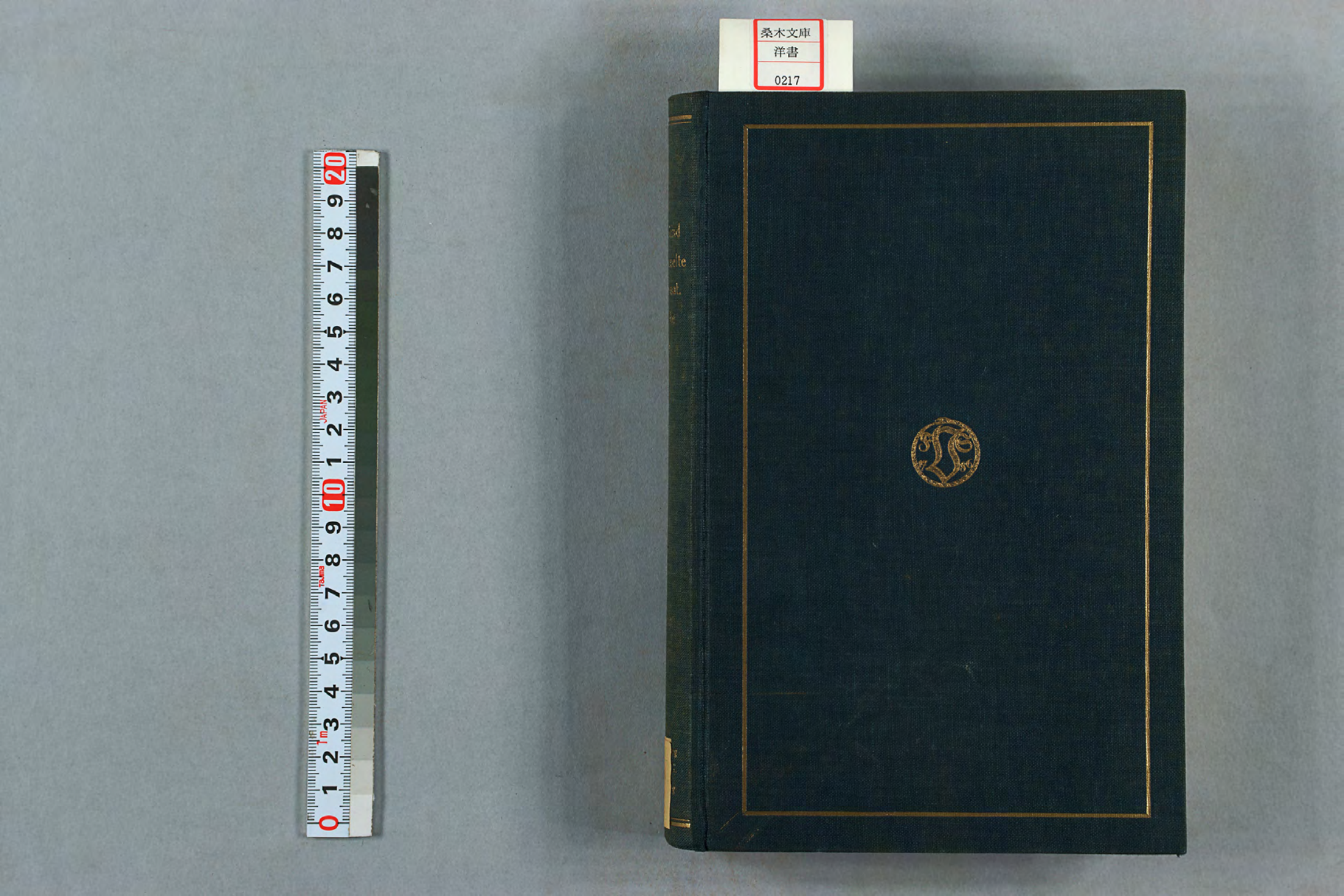

Richard Dedekind

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

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 $e_1, e_2 \dots e_n$ 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 $\iota, \iota', \iota''\ldots$ 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 $\iota, \iota', \iota''\ldots$, 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

$$\eta_{t,rs} = \eta_{t,sr} \tag{1}$$

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

*) 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

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

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 $x', x'' \dots x^{(n)}$ 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 $e_1, e_2 \dots e_n$, 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

