XLVI.

Über die Theorie der ganzen algebraischen Zahlen.

[Supplement XI von Dirichlets Vorlesungen über Zahlentheorie, 4. Aufl., S. 434—657 (1894).]

Inhalt.

		Seite
§ 159.	Theorie der komplexen ganzen Zahlen von Gauß	2
§ 160.	Zahlenkörper	20
§ 161.	Permutationen eines Körpers	24
§ 162.	Resultanten von Permutationen	29
§ 163.	Multipla und Divisoren von Permutationen	30
§ 164.	Irreduzible Systeme. Endliche Körper	33
§ 165.	Permutationen endlicher Körper	41
§ 166.	Gruppen von Permutationen	50
§ 167.	Spuren, Normen, Diskriminanten	53
§ 168.	Moduln	60
§ 169.	Teilbarkeit der Moduln	62
§ 170.	Produkte und Quotienten von Moduln. Ordnungen	67
§ 171.	Kongruenzen und Zahlklassen	74
§ 172.	Endliche Moduln	80
§ 173.	Ganze algebraische Zahlen	90
§ 174.	Teilbarkeit der ganzen Zahlen	98
§ 175.	System der ganzen Zahlen eines endlichen Körpers	101
§ 176.	Zerlegung in unzerlegbare Faktoren. Ideale Zahlen	107
§ 177.	Ideale. Teilbarkeit und Multiplikation	116
§ 178.	Relative Primideale	121
§ 179.	Primideale	126
§ 180.	Normen der Ideale. Kongruenzen	130
§ 181.	Idealklassen und deren Komposition	139
§ 182.	Zerlegbare Formen und deren Komposition	146
§ 183.	Einheiten eines endlichen Körpers	156
§ 184.	Anzahl der Idealklassen	169
§ 185.	Beispiel aus der Kreisteilung	178
§ 186.	Quadratische Körper	200
§ 187.	Moduln in quadratischen Körpern	206

§ 159.

Der Begriff der ganzen Zahl hat in diesem Jahrhundert eine Erweiterung erfahren, durch welche der Zahlentheorie wesentlich neue Bahnen eröffnet sind; den ersten und wichtigsten Schritt auf diesem Gebiete hat Gauß*) getan, und wir wollen zunächst die Theorie der von ihm eingeführten ganzen komplexen Zahlen wenigstens in ihren wichtigsten Grundzügen darstellen, weil hierdurch das Verständnis der später folgenden Untersuchungen über die allgemeinsten ganzen algebraischen Zahlen gewiß erleichtert wird.

Bisher haben wir unter ganzen Zahlen ausschließlich die Zahlen

$$0, \pm 1, \pm 2, \pm 3, \pm 4 \ldots$$

verstanden, nämlich alle diejenigen Zahlen, welche durch wiederholte Addition und Subtraktion aus der Zahl 1 entstehen; diese Zahlen reproduzieren sich durch Addition, Subtraktion und Multiplikation, oder mit anderen Worten, die Summen, Differenzen und Produkte von je zwei ganzen Zahlen sind wieder ganze Zahlen. Dagegen führt die vierte Grundoperation, die Division, auf den umfassenderen Begriff der rationalen Zahlen, unter welchem Namen die Quotienten**) von irgend zwei ganzen Zahlen verstanden werden; offenbar reproduzieren sich diese rationalen Zahlen durch alle vier Grundoperationen. Jedes System von reellen oder komplexen Zahlen, welches diese fundamentale Eigenschaft der Reproduktion besitzt, wollen wir künftig einen Zahlkörper oder kurz einen Körper nennen; der Inbegriff R aller rationalen Zahlen ist daher ein Körper, und zwar bildet er das einfachste Beispiel eines solchen. Dieser Körper R der rationalen Zahlen besteht nun aus ganzen und gebrochenen, d. h. nicht ganzen Zahlen; die ersteren wollen wir in Zukunft rationale ganze Zahlen nennen, um sie von den neu einzuführenden ganzen Zahlen zu unterscheiden.

---

*) Theoria residuorum biquadraticorum. II. 1832. — Vgl. die Abhandlungen von Dirichlet: Recherches sur les formes quadratiques à coefficients et à indéterminées complexes (Crelles Journal, Bd. 24) und Untersuchungen über die Theorie der complexen Zahlen (Abh. d. Berliner Akad. 1841).

**) Dem Begriffe eines Quotienten gemäß wird es hier und im folgenden als selbstverständlich angesehen, daß der Divisor oder Nenner eine von Null verschiedene Zahl ist.

Wir wenden uns nun, indem wir zur Abkürzung $\sqrt{-1} = i$ setzen, zu der Betrachtung desjenigen Körpers J, welcher aus allen komplexen Zahlen ω von der Form

$$x + yi$$

besteht, wo x und y willkürliche rationale Zahlen bedeuten, die wir die Koordinaten der Zahl ω nennen wollen. Diese Zahlen ω bilden in der Tat einen Körper; denn wenn

$$\alpha = x_1 + y_1 i \text{ und } \beta = x_2 + y_2 i$$

irgend zwei solche Zahlen sind, so gehören auch ihre Summe, Differenz, ihr Produkt und Quotient, d. h. die Zahlen

$$\begin{aligned} \alpha \pm \beta &= (x_1 \pm x_2) + (y_1 \pm y_2) i \\ \alpha\beta &= (x_1 x_2 - y_1 y_2) + (x_1 y_2 + y_1 x_2) i \\ \frac{\alpha}{\beta} &= \frac{x_1 x_2 + y_1 y_2}{x_2^2 + y_2^2} + \frac{y_1 x_2 - x_1 y_2}{x_2^2 + y_2^2} i \end{aligned}$$

demselben System J an. Dieser Körper J, welcher offenbar auch alle rationalen Zahlen enthält, soll ein Körper zweiten Grades oder ein quadratischer Körper heißen, weil alle seine Zahlen ω durch wiederholte Anwendung der vier Grundoperationen aus der einen Zahl i entstehen, welche eine Wurzel der mit rationalen Koeffizienten behafteten quadratischen Gleichung

$$i^2 + 1 = 0$$

ist. Diese Gleichung hat die Zahl $-i$ zur zweiten Wurzel; ist nun $\omega = x + yi$ auf die angegebene Weise aus i entstanden, also eine Zahl des Körpers J, so wird aus der Zahl $-i$ durch dieselben Operationen die mit ω konjugierte Zahl $x - yi$ entstehen, die ebenfalls dem Körper J angehört, und welche wir immer mit ω' bezeichnen wollen. Dann ist umgekehrt die mit ω' konjugierte Zahl $(\omega')' = \omega$, und man überzeugt sich leicht, daß für je zwei Zahlen α, β des Körpers J die folgenden Gesetze gelten:

$$\begin{aligned} (\alpha \pm \beta)' &= \alpha' \pm \beta' \\ (\alpha\beta)' &= \alpha'\beta' \\ \left(\frac{\alpha}{\beta}\right)' &= \frac{\alpha'}{\beta'}. \end{aligned}$$

Unter der Norm einer Zahl ω verstehen wir das Produkt $\omega\omega'$ aus den beiden konjugierten Zahlen ω und ω', und wir bezeichnen diese Norm durch das Symbol $N(\omega)$; es wird daher

$$N(x + yi) = (x + yi)(x - yi) = x^2 + y^2,$$

und hieraus folgt, daß die Norm immer eine positive rationale Zahl ist und nur dann verschwindet, wenn $\omega = 0$, also $x = 0$ und $y = 0$ ist. Da ferner $(\alpha\beta)' = \alpha'\beta'$, also

$$(\alpha\beta)(\alpha\beta)' = (\alpha\alpha')(\beta\beta')$$

ist, so ergibt sich der Satz:

$$N(\alpha\beta) = N(\alpha)N(\beta),$$

d. h. die Norm eines Produktes ist gleich dem Produkte aus den Normen der Faktoren; und ein ganz ähnlicher Satz gilt offenbar auch für die Quotienten.

Wir teilen nun alle Zahlen des Körpers J in zwei große Klassen ein; eine solche Zahl $\omega = x + yi$ soll eine ganze komplexe oder kürzer eine ganze Zahl heißen, wenn ihre beiden Koordinaten x, y ganze rationale Zahlen sind; ist aber mindestens eine der beiden Koordinaten eine gebrochene Zahl, so soll auch ω eine gebrochene Zahl heißen. Offenbar bilden die ganzen rationalen Zahlen x einen Teil des Systems aller ganzen komplexen Zahlen, und umgekehrt ist jede ganze komplexe Zahl $x + yi$, wenn sie zugleich rational ist, notwendig eine ganze rationale Zahl x. Unter einer natürlichen Zahl verstehen wir nach altem Herkommen immer eine positive, also von Null verschiedene, ganze rationale Zahl.

Aus den obigen Formeln für die Summe, Differenz und das Produkt zweier in J enthaltenen Zahlen leuchtet nun zunächst ein, daß unsere ganzen Zahlen sich durch Addition, Subtraktion und Multiplikation reproduzieren. Die Analogie mit der Theorie der rationalen Zahlen veranlaßt uns daher, den Begriff der Teilbarkeit einzuführen: die ganze Zahl α heißt teilbar durch die ganze Zahl β, wenn $\alpha = \beta\gamma$, und γ ebenfalls eine ganze Zahl ist; zugleich heißt α ein Vielfaches oder Multiplum von β, und β ein Teiler oder Divisor oder Faktor von α, oder man sagt auch, β gehe in α auf. Aus dieser Erklärung, durch welche der Begriff der Teilbarkeit für rationale ganze Zahlen nicht geändert wird, ergeben sich (wie in § 3) die beiden folgenden Elementarsätze:

I. Sind α und β teilbar durch μ, so sind auch die Zahlen $\alpha + \beta$ und $\alpha - \beta$ teilbar durch μ. Denn aus $\alpha = \mu\alpha_1$ und $\beta = \mu\beta_1$ folgt $\alpha \pm \beta = \mu(\alpha_1 \pm \beta_1)$, und da α_1, β_1 ganze Zahlen sind, so gilt dasselbe auch von den Zahlen $\alpha_1 \pm \beta_1$.

