} + m + n\right) q, \end{aligned}$$

und da die in der Klammer rechts enthaltene Summe bei Vertauschung von p mit q ungeändert bleibt, so folgt aus (24) die Doppelgleichung

$$2X = 2Y = \frac{p-1}{2}\,\frac{q-1}{2} + m + n, \tag{25}$$

worin abermals der Reziprozitätssatz enthalten ist. Zugleich ergibt sich aus der Kongruenz (23), daß die Summe $X = Y$ stets gerade ist.

Ein anderer Weg, die Summe X zu bestimmen, ergibt sich aus der durch (5) bestimmten Verteilung der Reste b in symmetrische Paare. Bezeichnet man mit x, x' die den Faktoren k, k' entsprechenden Quotienten, so ist

$$kp = b + xq, \quad k'p = b' + x'q,$$

also

$$(b + b') + (x + x')q = \frac{q+1}{2}\, p,$$

und aus (6), (7), (8) folgt

$$x + x' = \frac{p+1}{2} \text{ im Intervalle (7)},$$

$$x + x' = \frac{p-1}{2} \text{ im Intervalle (8)}.$$

Da nun x' sowohl in (7) wie in (8) dieselben Werte wie x durchläuft, deren Anzahl bzw. $m + n$ und $\frac{q-1}{2} - m - n$ ist, so erhält man im ganzen

$$2X = \frac{p+1}{2}(m+n) + \frac{p-1}{2}\left(\frac{q-1}{2} - m - n\right),$$

was mit (25) übereinstimmt.

Hiermit ist das Wesentliche der Formeln erschöpft, die Zeller mir in seinem zweiten Briefe (vom 7. Oktober 1872) mitgeteilt hat, wo er auch beiläufig bemerkt, daß die Größen X, $X - n$, $X - m$ bzw. mit den auf ganz andere Weise definierten Anzahlen α, β, γ im fünften Beweise von Gauß übereinstimmen (wo die Zeichen m, M, n, N durch die ihnen hier entsprechenden p, q, m, n zu ersetzen sind); doch wird der Zusammenhang zwischen den beiden verschiedenen Definitionen nicht untersucht.

Die Gleichheit der beiden Quotientensummen X, Y ist hier auf einem Wege erkannt, der alle früheren Resultate voraussetzt. Diese Gleichheit besteht, wie ich noch bemerken will, selbst dann, wenn die beiden ungeraden Zahlen p, q irgendeinen gemeinsamen Teiler haben; der kürzeste Weg, sie zu beweisen, scheint der folgende zu sein, wobei es auch gleichgültig bleibt, welche der Zahlen p, q die

kleinere ist. Läßt man die Faktoren h, k alle ihre Werte durchlaufen, so kann die Anzahl α der Fälle, in denen die Produktsumme

$$hq + kp > \frac{pq}{2}$$

wird, auf zwei verschiedene Arten bestimmt werden. Wählt man zuerst einen bestimmten Faktor k und setzt $kp = b + xq$ wie in (2), so findet man leicht, daß dieser Quotient x zugleich die Anzahl aller derjenigen Faktoren h ist, welche für diesen Wert k der vorstehenden Forderung genügen, und hieraus folgt offenbar $\alpha = X$. Wählt man aber zuerst einen bestimmten Faktor h und setzt $hq = a + yp$ wie in (1), so erhält man auf dieselbe Weise die Antwort $\alpha = Y$; mithin ist $X = Y$, w. z. b. w.

Aus dem Nachlaß.

Die folgenden aus dem Nachlaß publizierten Stücke haben zum großen Teil neben dem historischen Interesse auch solches durch Auffassung und Methode, wenn auch die Resultate unterdes unabhängig wiedergefunden sind. Es handelt sich um fertige oder fast fertige Ausarbeitungen; auf die Publikation von Unausgearbeitetem konnte um so eher verzichtet werden, als Dedekind in den folgenden Briefen an Frobenius davon ein viel klareres Bild gegeben hat, als es der Nachlaß bot.

Der Nachlaß bestand aus etwa 50 Mappen, Dedekind hatte alles und jedes aufgehoben; es ist also nicht ausgeschlossen, daß sich gelegentlich noch etwas zur Publikation Geeignetes findet. Als historisch interessant ist vielleicht noch zu erwähnen eine wohl unmittelbar an die ersten Vorlesungen anschließende Darstellung der Galoisschen Theorie; oder auch eine sehr ausführliche, aus früher Zeit stammende Darstellung der Riemannschen Geometrie, aus der in die Riemann-Ausgabe (Lateinische Preisarbeit) nur kurze Auszüge durch Weber übernommen wurden. **Noether.**

XXXV.

Allgemeine Sätze über Räume.

§ 1.

Ein System von Punkten $p, p' \cdots$ bildet einen Körper, wenn für jeden Punkt p desselben sich eine Länge δ von der Beschaffenheit angeben läßt, daß alle Punkte, deren Abstand von p kleiner als δ ist, ebenfalls dem System P angehören. Die Punkte $p, p' \cdots$ liegen innerhalb P.

§ 2.

Ist P' ein Körper, dessen sämtliche Punkte auch Punkte des Körpers P sind, so heißt P' ein Teil von P.

§ 3.

Satz. Alle Punkte, deren Abstand von einem festen Punkte p kleiner als eine gegebene Länge δ ist, bilden einen Körper (der Kugel heißt; p heißt der Mittelpunkt, δ der Durchmesser desselben).

Beweis. Ist $pp' < \delta$, so wähle man $\delta' < \delta - pp'$; so sind alle Punkte p'', für welche $p'p'' < \delta'$ ist, auch solche Punkte p'', für welche $pp'' < \delta$ ist (weil $pp'' \leqq pp' + p'p''$).

§ 4.

Ist P ein Körper und m ein Punkt, um welchen sich eine Kugel beschreiben läßt, deren sämtliche Punkte nicht innerhalb P liegen, so sagt man, der Punkt m liege außerhalb P.

§ 5.

Satz. Ist P ein Körper, und existiert wenigstens ein Punkt m außerhalb P, so gibt es auch unendlich viele solche Punkte außerhalb P, und dieselben bilden einen Körper.

Beweis. Da m außerhalb P liegt, so gibt es eine um m beschriebene Kugel K, deren sämtliche Punkte m' nicht innerhalb P liegen. Alle diese Punkte m' liegen außerhalb P; denn ist δ der Halbmesser von K, und also $mm' < \delta$, so beschreibe man um m' mit einem Halbmesser $\delta' < \delta - mm'$ eine Kugel K', so bildet K' einen Teil von K; also liegt m' (nach § 4) außerhalb P. Daß das System M aller außerhalb P liegenden Punkte m einen Körper bildet, folgt auf dieselbe Weise.

§ 6.

Ist P ein Körper und π ein Punkt, welcher weder innerhalb P noch außerhalb P liegt, so heißt π ein Grenzpunkt von P.

§ 7.

Ist P ein Körper und Π das System aller Grenzpunkte π von P (wenn überhaupt solche vorhanden), so heißt Π die Begrenzung von P.

§ 8.

Satz. Liegen sämtliche Punkte eines Körpers P' nicht innerhalb eines Körpers P, so liegen sie auch sämtlich außerhalb P.

Beweis. Es sei m' ein beliebiger Punkt von P'; so läßt sich um m' eine Kugel beschreiben, deren sämtliche Punkte innerhalb P', also nicht innerhalb P liegen. Nach § 4 liegt m' außerhalb P.

§ 9.

Satz. Ein System Π' von Punkten π, welche sämtlich Grenzpunkte eines Körpers P sind, kann keinen Körper bilden.

Beweis. Die Punkte π von Π' liegen (nach § 6) sämtlich nicht innerhalb von P. Wäre Π' ein Körper, so lägen alle Punkte π von Π' (nach § 8) außerhalb P. Weil aber die Punkte π von Π' sämtlich Grenzpunkte von P sind, ist dies (nach § 6) unmöglich.

Erläuterungen zur vorstehenden Abhandlung.

Diese ersten Begriffe der Punktmengenlehre — eine Weiterführung findet sich in dem nächsten Stück — werden des historischen Interesses halber wiedergegeben. Dedekind sagt darüber in einem Brief an Cantor (vom 19. Januar 1879, über Invarianz der Dimension):

„Bei einer Publikation würde ich es für wünschenswert halten, wenn die Namen oder Kunstausdrücke der Mannigfaltigkeitslehre (beiläufig gesagt, ich würde dem ebenfalls Riemannschen Wort „Gebiet“ seiner Kürze halber entschieden den Vorzug vor dem schwerfälligen Worte „Mannigfaltigkeit“ geben) recht genau definiert würden; es wäre sehr verdienstlich, wenn diese ganze „Gebietslehre“ ab ovo dargestellt würde, ohne die geometrische Anschauung zuzuziehen; und dabei müßte z. B. der Begriff einer von dem Punkte a nach dem Punkte b innerhalb des Gebietes G stetig führenden Linie recht bestimmt und deutlich definiert werden. Die Definitionen von Netto*) (dessen Abhandlung mir sehr wohl gefällt, und dessen Beweis, wie ich glaube, mit einigen Modifikationen ganz zutreffend wird) enthalten einen guten Keim, aber sie scheinen mir der Vereinfachung und zugleich einer Vervollständigung fähig. Ich würde mir ein solches Urteil nicht erlauben, wenn ich nicht vor vielen Jahren, als ich noch die Dirichletsche Potentialvorlesung herausgeben und dabei das sogenannte Dirichletsche Prinzip strenger begründen wollte, mich schon recht viel mit solchen Fragen beschäftigt hätte. Ich habe einige solche Definitionen, die mir eine recht gute Grundlage zu geben scheinen; aber ich habe später die ganze Sache liegen lassen, und könnte für den Augenblick nur Unvollständiges geben, da ich durch die Umarbeitung der Dirichletschen Zahlentheorie ganz in Anspruch genommen bin.“

Noether.

*) Crelle 1878.

XXXVI.

Beweis und Anwendungen eines allgemeinen Satzes über mehrfach ausgedehnte stetige Gebiete.

In meiner Schrift „Stetigkeit und irrationale Zahlen" (§ 5, IV), welche im Jahre 1872 erschienen und kürzlich unverändert wieder abgedruckt ist, habe ich den Beweis desjenigen Prinzips veröffentlicht, welches ich schon seit dem Herbst 1858 als eine sichere und zugleich einfache Grundlage für die Infinitesimal-Analysis und für die Untersuchung aller stetigen Gebiete erkannt und auf die wichtigsten dahingehörigen Fragen immer mit dem gewünschten Erfolg angewandt hatte. Das Prinzip ist auszusprechen: Zerfallen alle reellen Zahlen in zwei Klassen von der Art, daß jede Zahl der ersten Klasse algebraisch kleiner ist als jede Zahl der zweiten Klasse, so gibt es entweder in der ersten Klasse eine größte, oder in der zweiten Klasse eine kleinste Zahl.

Daß außer mir noch andere Mathematiker, insbesondere Weierstraß und G. Cantor, sich mit solchen Fragen beschäftigten, habe ich zuerst durch die Veröffentlichung einer Abhandlung von Heine (Die Elemente der Funktionenlehre, Crelles Journal, Bd. 74) im Jahre 1872 erfahren. Seitdem ist bekanntlich dieser Gegenstand in mehreren verdienstlichen Werken ausführlich und auf sehr verschiedene Art behandelt, doch scheint es mir, als ob die in denselben vorgetragenen Beweise nicht immer den kürzesten Weg einschlagen; insbesondere halte ich die oft benutzte Halbierungsmethode der Intervalle, die meines Wissens von Bolzano herrührt*), für einen zu weit-

*) Sie findet sich wohl zuerst in einer kleinen Schrift aus dem Jahre 1817, deren Titel ich nicht mehr genau anzugeben weiß, in welcher Bolzano den Satz zu beweisen versucht, daß eine stetige reelle Funktion einer reellen Variabelen in einem Intervall, in welchem sie sowohl positive wie negative Werte besitzt, auch den Wert Null annehmen muß. Diese Schrift ist wegen der vortrefflich geschriebenen Einleitung sehr lesenswert, aber an einer entscheidenden Stelle (in § 7) verfällt

läufigen Umweg, auf welchem das erstrebte Ziel nicht früh genug zum Bewußtsein kommt. Nun ist es oft nur Sache der Gewöhnung und des Geschmackes, ob man dem einen oder dem anderen Beweis den Vorzug zuerkennen will, und deshalb erlaube ich mir, als Beispiel meiner Beweismethode im folgenden einen allgemeinen Satz zu behandeln, welcher zahlreiche Anwendungen auf bekannte Fälle gestattet.

§ 1.

Ich bespreche zunächst eine Erscheinung, die bei Systemen von beliebigen Elementen eintreten kann, und benutze hierbei einige Begriffe und Kunstausdrücke in demselben Sinne wie in meiner Schrift „Was sind und was sollen die Zahlen?“ (Braunschweig, 1888); doch wird es zum Verständnis wohl genügen, wenn ich an folgendes erinnere. Ein System S ist bestimmt, wenn alle Elemente bestimmt sind, aus denen es besteht. Ein System T heißt Teil von S, wenn jedes Element von T auch Element von S ist, und zwar heißt T ein echter Teil von S, wenn T von S verschieden ist. Ein System T heißt Gemeinteil der Systeme $A, B, C \cdots$, wenn T Teil von jedem dieser Systeme ist, und unter ihrer Gemeinheit wird das System aller derjenigen Elemente verstanden, welche zugleich Elemente von jedem dieser Systeme sind; wenn es gar kein solches, allen Systemen $A, B, C \cdots$ gemeinsames Element gibt, so besitzen sie auch keinen Gemeinteil und keine Gemeinheit. Dagegen gibt es in allen Fällen ein, aus $A, B, C \cdots$ zusammengesetztes System M, welches dadurch vollständig bestimmt ist, daß jedes und nur jedes solche Ding als

---

der Verfasser in vollständige Verwirrung, und der Beweis mißlingt gänzlich, der ohne vorgängige Feststellung der Stetigkeit des reellen Zahlgebietes auch gar nicht gelingen kann.

Nach einer Mitteilung (1892, 12. 19.) von Herrn Prof. H. A. Schwarz (Villenkolonie Grunewald bei Berlin, Hubertusallee 13), der mir auch früher dies Werk von Bolzano eine zeitlang geliehen hatte, ist der Titel desselben folgender:

Beweis des Lehrsatzes, dass zwischen je zwey Werthen, die ein entgegengesetztes Resultat gewähren, wenigstens eine reelle Wurzel der Gleichung liege; von Bernard Bolzano. — Für die Abhandlungen der Königl. Gesellschaft der Wissenschaften. — Prag 1817. —

Vgl. Brief von H. A. Schwarz (1888, 4. 21.) an mich, und meine Antwort (1888, 4. 25.) mit Kritik von Bolzano und einigen Beweisen. —

Ferner: Brief von H. Weber (1892, 11. 18.) mit Beweis der Existenz einer Wurzel jeder algebraischen Gleichung; zu vergleichen auch mit meinem Beweise in meinem Briefe (1878, 6. 23.) an R. Lipschitz. —

Element von M gilt, welches Element von mindestens einem der Systeme A, B, $C \cdots$ ist. Statt der etwas schwerfälligen Bezeichnung, welche ich aus gewissen Gründen in der oben erwähnten Schrift gebraucht habe, will ich hier nach Schröder dieses System M mit $A + B + C + \cdots$ bezeichnen und die Summe der Systeme A, B, $C \cdots$ nennen. Jedes der letzteren ist ein Teil dieser Summe.

Hierauf gehe ich zur Erörterung eines, wie ich glaube, neuen Begriffs über, der für unsere Untersuchung von besonderer Wichtigkeit ist. Unter einem Teilschnitt φ eines Systems S verstehe ich eine Einteilung aller seiner Teile in zwei Arten, nämlich in reine und unreine Teile, welche den folgenden drei Bedingungen genügt.

1. Jeder Teil von S ist entweder rein oder unrein, aber niemals beides zugleich.

2. Jeder Teil eines reinen Teils ist rein.

3. Die Summe von je zwei reinen Teilen ist rein.

Offenbar lassen sich die beiden letzten Bedingungen auch in die folgende zusammenziehen:

4. Die Summe von zwei Teilen ist dann und nur dann rein, wenn beide Teile rein sind. Oder mit anderen Worten: die Summe von zwei Teilen ist dann und nur dann unrein, wenn mindestens einer der beiden Teile unrein ist.

Diese letzte Fassung erinnert an den Satz über das Verschwinden eines arithmetischen Produktes und führt zu der folgenden Charakterisierung des Teilschnittes φ, von der ich bisweilen Gebrauch machen werde. Belegt man jeden Teil A des Systems S mit einer Zahl $\varphi(A)$, welche $= 1$ oder $= 0$ sein soll, je nachdem A rein oder unrein ist, so ist

5. $$\varphi(A + B) = \varphi(A)\,\varphi(B),$$

wo A, B beliebige Teile von S bedeuten. Und umgekehrt, wenn jedem Teile A eines Systems S eine Zahl $\varphi(A)$ in der Weise entspricht, daß das vorstehende Gesetz 5. erfüllt wird, so ist hierdurch ein Teilschnitt φ von S bestimmt; denn aus $A + A = A$ ergibt sich zunächst, daß $\varphi(A) = 1$ oder $= 0$ sein muß, und wenn man A rein oder unrein nennt, je nachdem das Erstere oder das Letztere der Fall ist, so sind die obigen drei Bedingungen eines Teilschnittes wirklich erfüllt.

Ich füge noch die folgenden Bemerkungen hinzu. Jeder bestimmte Teil T eines Systems S erzeugt einen Teilschnitt von S,

welcher dadurch bestimmt ist, daß jeder beliebige Teil A von S als rein oder unrein gilt, je nachdem A Teil von T ist oder nicht: T selbst ist folglich ein reiner Teil. Auf den ersten Blick könnte es auch scheinen, als müßte jeder Teilschnitt φ von S auf solche Weise durch einen bestimmten Teil T von S erzeugt werden; da nämlich jedes Element von S auch ein Teil von S und folglich entweder rein oder unrein ist, so liegt es nahe, den Inbegriff T aller reinen Elemente zu betrachten und nach 3. zu glauben, der Teilschnitt φ werde durch T erzeugt. Allein dieser Schluß ist nur dann sicher, wenn T ein endliches System ist, d. h. aus einer endlichen Anzahl von Elementen besteht; in der Tat kann aus der Eigenschaft 3. durch vollständige Induktion (durch den Schluß von n auf $n + 1$) nur gefolgert werden, daß die Summe von lauter reinen Teilen $A, B, C \cdots$ gewiß rein ist, wenn ihre Anzahl endlich ist, während eine Summe von unendlich vielen reinen Teilen sehr wohl unrein sein kann. Um sich hiervon zu überzeugen, genügt es, das folgende Beispiel zu betrachten: ist S ein unendliches System, und nennt man jeden Teil A von S rein oder unrein, je nachdem A endlich oder unendlich ist, so sind die obigen drei Bedingungen eines Teilschnittes offenbar erfüllt; aber obgleich alle Elemente von S rein sind, so ist ihre Gesamtheit S doch unrein. Hieraus geht hervor, daß ein Teilschnitt durch die Einteilung aller Elemente in reine und unreine noch keineswegs bestimmt ist. Man könnte sich nun vielleicht veranlaßt fühlen, den Begriff eines Teilschnittes so abzuändern, daß die Bedingung 3. für jede Summe von lauter reinen Teilen gelten soll; allein hierdurch würde die Tragweite des Begriffs wesentlichen Schaden erleiden.

Eine zweite Bemerkung besteht in folgendem. Während die Fassung des in der Einleitung ausgesprochenen Prinzips der Stetigkeit schon die Voraussetzung enthält, daß jede der beiden dortigen Klassen mindestens eine Zahl enthält, also wirklich existiert — weil sonst von einer Vergleichung der Zahlen der einen Klasse mit denen der anderen gar keine Rede sein könnte —, so sollen hier bei dem Begriff des Teilschnittes auch die beiden Fälle zugelassen werden, daß alle Teile rein, oder daß alle Teile unrein sind. Man kann dann allgemein behaupten, daß, wenn T ein Teil von S ist, in jedem Teilschnitt φ des Systems S ein Teilschnitt ψ des Systems T enthalten ist, welcher dadurch vollständig bestimmt wird, daß jeder Teil A

von T für rein oder unrein gelten soll, je nachdem er durch den Teilschnitt φ für rein oder unrein erklärt ist; dies kann mit Benutzung der oben erwähnten Charakterisierung durch die Zahlen 1 und 0 auch so ausgesprochen werden, daß allgemein $\psi(A) = \varphi(A)$ sein soll. Für unsere Zwecke ist aber besonders wichtig, daß umgekehrt, wenn T ein echter Teil von S ist, jeder Teilschnitt ψ des Systems T zu einem Teilschnitt φ des Systems S in der Weise erweitert werden kann, daß ψ in φ enthalten ist; eine solche Erweiterung kann auf verschiedene, häufig auf unendlich viele Arten geschehen*), doch soll hier, wenn schlechthin von der Erweiterung φ des Teilschnittes ψ die Rede ist, immer nur die folgende Art gemeint sein: jeder Teil A von S soll dann und nur dann für unrein gelten, wenn es einen Gemeinteil von A und T gibt, welcher durch den Teilschnitt ψ für unrein erklärt ist. Daß diese auf ψ gegründete Einteilung φ aller Teile von S wirklich einen Teilschnitt von S bildet, ergibt sich leicht; denn von den drei obigen Bedingungen sind die beiden ersten offenbar erfüllt, und wenn weder in A noch in B ein unreiner Teil von T enthalten ist, so gilt dasselbe auch von der Summe $A + B$, weil jeder Teil der letzteren entweder Teil von A, oder Teil von B, oder von der Form $A_1 + B_1$ ist, wo A_1 Teil von A, und B_1 Teil von B ist; mithin ist auch die dritte Bedingung erfüllt, also φ ein Teilschnitt von S, und offenbar ist ψ in φ enthalten.

Eine dritte und letzte Bemerkung bezieht sich auf eine Verbindung des Teilschnittes φ eines Systems S mit irgendeiner Abbildung desselben Systems. Das Wesen einer solchen Abbildung besteht bekanntlich darin, daß jedem bestimmten Element a des Systems S ein Bild, d. h. ein bestimmtes Element entspricht, welches wir mit a' bezeichnen wollen; ist A irgend ein Teil von S, so soll der Kürze halber unter dem Bilde von A dasjenige System A' verstanden werden, dessen Elemente die Bilder aller Elemente von A sind. Vermöge einer solchen Abbildung entspringt nun aus einem Teilschnitt φ des Systems S eine bestimmte Einteilung φ' aller Teile P des Systems S' in reine und unreine Teile, wenn nämlich festgesetzt wird, daß P stets und nur dann für unrein gelten soll, wenn es einen unreinen Teil U von S gibt, dessen Bild U' Teil von P

*) Die allgemeinere Frage, wann und wie sich gegebene Teilschnitte von Systemen $A, B, C \cdots$ zu einem einzigen Teilschnitte ihrer Summe $A + B + C + \cdots$ zusammensetzen lassen, ist leicht zu beantworten.

ist; daß diese Einteilung φ' wieder einen Teilschnitt des Systems S' bildet, ergibt sich auf ähnliche Weise, wie in der vorhergehenden Bemerkung, und wir dürfen es daher dem Leser überlassen, diesen Nachweis zu führen.

§ 2.

Um diesen Begriff des Teilschnittes auf Systeme von Zahlen — und zwar immer nur von reellen Zahlen — anzuwenden, schicke ich folgende Erklärungen voraus. Ist c eine Zahl, so soll das Zeichen $[c]$ das System aller derjenigen Zahlen bedeuten, welche im algebraischen Sinne $\leqq c$ sind. Bedeutet ferner h eine positive Zahl (nicht Null), so bezeichne ich mit $(c)_h$ das System aller derjenigen Zahlen x, welche den Bedingungen $c - h \leqq x \leqq c + h$ genügen, und ich nenne jedes solche System eine Hülle von c, h ihren Halbmesser, c ihren Mittelpunkt. Zufolge der Erklärung einer Summe von Systemen (§ 1) ist dann

$$[c + h] = [c - h] + (c)_h,$$

wo selbstverständlich das Zeichen $c + h$ die arithmetische Summe der Zahlen c und h, nicht nur das aus den beiden Elementen c und h bestehende System bedeutet. Ist T irgendein System von Zahlen, so soll die Zahl c eine Beizahl von T heißen, wenn in jeder Hülle von c mindestens eine Zahl des Systems T enthalten ist; offenbar ist jede Zahl des Systems T auch eine Beizahl von T, und wenn zugleich das Umgekehrte gilt, so soll T ein selbständiges System heißen*). Man erkennt leicht, daß das System T_0 aller Beizahlen von T stets selbständig ist; denn wenn c_0 eine Beizahl von T_0 bedeutet, so ist in jeder Hülle $(c_0)_h$ mindestens eine Zahl des Systems T_0, also eine Beizahl c des Systems T enthalten, und da in der Hülle $(c)_h$, also auch in jeder Hülle $(c_0)_{2h}$ mindestens eine Zahl des Systems T enthalten ist, so ist c_0 selbst eine Beizahl von T, also in T_0 enthalten, w. z. b. w. Nennen wir ferner T ein begrenztes System, wenn es eine Zahl gibt, welche absolut größer ist, als jede Zahl in T, so besteht folgender Satz:

Werden alle Teile eines begrenzten Zahlensystems T durch einen Teilschnitt ψ in reine und unreine Teile ein-

*) Diese Begriffe einer Beizahl und eines selbständigen Systems sind wohl zu unterscheiden von dem, was G. Cantor einen Grenzpunkt eines Systems und eine perfekte Mannigfaltigkeit nennt.

geteilt, und ist T selbst unrein, so gibt es eine kleinste Zahl c von der Art, daß in jeder Hülle von c ein unreiner Teil von T enthalten ist.

Der Beweis gewinnt die einfachste Ausdrucksweise, wenn man nach der in § 1 gegebenen Vorschrift den Teilschnitt ψ zu einem Teilschnitt φ des Systems S aller Zahlen erweitert, wodurch die Behauptung des Satzes sich offenbar in die folgende verwandelt: es gibt eine kleinste Zahl c, deren Hüllen sämtlich unrein sind. Um dieselbe zu beweisen, teile man alle Zahlen x in zwei Klassen A, B ein, indem man x in A oder in B aufnimmt, je nachdem das System $[x]$ rein oder unrein ist. Da T begrenzt ist, so gibt es eine positive Zahl e, welche absolut größer ist als jede Zahl in T; dann gehört $-e$ der Klasse A an, weil das System $[-e]$ gar keine Zahl mit T gemein hat und folglich rein ist; aber $+e$ gehört zu B, weil das unreine System T ein Teil von $[e]$, also auch letzteres System unrein ist. Mithin existieren beide Klassen A, B. Jede Zahl a der Klasse A ist algebraisch kleiner als jede Zahl b in B, weil, wenn $a \geqq b$ wäre, das reine System $[a]$ einen unreinen Teil $[b]$ besäße, was dem Begriff des Teilschnittes widerspricht. Nach dem in der Einleitung ausgesprochenen Prinzip der Stetigkeit gibt es daher eine Zahl c, welche entweder die größte in A oder die kleinste in B ist, so daß, wenn h irgendeine positive Zahl bedeutet, $c - h$ in A, $c + h$ in B enthalten ist; da nun das unreine System $[c + h]$ die Summe des reinen Systems $[c - h]$ und der Hülle $(c)_h$ ist, so folgt aus dem Begriff des Teilschnittes, daß die letztere stets unrein ist. Wenn endlich $a < c$ ist, so kann man eine positive Zahl h so wählen, daß $a + h$ auch der Klasse A angehört, woraus folgt, daß die Hülle $(a)_h$ als Teil des reinen Systems $[a + h]$ ebenfalls rein ist. Mithin ist c die kleinste Zahl, deren sämtliche Hüllen unrein sind, w. z. b. w.

Die Zahl c ist offenbar eine Beizahl des Systems T; ist daher letzteres selbständig, so ist c selbst in T enthalten.

Der bewiesene Satz umfaßt sehr viele, vielleicht alle diejenigen Existenz-Sätze, welche in der Theorie der Funktionen von einer reellen Veränderlichen behandelt zu werden pflegen. Es wird aber nicht nötig sein, dies hier auszuführen, weil wir später (§ 4) dieselben Sätze für Funktionen von mehreren Veränderlichen beweisen werden.

§ 3.

Ein ganz ähnlicher Satz gilt nun auch für den n-fach ausgedehnten stetigen Zahlenraum S. Unter einem Elemente oder einem Punkte $\mathfrak{a}$ dieses Raumes verstehe ich, wie üblich, jede bestimmte Folge von n reellen Zahlen $a_1, a_2 \cdots a_{n-1}, a_n$, und diese sollen die Koordinaten von $\mathfrak{a}$ heißen. Ist h irgendeine positive Zahl (nicht Null), so soll mit $(\mathfrak{a})_h$ das System aller der Punkte bezeichnet werden, deren Koordinaten $x_1, x_2 \cdots x_n$ den Bedingungen

$$a_1 - h \leqq x_1 \leqq a_1 + h,\ a_2 - h \leqq x_2 \leqq a_2 + h,\ \cdots,\ a_n - h \leqq x_n \leqq a_n + h$$

genügen, und ich nenne jedes solche System $(\mathfrak{a})_h$ eine Hülle von $\mathfrak{a}$, h ihren Halbmesser, $\mathfrak{a}$ ihren Mittelpunkt. Ist T irgendein System von Punkten, also ein Teil von S, so soll der Punkt $\mathfrak{c}$ ein Beipunkt von T heißen, wenn in jeder Hülle von $\mathfrak{c}$ mindestens ein Punkt von T enthalten ist; offenbar ist jeder Punkt des Systems T auch ein Beipunkt von T, und wenn zugleich das Umgekehrte gilt, so soll T ein selbständiges System heißen; man überzeugt sich leicht (wie in § 2), daß das System T_0 aller Beipunkte von T stets selbständig ist. Das System T heißt begrenzt, wenn es eine Zahl gibt, welche absolut größer ist als jede Koordinate jedes in T enthaltenen Punktes.

Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei verschiedene Punkte, deren $r$te Koordinaten bzw. mit a_r, b_r bezeichnet werden, so will ich $\mathfrak{a}$ den tieferen, $\mathfrak{b}$ den höheren nennen, wenn in der Folge der Differenzen

$$b_1 - a_1,\quad b_2 - a_2,\quad \cdots,\quad b_n - a_n$$

die erste, welche nicht verschwindet, einen positiven Wert hat, und dies soll kurz durch die Symbole $\mathfrak{a} < \mathfrak{b}$, $\mathfrak{b} > \mathfrak{a}$ bezeichnet werden*). Von je zwei verschiedenen Punkten ist immer einer der tiefere, der andere der höhere, und der Gebrauch des Komparativs rechtfertigt sich dadurch, daß aus $\mathfrak{a} < \mathfrak{b}$ und $\mathfrak{b} < \mathfrak{c}$ stets $\mathfrak{a} < \mathfrak{c}$ folgt. Zugleich leuchtet ein, was es heißen soll, wenn ein Punkt der tiefste oder der höchste Punkt eines Systems genannt wird.

Alle diese Namen und Bezeichnungen entsprechen, wenn $n = 1$ ist, denjenigen, welche in § 2 gebraucht sind; ist aber $n > 1$, so tritt noch folgendes hinzu. Unterdrückt man die letzte Koordinate a_n des Punktes $\mathfrak{a}$, so bildet die Folge der übrigen $a_1, a_2 \cdots a_{n-1}$ einen

*) Bei dieser Unterscheidung ist von wesentlicher Bedeutung die Reihenfolge der Koordinaten, die natürlich durch jede andere ersetzt werden kann.

Punkt $\mathfrak{a}'$ des $(n-1)$fachen Zahlenraumes; dieser Punkt $\mathfrak{a}'$ soll das Bild oder die Projektion des Punktes $\mathfrak{a}$ heißen, und wenn T irgend ein Teil von S ist, so soll unter seiner Projektion T' dasjenige System verstanden werden, dessen Elemente die Projektionen aller in T enthaltenen Punkte sind, und welches folglich ein Teil des ganzen $(n-1)$fachen Zahlenraumes S' ist. Die Projektion der Hülle $(\mathfrak{a})_h$ ist die Hülle $(\mathfrak{a}')_h$ der Projektion $\mathfrak{a}'$. Jeder Punkt $\mathfrak{a}$ des Raumes S ist vollständig bestimmt durch Angabe seiner Projektion $\mathfrak{a}'$ und seiner letzten Koordinate a_n und kann daher durch das Symbol $(\mathfrak{a}', a_n)$ bezeichnet werden; allgemeiner, wenn P irgendein Teil von S', und Q irgendein Teil des einfachen Zahlenraumes ist, so soll mit (P, Q) das System aller derjenigen Punkte $\mathfrak{a}$ in S bezeichnet werden, deren Projektion $\mathfrak{a}'$ in P, und deren letzte Koordinate a_n in Q enthalten ist. Die Einführung der Projektionen soll dazu dienen, um mit Hilfe der vollständigen Induktion den folgenden allgemeinen Satz zu beweisen:

I. Ist T ein begrenztes System von Punkten im n-fachen Zahlenraum S, und werden alle Teile von T durch einen Teilschnitt ψ in reine und unreine Teile eingeteilt, so gibt es, wenn T selbst unrein ist, einen tiefsten Punkt $\mathfrak{c}$ von der Art, daß in jeder Hülle von $\mathfrak{c}$ ein unreiner Teil von T enthalten ist.

Auch hier erleichtern wir uns den Beweis, indem wir den Teilschnitt ψ des Systems T nach der in § 1 gegebenen Vorschrift zu einem Teilschnitt φ des ganzen n-fachen Zahlenraumes S erweitern, wodurch unser Satz sich offenbar in den folgenden verwandelt:

Ist T ein begrenzter Teil von S, und werden alle Teile von S durch einen Teilschnitt φ in reine und unreine Teile so eingeteilt, daß T für unrein, und daß jeder Teil, welcher mit T keinen Punkt gemein hat, für rein gilt, so gibt es einen tiefsten Punkt $\mathfrak{c}$, dessen Hüllen sämtlich unrein sind.