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

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

$$\sigma_r = \sum \eta_{t,rt} \tag{25}$$

und

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

setzt, die Determinante

$$\Delta = \sum \pm \tau_{11} \tau_{22} \cdots \tau_{nn} \tag{27}$$

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

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

und

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

und folglich

$$\Delta = e^2, \tag{30}$$

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

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

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 $\delta\xi_1$, $\delta\xi_2 \dots \delta\xi_n$ 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 $d\tau_1, d\tau_2 \dots d\tau_n$ 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

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

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

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

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 $p \pm 1$ 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

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

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

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

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 $\varphi_{n+1}, \varphi_{n+2}, \dots$ 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

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

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

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

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 $1, 2 \dots n$ 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

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

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

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

entsprechen, das Resultat

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

und hieraus mit Rücksicht auf (80)

$$\Delta = e^2; \tag{85}$$

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 $\eta_{t,rs}$ 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

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

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

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

an, woraus leicht der Satz

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

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

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

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

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

unmittelbar das Resultat $d x d' x = d'' x$, 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 $\eta_{t,rs}$ 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 „Dedekindschen 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:

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

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,

M' durch 1, 0, 0
M'' „ 2, 1, 1
M''' „ 0, −1, 1

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 a 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 a ein Produkt von der Form

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

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

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

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

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

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 a 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 $x_0, x_1, x_2 \dots x_m$ 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

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

bezeichnet wird; das System der Zahlen $a_0, a_1 \dots a_m$ 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

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

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

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

wo die Zahlen $p_0, p_1 \dots$ 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

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

besteht aus allen Produkten α von $n+1$ gleichen oder verschiedenen Faktoren aus der Reihe $a_0, a_1 \dots a_m$; 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 $a_0, a_1 \dots a_m$ 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

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

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

$$0, 1, 2 \dots m$$

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

$$s_0 < s_1 < s_2 \cdots < s_n, \tag{s}$$

so können die Differenzen $r_0 - s_0, r_1 - s_1 \dots r_n - s_n$ 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 $0, 1, 2 \dots m$ 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 $\alpha_0, \alpha_1 \dots$ 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

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

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

VII. Bildet man aus den Koeffizienten der drei ganzen Funktionen

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

die drei endlichen Moduln

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

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

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

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

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 $e_r fg$ 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 $\mathfrak{m}\mathfrak{n}$ 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

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

und

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

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

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

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

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

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

$$\begin{gathered} \alpha\alpha''',\ \ \alpha\beta''',\ \ \alpha\sigma_r, \\ \beta\alpha''',\ \ \beta\beta''',\ \ \beta\sigma_r, \\ \mu_r\alpha''',\ \ \mu_r\beta''',\ \ \mu_r\sigma_s \end{gathered}$$

ganze Zahlen, weil sie in der Form

$$\begin{gathered} \alpha\alpha'\cdot\alpha\alpha'',\ \ \alpha\beta'\cdot\beta\beta'',\ \ \alpha\alpha'\cdot\alpha\nu_r + \alpha\beta'\cdot\beta\varrho_r, \\ \alpha\alpha''\cdot\beta\alpha',\ \ \beta\beta'\cdot\beta\beta'',\ \ \alpha\nu_r\cdot\beta\alpha' + \beta\beta'\cdot\beta\varrho_r, \\ \alpha\alpha'\cdot\mu_r\alpha'',\ \ \beta\beta'\cdot\mu_r\beta'',\ \ \alpha\alpha'\cdot\mu_r\nu_s + \beta\beta'\cdot\mu_r\varrho_s \end{gathered}$$

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

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

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

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

auch der Modul

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

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 $\mathfrak{m}\mathfrak{n}$ 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)

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

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

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

Ebenso geht aus (10) hervor, daß die Gleichung

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

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

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

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

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

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,

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

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

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

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

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

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

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

w. z. b. w.