II. Ist $\varkappa$ teilbar durch λ, und λ teilbar durch μ, so ist auch $\varkappa$ teilbar durch μ. Denn aus $\varkappa = \alpha\lambda$ und $\lambda = \beta\mu$ folgt $\varkappa = (\alpha\beta)\mu$, und da α und β ganze Zahlen sind, so ist auch $\alpha\beta$ eine ganze Zahl.

Ist $\omega = x + yi$ eine ganze Zahl, so ist offenbar die konjugierte Zahl $\omega' = x - yi$ ebenfalls eine ganze Zahl, und folglich ist $N(\omega)$ teilbar durch ω. Diese Norm ist immer eine natürliche Zahl, wenn ω von Null verschieden ist, und aus dem Satze über die Norm eines Produktes ergibt sich der folgende, welcher aber nicht umgekehrt werden darf:

Ist α teilbar durch β, so ist $N(\alpha)$ auch teilbar durch $N(\beta)$.

Unter einer Einheit wird jede ganze Zahl ε verstanden, welche ein Divisor der Zahl 1 ist und folglich auch in allen ganzen Zahlen aufgeht; nach dem vorstehenden Satze muß $N(\varepsilon)$ in $N(1)$, d. h. in der Zahl 1 aufgehen, und folglich muß

$$N(\varepsilon) = 1, \quad \text{d. h. } \varepsilon\varepsilon' = 1$$

sein; und umgekehrt leuchtet ein, daß jede ganze Zahl ε, deren Norm $= 1$ ist, gewiß eine Einheit ist. Setzt man nun $\varepsilon = x + yi$, so ist $x^2 + y^2 = 1$, und da x, y ganze rationale Zahlen sind, so ist entweder $x^2 = 1$ und $y = 0$, oder $x = 0$ und $y^2 = 1$; man erhält daher die folgenden vier Einheiten

$$\varepsilon = 1, \ -1, \ i, \ -i,$$

welche man auch in der Form

$$\varepsilon = i^n$$

zusammenfassen kann, wo n eine beliebige ganze rationale Zahl bedeutet. In der Theorie der rationalen Zahlen gibt es nur zwei Einheiten, nämlich die Zahlen ± 1.

Sind zwei ganze, von Null verschiedene Zahlen α, β gegenseitig durch einander teilbar, so sind die Quotienten

$$\frac{\beta}{\alpha} \text{ und } \frac{\alpha}{\beta}$$

ganze Zahlen, und da ihr Produkt $= 1$ ist, so sind sie notwendig Einheiten, mithin ist $\beta = \alpha\varepsilon$, wo ε eine Einheit; umgekehrt, wenn dies der Fall ist, so ist auch $\alpha = \beta\varepsilon'$, also ist jede der beiden Zahlen α, β durch die andere teilbar. Zwei solche Zahlen heißen assoziierte Zahlen, und es leuchtet ein, daß je vier assoziierte Zahlen

$$\alpha, \ \alpha i, \ -\alpha, \ -\alpha i$$

bei allen Fragen der Teilbarkeit sich ganz gleich verhalten; ist nämlich eine ganze Zahl α teilbar durch eine ganze Zahl μ, so ist auch jede mit α assoziierte Zahl durch jede mit μ assoziierte Zahl teilbar. Wir sehen daher im folgenden vier solche assoziierte Zahlen als nicht wesentlich verschieden an.

Um nun eine ausreichende Grundlage für die Theorie der Teilbarkeit in unserem Gebiete der ganzen komplexen Zahlen zu gewinnen, bemerken wir zunächst, daß jede dem Körper J angehörige Zahl $\omega = x + yi$, mag sie ganz oder gebrochen sein, stets als Summe von zwei Zahlen ν und ω_1 dargestellt werden kann, von denen die erstere ν eine ganze Zahl ist, während $N(\omega_1) < 1$ wird; sondert man nämlich aus den rationalen Koordinaten x, y die nächstliegenden ganzen Zahlen r, s aus, so wird $x = r + x_1$, $y = s + y_1$, wo x_1, y_1 rationale Zahlen bedeuten, deren absolute Werte $\leqq \frac{1}{2}$ sind; setzt man daher $\nu = r + si$, $\omega_1 = x_1 + y_1 i$, so wird $\omega = \nu + \omega_1$, wo ν eine ganze Zahl, und

$$N(\omega_1) = x_1^2 + y_1^2 \leqq \tfrac{1}{2} < 1$$

ist. Hieraus ergibt sich unmittelbar der folgende wichtige Satz:

Ist α eine beliebige ganze, und β eine von Null verschiedene ganze Zahl, so kann man zwei ganze Zahlen γ und ν immer so wählen, daß

$$\alpha = \nu\beta + \gamma, \quad \text{und} \quad N(\gamma) < N(\beta)$$

wird.

Da nämlich der Quotient der beiden Zahlen α, β eine dem Körper J angehörige Zahl ω ist, so kann man

$$\frac{\alpha}{\beta} = \nu + \omega_1, \quad \text{also} \quad \alpha = \nu\beta + \beta\omega_1$$

setzen, wo ν eine ganze Zahl, und $N(\omega_1) < 1$ ist; hieraus folgt aber, daß die Zahl $\gamma = \beta\omega_1 = \alpha - \nu\beta$ ebenfalls eine ganze Zahl, und daß ihre Norm

$$N(\gamma) = N(\beta)\, N(\omega_1) < N(\beta)$$

ist, was zu beweisen war.

Mit Hilfe dieses Satzes läßt sich nun die Aufgabe behandeln, alle gemeinschaftlichen Divisoren von zwei gegebenen ganzen Zahlen α, β zu finden (vgl. § 4); behalten nämlich ν und γ die eben festgesetzte Bedeutung, so ergibt sich aus den obigen Elementarsätzen I. und II., daß jeder gemeinschaftliche Divisor von α, β auch gemein-

schaftlicher Divisor von β, γ ist, und umgekehrt; man wird daher, wenn γ nicht $= 0$ ist, wieder zwei ganze Zahlen δ und π so bestimmen, daß

$$\beta = \pi\gamma + \delta, \quad \text{und} \quad N(\delta) < N(\gamma)$$

wird, und wenn δ noch nicht $= 0$ ist, wird man auf dieselbe Weise so lange fortfahren, bis unter den sukzessiven Divisionsresten γ, δ ... die Zahl Null auftritt. Dies muß notwendig nach einer endlichen Anzahl von Operationen geschehen, weil die Normen dieser Reste natürliche Zahlen sind, die beständig abnehmen. Ist μ der letzte von diesen Resten, welcher einen von Null verschiedenen Wert hat, so haben wir eine Kette von Gleichungen von der Form

$$\begin{aligned} \alpha &= \nu\beta + \gamma \\ \beta &= \pi\gamma + \delta \\ &\cdots\cdots \\ \varkappa &= \sigma\lambda + \mu \\ \lambda &= \tau\mu, \end{aligned}$$

aus welcher hervorgeht, daß μ gemeinschaftlicher Divisor von α, β, und daß umgekehrt jeder gemeinschaftliche Divisor von α, β notwendig ein Divisor von μ ist. Diese Zahl μ, und ebenso jede mit ihr assoziierte Zahl, heißt der größte gemeinschaftliche Divisor von α und β, weil er unter allen gemeinschaftlichen Divisoren die größte Norm hat. Sind α und β rational, so ist μ ebenfalls rational und identisch mit derjenigen Zahl, welche in der Theorie der rationalen Zahlen der größte gemeinschaftliche Divisor von α und β genannt wurde.

Durch Umkehrung der obigen Gleichungen, wobei man sich wieder des Eulerschen Algorithmus (§ 23) bedienen kann, ergibt sich, daß immer zwei ganze Zahlen ξ, η existieren, welche der Bedingung

$$\alpha\xi + \beta\eta = \mu$$

genügen (im Falle $\gamma = 0$, $\mu = \beta$ kann man $\xi = 0$, $\eta = 1$ setzen), und derselbe Satz gilt offenbar auch dann, wenn μ nicht den größten gemeinschaftlichen Teiler von α, β selbst, sondern irgendeine durch denselben teilbare Zahl bedeutet.

Nachdem für je zwei ganze Zahlen α, β (die nicht beide verschwinden) die Existenz eines größten gemeinschaftlichen Teilers nachgewiesen, und zugleich eine Methode zur Auffindung desselben angegeben ist, leuchtet ein, daß die Lehre von der Teilbarkeit der komplexen

ganzen Zahlen sich ganz ähnlich gestalten muß, wie bei den rationalen Zahlen. Wir heben zunächst folgende Punkte hervor. Zwei ganze Zahlen α, β heißen relative Primzahlen oder Zahlen ohne gemeinschaftlichen Divisor, wenn sie außer den vier Einheiten keinen gemeinschaftlichen Divisor besitzen; es gibt dann immer zwei ganze Zahlen ξ, η, welche der Bedingung

$$\alpha\xi + \beta\eta = 1$$

genügen, und umgekehrt folgt aus der vorstehenden Gleichung, daß α, β relative Primzahlen sind. Ist nun ω eine beliebige ganze Zahl, so ergibt sich aus

$$\alpha(\omega\xi) + (\beta\omega)\eta = \omega,$$

daß jeder gemeinschaftliche Teiler von α und $\beta\omega$ notwendig Divisor von ω ist (vgl. § 5); wenn daher ω ebenfalls relative Primzahl zu α ist, so folgt, daß auch das Produkt $\beta\omega$ relative Primzahl zu α ist, und dieser Satz, wiederholt angewendet, liefert den folgenden:

Wenn jede der Zahlen $\alpha_1, \alpha_2, \alpha_3 \ldots$ relative Primzahl zu jeder der Zahlen $\beta_1, \beta_2 \ldots$ ist, so sind auch die beiden Produkte $\alpha_1\alpha_2\alpha_3 \ldots$ und $\beta_1\beta_2 \ldots$ relative Primzahlen.