Dies ist für den Fall $n = 1$ schon in § 2 bewiesen, und wir brauchen daher nur zu zeigen, daß aus der Wahrheit dieses Satzes für den $(n-1)$fachen Raum S' auch seine Wahrheit für den n-fachen Raum S folgt. Zu diesem Zwecke leiten wir nach der am Schlusse von § 1 gegebenen Vorschrift aus dem Teilschnitt φ einen Teilschnitt φ' des Raumes S' ab, indem wir irgendeinen Teil P des letzteren dann und nur dann für unrein erklären, wenn es einen

unreinen Teil U von S gibt, dessen Projektion U' Teil von P ist. Die Projektion T' des begrenzten und unreinen Teiles T von S ist offenbar ein begrenzter und unreiner Teil von S', und jeder Teil P von S', der mit T' keinen Punkt gemein hat, ist gewiß rein; denn jeder unreine Teil U von S hat mindestens einen Punkt a mit T gemein und seine Projektion U' kann daher, weil sie mindestens einen Punkt a' mit T' gemein hat, nicht Teil von P sein. Nehmen wir daher an, der oben ausgesprochene Satz gelte für den $(n-1)$fachen Raum S', so gibt es in demselben einen tiefsten Punkt c', dessen Hüllen sämtlich unrein sind, und folglich gibt es, wenn k irgend eine positive Zahl bedeutet, immer einen unreinen Teil U von S, dessen Projektion U' Teil der Hülle $(c')_k$ ist. Bedeutet nun Q den ganzen einfachen Zahlenraum, so ist U jedenfalls ein Teil des Systems $((c')_k, Q)$, und folglich ist auch letzteres ein unreiner Teil des Raumes S. Da ferner T begrenzt ist, so gibt es eine positive Zahl e, welche absolut größer ist, als jede Koordinate jedes Punktes in T; bezeichnet man daher mit E das System aller derjenigen Zahlen, welche algebraisch größer als e sind, so hat das System $((c')_k, E)$ keinen Punkt mit T gemein und ist folglich rein, und da das unreine System

$$((c')_k, Q) = ((c')_k, E) + ((c')_k, [e])$$

ist, so ist auch das zweite System rechter Hand unrein. Zugleich leuchtet ein, daß das System $((c')_k, [-e])$ rein ist, weil es keinen Punkt mit T gemein hat. Hierauf teilen wir alle reellen Zahlen x in zwei Klassen A, B ein; die Zahl x soll zur zweiten Klasse B gehören, wenn jeder positiven Zahl k ein unreines System $((c')_k, [x])$ entspricht; im entgegengesetzten Falle soll x zur ersten Klasse A gehören. Offenbar ist $-e$ in A, aber $+e$ in B enthalten, also existieren beide Klassen. Jede Zahl a der Klasse A ist algebraisch kleiner als jede Zahl b der Klasse B, weil, wenn $a \geqq b$ wäre, es ein reines System $((c')_k, [a])$ gäbe, welches einen unreinen Teil $((c')_k, [b])$ besäße, was dem Begriff eines Teilschnittes φ widerspricht. Nach dem in der Einleitung ausgesprochenen Stetigkeitsprinzip gibt es daher eine Zahl c, welche entweder die größte in A oder die kleinste in B ist, und wir wollen zeigen, daß der hierdurch bestimmte Punkt $c = (c', c)$ die in dem obigen Satze behauptete Eigenschaft besitzt. Bedeutet h irgendeine positive Zahl, so gehört $c - h$ zur Klasse A,

und folglich gibt es eine positive Zahl k, welche ein reines System $((\mathfrak{c}')_k, [c - h])$ erzeugt, und wenn l die kleinste der beiden Zahlen h, k bedeutet, so ist das System $((\mathfrak{c}')_l, [c - h])$ als ein Teil des vorigen ebenfalls rein. Da andererseits $c + h$ zur Klasse B gehört, so ist das System $((\mathfrak{c}')_l, [c + h])$ unrein, und da es die Summe des vorigen und des Systems $((\mathfrak{c}')_l, (\mathfrak{c})_h)$ ist, so ist letzteres ebenfalls unrein; dieses ist aber, weil $l \leqq h$ ist, ein Teil des Systems $((\mathfrak{c}')_h, (\mathfrak{c})_h) = (\mathfrak{c})_h$, und folglich ist jede Hülle des Punktes $\mathfrak{c}$ unrein. Wir haben noch zu zeigen, daß $\mathfrak{c}$ der tiefste solche Punkt ist, daß also jeder tiefere Punkt $\mathfrak{a}$ mindestens eine reine Hülle besitzt. Aus $\mathfrak{a} < \mathfrak{c}$ folgt gewiß $\mathfrak{a}' \leqq \mathfrak{c}'$; ist nun zunächst $\mathfrak{a}' < \mathfrak{c}'$, so gibt es zufolge der Definition des Punktes $\mathfrak{c}'$ und des Teilschnittes φ' mindestens eine reine Hülle $(\mathfrak{a}')_h$, und da dieselbe die Projektion der Hülle $(\mathfrak{a})_h$ ist, so muß auch letztere rein sein. Ist aber $\mathfrak{a}' = \mathfrak{c}'$, so ist die letzte Koordinate a des Punktes $\mathfrak{a}$ algebraisch kleiner als c; man kann daher eine positive Zahl l so wählen, daß auch $a + l$ zur Klasse A gehört; dann gibt es eine positive Zahl k, welche ein reines System $((\mathfrak{c}')_k, [a + l])$ erzeugt; bedeutet nun h die kleinste der beiden Zahlen k, l, so ist die Hülle $(\mathfrak{a})_h$ als Teil dieses reinen Systems ebenfalls rein, w. z. b. w.

Nachdem der Satz hiermit allgemein bewiesen ist, mag noch bemerkt werden, daß der Punkt $\mathfrak{c}$ ein Beipunkt des Systems T und folglich, falls letzteres selbständig ist, selbst in T enthalten ist.

§ 4*).

Bei den nun folgenden Anwendungen beschränke ich mich auf einige sehr bekannte Sätze; ihr Beweis kommt immer auf eine zweckmäßige, den Bedingungen 1 bis 4 genügende Definition der reinen und unreinen Systeme zurück.

II. Ist U ein bestimmter Teil von T, so gibt es einen tiefsten Punkt von der Beschaffenheit, daß jede seiner Hüllen mindestens einen Punkt von U enthält.

Dies geht unmittelbar aus dem obigen Satze I (§ 3) hervor, wenn man jeden Teil von T unrein oder rein nennt, je nachdem er mindestens einen oder keinen Punkt von U enthält; denn diese Definition genügt offenbar den Bedingungen 1 bis 4 (§ 1).

*) [In diesem der ersten Fassung entnommenen Paragraphen (vgl. die Erläuterungen) ist T als beschränkt und abgeschlossen vorausgesetzt, so daß der obige Punkt $\mathfrak{c}$ stets zu T gehört (§ 3, Schluß). E. N.]

Die folgenden Sätze beziehen sich auf irgendeine eindeutige reelle Funktion der beiden Variabelen x, y; jedem Punkte $\mathfrak{p} = (x, y)$ von T entspricht eine bestimmte reelle Zahl $\mathfrak{p}'$, die ich das Bild des Punktes $\mathfrak{p}$ nenne, und wenn U irgendein Teil von T ist, so soll U' das Bild von U, d. h. den Inbegriff der Bilder $\mathfrak{p}'$ aller in U enthaltenen Punkte $\mathfrak{p}$ bedeuten.

III. Es gibt einen tiefsten Punkt (a, b) von folgender Beschaffenheit: ist c irgendeine Zahl des Systems T', so gibt es in jeder Hülle von (a, b) mindestens einen Punkt $\mathfrak{p}$, dessen Bild $\mathfrak{p}' \leqq c$ ist.

Dies geht unmittelbar aus dem Satze I hervor, wenn man jeden Teil U von T rein oder unrein nennt, je nachdem es in T' mindestens eine oder keine Zahl gibt, die kleiner als jede Zahl in U' ist; denn diese Definition genügt den Bedingungen 1 bis 4.

IV. Ist c ein Beiwert (§ 2) des Systems T', so gibt es einen tiefsten Punkt (a, b) von folgender Beschaffenheit: ist H irgendeine Hülle von (a, b), so ist c auch Beiwert des Systems H'.

Dies geht unmittelbar aus dem Satze I hervor, wenn man jeden Teil U von T unrein oder rein nennt, je nachdem c Beiwert von U' ist oder nicht; denn diese Definition genügt den Bedingungen 1 bis 4.

Die Abbildung (Funktion) heißt stetig im Punkte $\mathfrak{p}$, wenn, wie klein auch die positive Größe k gegeben sein mag, man immer eine Hülle H von $\mathfrak{p}$ so wählen kann, daß alle Zahlen in H' um weniger als k von $\mathfrak{p}'$, also um weniger als $2k$ voneinander verschieden sind. Die Funktion heißt stetig in T, wenn sie in jedem Punkte von T stetig ist. Dann ergeben sich aus den Sätzen III und IV die folgenden Sätze:

V. Eine in T stetige Funktion besitzt einen kleinsten Wert, und es gibt einen tiefsten Punkt, in welchem die Funktion diesen Minimumwert annimmt.

Denn wenn es in T' eine Zahl c gäbe, welche kleiner als $(a, b)'$ ist, wo (a, b) den in III bestimmten Punkt bedeutet, so könnte man eine Hülle H von (a, b) so wählen, daß alle Zahlen in H' größer als c wären, was im Widerspruch mit der dort bewiesenen Eigenschaft des Punktes (a, b) steht; mithin ist $(a, b)'$ die kleinste Zahl in T'. Und es kann auch keinen tieferen Punkt (α, β) geben, in

welchem derselbe Minimumwert $(\alpha, \beta)' = (a, b)'$ auftritt, weil ein solcher Punkt (α, β) gewiß dieselbe, in III angegebene Beschaffenheit besitzt, wie (a, b).

VI. Ist die Abbildung (Funktion) stetig in T, so ist jeder Beiwert c von T' auch eine Zahl in T', und es gibt einen tiefsten Punkt (a, b), in welchem die Funktion diesen Wert $c = (a, b)'$ annimmt.

Denn wenn (a, b) den in IV bestimmten Punkt bedeutet, so kann $(a, b)'$ nicht von c verschieden sein, weil man sonst eine Hülle H von (a, b) so wählen könnte, daß alle Zahlen in H' um mehr als eine bestimmte positive Größe von c verschieden wären, also c kein Beiwert von H' wäre, was in Widerspruch mit IV steht; mithin ist $(a, b)' = c$. Und es kann auch keinen tieferen Punkt (α, β) geben, dessen Bild $(\alpha, \beta)' = c$ ist.

VII*). Besitzt eine in T stetige Funktion sowohl positive als auch negative Werte, so gibt es auch einen tiefsten Punkt, in welchem sie verschwindet.

Dies versteht sich von selbst, wenn die Funktion im Nullpunkte (0,0) verschwindet. Ist aber $(0,0)'$ positiv (auf welchen Fall wir uns beschränken dürfen), so soll ein Teil U von T rein heißen, wenn U' aus lauter positiven Zahlen besteht; im entgegengesetzten Falle heiße U unrein. Da diese Definition den Bedingungen 1. bis 4. genügt, so gibt es (nach Satz I) einen tiefsten Punkt (a, b) von der Beschaffenheit, daß jede seiner Hüllen H unrein ist.

Ich behaupte, daß $(a, b)' = 0$ ist. Denn jedenfalls kann $(a, b)'$ nicht positiv sein, weil es sonst zufolge der Stetigkeit auch reine Hüllen H gäbe. Nehmen wir ferner an, $(a, b)'$ sei negativ, so kann man zufolge der Stetigkeit eine Hülle H so wählen, daß H' aus lauter negativen Zahlen besteht; da aber (a, b) nicht der Nullpunkt ist, so gibt es in H gewiß einen Punkt (α, β), der tiefer ist als (a, b), und da $(\alpha, \beta)'$ negativ ist, so wäre auch jede Hülle von (α, β) unrein, während doch (a, b) der tiefste Punkt ist, der diese Eigenschaft besitzt. Mithin ist $(a, b)' = 0$, und es kann auch keinen tieferen Punkt als (a, b) geben, in welchem die Funktion verschwindet, weil wieder jede Hülle eines solchen Punktes unrein ist, w. z. b. w.

*) [Der Beweis gilt in der hier gegebenen Fassung nur für das Quadrat $0 \leqq x \leqq 1$, $0 \leqq y \leqq 1$. Dedekind hatte die allgemeinere Gültigkeit des Satzes bemerkt, ohne die nötigen Abänderungen hinzuschreiben. E. N.]

Ich schließe mit folgendem, für den Begriff des Doppelintegrals wichtigen Satze:

VIII. Ist z eine in T stetige Funktion, und k eine positive Größe, so kann man eine für alle Punkte $\mathfrak{p}$ gemeinsame positive Größe h so wählen, daß z in jeder Hülle $(\mathfrak{p}, h)$ sich um weniger als k ändert.

Um dies zu beweisen, bemerke ich zunächst folgendes. Ist $\mathfrak{p}$ ein bestimmter Punkt in T, so gibt es zufolge der Stetigkeit der Funktion z eine Hülle $(\mathfrak{p}, 2h)$, in welcher z sich um weniger als k ändert; betrachtet man nun alle Punkte $\mathfrak{q}$ der Hülle $(\mathfrak{p}, h)$, so ist jede Hülle $(\mathfrak{q}, h)$, deren Halbmesser $= h$, ein Teil von $(\mathfrak{p}, 2h)$, und folglich ändert sich z auch in jeder solchen Hülle $(\mathfrak{q}, h)$ um weniger als k; das Punktsystem $U = (\mathfrak{p}, h)$ hat daher die Eigenschaft, welche unser Satz dem ganzen T zuschreibt: man kann alle Punkte des Systems U in Hüllen vom gemeinsamen Halbmesser h so einschließen, daß z in jeder einzelnen solchen Hülle sich um weniger als k ändert. Nehmen wir nun an, unser Satz sei unrichtig, so nennen wir, wenn dies auch unpassend klingen mag, einen Teil von T rein oder unrein, je nachdem er die eben ausgesprochene Eigenschaft besitzt oder nicht besitzt. Diese Einteilung genügt offenbar den Bedingungen eines Teilschnittes, auch der letzten; denn wenn h_1, h_2 genügend kleine (geeignete) Halbmesser für die reinen Systeme U_1, U_2 sind, so ist die kleinste der beiden Zahlen h_1, h_2 ein genügend kleiner Halbmesser für das aus U_1 und U_2 zusammengesetzte System. Nach dem Satz I müßte es daher mindestens einen Punkt $\mathfrak{p}$ geben, dessen Hüllen sämtlich unrein sind, während doch oben gezeigt ist, daß jeder Punkt $\mathfrak{p}$ eine reine Hülle besitzt. Mithin muß auch T rein sein, w. z. b. w.

Erläuterungen zur vorstehenden Abhandlung.

Das Manuskript lag in zwei Fassungen vor, von denen die zweite von Dedekind als „sorgfältigere Fassung desselben Gegenstandes" bezeichnet war. In dieser zweiten Fassung fehlte aber die Einleitung und der Paragraph mit den Anwendungen, die daher aus der ersten Fassung übernommen sind (wobei x, y statt $x_1, \cdots, x_n$ stehen blieb).

Zur Terminologie ist zu bemerken, daß die Dedekindschen Bezeichnungen „Beipunkt" und „selbständiges System" dem „Berührpunkt" (vgl. Hausdorff, Mengenlehre) und der „abgeschlossenen Menge" entsprechen; der Übergang von T zum „selbständigen System T_0" ist der Übergang zur „abgeschlossenen Hülle"

(Dedekind gebraucht den Ausdruck „Hülle“ für n-dimensionale abgeschlossene Würfelumgebung eines Punktes).

Den Anwendungen kann vielleicht noch hinzugefügt werden der Heine-Borelsche Überdeckungssatz:

Es sei jedem Punkt $\mathfrak{p}$ von T (wo T abgeschlossen und beschränkt) eine $\mathfrak{p}$ enthaltende offene Menge $\delta_{\mathfrak{p}}$ zugeordnet. Man nenne eine Untermenge U von T rein oder unrein, je nachdem U durch endlich viele $\delta_{\mathfrak{p}}$ überdeckt wird oder nicht. Ist T unrein — d. h. der Überdeckungssatz nicht erfüllt —, so gibt es einen Punkt $\mathfrak{c}$ von T derart, daß jede Würfelumgebung von $\mathfrak{c}$ unrein. Das ist aber ein Widerspruch; denn ist $\delta_{\mathfrak{c}}$ die $\mathfrak{c}$ zugeordnete offene Menge, $W_{\mathfrak{c}} \subseteq \delta_{\mathfrak{c}}$ eine Würfelumgebung von $\mathfrak{c}$ (eine solche existiert, da die W eine Basis aller Umgebungen bilden), so ist $W_{\mathfrak{c}}$ rein; denn es wird von einem $\delta_{\mathfrak{c}}$ überdeckt.

Noether.

XXXVII.

Stetiges System aller Abbildungen der natürlichen Zahlenreihe N in sich selbst.

1. Abbildung α von N in sich selbst. Ist n eine natürliche Zahl, so sei $n\alpha$ das durch α erzeugte Bild von n; $n\alpha$ ist eine natürliche Zahl.

2. Sind α, β Abbildungen von N in sich selbst und verschieden voneinander, so gibt es mindestens eine natürliche Zahl n, für welche die Differenz $n\alpha - n\beta$ von Null verschieden ist, und unter diesen Zahlen n gibt es eine kleinste r. Dann ist

$$x\alpha = x\beta, \quad \text{falls} \quad x < r,$$

und $r\alpha - r\beta$ ist entweder positiv oder negativ. Im ersten Falle

$$r\alpha > r\beta$$

heiße α größer als β, β kleiner als α, in Zeichen

$$\alpha > \beta \quad \text{und} \quad \beta < \alpha.$$

Im zweiten Falle ist $r\beta > r\alpha$, mithin $\beta > \alpha$, $\alpha < \beta$. Also: von zwei verschiedenen Abbildungen α, β ist immer eine und nur eine größer als die andere.

3. Satz: Sind α, β, γ drei verschiedene Abbildungen von N in sich selbst, und ist $\alpha > \beta$, $\beta > \gamma$, so ist auch $\alpha > \gamma$.

Beweis: Zufolge der beiden Annahmen $\alpha > \beta$, $\beta > \gamma$ gibt es zwei natürliche Zahlen r, s von folgender Beschaffenheit:

$$r\alpha > r\beta, \quad x\alpha = x\beta \quad \text{für} \quad x < r,$$
$$s\beta > s\gamma, \quad y\beta = y\gamma \quad \text{für} \quad y < s.$$

Nun sind zwei Fälle denkbar: entweder ist $r \leqq s$, oder es ist $r > s$. Im ersten Falle ist $r\alpha > r\beta$ und, je nachdem $r < s$ oder $r = s$ ist, $r\beta = r\gamma$ oder $r\beta > r\gamma$, also gewiß $r\alpha > r\gamma$, und da

jede Zahl x, welche $< r$, auch $< s$ ist, so ist $x\alpha = x\beta$ und $x\beta = x\gamma$, also auch $x\alpha = x\gamma$, mithin

$$r\alpha > r\gamma \quad \text{und} \quad x\alpha = x\gamma \quad \text{für} \quad x < r, \quad \text{also} \quad \alpha > \gamma,$$

w. z. b. w.

Im zweiten Falle $r > s$ ist $s\alpha = s\beta$ und $s\beta > s\gamma$, also auch $s\alpha > s\gamma$, und da jede Zahl y, welche $< s$, auch $< r$ ist, so folgt $y\alpha = y\beta$, und $y\beta = y\gamma$, also $y\alpha = y\gamma$, mithin

$$s\alpha > s\gamma \quad \text{und} \quad y\alpha = y\gamma \quad \text{für} \quad y < s, \quad \text{also} \quad \alpha > \gamma,$$

w. z. b. w.

[Diese kleine Bemerkung trägt das Datum 1891. 1. 2.]

XXXVIII.

Charakteristische Eigenschaft einklassiger Körper Ω.

Die erforderliche und hinreichende Bedingung dafür, daß ein endlicher Körper Ω einklassig ist, besteht darin, daß für je zwei ganze Zahlen α, β in Ω, deren letztere β von Null verschieden ist, immer zwei ganze Zahlen μ, ν in Ω gewählt werden können, deren erstere μ relative Primzahl zu β ist, und für welche die Norm $N(\alpha\mu + \beta\nu)$ absolut $< N(\beta)$ ist.

Beweis. I. Ist Ω einklassig, und $\mathfrak{o}$ die Hauptordnung, d. h. das System aller ganzen Zahlen in Ω, so ist

$$\mathfrak{o}\alpha + \mathfrak{o}\beta = \mathfrak{o}\delta \text{ (Hauptideal).}$$

Ist α teilbar durch β, so kann man $\delta = \beta$, $\alpha = \beta\gamma$, $\mu = -1$, $\nu = \gamma$ setzen, wodurch den Forderungen genügt wird, weil μ relative Primzahl zu β, wo $N(\alpha\mu + \beta\nu) = 0$ abs. $< N(\beta)$ ist. Wenn aber α nicht teilbar durch β ist, so setze man

$$\alpha = \delta\alpha_1, \ \beta = \delta\beta_1, \quad \text{also} \quad \mathfrak{o}\alpha_1 + \mathfrak{o}\beta_1 = \mathfrak{o};$$

mithin sind α_1, β_1 relative Primzahlen, und es gibt ganze Zahlen α_2, die der Kongruenz

$$\alpha_1\alpha_2 \equiv 1 \pmod{\beta_1}$$

genügen (§ 174, S. 533, § 178, XIII, S. 559 und S. 556).

Ist nun π das Produkt aller derjenigen in δ aufgehenden Primzahlen des Körpers Ω, die nicht in β_1 aufgehen (evtl. $\pi = 1$, wenn es keine solche Primzahl gibt), so sind β_1, π relative Primzahlen, und folglich (§ 180, II, S. 568) gibt es in $\mathfrak{o}$ Zahlen μ, die den simultanen Kongruenzen

$$\mu \equiv \alpha_2 \pmod{\beta_1}, \ \mu \equiv 1 \pmod{\pi}$$

genügen; hieraus folgt, daß μ relative Primzahl zu π und (wie α_2) zu β_1, also auch zu β ist, weil jede in $\beta = \delta\beta_1$ aufgehende Primzahl entweder in β_1 oder in δ, also in π aufgeht. Aus der ersteren dieser Folgerungen folgt ferner

$$\alpha_1\mu \equiv \alpha_1\alpha_2 \equiv 1 \pmod{\beta_1},$$

also gibt es in $\mathfrak{o}$ eine Zahl ν, die der Bedingung

$$\alpha_1\mu + \beta_1\nu = 1, \quad \alpha\mu + \beta\nu = \delta$$

genügt, woraus der Beweis von I, nämlich

$$N(\alpha\mu + \beta\nu) = N(\delta) = \frac{N(\beta)}{N(\beta_1)} \text{ abs.} < N(\beta)$$

folgt, weil β_1 keine Einheit, also $N(\beta_1) > 1$ ist (α nicht teilbar durch β).

II. Umkehrung: Der endliche Körper Ω, dessen Hauptordnung $\mathfrak{o}$, ist gewiß einklassig, wenn es für je zwei Zahlen α, β in $\mathfrak{o}$, deren letztere von Null verschieden ist, immer zwei Zahlen μ, ν in $\mathfrak{o}$ gibt, deren erstere relative Primzahl zu β ist, und die der Bedingung

$$N(\alpha\mu + \beta\nu) \text{ abs.} < N(\beta)$$

genügen.

Bei dem Beweise wollen wir, wenn α, β, α', β' Zahlen in $\mathfrak{o}$ sind, durch das Zeichen

$$(\alpha, \beta) \sim (\alpha', \beta')$$

andeuten, daß der Komplex aller gemeinsamen Teiler von α, β identisch mit dem aller gemeinsamen Teiler von α', β' ist. Sind nun α, β gegeben, und μ, ν so gewählt, daß sie den beiden Bedingungen genügen, und setzen wir

$$\gamma = \alpha\mu + \beta\nu,$$

so folgt daraus

$$(\alpha, \beta) \sim (\beta, \gamma);$$

denn offenbar ist jeder gemeinsame Teiler von α, β auch ein Teiler von γ, also gemeinsamer Teiler von β, γ; und aus $\alpha\mu = \gamma - \beta\nu$ folgt, daß jeder gemeinsame Teiler von β, γ auch ein Teiler von $\alpha\mu$ und, weil er als Teiler von β relative Primzahl zu μ ist, auch Teiler von α, also gemeinsamer Teiler von α, β ist, wie behauptet war. Aus jedem Paare α, β, wo β von Null verschieden, kann man daher eine Zahl γ in $\mathfrak{o}$ bilden, die den Bedingungen

$$(\alpha, \beta) \sim (\beta, \gamma) \quad \text{und} \quad N(\gamma) \text{ abs.} < N(\beta)$$

genügt.

Der Fall $\gamma = 0$ tritt offenbar nur dann ein, wenn jeder Teiler von β, also auch β selbst in α aufgeht (und umgekehrt, wenn α durch β teilbar ist, so kann man μ, ν wie in I so wählen, daß $\gamma = 0$ wird); in diesem Fall besitzen also α, β einen größten gemeinsamen Teiler β.

Ist aber γ von Null verschieden, so kann man wieder eine Zahl δ in $\mathfrak{o}$ bilden, die den Bedingungen

$$(\gamma, \delta) \sim (\beta, \gamma) \sim (\alpha, \beta) \quad \text{und} \quad N(\delta) < N(\gamma) < N(\beta)$$

genügt, woraus offenbar auch $(\gamma, \delta) \sim (\alpha, \beta)$ folgt. Fährt man, wenn δ nicht Null ist, so fort, so erhält man eine Reihe von Zahlen $\beta, \gamma, \delta, \varepsilon, \cdots$ in $\mathfrak{o}$, deren Normen absolut immer kleiner werden; es muß daher in dieser Reihe nach einer endlichen Anzahl von Schritten auch die Zahl Null auftauchen, und wenn τ in ihr die letzte von Null verschiedene Zahl ist, so ergibt sich:

$$(\alpha, \beta) \sim (\tau, 0),$$

woraus wie oben folgt, daß je zwei Zahlen α, β in $\mathfrak{o}$, deren letzte nicht verschwindet, einen größten gemeinsamen Teiler τ in $\mathfrak{o}$ besitzen, was auch durch

$$\mathfrak{o}\alpha + \mathfrak{o}\beta = \mathfrak{o}\tau$$

ausgedrückt werden kann; mithin ist (§ 178, XII, S. 559) jedes Ideal des Körpers Ω ein Hauptideal, d. h. Ω ist einklassig, w. z. b. w.

Erläuterungen zur vorstehenden Abhandlung.

Das hier gegebene Kriterium ist erst in neuester Zeit — im Rahmen allgemeinerer Untersuchungen — wiedergefunden worden: H. Hasse, Über eindeutige Zerlegung in Primelemente oder in Primhauptideale in Integritätsbereichen. J. f. M. **159** (1928), S. 3—12. Die Zitate beziehen sich auf die 4. Auflage von Dirichlet-Dedekind; der Satz selbst liegt aber viel weiter zurück, wie eine nicht druckfertige, sehr alte Ausarbeitung zeigt.

Noether.

XXXIX.

Konstruktion von Quaternionkörpern.

Der in dem Quaternionkörper Ω enthaltene biquadratische Körper sei H; man kann dann

$$\Omega = H(\omega), \quad \omega^2 = \mu$$

setzen, wo μ eine ganze Zahl in H bedeutet. Jede Zahl in Ω ist von der Form $x + y\omega$, wo x, y in H enthalten; soll das Quadrat $(x + y\omega)^2 = (x^2 + \mu y^2) + 2xy\omega$ in H enthalten sein, so muß $xy = 0$ sein, also $x = 0$, falls $x + y\omega$ nicht in H enthalten (also nicht $y = 0$) ist.

Bezeichnet man die Quaterniongruppe Q des Körpers Ω mit 1, α, β, γ, ε, $\varepsilon\alpha$, $\varepsilon\beta$, $\varepsilon\gamma$, wo

$$\begin{gathered}
\varepsilon^2 = 1, \\
\varepsilon = \alpha^2 = \beta^2 = \gamma^2 = \alpha^{-2} = \beta^{-2} = \gamma^{-2}, \\
\beta\gamma = \alpha, \quad \gamma\alpha = \beta, \quad \alpha\beta = \gamma, \\
\gamma\beta = \alpha^{-1} = \varepsilon\alpha, \quad \alpha\gamma = \beta^{-1} = \varepsilon\beta, \quad \beta\alpha = \gamma^{-1} = \varepsilon\gamma,
\end{gathered}$$

so liegt $(\omega\alpha)^2 = \mu\alpha$ in H, und da $\omega\alpha$ in Ω, aber nicht in H enthalten ist, so kann man

$$\omega\alpha = u\omega$$

und entsprechend

$$\begin{aligned}
\omega\beta &= v\omega, \\
\omega\gamma &= w\omega
\end{aligned}$$

setzen, wo u, v, w Zahlen in H sind. Sodann ist

$$\omega\varepsilon = -\omega, \quad \mu\varepsilon = \mu,$$

also

$$\begin{aligned}
\omega\alpha^2 &= \omega\varepsilon &&= -\omega &&= \omega u(u\alpha), \\
\omega\beta\alpha &= \omega\varepsilon\gamma &&= -\omega w &&= \omega u(v\alpha), \\
\omega\gamma\alpha &= \omega\beta &&= \omega v &&= \omega u(w\alpha),
\end{aligned}$$

und entsprechend ergibt sich

$$\begin{aligned} \omega w &= \omega v\ (u\beta), & -\omega v &= \omega w\ (u\gamma),\\ -\omega &= \omega v\ (v\beta), & \omega u &= \omega w\ (v\gamma),\\ -\omega u &= \omega v\ (w\beta), & -\omega &= \omega w\ (w\gamma), \end{aligned}$$

folglich

$$(1)\quad \begin{cases} u\alpha = -u^{-1}, & u\beta = wv^{-1}, & u\gamma = -vw^{-1},\\ v\alpha = -wu^{-1}, & v\beta = -v^{-1}, & v\gamma = uw^{-1},\\ w\alpha = vu^{-1}, & w\beta = -uv^{-1}, & w\gamma = -w^{-1}; \end{cases}$$

$$\mu\alpha = \mu u^2, \qquad \mu\beta = \mu v^2, \qquad \mu\gamma = \mu w^2.$$

Ist H insbesondere einklassig, so kann man μ als eine durch kein Primzahlquadrat in H teilbare ganze Zahl in H annehmen. Dann sind auch $\mu\alpha$, $\mu\beta$, $\mu\gamma$ durch kein Primzahlquadrat teilbar, und somit müssen u, v, w Einheiten sein. Ist daher π eine in μ aufgehende Primzahl in H, so müssen auch $\pi\alpha$, $\pi\beta$, $\pi\gamma$ in μ aufgehen; bedeutet p die durch π teilbare natürliche Primzahl, so muß daher, wenn p durch kein Primzahlquadrat in H teilbar ist, also p nicht in der Grundzahl von H aufgeht, die Zahl μ durch das Produkt p aller verschiedenen in p aufgehenden Primzahlen π teilbar sein. Die Zahl μ ist also das Produkt aus einer natürlichen Zahl m, einer Einheit und möglicherweise noch einer oder mehreren voneinander verschiedenen in der Grundzahl aufgehenden Primzahlen in H; dabei ist m ein Produkt von lauter voneinander und von den Primteilern der Grundzahl verschiedenen natürlichen Primzahlen.

Beispielsweise sei H der einklassige Körper $R(\sqrt{2}, \sqrt{3}, \sqrt{6})$, wo R den Körper der rationalen Zahlen bedeutet; μ sei wiederum eine durch kein Primzahlquadrat in H teilbare ganze Zahl in H. Die Grundzahl (48^2) von H setzt sich aus den Primfaktoren 2 und 3 zusammen. Dabei ist 3 das Quadrat der Primzahl $\sqrt{3}$ in H, und 2 ist bis auf eine Einheit als Faktor die vierte Potenz der Primzahl

$$1 + \eta = 1 + \frac{1+\sqrt{3}}{\sqrt{2}} = \frac{1+\sqrt{2}+\sqrt{3}}{\sqrt{2}}$$

in H. Die Fundamentaleinheiten in H sind ferner

$$\alpha = 1 + \sqrt{2}, \quad \eta = \frac{1+\sqrt{3}}{\sqrt{2}} = \sqrt{b} = \sqrt{2+\sqrt{3}},$$

$$\tau = \sqrt{2} + \sqrt{3} = \sqrt{c} = \sqrt{5+2\sqrt{6}}.$$

Also kann man setzen

$$\mu = \pm m a^{e_1} \eta^{e_2} \tau^{e_3} (1+\eta)^{e_4} (\sqrt{3})^{e_5},$$

wo m eine durch kein Primzahlquadrat teilbare natürliche Zahl und relative Primzahl zu 6 ist und jede der Zahlen e_1, e_2, e_3, e_4, e_5 gleich 0 oder 1 ist.

Man kann jetzt setzen

$$(\sqrt{2}, \sqrt{3}, \sqrt{6}, \omega)\ \alpha = (\ \sqrt{2}, -\sqrt{3}, -\sqrt{6}, u\omega),$$
$$(\sqrt{2}, \sqrt{3}, \sqrt{6}, \omega)\ \beta = (-\sqrt{2}, \sqrt{3}, -\sqrt{6}, v\omega), \quad \omega\varepsilon = -\omega, \mu\varepsilon = \mu.$$
$$(\sqrt{2}, \sqrt{3}, \sqrt{6}, \omega)\ \gamma = (-\sqrt{2}, -\sqrt{3}, \sqrt{6}, w\omega),$$

Dann ist

$$\begin{aligned} a\alpha &= a, & a\beta &= -a^{-1}, & a\gamma &= -a^{-1}, \\ \eta\alpha &= -\eta^{-1}, & \eta\beta &= -\eta, & \eta\gamma &= \eta^{-1}, \\ \tau\alpha &= -\tau^{-1}, & \tau\beta &= \tau^{-1}, & \tau\gamma &= -\tau, \end{aligned}$$

$(1+\eta)\alpha = -\eta^{-1}(1-\eta)$, $(1+\eta)\beta = 1-\eta$, $(1+\eta)\gamma = \eta^{-1}(1+\eta)$,

also, da man leicht

$$\frac{1-\eta}{1+\eta} = -\tau^{-1}$$

bestätigt,

$$(1+\eta)\alpha = (1+\eta)\eta^{-1}\tau^{-1}, \quad (1+\eta)\beta = -(1+\eta)\tau^{-1},$$
$$(1+\eta)\gamma = (1+\eta)\eta^{-1},$$

endlich

$$(\sqrt{3})\alpha = -\sqrt{3}, \quad (\sqrt{3})\beta = \sqrt{3}, \quad (\sqrt{3})\gamma = -\sqrt{3}.$$

Also ist

$$\mu\alpha = \pm m a^{e_1} (-\eta^{-1})^{e_2} (-\tau^{-1})^{e_3} (1+\eta)^{e_4} \eta^{-e_4} \tau^{-e_4} (-\sqrt{3})^{e_5}$$
$$= \pm m a^{e_1} (-1)^{e_2+e_3+e_5} \eta^{-e_2-e_4} \tau^{-e_3-e_4} (1+\eta)^{e_4} (\sqrt{3})^{e_5},$$

$$\frac{\mu\alpha}{\mu} = (-1)^{e_2+e_3+e_5} \eta^{-2e_2-e_4} \tau^{-2e_3-e_4} = u^2,$$

also

$$e_4 = 0, \quad e_2 + e_3 + e_5 \equiv 0 \pmod 2, \quad u = (\pm)'\ \eta^{-e_2} \tau^{-e_3},$$
$$\mu = \pm m a^{e_1} \eta^{e_2} \tau^{e_3} (\sqrt{3})^{e_5}.$$

Hieraus ergibt sich weiter

$$\mu\beta = \pm m (-a^{-1})^{e_1} (-\eta)^{e_2} \tau^{-e_3} (\sqrt{3})^{e_5},$$
$$\frac{\mu\beta}{\mu} = (-1)^{e_1+e_2} a^{-2e_1} \tau^{-2e_3} = v^2,$$

also

$$e_1 + e_2 \equiv 0 \pmod 2, \quad e_1 = e_2, \quad v = (\pm)'' a^{-e_1} \tau^{-e_3},$$
$$\mu = \pm m a^{e_1} \eta^{e_1} \tau^{e_3} (\sqrt{3})^{e_5}$$

und mit Rücksicht auf das Obige auch

$$u = (\pm)' \eta^{-e_1} \tau^{-e_3},$$
$$e_1 + e_3 + e_5 \equiv 0 \pmod 2.$$

Unter Benutzung von (1) erhält man weiter

$$u\alpha = (\pm)' (-\eta^{-1})^{-e_1} (-\tau^{-1})^{-e_3} = (\pm)' (-1)^{e_1+e_3} \eta^{e_1} \tau^{e_3}$$
$$= -u^{-1} = -(\pm)' \eta^{e_1} \tau^{e_3},$$

also

$$(-1)^{e_1+e_3} = -1, \quad e_1 + e_3 \equiv 1 \pmod 2;$$

also ist

$$e_5 = 1,$$
$$\mu = \pm m a^{e_1} \eta^{e_1} \tau^{e_3} \sqrt{3}$$

und entweder $e_1 = 0$, $e_3 = 1$ oder $e_1 = 1$, $e_3 = 0$. In ähnlicher Weise ergibt sich

$$v\beta = (\pm)'' (-a^{-1})^{-e_1} \tau^{e_3} = (\pm)'' (-1)^{e_1} a^{e_1} \tau^{e_3}$$
$$= -v^{-1} = -(\pm)'' a^{e_1} \tau^{e_3},$$

also

$$(-1)^{e_1} = -1, \quad e_1 = 1, \quad e_3 = 0,$$
$$\mu = \pm m a \eta \sqrt{3}. \tag{2}$$

Mein erstes Beispiel (1886) war

$$\mu = (1 + \sqrt{2})(\sqrt{2} + \sqrt{3})\sqrt{2}\sqrt{3} = a\tau\sqrt{2}\sqrt{3}.$$

Diese Zahl hat nicht die Gestalt (2); das erklärt sich daraus, daß μ oben als durch kein Primzahlquadrat teilbar vorausgesetzt wurde. In der Tat unterscheidet sich μ von der unter (2) fallenden Zahl $a\eta\sqrt{3}$ nur durch den Faktor

$$\frac{\tau\sqrt{2}}{\eta} = \frac{2(\sqrt{2} + \sqrt{3})}{1 + \sqrt{3}},$$

der das Quadrat der Zahl $1 - \dfrac{1 - \sqrt{3}}{\sqrt{2}}$ in H ist.