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

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

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

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

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

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

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

woraus wir die für unseren Zweck hinreichenden Folgerungen

(25) $$\mathfrak{p}' > \mathfrak{q}' + \mathfrak{m}, \quad \mathfrak{q}' > \mathfrak{p}' + \mathfrak{m}$$

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

(26) $$\mathfrak{p} - \mathfrak{m} = p\mathfrak{p}', \quad \mathfrak{q} - \mathfrak{m} = q\mathfrak{q}'$$

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

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

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

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

*) 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 $(a;\ b)$ 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 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 verschiedene 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

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

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 $(a; b)$ als den größten gemeinsamen Teiler aller Produkte

$$\frac{p_1 - a_1}{p_1} \cdot \frac{p_2 - a_2}{p_2} \cdots \frac{p_n - a_n}{p_n}$$

erklären, die allen zur Darstellung (17) tauglichen Folgen von einfachen Moduln $p_1, p_2, \cdots, p_n$ entsprechen. Immerhin bleibt die eine wie die andere Definition von $(a; b)$ hinsichtlich ihrer Einfachheit außerordentlich weit zurück hinter der Definition des alten Symbols (a, b), welche sich unmittelbar auf die Betrachtung der in den Moduln a, 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) $$(\varrho + \sigma)\,\mathfrak{m} > \varrho\,\mathfrak{m} + \sigma\,\mathfrak{m}$$

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

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*)

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

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

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

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

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

und die zu beweisende Gleichung (64) lautet

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

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

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

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

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

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

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

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

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 α_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) $$(\mathfrak{a}, \mathfrak{b}, z) = \mathfrak{N}\,(\mathfrak{a}, \mathfrak{b}, \mathfrak{o}),$$

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

$$(1) \qquad \varphi^{-1} S \varphi = S, \qquad S\varphi = \varphi S$$

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

(2) $$R = PQ$$

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 Quaternionengruppe 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

(3) $$\varepsilon^2 = 1,$$

(4) $$\alpha^2 = \alpha^{-2} = \beta^2 = \beta^{-2} = \gamma^2 = \gamma^{-2} = \varepsilon,$$

(5) $$\varepsilon\alpha = \alpha\varepsilon = \alpha^{-1}, \quad \varepsilon\beta = \beta\varepsilon = \beta^{-1}, \quad \varepsilon\gamma = \gamma\varepsilon = \gamma^{-1},$$

(6) $$\varepsilon\alpha^{-1} = \alpha^{-1}\varepsilon = \alpha, \quad \varepsilon\beta^{-1} = \beta^{-1}\varepsilon = \beta, \quad \varepsilon\gamma^{-1} = \gamma^{-1}\varepsilon = \gamma.$$

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

(7) $$\beta\gamma = \alpha, \quad \gamma\alpha = \beta, \quad \alpha\beta = \gamma.$$

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

(18) $$Q = [\alpha] + [\alpha]\beta$$

und

(19) $$\beta^{-1}[\alpha]\beta = [\alpha^{-1}] = [\alpha]$$

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

(20) $$\psi\varphi = \varphi\psi\varepsilon$$

definierte Element

(21) $$\varepsilon = (\psi^{-1}\varphi^{-1}\psi)\varphi = \psi^{-1}(\varphi^{-1}\psi\varphi)$$

*) 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

(22) $$\varrho^{-1}\sigma^s\varrho = (\varrho^{-1}\sigma\varrho)^s$$

ergeben, bilden den folgenden Satz:

III. Ist ε der Kommutator der Elemente φ, ψ einer Hamiltonschen Gruppe, so ist

(23) $$\psi^n\varphi^m = \varphi^m\psi^n\varepsilon^{mn},$$

(24) $$(\varphi^m\psi^n)^t = \varphi^{mt}\psi^{nt}\varepsilon^{\frac{1}{2}mnt(t-1)},$$

und die durch φ und ψ erzeugte Gruppe ist

(25) $$[\varphi, \psi] = [\varphi][\psi] = [\psi][\varphi].$$

Setzt man ferner

(26) $$\varphi_1 = \varphi^m\psi^n, \qquad \psi_1 = \varphi^r\psi^s,$$

so ist

(27) $$\varepsilon_1 = \varepsilon^{ms-nr}$$

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

$$\psi^{b't} = \psi^{bceu} = \varphi^{acheu} = \varphi^{ha't}$$

folgt, so geht die obige Bedingung für t in

$$\varepsilon^{-\frac{1}{2}ha'b'ceu(ceu-1)} = \varepsilon,$$

also in die Kongruenz

$$-\tfrac{1}{2}ha'b'ceu(ceu-1) \equiv 1 \,(\mathrm{mod.}\ e)$$

über. Da unter den Faktoren der linken Seite sich auch die Zahl e befindet, so ergibt sich durch Multiplikation mit 2 das Resultat

$$2 \equiv 0 \,(\mathrm{mod.}\ e),$$

also zufolge (28)