Aus derselben Gleichung ergeben sich offenbar auch die folgenden Sätze:

Sind α, β relative Primzahlen, und ist $\beta\omega$ teilbar durch α, so ist auch ω teilbar durch α.

Ist ω ein gemeinschaftliches Multiplum der beiden relativen Primzahlen α, β, so ist ω auch durch ihr Produkt $\alpha\beta$ teilbar.

Unter einer komplexen Primzahl ist eine ganze Zahl π zu verstehen, welche keine Einheit ist, und deren Divisoren entweder mit π assoziiert oder Einheiten sind (vgl. § 8). Ist nun α eine beliebige ganze Zahl, so muß einer und nur einer der beiden folgenden Fälle eintreten: entweder ist α teilbar durch die Primzahl π, oder α ist relative Primzahl zu π; denn der größte gemeinschaftliche Teiler der beiden Zahlen α, π ist entweder assoziiert mit π oder eine Einheit. Mit Rücksicht auf das Vorhergehende folgt hieraus offenbar der Satz:

Wenn ein Produkt aus mehreren ganzen Zahlen α, β, $\gamma \ldots$ durch eine Primzahl π teilbar ist, so geht π mindestens in einem der Faktoren α, β, $\gamma \ldots$ auf.

Jede ganze, von Null verschiedene Zahl α ist nun entweder eine Einheit, oder eine Primzahl, oder sie besitzt mindestens einen Divisor β, welcher weder eine Einheit, noch mit α assoziiert ist; in diesem letzten Falle heißt α eine zusammengesetzte Zahl, und wenn $\alpha = \beta\lambda$ gesetzt wird, so ist auch λ keine Einheit, und da $N(\alpha) = N(\beta)N(\lambda)$ ist, so ergibt sich $N(\alpha) > N(\beta) > 1$, weil die vier Einheiten die einzigen Zahlen sind, deren Norm $= 1$ ist. Hieraus folgt leicht (vgl. § 8), daß mindestens eine in α aufgehende Primzahl existiert; denn wenn β noch keine Primzahl, mithin eine zusammengesetzte Zahl ist, so besitzt sie wieder einen Divisor γ, der der Bedingung $N(\beta) > N(\gamma) > 1$ genügt, und wenn γ noch keine Primzahl ist, so kann man in derselben Weise so lange fortfahren, bis in der Reihe der Zahlen α, β, γ ... eine Primzahl π auftritt, was nach einer endlichen Anzahl von Zerlegungen geschehen muß, weil die Reihe der beständig abnehmenden natürlichen Zahlen $N(\alpha)$, $N(\beta)$, $N(\gamma)$ ... notwendig einmal abbrechen wird. Offenbar ist nun α teilbar durch π und folglich von der Form $\pi\alpha_1$, wo α_1 entweder eine Primzahl oder eine zusammengesetzte Zahl ist; im letzteren Falle kann man wieder $\alpha_1 = \pi_1\alpha_2$, also $\alpha = \pi\pi_1\alpha_2$ setzen, wo π_1 eine Primzahl bedeutet, und wenn α_2 noch keine Primzahl, sondern eine zusammengesetzte Zahl ist, so kann man in derselben Weise fortfahren, bis in der Reihe der Zahlen α_1, α_2 ... eine Primzahl $\alpha_n = \pi_n$ auftritt, was, wie sich abermals aus der Betrachtung der Normen ergibt, nach einer endlichen Anzahl von Zerlegungen geschehen muß. Dann ist die zusammengesetzte Zahl

$$\alpha = \pi\pi_1\pi_2 \dots \pi_n$$

dargestellt als ein Produkt von $n + 1$ Faktoren, welche sämtlich Primzahlen sind. Gesetzt nun, dieselbe Zahl α sei auch ein Produkt aus $m + 1$ Primzahlen ϱ, ϱ_1, ϱ_2 ... ϱ_m, also

$$\pi\pi_1\pi_2 \dots \pi_n = \varrho\varrho_1\varrho_2 \dots \varrho_m,$$

so muß nach dem oben bewiesenen Satze die in diesem Produkte α aufgehende Primzahl π notwendig in einem der Faktoren ϱ, ϱ_1, ϱ_2 ... ϱ_m, z. B. in ϱ aufgehen; da aber ϱ ebenfalls eine Primzahl ist und folglich außer den Einheiten nur solche Divisoren besitzt, welche mit ϱ assoziiert sind, so muß $\pi = \varepsilon\varrho$ sein, wo ε eine Einheit bedeutet, und hieraus folgt durch Division mit ϱ die Gleichung

$$\varepsilon\pi_1\pi_2 \dots \pi_n = \varrho_1\varrho_2 \dots \varrho_m;$$

da nun das Produkt rechter Hand durch die Primzahl π_1 teilbar ist, so muß zufolge derselben Schlüsse die Zahl π_1 mit einem der Faktoren dieses Produktes, z. B. mit ϱ_1 assoziiert, also von der Form $\varepsilon_1 \varrho_1$ sein, wo ε_1 eine Einheit bedeutet. Die durch Division mit ϱ_1 entstehende Gleichung

$$\varepsilon \varepsilon_1 \pi_2 \dots \pi_n = \varrho_2 \dots \varrho_m$$

kann man offenbar in derselben Weise weiter behandeln; es ergibt sich hieraus zunächst, daß m nicht kleiner als n ist, und daß man $\pi_2 = \varepsilon_2 \varrho_2$, $\pi_3 = \varepsilon_3 \varrho_3 \dots \pi_n = \varepsilon_n \varrho_n$ setzen kann, wo ε_2, $\varepsilon_3 \dots \varepsilon_n$ Einheiten bedeuten. Wäre nun $m > n$, so würde sich

$$\varepsilon \varepsilon_1 \varepsilon_2 \dots \varepsilon_n = \varrho_{n+1} \varrho_{n+2} \dots \varrho_m$$

ergeben, und es wäre folglich ein Produkt von lauter Einheiten durch mindestens eine Primzahl ϱ_{n+1} teilbar, was unmöglich ist. Mithin ist $m = n$, und die beiden Zerlegungen der Zahl α in Primfaktoren sind wesentlich identisch, d. h. wenn in der einen Zerlegung genau r Faktoren auftreten, welche mit einer und derselben Primzahl π assoziiert sind, so finden sich auch in der anderen Zerlegung genau r solche mit π assoziierte Faktoren. In diesem Sinne ist der hiermit bewiesene Fundamentalsatz (vgl. § 8) zu verstehen:

Jede zusammengesetzte Zahl läßt sich stets und wesentlich nur auf eine einzige Weise als Produkt aus einer endlichen Anzahl von Primzahlen darstellen.

Es ist nun auch nicht schwer, sich einen deutlichen Überblick über alle in unserem Körper J vorhandenen komplexen Primzahlen π zu verschaffen. Es gibt offenbar unendlich viele natürliche Zahlen, die durch eine bestimmte Primzahl π teilbar sind (eine solche ist z. B. $N(\pi) = \pi\pi'$); von allen diesen Zahlen muß die kleinste p notwendig eine natürliche Primzahl, d. h. eine positive Primzahl des Körpers R, also eine Primzahl im alten Sinne des Wortes sein; denn p ist > 1, weil sonst π eine Einheit wäre, und p kann auch nicht ein Produkt von zwei kleineren natürlichen Zahlen sein, weil sonst π als Primzahl in einer derselben aufgehen müßte, was aber der Definition von p widerspricht. Jede komplexe Primzahl π ist daher Divisor von einer (und offenbar auch nur von einer einzigen) natürlichen Primzahl p, und es werden folglich alle komplexen Primzahlen π entdeckt werden, wenn man die Divisoren aller natürlichen Primzahlen p aufsucht. Es sei daher p eine natürliche Primzahl,

und π eine in p aufgehende komplexe Primzahl, so ist $N(\pi)$ ein Divisor von $p^2 = N(p)$, und folglich ist $N(\pi)$ entweder $= p$ oder $= p^2$; je nachdem der erste oder zweite Fall eintritt, wollen wir π eine Primzahl ersten oder zweiten Grades nennen. Im ersten Falle ist $p = \pi\pi' = N(\pi)$ das Produkt aus zwei konjugierten Primzahlen ersten Grades, weil offenbar π' stets gleichzeitig mit π eine Primzahl ist; im zweiten Falle ist $p = \pi\varepsilon$, $N(\varepsilon) = 1$, also ist p assoziiert mit π und folglich selbst eine komplexe Primzahl zweiten Grades.