Ist umgekehrt μ von der Gestalt (2), wo m eine beliebige durch kein Primzahlquadrat teilbare und zu 6 teilerfremde natürliche Zahl ist, und ist $\omega^2 = \mu$, so erzeugt ω über dem Körper H einen Quaternionkörper. Das erkennt man folgendermaßen:

Man bezeichne mit α, β, γ drei Permutationen des Körpers $\Omega = H(\omega)$, welche die auf den biquadratischen Körper $R(\sqrt{2}, \sqrt{3})$ bezüglichen Eigenschaften

$$(3)\qquad \begin{cases} (\sqrt{2}, \sqrt{3}, \sqrt{6})\,\alpha = (\ \sqrt{2}, -\sqrt{3}, -\sqrt{6}), \\ (\sqrt{2}, \sqrt{3}, \sqrt{6})\,\beta = (-\sqrt{2}, \ \sqrt{3}, -\sqrt{6}), \\ (\sqrt{2}, \sqrt{3}, \sqrt{6})\,\gamma = (-\sqrt{2}, -\sqrt{3}, \ \sqrt{6}) \end{cases}$$

besitzen [solcher Permutationen α, β, γ gibt es je eine oder je zwei, je nachdem der noch unbekannte Grad von Ω gleich 4 oder 8 ist, da zu jeder Permutation des biquadratischen Körpers $R(\sqrt{2}, \sqrt{3})$ genau eine bzw. zwei Permutationen von Ω als Multipla gehören]; die identische Permutation von Ω sei 1. Nun ist

$$\omega^2\alpha = \pm m(1+\sqrt{2})\,\frac{1-\sqrt{3}}{\sqrt{2}}(-\sqrt{3}) = \omega^2\left(\frac{1-\sqrt{3}}{\sqrt{2}}\right)^2,$$

$$\omega^2\beta = \pm m(1-\sqrt{2})\,\frac{1+\sqrt{3}}{-\sqrt{2}}\ \sqrt{3}\ = \omega^2(1-\sqrt{2})^2,$$

$$\omega^2\gamma = \pm m(1-\sqrt{2})\,\frac{1-\sqrt{3}}{-\sqrt{2}}(-\sqrt{3}) = \omega^2(1-\sqrt{2})^2\left(\frac{1-\sqrt{3}}{\sqrt{2}}\right)^2,$$

mithin

$$(4)\qquad \begin{cases} \omega\alpha = \omega\,\dfrac{1-\sqrt{3}}{\sqrt{2}}\cdot e_1, \\ \omega\beta = \omega(1-\sqrt{2})\cdot e_2, \qquad\qquad (e_1^2 = e_2^2 = e_3^2 = 1). \\ \omega\gamma = \omega(1-\sqrt{2})\,\dfrac{1-\sqrt{3}}{\sqrt{2}}\cdot e_3 \end{cases}$$

Hieraus folgt weiter

$$(5)\qquad \begin{cases} \omega\alpha^2 = \omega\,\dfrac{1-\sqrt{3}}{\sqrt{2}}\,e_1\cdot\dfrac{1+\sqrt{3}}{\sqrt{2}}\,e_1 = -\omega, \\ \omega\beta^2 = \omega(1-\sqrt{2})\,e_2\cdot(1+\sqrt{2})\,e_2 = -\omega, \\ \omega\gamma^2 = \omega(1-\sqrt{2})\,\dfrac{1-\sqrt{3}}{\sqrt{2}}\,e_3\cdot(1+\sqrt{2})\,\dfrac{1+\sqrt{3}}{-\sqrt{2}}\,e_3 = -\omega, \end{cases}$$

also

$$(6)\quad (\sqrt{2}, \sqrt{3}, \omega)\,\alpha^2 = (\sqrt{2}, \sqrt{3}, \omega)\,\beta^2 = (\sqrt{2}, \sqrt{3}, \omega)\,\gamma^2 = (\sqrt{2}, \sqrt{3}, -\omega).$$

Man kann also setzen

$$\alpha^2 = \beta^2 = \gamma^2 = \varepsilon. \tag{7}$$

Aus (5) oder (6) geht hervor, daß ω nicht in $R(\sqrt{2}, \sqrt{3})$ enthalten ist, weil sonst zufolge $(\sqrt{2}, \sqrt{3})\,\alpha^2 = (\sqrt{2}, \sqrt{3})$ auch $\omega\,\alpha^2$ gleich ω sein müßte; mithin ist $R(\sqrt{2}, \sqrt{3}, \omega)$ vom Grade 8, und da derselbe durch fünf verschiedene Permutationen 1, α, β, γ, ε in sich selbst übergeht, so muß dasselbe auch für seine übrigen drei Permutationen gelten; mithin ist er ein Normalkörper. Aus (5) und (4) folgt weiter

$$\omega\,\alpha^3 = -\omega\,\alpha = -\omega\,\frac{1-\sqrt{3}}{\sqrt{2}}\,e_1,$$
$$\omega\,\beta^3 = -\omega\,\beta = -\omega(1-\sqrt{2})\,e_2,$$
$$\omega\,\gamma^3 = -\omega\,\gamma = -\omega(1-\sqrt{2})\,\frac{1-\sqrt{3}}{\sqrt{2}}\,e_3;$$

vergleicht man mit (4) und bedenkt, daß α^3, β^3, γ^3 auf den Körper $R(\sqrt{2}, \sqrt{3})$ genau so wirken wie α, β, γ in (3), so dürfen wir offenbar $e_1 = e_2 = e_3 = -1$ annehmen, wodurch

$$\omega\,\alpha = -\omega\,\frac{1-\sqrt{3}}{\sqrt{2}},\quad \omega\,\beta = -\omega(1-\sqrt{2}),\quad \omega\,\gamma = -\omega(1-\sqrt{2})\,\frac{1-\sqrt{3}}{\sqrt{2}},$$

$$\omega\,\alpha^3 = \omega\,\frac{1-\sqrt{3}}{\sqrt{2}},\quad \omega\,\beta^3 = \omega(1-\sqrt{2}),\quad \omega\,\gamma^3 = \omega(1-\sqrt{2})\,\frac{1-\sqrt{3}}{\sqrt{2}}$$

wird. Zufolge (7) ist ferner

$$\alpha^3 = \varepsilon\,\alpha = \alpha\,\varepsilon = \alpha_1,\quad \beta^3 = \varepsilon\,\beta = \beta\,\varepsilon = \beta_1,\quad \gamma^3 = \varepsilon\,\gamma = \gamma\,\varepsilon = \gamma_1,$$

$$(\sqrt{2}, \sqrt{3}, \omega)\,\alpha_1 = (\sqrt{2}, \sqrt{3}, \omega)\,\varepsilon\,\alpha = (\sqrt{2}, \sqrt{3}, -\omega)\,\alpha = (\sqrt{2}, -\sqrt{3}, -\omega\alpha),$$
$$(\sqrt{2}, \sqrt{3}, \omega)\,\beta_1 = (\sqrt{2}, \sqrt{3}, \omega)\,\varepsilon\,\beta = (\sqrt{2}, \sqrt{3}, -\omega)\,\beta = (-\sqrt{2}, \sqrt{3}, -\omega\beta),$$
$$(\sqrt{2}, \sqrt{3}, \omega)\,\gamma_1 = (\sqrt{2}, \sqrt{3}, \omega)\,\varepsilon\,\gamma = (\sqrt{2}, \sqrt{3}, -\omega)\,\gamma = (-\sqrt{2}, -\sqrt{3}, -\omega\gamma),$$

und da

$$(\sqrt{2}, \sqrt{3}, \omega)\,\varepsilon^2 = (\sqrt{2}, \sqrt{3}, -\omega)\,\varepsilon = (\sqrt{2}, \sqrt{3}, \omega),$$

so ist

$$\varepsilon^2 = 1 = \alpha^4 = \beta^4 = \gamma^4 = \alpha_1^4 = \beta_1^4 = \gamma_1^4;$$
$$\alpha_1^2 = \beta_1^2 = \gamma_1^2 = \varepsilon;$$
$$\alpha_1^3 = \alpha,\ \beta_1^3 = \beta,\ \gamma_1^3 = \gamma.$$

Ferner ist

$$\omega\beta\gamma = [-\omega(1-\sqrt{2})]\gamma = \omega(1-\sqrt{2})\frac{1-\sqrt{3}}{\sqrt{2}}\cdot(1+\sqrt{2})$$

$$= -\omega\frac{1-\sqrt{3}}{\sqrt{2}} = \omega\alpha, (\sqrt{2},\sqrt{3})\beta\gamma = (-\sqrt{2},\sqrt{3})\gamma = (\sqrt{2},-\sqrt{3})$$

$$= (\sqrt{2},\sqrt{3})\alpha;$$

$$\omega\gamma\alpha = \left[-\omega(1-\sqrt{2})\frac{1-\sqrt{3}}{\sqrt{2}}\right]\alpha = \omega\frac{1-\sqrt{3}}{\sqrt{2}}\cdot(1-\sqrt{2})\frac{1+\sqrt{3}}{\sqrt{2}}$$

$$= -\omega(1-\sqrt{2}) = \omega\beta, (\sqrt{2},\sqrt{3})\gamma\alpha = (-\sqrt{2},-\sqrt{3})\alpha$$

$$= (-\sqrt{2},\sqrt{3}) = (\sqrt{2},\sqrt{3})\beta;$$

$$\omega\alpha\beta = \left(-\omega\frac{1-\sqrt{3}}{\sqrt{2}}\right)\beta = \omega(1-\sqrt{2})\cdot\frac{1-\sqrt{3}}{-\sqrt{2}} = \omega\gamma,$$

$$(\sqrt{2},\sqrt{3})\alpha\beta = (\sqrt{2},-\sqrt{3})\beta = (-\sqrt{2},-\sqrt{3}) = (\sqrt{2},\sqrt{3})\gamma.$$

Daraus ergeben sich die drei ersten der sechs folgenden Gleichungen:

$$\beta\gamma = \alpha\,, \quad \gamma\alpha = \beta\,, \quad \alpha\beta = \gamma\,,$$
$$\gamma\beta = \alpha_1, \quad \alpha\gamma = \beta_1, \quad \beta\alpha = \gamma_1,$$

aus denen die übrigen und das Schema der Komposition folgen.

Notwendige und hinreichende Bedingung bei allgemeinem biquadratischem Unterkörper.

Über dem Körper $H = R(\sqrt{a},\sqrt{b})$, wo a und b relative Primzahlen, voneinander und von 1 verschieden und durch kein Primzahlquadrat teilbar sind, sei ein Quaternionkörper $\Omega = H(\omega)$ errichtet. Sind α, β, γ, ε Permutationen dieses Körpers mit den Eigenschaften

$$\varepsilon^2 = 1,$$
$$\alpha^2 = \beta^2 = \gamma^2 = \varepsilon,$$
$$\beta\gamma = \alpha, \quad \gamma\alpha = \beta, \quad \alpha\beta = \gamma,$$

so liegen die Zahlen

$$\omega(\omega\alpha) = u, \quad \omega(\omega\beta) = v, \quad \omega(\omega\gamma) = w$$

in H*), und es ist

$$\omega\varepsilon = -\omega,$$
$$\omega(\omega\alpha) = u = -u\alpha, \quad (\omega\beta)(\omega\gamma) = u\beta = -u\gamma;$$
$$\omega(\omega\beta) = v = -v\beta, \quad (\omega\gamma)(\omega\alpha) = v\gamma = -v\alpha;$$
$$\omega(\omega\gamma) = w = -w\gamma, \quad (\omega\alpha)(\omega\beta) = w\alpha = -w\beta.$$

*) [Vgl. den Anfang.]

Bezeichnet man $\omega(\omega\alpha)(\omega\beta)(\omega\gamma)$ mit h, so ist

$$\omega(\omega\alpha)(\omega\beta)(\omega\gamma) = u(u\beta) = v(v\gamma) = w(w\alpha) = h,$$

$$\omega^2 = \frac{uvw}{h}.$$

Man kann annehmen, es sei

$$(\sqrt{a}, \sqrt{b}, \sqrt{a}\sqrt{b})\,\alpha = (\quad \sqrt{a}, -\sqrt{b}, -\sqrt{a}\sqrt{b}),$$
$$(\sqrt{a}, \sqrt{b}, \sqrt{a}\sqrt{b})\,\beta = (-\sqrt{a}, \quad \sqrt{b}, -\sqrt{a}\sqrt{b}),$$
$$(\sqrt{a}, \sqrt{b}, \sqrt{a}\sqrt{b})\,\gamma = (-\sqrt{a}, -\sqrt{b}, \quad \sqrt{a}\sqrt{b}).$$

Man setze nun

$$u = q + x\sqrt{a} + y\sqrt{b} + z\sqrt{a}\sqrt{b}$$

mit rationalen q, x, y, z. Dann ist

$$u\alpha = q + x\sqrt{a} - y\sqrt{b} - z\sqrt{a}\sqrt{b},$$

und wegen $u = -u\alpha$ muß

$$u = (y + z\sqrt{a})\sqrt{b}, \quad u\beta = (y - z\sqrt{a})\sqrt{b}$$

sein. In entsprechender Weise ergibt sich

$$v = (y_1 + z_1\sqrt{b})\sqrt{a}, \quad v\gamma = -(y_1 - z_1\sqrt{b})\sqrt{a},$$
$$w = y_2\sqrt{a} + z_2\sqrt{b}, \quad w\alpha = y_2\sqrt{a} - z_2\sqrt{b}$$

mit rationalen y_1, z_1, y_2, z_2, also

$$h = b(y^2 - az^2) = -a(y_1^2 - bz_1^2) = ay_2^2 - bz_2^2.$$

Man kann voraussetzen, daß y, z, y_1, z_1, y_2, z_2 ganze rationale Zahlen sind, da man sonst ω nur mit einer passenden natürlichen Zahl zu multiplizieren braucht. Wegen der über a und b getroffenen Voraussetzungen kann man also setzen

$$y = ar, \quad y_1 = bs, \quad y_2 = bt, \quad z_2 = ap$$

mit ganzen rationalen r, s, t, p. Es folgt

$$\frac{h}{ab} = ar^2 - z^2 = z_1^2 - bs^2 = bt^2 - ap^2\ *).$$

*) [Die Bedingung ist auch hinreichend; vgl. die Erläuterung.]

Erläuterungen zur vorstehenden Abhandlung.

Die Arbeit findet sich im Nachlaß in nicht ganz druckfertiger Gestalt. In der wohl ziemlich gleichzeitigen Arbeit „Über Gruppen, deren sämtliche Teiler Normalteiler sind“ (XXVII) ist das Hauptergebnis vorweggenommen, da der dortige Ausdruck

$$\omega^2 = r(2+\sqrt{2})(3+\sqrt{6}) \qquad (r \neq 0 \text{ beliebig rational})$$

sich nur durch einen in $R(\sqrt{2}, \sqrt{3})$ quadratischen Faktor von der Normalform (2) unterscheidet. (Vgl. die Rechnung auf S. 379. Durch einen solchen Faktor unterscheidet sich auch das obige r von dem dortigen m.)

Das Ergebnis, daß jeder Quaternionkörper über $R(\sqrt{2}, \sqrt{3})$ durch die Quadratwurzel eines Ausdrucks (2) erzeugt wird, scheint erst aus späterer Zeit zu stammen. Aber daß die Quadratwurzeln aus den Zahlen (2) Beispiele von Quaternionkörpern ergeben, findet sich schon auf einem von Dedekind mit dem Datum des 15. Februar 1886 versehenen Blatt bewiesen *) (vgl. XXVII, S. 91). Jene Tatsache ergibt sich als Sonderfall einer von Dedekind am vorhergehenden Tage gefundenen, zunächst als notwendig erkannten Bedingung, die sich auf die Unterkörper vierten Grades beliebiger Quaternionkörper bezieht und in einigen diophantischen Gleichungen besteht. Diese Bemerkungen tragen das Datum des 14. Februar 1886 und sind hier am Schluß unter Hinzufügung überleitender Worte wiedergegeben. Die diophantischen Gleichungen sind übrigens auch hinreichend; das ergibt sich unschwer, indem man in den Bezeichnungen von S. 383

$$\omega^2 = \frac{uvw}{h}$$

setzt und die Isomorphismen des durch ω erzeugten Oberkörpers untersucht.

Die in der Erläuterung zu XXVII erwähnte Arbeit von Mertens über denselben Gegenstand geht von der Gleichung und nicht vom Körper aus und beschränkt sich auf die Aufstellung einer notwendigen Bedingung.

W. Weber.

---

*) Die dortige Herleitung ist fast wörtlich, nur mit den erforderlichen Verallgemeinerungen, in diese Arbeit aufgenommen worden, da der betreffende Teil im späteren Manuskript nur angedeutet war.

XL.

Zur Theorie der Ideale (Göttingen 1894). Anwendung auf die Kreiskörper.

Lemma 1. Ist m eine natürliche Zahl, und α eine primitive Wurzel der Gleichung

$$\alpha^m = 1,$$

so ist

$$\alpha - 1 = 0,$$

wenn $m = 1$,

$$(\alpha - 1)^{\varphi(m)} = \varepsilon p,$$

wenn m durch eine und nur eine Primzahl p teilbar ist, und ε eine Einheit bedeutet; $\alpha - 1 = \varepsilon$, wenn m durch mindestens zwei verschiedene Primzahlen teilbar ist.

Beweis. Der erste Fall ist evident. Durchläuft $\alpha' = \alpha^r$ im zweiten Falle alle $\varphi(m)$ primitiven m-ten Einheitswurzeln, und nimmt man $rr' \equiv 1 \pmod{m}$, so sind

$$\frac{\alpha' - 1}{\alpha - 1} = \frac{\alpha^r - 1}{\alpha - 1} \quad \text{und} \quad \frac{\alpha - 1}{\alpha' - 1} = \frac{\alpha'^{r'} - 1}{\alpha' - 1}$$

ganz, also Einheiten, und da

$$\prod(x - \alpha') = \frac{x^m - 1}{x^{\frac{m}{p}} - 1}, \quad \text{also} \quad \prod(1 - \alpha') = p,$$

so folgt das zweite Resultat. Ist endlich $m = pqn$ durch zwei verschiedene Primzahlen p, q teilbar, so ist $\alpha - 1$ gemeinsamer Teiler von $\alpha^{qn} - 1$ und $\alpha^{pn} - 1$, also (nach dem zweiten Fall) gemeinsamer Teiler von p und q, also eine Einheit, w. z. b. w.

Lemma 2. Es sei $\mathfrak{p}$ ein Primideal eines endlichen Körpers Ω, und p die durch $\mathfrak{p}$ teilbare natürliche Primzahl, $N(\mathfrak{p}) = p^f$, wo f der Grad von $\mathfrak{p}$. Ist nun α eine in Ω enthaltene primitive m-te Einheitswurzel, und setzt man $m = m'p'$, wo p' die höchste in m aufgehende Potenz von p ist, so gehört α zum Exponent $m' \pmod{\mathfrak{p}}$.

Beweis. Ist ω relative Primzahl zu $\mathfrak{p}$ in Ω, so ist

$$\omega^{N(\mathfrak{p})-1} \equiv 1 \pmod{\mathfrak{p}},$$

und der Exponent, zu welchem ω gehört (mod. $\mathfrak{p}$), ist die kleinste natürliche Zahl e, welche der Bedingung $\omega^e \equiv 1$ (mod. $\mathfrak{p}$) genügt; dann ist e ein Divisor von $N(\mathfrak{p})-1$, also gewiß unteilbar durch p. Wendet man dies auf den Fall $\omega = \alpha$ an, so folgt aus $\alpha^m = \alpha^{m'p'} = 1 \equiv 1 \pmod{\mathfrak{p}}$, daß e Divisor von $m'p'$, also auch von m' ist. Setzt man nun $m' = ee'$, so ist α^e eine primitive $(e'p')$-te Einheitswurzel, und da $\alpha^e - 1 \equiv 0 \pmod{\mathfrak{p}}$, also keine Einheit ist, so sind (nach Lemma 1) nur zwei Fälle möglich: Entweder ist $e'p' = 1$, also $e' = 1$, $e = m' = m$. Oder $e'p'$ ist durch eine und nur eine Primzahl q teilbar; dann ist $\alpha^e - 1$ (nach Lemma 1) Divisor von q, und da $\alpha^e - 1$, also auch q durch $\mathfrak{p}$ teilbar ist, so muß $q = p$ sein; also ist $e'p'$ Potenz von p, und da e' als Divisor von m' nicht durch p teilbar ist, so muß auch in diesem Falle $e' = 1$, $e = m'$ sein. Also ist in beiden Fällen $e = m'$, w. z. b. w.

Zusatz. Da e Divisor von $N(\mathfrak{p})-1 = p^f - 1$ ist, so folgt $p^f \equiv 1 \pmod{m'}$.

Lemma 3. Es sei wieder α eine primitive m-te Einheitswurzel, und $\Omega = R(\alpha) = K_m$ der durch α erzeugte Körper. Als bekannt wird nur Folgendes vorausgesetzt. Die sämtlichen $\varphi(m)$ primitiven m-ten Einheitswurzeln $\alpha' = \alpha^r$, wo r alle nach m inkongruenten relativen Primzahlen zu m durchläuft, sind die sämtlichen Wurzeln einer Gleichung vom Grade $\varphi(m)$ mit rationalen Koeffizienten (ihre Irreduzibilität soll erst bewiesen, nicht vorausgesetzt werden). Jedenfalls folgt hieraus, daß alle n mit α konjugierten Zahlen unter diesen Zahlen α' zu suchen sind; durch jede der n entsprechenden Permutationen φ' geht α in eine dieser n Zahlen $\alpha\varphi' = \alpha' = \alpha^{r'}$ über, und da $\Omega' = \Omega\varphi' = R(\alpha') = R(\alpha^{r'})$ offenbar ein Divisor von Ω und folglich (!) auch $= \Omega$ ist, so ist Ω ein Normalkörper. Sind φ', φ'' zwei solche Permutationen von Ω, und zwar $\alpha\varphi' = \alpha^{r'}$, $\alpha\varphi'' = \alpha^{r''}$, so folgt $(\alpha\varphi')\,\varphi'' = (\alpha^{r'})\,\varphi'' = (\alpha\varphi'')^{r'} = (\alpha^{r''})^{r'} = \alpha^{r'r''}$, ebenso $(\alpha\varphi'')\,\varphi' = \alpha^{r'r''}$, mithin $\varphi'\varphi'' = \varphi''\varphi'$, d. h. Ω ist ein Abelscher Körper, und die Gruppe Φ aller n Permutationen φ ist eine Abelsche Gruppe. Man kann eine Permutation φ, durch welche α in $\alpha\varphi = \alpha^r$ übergeht, kurz als Permutation r bezeichnen, wo r ein beliebiger Repräsentant der ganzen Zahlenklasse r (mod. m) ist, und die Zu-

sammensetzung der Permutationen φ in der Gruppe Φ entspricht der Multiplikation dieser Zahlenklassen; die identische Permutation entspricht der Zahlenklasse 1 (mod. m). Diese Gruppe Φ ist dann ein Teiler der aus allen $\varphi(m)$ Klassen bestehenden Gruppe, also ihr Grad n ein Divisor von $\varphi(m)$.

Satz: Es ist $n = \varphi(m)$; d. h. die Gleichung, deren Wurzeln die $\varphi(m)$ primitiven m-ten Einheitswurzeln sind, ist irreduzibel; Φ ist die Gruppe aller $\varphi(m)$ Zahlenklassen r (mod. m), deren Elemente r relative Primzahlen zu m sind.

Beweis. Ist p eine natürliche Primzahl, die nicht in m aufgeht, und $\mathfrak{p}$ irgendein in p aufgehendes Primideal des Körpers Ω, so gibt es [zur Theorie der Ideale] in der Gruppe Φ mindestens eine Permutation ψ_0 von der Art, daß jede ganze Zahl ω in Ω der Kongruenz

$$\omega^p \equiv \omega\,\psi_0 \pmod{\mathfrak{p}}$$

genügt. Wendet man dies auf $\omega = \alpha$ an und setzt

$$\alpha\,\psi_0 = \alpha^{p_0},$$

wo p_0 relative Primzahl zu m, durch welche ψ_0 vollständig definiert ist, so folgt

$$\alpha^p \equiv \alpha^{p_0} \pmod{\mathfrak{p}}.$$

Wendet man hierauf das obige Lemma 2 an, so ist $p' = 1$, $m' = m$ zu setzen, also gehört α (mod. $\mathfrak{p}$) zum Exponent m, mithin ist $p_0 \equiv p$ (mod. m), und folglich $\alpha\,\psi_0 = \alpha^{p_0} = \alpha^p$. Es ist daher α^p konjugiert mit α. Ist nun r eine beliebige relative Primzahl zu m, so kann man immer $r \equiv p_1 p_2 p_3 \cdots \pmod{m}$ setzen, wo $p_1, p_2, p_3 \cdots$ natürliche Primzahlen bedeuten; nun gibt es, wie eben gezeigt, immer Permutationen $\varphi_1, \varphi_2, \varphi_3, \cdots$ in der Gruppe Φ, für welche $\alpha\,\varphi_1 = \alpha^{p_1}$, $\alpha\,\varphi_2 = \alpha^{p_2}$, $\alpha\,\varphi_3 = \alpha^{p_3} \cdots$, also auch $\alpha\,\varphi_1\,\varphi_2\,\varphi_3 \cdots = \alpha^{p_1 p_2 p_3 \cdots} = \alpha^r$ wird; mithin ist jede Potenz α^r, d. h. jede primitive m-te Einheitswurzel α' konjugiert mit α, w. z. b. w. (Ähnlichkeit mit meinem Beweise in Crelles Journal Bd. 54).

Erläuterungen zur vorstehenden Abhandlung.

Der hier gegebene Irreduzibilitätsbeweis der Kreisteilungsgleichung beruht auf den beiden Tatsachen:

1. Eine primitive m-te Einheitswurzel bleibt primitiv modulo jedem nicht in m aufgehenden Primideal $\mathfrak{p}$ des Körpers K dieser Einheitswurzeln.

2. Es gibt eine Substitution ψ_0 der Zerlegungsgruppe von $\mathfrak{p}$, für die $\omega\,\psi_0 \equiv \omega^p (\mathfrak{p})$ für jedes ganze ω aus K.

Die vermöge 2. gegebene Zuordnung zwischen Galoisgruppe und Klassengruppe — aus der die Irreduzibilität unmittelbar folgt — ist die Zuordnung im Sinn des allgemeinen Artinschen Reziprozitätsgesetzes, aber in stark abgeschwächter und daher elementarer Form. Denn die Zuordnung geschieht nur zu allen Primzahlen enthaltenden Klassen, also zu einem Erzeugendensystem der Klassengruppe, was zur Festlegung des ganzen Isomorphismus hier ausreicht. Die Frage, ob dieses Erzeugendensystem die Klassengruppe erschöpft, also der Satz von der arithmetischen Progression, bleibt unberührt.

Daß auch die Irreduzibilität der Valenzgleichung in der Theorie der komplexen Multiplikation sich entsprechend beweisen läßt, hat Dedekind an anderer Stelle ohne Beweis-Ausführung bemerkt. Es handelt sich wohl wesentlich um den in Weber, Algebra, Bd. 3, § 122 (2. Auflage) übergegangenen Beweis für die Irreduzibilität der Klassengleichung.

Noether.

XLI.

Gruppencharaktere von Zahlklassen in endlichen Körpern.

Ist $\mathfrak{o}$ das System aller ganzen Zahlen ω des endlichen Körpers Ω, und $\mathfrak{m}$ ein Ideal in $\mathfrak{o}$, so bestehen alle diejenigen Zahlen μ in $\mathfrak{o}$, welche relative Primzahlen zu $\mathfrak{m}$ sind, aus $\varphi(\mathfrak{m})$ Klassen $\mathfrak{m} + \mu$, welche eine Abelsche Gruppe bilden: multipliziert man jede Zahl einer solchen Klasse $\mathfrak{m} + \mu_1$ mit jeder Zahl einer solchen Klasse $\mathfrak{m} + \mu_2$, so gehören alle diese Produkte wieder einer einzigen solchen Klasse $\mathfrak{m} + \mu_1 \mu_2$ an (was man durch $\mathfrak{m} + \mu_1 \mu_2 = (\mathfrak{m} + \mu_1)(\mathfrak{m} + \mu_2)$ bezeichnen könnte). Zunächst einige Hülfssätze*).

Satz 1. Ist ν relative Primzahl zum Ideal $\mathfrak{n}$, so gibt es Zahlen μ, welche relative Primzahlen zum Ideal $\mathfrak{m}$ sind und zugleich die Kongruenz

$$\mu \equiv \nu \pmod{\mathfrak{n}} \tag{1}$$

erfüllen, d. h. in der Klasse $\mathfrak{n} + \nu$ enthalten sind; das System aller dieser Zahlen μ besteht aus $\varphi(\mathfrak{p})$ Klassen $\mathfrak{n}\mathfrak{p} + \mu$, wo $\mathfrak{p}$ das Produkt aller derjenigen in $\mathfrak{m}$ aufgehenden verschiedenen Primideale bedeutet, welche nicht in $\mathfrak{n}$ aufgehen (falls gar kein solches Primideal vorhanden ist, ist $\mathfrak{p} = \mathfrak{o}$ zu setzen).

Beweis. Alle Zahlen π, die relative Primzahlen zu $\mathfrak{p}$ sind, bestehen aus $\varphi(\mathfrak{p})$ Klassen $\mathfrak{p} + \pi$. Soll eine Zahl μ, die der Kongruenz (1) genügt, relative Primzahl zu $\mathfrak{m}$ werden, so ist erforderlich, daß sie auch einer dieser Klassen $\mathfrak{p} + \pi$ angehört, also einer der $\varphi(\mathfrak{p})$ entsprechenden Kongruenzen

$$\mu \equiv \pi \pmod{\mathfrak{p}} \tag{2}$$

genügt; und dies ist auch hinreichend, weil μ zufolge (1) durch kein Primideal teilbar ist, welches sowohl in $\mathfrak{m}$ als in $\mathfrak{n}$ aufgeht. Da

*) Besser gleich von Anfang an: Sind $\mathfrak{m}$, $\mathfrak{n}$ Ideale, ω eine Zahl in $\mathfrak{o}$, so soll mit $(\mathfrak{m}; \mathfrak{n} + \omega)$ das System aller derjenigen in der Klasse $\mathfrak{n} + \omega$ enthaltenen Zahlen bezeichnet werden, welche relative Primzahlen zu $\mathfrak{m}$ sind. — Bedingung der Existenz: $\mathfrak{m} + \mathfrak{n} + \mathfrak{o}\omega = \mathfrak{o}$, d. h. ω relative Primzahl zu $\mathfrak{m} + \mathfrak{n}$.

ferner $\mathfrak{n}$, $\mathfrak{p}$ relative Primideale sind, so liefert die Kongruenz (1) in Verbindung mit je einer der $\varphi(\mathfrak{p})$ Kongruenzen (2) je eine Zahlklasse $\mathfrak{n}\mathfrak{p} + \mu$, und diese $\varphi(\mathfrak{p})$ Klassen sind verschieden voneinander; w. z. b. w.

Zusatz 1. Bedeutet $\mathfrak{m}'$ das kleinste gemeinsame Vielfache der Ideale $\mathfrak{m}$, $\mathfrak{n}$, so ist $\mathfrak{m}'$ auch teilbar durch $\mathfrak{n}\mathfrak{p}$, also auch das kleinste gemeinsame Vielfache von $\mathfrak{m}$, $\mathfrak{n}\mathfrak{p}$; jede Klasse $\mathfrak{n}\mathfrak{p} + \mu$ besteht aus $(\mathfrak{n}\mathfrak{p}, \mathfrak{m}')$ Klassen $\mathfrak{m}' + \mu$, und folglich ist

$$(3) \qquad (\mathfrak{n}\mathfrak{p}, \mathfrak{m}')\,\varphi(\mathfrak{p}) = \frac{N(\mathfrak{m}')\,\varphi(\mathfrak{p})}{N(\mathfrak{n}\mathfrak{p})} = \frac{N(\mathfrak{m}')}{N(\mathfrak{n})} \cdot \frac{\varphi(\mathfrak{p})}{N(\mathfrak{p})}$$

die Anzahl der sämtlichen verschiedenen Klassen $\mathfrak{m}' + \mu$, aus welchen das System der Zahlen μ besteht.