(37) $$e = 2, \quad \varepsilon^2 = 1,$$

und hierdurch geht die vorstehende Kongruenz in

$$ha'b'cu \equiv 1 \,(\mathrm{mod.}\ 2)$$

über, woraus mit Rücksicht auf (36) auch

(38) $$1 \equiv h \equiv a' \equiv b' \equiv c \equiv a \equiv b \,(\mathrm{mod.}\ 2)$$

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

$$mn \equiv d-1 \,(\mathrm{mod.}\ 2);$$

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 $\frac{1}{2}t(t-1) \equiv u \,(\mathrm{mod.}\ 2)$; 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) $$d \equiv 1 \,(\mathrm{mod.}\ 2)$$

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 $\equiv 4 \,(\mathrm{mod.}\ 8)$; 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:

$$\left\{\begin{aligned} & d = d, \\ & a' = \frac{a_1}{d}, \quad b' = \frac{b_1}{d}, \quad c' = \frac{c_1}{d}, \\ & a'' = \frac{ad}{b_1c_1}, \quad b'' = \frac{bd}{c_1a_1}, \quad c'' = \frac{cd}{a_1b_1}. \end{aligned}\right. \tag{4}$$

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

$$\left\{\begin{aligned} &\text{der Zahlen } b, c \quad \text{mit } a_2, \\ &\quad\ \ " \quad\ \ c, a \quad\ \ " \ b_2, \\ &\quad\ \ " \quad\ \ a, b \quad\ \ " \ c_2, \\ &\quad\ \ " \quad\ \ a, b, c \ " \ m, \end{aligned}\right. \tag{5}$$

so erhält man nach bekannten Regeln

$$\left\{\begin{aligned} a_2 &= \frac{bc}{a_1} = da'b'c'b''c'', \\ b_2 &= \frac{ca}{b_1} = da'b'c'c''a'', \\ c_2 &= \frac{ab}{c_1} = da'b'c'a''b''. \end{aligned}\right. \tag{6}$$

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

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

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

**) Vgl. D. § 178, S. 555.

§ 2.

Vier Zahlen.

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

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

und man bezeichne den größten gemeinsamen Teiler

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

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

setzen, wo die vier ganzen Zahlen

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

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

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

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

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

in welchen sechs neue ganze Zahlen

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

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

in welchen abermals vier neue ganze Zahlen:

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

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

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

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

Fügen wir zu diesen Gleichungen noch die selbstverständliche

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

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

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

§ 3.

Kombinationen.

Um diese Betrachtungen auf ein beliebiges System von n gegebenen Zahlen

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

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

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

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

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

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

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

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

dann wird

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

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

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

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

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

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

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

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

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

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

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

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

was zufolge A zunächst die Form

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$(8) \qquad \beta = \varrho + \omega, \quad \delta = \sigma + \omega,$$
$$(9) \qquad \alpha + \varrho = \gamma + \sigma = \alpha + \gamma$$

genügen.

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

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

und

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

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

$$\sigma + \tau = \alpha - (\gamma + \delta) = \alpha - (\alpha + \beta) = \alpha,$$
$$\varrho + \omega = \beta - (\gamma + \delta) = \beta - (\alpha + \beta) = \beta,$$
$$\varrho + \tau = \gamma - (\alpha + \beta) = \gamma - (\gamma + \delta) = \gamma,$$
$$\sigma + \omega = \delta - (\alpha + \beta) = \delta - (\gamma + \delta) = \delta,$$

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

Der Vollständigkeit wegen erwähnen wir ferner, daß offenbar immer

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

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

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

§ 4.