Die Entscheidung über das Eintreten des einen oder anderen Falles je nach der Beschaffenheit der natürlichen Primzahl p würde sich augenblicklich aus der Theorie der binären quadratischen Formen von der Determinante -1 ergeben (§ 68); allein unser Hauptziel besteht gerade darin, nachzuweisen, daß die Theorie der Formen überhaupt entbehrlich ist, oder vielmehr, daß sie auf die einfachere und zugleich tiefer eindringende Theorie der ganzen algebraischen Zahlen zurückgeführt werden kann. Wir suchen daher auch hier unsere Aufgabe selbständig zu lösen. Es leuchtet nun ein, daß der zweite Fall jedesmal stattfinden muß, wenn $p \equiv 3 \pmod 4$ ist; denn da die Norm einer jeden ganzen komplexen Zahl eine Summe von zwei ganzen rationalen Quadratzahlen ist und folglich, durch vier dividiert, den Rest 0, 1 oder 2 läßt, je nachdem beide Quadrate gerade, oder eines, oder beide ungerade sind, so kann der erste Fall höchstens dann eintreten, wenn $p = 2$, oder $p \equiv 1 \pmod 4$ ist. Wir erhalten hiermit das erste Resultat:

Jede natürliche Primzahl p von der Form $4h + 3$ ist eine komplexe Primzahl zweiten Grades.

Der Fall $p = 2$ erledigt sich unmittelbar durch die Bemerkung, daß

$$2 = N(1 - i) = (1 - i)(1 + i) = i(1 - i)^2$$

ist, und liefert das Resultat:

Die Zahl 2 ist assoziiert mit dem Quadrate der Primzahl ersten Grades $1 - i$.

Es handelt sich jetzt nur noch um die natürlichen Primzahlen p von der Form $4h + 1$; die Entscheidung wird sofort gegeben, sobald man aus der Theorie der rationalen Zahlen den Satz (§ 40) entlehnt, daß die Zahl -1 quadratischer Rest von jeder solchen Zahl p ist, daß also eine ganze rationale Zahl x existiert, für welche $x^2 + 1$,

d. h. das Produkt $(x + i)(x - i)$ durch p teilbar ist; da nämlich keiner der beiden Faktoren $x + i$, $x - i$ durch p teilbar ist, so kann (nach dem obigen Satze) p keine komplexe Primzahl sein, und folglich ist p gewiß das Produkt aus zwei konjugierten Primzahlen ersten Grades π und π'. Setzt man $\pi = a + bi$, so ergibt sich auf diese Weise der Fermatsche Satz (§ 68)

$$p = a^2 + b^2.$$

Die beiden Primzahlen π, π' können nicht assoziiert sein, weil aus $a - bi = i^n(a + bi)$ entweder $b = 0$, oder $a = 0$, oder $a^2 = b^2$ folgen würde, was alles unmöglich ist. Mithin ergibt sich das letzte Resultat:

Jede natürliche Primzahl p von der Form $4h + 1$ ist das Produkt aus zwei konjugierten, nicht assoziierten komplexen Primzahlen ersten Grades.

Will man aber den obigen Satz aus der Theorie der quadratischen Reste nicht voraussetzen, so ergibt sich dasselbe Resultat im weiteren Fortgange der Theorie unserer komplexen Zahlen, wie folgt. Zwei ganze komplexe Zahlen α, β heißen kongruent in bezug auf eine dritte μ, den Modulus, wenn ihre Differenz $\alpha - \beta$ durch μ teilbar ist, und dies wird durch die Kongruenz

$$\alpha \equiv \beta \pmod{\mu}$$

angedeutet. Es leuchtet dann ohne weiteres ein, daß die elementaren Sätze über Kongruenzen (§ 17) von den rationalen Zahlen unmittelbar auf die komplexen Zahlen übertragen werden dürfen, und es ergibt sich ebenso wie früher (§ 26), daß eine Kongruenz n^{ten} Grades, deren Modulus eine komplexe Primzahl ist, niemals mehr als n inkongruente Wurzeln besitzen kann. Ist nun p eine natürliche Primzahl von der Form $4h + 1$, so wird die Kongruenz $(p - 1)^{\text{ten}}$ Grades

$$\omega^{p-1} \equiv 1 \pmod{p}$$

durch mindestens p inkongruente Zahlen ω, nämlich durch $\omega = i$ und (nach § 19) durch $\omega = 1, 2, 3 \ldots (p - 1)$ befriedigt; mithin ist der Modulus p keine komplexe Primzahl, und hieraus folgt dasselbe Resultat wie oben.

Nachdem die Grundlagen der Theorie der komplexen ganzen Zahlen im vorhergehenden gewonnen sind, wollen wir uns darauf beschränken, einige wenige Fragen zu behandeln, bei deren Auswahl uns der Wunsch leitet, gewisse Begriffe, welche in der später folgenden

allgemeinen Theorie der ganzen algebraischen Zahlen auftreten werden, an dem einfachen, uns vorliegenden Beispiel des Körpers J zu entwickeln.

Ist μ eine ganze komplexe, und zwar von Null verschiedene Zahl, so teilen wir alle ganzen komplexen Zahlen in Zahl-Klassen ein, indem wir zwei Zahlen stets und nur dann in dieselbe Klasse aufnehmen, wenn sie in bezug auf μ kongruent sind (vgl. § 18); der Grund für die Möglichkeit einer solchen Einteilung liegt darin, daß zwei mit einer dritten kongruente Zahlen notwendig auch miteinander kongruent sind. Wir stellen uns die Aufgabe, die Anzahl dieser verschiedenen Klassen zu bestimmen. Zu diesem Zweck betrachten wir vorläufig nur eine einzige von diesen Klassen, nämlich den Inbegriff $\mathfrak{m}$ aller derjenigen Zahlen, welche durch μ teilbar, d. h. $\equiv 0 \pmod{\mu}$ sind. Dieser Inbegriff $\mathfrak{m}$ ist identisch mit dem System aller Zahlen von der Form $\mu(x + yi)$, wo x und y willkürliche ganze rationale Zahlen bedeuten. Auf solche homogene lineare Formen, in welchen die Variablen ganze rationale Zahlen sind, werden wir in der Folge*) sehr häufig stoßen, und wir wollen, wenn z. B. α, β irgendwelche reelle oder komplexe Konstanten, x und y aber willkürliche ganze rationale Zahlen bedeuten, den Inbegriff aller in der Linearform $\alpha x + \beta y$ enthaltenen Werte zur Abkürzung mit dem Symbol $[\alpha, \beta]$ bezeichnen, welches also von jetzt an in ganz anderer Bedeutung gebraucht wird, als früher bei dem Eulerschen Kettenbruch-Algorithmus. Die beiden Konstanten α, β, welche wir die Basiszahlen des Systems $[\alpha, \beta]$ nennen, können nun auf unendlich mannigfaltige Weise abgeändert, d. h. durch andere Basiszahlen α_1, β_1 ersetzt werden, und zwar so, daß das System $[\alpha_1, \beta_1]$ vollständig identisch mit dem System $[\alpha, \beta]$ bleibt. Dies wird z. B. immer dann eintreten, wenn zwischen den beiden Paaren von Basiszahlen zwei Relationen von der Form

$$\alpha = p\alpha_1 + q\beta_1, \quad \beta = r\alpha_1 + s\beta_1$$

stattfinden, wo p, q, r, s vier ganze rationale Zahlen bedeuten, deren Determinante

$$ps - qr = \pm 1$$

ist; denn hieraus folgt umgekehrt

$$\pm\alpha_1 = s\alpha - q\beta, \quad \pm\beta_1 = -r\alpha + p\beta,$$

*) Vgl. §§ 168, 172.

mithin ist jede Zahl, welche dem einen der beiden Systeme $[\alpha, \beta]$, $[\alpha_1, \beta_1]$ angehört, auch in dem anderen enthalten, was wir kurz durch $[\alpha, \beta] = [\alpha_1, \beta_1]$ ausdrücken wollen.

Eine solche Transformation der Basis wollen wir auf unseren Fall anwenden, in welchem es sich um das System

$$\mathfrak{m} = [\mu, \mu i]$$

aller durch μ teilbaren Zahlen $\mu(x + yi)$ handelt. Wir bezeichnen mit m die größte in μ aufgehende natürliche Zahl und setzen demgemäß

$$\mu = m(p - qi), \quad \mu i = m(q + pi),$$

wo p, q ganze rationale Zahlen ohne gemeinschaftlichen Teiler bedeuten; hierauf wählen wir (nach § 24) zwei ganze rationale Zahlen r, s, welche der Bedingung

$$ps - qr = 1$$

genügen, und setzen

$$a = p^2 + q^2, \quad b = pr + qs,$$

so ist

$$ma = p.\mu + q.\mu i$$
$$m(b + i) = r.\mu + s.\mu i,$$

und hieraus folgt nach der obigen Bemerkung, daß diese beiden Zahlen ma und $m(b + i)$ ebenfalls eine Basis des Systems $\mathfrak{m}$ bilden, d. h. es wird

$$\mathfrak{m} = [ma, m(b + i)].$$

Mit Hilfe dieser Transformation können wir leicht die Anzahl aller in bezug auf den Modul μ inkongruenten Zahlen bestimmen. Denn wenn

$$\omega = h + ki$$

eine beliebige gegebene ganze komplexe Zahl ist, so erhält man die Klasse, welche aus allen mit ihr kongruenten Zahlen

$$\omega_1 = h_1 + k_1 i$$

besteht, indem man

$$\omega_1 = \omega + max + m(b + i)y,$$

also

$$h_1 = h + max + mby, \quad k_1 = k + my$$

setzt, wo x, y alle ganzen rationalen Zahlen durchlaufen; aus der Form dieser beiden Gleichungen geht aber hervor, daß man zuerst y, hierauf x immer und nur auf eine einzige Weise so bestimmen kann, daß

$$0 \leqq k_1 < m \text{ und } 0 \leqq h_1 < ma$$

wird. Es gibt daher in jeder Klasse einen und nur einen Repräsentanten $\omega_1 = h_1 + k_1 i$, welcher den beiden vorstehenden Bedingungen genügt; mithin ist die Anzahl aller verschiedenen Klassen gleich der Anzahl aller verschiedenen, diese Bedingungen erfüllenden Paare h_1, k_1, also gleich dem Produkte $m^2 a = N(\mu)$ aus der Anzahl m der Werte von k_1 und der Anzahl ma der Werte von h_1. Wir erhalten mithin das folgende Resultat:

Die Anzahl aller in bezug auf den Modul μ inkongruenten Zahlen ist $= N(\mu)$.