Zusatz 2. Ist $\mathfrak{n}$ ein Teiler von $\mathfrak{m}$, also $\mathfrak{m}' = \mathfrak{m}$, und bedeutet $\mathfrak{q}$ das Produkt aller verschiedenen in $\mathfrak{n}$ aufgehenden, also $\mathfrak{p}\,\mathfrak{q}$ das Produkt aller verschiedenen in $\mathfrak{m}$ aufgehenden Primideale, so ist

$$\varphi(\mathfrak{m}) = N(\mathfrak{m})\frac{\varphi(\mathfrak{p}\,\mathfrak{q})}{N(\mathfrak{p}\,\mathfrak{q})} = N(\mathfrak{m})\frac{\varphi(\mathfrak{p})}{N(\mathfrak{p})} \cdot \frac{\varphi(\mathfrak{q})}{N(\mathfrak{q})},$$

$$\varphi(\mathfrak{n}) = N(\mathfrak{n})\frac{\varphi(\mathfrak{q})}{N(\mathfrak{q})},$$

und folglich ist

$$(4) \qquad \frac{N(\mathfrak{m})}{N(\mathfrak{n})} \cdot \frac{\varphi(\mathfrak{p})}{N(\mathfrak{p})} = \frac{\varphi(\mathfrak{m})}{\varphi(\mathfrak{n})}$$

die Anzahl aller Klassen $\mathfrak{m} + \mu$, aus denen das System der Zahlen μ besteht. [Läßt man ν in (1) die $\varphi(\mathfrak{n})$ verschiedenen Zahlklassen $\mathfrak{n} + \nu$ durchlaufen, welche aus relativen Primzahlen zu $\mathfrak{n}$ bestehen, so erhält man die sämtlichen $\varphi(\mathfrak{m}) = \frac{\varphi(\mathfrak{m})}{\varphi(\mathfrak{n})}\varphi(\mathfrak{n})$ Zahlklassen $\mathfrak{m} + \mu$, welche aus relativen Primzahlen zu $\mathfrak{m}$ bestehen.]

Definition 1. Ist das Ideal $\mathfrak{n}$ ein Divisor des Ideals $\mathfrak{m}$, so soll mit $\binom{\mathfrak{m}}{\mathfrak{n}}$ das System aller derjenigen Zahlen ν bezeichnet werden, welche der Kongruenz

$$(5) \qquad \nu \equiv 1 \pmod{\mathfrak{n}}$$

genügen und zugleich relative Primzahlen zu $\mathfrak{m}$ sind; dasselbe besteht aus $\frac{\varphi(\mathfrak{m})}{\varphi(\mathfrak{n})}$ Klassen $\mathfrak{m} + \nu$, die mit

$$(6) \qquad \mathfrak{m} + \nu_1, \mathfrak{m} + \nu_2 \ldots \mathfrak{m} + \nu_n$$

bezeichnet werden mögen, wenn zur Abkürzung

$$\frac{\varphi(\mathfrak{m})}{\varphi(\mathfrak{n})} = n \tag{7}$$

gesetzt wird. — Das System $\binom{\mathfrak{m}}{0}$ besteht aus allen relativen Primzahlen μ zu $\mathfrak{m}$, nämlich aus $\varphi(\mathfrak{m})$ Klassen $\mathfrak{m} + \mu$; das System $\binom{\mathfrak{m}}{\mathfrak{m}}$ besteht aus der einzigen Klasse $\mathfrak{m} + 1$.

Satz 2. Die n Klassen $\mathfrak{m} + \nu$ des Systems $\binom{\mathfrak{m}}{\mathfrak{n}}$ bilden eine Abelsche Gruppe; sind μ, μ' zwei nach $\mathfrak{n}$ kongruente relative Primzahlen zu $\mathfrak{m}$, d. h. also Zahlen in $\binom{\mathfrak{m}}{0}$, so ist

$$\mu' \equiv \mu\nu \pmod{\mathfrak{m}} \tag{8}$$

und umgekehrt.

Beweis. Denn sind ν, ν' Zahlen in $\binom{\mathfrak{m}}{\mathfrak{n}}$, also $\nu \equiv \nu' \equiv 1 \pmod{\mathfrak{n}}$, so ist auch $\nu\nu' \equiv 1 \pmod{\mathfrak{n}}$, und da ν, ν' relative Primzahlen zu $\mathfrak{m}$, d. h. in $\binom{\mathfrak{m}}{0}$ enthalten sind, so ist auch $\nu\nu'$ in $\binom{\mathfrak{m}}{0}$, also auch in $\binom{\mathfrak{m}}{\mathfrak{n}}$ enthalten. Sind ferner μ, μ' Zahlen in $\binom{\mathfrak{m}}{0}$, so gibt es stets eine und nur eine Klasse $\mathfrak{m} + \nu$ in $\binom{\mathfrak{m}}{0}$, welche der Kongruenz (8) und folglich auch der Kongruenz $\mu' \equiv \mu\nu \pmod{\mathfrak{n}}$ genügt; ist nun $\mu' \equiv \mu \pmod{\mathfrak{n}}$, so folgt, weil μ', μ auch in $\binom{\mathfrak{n}}{0}$ enthalten sind, $1 \equiv \nu \pmod{\mathfrak{n}}$, d. h. ν ist in $\binom{\mathfrak{m}}{\mathfrak{n}}$ enthalten. Umgekehrt: genügen drei Zahlen ν, μ, μ' in $\binom{\mathfrak{m}}{0}$ der Kongruenz (8), und ist ν in $\binom{\mathfrak{m}}{\mathfrak{n}}$ enthalten, genügt also der Kongruenz (5), so folgt $\mu' \equiv \mu \pmod{\mathfrak{n}}$. W. z. b. w.

Satz 3. Sind $\mathfrak{a}$, $\mathfrak{b}$ Faktoren des Ideals $\mathfrak{m}$, so ist die Gruppe

$\binom{\mathfrak{m}}{\mathfrak{a} - \mathfrak{b}}$ der größte gem. Divisor

$\binom{\mathfrak{m}}{\mathfrak{a} + \mathfrak{b}}$ das kleinste gem. Multiplum

} der Gruppen $\binom{\mathfrak{m}}{\mathfrak{a}}$, $\binom{\mathfrak{m}}{\mathfrak{b}}$.

Beweis. Das Erstere leicht; denn wenn $\mathfrak{m} + \mu$ eine beiden Gruppen $\binom{\mathfrak{m}}{\mathfrak{a}}$, $\binom{\mathfrak{m}}{\mathfrak{b}}$ gemeinsame Klasse ist, so ist $\mu \equiv 1 \pmod{\mathfrak{a}}$ und $\mu \equiv 1 \pmod{\mathfrak{b}}$, also auch $\mu \equiv 1 \pmod{\mathfrak{a} - \mathfrak{b}}$, d. h. die Klasse $\mathfrak{m} + \mu$ ist in $\binom{\mathfrak{m}}{\mathfrak{a} - \mathfrak{b}}$ enthalten; und umgekehrt, wenn letzteres der Fall, so ist $\mu \equiv 1 \pmod{\mathfrak{a} - \mathfrak{b}}$, also auch $\mu \equiv 1 \pmod{\mathfrak{a}}$ und $\mu \equiv 1 \pmod{\mathfrak{b}}$, d. h. die Klasse $\mathfrak{m} + \mu$ ist beiden Gruppen $\binom{\mathfrak{m}}{\mathfrak{a}}$, $\binom{\mathfrak{m}}{\mathfrak{b}}$ gemeinsam, w. z. b. w. — Das Letztere liegt etwas tiefer. Ist $\boldsymbol{M}$ das kl. gem. Multiplum von $\binom{\mathfrak{m}}{\mathfrak{a}}$, $\binom{\mathfrak{m}}{\mathfrak{b}}$, so sind alle Klassen $\mathfrak{m} + \alpha$ von $\binom{\mathfrak{m}}{\mathfrak{a}}$ und alle Klassen $\mathfrak{m} + \beta$ von $\binom{\mathfrak{m}}{\mathfrak{b}}$, also auch alle Klassen $\mathfrak{m} + \alpha\beta$ in $\boldsymbol{M}$ enthalten, und das System dieser Klassen $\mathfrak{m} + \alpha\beta$, welches eine Gruppe bildet $(\alpha_1\beta_1 \cdot \alpha_2\beta_2 \equiv (\alpha_1\alpha_2)\,(\beta_1\beta_2))$, ist identisch mit $\boldsymbol{M}$. Da nun $\alpha \equiv 1 \pmod{\mathfrak{a}}$ und $\beta \equiv 1 \pmod{\mathfrak{b}}$, so ist auch $\alpha \equiv \beta \equiv \alpha\beta \equiv 1 \pmod{\mathfrak{a} + \mathfrak{b}}$, und folglich sind alle Klassen $\mathfrak{m} + \alpha\beta$ von $\boldsymbol{M}$ in $\binom{\mathfrak{m}}{\mathfrak{a} + \mathfrak{b}}$ enthalten. Umgekehrt, wenn $\mathfrak{m} + \mu$ eine Klasse in $\binom{\mathfrak{m}}{\mathfrak{a} + \mathfrak{b}}$, also $\mu \equiv 1 \pmod{\mathfrak{a} + \mathfrak{b}}$ und relative Primzahl zu $\mathfrak{m}$ ist, so kann man zunächst eine Zahl α_0 bestimmen, welche gleichzeitig den Kongruenzen $\alpha_0 \equiv 1 \pmod{\mathfrak{a}}$, $\alpha_0 \equiv \mu \pmod{\mathfrak{b}}$ genügt [D. § 171, III, alle diese Zahlen α_0 bilden eine Klasse $(\mathfrak{a} - \mathfrak{b}) + \alpha_0$], und zwar wird α_0 relative Primzahl zu $\mathfrak{a}$ und $\mathfrak{b}$, also auch zu $\mathfrak{a} - \mathfrak{b}$; nach Satz 1 gibt es daher auch Zahlen α, welche relative Primzahlen zu $\mathfrak{m}$ sind und der Kongruenz $\alpha \equiv \alpha_0 \pmod{\mathfrak{a} - \mathfrak{b}}$, also auch den Kongruenzen $\alpha \equiv 1 \pmod{\mathfrak{a}}$, $\alpha \equiv \mu \pmod{\mathfrak{b}}$ genügen (nach Zusatz 2 gibt es $\frac{\varphi(\mathfrak{m})}{\varphi(\mathfrak{a} - \mathfrak{b})}$ verschiedene solche Klassen $\mathfrak{m} + \alpha$). Da α relative Primzahl zu $\mathfrak{m}$ (α enthalten in $\binom{\mathfrak{m}}{\mathfrak{a}}$), so kann man β so bestimmen, daß $\alpha\beta \equiv \mu \pmod{\mathfrak{m}}$ wird; weil μ relative Primzahl zu $\mathfrak{m}$, so gilt dasselbe auch von β; da ferner $\alpha \equiv \mu \pmod{\mathfrak{b}}$, so ist $\mu\beta \equiv \mu \pmod{\mathfrak{b}}$, und da μ relative Primzahl zu $\mathfrak{m}$, also auch zu $\mathfrak{b}$, so folgt $\beta \equiv 1 \pmod{\mathfrak{b}}$, d. h. β ist enthalten in $\binom{\mathfrak{m}}{\mathfrak{b}}$. Also ist jede in $\binom{\mathfrak{m}}{\mathfrak{a} + \mathfrak{b}}$ enthaltene Klasse

$\mathfrak{m}+\mu$ von der Form $\mathfrak{m}+\alpha\beta$, wo $\mathfrak{m}+\alpha$ in $\binom{\mathfrak{m}}{\mathfrak{a}}$, $\mathfrak{m}+\beta$ in $\binom{\mathfrak{m}}{\mathfrak{b}}$ enthalten, d. h. jede Klasse $\mathfrak{m}+\mu$ von $\binom{\mathfrak{m}}{\mathfrak{a}+\mathfrak{b}}$ ist in M enthalten. Also $M=\binom{\mathfrak{m}}{\mathfrak{a}+\mathfrak{b}}$, w. z. b. w.

Bemerkung. Der zweite Teil des zweiten Satzes kann auch so bewiesen werden. Nach einem allgemeinen Satze über Abelsche Gruppen A, B, deren gr. gem. Div. D, kl. gem. Multiplum M, ist $ab=\partial m$, wo a, b, ∂, m die Grade (Anzahlen der Elemente) von A, B, D, M bedeuten (D. § 149, S. 396 — 397). Setzt man $A=\binom{\mathfrak{m}}{\mathfrak{a}}$, $B=\binom{\mathfrak{m}}{\mathfrak{b}}$, so ist nach dem ersten Teile

$$D=\binom{\mathfrak{m}}{\mathfrak{a}-\mathfrak{b}},\ \text{also}\ a=\frac{\varphi(\mathfrak{m})}{\varphi(\mathfrak{a})},\quad b=\frac{\varphi(\mathfrak{m})}{\varphi(\mathfrak{b})},\ \partial=\frac{\varphi(\mathfrak{m})}{\varphi(\mathfrak{a}-\mathfrak{b})},$$

also

$$m=\frac{\varphi(\mathfrak{m})\,\varphi(\mathfrak{a}-\mathfrak{b})}{\varphi(\mathfrak{a})\,\varphi(\mathfrak{b})}=\frac{\varphi(\mathfrak{m})}{\varphi(\mathfrak{a}+\mathfrak{b})}$$

[weil allgemein $\varphi(\mathfrak{a})\,\varphi(\mathfrak{b})=\varphi(\mathfrak{a}-\mathfrak{b})\,\varphi(\mathfrak{a}+\mathfrak{b})$ ist, leicht zu zeigen*)]. Da nun im ersten Teile des Beweises des zweiten Satzes schon gezeigt ist, daß M in $\binom{\mathfrak{m}}{\mathfrak{a}+\mathfrak{b}}$ enthalten, so muß, weil M denselben Grad $m=\frac{\varphi(\mathfrak{m})}{\varphi(\mathfrak{a}+\mathfrak{b})}$ besitzt wie $\binom{\mathfrak{m}}{\mathfrak{a}+\mathfrak{b}}$, notwendig $M=\binom{\mathfrak{m}}{\mathfrak{a}+\mathfrak{b}}$ sein, w. z. b. w.

Definition 2. Ist die Klassengruppe H ein Divisor von $\binom{\mathfrak{m}}{\mathfrak{o}}$, so betrachte man alle diejenigen Faktoren $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ ... von $\mathfrak{m}$, deren zugehörige Klassengruppen $\binom{\mathfrak{m}}{\mathfrak{a}}$, $\binom{\mathfrak{m}}{\mathfrak{b}}$, $\binom{\mathfrak{m}}{\mathfrak{c}}$... Divisoren von H sind

*) $\mathfrak{p}$ das Produkt aller verschiedenen Primideale, die in $\mathfrak{a}$, nicht in $\mathfrak{b}$,
$\mathfrak{q}$ „ „ „ „ „ „ nicht in $\mathfrak{a}$, aber in $\mathfrak{b}$,
$\mathfrak{r}$ „ „ „ „ „ „ in $\mathfrak{a}$ und in $\mathfrak{b}$
aufgehen; so ist $\varphi(\mathfrak{a})=N(\mathfrak{a})\frac{\varphi(\mathfrak{p}\mathfrak{r})}{N(\mathfrak{p}\mathfrak{r})}=N(\mathfrak{a})\frac{\varphi(\mathfrak{p})}{N(\mathfrak{p})}\cdot\frac{\varphi(\mathfrak{r})}{N(\mathfrak{r})}$,

$$\varphi(\mathfrak{b})=N(\mathfrak{b})\frac{\varphi(\mathfrak{q}\mathfrak{r})}{N(\mathfrak{q}\mathfrak{r})}=N(\mathfrak{b})\frac{\varphi(\mathfrak{q})}{N(\mathfrak{q})}\cdot\frac{\varphi(\mathfrak{r})}{N(\mathfrak{r})},$$

$$\varphi(\mathfrak{a}-\mathfrak{b})=N(\mathfrak{a}-\mathfrak{b})\frac{\varphi(\mathfrak{p}\mathfrak{q}\mathfrak{r})}{N(\mathfrak{p}\mathfrak{q}\mathfrak{r})}=N(\mathfrak{a}-\mathfrak{b})\frac{\varphi(\mathfrak{p})}{N(\mathfrak{p})}\cdot\frac{\varphi(\mathfrak{q})}{N(\mathfrak{q})}\cdot\frac{\varphi(\mathfrak{r})}{N(\mathfrak{r})},$$

$$\varphi(\mathfrak{a}+\mathfrak{b})=N(\mathfrak{a}+\mathfrak{b})\frac{\varphi(\mathfrak{r})}{N(\mathfrak{r})},$$

und da $\mathfrak{a}\mathfrak{b}=(\mathfrak{a}-\mathfrak{b})(\mathfrak{a}+\mathfrak{b})$, also auch $N(\mathfrak{a})\,N(\mathfrak{b})=N(\mathfrak{a}-\mathfrak{b})\,N(\mathfrak{a}+\mathfrak{b})$, so folgt auch $\varphi(\mathfrak{a})\,\varphi(\mathfrak{b})=\varphi(\mathfrak{a}-\mathfrak{b})\,\varphi(\mathfrak{a}+\mathfrak{b})$, w. z. b. w.

(jedenfalls ist $\binom{\mathfrak{m}}{\mathfrak{m}} = \mathfrak{m} + 1$ in der Gruppe H enthalten). Nach dem eben bewiesenen Satze befindet sich unter diesen Idealen $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \ldots$ auch deren größter gemeinsamer Divisor $\mathfrak{n} = \mathfrak{a} + \mathfrak{b} + \mathfrak{c} \ldots$, und offenbar sind $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \ldots$ die sämtlichen Ideale, welche Multipla von $\mathfrak{n}$ und zugleich Divisoren von $\mathfrak{m}$ sind. Dieses Ideal $\mathfrak{n}$ soll der Exponent der Gruppe H heißen. Die charakteristische Eigenschaft desselben besteht hierin:

1. Ist ν relative Primzahl zu $\mathfrak{m}$ und $\equiv 1 \pmod{\mathfrak{n}}$, so ist die Klasse $\mathfrak{m} + \nu$ in H enthalten (d. h. $\binom{\mathfrak{m}}{\mathfrak{n}}$ Divisor von H).

2. Ist $\mathfrak{n}'$ Faktor von $\mathfrak{m}$, aber nicht teilbar durch $\mathfrak{n}$, so gibt es eine Zahl ν', welche der Kongruenz $\nu' \equiv 1 \pmod{\mathfrak{n}'}$ genügt und relative Primzahl zu $\mathfrak{m}$ ist und der Art, daß die Klasse $\mathfrak{m} + \nu'$ nicht in H enthalten ist (d. h. $\binom{\mathfrak{m}}{\mathfrak{n}'}$ nicht Divisor von H).

Oder: $\binom{\mathfrak{m}}{\mathfrak{n}'}$ ist Divisor von H oder nicht, je nachdem $\mathfrak{n}'$ teilbar ist durch $\mathfrak{n}$ oder nicht.

Definition 3. Eine Funktion ψ, welche für jede in $\mathfrak{o}$ enthaltene Zahl ω einen bestimmten endlichen Wert $\psi(\omega)$ besitzt, soll eine Klassenfunktion für das Ideal $\mathfrak{m}$ oder auch periodisch nach $\mathfrak{m}$ heißen, wenn je zwei nach $\mathfrak{m}$ kongruente Zahlen α, β einen und denselben Wert $\psi(\alpha) = \psi(\beta)$ erzeugen, d. h. wenn für jede in $\mathfrak{o}$ enthaltene Zahl ω und jede in $\mathfrak{m}$ enthaltene Zahl μ stets

$$\psi(\omega) = \psi(\omega + \mu) \qquad [\text{Bezeichnung: } \psi(\mathfrak{m} + \omega) = \psi(\omega)]$$

ist; das Ideal $\mathfrak{m}$ heißt eine Periode von ψ.

Offenbar ist jedes Vielfache einer Periode von ψ ebenfalls eine Periode von ψ.

Bemerkung. Man könnte bei dem Begriffe einer Periode $\mathfrak{m}$ von ψ größerer Allgemeinheit wegen davon absehen, daß $\mathfrak{m}$ ein Ideal in $\mathfrak{o}$ sein soll, und lediglich annehmen, daß $\mathfrak{m}$ irgend ein Modul sein soll, mit der einzigen Beschränkung, daß $(\mathfrak{o}, \mathfrak{m}) > 0$, also ψ nur eine endliche Anzahl verschiedener Werte haben soll. Dies würde aber keine wirkliche Erweiterung des obigen Begriffs geben; denn zufolge der letzten Bemerkung würde auch der Modul $\mathfrak{o} - \mathfrak{m}$ als Multiplum von $\mathfrak{m}$, und ebenso das kleinste durch den Modul $\mathfrak{m}$ oder $\mathfrak{o} - \mathfrak{m}$

teilbare Ideal, welches immer $= \frac{\mathfrak{o} - \mathfrak{m}}{\mathfrak{o}}$ ist, ebenfalls eine Periode von ψ sein. Dagegen würde eine Erweiterung des Begriffs dadurch eintreten (?) *), daß die Funktion ψ nicht auf alle Zahlen von $\mathfrak{o}$, sondern nur auf alle Zahlen irgend einer Ordnung wirkt. —

Satz 4. Sind die Ideale $\mathfrak{a}$, $\mathfrak{b}$ Perioden der Funktion ψ, so ist auch ihr größter gemeinsamer Teiler $\mathfrak{a} + \mathfrak{b}$ eine Periode von ψ.

Beweis. Denn wenn ω, α, β beliebige Zahlen in $\mathfrak{o}$, $\mathfrak{a}$, $\mathfrak{b}$ bedeuten, so ist nach der Annahme $\psi(\omega) = \psi(\omega + \alpha)$ und $\psi(\omega) = \psi(\omega + \beta)$; ersetzt man in der letzten Gleichung ω durch $\omega + \alpha$, so folgt $\psi(\omega) = \psi(\omega + \alpha) = \psi(\omega + \alpha + \beta)$, also $\psi(\omega) = \psi(\omega + \delta)$, wo $\delta = \alpha + \beta$ jede Zahl des Ideals $\mathfrak{a} + \mathfrak{b}$ bedeutet, w. z. b. w. —

Hieraus geht hervor, daß der gr. gem. Teiler $\mathfrak{m}$ aller Perioden von ψ ebenfalls eine Periode von ψ ist, und daß folglich alle Perioden von ψ die sämtlichen Vielfachen von $\mathfrak{m}$ sind, welches Ideal die kleinste Periode von ψ heißen soll, weil sie von allen Perioden die kleinste Norm besitzt. (Besser Hauptperiode!)

Definition 4. Eine (nach $\mathfrak{m}$ periodische) Funktion ψ aller in $\mathfrak{o}$ enthaltenen Zahlen soll ein Charakter heißen, wenn für je zwei solche Zahlen ω, ω' das Gesetz

$$\psi(\omega\,\omega') = \psi(\omega)\,\psi(\omega')$$

gilt, und ψ nicht für alle ω verschwindet. —

Satz 5. Ist der Charakter ψ periodisch, und ist $\mathfrak{m}$ seine kleinste Periode, so ist $\psi(\omega)$ dann und nur dann von Null verschieden, und zwar

$$\psi(\omega)^{\varphi(\mathfrak{m})} = 1,$$

wenn ω relative Primzahl zu $\mathfrak{m}$ ist.

Beweis. Da $\omega \cdot 1 = \omega$, also $\psi(\omega)\,\psi(1) = \psi(\omega)$ ist und $\psi(\omega)$ nicht für alle ω verschwindet, so ist

$$\psi(1) = 1.$$

Ist ω relative Primzahl zu $\mathfrak{m}$, also $\omega^{\varphi(\mathfrak{m})} \equiv 1 \,(\mathrm{mod.}\,\mathfrak{m})$, so folgt

$$\psi\{\omega^{\varphi(\mathfrak{m})}\} = \psi(\omega)^{\varphi(\mathfrak{m})} = \psi(1) = 1.$$

Ist aber ω nicht relative Primzahl zu $\mathfrak{m}$, so ist das kleinste gemeinsame Vielfache $\mathfrak{o}\,\omega - \mathfrak{m}$ von $\mathfrak{o}\,\omega$ und $\mathfrak{m}$ von der Form $\omega\,\mathfrak{m}'$, wo das Ideal $\mathfrak{m}'$ ein echter Teiler von $\mathfrak{m}$ $(\mathfrak{m} = \mathfrak{m}'(\mathfrak{o}\,\omega + \mathfrak{m}))$ und folglich keine Periode von ψ ist; es gibt daher zwei nach $\mathfrak{m}'$ kon-

*) [Das Fragezeichen ist später zugefügt.]

gruente Zahlen α, β, welche verschiedene Werte $\psi(\alpha)$, $\psi(\beta)$ erzeugen; da nun $\omega(\alpha - \beta)$ teilbar durch $\omega\mathfrak{m}'$, also auch durch $\mathfrak{m}$ ist, so folgt

$$\omega\alpha \equiv \omega\beta \pmod{\mathfrak{m}}; \quad \psi(\omega\alpha) = \psi(\omega\beta), \quad \psi(\omega)\psi(\alpha) = \psi(\omega)\psi(\beta),$$

mithin

$$\psi(\omega) = 0,$$

w. z. b. w.

Definition 5. Die Anzahl der verschiedenen Charaktere ψ von kleinster Periode $\mathfrak{m}$ soll mit $\varphi'(\mathfrak{m})$ bezeichnet werden. [Besser $\varphi_1(\mathfrak{m})$!]

Zu ihrer Bestimmung dient folgende Betrachtung. Ist ψ ein solcher Charakter, so kann er zugleich aufgefaßt werden als einer der $\varphi(\mathfrak{m})$ Charaktere der Abelschen Gruppe, welche von den $\varphi(\mathfrak{m})$ Klassen $\mathfrak{m} + \varrho$ gebildet wird, die den sämtlichen nach $\mathfrak{m}$ inkongruenten relativen Primzahlen ϱ zu $\mathfrak{m}$ entsprechen; in dem Sinne $\psi(\mathfrak{m} + \varrho) = \psi(\mu + \varrho) = \psi(\varrho)$, $\psi(\mathfrak{m} + \varrho)\psi(\mathfrak{m} + \varrho') = \psi(\mathfrak{m} + \varrho\varrho')$. Umgekehrt, ist ψ ein Charakter dieser Abelschen Gruppe von Klassen $\mathfrak{m} + \varrho$, und setzt man $\psi(\omega) = \psi(\mathfrak{m} + \omega)$ oder $= 0$, je nachdem ω relative Primzahl zu $\mathfrak{m}$ ist oder nicht, so ist $\psi(\omega)$ offenbar eine Funktion von der Periode $\mathfrak{m}$, weil immer $\psi(\omega) = \psi(\omega + \mu)$, und zwar ein Charakter, weil offenbar $\psi(\omega\omega') = \psi(\omega)\psi(\omega')$. Die kleinste Periode $\mathfrak{n}$ dieses Charakters ψ ist notwendig ein Divisor von $\mathfrak{m}$; da nun ein Charakter $\psi(\omega)$ von der kleinsten Periode $\mathfrak{n}$ stets und nur dann verschwindet (nach Satz 5), wenn ω relative Primzahl zu $\mathfrak{n}$ ist, und da andererseits $\psi(\omega)$ nach Definition stets und nur dann verschwindet, wenn ω relative Primzahl zu $\mathfrak{m}$ ist, so deckt sich das System $\binom{\mathfrak{n}}{0}$ aller relativen Primzahlen zu $\mathfrak{n}$ mit dem System $\binom{\mathfrak{m}}{0}$ aller relativen Primzahlen zu $\mathfrak{m}$; setzt man daher $\mathfrak{m} = \mathfrak{p}\mathfrak{m}'$, wo $\mathfrak{p}$ das Produkt aller verschiedenen in $\mathfrak{m}$ aufgehenden Primideale bedeutet (oder $\mathfrak{o}$, falls $\mathfrak{m} = \mathfrak{o}$ ist), so muß $\mathfrak{n} = \mathfrak{p}\mathfrak{n}'$ sein, wo $\mathfrak{n}'$ ein Divisor von $\mathfrak{m}'$. Umgekehrt: ist ψ ein Charakter von kleinster Periode $\mathfrak{n} = \mathfrak{p}\mathfrak{n}'$, wo $\mathfrak{n}'$ irgend ein Divisor von $\mathfrak{m}'$, so ist $\psi(\omega)$ auch ein Charakter von der Periode $\mathfrak{m}$, welcher stets und nur dann von Null verschieden ist, wenn ω relative Primzahl zu $\mathfrak{m}$ ist, und ihm entspricht ein vollständig bestimmter Abelscher Klassencharakter $\psi(\mathfrak{m} + \varrho)$. Mithin verteilen sich die sämtlichen $\varphi(\mathfrak{m})$ Charaktere $\psi(\mathfrak{m} + \varrho)$ in ebenso viele Systeme, als es Divisoren $\mathfrak{n}'$ von $\mathfrak{m}'$ gibt, und da dasjenige System, welches zu $\mathfrak{n}'$ gehört, aus $\varphi'(\mathfrak{p}\mathfrak{n}')$

Individuen besteht, so ergibt sich, daß die über alle $\mathfrak{n}'$ ausgedehnte Summe

$$\sum \varphi'(\mathfrak{p}\mathfrak{n}') = \varphi(\mathfrak{m}) = N(\mathfrak{m})\frac{\varphi(\mathfrak{p})}{N(\mathfrak{p})} = N(\mathfrak{m}')\varphi(\mathfrak{p}),$$

also

$$\sum \frac{\varphi'(\mathfrak{p}\mathfrak{n}')}{\varphi(\mathfrak{p})} = N(\mathfrak{m}')$$

ist. Da dieser Satz für jedes Ideal $\mathfrak{m}'$ gilt, welches nur durch solche Primideale teilbar ist, die in $\mathfrak{p}$ aufgehen, so folgt, wenn man $\mathfrak{m}'$ durch jeden Divisor von $\mathfrak{m}'$ ersetzt, nach bekannten Sätzen

$$\varphi'(\mathfrak{m}) = \varphi(\mathfrak{p})\varphi(\mathfrak{m}') = \varphi(\mathfrak{p})\varphi\left(\frac{\mathfrak{m}}{\mathfrak{p}}\right). \quad \text{Satz 6.}$$

Satz 7. Sind $\mathfrak{m}_1$, $\mathfrak{m}_2$ relative Primideale, so ist

$$\varphi'(\mathfrak{m}_1\mathfrak{m}_2) = \varphi'(\mathfrak{m}_1)\varphi'(\mathfrak{m}_2).$$

Beweis. Denn bedeuten $\mathfrak{p}_1$, $\mathfrak{p}_2$ die Produkte aller verschiedenen, bzw. in $\mathfrak{m}_1$, $\mathfrak{m}_2$ aufgehenden Primideale, so ist $\mathfrak{p}_1\mathfrak{p}_2$ das Produkt aller verschiedenen in $\mathfrak{m}_1\mathfrak{m}_2$ aufgehenden Primideale, also

$$\varphi'(\mathfrak{m}_1\mathfrak{m}_2) = \varphi(\mathfrak{p}_1\mathfrak{p}_2)\varphi\left(\frac{\mathfrak{m}_1\mathfrak{m}_2}{\mathfrak{p}_1\mathfrak{p}_2}\right) = \varphi(\mathfrak{p}_1)\varphi\left(\frac{\mathfrak{m}_1}{\mathfrak{p}_1}\right)\cdot\varphi(\mathfrak{p}_2)\varphi\left(\frac{\mathfrak{m}_2}{\mathfrak{p}_2}\right) = \varphi'(\mathfrak{m}_1)\varphi'(\mathfrak{m}_2),$$

w. z. b. w.

Definition 6. Es bedeute $\Phi'(\mathfrak{m})$ die Anzahl aller verschiedenen Charaktere von der Periode $\mathfrak{m}$, also

$$\Phi'(\mathfrak{m}) = \sum \varphi'(\mathfrak{n}),$$

wo $\mathfrak{n}$ alle Faktoren von $\mathfrak{m}$ durchläuft (weil jeder Charakter von der Periode $\mathfrak{m}$ einen der Faktoren $\mathfrak{n}$ zur kleinsten Periode hat, und umgekehrt).

Satz 8. Sind $\mathfrak{m}_1$, $\mathfrak{m}_2$ relative Primideale, so ist

$$\Phi'(\mathfrak{m}_1\mathfrak{m}_2) = \Phi'(\mathfrak{m}_1)\Phi'(\mathfrak{m}_2).$$

Beweis. Denn jeder Divisor von $\mathfrak{m}_1\mathfrak{m}_2$ läßt sich stets und nur auf eine Weise in die Form $\mathfrak{n}_1\mathfrak{n}_2$ setzen, wo $\mathfrak{n}_1$, $\mathfrak{n}_2$ Faktoren von $\mathfrak{m}_1$, $\mathfrak{m}_2$, und umgekehrt, also

$$\begin{aligned}\Phi'(\mathfrak{m}_1\mathfrak{m}_2) &= \sum \varphi'(\mathfrak{n}_1\mathfrak{n}_2) = \sum \varphi'(\mathfrak{n}_1)\varphi'(\mathfrak{n}_2)\\ &= \sum \varphi'(\mathfrak{n}_1)\sum \varphi'(\mathfrak{n}_2) = \Phi'(\mathfrak{m}_1)\Phi'(\mathfrak{m}_2),\end{aligned}$$

w. z. b. w.

Satz 9. Ist $\mathfrak{m}$ teilbar durch das Primideal $\mathfrak{p}$ und kein anderes, also $= \mathfrak{p}^n$, wo $n \geqq 1$, so ist

$$\Phi'(\mathfrak{m}) = 1 + \varphi(\mathfrak{p}^n) = 1 + \varphi(\mathfrak{m}).$$

Beweis. Denn es ist (nach Satz 6)

$$\begin{aligned}\Phi'(\mathfrak{m}) &= \varphi'(\mathfrak{o}) + \varphi'(\mathfrak{p}) + \varphi'(\mathfrak{p}^2) + \cdots + \varphi'(\mathfrak{p}^n)\\ &= 1 + \varphi(\mathfrak{p}) + \varphi(\mathfrak{p})\varphi(\mathfrak{p}) + \varphi(\mathfrak{p})\varphi(\mathfrak{p}^2) + \cdots + \varphi(\mathfrak{p})\varphi(\mathfrak{p}^{n-1})\\ &= 1 + \varphi(\mathfrak{p})\{\varphi(\mathfrak{o}) + \varphi(\mathfrak{p}) + \cdots + \varphi(\mathfrak{p}^{n-1})\} = 1 + \varphi(\mathfrak{p})N(\mathfrak{p}^{n-1})\\ &= 1 + \varphi(\mathfrak{p}^n).\end{aligned}$$

Satz 10. Ist $\mathfrak{m} = \mathfrak{a}\,\mathfrak{b}\,\mathfrak{c}\ldots$, wo $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}\ldots$ (wirkliche) Potenzen von lauter verschiedenen Primidealen (nicht $= \mathfrak{o}$), so ist

$$\Phi'(\mathfrak{m}) = (1 + \varphi(\mathfrak{a}))(1 + \varphi(\mathfrak{b}))(1 + \varphi(\mathfrak{c}))\ldots$$

Beweis unmittelbar aus (8) und (9).