Bemerkungen über Dualgruppen.

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

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

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

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

Ein System $\mathfrak{A}$ von irgendwelchen Dingen $\alpha, \beta, \gamma \cdots$ soll eine Dualgruppe heißen, wenn es zwei Operationen $\dotplus$ 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 $\alpha, \beta, \gamma \cdots$, 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*) $\alpha, \beta, \gamma \cdots$ 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 $\alpha, \beta, \gamma \cdots$, 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 $\alpha, \beta, \gamma \cdots$, 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 $\alpha_1, \alpha_2 \cdots \alpha_n$ 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 $\alpha, \beta, \gamma \cdots$ 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, $\alpha, \beta, \gamma, \delta, \varepsilon$, 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 $\alpha + \dot{\omega}$ darstellbaren Dinge α_1 bezeichnen*), wo ω jedes Ding in $\mathfrak{A}$ bedeuten kann. Diese Systeme von der Form α' besitzen die folgenden sechs charakteristischen Eigenschaften, in welchen die beiden Operationen $\pm$ gar nicht mehr auftreten:

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

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

II. Das Ding α ist in α' enthalten.

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

IV. Ist das Ding α_1 in α' enthalten, so ist das System α'_1 ein Teil von α'.

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

VI. Für je zwei Dinge α, β in $\mathfrak{A}$ gibt es ein Ding μ in $\mathfrak{A}$, welches den beiden folgenden Bedingungen genügt: α' und β' sind Teile von μ', und wenn α', β' Teile von einem System μ'_2 sind, so ist auch μ' ein Teil von μ'_2.

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

Läßt man nun die Erinnerung an die Operationen $\pm$ gänzlich fallen, und nimmt man lediglich an, es gelten in einem System $\mathfrak{A}$ die vorstehenden sechs Eigenschaften, so kann man den Systemen α' eine zweite Klasse von Systemen α'' innerhalb $\mathfrak{A}$ gegenüberstellen, deren Erklärung die folgende ist. Bedeutet α irgendein Ding in $\mathfrak{A}$, so gibt es zufolge II. mindestens ein Ding α_2 von der Art, daß α in α'_2 enthalten ist, und mit α'' soll der Inbegriff aller dieser Dinge α_2 bezeichnet werden. Man wird sich leicht überzeugen, daß diese Systeme α'' (wenn man zugleich α_1, ν, μ, μ_2 bzw. durch α_2, μ, ν, ν_1 ersetzt) genau dieselben sechs Eigenschaften besitzen wie die Systeme α', und rückwärts ergibt sich aus den Systemen α'', falls diese gegeben sind, auf dieselbe Weise wieder die Konstruktion der Systeme α'.

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

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

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

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

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

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

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

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

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

*) Vgl. D. § 169, S. 499, Anmerkung.

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

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

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

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

und

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

also auch die beiden folgenden**):

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

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

§ 5.

Abelsche Gruppe $\mathfrak{G}$.

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

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

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

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

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

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

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

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

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

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

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

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

woraus

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§ 6.

Ganze Elemente in $\mathfrak{G}$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

also

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

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

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

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

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

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

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

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

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

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

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

also

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

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

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

also zufolge (1) auch

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

und hieraus ergibt sich das allgemeine Gesetz

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

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

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

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

wo k die algebraisch kleinste der Zahlen r, s bedeutet. In der aus allen Potenzen eines Elementes 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 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 $a + b$ von je zwei solchen Idealbrüchen a, 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 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 α eine bestimmte von Null verschiedene algebraische Zahl*) und o das System aller algebraischen Einheiten**), so bilden alle mit α assoziierten Zahlen, d. h. alle Produkte von der