Es hat nun auch keine Schwierigkeit, die Anzahl $\psi(\mu)$ aller derjenigen von diesen inkongruenten Zahlen zu bestimmen, welche relative Primzahlen zum Modul μ sind; diese Funktion $\psi(\mu)$ hat für unsere jetzige Zahlentheorie augenscheinlich dieselbe Wichtigkeit, wie die Funktion $\varphi(m)$ für die Theorie der rationalen Zahlen (§§ 11 — 14, 138); durch Betrachtungen, welche den damals angestellten ganz ähnlich sind, findet man

$$\psi(\mu) = 1,$$

wenn μ eine Einheit ist, sonst aber

$$\psi(\mu) = N(\mu) \prod \left(1 - \frac{1}{N(\pi)}\right),$$

wo das Produktzeichen sich auf alle wesentlich verschiedenen, in μ aufgehenden Primzahlen π bezieht; außerdem ist

$$\psi(\mu_1 \mu_2) = \psi(\mu_1)\psi(\mu_2),$$

wenn μ_1, μ_2 relative Primzahlen sind, und

$$\Sigma \psi(\delta) = N(\mu),$$

wo das Summenzeichen sich auf alle wesentlich verschiedenen Divisoren δ der Zahl μ bezieht. Ist ferner ω relative Primzahl zu μ, so ist stets

$$\omega^{\psi(\mu)} \equiv 1 \pmod{\mu},$$

was dem Satze von Fermat entspricht (§§ 19, 127). Wir müssen aber der Kürze halber die Durchführung der Beweise dieser Sätze dem Leser überlassen, und wir dürfen dies um so eher tun, als wir später (§ 180) dieselben Fragen in ihrer allgemeinsten Form behandeln werden.

Dagegen wollen wir noch mit einigen Worten auf den Zusammenhang eingehen, welcher zwischen der Theorie der komplexen ganzen

Zahlen und derjenigen der quadratischen Formen von der Determinante — 1 besteht. Wir haben oben das System $\mathfrak{m} = [\mu, \mu i]$ aller durch μ teilbaren Zahlen in die Form $[m a, m(b + i)]$ gebracht, wo die Zahlen m, a, b nach gewissen Regeln aus der gegebenen Zahl μ abzuleiten waren; von diesen drei Zahlen waren m und a völlig bestimmt, während b von der Wahl der beiden Hilfszahlen r, s abhing; jedes andere Paar r_1, s_1, welches der Bedingung

$$p s_1 - q r_1 = 1$$

genügt, ist (nach § 24) von der Form

$$r_1 = r + h p, \; s_1 = s + h q,$$

wo h eine willkürliche ganze rationale Zahl bedeutet, und liefert an Stelle von b die Zahl

$$b_1 = p r_1 + q s_1 = b + h a \equiv b \pmod{a};$$

die rationalen Zahlen b_1 durchlaufen daher alle Individuen einer völlig bestimmten Zahlklasse in bezug auf den Modul a, und es ist offenbar gleichgültig, welchen Repräsentanten b dieser Klasse man wählt. Dieselbe läßt sich auch direkt, ohne Zuziehung der Hilfszahlen r, s definieren; da nämlich $a = p^2 + q^2$ ist, so ergibt sich aus der Definition von b, daß

$$p b \equiv q, \; q b \equiv -p \pmod{a}$$

ist, und da jede der beiden gegebenen Zahlen p, q, weil sie keinen gemeinschaftlichen Teiler haben, notwendig relative Primzahl zu a ist, so ist b durch jede einzelne dieser beiden Kongruenzen vollständig bestimmt in bezug auf den Modul a. Quadriert man eine dieser Kongruenzen und bedenkt, daß $p^2 \equiv -q^2 \pmod{a}$ ist, so ergibt sich

$$b^2 \equiv -1 \pmod{a};$$

es ist folglich

$$b^2 = -1 + a c,$$

wo c, wie a, eine natürliche Zahl, und (a, b, c) ist eine positive quadratische Form von der Determinante — 1. Nun sind alle durch μ teilbaren, also in dem System $\mathfrak{m}$ enthaltenen Zahlen λ von der Form

$$\lambda = m(a x + (b + i) y),$$

wo x, y willkürliche ganze rationale Zahlen bedeuten, und durch Multiplikation mit der konjugierten Zahl λ' erhält man, weil $m^2 a = N(\mu)$ ist, das Resultat

$$N(\lambda) = N(\mu)(a x^2 + 2 b x y + c y^2).$$

Auf diese Weise führt jede bestimmte ganze komplexe Zahl μ zu einer bestimmten Schar von parallelen*) quadratischen Formen (a, b, c), deren Determinante $= -1$ ist.

Umgekehrt, wenn (a, b, c) eine solche (positive) Form, und folglich

$$ac = (b + i)(b - i)$$

ist, so bezeichnen wir mit γ den größten gemeinschaftlichen Teiler der beiden ganzen komplexen Zahlen a und $b + i$, und setzen

$$a = \alpha\gamma, \quad b + i = \beta\gamma;$$

da nun α, β relative Primzahlen sind und beide in der Zahl $\alpha c = \beta(b - i)$ aufgehen, so muß diese durch das Produkt $\alpha\beta$ teilbar sein, und folglich ist

$$c = \beta\delta, \quad b - i = \alpha\delta,$$

wo δ ebenfalls eine ganze komplexe Zahl bedeutet. Ersetzt man, was stets erlaubt ist, alle hier auftretenden Zahlen durch die konjugierten Zahlen, so ergibt sich

$$a = \alpha'\gamma', \quad b + i = \alpha'\delta',$$

und da γ der größte gemeinschaftliche Teiler dieser beiden Zahlen ist, so muß die in beiden aufgehende Zahl α' notwendig auch in γ aufgehen; setzt man demgemäß

$$\gamma = \varepsilon\alpha',$$

so folgt

$$a = \varepsilon\alpha\alpha' = \varepsilon N(\alpha),$$

mithin ist ε eine natürliche Zahl, und da dieselbe in γ, also auch in $b + i$ aufgeht, so muß sie $= 1$ sein. Wir erhalten daher $\gamma = \alpha'$, also

$$a = \alpha\alpha' = N(\alpha), \quad b + i = \beta\alpha';$$

da aber $b + i = \alpha'\delta'$, so folgt $\delta' = \beta$, $\delta = \beta'$, mithin

$$c = \beta\beta' = N(\beta), \quad b - i = \alpha\beta'.$$

Man setze nun

$$\alpha = p + qi, \quad \beta = r + si,$$

so folgt

$$a = p^2 + q^2, \quad c = r^2 + s^2$$
$$b = pr + qs, \quad 1 = ps - qr,$$

mithin geht die Form $(1, 0, 1)$ durch die Substitution $\left(\begin{smallmatrix} p, & r \\ q, & s \end{smallmatrix}\right)$ in die Form (a, b, c) über (§ 54); unsere Theorie der ganzen komplexen

*) Vgl. § 56, Anmerkung.

Zahlen liefert also unmittelbar den Beweis, daß alle (positiven) Formen von der Determinante -1 äquivalent sind (§ 68). —

Genau in derselben Weise, wie hier die ganzen komplexen Zahlen $x + yi$ untersucht sind, würden sich noch manche andere Gebiete von ganzen Zahlen behandeln lassen. Bedeutet z. B. θ eine Wurzel von einer der folgenden acht quadratischen Gleichungen

$$\theta^2 + \theta + 1 = 0, \quad \theta^2 + \theta + 2 = 0, \quad \theta^2 + 2 = 0, \quad \theta^2 + \theta + 3 = 0,$$
$$\theta^2 + \theta - 1 = 0, \quad \theta^2 - 2 = 0, \quad \theta^2 - 3 = 0, \quad \theta^2 + \theta - 3 = 0,$$

und läßt man x, y alle ganzen und gebrochenen rationalen Zahlen durchlaufen, so bilden die entsprechenden Zahlen von der Form $x + y\theta$ einen quadratischen Körper; nach der allgemeinsten Definition der ganzen algebraischen Zahl, welche wir in § 173 aufstellen werden, sind von diesen Zahlen $x + y\theta$ alle und nur diejenigen als ganze Zahlen anzusehen, deren Koordinaten x, y ganze rationale Zahlen sind. In jedem der acht auf diese Weise gebildeten Gebiete $[1, \theta]$ von ganzen algebraischen Zahlen gelten nun dieselben Fundamentalgesetze über die Teilbarkeit und die Zusammensetzung der Zahlen aus solchen Zahlen, welche den Namen von Primzahlen verdienen. Dies ergibt sich sofort durch die Bemerkung, daß in allen diesen Fällen der größte gemeinschaftliche Teiler von zwei solchen ganzen Zahlen sich durch den bekannten Divisionsprozeß finden läßt; man erkennt auch ebenso leicht den Zusammenhang dieser Zahlgebiete mit den quadratischen Formen teils erster, teils zweiter Art (§ 61), deren Determinanten die acht Zahlen

$$-3, \quad -7, \quad -2, \quad -11,$$
$$+5, \quad +2, \quad +3, \quad +13$$

sind. In den letzten vier Fällen gibt es zwar unendlich viele Einheiten (welche den sämtlichen Lösungen der Pellschen Gleichung entsprechen), doch wird hierdurch die Theorie dieser Gebiete nicht wesentlich erschwert. Die genannten Formen bilden jedesmal eine einzige Klasse; nur für die Determinante $+3$ gibt es zwei Klassen, welche aber durch Multiplikation mit -1 ineinander übergehen (vgl. §§ 181, 182).