Gehen wir näher ein auf die Verteilung der $\varphi(\mathfrak{m})$ Charaktere ψ der aus den Klassen $\mathfrak{m} + \varrho$ bestehenden Abelschen Gruppe auf die Faktoren $\mathfrak{n} = \mathfrak{p}\mathfrak{n}'$ von $\mathfrak{m} = \mathfrak{p}\mathfrak{m}'$, wo $\mathfrak{p}$, $\mathfrak{m}'$, $\mathfrak{n}'$ die obige Bedeutung haben. Es sei ψ ein solcher Charakter, und (ψ) die Gruppe aller derjenigen Klassen $\mathfrak{m} + \varrho$, welche der Bedingung

$$\psi(\mathfrak{m} + \varrho) = \psi(\varrho) = 1$$

genügen (aus $\psi(\varrho) = 1$, $\psi(\varrho') = 1$ folgt auch $\psi(\varrho\,\varrho') = 1$). Sind nun $\mathfrak{m} + \alpha$, $\mathfrak{m} + \beta$ irgend zwei Klassen der Gruppe $\binom{\mathfrak{m}}{\mathfrak{o}}$, welche denselben Charakter $\psi(\mathfrak{m} + \alpha) = \psi(\mathfrak{m} + \beta)$ besitzen, so kann man stets eine und nur eine Klasse $\mathfrak{m} + \varrho$ so bestimmen, daß $\alpha\,\varrho \equiv \beta \pmod{\mathfrak{m}}$, also $(\mathfrak{m} + \alpha)(\mathfrak{m} + \varrho) = \mathfrak{m} + \beta$, also $\psi(\mathfrak{m} + \alpha)\psi(\mathfrak{m} + \varrho) = \psi(\mathfrak{m} + \beta) = \psi(\mathfrak{m} + \alpha)$, also $\psi(\mathfrak{m} + \varrho) = 1$ wird; mithin ist $\beta \equiv \alpha\,\varrho$, wo $\mathfrak{m} + \varrho$ der Gruppe (ψ) angehört; und umgekehrt, durchläuft $\mathfrak{m} + \varrho$ alle Klassen der Gruppe (ψ), während α eine feste Klasse, so ist $\psi(\mathfrak{m} + \alpha\,\varrho) = \psi(\mathfrak{m} + \alpha)$. Die Gruppe $\binom{\mathfrak{m}}{\mathfrak{o}}$ besteht aus einer Anzahl von Komplexen von der Form $(\psi)(\mathfrak{m} + \alpha)$; alle und nur die Klassen, welche einem und demselben solchen Komplex angehören, erzeugen einen und denselben Wert des Charakters ψ; die Anzahl der verschiedenen Komplexe $(\psi)(\mathfrak{m} + \alpha)$, aus denen $\binom{\mathfrak{m}}{\mathfrak{o}}$ besteht, ist auch die Anzahl der verschiedenen Werte des Charakters ψ. (Dies ist eine allgemeine Eigenschaft der Charaktere Abelscher Gruppen.) (ψ) heiße die Gruppe des Charakters ψ.

Nun sei $\mathfrak{a}$ der Exponent der Gruppe (ψ) (Definition 2), so soll $\mathfrak{a}$ auch der Exponent des Charakters ψ heißen. Wir betrachten

das System $\binom{\mathfrak{a}}{0}$ aller relativen Primzahlen σ zu $\mathfrak{a}$, welches aus $\varphi(\mathfrak{a})$ Klassen $\mathfrak{a}+\sigma$ besteht. Das System aller der Zahlen, welche eine bestimmte solche Klasse $\mathfrak{a}+\sigma$ mit dem System $\binom{\mathfrak{m}}{0}$ gemein hat, besteht [nach (4) in Zusatz 2] aus $\frac{\varphi(\mathfrak{m})}{\varphi(\mathfrak{a})}$ Klassen $\mathfrak{m}+\mu$. Ein solches System, welches der Klasse $\mathfrak{a}+1$ entspricht, ist die Gruppe $\binom{\mathfrak{m}}{\mathfrak{a}}$, welche ein Divisor der Gruppe (ψ) ist. Und wenn $\mathfrak{m}+\mu$ eine der $\frac{\varphi(\mathfrak{m})}{\varphi(\mathfrak{a})}$ Klassen von $\binom{\mathfrak{m}}{0}$ ist, welche in $\mathfrak{a}+\sigma$ enthalten sind, so ist der Komplex $\binom{\mathfrak{m}}{\mathfrak{a}}(\mathfrak{m}+\mu)$ das System aller dieser Klassen, welche folglich auch in dem Komplex $(\psi)(\mathfrak{m}+\mu)$ enthalten sind; mithin hat der Charakter ψ für alle diese, der Klasse $\mathfrak{a}+\sigma$ entsprechenden Klassen $\mathfrak{m}+\mu$ einen und denselben Wert. Definiert man nun eine Klassenfunktion $\psi'(\mathfrak{a}+\sigma)$ so, daß $\psi'(\mathfrak{a}+\sigma)=\psi(\mathfrak{m}+\mu)$ wird, so ist ψ' für jede Klasse $\mathfrak{a}+\sigma$ eindeutig bestimmt, und zwar ist ψ' ein Charakter der Abelschen Gruppe $\binom{\mathfrak{a}}{0}$, welche aus diesen $\varphi(\mathfrak{a})$ Klassen $\mathfrak{a}+\sigma$ besteht. Denn wenn $\mathfrak{a}+\sigma_1$, $\mathfrak{a}+\sigma_2$ irgend zwei Klassen in $\binom{\mathfrak{a}}{0}$ bedeuten, und wenn $\mathfrak{m}+\mu_1$, $\mathfrak{m}+\mu_2$ irgend zwei bzw. in ihnen enthaltene Klassen von $\binom{\mathfrak{m}}{0}$ bedeuten, so ist das Produkt der letzteren $(\mathfrak{m}+\mu_1)(\mathfrak{m}+\mu_2)=\mathfrak{m}+\mu_1\mu_2$ in dem Produkte $(\mathfrak{a}+\sigma_1)(\mathfrak{a}+\sigma_2)=\mathfrak{a}+\sigma_1\sigma_2$ enthalten; da nun $\psi'(\mathfrak{a}+\sigma_1)=\psi(\mathfrak{m}+\mu_1)$, und $\psi'(\mathfrak{a}+\sigma_2)=\psi(\mathfrak{m}+\mu_2)$ ist, so folgt $\psi'(\mathfrak{a}+\sigma_1)\,\psi'(\mathfrak{a}+\sigma_2)=\psi(\mathfrak{m}+\mu_1)\,\psi(\mathfrak{m}+\mu_2)=\psi(\mathfrak{m}+\mu_1\mu_2)=\psi'(\mathfrak{a}+\sigma_1\sigma_2)$, w. z. b. w. Und zwar ist $\mathfrak{a}$ selbst der Exponent dieses Charakters ψ' oder der Gruppe (ψ'). Denn wenn $\mathfrak{b}$ ein echter Faktor von $\mathfrak{a}$ ist, so ist $\binom{\mathfrak{m}}{\mathfrak{b}}$ nicht in der Gruppe (ψ) enthalten (Definition 2), es gibt folglich eine in $\mathfrak{b}+1$ enthaltene Klasse $\mathfrak{m}+\lambda$, welche nicht in (ψ) enthalten ist, woraus folgt, daß $\psi'(\mathfrak{a}+\lambda)=\psi(\mathfrak{m}+\lambda)$ nicht $=1$ ist; mithin ist die in $\mathfrak{b}+1=\mathfrak{b}+\lambda$, also auch in $\binom{\mathfrak{a}}{\mathfrak{b}}$ enthaltene Klasse $\mathfrak{a}+\lambda$ nicht in der Gruppe (ψ') enthalten, w. z. b. w. [während $\binom{\mathfrak{a}}{\mathfrak{a}}=\mathfrak{a}+1$ in (ψ') enthalten ist].

Also: jeder Charakter ψ der Abelschen Gruppe $\binom{\mathfrak{m}}{0}$, dessen Exponent der Faktor $\mathfrak{a}$ von $\mathfrak{m}$ ist, erzeugt in der angegebenen Weise ($\psi(\mathfrak{m}+\mu) = \psi'(\mathfrak{a}+\mu)$) einen bestimmten Charakter ψ' der Abelschen Gruppe $\binom{\mathfrak{a}}{0}$, dessen Exponent $\mathfrak{a}$ ist.

Umgekehrt: Ist $\mathfrak{a}$ Faktor des Ideals $\mathfrak{m}$ und ψ' ein Charakter der Abelschen Gruppe $\binom{\mathfrak{a}}{0}$, dessen Exponent $\mathfrak{a}$, so wird ψ' in der angegebenen Weise ($\psi(\mathfrak{m}+\mu) = \psi'(\mathfrak{a}+\mu)$) durch einen und nur einen Charakter ψ der Abelschen Gruppe $\binom{\mathfrak{m}}{0}$ erzeugt; und dann ist gewiß $\mathfrak{a}$ auch der Exponent von ψ (allgemeiner: ψ und ψ' haben einen und denselben Exponenten).

Erläuterungen zur vorstehenden Abhandlung.

Es handelt sich um die „Sparsamkeit", von der Dedekind in dem im Nachlaß publizierten Brief an Frobenius vom 8. Juli 1896 spricht. Und zwar werden die „natürlichen" Charaktere — jetzt gewöhnlich als eigentliche bezeichnet — allgemeiner als im Brief für einen (endlichen) algebraischen Zahlkörper erklärt. Zugleich gelangt Dedekind zum Begriff des Führers, insbesondere des Führers eines Charakters — in Anlehnung an den Fall des Kreiskörpers als Exponent bezeichnet —; zwar bei Zugrundelegung einer Zahlklasseneinteilung, aber mit Überlegungen, die genau so im allgemeinen Fall der Klassenkörpertheorie gelten.

Die Anwendung dieser Begriffe auf die Zerlegung der Zetafunktion eines beliebigen Kreiskörpers in eigentliche L-Reihen — unter Benutzung der bekannten Primidealzerlegung — ist in dem erwähnten Brief auseinandergesetzt; der Führer-Diskriminantensatz für den Kreiskörper wird in XLII gebracht.

Über seine Publikationsabsichten, anläßlich eines Beitrags für die Festschrift zur Braunschweiger Naturforscherversammlung, schreibt Dedekind an Frobenius (13. April 1897): . . . ich beschloß, meine langjährigen Arbeiten über die allgemeinsten Kreiskörper (lediglich auf Grund des „Skelettes" vom 8. Juni 1882 behandelt, dazu gehören die „natürlichen" Charaktere und die „Sparsamkeit", wovon ich Ihnen im vorigen Jahre geschrieben habe) zum Gegenstande zu wählen; allein diese Sache ist so umfassend, und meine Krankheit machte mir einen solchen Querstrich, daß ich daran verzweifle, es rechtzeitig fertig zu machen. . . . (18. April 1897): ... Ihren Rat, für meinen Beitrag zur Festschrift doch mein zweites Thema (allgemeinste Kreiskörper-Ideale) zu wählen, werde ich schwerlich befolgen können; eine Trennung in zwei Teile, deren zweiter dann an einem ganz andern Orte (etwa in Crelle?) erscheinen müßte, wäre doch sehr unangenehm. . . .

Inwieweit diese nicht publizierten Arbeiten — zu denen auch XL, XLII und die Ausarbeitung von XVI aus Bd. I gehören — auf die Entwicklung der Klassenkörpertheorie von Einfluß gewesen sind, läßt sich nicht mehr feststellen, da der Briefwechsel Dedekind-Weber aus diesen Jahren anscheinend nicht mehr existiert. **Noether.**

XLII.

Grundideale von Kreiskörpern.

Es sei m eine natürliche Zahl, die im folgenden stets beibehalten wird. Ist a ein Divisor von m, so soll mit

$$\varepsilon a$$

der Inbegriff aller ganzen rationalen Zahlen bezeichnet werden, welche relative Primzahlen zu m (also auch zu a) und $\equiv 1 \pmod{a}$ sind. Dieser Inbegriff besteht aus

$$\frac{\varphi(m)}{\varphi(a)}$$

Klassen $(\mathrm{mod.}\, m)$, und diese Klassen bilden eine Gruppe, welche selbst mit εa bezeichnet werden soll.

Hiernach ist $\varepsilon 1$ der Inbegriff aller relativen Primzahlen zu m, welcher aus $\varphi(m)$ Klassen besteht. Ebenso ist εm die Hauptklasse.

$$(\varepsilon m, \varepsilon a) = \frac{\varphi(m)}{\varphi(a)}; \quad (\varepsilon a, \varepsilon 1) = \varphi(a).$$

Sind a, b Divisoren von m, c ihr kleinstes gemeinsames Vielfaches, d ihr größter gemeinsamer Teiler, also $ab = cd$, so ist

$\left.\begin{array}{l} \varepsilon d \text{ das kleinste gemeinsame Vielfache} \\ \varepsilon c \text{ der größte gemeinsame Teiler} \end{array}\right\}$ der Gruppen $\varepsilon a, \varepsilon b$,

$$\varepsilon d = \varepsilon a \cdot \varepsilon b,$$
$$\varepsilon c = \varepsilon a \,|\, \varepsilon b,$$

wo $|$ das Zeichen für den größten gemeinsamen Teiler von Gruppen ist. Ist H irgendeine in $\varepsilon 1$ als Teiler enthaltene Gruppe, so ist das kleinste gemeinsame Vielfache aller in H enthaltenen Gruppen von der Form εa selbst eine solche Gruppe εd, wo d der größte gemeinsame Teiler aller a. Diese Zahl d heißt der Exponent der Gruppe H. Also: Ist a teilbar durch d, so ist εa in H enthalten; ist a nicht teilbar durch d, so ist εa nicht in H enthalten.

Es sei θ eine primitive Wurzel der Gleichung $\theta^m = 1$; $K(m) = R(\theta)$ sei der durch θ erzeugte vollständige Kreiskörper vom Grade $\varphi(m)$; dieser gehört zur Gruppe $\varepsilon m \equiv 1 \pmod{m}$.

Es sei $\mathfrak{Q}$ ein Divisor von $K(m)$, zur Gruppe H gehörig und vom Grade $n = (H, \varepsilon 1)$. Durchläuft h alle in H enthaltenen $\frac{\varphi(m)}{n}$ Klassen, so ist

$$f(x) = \Pi(x - \theta^h)$$

die in $\mathfrak{Q}$ irreduzibele Funktion von x, welche für $x = \theta$ verschwindet, und das Grundideal von $K(m)$ in bezug auf $\mathfrak{Q}$ ist ($\sim$ bedeutet: assoziiert mit)

$$\sim f'(\theta) = \Pi(\theta - \theta^h) \sim \Pi(1 - \theta^{h-1}), \quad \text{mit Ausschluß von } h \equiv 1 \pmod{m}.$$

Jeder Faktor $(1 - \theta^{h-1})$ ist nur dann keine Einheit, sondern Faktor einer in m aufgehenden natürlichen Primzahl p, wenn der kleinste Nenner des Bruches $\frac{h-1}{m}$ eine Potenz von p ist; und zwar ist gleichzeitig (Modul-Bezeichnung)

$$\left[1, \frac{h-1}{m}\right] = \left[\frac{1}{p^s}\right] \text{ mit } 1 - \theta^{h-1} \sim p^{\frac{1}{\varphi(p^s)}}; \quad s > 0.$$

Nun sei m' der größte durch p nicht teilbare Divisor von

$$m = m' p^k; \quad k > 0.$$

Damit eine Zahl h der vorstehenden Bedingung genüge, ist erforderlich

$$h \equiv 1 \left(\text{mod.} \frac{m}{p^s} = m' p^{k-s}\right), \quad h - 1 = u \cdot m' p^{k-s},$$

wo, wenn $s > 0$ ist, u nicht teilbar durch p; d. h. h muß eine Zahl der Gruppe $\varepsilon \frac{m}{p^s}$ sein, also ein Element des größten gemeinsamen Teilers

$$Q_s = H \mid \varepsilon \frac{m}{p^s}$$

der Gruppen H und $\varepsilon \frac{m}{p^s}$; es sei

$$q_s = (\varepsilon m, Q_s)$$

der Grad von Q_s. Es darf aber h nicht $\equiv 1 \left(\text{mod.} \frac{m}{p^{s-1}} = \frac{m}{p^s} \cdot p\right)$, also nicht in $\varepsilon \frac{m}{p^{s-1}}$ enthalten, also keine der q_{s-1} Zahlen in Q_{s-1} sein. Mithin ist $q_s - q_{s-1}$ die Anzahl der obigen h, und folglich ist der betreffende Faktor von $f'(\theta)$, welcher nur Faktoren von p enthält,

$$\sim p^{\frac{q_1 - q_0}{\varphi(p)} + \frac{q_2 - q_1}{\varphi(p^2)} + \frac{q_3 - q_2}{\varphi(p^3)} + \cdots + \frac{q_k - q_{k-1}}{\varphi(p^k)}}.$$

Offenbar ist

$$Q_0 = \varepsilon m, \quad q_0 = 1.$$

Der Grad der Gruppe $\varepsilon \frac{m}{p^s}$ ist

$$\frac{\varphi(m)}{\varphi\left(\frac{m}{p^s}\right)} = \frac{\varphi(m')\,\varphi(p^k)}{\varphi(m')\,\varphi(p^{k-s})} = \frac{\varphi(p^k)}{\varphi(p^{k-s})} = p^s \text{ oder } = \varphi(p^k) = p^k - p^{k-1},$$

je nachdem $s < k$ oder $s = k$.

Also ist q_s Divisor von p^s, wenn $s < k$, und q_k Divisor von $\varphi(p^k)$. Außerdem ist Q_s Divisor von Q_{s+1}, also auch q_s Divisor von q_{s+1}. Ferner ist

$$\left(Q_s,\ \varepsilon \frac{m}{p^s}\right) = \left(H,\ \varepsilon \frac{m}{p^s}\right) = \left(H,\ H\,\varepsilon \frac{m}{p^s}\right),$$

$$q_s \left(H,\ H\,\varepsilon \frac{m}{p^s}\right) = (\varepsilon m, Q_s)\left(Q_s,\ \varepsilon \frac{m}{p^s}\right) = \left(\varepsilon m,\ \varepsilon \frac{m}{p^s}\right) = \frac{\varphi(p^k)}{\varphi(p^{k-s})},$$

$$\frac{q_1}{p} = \frac{1}{\left(H, \varepsilon \frac{m}{p}\right)}, \quad \frac{q_2}{p^2} = \frac{1}{\left(H, \varepsilon \frac{m}{p^2}\right)}, \quad \cdots, \quad \frac{q_{k-1}}{p^{k-1}} = \frac{1}{\left(H, \varepsilon \frac{m}{p^{k-1}}\right)},$$

$$\frac{q_k}{\varphi(p^k)} = \frac{1}{\left(H, \varepsilon \frac{m}{p^k}\right)}, \quad \frac{q_0}{1} = \frac{1}{(H, \varepsilon m)} = 1.$$

Ist Ω der Körper $R = K(1)$ der rationalen Zahlen, so ist $H = \varepsilon 1$ die Gesamtgruppe, mithin $Q_s = \varepsilon \frac{m}{p^s}$, und

$$q_s = \frac{\varphi(p^k)}{\varphi(p^{k-s})},$$

$$q_k - q_{k-1} = \varphi(p^k) - p^{k-1} = (p-2)\,p^{k-1} = \frac{p-2}{p-1}\,\varphi(p^k),$$

$$q_{k-1} - q_{k-2} = p^{k-1} - p^{k-2} = \varphi(p^{k-1}), \quad q_{k-2} - q_{k-3} = \varphi(p^{k-2});$$

$$\cdots\ q_1 - q_0 = p - 1 = \varphi(p),$$

und folglich wird

$$p^{k-1+\frac{p-2}{p-1}} = p^{k-\frac{1}{p-1}}$$

der betreffende Faktor des absoluten (d. h. nach R genommenen) Grundideals von $K(m)$.

Wenn Ω und H wieder die allgemeine Bedeutung haben, so ist daher

$$p^{k-\frac{1}{p-1}-\frac{q_1-q_0}{\varphi(p)}-\frac{q_2-q_1}{\varphi(p^2)}-\cdots-\frac{q_k-q_{k-1}}{\varphi(p^k)}}$$

$$= p^{k-\frac{q_1}{p}-\frac{q_2}{p^2}-\cdots-\frac{q_{k-1}}{p^{k-1}}-\frac{q_k}{\varphi(p^k)}}$$

$$= p^{\sum\left(1-\frac{1}{\left(H,\ \varepsilon\frac{m}{p^s}\right)}\right)} = p^{\sum\left(1-\frac{1}{\left(\Omega,\ K\left(\frac{m}{p^s}\right)\right)}\right)}$$

der betreffende Faktor des Grundideals des Körpers Ω nach R.

Da alle $\varepsilon\frac{m}{p^s}$ Teiler der Gruppe $\varepsilon\frac{m}{p^k} = \varepsilon m'$ sind, so ist Q_s auch der gr. g. T. von H, $\varepsilon\frac{m}{p^s}$ und $\varepsilon m'$, also auch Q_s der gr. g. T. von Q_k und $\varepsilon\frac{m}{p^s}$.

Ist ψ ein Charakter der Abelschen Gruppe $\varepsilon 1$, so soll ψ_0 die Gruppe aller derjenigen Elemente r von $\varepsilon 1$ bedeuten, für welche $\psi(r) = 1$ ist, und unter dem Exponenten von ψ soll der Exponent der Gruppe ψ_0 verstanden sein.

Ist H irgendein Teiler von $\varepsilon 1$ und (wie oben) Ω der zugehörige Körper vom Grade $n = (H, \varepsilon 1)$, so ist n die Anzahl aller derjenigen Charaktere ψ, deren Gruppen ψ_0 Vielfache von H sind.

Es soll das Produkt der Exponenten dieser n Charaktere ψ oder vielmehr die höchste in demselben aufgehende Potenz von p ermittelt werden.

Es sei ψ einer dieser n Charaktere und sein Exponent $= m'' p^{k-s}$, wo m'' nicht teilbar durch p, also Divisor von m', und $0 \leqq s < k$.

Dann ist $\varepsilon m'' p^{k-s}$ Teiler von ψ_0, also auch $\varepsilon m' p^{k-s} = \varepsilon\frac{m}{p^s}$ Teiler von ψ_0; also ist auch $H\varepsilon\frac{m}{p^s}$ Teiler von ψ_0.

Umgekehrt aber, wenn $H\varepsilon\frac{m}{p^s}$ Teiler von ψ_0, so ist der Exponent von ψ_0 ein Divisor von $\frac{m}{p^s}$, und die höchste in ihm aufgehende Potenz von p ist Divisor von p^{k-s}.

Nun ist $\left(H\,\varepsilon\,\frac{m}{p^s},\,\varepsilon\,1\right)$ die Anzahl aller dieser ψ, also ebenso $\left(H\,\varepsilon\,\frac{m}{p^{s+1}},\,\varepsilon\,1\right)$ die Anzahl aller ψ, deren Exponent höchstens durch p^{k-s-1} teilbar ist, also $\left(H\,\varepsilon\,\frac{m}{p^s},\,\varepsilon\,1\right) - \left(H\,\varepsilon\,\frac{m}{p^{s+1}},\,\varepsilon\,1\right)$ die Anzahl derjenigen ψ, deren Exponent die Potenz p^{k-s} genau enthält.

Nun ist

$$(H,\,\varepsilon\,1) = \left(H,\,H\,\varepsilon\,\frac{m}{p^s}\right)\left(H\,\varepsilon\,\frac{m}{p^s},\,\varepsilon\,1\right) = n;$$

und

$$q_s\left(H,\,H\,\varepsilon\,\frac{m}{p^s}\right) = \frac{\varphi\,(p^k)}{\varphi\,(p^{k-s})},$$

folglich

$$\frac{\varphi\,(p^k)}{\varphi\,(p^{k-s})}\left(H\,\varepsilon\,\frac{m}{p^s},\,\varepsilon\,1\right) = n\,q_s,\ \left(H\,\varepsilon\,\frac{m}{p^s},\,\varepsilon\,1\right) = n\,q_s\,\frac{\varphi\,(p^{k-s})}{\varphi\,(p^k)}$$

$$= \frac{n\,q_s}{p^s} \text{ oder } = \frac{n\,q_k}{\varphi\,(p^k)},$$

je nachdem

$$s < k \quad \text{oder} \quad s = k.$$

Also ist

1	$\frac{n\,q_{k-1}}{p^{k-1}} - \frac{n\,q_k}{\varphi\,(p^k)}$	Anzahl der ψ, in deren Exponent der Faktor	p,
2	$\frac{n\,q_{k-2}}{p^{k-2}} - \frac{n\,q_{k-1}}{p^{k-1}}$	„ „ „ „ „ „ „ „	p^2,
$k-1$	$\frac{n\,q_1}{p} - \frac{n\,q_2}{p^2}$	„ „ „ „ „ „ „ „	p^{k-1},
k	$n - \frac{n\,q_1}{p}$	„ „ „ „ „ „ „ „	p^k.

Also

$$p^{kn - \frac{nq_1}{p} - \frac{nq_2}{p^2} - \cdots - \frac{nq_{k-1}}{p^{k-1}} - \frac{nq_k}{\varphi(p^k)}} = \left(p^{k - \frac{q_1}{p} - \frac{q_2}{p^2} - \cdots - \frac{q_{k-1}}{p^{k-1}} - \frac{q_k}{\varphi(p^k)}}\right)^n.$$

Mithin ist dies Produkt aller Exponenten der n Charaktere ψ des Körpers Ω zugleich die n^{te} Potenz des Grundideals von Ω, d. h. $= \pm$ Grundzahl von Ω, w. z. b. w. (Norm des Grundideals.)

Erläuterungen. 1. Ist die Gruppe H von Elementen h irgendein Teiler der Gruppe $\varepsilon\,1$, so ist

$$(H,\,\varepsilon\,1)$$

die Anzahl aller derjenigen Charaktere ψ der Gruppe $\varepsilon 1$, welche Multipla des identischen (oder Haupt-) Charakters der Gruppe H sind, welche also für alle Elemente h der Gruppe H der Bedingung

$$\psi(h) = 1$$

genügen; oder mit anderen Worten: $(H, \varepsilon 1)$ ist die Anzahl aller derjenigen Charaktere ψ, deren Gruppen ψ_0 Vielfache von H sind, also der Bedingung

$$(\psi_0, H) = 1$$

genügen.

2. Ist a (wie auf S. 401) irgendein Divisor von m, und εa wieder die Gruppe von $\frac{\varphi(m)}{\varphi(a)}$ Klassen (mod. m), deren Zahlen relative Primzahlen zu m und zugleich $\equiv 1 \pmod{a}$ sind, so ist die Aussage

$$(H, \varepsilon a) = 1 \quad \text{(also } \varepsilon a \text{ Teiler von } H)$$

gleichbedeutend damit, daß der Exponent d der Gruppe H ein Divisor von a ist.

3. Speziell bedeutet also die Aussage

$$(\psi_0, \varepsilon a) = 1,$$

daß der Exponent des Charakters ψ (d. h. der Exponent der Gruppe ψ_0) Divisor von a ist.

4. Das System der beiden gleichzeitigen Aussagen

$$(\psi_0, H) = 1, \quad (\psi_0, \varepsilon a) = 1$$

ist gleichbedeutend mit der einen Aussage

$$(\psi_0, H \varepsilon a) = 1;$$

diese letztere bedeutet also, daß erstens ψ ein Multiplum des Hauptcharakters der Gruppe H [also $\psi(h) = 1$ für alle h], und daß zweitens der Exponent von ψ ein Divisor von a ist; zufolge 1. (wenn dort H durch $H \varepsilon a$ ersetzt wird) ist

$$(H \varepsilon a, \varepsilon 1) \quad \text{die Anzahl} = f(a)$$

aller dieser Charaktere.

5. Bedeutet daher, wenn a irgendein Divisor von m, und H eine feste Gruppe ist,

$$f'(a)$$

die Anzahl aller derjenigen Charaktere ψ der Gruppe $\varepsilon 1$, welche

Multipla des Hauptcharakters von H sind, und deren Exponent $= a$ ist, so ist die über alle Divisoren d von a erstreckte Summe

$$\sum f'(d) = (H\,\varepsilon\,a,\ \varepsilon\,1) = f(a)$$

und folglich umgekehrt

$$f'(a) = \sum \eta\left(\frac{a}{d}\right)(H\,\varepsilon\,d,\ \varepsilon\,1) = \sum \eta\left(\frac{a}{d}\right) f(d),\ d \text{ alle Divisoren von } a,$$

wo η die Funktion von Mertens-Cantor bedeutet.

6. Das Produkt der Exponenten aller Charaktere ψ, welche Multipla des Hauptcharakters der Gruppe sind, und deren Anzahl zufolge 1. $= (H,\ \varepsilon\,1)$ ist, ist daher das über alle Divisoren a von m ausgedehnte Produkt

$$\Pi a^{f'(a)}.$$

7. Setzt man

$$n = (H,\ \varepsilon\,1),$$

so ist

$$n = (H,\ H\,\varepsilon\,a)(H\,\varepsilon\,a,\ \varepsilon\,1);\quad (H\,\varepsilon\,a,\ \varepsilon\,1) = \frac{n}{(H,\ H\,\varepsilon\,a)};$$

ferner ist

$$(H,\ H\,\varepsilon\,a) = (H,\ \varepsilon\,a) = (H\,|\,\varepsilon\,a,\ \varepsilon\,a),$$

wo $A\,|\,B$ allgemein den größten gemeinsamen Teiler der Gruppen A, B bedeutet; immer ist $(A,\ B) = (A,\ A\,B) = (A\,|\,B,\ B)$. Ferner ist

$$(\varepsilon\,m,\ \varepsilon\,a) = \frac{\varphi(m)}{\varphi(a)} = (\varepsilon\,m,\ H\,|\,\varepsilon\,a)(H\,|\,\varepsilon\,a,\ \varepsilon\,a);$$

bezeichnet man daher

$$(\varepsilon\,m,\ H\,|\,\varepsilon\,a) = t(a),$$

welches der Grad des größten gemeinsamen Teilers $H\,|\,\varepsilon\,a$ der beiden Gruppen H und $\varepsilon\,a$ ist, so wird

$$(H\,|\,\varepsilon\,a,\ \varepsilon\,a) = \frac{\varphi(m)}{\varphi(a)} \cdot \frac{1}{t(a)};\quad (H\,\varepsilon\,a,\ \varepsilon\,1) = \frac{n}{\varphi(m)} \cdot \varphi(a)\,t(a) = f(a).$$

Außerdem ist

$$\varphi(m) = (\varepsilon\,m,\ \varepsilon\,1) = (\varepsilon\,m,\ H)(H,\ \varepsilon\,1) = (\varepsilon\,m,\ H)\,n;\ \frac{\varphi(m)}{n} = (\varepsilon\,m,\ H).$$

8. Es werden nur noch solche Charaktere ψ der Gruppe $\varepsilon\,1$ betrachtet, welche Multipla des Hauptcharakters der Gruppe H sind, also der Bedingung $(\psi_0,\ H) = 1$ genügen und deren Anzahl $= n = (H,\ \varepsilon\,1)$ ist.

Ist nun p eine in m aufgehende natürliche Primzahl und

$$m = m' p^k, \quad k > 0, \quad m' \text{ nicht teilbar durch } p,$$

so ist

$$\left(H \varepsilon \frac{m}{p^s}, \varepsilon 1\right), \quad \text{wo } 0 \leqq s \leqq k,$$

die Anzahl derjenigen Charaktere ψ, deren Exponenten Divisoren von

$$\frac{m}{p^s} = m' p^{k-s}$$

sind. Also

$(H \varepsilon m', \varepsilon 1)$ Anzahl der ψ, deren Exponenten Divisoren von m'	$= f(m')$
$(H \varepsilon m' p, \varepsilon 1)$ Anzahl der ψ, deren Exponenten Divisoren von $m' p$	$= f(m' p)$
$(H \varepsilon m' p^2, \varepsilon 1)$ Anzahl der ψ, deren Exponenten Divisoren von $m' p^2$	$= f(m' p^2)$
. . . . .	. . . . .
$(H \varepsilon m' p^{k-1}, \varepsilon 1)$ Anzahl der ψ, deren Exponenten Divisoren von $m' p^{k-1}$	$= f(m' p^{k-1})$
$n = (H \varepsilon m' p^k, \varepsilon 1)$ Anzahl der ψ, deren Exponenten Divisoren von $m' p^k = m$	$= f(m' p^k) = f(m)$

$= (H \varepsilon m, \varepsilon 1)$

$= (H, \varepsilon 1)$.

Also ist

$(H \varepsilon m' p, \varepsilon 1) - (H \varepsilon m', \varepsilon 1)$ Anzahl der ψ, deren Exponenten den Faktor p, nicht den Faktor p^2 enthalten,

$(H \varepsilon m' p^2, \varepsilon 1) - (H \varepsilon m' p, \varepsilon 1)$ Anzahl der ψ, deren Exponenten den Faktor p^2, nicht den Faktor p^3 enthalten,

. . . . . .

$(H \varepsilon m' p^k, \varepsilon 1) - (H \varepsilon m' p^{k-1}, \varepsilon 1)$ Anzahl der ψ, deren Exponenten den Faktor p^k, nicht den Faktor p^{k+1} enthalten.

Mithin ist der Exponent der höchsten im Produkte der Exponenten aller n Charaktere ψ aufgehenden Potenz von p

$$= \{(H \varepsilon m' p, \varepsilon 1) - (H \varepsilon m', \varepsilon 1)\} + 2\{(H \varepsilon m' p^2, \varepsilon 1) - (H \varepsilon m' p, \varepsilon 1)\} + \cdots + k\{(H \varepsilon m' p^k, \varepsilon 1) - (H \varepsilon m' p^{k-1}, \varepsilon 1)\}$$

$$= k(H, \varepsilon 1) - \{(H \varepsilon m', \varepsilon 1) + (H \varepsilon m' p, \varepsilon 1) + \cdots + (H \varepsilon m' p^{k-1}, \varepsilon 1)\}$$

$$= kn - \sum_{s=0}^{s=k-1} f(m' p^s).$$

Es ist aber

$$(H,\ \varepsilon\,1) = (H,\ H\,\varepsilon\,m'\,p^s)(H\,\varepsilon\,m'\,p^s,\ \varepsilon\,1) = (H,\ \varepsilon\,m'\,p^s)\,f(m'\,p^s),$$

also wird der Potenzexponent von p

$$= n\left\{k - \sum_{s=0}^{s=k-1} \frac{1}{(H,\ \varepsilon\,m'\,p^s)}\right\}.$$

Es ist aber

$$(H,\ \varepsilon\,m'\,p^s) = (H\,|\,\varepsilon\,m'\,p^s,\ \varepsilon\,m'\,p^s),$$

also

$$(\varepsilon\,m,\ H\,|\,\varepsilon\,m'\,p^s)(H,\ \varepsilon\,m'\,p^s) = (\varepsilon\,m,\ \varepsilon\,m'\,p^s) = \frac{\varphi\,(m)}{\varphi\,(m'\,p^s)} = \frac{\varphi\,(p^k)}{\varphi\,(p^s)},$$

also

$$\frac{1}{(H,\ \varepsilon\,m'\,p^s)} = \frac{(\varepsilon\,m,\ H\,|\,\varepsilon\,m'\,p^s)}{p^{k-s}},\ \text{wenn}\ s > 0,$$

und

$$\frac{1}{(H,\ \varepsilon\,m')} = \frac{(\varepsilon\,m,\ H\,|\,\varepsilon\,m')}{\varphi\,(p^k)}.$$

Also wird der obige Potenzexponent von p

$$= n\left\{k - \frac{(\varepsilon\,m,\ H\,|\,\varepsilon\,m')}{\varphi\,(p^k)} - \sum_{s=1}^{s=k-1} \frac{(\varepsilon\,m,\ H\,|\,\varepsilon\,m'\,p^s)}{p^{k-s}}\right\}.$$

Erläuterungen zur vorstehenden Abhandlung.