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

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

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

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

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

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

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

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

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

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

Wir nennen ein Element $\mathfrak{a}$ der Gruppe $\mathfrak{G}$ ganz, wenn $\mathfrak{a} + \mathfrak{o} = \mathfrak{o}$ ist, im entgegengesetzten Falle gebrochen. Dann ergibt sich zunächst, daß alle Produkte und Summen von ganzen Elementen ebenfalls ganz sind; denn durch Addition der beiden Gleichungen $\mathfrak{a} + \mathfrak{o} = \mathfrak{o}$, $\mathfrak{b} + \mathfrak{o} = \mathfrak{o}$ erhält man $(\mathfrak{a} + \mathfrak{b}) + \mathfrak{o} = \mathfrak{o}$; multipliziert man ferner die erste mit $\mathfrak{b}$, so folgt $\mathfrak{ab} + \mathfrak{b} = \mathfrak{b}$, und wenn man auf beiden Seiten $\mathfrak{o}$ addiert, so ergibt sich $\mathfrak{ab} + \mathfrak{o} = \mathfrak{o}$, 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 $\mathfrak{ab}^{-1}$ ein ganzes Element $\mathfrak{g}$, also $\mathfrak{a} = \mathfrak{bg}$ 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

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

oder, was dasselbe sagt, durch

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

und zugleich gilt der Satz

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

*) Vgl. D. § 178, S. 555.

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

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

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

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

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

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

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

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

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

§ 7.

Lösung der Aufgabe.

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

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

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

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

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

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 $\alpha,\ \beta$ von 0 verschieden und ω beliebig, so ist

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

Beweis. Zunächst leuchtet ein, daß dieser Satz für $\omega = 0$ gilt. Denn wenn ε alle Elemente der Kombination α, ebenso η alle Elemente der Kombination β durchläuft, so ist $(\alpha,\ 0)$ zufolge (3) die Summe aller $(\varepsilon,\ 0)$, ebenso ist $(\beta,\ 0)$ die Summe aller $(\eta,\ 0)$, und $(\alpha + \beta,\ 0)$ ist die Summe aller $(\theta,\ 0)$, wo θ alle Elemente der Kombination $(\alpha + \beta)$ durchläuft. Nun tritt zwar, wenn α und β gemeinsame Elemente $\varepsilon = \eta$ besitzen, das Glied $(\varepsilon,\ 0) = (\eta,\ 0)$ auf der linken Seite der zu beweisenden Gleichung (4) sowohl in der Summe $(\alpha,\ 0)$ wie in der Summe $(\beta,\ 0)$ auf, allein zufolge des Satzes $\mathfrak{a} + \mathfrak{a} = \mathfrak{a}$ 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

$$\begin{aligned} &(\alpha + \varepsilon,\ \omega) = \mathfrak{a} + \mathfrak{c}, \qquad (\beta + \varepsilon,\ \omega) = \mathfrak{b} + \mathfrak{c}, \\ &(\alpha + \beta,\ \omega) = \mathfrak{a} + \mathfrak{b}, \quad (\alpha + \beta + \varepsilon,\ \omega) = \mathfrak{a} + \mathfrak{b} + \mathfrak{c}, \end{aligned}$$

und aus dem speziellen Produktsatz II in § 5 ergibt sich

$$\begin{aligned} &\mathfrak{a} = (\mathfrak{a} + \mathfrak{c})(\alpha,\ \omega + \varepsilon), \quad \mathfrak{b} = (\mathfrak{b} + \mathfrak{c})(\beta,\ \omega + \varepsilon), \\ &\mathfrak{a} + \mathfrak{b} = (\mathfrak{a} + \mathfrak{b} + \mathfrak{c})(\alpha + \beta,\ \omega + \varepsilon). \end{aligned}$$

Hieraus folgt weiter

$$\begin{aligned} (\mathfrak{a} + \mathfrak{c})(\mathfrak{b} + \mathfrak{c})\{(\alpha,\ \omega + \varepsilon) + (\beta,\ \omega + \varepsilon)\} &= \mathfrak{a}(\mathfrak{b} + \mathfrak{c}) + \mathfrak{b}(\mathfrak{a} + \mathfrak{c}) \\ &= \mathfrak{b}\mathfrak{c} + \mathfrak{c}\mathfrak{a} + \mathfrak{a}\mathfrak{b}; \end{aligned}$$

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 $= \mathfrak{o}$, 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 $(\alpha, \beta) + \mathfrak{o} = \mathfrak{o}$, 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

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

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 $=\mathfrak{o}$ 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

$$(\alpha,\beta)=\Pi(\alpha+\gamma_1,\beta+\gamma_2) \tag{8}$$

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.