Es gibt ferner Zahlengebiete, in welchen zwar der genannte Divisionsprozeß (wenigstens in seiner obigen, einfachsten Form) nicht mehr gelingt, in welchen aber dennoch dieselben Gesetze der Zusammensetzung der Zahlen aus Primzahlen gelten. Ein Beispiel hierzu

liefert das Gebiet der ganzen Zahlen von der Form $x + y\theta$, wo θ eine Wurzel der Gleichung

$$\theta^2 + \theta + 5 = 0$$

ist; die entsprechenden quadratischen Formen zweiter Art von der Determinante — 19 bilden wieder nur eine einzige Klasse.

Gänzlich anders verhält es sich aber z. B. mit dem Gebiete $[1, \theta]$ der ganzen Zahlen von der Form $x + y\theta$, wo θ eine Wurzel der Gleichung

$$\theta^2 + 5 = 0$$

bedeutet, und x, y wieder alle ganzen rationalen Zahlen durchlaufen. Hier gelingt der genannte Divisionsprozeß nicht mehr, und zugleich tritt hier zum ersten Male die eigentümliche Erscheinung auf, daß Zahlen, welche nicht weiter in Faktoren von kleinerer Norm zerlegt werden können, doch nicht den Charakter von eigentlichen Primzahlen besitzen, daß vielmehr eine und dieselbe Zahl häufig auf mehrere, wesentlich verschiedene Arten als Produkt von solchen unzerlegbaren Zahlen dargestellt werden kann; es ist z. B. die Zahl 21 gleich

$$3 \cdot 7 = (1 + 2\theta)(1 - 2\theta)$$

und jede der vier Zahlen 3, 7, $1 \pm 2\theta$ eine unzerlegbare Zahl*). Die entsprechenden quadratischen Formen von der Determinante — 5 zerfallen in zwei verschiedene Klassen, als deren Repräsentanten die Formen (1, 0, 5) und (2, 1, 3) angesehen werden können (§ 71), und hiermit hängt die eben beschriebene Erscheinung untrennbar zusammen.

Dieselbe Erscheinung tritt bei unendlich vielen anderen Gebieten von ganzen algebraischen Zahlen in Körpern zweiten oder höheren Grades auf; in allen diesen Fällen schien es ein durchaus hoffnungsloses Unternehmen, die Zusammensetzung und Teilbarkeit der Zahlen auf einfache Gesetze zurückführen zu wollen. Allein, wie es sich bei ähnlicher Lage der Dinge schon öfter in der Entwicklung der mathematischen Wissenschaften ereignet hat, so ist auch hier diese scheinbar unüberwindliche Schwierigkeit zur Quelle einer wahrhaft großen und folgenschweren Entdeckung geworden; in der Tat fand Kummer **) bei der Untersuchung derjenigen Zahlengebiete, auf welche das Problem der Kreisteilung führt, daß die alten Euklidischen

*) Vgl. §§ 16, 176.

**) Zur Theorie der komplexen Zahlen (Crelles Journal, Bd. 35).

Gesetze der Teilbarkeit auch in diesen Gebieten ihre volle Geltung wieder erlangen, sobald dieselben durch die Einführung neuer Zahlen, die er ideale Zahlen nannte, vervollständigt werden. Dasselbe Resultat für jedes, aus einer beliebigen algebraischen Gleichung entspringende Gebiet von ganzen Zahlen zu erreichen, ist nun die Aufgabe, die wir in diesem letzten Supplemente des vorliegenden Werkes behandeln und dadurch lösen wollen, daß wir die Grundlagen einer allgemeinen Zahlentheorie entwickeln, welche alle speziellen Fälle ohne Ausnahme umfaßt.

§ 160.

Um dieses Ziel zu erreichen, müssen wir uns vor allem mit den wichtigsten Grundlagen der heutigen Algebra beschäftigen, was in den nächsten Paragraphen (bis § 167) geschehen soll. Den Ausgangspunkt für unsere Darstellung dieses Gegenstandes bildet der folgende, schon oben erwähnte Begriff:

Ein System A von reellen oder komplexen Zahlen a soll ein Körper*) heißen, wenn die Summen, Differenzen, Produkte und Quotienten von je zwei dieser Zahlen a demselben System A angehören.

Dieselbe Eigenschaft sprechen wir auch so aus, daß die Zahlen eines Körpers sich durch die rationalen Operationen (Addition, Subtraktion, Multiplikation, Division) reproduzieren. Hierbei sehen wir es als selbstverständlich an, daß die Zahl Null niemals den Nenner eines Quotienten bilden kann; wir setzen deshalb auch immer voraus, daß ein Körper mindestens eine von Null verschiedene Zahl enthält, weil sonst von einem Quotienten innerhalb dieses Systems gar nicht gesprochen werden könnte.

*) Vgl. § 159 der zweiten Auflage dieses Werkes (1871). Dieser Name soll, ähnlich wie in den Naturwissenschaften, in der Geometrie und im Leben der menschlichen Gesellschaft, auch hier ein System bezeichnen, das eine gewisse Vollständigkeit, Vollkommenheit, Abgeschlossenheit besitzt, wodurch es als ein organisches Ganzes, als eine natürliche Einheit erscheint. Anfangs, in meinen Göttinger Vorlesungen (1857 bis 1858), hatte ich denselben Begriff mit dem Namen eines rationalen Gebietes belegt, der aber weniger bequem ist. Der Begriff fällt im wesentlichen zusammen mit dem, was Kronecker einen Rationalitätsbereich genannt hat (Grundzüge einer arithmetischen Theorie der algebraischen Größen. 1882). Vgl. auch die von H. Weber und mir verfaßte Theorie der algebraischen Funktionen einer Veränderlichen (Crelles Journal, Bd. 92, 1882).

Offenbar bildet das System R aller rationalen Zahlen einen Körper, und dies ist der einfachste oder, wie man auch sagen kann, der kleinste Körper, weil er in jedem anderen Körper A vollständig enthalten ist. In der Tat, wählt man aus A nach Belieben eine von Null verschiedene Zahl a aus, so ist der Quotient dieser Zahl a in sich selbst, d. h. die Zahl 1, zufolge der Definition ebenfalls in A enthalten, und da aus dieser Zahl durch wiederholte Addition und Subtraktion alle ganzen rationalen Zahlen, und hieraus durch Division alle rationalen Zahlen entstehen, so ist R gänzlich in A enthalten.

Jede bestimmte irrationale Wurzel θ einer quadratischen Gleichung mit rationalen Koeffizienten erzeugt, wie schon in § 159 bemerkt ist, einen bestimmten quadratischen Körper, den wir mit $R(\theta)$ bezeichnen werden; er besteht aus allen Zahlen von der Form $x + y\theta$, wo x und y alle rationalen Zahlen durchlaufen. Man sieht leicht ein, daß es unendlich viele verschiedene quadratische Körper $R(\theta)$ gibt, obgleich ein und derselbe Körper immer durch unendlich viele verschiedene Zahlen θ erzeugt wird.

Das System Z aller reellen und komplexen Zahlen ist ebenfalls ein Körper, und zwar der denkbar größte, weil jeder andere Körper in ihm enthalten ist. Zwischen den beiden Extremen R und Z liegt ferner der Körper, welcher aus allen reellen, sowohl rationalen als irrationalen Zahlen besteht.

Man hat, wie schon die eben erwähnten Beispiele zeigen, sehr häufig auszudrücken, daß alle Zahlen eines Körpers D auch einem Körper M angehören; in diesem Falle wollen wir der Kürze halber D einen Divisor von M, umgekehrt M ein Multiplum von D nennen. Hiernach ist jeder Körper Divisor und Multiplum von sich selbst, und wenn jeder der beiden Körper A, B Divisor des anderen ist, so sind sie identisch, was durch $A = B$ bezeichnet wird. Ist D ein Divisor von M, aber verschieden von M, so mag D ein echter Divisor von M, und M ein echtes Multiplum von D heißen. Ist A Divisor von B, und B Divisor von C, so ist A auch Divisor von C. Der Körper R ist ein gemeinschaftlicher Divisor, der Körper Z ein gemeinsames Multiplum aller Körper.

Aus gegebenen Körpern lassen sich nun nach bestimmten Regeln neue Körper bilden; wir betrachten im folgenden zwei solche Körper-

bildungen, nämlich die des größten gemeinsamen Divisors und die des kleinsten gemeinsamen Multiplums oder des Produktes.

Sind A, B zwei beliebige Körper, so ist der Inbegriff D aller derjenigen Zahlen $u, v \ldots$, welche beiden Körpern gemeinsam angehören, wieder ein Körper, weil die Summen, Differenzen, Produkte, Quotienten von u, v sowohl in A als in B, also auch in D enthalten sind. Dieser Körper D ist ein gemeinsamer Divisor von A, B, und er soll der größte gemeinsame Divisor von A, B heißen, weil jeder andere offenbar Divisor von D ist. Wenn A Divisor von B ist, so ist $D = A$, und umgekehrt.

Diese Betrachtung läßt sich unmittelbar auf ein System von mehr als zwei, ja von unendlich vielen Körpern A, $B \ldots$ übertragen; die Gesamtheit derjenigen Zahlen, welche allen diesen Körpern gemeinsam angehören, ist ein Körper und heißt ihr größter gemeinsamer Divisor.