Es handelt sich um eine Anwendung der in XLI entwickelten allgemeinen Begriffe.

Der hier für den Kreiskörper gegebene Führer-Diskriminantensatz — Darstellung der Diskriminante als Produkt der Führer (Exponenten bei Dedekind) der Charaktere der zugehörigen Klassengruppe — ist im allgemeinen Fall der relativ-Abelschen Körper auf zwei verschiedene Arten erbracht: mit transzendenten Methoden (Heckesche L-Reihen mit Größencharakteren) und arithmetisch unter Benutzung des Umkehrsatzes der Klassenkörpertheorie (vgl. den Bericht von Hasse, I, II; Jahresber. d. d. Math.-Ver. **35** und Ergänzungsbd. VI).

Das Analogon für Galoissche, nicht Abelsche Körper hat neuerdings E. Artin aufgestellt (Journ. f. Math. **164** (1931)).

Noether.

XLIII.

Untersuchung der Gruppe X.

(Einige Sätze aus der Untersuchung der Beziehungen zwischen den Idealen in verschiedenen Körpern. Schreiben an G. Frobenius vom 8. Juni 1882.)

Es sei χ eine nicht identische Permutation der Gruppe X (also $g > 1$), und $\mathfrak{p}^r$ die höchste in allen Differenzen $\omega\chi - \omega$ aufgehende Potenz von $\mathfrak{p}$, also

$$\omega\chi \equiv \omega \pmod{\mathfrak{p}^r},$$

aber nicht identisch

$$\omega\chi \equiv \omega \pmod{\mathfrak{p}^{r+1}}, \quad r \geqq 1.$$

Dann sei $\mathfrak{o}_1$ das System aller derjenigen Zahlen ω_1 in $\mathfrak{o}$, welche die Kongruenz

$$\omega_1\chi \equiv \omega_1 \pmod{\mathfrak{p}^{r+1}}$$

erfüllen. Zunächst leuchtet ein, daß $\mathfrak{o}_1$ ein Modul ist, weil aus $\alpha\chi \equiv \alpha$, $\beta\chi \equiv \beta \pmod{\mathfrak{p}^{r+1}}$ auch $(\alpha - \beta)\chi = \alpha\chi - \beta\chi \equiv \alpha - \beta \pmod{\mathfrak{p}^{r+1}}$ folgt, und zwar ist $\mathfrak{o}_1$ ein echtes Vielfaches von $\mathfrak{o}$, weil $\mathfrak{o}$ nicht teilbar durch $\mathfrak{o}_1$ ist. Da ferner $\mathfrak{p}\chi = \mathfrak{p}$, also auch $\mathfrak{p}^{r+1}\chi = \mathfrak{p}^{r+1}$ ist, so genügt jede in $\mathfrak{p}^{r+1}$ enthaltene Zahl π_{r+1}, weil $\pi_{r+1}\chi = \pi'_{r+1}$ ebenfalls in $\mathfrak{p}^{r+1}$ enthalten ist, der Kongruenz $\pi_{r+1}\chi \equiv \pi_{r+1} \pmod{\mathfrak{p}^{r+1}}$, weil $\pi'_{r+1} \equiv \pi_{r+1} \equiv 0 \pmod{\mathfrak{p}^{r+1}}$ ist; mithin ist $\mathfrak{p}^{r+1}$ teilbar durch $\mathfrak{o}_1$, und folglich enthält $\mathfrak{o}_1$ auch n voneinander unabhängige Zahlen; $\mathfrak{o}_1$ ist ein endlicher n-gliedriger Modul, dessen Basis zugleich eine Basis des Körpers Ω ist. Da $\mathfrak{o} < \mathfrak{o}_1 < \mathfrak{p}^{r+1}$, so ist

$$(\mathfrak{o}, \mathfrak{p}^{r+1}) = p^{(r+1)f} = (\mathfrak{o}, \mathfrak{o}_1)(\mathfrak{o}_1, \mathfrak{p}^{r+1}),$$

also

$$(\mathfrak{o}, \mathfrak{o}_1) = p^h, \quad 0 < h \leqq (r+1)f.$$

Sodann leuchtet ein, daß $\mathfrak{o}_1$ eine Ordnung ist; denn für jede ganze rationale, d. h. in $\mathfrak{z}$ enthaltene Zahl z ist $z\chi = z$, also ist $\mathfrak{z} > \mathfrak{o}_1$,

und da aus $\alpha\chi \equiv \alpha$, $\beta\chi \equiv \beta \pmod{\mathfrak{p}^{r+1}}$ auch $(\alpha\beta)\chi = \alpha\chi \cdot \beta\chi \equiv \alpha\beta \pmod{\mathfrak{p}^{r+1}}$ folgt, so ist auch $\mathfrak{o}_1^2 > \mathfrak{o}_1$, w. z. b. w. (D., S. 505). Da $\mathfrak{p}^{r+1} > \mathfrak{o}_1$, so ist der Führer

$$\frac{\mathfrak{o}_1}{\mathfrak{o}} = \mathfrak{p}^k, \quad 0 < k \leqq r+1, \quad (\mathfrak{o}, \mathfrak{o}_1)(\mathfrak{o}_1, \mathfrak{p}^k) = (\mathfrak{o}, \mathfrak{p}^k) = p^{kf},$$
$$0 < h \leqq kf$$

oder vielmehr $0 < h < kf$, weil $\mathfrak{o}_1$ notwendig ein echter Teiler von $\mathfrak{p}^k$ ist.

Nun sei ϱ eine bestimmte durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbare Zahl, so ist $\mathfrak{o}\varrho + \mathfrak{p}^2 = \mathfrak{p}$, also $\mathfrak{o}\varrho^r + \mathfrak{p}^{2r} = \mathfrak{o}\varrho^r + \mathfrak{p}^{r+1} = \mathfrak{p}^r$; da nun alle $\omega\chi - \omega$ in $\mathfrak{p}^r$ enthalten sind, so kann man setzen

$$\omega\chi \equiv \omega + \varrho^r d\omega \pmod{\mathfrak{p}^{2r}},$$

wo $d\omega$ eine zu ω gehörige Zahl ist, die mod. $\mathfrak{p}^r$ bestimmt ist. Für alle in $\mathfrak{o}_1$ enthaltenen Zahlen ω_1, und nur für diese, ist

$$d\omega_1 \equiv 0 \pmod{\mathfrak{p}}.$$

Nun folgen aus $(\alpha \pm \beta)\chi = \alpha\chi \pm \beta\chi$ und $(\alpha\beta)\chi = (\alpha\chi)(\beta\chi)$, und aus

$$\alpha\chi \equiv \alpha + \varrho^r d\alpha, \quad \beta\chi \equiv \beta + \varrho^r d\beta \pmod{\mathfrak{p}^{2r}}$$

die Gesetze (Differentialrechnung)

$$d(\alpha \pm \beta) \equiv d\alpha \pm d\beta, \quad d(\alpha\beta) \equiv \beta d\alpha + \alpha d\beta \pmod{\mathfrak{p}^r}$$

und hieraus weiter

$$d(\omega^m) \equiv m\omega^{m-1} d\omega \pmod{\mathfrak{p}^r}.$$

Da hieraus $d(\varrho^2) \equiv 2\varrho d\varrho \pmod{\mathfrak{p}^r}$, also $d(\varrho^2) \equiv 0 \pmod{\mathfrak{p}}$ folgt, so ist ϱ^2 in $\mathfrak{o}_1$ enthalten; da ferner $\mathfrak{p}^2 = \mathfrak{o}\varrho^2 + \mathfrak{p}^{r+1}$, also jede in $\mathfrak{p}^2$ enthaltene Zahl

$$\pi_2 = \omega\varrho^2 + \pi_{r+1}$$

gesetzt werden kann, wo ω in $\mathfrak{o}$, π_{r+1} in $\mathfrak{p}^{r+1}$ enthalten ist, so folgt $d\pi_2 \equiv \omega d(\varrho^2) + \varrho^2 d\omega + d\pi_{r+1} \pmod{\mathfrak{p}^r}$, also $d\pi_2 \equiv 0 \pmod{\mathfrak{p}}$, folglich $\mathfrak{p}^2 > \mathfrak{o}_1$, also $k = 1$ oder $= 2$.

[Dieser Satz über die Substitutionen der höheren Verzweigungsgruppen — der, nach der Überschrift zu schließen, vor der Publikation in den Göttinger Nachrichten zu liegen scheint — wurde in der Literatur nie in dieser Fassung ausgesprochen. E. N.]

XLIV.

Ideale in Normalkörpern.

Ist χ irgend eine Permutation des Normalkörpers Ω, ω irgend eine Zahl in Ω, so setze man

$$\omega\chi = \omega + d\omega, \quad \omega\chi^s = \omega + \frac{s}{1}d\omega + \frac{s(s-1)}{1\cdot 2}d^2\omega + \cdots = (1+d)^s\omega,$$

$$d^s\omega = \omega(\chi - 1)^s \text{ symbolisch};$$

aus $(\alpha \pm \beta)\chi = \alpha\chi \pm \beta\chi$ und $(\alpha\beta)\chi = (\alpha\chi)(\beta\chi)$ folgt

$$d(\alpha \pm \beta) = d\alpha \pm d\beta, \quad d(\alpha\beta) = \beta d\alpha + \alpha d\beta + d\alpha d\beta.$$

Alle Zahlen ω, welche der Bedingung $d\omega = 0$ genügen, bilden den zu der Gruppe 1, χ, χ^2, χ^3 $\cdots$ gehörigen Körper, welcher $= \Omega$ ist, falls χ die identische Permutation von Ω ist.

Von jetzt ab bedeute ω jede ganze Zahl des Körpers Ω, also jede Zahl in $\mathfrak{o}$, so ist $d\omega$ ebenfalls in $\mathfrak{o}$ enthalten, und zufolge $d(\alpha - \beta) = d\alpha - d\beta$ bilden alle diese Zahlen $d\omega$ einen durch $\mathfrak{o}$ teilbaren Modul, der mit $d\mathfrak{o}$ bezeichnet werden kann. Ist χ die identische Permutation, so ist $d\mathfrak{o} = 0$. Ist h der kleinste positive Exponent, für welchen $\chi^h = 1$, so ist $n = hk$ der Grad von Ω (Bezeichnung wie im Schreiben an G. Frobenius von 1882. 6. 8.), k der Grad des Körpers aller derjenigen Zahlen ω, deren $d\omega = 0$. Ist

$$\mathfrak{e} = [\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_k]$$

das System aller ganzen Zahlen dieses Körpers, und

$$\mathfrak{o} = [\omega_1, \omega_2, \cdots, \omega_n],$$

so folgt, weil gleichzeitig

$$\omega = x_1\omega_1 + x_2\omega_2 + \cdots + x_n\omega_n$$

und

$$d\omega = x_1 d\omega_1 + x_2 d\omega_2 + \cdots + x_n d\omega_n$$

ist,

$$d\mathfrak{o} = [d\omega_1, d\omega_2, \cdots, d\omega_n].$$

Da nun

$$\varepsilon_r = a_{1,r}\omega_1 + a_{2,r}\omega_2 + \cdots + a_{n,r}\omega_n,$$

also

$$0 = a_{1,r}d\omega_1 + a_{2,r}d\omega_2 + \cdots + a_{n,r}d\omega_n$$

und die aus den ganzen rationalen Zahlen $a_{\varrho,r}$ gebildeten Determinanten k^{ten} Grades nicht alle verschwinden, so sind von den n Zahlen $d\omega_1$, $d\omega_2$, $\cdots$, $d\omega_n$ höchstens $n - k = (h-1)k$ voneinander unabhängig. Umgekehrt: findet zwischen diesen Zahlen $d\omega_\iota$ eine Relation $\sum x_\iota d\omega_\iota = 0$ statt, mit ganzen rationalen Koeffizienten x_ι, so ist $d\sum x_\iota\omega_\iota = 0$, also $\sum x_\iota\omega_\iota$ in $\mathfrak{e}$ enthalten, also

$$\sum x_\iota\omega_\iota = \sum y_\iota\varepsilon_\iota, \quad x_r = \sum y_\iota a_{r,\iota}.$$

Als Basis des Körpers Ω kann man

$$\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_k, \quad \omega_{k+1}, \cdots, \omega_n$$

wählen, wo $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_k$ eine Basis des zu der Gruppe χ gehörigen Körpers Ω' bilden,

$$\omega = h_1\varepsilon_1 + h_2\varepsilon_2 + \cdots + h_k\varepsilon_k + h_{k+1}\omega_{k+1} + \cdots + h_n\omega_n,$$
$$d\omega = h_{k+1}d\omega_{k+1} + \cdots + h_n d\omega_n,$$

$d\omega_{k+1}, \cdots, d\omega_n$ Basis der Schar $d\Omega$.

Denn wäre

$$h_{k+1}d\omega_{k+1} + \cdots + h_n d\omega_n = 0,$$

so ist

$$h_{k+1}\omega_{k+1} + \cdots + h_n\omega_n$$

in Ω' enthalten, also

$$= h_1\varepsilon_1 + \cdots + h_k\varepsilon_k,$$

woraus folgt, daß alle $h = 0$ sind.

[Diese formale Differentiation war offenbar zur Untersuchung der Differente gedacht, wie weitere angefangene Rechnungen zeigen, wo dieselben Betrachtungen modulo p auftreten; darauf weist auch die Überschrift hin. E. N.]

XLV.

Aus Briefen an Frobenius*).

8. Juni 1882**).

... Die Ihnen bekannte Existenz einer Substitution F (bei mir Permutation ψ_0), für welche $\omega^p \equiv F\omega \pmod{\mathfrak{p}}$, bildet auch bei mir die eigentliche Basis; Sie schreiben zwar: „Ich irre wohl nicht, wenn ich annehme, dass der durch diesen Satz angedeutete Weg einer von denen ist, die auch Sie früher einmal eingeschlagen, dann aber wohl schliesslich verlassen und durch einen bessern ersetzt haben.“ Aber ich glaube kaum, dass es einen besseren Weg giebt. Mit Hülfe der Theorie der höheren Congruenzen und mit viel Geduld und Zeit ist es mir nach und nach gelungen, die Schwierigkeiten zu überwinden und die Gesetze möglichst einfach zu gestalten. In diesen ist auch, wie Sie vermuthen, der Satz enthalten, für den Sie einen Beweis wünschen, und den Sie so aussprechen:

Ist eine rationale Primzahl $\mathfrak{o}'p = \mathfrak{p}'_1\mathfrak{p}'_2 \cdots \mathfrak{p}'_{e'}$, wo $\mathfrak{p}'_1, \mathfrak{p}'_2 \cdots \mathfrak{p}'_{e'}$ verschiedene Primideale in $\mathfrak{o}'$ von den Graden $f'_1, f'_2, \cdots f'_{e'}$ sind, so giebt es in der Gruppe Φ des Körpers Ω' eine Substitution ψ_0, die aus e' Cyklen von $f'_1, f'_2, \cdots f'_{e'}$ Elementen besteht.

In der That, wenn alle $a_r = 1$, mithin alle $g_r = g$ sind, so ist X gemeinschaftlicher Theiler aller $\varphi_r \Phi' \varphi_r^{-1}$ und überhaupt aller mit Φ' conjugirten Gruppen $\varphi \Phi' \varphi^{-1}$; da diese aber, wenn wirklich Φ die

---

*) [Diese Briefe wurden durch Herrn Landau freundlichst zur Verfügung gestellt. Die Briefe von Frobenius an Dedekind waren im Nachlaß nicht zu finden; es fehlten im Nachlaß die Briefe aus den Jahren 1880—1900. E. N.]

**) [Im wesentlichen wiedergegeben bei Frobenius: Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe. Sitzungsber. d. Preuß. Akademie d. Wissensch. 1896. E. N.]

Gruppe von Ω', d. h. Ω die Norm von Ω' ist, keinen gemeinsamen Theiler haben, so muß $X = 1$, $g = 1$ sein, d. h. p ist durch kein Primidealquadrat in Ω theilbar. Dann ist

$$\Psi'_r = 1 + \psi_r^{f'_r} + \psi_r^{2f'_r} + \cdots + \psi_r^{(f_r-1)f'_r},$$

wo $\psi_r = \varphi_r^{-1}\psi_0\varphi_r$,

$$\Phi'\varphi_r^{-1}\Psi = \Phi'\varphi_r^{-1} + \Phi'\varphi_r^{-1}\psi_0 + \Phi'\varphi_r^{-1}\psi_0^2 + \cdots + \Phi'\varphi_r^{-1}\psi_0^{f'_r-1};$$

ersetzt man in der Zerlegung

$$\Phi = \Phi'\varphi_1^{-1}\Psi + \cdots + \Phi'\varphi_{e'}^{-1}\Psi$$

jeden einzelnen Complex $\Phi'\varphi_r^{-1}\Psi$ durch das vorstehende System der f'_r Complexe, so wird Φ überhaupt in

$$n' = f'_1 + f'_2 + \cdots + f'_{e'}$$

Complexe $\Phi'\varphi$ zerlegt, deren jedem bekanntlich eine Permutation von Ω' (eine Wurzel der irreductibeln Gleichung vom Grade n') entspricht; die Permutation ψ_0 verwandelt dieselben in die Complexe $\Phi'\varphi\psi_0$, bringt also eine Permutation dieser n' Complexe (Elemente) $\Phi'\varphi$ hervor, bei welcher die in $\Phi'\varphi_r^{-1}\Psi$ enthaltenen f'_r Complexe (Elemente, Wurzeln) cyklisch in einander übergehen.

14. Juni 1882*).

... Auf den hiermit wieder zurückerfolgenden Blättern (13—15) haben Sie die Existenz einer Permutation ψ_0 (oder Substitution F) sehr kurz bewiesen. Bei mir ergiebt sich dieselbe z. B. aus der leicht zu beweisenden Existenz einer ganzen Zahl Θ, welche (mod. $\mathfrak{p}$) einer irreductibelen Congruenz f^{ten} Grades mit rationalen Coefficienten genügt, und welche man zugleich (für unseren Zweck) so wählen kann, dass sie nicht durch $\mathfrak{p}$, wohl aber durch jedes andere in p aufgehende Primideal theilbar ist; wenn nun $f(t) = \Pi(t - \Theta|\varphi)$, so ist $f(\Theta) = 0$, mithin $f(\Theta^p) \equiv 0$ (mod. $\mathfrak{p}$), folglich $\Theta^p \equiv \Theta|\psi_0$ (mod. $\mathfrak{p}$); wäre ferner $\mathfrak{p}|\psi_0^{-1}$ verschieden von $\mathfrak{p}$, so wäre $\Theta \equiv 0$ (mod. $\mathfrak{p}|\psi_0^{-1}$), also $\Theta|\psi_0 \equiv 0$ (mod. $\mathfrak{p}$), also $\Theta^p \equiv 0$ (mod. $\mathfrak{p}$), also auch $\Theta \equiv 0$ (mod. $\mathfrak{p}$), contra hyp. Also $\mathfrak{p}|\psi_0^{-1} = \mathfrak{p}$; $\mathfrak{p}|\psi_0 = \mathfrak{p}$. Nun ist (zufolge Def. von Θ)

*) [Im wesentlichen wiedergegeben bei Frobenius: Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe. E. N.]

jede ganze Zahl $\omega \equiv F(\Theta)$ (mod. $\mathfrak{p}$), wo $F(t)$ eine ganze Function mit ganzen rationalen Coefficienten; mithin $\omega \,|\, \psi_0 \equiv F(\Theta) \,|\, \psi_0 = F(\Theta \,|\, \psi_0) \equiv F(\Theta^p) \equiv F(\Theta)^p \equiv \omega^p$ (mod. $\mathfrak{p} \,|\, \psi_0 = \mathfrak{p}$).

5. Februar 1883*).

... Ihr thätiges Interesse an der Zahlentheorie ist mir sehr erfreulich, und die grosse Abkürzung der Untersuchung über die Discriminante, die Sie und Hr. Stickelberger aufgefunden haben, gefällt mir besonders deshalb, weil die mir immer unliebsame Zuziehung der Theorie der höheren Congruenzen (mit Variabeln) wieder aufgehoben wird. Ihr rationales $R(\omega)$ ist mir freilich lange bekannt gewesen, aber ich habe nie daran gedacht, es auf so glückliche Weise zu verwenden. Immerhin lege ich aus besonderen, persönlichen Gründen einigen Werth auf den Satz, dass es immer eine reguläre Ordnung giebt, deren Führer durch ein gegebenes Primideal nicht theilbar ist; hierin besteht für mich der letzte Rest und wirkliche Kern ehemaliger Vermuthungen, die zu klären ich lange Zeit gebraucht habe. Zwar weiss ich nicht mehr, ob ich jemals geglaubt habe, jedes System $\mathfrak{o}$ aller in einem Körper Ω enthaltenen ganzen Zahlen sei eine reguläre Ordnung (welcher Fall für die ersten Kummer'schen Untersuchungen so sehr günstig gewesen ist), aber lange Zeit habe ich es für äusserst wahrscheinlich gehalten und kaum bezweifelt, dass es immer reguläre Ordnungen $\mathfrak{n}$ gebe, für welche $(\mathfrak{o}, \mathfrak{n})$ durch eine gegebene rationale Primzahl nicht theilbar ist; meine alten Papiere enthalten viele Beweisversuche, die natürlich immer im Sande verlaufen, bis endlich die bessere Erkenntniss kam; und dann hat es wieder lange gedauert, bis ich (etwa vor zwei Jahren, wie ich glaube) das oben genannte Residuum sicher stellen konnte.

Ihr Kriterium darüber, ob ein Ideal $\mathfrak{k}$ Führer einer Ordnung sein kann, scheint mir mit dem meinigen auch äusserlich fast identisch zu werden, sobald man die Elementartheiler Ihrer Determinante als invariante Theiler der Classenanzahl $(\mathfrak{b}, \mathfrak{a})$ für beliebige Moduln $\mathfrak{a}$, $\mathfrak{b}$ auffasst, die ganz unabhängig von Determinanten definirt werden können und von denen der erste der kleinste Multiplicator

*) [Einige Einzelheiten aus diesem Briefe sind in § 170 der vierten Auflage der Zahlentheorie übernommen; der in dem Briefe gegebene volle Überblick über die Fragen der Modultheorie ist nirgends publiziert. Für den Schluß des Briefes vgl. XXIX. E. N.]

ist, der $\mathfrak{b}$ in ein Multiplum von $\mathfrak{a}$ verwandelt. Sie haben, wie Sie schreiben, aus Ihrer Form noch keinen Nutzen ziehen können für die Beantwortung der Frage nach den Ordnungen, die ein solches Ideal zum Führer haben; dasselbe gilt auch für meine Form. Diese Aufgabe will besonders angegriffen sein. Es leuchtet ein, dass das kleinste gemeinschaftliche Vielfache beliebig vieler Ordnungen $\mathfrak{n}_1, \mathfrak{n}_2 \cdots$ immer wieder eine Ordnung $\mathfrak{n}$ ist, deren Führer $\mathfrak{k}$ zugleich das kleinste gemeinschaftliche Vielfache von den Führern $\mathfrak{k}_1, \mathfrak{k}_2 \cdots$ jener Ordnungen ist; und dieser Satz lässt sich wenigstens dahin umkehren, dass jede Ordnung $\mathfrak{n}$ das kleinste gemeinschaftliche Vielfache solcher Ordnungen $\mathfrak{n}_1, \mathfrak{n}_2 \cdots$ ist, für welche $(\mathfrak{o}, \mathfrak{n}_1)$, $(\mathfrak{o}, \mathfrak{n}_2) \cdots$ die verschiedenen in $(\mathfrak{o}, \mathfrak{n})$ aufgehenden höchsten Primzahlpotenzen sind; dadurch wird die Untersuchung auf die Betrachtung solcher Ordnungsführer $\mathfrak{k}$ zurückgeführt, deren Normen Primzahlpotenzen sind. Die nähere Untersuchung, die mehr lästig, als principiell schwierig ist, ergiebt eine große Reichhaltigkeit; die Grundlage bildet der einfachste Fall, wo $\mathfrak{k}$ ein Primideal $\mathfrak{p}$ vom Grade f ist: die Anzahl der verschiedenen Ordnungen $\mathfrak{n}$, welche $\mathfrak{p}$ zum Führer haben, ist um eins kleiner, als die Anzahl der Divisoren m von f; jedem echten Divisor m entspricht eine Ordnung $\mathfrak{n}$, welche aus den sämmtlichen Wurzeln ν der Congruenz

$$\nu^{p^m} \equiv \nu \pmod{\mathfrak{p}}$$

besteht; $(\mathfrak{n}, \mathfrak{p}) = p^m$; $N(\mathfrak{p}) = p^f$.

Diese Untersuchung bildet ein Capitel der allgemeinen Theorie der n-gliedrigen Moduln in einem Körper n^{ten} Grades, welche in meiner Gauss-Festschrift (1877), wie ich dort ausdrücklich bemerkt habe, keineswegs vollständig behandelt ist; aber ihre wichtigsten Grundlagen sind doch in dieser Schrift enthalten. Es kommt hierbei auf den Unterschied zwischen umkehrbaren und nicht umkehrbaren Moduln an; ich nenne einen Modul $\mathfrak{a}$ umkehrbar (auch im allgemeinsten Sinn des Worts Modul), wenn ein Modul $\mathfrak{b}$ existirt, für welchen $\mathfrak{a}\mathfrak{b} = \mathfrak{a}^0$, d. h. gleich der Ordnung von $\mathfrak{a}$ wird; alle solche Moduln $\mathfrak{b}$ liefern ein und dasselbe Product $\mathfrak{b}\mathfrak{a}^0$, das ich mit $\mathfrak{a}^{-1}$ bezeichne, und dessen Ordnung immer $= \mathfrak{a}^0$ ist; jedes Product von umkehrbaren Moduln ist wieder ein umkehrbarer Modul, und seine Ordnung ist das Product aus den Ordnungen der Factoren. Unter den n-gliedrigen Moduln eines Körpers Ω vom Grade n sind die einfachsten die Moduln, deren Ordnung $= \mathfrak{o}$; sie sind alle umkehrbar und identisch

mit den Ideal-Quotienten; die Regeln ihrer Multiplication und Division stimmen genau mit denjenigen für rationale Brüche überein; die Definition der Norm ist selbstverständlich. Ähnliches (mit Modification) gilt für die Moduln einer jeden regulären, allgemeiner jeder solchen Ordnung $\mathfrak{n}$, deren Complement $\mathfrak{n}'$ umkehrbar ist (weil für jeden solchen Modul $\mathfrak{a}$ immer $\mathfrak{a}\mathfrak{a}' = \mathfrak{n}'$ ist). Aber sobald $n > 2$ ist, haben durchaus nicht mehr alle Ordnungen diese Eigenschaft. Ist nun $\mathfrak{m}$ ein beliebiger Modul, $\mathfrak{n}$ seine Ordnung, so ist $\mathfrak{m}\mathfrak{o}$ immer ein Modul der Ordnung $\mathfrak{o}$, also ein Ideal-Quotient, und der Führer von $\mathfrak{m}$, d. h. der Quotient $\frac{\mathfrak{m}}{\mathfrak{o}}$ ist $= \mathfrak{f}\mathfrak{m}$, wo $\mathfrak{f}$ der Führer von $\mathfrak{n}$; $N(\mathfrak{m})$ wird definirt als $N(\mathfrak{m}\mathfrak{o})$. Umgekehrt, ist $\mathfrak{a}$ ein Modul der Ordnung $\mathfrak{o}$, so folgt aus der Festschrift (1877) die wichtige Existenz mindestens eines umkehrbaren Moduls $\mathfrak{m}$ jeder Ordnung $\mathfrak{n}$, für welchen $\mathfrak{m}\mathfrak{o} = \mathfrak{a}$ wird; und die sämmtlichen Moduln $\mathfrak{m}_1$ derselben Ordnung $\mathfrak{n}$, welche derselben Forderung $\mathfrak{m}_1\mathfrak{o} = \mathfrak{a}$ genügen, sind die sämmtlichen Producte $\mathfrak{m}\mathfrak{e}$, wo $\mathfrak{e}$ alle diejenigen Moduln der Ordnung $\mathfrak{n}$ durchläuft, für welche $\mathfrak{e}\mathfrak{o} = \mathfrak{o}$ wird. Der Reichthum an solchen Moduln $\mathfrak{e}$ ist sehr gross; sie sind natürlich lauter ganze Moduln, d. h. Vielfache von $\mathfrak{o}$, und zugleich Theiler des Führers $\mathfrak{f}$, da $\frac{\mathfrak{e}}{\mathfrak{o}} = \frac{\mathfrak{n}}{\mathfrak{o}} = \mathfrak{f}$ ist.

Hierin bestehen, wenn ich mich recht erinnere, die hauptsächlichsten Gedanken der genannten Theorie, die ich übrigens noch niemals vollständig ausgearbeitet habe; doch hoffe ich, Ihnen nichts Unrichtiges geschrieben zu haben. Wichtig ist diese Theorie, und namentlich scheint sie unerlässlich für die Aufstellung der allgemeinsten Gesetze, welche die bisher bekannten, sogenannten Reciprocitätssätze in sich schliessen. Bei cubischen Körpern Ω z. B. kommt die Primideal-Zerlegung derjenigen rationalen Primzahlen p, von denen die Grundzahl $D = \Delta(\Omega)$ quadratischer Rest ist (die übrigen p machen keine Schwierigkeit), auf die Betrachtung der ursprünglichen quadratischen Formen $(a, \frac{1}{2}b, c)$ zurück, deren Discriminante $b^2 - 4ac = D$ ist; die Anzahl der Classen dieser Formen oder der entsprechenden Modul-Classen ist immer durch 3 theilbar, und ein gewisses Drittel dieser Classen bildet eine Gruppe; je nachdem p durch eine Form dieser Gruppe darstellbar ist oder nicht, ist $\mathfrak{o}p$ in Ω ein Product von drei Primidealen ersten Grades oder ein Primideal dritten Grades. Für negative D hängt dies mit der complexen Multiplication der

elliptischen Functionen zusammen, was auch Kronecker vollständig erkannt zu haben scheint. Ich habe diesen Satz, der ohne jeden Zweifel ganz allgemein, auch für positive D gilt, vor 11 Jahren durch Induction gefunden (Schlömilch's Zeitschrift, Jahrgang 18; 1873. Literaturzeitung S. 22 und S. 43, wo der durch die Schuld des Herrn Schlömilch ausgelassene Zusatz steht), gestehe aber gern, dass ich ihn noch nicht für alle Fälle bewiesen habe; doch hoffe ich dies noch zu erreichen. Er gilt sogar, wenn D eine positive Quadratzahl, mithin Ω ein Normalkörper ist, der aus der Kreistheilung entspringt. Ich glaube gewiss, man wird dereinst ganz allgemeine Gesetze finden, welche gestatten, die Primideale eines Körpers unmittelbar abzuleiten aus seiner Discriminante und seinen übrigen Invarianten (die auch Ideale verwandter Körper sein können); doch mögen wir wohl noch recht weit von diesem Ziele entfernt sein! In den letzten Jahren habe ich mich sehr wenig mit diesen Fragen beschäftigt, zu denen ich aber grosse Lust habe zurückzukehren, weil sie mir von allen die interessantesten zu sein scheinen. . . .

8. Februar 1895*).

. . . Auf Ihre Arbeit über die Gruppen bin ich sehr gespannt, da die Einfachheit Ihrer Methoden, unter Anderem Ihr Beweis, dass in einer Gruppe, deren Grad durch die Primzahl p theilbar ist, es immer ein Element p^{ter} Ordnung giebt, mich sehr erfreut hat; ich war in den ersten Jahren meiner Gruppen-Studien (1855—1858) auf einem viel umständlicheren Wege dahin gekommen. Auch später habe ich gewisse Gruppen-Fragen immer nur so weit verfolgt, wie es Veranlassungen von anderer Seite her mit sich brachten; sollte es also der Zufall wollen, dass ich mich mit dem Gegenstande Ihrer Arbeit schon jemals beschäftigt hätte, so würde ich doch gewiss weit hinter Ihnen zurückgeblieben sein. Um auf gut Glück zu rathen, frage ich: drängen sich in Ihre Untersuchung auch übercomplexe Grössen ein mit nicht commutativer Multiplication? Doch will ich Sie keineswegs mit der Bitte um eine Antwort bemühen, die

*) [Die jetzt folgenden Briefstellen geben einen wesentlichen Beitrag zur Geschichte der Theorie der hyperkomplexen Größen und der Gruppendeterminante. Auf die Rolle, die Dedekind in dieser Theorie gespielt hat, weist Frobenius an verschiedenen Stellen hin, in den Einleitungen zu den Arbeiten über Gruppencharaktere, über die Primfaktoren der Gruppendeterminante und über die Darstellung der endlichen Gruppen. E. N.]

ich am besten durch Ihre Abhandlung erhalten werde. Ihre äusserst scharfsinnige Untersuchung über die Elementartheiler der Determinanten habe ich mit grossem Interesse studirt; ich leugne nicht, dass ich bei dem Beweise in §. 1 die unbestimmte Empfindung habe, als könnte er auch wohl ohne die Gleichung (6) auf S. 4 gelingen, aber ich bin ganz ausser Stande, etwas Anderes an die Stelle zu setzen. . . .

12. Februar 1895.

. . . Keine Entschuldigung habe ich für meine gewagte Bemerkung bezüglich Ihrer Abhandlung über die Elementartheiler — die unbestimmte Empfindung entspringt aus einer in diesem Falle wohl sehr thörichten Abneigung gegen Potenzen-Folgen — um so mehr muss ich um Nachsicht wegen deren Äusserung bitten. Auch meine Frage wegen der Benutzung übercomplexer Grössen in der Gruppen-Theorie war sehr dreist; sie ging hervor aus einer Beobachtung, die ich im Februar 1886 gemacht, dann aber nicht weiter verfolgt habe, obwohl sie mir merkwürdig genug erschien; vielleicht darf ich mir einmal erlauben, sie Ihnen vorzulegen, auf die Gefahr hin, dass sie vor Ihrer Kritik gänzlich dahin schwindet, möglicherweise auch gar nicht einmal neu ist. . . .

25. März 1896.

. . . Da ich einmal von Gruppen spreche, so möchte ich noch eine andere Betrachtung erwähnen, auf die ich im Februar 1886 gekommen bin. Zu jeder Gruppe n^{ten} Grades G bilde ich eine Form n^{ten} Grades H mit n Variabelen, die ich die Determinante von G nenne: sind $1, 2 \cdots n$ die in irgend einer Ordnung aufgeschriebenen Elemente von G, so lasse ich jedem Elemente r der Gruppe G eine Variabele x_r entsprechen, und bilde die Determinante

$$H = \begin{vmatrix} x_{11'}, & x_{21'} \cdots x_{n1'} \\ x_{12'}, & x_{22'} \cdots x_{n2'} \\ \cdot & \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \\ x_{1n'}, & x_{2n'} \cdots x_{nn'} \end{vmatrix},$$

wo r' das zu r reciproke Element von G bedeutet. Ist G eine Abel'sche Gruppe, und sind $\psi', \psi'' \cdots \psi^{(n)}$ die ihr entsprechenden Charaktere (Einheitswurzeln), so ist die Determinante H eine zerlegbare Form, nämlich das Product der n linearen Factoren

$$\sum_{r}^{r} \psi^{(s)}(r)\, x_r = \psi^{(s)}(1)\, x_1 + \cdots + \psi^{(s)}(n)\, x_n,$$

die den n Werthen von s entsprechen (ein Satz, welcher in dieser Allgemeinheit, wie ich glaube, noch nicht ausgesprochen ist). Wenn aber G keine Abel'sche Gruppe ist, so besitzt ihre Determinante H, soweit ich es untersucht habe, ausser linearen Factoren (wie z. B. immer $x_1 + x_2 + \cdots + x_n$) auch Factoren höheren Grades, die im gewöhnlichen Sinne unzerlegbar sind; aber diese werden wieder zerlegbar in lineare Factoren, wenn man ausser den gewöhnlichen Zahlen als Coefficienten auch übercomplexe Zahlen (mit nicht commutativer Multiplication) gestattet, die den Gesetzen der Gruppe G entsprechen. Bei der obigen Quaternion-Gruppe Q z. B. treten auf diese Weise bei der erzwungenen Zerlegung ihrer Determinante in lineare Factoren (deren vier gewöhnliche Coefficienten haben) in der That Hamilton's Quaternion-Zahlen auf. Man darf überhaupt wohl vermuthen, dass die Eigenschaften einer Gruppe G hinsichtlich ihrer Theiler sich in der Zerlegung ihrer Determinante H wiederspiegeln werden; ausser einer Spur, die auf einen Zusammenhang zwischen der Anzahl der gewöhnlichen linearen Factoren von H und denjenigen Normaltheilern A von G hindeutet, welche die Eigenschaft $Ars = Asr$ besitzen, habe ich aber noch gar Nichts gefunden, und es ist überhaupt wohl möglich, dass bei der ganzen Sache vorläufig wenig herauskommen wird. ...

3. April 1896.

... Erwähnen möchte ich noch Folgendes*). Man sieht leicht, dass Q durch 24 Transformationen, bei welchen sich nur die sechs Buchstaben α, α^{-1}, β, β^{-1}, γ, γ^{-1} mit einander vertauschen, isomorph in sich selbst übergeht; die Gruppe T dieser Transformationen ist also eine Untergruppe von der Gruppe V_6 aller 720 Versetzungen von 6 Elementen, und zwar habe ich gefunden, dass diese Gruppe T isomorph ist mit der Gruppe V_4 aller 24 Versetzungen von 4 Elementen a, b, c, d. Bezeichnet man nämlich allgemein mit (a, d) die Vertauschung (Transposition) von nur zwei verschiedenen Elementen a, d, so wird die Gruppe T erzeugt durch die drei Elemente zweiten Grades

$$(\alpha, \alpha^{-1})\,(\beta, \gamma)\,(\beta^{-1}, \gamma^{-1}) \equiv (a, d),$$
$$(\beta, \beta^{-1})\,(\gamma, \alpha)\,(\gamma^{-1}, \alpha^{-1}) \equiv (b, d),$$
$$(\gamma, \gamma^{-1})\,(\alpha, \beta)\,(\alpha^{-1}, \beta^{-1}) \equiv (c, d),$$

*) [Es war hier und im vorangehenden Brief ein Überblick über die Arbeit XXVII über Gruppen, deren sämtliche Teiler normal sind, vorangegangen; Q bedeutet die Quaternionengruppe. E. N.]

wo das Zeichen $\equiv$ das isomorphische Entsprechen bedeuten soll. Dass die Gruppe V_6 eine solche transitive Untergruppe $T \equiv V_4$ (vom Index 30) besitzt, wird wohl schon lange bekannt sein; jedenfalls soll dies von meinem Aufsatz über die Hamilton'schen Gruppen ausgeschlossen werden.

Ebenso wenig werde ich dort von der allgemeinen Bedeutung der Commutatoren $\psi^{-1}\varphi^{-1}\psi\varphi$ sprechen, auf welche ich vor vielen Jahren bei der Aufgabe gekommen bin, aus irgend einem Normal-Körper alle darin enthaltenen Abel'schen Körper auszuscheiden. Man findet leicht (— was, wie ich aus Ihrem Briefe schliesse, auch Ihnen gewiss bekannt ist —) den Satz: „Die erforderliche und hinreichende Bedingung dafür, dass A ein invarianter Theiler der Gruppe G, und zugleich G/A eine Abel'sche Gruppe ist ($Ars = Asr$), besteht darin, dass alle Commutatoren von je zwei Elementen r, s der Gruppe G in der Gruppe A enthalten sind; die kleinste solche Gruppe A (diejenige nämlich, welche durch alle Commutatoren erzeugt wird) ist der gemeinsame Theiler von allen A." Ich erwähne dies auch nur, um nochmals auf die von Ihnen günstig aufgenommene Determinante H irgend einer Gruppe G zurückzukommen, welche ich vor 10 Jahren an einigen sehr speciellen Beispielen (V_3 vom Grade 6, Q vom Grade 8) und einigen allgemeineren (complexe Multiplication) untersucht habe. Auf Ihre Anfrage wegen des einen Punctes gestehe ich, dass ich nichts Bestimmtes weiss, aber ich vermuthe allerdings, dass die Anzahl der linearen Factoren der Determinante H der Index der eben genannten kleinsten Gruppe A, also der Grad der Abel'schen Gruppe G/A ist, und dass diese Factoren in gewisser Weise den Charakteren dieser letzteren Gruppe entsprechen. Es würde mich sehr freuen, wenn Sie sich in diese Dinge versenken wollten, weil ich deutlich fühle, dass ich hier Nichts zu Stande bringen werde. Dass Ihre Determinante der Charakteristiken-Gruppe in den Thetafunctionen wesentlich mit meinem H übereinstimmt (besser umgekehrt), scheint mir nach Einblick in Ihre Abhandlung (Crelle 96, S. 100) ganz unzweifelhaft, und Ihnen gebührt daher auch die volle Priorität für diese Gruppen-Determinanten*). Was den Fall der Abel'schen

*) [Frobenius erwähnt in der Arbeit über die Primfaktoren der Gruppendeterminante, daß er vom Additionstheorem aus, und nicht durch die Gruppe der Relationen, auf die Determinante der Charakteristiken gekommen sei. E. N.]

Gruppen betrifft, so habe ich wohl in den Wiener Sitzungs-Berichten einige darauf bezügliche Aufsätze (von Gegenbauer?) gesehen; doch glaube ich nicht, dass der Satz in seiner Allgemeinheit dort ausgesprochen ist....

6. April 1896.

... Für den Fall, dass Sie sich noch näher mit den Gruppen-Determinanten beschäftigen wollen, erlaube ich mir hiermit, Ihnen wenigstens zwei von den Beispielen zu senden, die ich im Februar 1886 ausgerechnet habe; doch übergehe ich die übercomplexe Zerlegung der nicht linearen Factoren.

Beispiel 1.

Gruppe V_3 der sechs Versetzungen von drei Buchstaben a, b, c.

Bezeichnung und Composition der Substitutionen:

	a	b	c
1	a	b	c
2	b	c	a
3	c	a	b
4	a	c	b
5	c	b	a
6	b	a	c

	1^{-1}	2^{-1}	3^{-1}	4^{-1}	5^{-1}	6^{-1}
1	1	3	2	4	5	6
2	2	1	3	5	6	4
3	3	2	1	6	4	5
4	4	5	6	1	3	2
5	5	6	4	2	1	3
6	6	4	5	3	2	1

Setzt man $1 + \varrho + \varrho^2 = 0$

und
$$u = x_1 + x_2 + x_3, \qquad v = x_4 + x_5 + x_6,$$
$$u_1 = x_1 + \varrho\, x_2 + \varrho^2 x_3, \qquad v_1 = x_4 + \varrho\, x_5 + \varrho^2 x_6,$$
$$u_2 = x_1 + \varrho^2 x_2 + \varrho\, x_3, \qquad v_2 = x_4 + \varrho^2 x_5 + \varrho\, x_6,$$

so wird die Gruppen-Determinante

$$\begin{vmatrix} x_1 & x_3 & x_2 & x_4 & x_5 & x_6 \\ x_2 & x_1 & x_3 & x_5 & x_6 & x_4 \\ x_3 & x_2 & x_1 & x_6 & x_4 & x_5 \\ x_4 & x_5 & x_6 & x_1 & x_3 & x_2 \\ x_5 & x_6 & x_4 & x_2 & x_1 & x_3 \\ x_6 & x_4 & x_5 & x_3 & x_2 & x_1 \end{vmatrix} = (u + v)\,(u - v)\,(u_1 u_2 - v_1 v_2)^2$$

am kürzesten wohl durch Multiplication mit der Determinante

$$\begin{vmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \varrho & \varrho^2 & 1 & \varrho & \varrho^2 \\ 1 & \varrho^2 & \varrho & 1 & \varrho^2 & \varrho \\ 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & \varrho & \varrho^2 & -1 & -\varrho & -\varrho^2 \\ 1 & \varrho^2 & \varrho & -1 & -\varrho^2 & -\varrho \end{vmatrix} = 6^3 = 216.$$

Die Gruppe $1 + 2 + 3$ der Commutatoren hat den Index zwei, gleich der Anzahl der linearen Factoren.

Beispiel 2.

Bezeichnet man die Elemente $1, \varepsilon, \alpha, \alpha^{-1}, \beta, \beta^{-1}, \gamma, \gamma^{-1}$ der Quaternion-Gruppe Q mit 1, 2, 3, 4, 5, 6, 7, 8, so ist die entsprechende Gruppen-Determinante

$$\begin{vmatrix} x_1 & x_2 & x_4 & x_3 & x_6 & x_5 & x_8 & x_7 \\ x_2 & x_1 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \\ x_3 & x_4 & x_1 & x_2 & x_8 & x_7 & x_5 & x_6 \\ x_4 & x_3 & x_2 & x_1 & x_7 & x_8 & x_6 & x_5 \\ x_5 & x_6 & x_7 & x_8 & x_1 & x_2 & x_4 & x_3 \\ x_6 & x_5 & x_8 & x_7 & x_2 & x_1 & x_3 & x_4 \\ x_7 & x_8 & x_6 & x_5 & x_3 & x_4 & x_1 & x_2 \\ x_8 & x_7 & x_5 & x_6 & x_4 & x_3 & x_2 & x_1 \end{vmatrix}$$

$$= \begin{vmatrix} u_1 & u_2 & u_3 & u_4 \\ u_2 & u_1 & u_4 & u_3 \\ u_3 & u_4 & u_1 & u_2 \\ u_4 & u_3 & u_2 & u_1 \end{vmatrix} \times \begin{vmatrix} v_1 & -v_2 & -v_3 & -v_4 \\ v_2 & v_1 & -v_4 & v_3 \\ v_3 & v_4 & v_1 & -v_2 \\ v_4 & -v_3 & v_2 & v_1 \end{vmatrix}$$

$$= \begin{cases} (u_1 + u_2 + u_3 + u_4)\,(u_1 + u_2 - u_3 - u_4)\,(u_1 - u_2 + \\ \quad + u_3 - u_4)(u_1 - u_2 - u_3 + u_4) \\ \quad \times (v_1^2 + v_2^2 + v_3^2 + v_4^2)^2, \end{cases}$$

wo

$$\begin{Bmatrix} u_1 \\ v_1 \end{Bmatrix} = x_1 \pm x_2, \quad \begin{Bmatrix} u_2 \\ v_2 \end{Bmatrix} = x_3 \pm x_4, \quad \begin{Bmatrix} u_3 \\ v_3 \end{Bmatrix} = x_5 \pm x_6, \quad \begin{Bmatrix} u_4 \\ v_4 \end{Bmatrix} = x_7 \pm x_8.$$

Die Anzahl vier der linearen Factoren ist zugleich der Index der Commutator-Gruppe $[2] = 1 + 2$. Die Quadratsumme $v_1^2 + v_2^2$

$+ v_3^2 + v_4^2$ hat mich damals sehr erfreut und dazu veranlasst, auch andere Gruppen-Determinanten in lineare Factoren mit übercomplexen Coefficienten zu zerlegen; dies gelingt zwar, aber herausgekommen ist dabei Nichts!

Mit dem Wunsche, dass diese immerhin merkwürdigen Erscheinungen Sie zu einer tieferen Ergründung reizen mögen, verbleibe ich ...

27. April 1896.

... Aber so viel sehe ich zu meiner unaussprechlichen Freude auch jetzt schon, dass Sie in raschem Siegeslaufe wahrhaft bewunderungswürdige Erfolge errungen haben, und wenn ich heute auch ausser Stande bin, über die Sache selbst zu schreiben, so will ich doch nicht länger zögern, Ihnen meine herzlichsten Glückwünsche zu diesen Erfolgen zu senden, denen ich eine sehr hohe Bedeutung für die Gruppen-Theorie zuschreibe. Meine Bewunderung ist um so grösser, je aufrichtiger ich mir eingestehen muss, dass ich nimmermehr zu solchen Erfolgen hätte gelangen können, weil meiner gar zu einseitigen Bildung das erforderliche Rüstzeug fehlt, das Sie wie kein Anderer beherrschen. Ich würde daher auch Bedenken tragen, die beiliegenden Bogen Ihrer Einsicht zu unterbreiten, aber da Sie mich in einem Ihrer Briefe zur Mittheilung fernerer Beispiele von Gruppen-Determinanten aufgefordert haben, so sende ich Ihnen hierbei ein altes Beispiel 3. und ein daraus durch Verallgemeinerung kürzlich entstandenes Beispiel 4. auf die Gefahr hin, dass Sie über meine ungeübte Handhabung der Technik lächeln werden. Von der schon mehrmals erwähnten Zerlegung in hypercomplexe lineare Factoren, die, wie schwach sie mir augenblicklich auch erscheint, doch vielleicht den Keim von etwas Brauchbarem enthalten kann, werde ich mir ein anderes Mal zu schreiben erlauben, wenn mein Denken sich gebessert hat. ...

Gruppen-Determinanten.

Beispiel 3 (vom 17. Februar 1886).

Verallgemeinerung von Beispiel 1. — Es sei $\mathfrak{A}$ eine Abel'sche Gruppe von m Elementen

$$\alpha = 1, 2, 3 \cdots m,$$

und es seien

$$\psi = \psi_1, \psi_2, \psi_3 \cdots \psi_m$$

die Charaktere von $\mathfrak{A}$ (Dirichlet, Aufl. 3, S. 581; Aufl. 4, S. 612); dieselben bilden eine (mit $\mathfrak{A}$ isomorphe) Gruppe in der Weise, dass je zwei solche ψ', ψ'' einen Charakter $\psi'\psi''$ erzeugen, welcher durch $\psi'\psi''(\alpha) = \psi'(\alpha)\psi''(\alpha)$ für alle α definirt ist; $\psi^{-1}(\alpha) = \psi(\alpha^{-1})$; $\psi\psi^{-1} = \psi^0$ ist der Haupt-Charakter, $\psi^0(\alpha) = 1$ für alle α und alle ψ. Die aus den m^2 Einheits-Wurzeln $\psi(\alpha)$ gebildete Determinante

$$\Psi = \begin{vmatrix} \psi_1(1) & \cdots & \psi_1(m) \\ \cdot & \cdots & \cdot \\ \psi_m(1) & \cdots & \psi_m(m) \end{vmatrix} = \pm\Psi' = \pm \begin{vmatrix} \psi_1^{-1}(1) & \cdots & \psi_1^{-1}(m) \\ \cdot & \cdots & \cdot \\ \psi_m^{-1}(1) & \cdots & \psi_m^{-1}(m) \end{vmatrix}$$

ist von Null verschieden; $\Psi\Psi' = m^m$. —

Nun bilde ich aus $\mathfrak{A}$ durch Hinzufügung eines Elementes zweiter Ordnung β, welches sich mit den α nach dem Gesetze

$$\beta\alpha = \alpha^{-1}\beta$$

verbindet, das System

$$\mathfrak{G} = \mathfrak{A} + \mathfrak{A}\beta,$$

welches, wie man leicht sieht (vergl. das folgende Beispiel 4), eine Gruppe ist (im Beispiel 1. war $m = 3$). Es soll die Determinante D dieser Gruppe $\mathfrak{G}$ gebildet werden, also eine Function von $2m$ Variabelen x_α, y_α, die resp. den Elementen α, $\alpha\beta$ entsprechen, nämlich

$$D = \left|\begin{array}{ccc|ccc} x_{11^{-1}} & \cdots & x_{m1^{-1}} & y_{11} & \cdots & y_{m1} \\ \cdot & \cdots & \cdot & \cdot & \cdots & \cdot \\ x_{1m^{-1}} & \cdots & x_{mm^{-1}} & y_{1m} & \cdots & y_{mm} \\ \hline y_{11} & \cdots & y_{m1} & x_{11^{-1}} & \cdots & x_{m1^{-1}} \\ \cdot & \cdots & \cdot & \cdot & \cdots & \cdot \\ y_{1m} & \cdots & y_{mm} & x_{1m^{-1}} & \cdots & x_{mm^{-1}} \end{array}\right|$$

Um sie umzuformen, multiplicire ich sie zeilenweise mit

$$\Psi\Psi' = \left|\begin{array}{ccc|ccc} \psi_1(1) & \cdots & \psi_1(m) & 0 & \cdots & 0 \\ \cdot & \cdots & \cdot & \cdot & \cdots & \cdot \\ \psi_m(1) & \cdots & \psi_m(m) & 0 & \cdots & 0 \\ \hline 0 & \cdots & 0 & \psi_1^{-1}(1) & \cdots & \psi_1^{-1}(m) \\ \cdot & \cdots & \cdot & \cdot & \cdots & \cdot \\ 0 & \cdots & 0 & \psi_m^{-1}(1) & \cdots & \psi_m^{-1}(m) \end{array}\right|$$

und zwar (wie immer im Folgenden) in der Weise, dass die Spalte des Productes durch die Zeile des Multiplicands D, die Zeile des

Productes durch die Zeile des Multiplicators $\mathfrak{P}\mathfrak{P}'$ bestimmt wird; führt man noch die Bezeichnungen

$$u_\mu = \sum^{\alpha} x_\alpha \psi_\mu(\alpha), \qquad v_\mu = \sum^{\alpha} y_\alpha \psi_\mu(\alpha),$$
$$u'_\mu = \sum^{\alpha} x_\alpha \psi_\mu^{-1}(\alpha), \qquad v'_\mu = \sum^{\alpha} y_\alpha \psi_\mu^{-1}(\alpha)$$

ein, so wird das Product

$$D_{\mathfrak{P}\mathfrak{P}'} = \left|\begin{array}{c|c} u_1\,\psi_1(1)\cdots u_1\,\psi_1(m) & v_1\,\psi_1^{-1}(1)\cdots v_1\,\psi_1^{-1}(m) \\ \cdots\cdots\cdots & \cdots\cdots\cdots \\ u_m\,\psi_m(1)\cdots u_m\,\psi_m(m) & v_m\,\psi_m^{-1}(1)\cdots v_m\,\psi_m^{-1}(m) \\ \hline v'_1\,\psi_1(1)\cdots v'_1\,\psi_1(m) & u'_1\,\psi_1^{-1}(1)\cdots u'_1\,\psi_1^{-1}(m) \\ \cdots\cdots\cdots & \cdots\cdots\cdots \\ v'_m\,\psi_m(1)\cdots v'_m\,\psi_m(m) & u'_m\,\psi_m^{-1}(1)\cdots u'_m\,\psi_m^{-1}(m) \end{array}\right|.$$

Diese Determinante ist aber zugleich das Product aus Multiplicand

$$\mathfrak{P}\mathfrak{P}' = \left|\begin{array}{ccc|ccc} \psi_1(1) & \cdots & \psi_m(1) & 0 & \cdots & 0 \\ \cdots & & \cdots & \cdots & & \cdots \\ \psi_1(m) & \cdots & \psi_m(m) & 0 & \cdots & 0 \\ \hline 0 & \cdots & 0 & \psi_1^{-1}(1) & \cdots & \psi_m^{-1}(1) \\ \cdots & & \cdots & \cdots & & \cdots \\ 0 & \cdots & 0 & \psi_1^{-1}(m) & \cdots & \psi_m^{-1}(m) \end{array}\right|$$

und Multiplicator

$$\prod^{\mu}(u_\mu u'_\mu - v_\mu v'_\mu) = \left|\begin{array}{ccc|ccc} u_1 & \cdots & 0 & v_1 & \cdots & 0 \\ \cdots & & \cdots & \cdots & & \cdots \\ 0 & \cdots & u_m & 0 & \cdots & v_m \\ \hline v'_1 & \cdots & 0 & u'_1 & \cdots & 0 \\ \cdots & & \cdots & \cdots & & \cdots \\ 0 & \cdots & v'_m & 0 & \cdots & u'_m \end{array}\right|.$$

Mithin ist unsere Gruppen-Determinante

$$D = \prod^{\mu}(u_\mu u'_\mu - v_\mu v'_\mu) = \prod^{\mu}\left|\begin{array}{cc} u_\mu, & v_\mu \\ v'_\mu, & u'_\mu \end{array}\right|$$

zunächst ein Product von m Factoren zweiten Grades. Bedeutet nun a die Anzahl der zweiseitigen (ambigen) Elemente $\alpha = \alpha^{-1}$ der Gruppe $\mathfrak{A}$, so ist $m = aa'$, wo a' die Anzahl aller verschiedenen

Quadrate α^2 bedeutet. Zugleich ist a die Anzahl aller zweiseitigen Charaktere $\psi = \psi^{-1}$; dies folgt unmittelbar aus der oben erwähnten Isomorphie der Gruppe $\mathfrak{A}$ mit der ihrer Charaktere, oder auch aus der Betrachtung der Gruppe $\mathfrak{A}'$ der a' Quadrate α^2, weil ihr Index $(\mathfrak{A}', \mathfrak{A}) = a$ nach einem allgemeinen Satz zugleich die Anzahl derjenigen Charaktere ψ von $\mathfrak{A}$ sein muß, welche den Haupt- (oder jeden anderen bestimmten) Charakter der Untergruppe $\mathfrak{A}'$ in sich schliessen, also die Eigenschaft $\psi(\alpha^2) = 1$, d. h. $\psi = \psi^{-1}$ haben. Für jeden zweiseitigen Charakter ψ_μ wird $u'_\mu = u_\mu$, $v'_\mu = v_\mu$, also $u_\mu u'_\mu - v_\mu v'_\mu = (u_\mu + v_\mu)(u_\mu - v_\mu)$, woraus $2a$ verschiedene lineare Factoren von D entspringen. Die übrigen $m - a$ Charaktere zerfallen in $\frac{1}{2}(m - a)$ Paare ψ_μ und $\psi_{\mu'} = \psi_\mu^{-1}$, und da $u_{\mu'} = u'_\mu$, $v_{\mu'} = v'_\mu$, $u'_{\mu'} = u_\mu$, $v'_{\mu'} = v_\mu$, so entspricht jedem Paar das Quadrat $(u_\mu u'_\mu - v_\mu v'_\mu)^2$ einer quadratischen Function, welche (im gewöhnlichen Sinne) unzerlegbar ist. Die Commutatoren von je zwei Elementen der Gruppe $\mathfrak{G}$ sind, wie man leicht findet, die a' Quadrate α^2; die von ihnen gebildete Gruppe $\mathfrak{A}'$ hat in $\mathfrak{G}$ den Index $(\mathfrak{A}', \mathfrak{G}) = (\mathfrak{A}', \mathfrak{A})(\mathfrak{A}, \mathfrak{G}) = 2a$, welcher mit der Anzahl der linearen Factoren von D übereinstimmt. —

Gruppen-Determinanten.

Beispiel 4 (vom 18. April 1896).

Verallgemeinerung von Beispiel 3. — Zu der Abel'schen Gruppe $\mathfrak{A}$ von m Elementen α (und m Charakteren ψ) lasse ich eine beliebige Gruppe $\mathfrak{B}$ von n Elementen β hinzutreten, welche sich mit jenen nach dem Gesetze

$$\beta\alpha = \alpha^{\beta'}\beta \tag{1}$$

verbinden, unter der Annahme, dass die den n Elementen β entsprechenden n Exponenten β' relative Primzahlen zu m sind und dem Gesetze

$$(\beta_1\beta_2)' \equiv \beta'_1\beta'_2 \pmod{m} \tag{2}$$

genügen. Ich nehme ferner an, dass $\mathfrak{A}$ und $\mathfrak{B}$ nur das Haupt-Element $\alpha^0 = \beta^0$ gemeinsam haben; dann bildet der aus mn verschiedenen Elementen $\alpha\beta$ bestehende Complex

$$\mathfrak{G} = \mathfrak{A}\mathfrak{B} \tag{3}$$

eine Gruppe. Dies ergiebt sich am deutlichsten, wenn man die Gruppen $\mathfrak{A}, \mathfrak{B}$ zunächst ganz getrennt betrachtet und jeder Combination

eines Elementes α von $\mathfrak{A}$ mit einem Elemente β von $\mathfrak{B}$ ein etwa mit (α, β) zu bezeichnendes Element eines neuen Systems $\mathfrak{G}$ entsprechen läßt, mit der Bedingung, daß diese mn Elemente (α, β) alle von einander verschieden sein sollen (der Einfachheit wegen); die Composition dieser Elemente definire man durch

$$(4) \qquad (\alpha_1, \beta_1)(\alpha_2, \beta_2) = (\alpha_1 \alpha_2^{\beta_1'}, \beta_1 \beta_2),$$

so ist $\mathfrak{G}$ wirklich eine Gruppe. Denn erstens gehorcht diese Composition (4) zufolge (2) dem associativen Gesetz; zweitens ist

$$(5) \qquad (\alpha^0, \beta^0)(\alpha, \beta) = (\alpha, \beta)(\alpha^0, \beta^0) = (\alpha, \beta),$$

weil $(\beta^0)' \equiv 1 \pmod{m}$; definirt man ferner die n Zahlen β'' durch

$$(6) \qquad \beta' \beta'' \equiv 1 \pmod{m},$$

woraus auch

$$(7) \qquad (\beta_1 \beta_2)'' \equiv \beta_1'' \beta_2'' \pmod{m}$$

folgt, so ist drittens

$$(8) \qquad (\alpha, \beta)(\alpha^{-\beta''}, \beta^{-1}) = (\alpha^{-\beta''}, \beta^{-1})(\alpha, \beta) = (\alpha^0, \beta^0).$$

Hiermit ist die Gruppen-Eigenschaft von $\mathfrak{G}$ bekanntlich erwiesen, und man kann

$$(9) \qquad (\alpha, \beta)^0 = (\alpha^0, \beta^0), \qquad (\alpha, \beta)^{-1} = (\alpha^{-\beta''}, \beta^{-1})$$

setzen. Zufolge (4) ist nun

$$(10) \qquad (\alpha, \beta) = (\alpha, \beta^0)(\alpha^0, \beta),$$

$$(11) \qquad (\alpha_1, \beta^0)(\alpha_2, \beta^0) = (\alpha_1 \alpha_2, \beta^0),$$

$$(12) \qquad (\alpha^0, \beta_1)(\alpha^0, \beta_2) = (\alpha^0, \beta_1 \beta_2).$$

Es giebt also in $\mathfrak{G}$ eine mit $\mathfrak{A}$ isomorphe Abel'sche Gruppe von m Elementen (α, β^0), und eine mit $\mathfrak{B}$ isomorphe Gruppe von n Elementen (α^0, β), und zufolge (10) ist $\mathfrak{G}$ das Product aus diesen beiden Gruppen, welche nur das Haupt-Element (α^0, β^0) gemeinsam haben; hieraus folgt die Berechtigung, in $\mathfrak{G}$ jedes Element (α, β^0) kurz durch α, jedes Element (α^0, β) kurz durch β zu bezeichnen, woraus dann $\alpha^0 = \beta^0$ und $(\alpha, \beta) = \alpha\beta$, $\mathfrak{G} = \mathfrak{A}\mathfrak{B}$ folgt. Die Composition (4) lautet

$$\alpha_1 \beta_1 \alpha_2 \beta_2 = \alpha_1 \alpha_2^{\beta_1'} \beta_1 \beta_2,$$

worin (1) enthalten ist. (In diesem Winter habe ich mich mit viel allgemeineren Zusammensetzungen von zwei Gruppen $\mathfrak{A}$, $\mathfrak{B}$ zu einer Product-Gruppe $\mathfrak{A}\mathfrak{B}$ beschäftigt). —

Bezeichnet man nun der Einfachheit halber die dem Elemente $\alpha\beta$ entsprechende Variabele der Gruppen-Determinante D selbst mit $\alpha\beta$ (statt mit $x_{\alpha\beta}$), und ordnet die letztere in n^2 Felder von je m^2 Elementen, so wird

$$D = \left|\begin{array}{ccc|c|ccc} \cdots(\alpha\beta_1)(\alpha_1\ \beta_1)^{-1}\cdots & & & \cdots & \cdots(\alpha\beta_n)(\alpha_1\ \beta_1)^{-1}\cdots \\ \cdots\cdots\cdots & & & \cdots & \cdots\cdots\cdots \\ \cdots(\alpha\beta_1)(\alpha_m\ \beta_1)^{-1}\cdots & & & \cdots & \cdots(\alpha\beta_n)(\alpha_m\ \beta_1)^{-1}\cdots \\ \hline \cdots\cdots\cdots & & & \cdots & \cdots\cdots\cdots \\ \hline \cdots(\alpha\beta_1)(\alpha_1\ \beta_n)^{-1}\cdots & & & \cdots & \cdots(\alpha\beta_n)(\alpha_1\ \beta_n)^{-1}\cdots \\ \cdots\cdots\cdots & & & \cdots & \cdots\cdots\cdots \\ \cdots(\alpha\beta_1)(\alpha_m\ \beta_n)^{-1}\cdots & & & \cdots & \cdots(\alpha\beta_n)(\alpha_m\ \beta_n)^{-1}\cdots \end{array}\right|,$$

wo α in jeder Zeile jedes Feldes alle m Elemente $\alpha_1, \alpha_2 \cdots \alpha_m$ von $\mathfrak{A}$ in derselben Ordnung durchläuft. Nun bilde ich aus jedem Charakter ψ von $\mathfrak{A}$ und jedem Element β von $\mathfrak{B}$ die lineare Function von m Variabelen

$$(\beta,\ \psi) = \sum^{\alpha}(\alpha\beta)\psi(\alpha);$$

die Charakter-Potenzen $\psi^{\beta''}$ sind ebenfalls Charaktere ψ, und man erhält

$$\sum^{\alpha}(\alpha\beta)(\alpha_\mu\beta_\nu)^{-1}\psi^{\beta''}(\alpha) = \sum^{\alpha}(\alpha\beta\beta_\nu^{-1}\alpha_\mu^{-1})\psi^{\beta''}(\alpha)$$

$$= \sum^{\alpha}(\alpha\alpha_\mu^{-\beta'\beta''_\nu}\beta\beta_\nu^{-1})\psi^{\beta''}(\alpha) = \sum^{\alpha}(\alpha\beta\beta_\nu^{-1})\psi^{\beta''}(\alpha\alpha_\mu^{\beta'\beta''_\nu})$$

$$= (\beta\beta_\nu^{-1},\ \psi^{\beta''})\psi^{\beta''_\nu}(\alpha_\mu).$$

Multiplicirt man daher (wie im Beispiel 3) den Multiplicand D mit dem Multiplicator

$$\pm\mathfrak{P}^n = \left|\begin{array}{ccc|ccc|ccc} \cdots\psi_1^{\beta''_1}(\alpha)\cdots & & & 0 & \cdot & 0 & 0 & \cdots & 0 \\ \cdots\cdots\cdots & & & \cdots & & & \cdots\cdots & & \\ \cdots\psi_m^{\beta''_1}(\alpha)\cdots & & & 0 & \cdot & 0 & 0 & \cdots & 0 \\ \hline 0 & \cdots & 0 & & & & 0 & \cdots & 0 \\ \hline 0 & \cdots & 0 & 0 & \cdot & 0 & \cdots\psi_1^{\beta''_n}(\alpha)\cdots & & \\ \cdots\cdots\cdots & & & \cdots & & & \cdots\cdots\cdots & & \\ 0 & \cdots & 0 & 0 & \cdot & 0 & \cdots\psi_m^{\beta''_n}(\alpha)\cdots & & \end{array}\right|,$$

so erhält man

$$\pm D\Psi^n = \begin{vmatrix} \cdots (\beta_1\beta_1^{-1}, \psi_1^{\beta_1''})\,\psi_1^{\beta_1''}(\alpha)\cdots & \cdots & \cdots (\beta_1\beta_n^{-1}, \psi_1^{\beta_1''})\,\psi_1^{\beta_n''}(\alpha)\cdots \\ \cdots (\beta_1\beta_1^{-1}, \psi_m^{\beta_1''})\,\psi_m^{\beta_1''}(\alpha)\cdots & \cdots & \cdots (\beta_1\beta_n^{-1}, \psi_m^{\beta_1''})\,\psi_m^{\beta_n''}(\alpha)\cdots \\ \cdots (\beta_n\beta_1^{-1}, \psi_1^{\beta_n''})\,\psi_1^{\beta_1''}(\alpha)\cdots & \cdots & \cdots (\beta_n\beta_n^{-1}, \psi_1^{\beta_n''})\,\psi_1^{\beta_n''}(\alpha)\cdots \\ \cdots (\beta_n\beta_1^{-1}, \psi_m^{\beta_n''})\,\psi_m^{\beta_1''}(\alpha)\cdots & \cdots & \cdots (\beta_n\beta_n^{-1}, \psi_m^{\beta_n''})\,\psi_m^{\beta_n''}(\alpha)\cdots \end{vmatrix}.$$

Dies ist wieder das Product aus dem Multiplicand

$$\pm\Psi^n = \begin{vmatrix} \psi_1^{\beta_1''}(\alpha_1) & \cdots & \psi_m^{\beta_1''}(\alpha_1) & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \cdots & & \cdots & \cdots & & \cdots & \cdots & & \cdots \\ \psi_1^{\beta_1''}(\alpha_m) & \cdots & \psi_m^{\beta_1''}(\alpha_m) & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & \cdots & & \cdots & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 & \psi_1^{\beta_n''}(\alpha_1) & \cdots & \psi_m^{\beta_n''}(\alpha_1) \\ \cdots & & \cdots & \cdots & & \cdots & \cdots & & \cdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 & \psi_1^{\beta_n''}(\alpha_m) & \cdots & \psi_m^{\beta_n''}(\alpha_m) \end{vmatrix}$$

und dem Multiplicator

$$\begin{vmatrix} (\beta_1\beta_1^{-1}, \psi_1^{\beta_1''})\cdots & 0 & \cdots & (\beta_1\beta_n^{-1}, \psi_1^{\beta_1''})\cdots & 0 \\ \cdots & & \cdots & \cdots & \cdots \\ 0 & \cdots (\beta_1\beta_1^{-1}, \psi_m^{\beta_1''}) & \cdots & 0 & \cdots (\beta_1\beta_n^{-1}, \psi_m^{\beta_1''}) \\ \cdots & & \cdots & \cdots & \cdots \\ (\beta_n\beta_1^{-1}, \psi_1^{\beta_n''})\cdots & 0 & \cdots & (\beta_n\beta_n^{-1}, \psi_1^{\beta_n''})\cdots & 0 \\ \cdots & & \cdots & \cdots & \cdots \\ 0 & \cdots (\beta_n\beta_1^{-1}, \psi_m^{\beta_n''}) & \cdots & 0 & \cdots (\beta_n\beta_n^{-1}, \psi_m^{\beta_n''}) \end{vmatrix},$$

welcher folglich $= D$ ist. Mithin ergiebt sich, wenn

$$D_\psi = \begin{vmatrix} (\beta_1\beta_1^{-1}, \psi^{\beta_1''})\cdots(\beta_1\beta_n^{-1}, \psi^{\beta_1''}) \\ \cdots \\ (\beta_n\beta_1^{-1}, \psi^{\beta_n''})\cdots(\beta_n\beta_n^{-1}, \psi^{\beta_n''}) \end{vmatrix}$$

gesetzt wird, unsere Gruppen-Determinante

$$D = \prod_{\psi} D_{\psi}$$

als Product von m Factoren n^{ten} Grades. —

Jeder Commutator der Gruppe $\mathfrak{B}$, d. h. jedes Element von der Form

$$\gamma = \beta_1^{-1}\beta_2^{-1}\beta_1\beta_2$$

ist permutabel mit jedem Element α von $\mathfrak{A}$, weil

$$\gamma' \equiv \beta_1''\beta_2''\beta_1'\beta_2' \equiv 1 \pmod{m},$$

also $\gamma\alpha = \alpha^{\gamma'}\gamma = \alpha\gamma$. Die von allen diesen Commutatoren γ erzeugte Gruppe sei $\mathfrak{C}$. Unter den Commutatoren der Product-Gruppe $\mathfrak{G} = \mathfrak{A}\mathfrak{B}$ sind zunächst die folgenden

$$\beta^{-1}\alpha^{-1}\beta\alpha = \alpha^{1-\beta''}$$

zu bemerken; bedeutet e den grössten gemeinsamen Theiler aller n Zahlen $1-\beta''$ oder $1-\beta'$ mit m (oder mit dem höchsten Element-Grade in $\mathfrak{A}$), so bilden diese Commutatoren die Gruppe $\mathfrak{A}'$ aller a' verschiedenen Potenzen α^e, und es ist $m = aa'$, wo $a = (\mathfrak{A}', \mathfrak{A})$ die Anzahl aller e-seitigen, d. h. derjenigen Elemente α bedeutet, welche der Bedingung $\alpha^e = \alpha^0$ genügen; da jedem Charakter χ der Gruppe $\mathfrak{A}'$, z. B. ihrem Hauptcharakter genau a Charaktere ψ der Gruppe $\mathfrak{A}$ entsprechen, welche Multipla von χ sind oder χ einschliessen, d. h. für alle Elemente von $\mathfrak{A}'$ mit χ übereinstimmen, so ist a auch die Anzahl aller e-seitigen Charaktere $\psi = \psi^{\beta'} = \psi^{\beta''}$ von $\mathfrak{A}$, was auch aus der Isomorphie von $\mathfrak{A}$ mit der Charakter-Gruppe folgen würde. Da ferner jeder beliebige Commutator der Gruppe $\mathfrak{G}$ von der Form

$$(\alpha_1\beta_1)^{-1}(\alpha_2\beta_2)^{-1}(\alpha_1\beta_1)(\alpha_2\beta_2)$$
$$= \alpha_1^{\beta_1''(\beta_2''-1)}\alpha_2^{\beta_2''(1-\beta_1'')}\cdot\beta_1^{-1}\beta_2^{-1}\beta_1\beta_2 = \alpha^e\gamma$$

ist, so erzeugen alle diese Commutatoren die Gruppe $\mathfrak{A}'\mathfrak{C}$, deren Index $(\mathfrak{A}'\mathfrak{C}, \mathfrak{A}\mathfrak{B}) = (\mathfrak{A}'\mathfrak{C}, \mathfrak{A}\mathfrak{C})(\mathfrak{A}\mathfrak{C}, \mathfrak{A}\mathfrak{B}) = a(\mathfrak{C}, \mathfrak{B})$ ist. Wenn nun ψ ein e-seitiger Charakter ist, so geht der ihm entsprechende Factor

$$D_{\psi} = \begin{vmatrix} (\beta_1\beta_1^{-1}, \psi) & \cdots & (\beta_n\beta_1^{-1}, \psi) \\ \cdot & \cdots & \cdot \\ (\beta_1\beta_n^{-1}, \psi) & \cdots & (\beta_n\beta_n^{-1}, \psi) \end{vmatrix},$$

von D aus der Determinante

$$\begin{vmatrix} y_{\beta_1\beta_1^{-1}} & \cdots & y_{\beta_n\beta_1^{-1}} \\ \cdot & \cdots & \cdot \\ y_{\beta_1\beta_n^{-1}} & \cdots & y_{\beta_n\beta_n^{-1}} \end{vmatrix}$$

der Gruppe $\mathfrak{B}$ offenbar durch die lineare Transformation $y_\beta = (\beta, \psi)$ hervor und enthält folglich dieselbe Anzahl linearer Factoren. Aber mehr kann man auf diese Weise wohl nicht schliessen.