Die zweite Art der Körperbildung beruht auf der folgenden, ebenfalls sehr einfachen Betrachtung. Ist ein bestimmtes System G von Zahlen g gegeben, deren Anzahl endlich oder unendlich sein kann, so gibt es immer solche Körper M' (z. B. den oben genannten Körper Z), in welchen alle diese Zahlen g enthalten sind; der größte gemeinsame Divisor M aller dieser Körper M' ist nach dem obigen selbst ein solcher Körper M', und zwar von allen der kleinste. Es ist wichtig, sich von diesem, durch das System G vollständig bestimmten Körper M durch eine einfache Konstruktion ein deutliches Bild zu verschaffen, wobei wir annehmen dürfen, daß G nicht aus der einzigen Zahl Null besteht. Zunächst muß M jede Zahl h enthalten, welche entweder selbst eine Zahl g oder doch ein Produkt aus mehreren*) Faktoren g ist; diese Zahlen h reproduzieren sich durch Multiplikation. Sodann muß M jede Zahl k enthalten, welche entweder selbst eine Zahl h oder doch eine Summe von mehreren Zahlen h ist; diese Zahlen k, unter denen sich auch die Zahlen g befinden, reproduzieren sich durch Addition und Multiplikation. Ferner muß M jede Differenz l von irgend zwei Zahlen k enthalten; diese Zahlen l reproduzieren sich durch Addition, Subtraktion und Multiplikation, und unter ihnen befinden sich auch alle Zahlen $k = (k + k) - k$. Endlich muß M

*) Hiermit soll, wie auch später, immer eine endliche Anzahl von Dingen bezeichnet werden.

auch jeden Quotienten m von irgend zwei Zahlen l enthalten; diese Zahlen m reproduzieren sich durch alle vier rationalen Operationen und bilden offenbar den Körper M, weil unter ihnen sich jede Zahl $l = ll:l$, folglich auch jede Zahl k, h, g befindet. Auf diese Weise hat sich ergeben, daß jede Zahl m dieses Körpers M durch eine endliche Anzahl rationaler Operationen aus den Zahlen g', g'' ... des gegebenen Systems G herstellbar ist; solche Zahlen m heißen rational darstellbar durch das System G; der Körper M ist der Inbegriff aller dieser Zahlen m und kann zweckmäßig durch $R(G)$ oder $R(g', g'' \ldots)$ bezeichnet werden. Im Anschluß an eine von Galois herrührende Ausdrucksweise wollen wir auch sagen, der Körper M entstehe aus dem Körper R der rationalen Zahlen durch Adjunktion des Systems G der Zahlen g', $g'' \ldots$; allgemeiner bezeichnen wir, wenn A irgendein Körper ist, mit $A(g', g'' \ldots)$ den durch Adjunktion der Zahlen g', $g'' \ldots$ aus A erzeugten Körper, d. h. den kleinsten Körper, welcher außer den Zahlen des Körpers A auch die Zahlen g', $g'' \ldots$ enthält.

Liegt nun irgendein System von Körpern A, $B \ldots$ vor, und nimmt man in das System G jede und nur jede solche Zahl g auf, welche in mindestens einem dieser Körper enthalten ist, so wird der entsprechende Körper M, welcher aus allen durch diese Zahlen g rational darstellbaren Zahlen m besteht, ein gemeinsames Multiplum von A, $B \ldots$, und zwar das kleinste, weil nach dem obigen jedes andere M' ein Multiplum von M ist. Der Kürze halber werden wir aber den Körper M auch das Produkt der Faktoren A, $B \ldots$ nennen und mit $AB \ldots$ bezeichnen, wobei die Anordnung der Faktoren gleichgültig ist; denn offenbar ist $AB = BA$, $(AB)C = A(BC)$ usw. Wendet man die oben beschriebene Konstruktion des Körpers M auf den Fall von zwei Körpern A, B an, so besteht das System G aus allen Zahlen a des Körpers A und allen Zahlen b des Körpers B, die Zahlen h sind die Produkte ab, die Zahlen k und l sind Summen von solchen Produkten, und folglich besteht das Produkt AB aus allen Quotienten von der Form

$$m = \frac{a'_1 b'_1 + a'_2 b'_2 + \cdots + a'_r b'_r}{a_1 b_1 + a_2 b_2 + \cdots + a_s b_s}.$$

Daß A ein Divisor von B ist, kann bequem durch $AB = B$ ausgedrückt werden, und immer ist $AA = A$.

§ 161.

Es geschieht in der Mathematik und in anderen Wissenschaften sehr häufig, daß, wenn ein System A von Dingen oder Elementen a vorliegt, jedes bestimmte Element a nach einem gewissen Gesetze durch ein bestimmtes, ihm entsprechendes Element a' ersetzt wird (welches in A enthalten sein kann oder auch nicht); ein solches Gesetz pflegt man eine Substitution zu nennen, und man sagt, daß durch diese Substitution das Element a in das Element a', und ebenso das System A in das System A' der Elemente a' übergeht*). Die Ausdrucksweise gestaltet sich noch etwas bequemer und anschaulicher, wenn man, was wir tun wollen, diese Substitution wie eine Abbildung des Systems A auffaßt und demgemäß a' das Bild von a, ebenso A' das Bild von A nennt. Der Deutlichkeit halber ist es oft notwendig, ein solches Abbildungsgesetz, um es von anderen zu unterscheiden, mit einem besonderen Zeichen, z. B. φ, zu belegen; geschieht dies, so wollen wir das Bild a', in welches a durch φ übergeht, auch durch $a\varphi$ bezeichnen; ist ferner T ein Teil von A, d. h. ein System von Elementen t, welche alle in A enthalten sind, so soll $T\varphi$ das System bedeuten, welches aus den Bildern $t\varphi$ aller dieser Elemente t besteht; demnach ist $A\varphi$ identisch mit dem obigen A'.

Wir wenden nun diesen Begriff auf einen beliebigen Zahlenkörper A an, betrachten aber nur solche Substitutionen φ, durch welche jede in A enthaltene Zahl a wieder in eine Zahl $a' = a\varphi$ übergeht. In dieser Allgemeinheit aufgefaßt, würden solche Substitutionen indessen noch gar kein Interesse darbieten; wir fragen vielmehr, ob es möglich ist, die Zahlen a des Körpers A in der Weise durch Zahlen a' abzubilden, daß alle zwischen den Zahlen a bestehenden rationalen Beziehungen sich vollständig auf die Bilder a' übertragen; oder mit anderen Worten, wir verlangen, daß, wenn aus beliebigen Zahlen $u, v, w \ldots$ des Körpers A

*) Schon in der dritten Auflage dieses Werkes (1879, Anmerkung auf S. 470) ist ausgesprochen, daß auf dieser Fähigkeit des Geistes, ein Ding a mit einem Ding a' zu vergleichen, oder a auf a' zu beziehen, oder dem a ein a' entsprechen zu lassen, ohne welche überhaupt kein Denken möglich ist, auch die gesamte Wissenschaft der Zahlen beruht. Die Durchführung dieses Gedankens ist seitdem veröffentlicht in meiner Schrift „Was sind und was sollen die Zahlen?“ (Braunschweig 1888); die daselbst angewandte Bezeichnungsweise für Abbildungen und deren Zusammensetzung weicht äußerlich von der hier gebrauchten ein wenig ab.

durch rationale Operationen eine Zahl t abgeleitet ist, welche folglich ebenfalls dem Körper A angehört, durch dieselben rationalen Operationen aus den Bildern u', v', w' ... immer das Bild t' der Zahl t entstehen soll. Eine Substitution oder Abbildung φ, welche sich durch diese Eigenschaft vor anderen auszeichnet, wollen wir eine Permutation des Körpers A nennen. Da jede rationale Operation aus einer endlichen Anzahl von einfachen Additionen, Subtraktionen, Multiplikationen und Divisionen zusammengesetzt ist, so leuchtet ein, daß die Abbildung φ stets und nur dann eine solche Permutation ist, wenn für je zwei in A enthaltene Zahlen u, v die folgenden vier Grundgesetze gelten:

$$(1) \qquad (u+v)' = u' + v'$$

$$(2) \qquad (u-v)' = u' - v'$$

$$(3) \qquad (uv)' = u'v'$$

$$(4) \qquad \left(\frac{u}{v}\right)' = \frac{u'}{v'}.$$

Von diesen für eine Permutation charakteristischen, d. h. erforderlichen und hinreichenden Bedingungen verlangt die letzte offenbar, daß die Bilder a' nicht alle verschwinden; umgekehrt, wenn eine Abbildung φ, durch welche jede Zahl a des Körpers A in eine Zahl a' übergeht, diese Eigenschaft besitzt und außerdem den Gesetzen (1) und (3) gehorcht, so ergeben sich hieraus, wie wir jetzt beweisen wollen, die Gesetze (2) und (4), und folglich ist φ eine Permutation des Körpers A. In der Tat, aus der Gleichung (1) folgt unmittelbar die Gleichung (2), wenn man, was offenbar erlaubt ist, die willkürliche Zahl u des Körpers A durch die ebenfalls in A enthaltene Zahl $(u - v)$ ersetzt; ebenso darf man in (3), wenn v von Null verschieden ist, u durch den Quotienten $u : v$ ersetzen, wodurch man zunächst

$$u' = \left(\frac{u}{v}\right)' v'$$

erhält; wäre nun $v' = 0$, so würden die Bilder u' von allen in A enthaltenen Zahlen u verschwinden, was aber im Widerspruch mit unserer ausdrücklichen Voraussetzung steht; mithin ist das Bild v' jeder von Null verschiedenen Zahl v ebenfalls von Null verschieden, und es gilt folglich das Gesetz (4), was zu beweisen war.