8. Juli 1896*).

. . . Nochmals bitte ich sehr um Entschuldigung für meine Saumseligkeit, für die ich nur wenige gute, aber viele schlechte Gründe angeben könnte; zu den letzteren gehört meine tadelnswerthe Schwäche, mich oft von Nebenfragen, die für die Hauptsache einer Untersuchung ganz werthlos sind, so gefangen nehmen zu lassen, dass ich darüber das eigentliche Ziel aus den Augen verliere. Zu den guten Gründen darf ich wohl den rechnen, dass ich in Folge Ihrer Anregung meine Papiere vom Februar 1886 über Gruppen-Determinanten und deren hypercomplexe lineare Factoren wieder durchstöbert habe.

Auf Ihre Frage, wann ich den allgemeinen Satz über die Zerlegung der Abel'schen Gruppen-Determinanten in lineare Charakter-Factoren gefunden habe, geben diese Papiere (12 Folioseiten vom 2. bis 17. Februar datirt, mit Formeln und nur wenigen Worten)**) nur den Aufschluss, dass dies schon in früherer Zeit geschehen sein muss. Sie behandeln nämlich (mit einer einzigen Ausnahme) nur noch Beispiele von nicht Abel'schen Gruppen, unter denen das vom 17. Februar 1886, welches ich Ihnen im April d. J. mitgetheilt habe, eine Gruppe $\mathfrak{G}$ betrifft, in der die allgemeinste Abel'sche Gruppe $\mathfrak{A}$ als Theiler enthalten ist; hierin steckt natürlich auch der obige Satz A über die Abel'schen Gruppen $\mathfrak{A}$, und die ganze Behandlung der Determinante von $\mathfrak{G}$ ist offenbar derjenigen nachgebildet, welche zur Zerlegung der Determinante von $\mathfrak{A}$, also zu dem Satze A führt; aber dieser Satz A wird nirgends mehr erwähnt. Auf den Begriff der allgemeinen Gruppen-Determinante bin ich zuerst bei dem Studium der Discriminante eines beliebigen Normalkörpers Ω geführt, indem ich solche (sehr nützliche) Basen von Ω betrachtete, die aus den Conjugirten einer einzigen Zahl ω bestehen (bisweilen besitzt auch das System $\mathfrak{o}$ aller ganzen Zahlen in Ω eine solche Basis, z. B. wenn ω eine m^{te} Einheits-Wurzel, und m durch kein Quadrat theil-

*) [Ein Auszug aus diesem Brief findet sich in der Einleitung der Arbeit über Gruppencharaktere von Frobenius. E. N.]

**) [Dem Inhalt nach vollständig in den hier veröffentlichten Briefen enthalten. E. N.]

bar ist, und dasselbe gilt dann auch von allen Divisoren von Ω, z. B. allen quadratischen Körpern von ungerader Grundzahl); dieses Studium fällt wahrscheinlich in die Zeit um 1880 oder noch früher, und damals werde ich wohl den Satz A gefunden haben; was mich aber veranlasst hat, im Februar 1886 auf die Gruppen-Determinanten zurückzukommen, weiss ich nicht mehr.

Ich füge einige Bemerkungen über die Charaktere der Abel'schen Gruppen $\mathfrak{A}$ hinzu. Das älteste Beispiel ihrer Anwendung ist wohl in den Resolventen von Lagrange (für cyklische $\mathfrak{A}$) zu erkennen. Sodann ist das (von Jacobi verallgemeinerte) Symbol von Legendre zu nennen. Die von Gauss (Art. 131) benutzten Zeichen R, N sind weniger glücklich, als die bestimmte Einführung der Einheits-Wurzeln ± 1 durch Legendre, und so kommt es (Art. 230), dass er auch unter dem Charakter einer Formen-Classe oder eines Geschlechtes eine Relation, nicht eine Zahl versteht; die der Zusammensetzung der Geschlechter entsprechende Zusammensetzung der Charaktere tritt zwar deutlich hervor (Art. 246—248), aber nicht als Multiplication von Zahlen. Die Umwandlung der Gauss'schen Geschlechts-Charaktere in Zahlen hat Dirichlet (Recherches sur diverses applications etc. §. 3) durch Benutzung des Symbols von Legendre bewirkt. Ferner hat Dirichlet in der Abhandlung über die arithmetische Progression alle Charaktere ψ (— ohne diesen Namen zu gebrauchen —) der Abel'schen Gruppe $G^{(m)}$ benutzt, welche von den $\varphi(m)$ Classen relativer Primzahlen zu m gebildet wird, und ebenso alle Charaktere der Gruppe der Formen-Classen (in der Skizze über die Darstellung unendlich vieler Primzahlen durch eine quadratische Form). Nach allem diesen lag es nahe, den Begriff und Namen der Charaktere für jede Abel'sche Gruppe $\mathfrak{A}$ einzuführen, wie ich es in der dritten Auflage von Dirichlet's Zahlentheorie gethan habe. Ich habe dort (in der vierten Auflage S. 612) zur Begründung der Existenz der Charaktere auf §. 149, also auf die Darstellung der Elemente von $\mathfrak{A}$ als Producte von Potenzen von Fundamental-Elementen hingedeutet; doch ziehe ich principiell den folgenden Weg vor, der Nichts von dieser Darstellung voraussetzt. Ist $\mathfrak{A}$ ein Theiler von $\mathfrak{B}$, so ist in jedem Charakter χ von $\mathfrak{B}$ ein Charakter ψ von $\mathfrak{A}$ enthalten (der für alle Elemente von $\mathfrak{A}$ mit χ übereinstimmt); ich nenne ψ den auf $\mathfrak{A}$ bezüglichen Divisor von χ, umgekehrt χ ein Multiplum von ψ. Dann ergiebt sich ganz leicht durch Induction

der Satz: Ist ψ ein Charakter von $\mathfrak{A}$, so ist der Index $(\mathfrak{A}, \mathfrak{B})$ [— mit $(\mathfrak{A}, \mathfrak{B})$ bezeichne ich auch in der allgemeinen Gruppen-Theorie die Anzahl der verschiedenen Complexe $\mathfrak{A}\beta$, aus denen der Complex $\mathfrak{A}\mathfrak{B}$ besteht —] zugleich die genaue Anzahl der verschiedenen Charaktere χ von $\mathfrak{B}$, welche Multipla von ψ sind. Dies leuchtet ein für $(\mathfrak{A}, \mathfrak{B}) = 1$, also $\mathfrak{A} = \mathfrak{B}$, und wenn es für alle Fälle $(\mathfrak{A}, \mathfrak{B}) < m$ bewiesen ist, so gilt es auch für $(\mathfrak{A}, \mathfrak{B}) = m$; denn entweder giebt es eine von $\mathfrak{A}$ und $\mathfrak{B}$ verschiedene Gruppe $\mathfrak{C}$, die Theiler von $\mathfrak{B}$ und Vielfaches von $\mathfrak{A}$ ist, oder nicht; in beiden Fällen ergiebt sich der Schluss leicht, weil im ersten Fall $m = (\mathfrak{A}, \mathfrak{B}) = (\mathfrak{A}, \mathfrak{C})(\mathfrak{C}, \mathfrak{B})$, also $(\mathfrak{A}, \mathfrak{C})$ und $(\mathfrak{C}, \mathfrak{B}) < m$ ist, und weil im zweiten Falle $\mathfrak{B} = \mathfrak{A} + \mathfrak{A}\beta + \mathfrak{A}\beta^2 + \cdots$ ist. Hierin ist aber Alles über Existenz und Anzahl der Charaktere enthalten, und der Satz ist ausserdem sehr nützlich.

Die Art, wie Dirichlet (bei der arithmetischen Progression) darthut, dass seine Reihen L_2 der zweiten Art von Null verschiedene Grenzwerthe haben, weil diese als Factoren der Classen-Anzahl der quadratischen Formen auftreten, führte mich, da ich die quadratischen Körper als Kreiskörper kannte, zu der Bemerkung (Aufl. 3, S. 596 und Aufl. 4, S. 625), dass eine ähnliche Schlussart auch für die Reihen L_3 der dritten Art gilt; denn wenn man den aus den m^{ten} Einheits-Wurzeln gebildeten Kreiskörper K_m betrachtet, und Kummer's Satz über dessen Primideale anwendet, so ist das Product aller $\varphi(m)$ Dirichlet'schen Reihen L identisch mit der Summe $\sum N(\mathfrak{a})^{-s}$, wo $\mathfrak{a}$ alle relativen Primideale zu m durchläuft. Ich weiss nicht, ob Kummer selbst diese Anwendung ausgesprochen hat, glaube es aber kaum.

Da Sie bei Ihrer Frage nach der Auffindungs-Zeit des obigen Satzes A die Classen-Anzahl der Ideale in einem beliebigen Kreiskörper erwähnen, so möchte ich Ihnen (wie neulich auch Weber) noch von einer schönen Sparsamkeit schreiben*), auf die Gefahr hin, dass dieselbe Ihnen, wie mir, schon lange bekannt ist. Die Identität

$$(1) \qquad \sum^{\mathfrak{a}} N(\mathfrak{a})^{-s} = \prod^{\psi} \sum^{n} \psi(n) n^{-s}$$

gilt nämlich auch dann, wenn $\mathfrak{a}$ alle Ideale in K_m, und n alle natürlichen Zahlen durchläuft, falls jeder der $\varphi(m)$ Charaktere ψ der

*) [Vergl. XLI.]

Gruppe $G^{(m)}$ eine erweiterte Bedeutung erhält, so dass ψ für jede ganze rationale Zahl x einen bestimmten Werth $\psi(x)$ annimmt, der mit dem ursprünglichen $\psi(x)$ übereinstimmt, wenn x relative Primzahl zu m ist, und ausserdem die Gesetze $\psi(x+m) = \psi(x)$ und $\psi(xy) = \psi(x)\psi(y)$ erfüllt. Eine solche Erweiterung eines gegebenen Charakters ψ von $G^{(m)}$ lässt sich im Allgemeinen auf mehrere Arten herstellen (deren Anzahl eine Potenz von 2 ist); von diesen genügt aber nur eine einzige der obigen Ideal-Identität (1), und zwar ist sie dadurch vollkommen bestimmt, daß $\psi(x)$ für möglichst wenige Zahlen x verschwinden soll. Einen so erweiterten Charakter ψ nenne ich einen natürlichen Charakter von $G^{(m)}$. Die oben gerühmte Sparsamkeit besteht nun zunächst darin, dass, wenn a ein Divisor von m, alle $\varphi(a)$ natürlichen Charaktere von $G^{(a)}$ auch natürliche Charaktere von $G^{(m)}$ sind; bezeichnet man daher mit $\varphi'(m)$ die Anzahl aller primitiven, nämlich derjenigen natürlichen Charaktere von $G^{(m)}$, welche zu keiner Gruppe $G^{(a)}$ mit kleinerem a gehören, so ist

$$\sum \varphi'(a) = \varphi(m); \tag{2}$$

mithin ist $\varphi'(ab) = \varphi'(a)\varphi'(b)$, wenn a, b relative Primzahlen sind, und für eine Primzahl p ist $\varphi'(p) = p-2$ und $\varphi'(p^n) = (p-1)^2 p^{n-2}$, falls $n > 1$; ferner ist $\varphi'(2m) = 0$, wenn m ungerade (es ist ja auch $K_{2m} = K_m$). Am schönsten offenbart sich aber die Sparsamkeit dadurch, dass die Identität (1) im folgenden Sinne für jeden Kreiskörper Ω gilt. Hat man m so gewählt, dass Ω Divisor von K_m wird, und ist H die Gruppe der Zahlclassen h (mod. m), zu welcher Ω gehört, also H Theiler von $G^{(m)}$, so gilt die Identität (1), wenn $\mathfrak{a}$ alle Ideale in Ω, und ψ alle diejenigen natürlichen Charaktere von $G^{(m)}$ durchläuft, welche der Bedingung $\psi(h) = 1$ genügen (alle Multipla des Haupt-Charakters von H); dies ist gewissermassen der analytische Ausdruck für meinen allgemeinen Satz über die Primideale von Ω (C. R. der Pariser Akademie vom 24. Mai 1880). —

Zu einem gründlichen Studium Ihrer Abhandlung „Über vertauschbare Matrizen“ bin ich aus den oben erwähnten schlechten Gründen noch nicht gekommen; doch glaube ich versichern zu können, dass ich auch bei meinen nach 1887 gelegentlich wieder aufgenommenen Versuchen, die Zerlegung in lineare Factoren auf einfachere Weise abzuleiten, durchaus nicht auf Ihre Wege gekommen bin. Doch

muthet mich Manches darin ähnlich an, wie meine übercomplexen Factoren der Gruppen-Determinanten, auf die ich aber heute nicht mehr eingehen kann. Vielleicht komme ich morgen dazu, die Armada dieser seltsamen Schiffe in See stechen zu lassen; doch wird es wohl heissen: Frobenius afflavit et dissipavit! ...

13. Juli 1896.

... Zuerst erwähne ich, dass mein Beispiel vom 17. Februar 1886 vollständiger und hübscher in der Gestalt $AB = BC$ dargestellt wird, wo A, B, C nicht Determinanten, sondern folgende Systeme, Matrizen, Formen bedeuten:

$$\left\{\begin{array}{ccc|ccc} x_{11}^{-1} & \cdots & x_{m1}^{-1} & y_{11} & \cdots & y_{m1} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ x_{1m}^{-1} & \cdots & x_{mm}^{-1} & y_{1m} & \cdots & y_{mm} \\ \hline y_{11} & \cdots & y_{m1} & x_{11}^{-1} & \cdots & x_{m1}^{-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ y_{1m} & \cdots & y_{mm} & x_{1m}^{-1} & \cdots & x_{mm}^{-1} \end{array}\right\} = A.$$

$$\left\{\begin{array}{cc|c|cc} \psi_1(1), & 0 & \cdots & \psi_m(1), & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \psi_1(m), & 0 & \cdots & \psi_m(m), & 0 \\ \hline 0, & \psi_1^{-1}(1) & \cdots & 0, & \psi_m^{-1}(1) \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0, & \psi_1^{-1}(m) & \cdots & 0, & \psi_m^{-1}(m) \end{array}\right\} = B,$$

$$\left\{\begin{array}{cc|ccc|cc} u_1, & v_1' & 0 & \cdots & 0 & 0, & 0 \\ v_1, & u_1' & 0 & \cdots & 0 & 0, & 0 \\ \hline 0, & 0 & \cdots & \cdots & \cdots & 0, & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0, & 0 & \cdots & \cdots & \cdots & 0, & 0 \\ \hline 0, & 0 & 0 & \cdots & 0 & u_m, & v_m' \\ 0, & 0 & 0 & \cdots & 0 & v_m, & u_m' \end{array}\right\} = C.$$

Hieraus folgt dann der Satz über die Zerlegung der Gruppen-Determinante D in die Factoren $u_\mu u_\mu' - v_\mu v_\mu'$. Doch das müssen Sie längst durchschaut haben. Im Folgenden beschäftige ich mich ausschliesslich mit dem ersten Beispiel (Fall $m = 3$) vom 2. und 3. Februar 1886; an diesem Beispiel habe ich damals auch zuerst die Zerlegung in hypercomplexe lineare Factoren ausgeführt, und

erst dieser Erfolg hat mich etwas später (jedenfalls vor dem 15. Februar) zu der Beschäftigung mit der Quaternion-Gruppe veranlasst; ich habe Ihnen, wie ich glaube, geschrieben, dass die Reihenfolge die umgekehrte gewesen ist; das war aber ein Irrthum. Nun also! Es war $1 + \varrho + \varrho^2 = 0$ und

$$\begin{vmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ x_3 & x_1 & x_2 & x_5 & x_6 & x_4 \\ x_2 & x_3 & x_1 & x_6 & x_4 & x_5 \\ x_4 & x_5 & x_6 & x_1 & x_2 & x_3 \\ x_5 & x_6 & x_4 & x_3 & x_1 & x_2 \\ x_6 & x_4 & x_5 & x_2 & x_3 & x_1 \end{vmatrix} = (u+v)(u-v)(u_1 u_2 - v_1 v_2)^2.$$

$$u = x_1 + x_2 + x_3, \quad u_1 = x_1 + \varrho x_2 + \varrho^2 x_3, \quad u_2 = x_1 + \varrho^2 x_2 + \varrho x_3,$$
$$v = x_4 + x_5 + x_6, \quad v_1 = x_4 + \varrho x_5 + \varrho^2 x_6, \quad v_2 = x_4 + \varrho^2 x_5 + \varrho x_6,$$

also

$$u_1 u_2 = x_1^2 + x_2^2 + x_3^2 - x_1 x_2 - x_1 x_3 - x_2 x_3,$$
$$v_1 v_2 = x_4^2 + x_5^2 + x_6^2 - x_4 x_5 - x_4 x_6 - x_5 x_6.$$

Nun sei

$$u_1 u_2 - v_1 v_2 = \alpha\beta,$$
$$\alpha = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 + \alpha_4 x_4 + \alpha_5 x_5 + \alpha_6 x_6,$$
$$\beta = \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3 + \beta_4 x_4 + \beta_5 x_5 + \beta_6 x_6.$$

Bei der Addition, Subtraction, Multiplication rechne ich mit den 12 Coefficienten α_r, β_r wie mit gewöhnlichen Zahlen und verzichte nur bei ihrer Multiplication mit einander auf das commutative Gesetz, während dasselbe bei ihrer Multiplication mit gewöhnlichen Zahlen und den Variabelen x_r bestehen bleiben soll. Ebenso wird durchweg das associative und distributive Gesetz angenommen. Die Forderung der Identität der Coefficienten (rs) von $x_r x_s$ in $u_1 u_2 - v_1 v_2$ und in $\alpha\beta$ ergiebt dann 21 Bedingungen; um mit ihnen etwas anfangen zu können, setze ich (wenn dadurch auch die Allgemeinheit beeinträchtigt wird)

(A) $$\alpha_1 = 1, \quad \beta_1 = 1,$$

wodurch die Forderung $(11) = \alpha_1\beta_1 = 1$ erfüllt ist. Dann folgt:

(B)
$$\begin{cases} (12) = \alpha_2 + \beta_2 = -1, & \beta_2 = -1 - \alpha_2, \\ (13) = \alpha_3 + \beta_3 = -1, & \beta_3 = -1 - \alpha_3, \\ (14) = \alpha_4 + \beta_4 = 0, & \beta_4 = -\alpha_4, \\ (15) = \alpha_5 + \beta_5 = 0, & \beta_5 = -\alpha_5, \\ (16) = \alpha_6 + \beta_6 = 0, & \beta_6 = -\alpha_6, \end{cases}$$

sodann

$$(C)\quad \begin{cases} (22) = \alpha_2\beta_2 = 1, & \alpha_2^2 = -1-\alpha_2, \\ (33) = \alpha_3\beta_3 = 1, & \alpha_3^2 = -1-\alpha_3, \\ (23) = \alpha_2\beta_3+\alpha_3\beta_2 = -1, & \alpha_2\alpha_3+\alpha_3\alpha_2 = +1-\alpha_2-\alpha_3, \end{cases}$$

ferner

$$(D)\quad \begin{cases} (44) = \alpha_4\beta_4 = -1, & \alpha_4^2 = 1, \\ (55) = \alpha_5\beta_5 = -1, & \alpha_5^2 = 1, \\ (66) = \alpha_6\beta_6 = -1, & \alpha_6^2 = 1, \\ (45) = \alpha_4\beta_5+\alpha_5\beta_4 = 1, & \alpha_4\alpha_5+\alpha_5\alpha_4 = -1, \\ (46) = \alpha_4\beta_6+\alpha_6\beta_4 = 1, & \alpha_4\alpha_6+\alpha_6\alpha_4 = -1, \\ (56) = \alpha_5\beta_6+\alpha_6\beta_5 = 1, & \alpha_5\alpha_6+\alpha_6\alpha_5 = -1, \end{cases}$$

endlich

$$(E)\quad \begin{cases} (24) = \alpha_2\beta_4+\alpha_4\beta_2 = 0, & \alpha_2\alpha_4+\alpha_4\alpha_2 = -\alpha_4, \\ (34) = \alpha_3\beta_4+\alpha_4\beta_3 = 0, & \alpha_3\alpha_4+\alpha_4\alpha_3 = -\alpha_4, \\ (25) = \alpha_2\beta_5+\alpha_5\beta_2 = 0, & \alpha_2\alpha_5+\alpha_5\alpha_2 = -\alpha_5, \\ (35) = \alpha_3\beta_5+\alpha_5\beta_3 = 0, & \alpha_3\alpha_5+\alpha_5\alpha_3 = -\alpha_5, \\ (26) = \alpha_2\beta_6+\alpha_6\beta_2 = 0, & \alpha_2\alpha_6+\alpha_6\alpha_2 = -\alpha_6, \\ (36) = \alpha_3\beta_6+\alpha_6\beta_3 = 0, & \alpha_3\alpha_6+\alpha_6\alpha_3 = -\alpha_6. \end{cases}$$

Zunächst folgt aus (A) und (B) ein Hoffnungsstrahl! Es wird nämlich

$$(F)\qquad \alpha+\beta = 2x_1-x_2-x_3, \quad \text{mithin} \quad \beta\alpha = \alpha\beta,$$

d. h. die linearen Factoren der Gruppen-Determinante sind alle permutabel mit einander, wodurch ihre Brauchbarkeit erheblich gewinnt.

Bedenkt man nun, dass aus (C) auch

$$\alpha_2^3 = \alpha_3^3 = 1,$$

ferner aus (D) z. B.

$$(\alpha_4\alpha_5)^2 = -1-\alpha_4\alpha_5 = \alpha_5\alpha_4, \quad (\alpha_4\alpha_5)^3 = (\alpha_5\alpha_4)^3 = 1,$$

und aus (C) und (E) z. B.

$$\alpha_2\alpha_4 = \alpha_4\alpha_2^2, \quad \alpha_4\alpha_2 = \alpha_2^2\alpha_4, \quad (\alpha_2\alpha_4)^2 = (\alpha_4\alpha_2)^2 = 1$$

folgt, so wird man fast mit Gewalt zu der Bemerkung getrieben, dass die 15 Bedingungen (C), (D), (E) widerspruchsfrei erfüllt werden,

wenn man zum Beispiel annimmt, dass die sechs Zahlen α_r bei ihrer Multiplication die Gesetze unserer Gruppe

(G)

1	α_2	α_3	α_4	α_5	α_6
α_2	α_3	1	α_5	α_6	α_4
α_3	1	α_2	α_6	α_4	α_5
α_4	α_6	α_5	1	α_3	α_2
α_5	α_4	α_6	α_2	1	α_3
α_6	α_5	α_4	α_3	α_2	1

befriedigen, und dass ausserdem die beiden Summen

(H) $$\eta = 1 + \alpha_2 + \alpha_3, \quad \omega = \alpha_4 + \alpha_5 + \alpha_6$$

verschwinden; zugleich bilden dann die Zahlen β_r^{-1} eine isomorphe Gruppe.

Mit diesem Ergebniss habe ich mich damals (am 3. Februar 1886) durchaus begnügt, und ich bin, weil es mir sehr merkwürdig schien, gleich zu anderen Beispielen übergegangen, erst zu einer Gruppe zehnten Grades, dann aber zu der Quaternion-Gruppe (deren Existenz nahe lag, mir aber bis dahin wahrscheinlich unbekannt geblieben war), und hier wurde ich durch das Auftreten der Summe von vier Quadraten beglückt. Damals habe ich auch zuerst Beispiele von Normalkörpern mit Quaternion-Gruppe construirt, was mir erst nach mehreren vergeblichen Versuchen gelang, als ich erkannte, dass der darin enthaltene biquadratische Abel'sche Körper (Product von drei quadratischen Körpern) durchaus reell sein muss. Dass aber diese Quaternion-Gruppe eine so grosse Rolle in den nicht Abel'schen (Hamilton'schen) Gruppen spielt, die nur Normaltheiler besitzen, habe ich erst im vorigen Jahre gefunden (zu der Vollendung der Abhandlung bin ich aber noch immer nicht gekommen).

Ich kehre zu dem obigen Beispiele der Versetzungen von drei Buchstaben zurück. Offenbar ist die durch (G) in Verbindung mit $\eta = 0$, $\omega = 0$ bestimmte Lösung der Bedingungen (C), (D), (E) nur eine particuläre, wie man schon daraus erkennt, dass die letzteren symmetrisch sowohl in Bezug auf α_2, α_3, als auch in Bezug auf α_4, α_5, α_6 sind. Aber wahrscheinlich giebt es ausser diesen zwei Lösungen

noch unendlich viele andere Arten, die sämmtlichen Producte der Zahlen α_r linear durch die letzteren so darzustellen, dass die Bedingungen (C), (D), (E) erfüllt werden unter Wahrung des associativen und distributiven Gesetzes. Man kann nämlich zwar leicht beweisen, dass

$$\eta^2 = 0, \quad \omega^2 = 0, \quad \eta\omega + \omega\eta = 0$$

sein muss; dass aber η und ω selbst $= 0$ sein müssen, habe ich nicht herstellen können. Freilich dürfte man ja sagen: da u_1, u_2 nur von den Differenzen $x_2 - x_1$, $x_3 - x_1$, und ebenso v_1, v_2 nur von den Differenzen $x_5 - x_4$, $x_6 - x_4$ abhängen, so kann man von vornherein verlangen, dass auch α, β nur von diesen vier Differenzen abhängen, worin ja die Bedeutung der Bedingungen $\eta = 0$, $\omega = 0$ liegt. Da ferner diese Differenzen umgekehrt durch die vier unabhängigen Variabelen u_1, u_2, v_1, v_2 sich ausdrücken lassen, so kommt das Ganze schliesslich auf eine Zerlegung der bilinearen Form oder Determinante

$$u_1 u_2 - v_1 v_2 = \alpha\beta$$

in lineare Factoren

$$\alpha = \varkappa_1 u_1 + \varkappa_2 u_2 + \lambda_1 v_1 + \lambda_2 v_2, \quad \beta = \mu_1 u_1 + \mu_2 u_2 + \nu_1 v_1 + \nu_2 v_2$$

hinaus, wo die Coefficienten $\varkappa$, λ, μ, ν zufolge der obigen Lösung sehr niedliche Theiler der Null werden!

Ich habe mich in der letzten Woche ziemlich viel mit den Bedingungen (C), (D), (E) beschäftigt, und wenn Sie es wünschen, so will ich Ihnen gern noch Alles aufschreiben, was ich dabei gefunden habe. Aber ich halte es für sehr wohl möglich, dass Sie nach der heutigen Probe auf die ganze Zerlegung in hypercomplexe Factoren gar keinen Werth legen; meine eigene Meinung darüber schwankt hin und her. ...

5. Dezember 1896*).

... Die Correctur**) habe ich sogleich mit dem besten Willen angegriffen, die Sache selbst dabei gründlich durchzunehmen, aber ich habe bald eingesehen, dass ich dazu viel mehr Zeit gebrauchen würde, als Ihnen erwünscht wäre; mein Anlauf hat daher nur bis etwa zur zehnten Seite ausgereicht, und dann habe ich mich begnügt, das

*) [In die Zwischenzeit fällt ein Besuch von Frobenius, auf den sich die Bemerkung über Anregung zur Darstellungstheorie (Einleitung zu der Arbeit über Darstellung endlicher Gruppen) zu beziehen scheint, da die Briefe nichts über Darstellung enthalten. E. N.]

**) [Es handelt sich um die Frobeniussche Arbeit über die Primfaktoren der Gruppendeterminante. E. N.]

Übrige nur durchzulesen, um den hauptsächlichen Inhalt in mich aufzunehmen. Derselbe erfüllt mich mit aufrichtiger Bewunderung; so schwierig die grosse Aufgabe war, so belohnend ist auch die Frucht Ihrer gewaltigen Arbeit geworden, die Ihrem Ruhmeskranze ein neues Blatt hinzufügt. Mir gefällt noch ganz besonders, dass nun auch Ihre Vorarbeiten in neuem Lichte erscheinen.

Alles Dies würde ich, wie ich Ihnen schon einmal gesagt habe, niemals zu Stande gebracht haben, aber desto mehr freue ich mich, Ihnen die erste Veranlassung zu dieser schönen Arbeit gegeben zu haben. ...

13. April 1897.

... Ich bin daher auch noch nicht im Stande, Ihre Mittheilungen über die Gruppen mit der erforderlichen vollständigen Klarheit in mich aufzunehmen; aber eine große Freude haben Sie mir doch durch dieselben bereitet; denn soweit ich sie verstehe, bleibt mir kein Zweifel, dass Sie einen neuen grossen Schritt auf Ihrer Siegesbahn gethan haben, und wenn dabei mein Luftschloss der Scheinzahlen vernichtet wird, so bin ich gar nicht betrübt darüber, sondern erfreut, dass Sie den wirklichen Kern der Sache aufdecken; auch zweifle ich gar nicht, dass Sie die letzten Schwierigkeiten ebenso überwinden werden wie im vorigen Jahr*). ...

*) [Gemeint ist die mehrfach erwähnte Zerlegung in hyperkomplexe Faktoren. Diese spielt eine wesentliche Rolle in der Theorie der nichtkommutativen Körper und deren Zerfällungskörper (vgl. Wedderburn, Transactions of the Am. Math. Soc., Bd. XXII, S. 129—135, 1921; die Wiedergabe bei Dickson: Algebras and their Arithmetics, S. 230 und weitergehende Untersuchungen von E. Noether und R. Brauer; zusammenfassende Darstellung bei v. d. Waerden, Moderne Algebra, Bd. II). Bei dem Dedekindschen Beispiel (Brief vom 13. Juli 1896) handelt es sich um den durch das „allgemeine Element" α (der entsprechenden zweiseitigen Komponente des Gruppenrings) erzeugten Zerfällungskörper, und um die Zerlegung der Norm von α in diesem (kommutativen) Körper; daher die Vertauschbarkeit $\alpha\beta = \beta\alpha$ (Formel (F)).

Daß die Zerlegung bei Frobenius nicht auftritt, erklärt sich daraus, daß Frobenius von vornherein den Körper aller komplexen Zahlen, also einen algebraisch abgeschlossenen Körper, als Koeffizientenbereich nimmt; hier gibt es keine endlichen nichtkommutativen Erweiterungskörper. Die durch das allgemeine Element erzeugten Zerfällungskörper existieren zwar, aber ihre Heranziehung wird unnötig. Das gilt übrigens auch von dem Dedekindschen Beispiel (nicht von dem Beispiel des Quaternionenkörpers), wo es sich schon um einen vollen Matrizenring über dem Körper der rationalen Zahlen handelt; wie Dedekind bemerkt, treten ja Teiler der Null bei der hyperkomplexen Zerlegung der Gruppendeterminante auf. E. N.]