Es ergibt sich ferner, daß das System A', in welches der Körper A durch eine Permutation φ übergeht, wieder ein Körper

ist. Berücksichtigt man nämlich, daß A' aus allen und nur solchen Zahlen u', v' ... besteht, welche Bilder von Zahlen u, v ... des Körpers A sind, und daß jede von Null verschiedene Zahl v' des Systems A' zufolge (1) gewiß das Bild einer von Null verschiedenen Zahl v des Körpers A ist, so ergibt sich, daß die Summen, Differenzen, Produkte, Quotienten von je zwei in A' enthaltenen Zahlen u', v' ebenfalls dem System A' angehören, weil sie zufolge der Gesetze (1), (2), (3), (4) ebenfalls Bilder von Zahlen des Körpers A sind; mithin ist A' ein Körper, was zu beweisen war.

Wir bemerken sodann, daß je zwei voneinander verschiedene Zahlen u, v des Körpers A auch voneinander verschiedene Bilder u', v' besitzen*), weil sonst zufolge (2) das Bild der von Null verschiedenen Zahl $(u - v)$ verschwinden würde, was, wie wir oben schon bewiesen haben, nicht möglich ist. Mithin ist jede bestimmte im Körper A' enthaltene Zahl a' das Bild von einer einzigen, völlig bestimmten Zahl a des Körpers A, und folglich kann man der Permutation φ, durch welche A in A' übergeht, eine mit φ^{-1} zu bezeichnende Abbildung des Körpers A' gegenüberstellen, durch welche jede bestimmte, in A' enthaltene Zahl a' in diese bestimmte Zahl a des Körpers A übergeht; diese Abbildung φ^{-1} ist aber gewiß eine Permutation des Körpers A'; denn wenn u', v' zwei beliebige Zahlen des Körpers A', und u, v die ihnen entsprechenden Zahlen des Körpers A bedeuten, so gehen zufolge (1) und (3) die Zahlen $u' + v'$ und $u'v'$ des Körpers A' durch φ^{-1} in die Zahlen $u + v$ und uv über, was zu zeigen war. Außerdem leuchtet ein, daß der Körper A' durch φ^{-1} in den vollen Körper A, nicht etwa in einen echten Divisor von A übergeht; denn jede in A enthaltene Zahl a ist wirklich das durch die Permutation φ^{-1} erzeugte Bild einer in A' enthaltenen Zahl a'. Wir wollen jede dieser beiden Permutationen φ und φ^{-1} die umgekehrte oder inverse der anderen nennen, die beiden Körper A und A' sollen konjugierte Körper, und je zwei einander entsprechende Zahlen a und a' sollen konjugierte Zahlen heißen.

Diejenige Abbildung eines Körpers A, durch welche jede seiner Zahlen in sich selbst übergeht, genügt offenbar den Bedingungen

*) Nach der in der oben zitierten Schrift (§ 3) gewählten Ausdrucksweise ist daher jede Permutation eines Körpers eine ähnliche oder deutliche Abbildung desselben; A und A' sind ähnliche Systeme.

(1), (2), (3), (4) und ist folglich eine Permutation; wir wollen sie die identische Permutation von A nennen. Hieraus geht hervor, daß jeder Körper mit sich selbst konjugiert ist.

Der in § 159 betrachtete Körper J oder $R(i)$ besitzt außer der identischen noch eine zweite Permutation, durch welche jede in ihm enthaltene Zahl $x + yi$ in die konjugierte Zahl $x - yi$ übergeht. Dieselbe Permutation gilt, wenn x, y nicht auf rationale Zahlen beschränkt werden, sondern beliebige reelle Zahlen bedeuten, auch für den aus allen Zahlen bestehenden Körper Z.

Wir haben im vorigen Paragraphen gesehen, daß jeder Körper A auch alle rationalen Zahlen enthält; ist nun φ wieder eine beliebige Permutation von A, und wendet man das Gesetz (4) auf den Fall $u = v$ an, so ergibt sich, daß $1' = 1$ ist, und hieraus folgt mit Rücksicht auf die Gesetze (1), (2), (3), (4), daß jede rationale Zahl des Körpers A, weil sie durch eine endliche Anzahl von einfachen rationalen Operationen aus der Zahl 1 entsteht, durch die Permutation φ in sich selbst übergeht. Der Körper R der rationalen Zahlen besitzt daher keine andere, als die identische Permutation.

Ist φ eine Permutation des Körpers A, so wollen wir umgekehrt sagen, A gehöre zu φ oder sei der zu φ gehörige Körper, oder wir wollen der Kürze halber A auch geradezu den Körper der Permutation φ nennen, während $A\varphi$ der durch φ erzeugte Körper heißt.

Daß φ und ψ nur verschiedene Zeichen für eine und dieselbe Körper-Permutation sind, werden wir durch $\varphi = \psi$ andeuten; hierin liegt also, daß φ und ψ Permutationen desselben Körpers A sind, und daß für jede in A enthaltene Zahl a stets $a\varphi = a\psi$ ist. Falls eine dieser beiden Bedingungen nicht erfüllt ist, nennen wir φ und ψ verschieden.

Bedeutet nun Φ ein System von Permutationen irgendwelcher Körper, so wollen wir eine in allen diesen Körpern (also auch in ihrem größten gemeinsamen Divisor) enthaltene Zahl einwertig, zweiwertig usw. in bezug auf Φ oder zu Φ nennen, je nachdem die Anzahl der verschiedenen Werte, in welche sie durch alle diese Permutationen übergeht, = 1, 2 usw. ist. Nach dem obigen ist daher jede rationale Zahl einwertig in bezug auf jedes System Φ; ebenso wichtig ist der folgende Satz:

Ist Φ ein System von n verschiedenen Permutationen $\varphi_1, \varphi_2 \ldots \varphi_n$ desselben Körpers A, so gibt es in letzterem unendlich viele Zahlen, welche n-wertig zu Φ sind.

Um dies zu beweisen, wollen wir, wenn t irgendeine Zahl in A bedeutet, der Kürze halber $t\varphi_r = t_r$ setzen. Ist $n = 2$, so versteht sich der Satz nach dem obigen von selbst. Ist $n > 2$, so dürfen wir annehmen, es sei schon eine Zahl a in A gefunden, welche durch die $n-1$ Permutationen $\varphi_2, \varphi_3 \dots \varphi_n$ in ebenso viele verschiedene Zahlen $a_2, a_3 \dots a_n$ übergeht. Wenn nun a_1 ebenfalls von allen diesen Zahlen verschieden ist, so besitzt die Zahl a die im Satze ausgesprochene Eigenschaft. Im entgegengesetzten Falle, wenn z. B. $a_1 = a_2$ ist, wähle man aus A eine andere Zahl b aus, welche durch φ_1, φ_2 in zwei verschiedene Zahlen b_1, b_2 übergeht, und betrachte alle Zahlen von der Form $y = ax + b$, welche durch beliebige rationale Zahlen x erzeugt werden und folglich demselben Körper A angehören; da x nach dem obigen durch jede Permutation in sich selbst übergeht, so ist nach den Gesetzen (1) und (3) allgemein $y_r = a_r x + b_r$, also auch

$$y_r - y_s = (a_r - a_s)\, x + (b_r - b_s),$$

wo r, s irgendeine Kombination von zwei verschiedenen Zahlen aus der Reihe $1, 2 \dots n$ bedeutet. Für die Kombination $r = 1$, $s = 2$ ergibt sich, daß die Zahlen y_1, y_2 stets voneinander verschieden ausfallen, wie auch die rationale Zahl x gewählt sein mag, weil $a_1 = a_2$, aber b_1 von b_2 verschieden ist. Für jede der übrigen Kombinationen r, s ist a_r verschieden von a_s, und folglich gibt es entweder gar keine oder nur eine rationale Zahl x, für die $y_r = y_s$ wird; schließt man, indem man alle Kombinationen durchgeht, diese etwa vorhandenen Zahlen x aus, deren Anzahl gewiß $< \frac{1}{2}n(n-1)$ ist, so erzeugt jede andere rationale Zahl x gewiß eine Zahl y, welche durch die n Permutationen in n verschiedene Zahlen $y_1, y_2 \dots y_n$ übergeht, was zu beweisen war.

Hieraus ziehen wir noch eine wichtige Folgerung. Nach einem sehr bekannten Satze der Determinanten-Theorie, auf den wir später (in § 167) noch einmal zurückkommen werden, ist das Produkt aller derjenigen Differenzen $y_r - y_s$, in denen $r < s$, gleich der Determinante

$$\begin{vmatrix} y_1^{n-1} & y_1^{n-2} & \dots & y_1 & 1 \\ y_2^{n-1} & y_2^{n-2} & \dots & y_2 & 1 \\ \dots & \dots & \dots & \dots & \dots \\ y_n^{n-1} & y_n^{n-2} & \dots & y_n & 1 \end{vmatrix},$$

deren Elemente die Potenzen $(y_r)^{n-s}$ sind, wo jetzt r, s unabhängig voneinander alle Werte $1, 2 \ldots n$ durchlaufen. Diese Determinante ist daher in unserem Falle von Null verschieden. Da nun $y_r = y\varphi_r$ und folglich nach dem Gesetze (3) die Potenz $(y_r)^{n-s} = (y^{n-s})\varphi_r$ ist, so erhält man, wenn man $y^{n-s} = a^{(s)}$ setzt, den Satz:

Sind die n Permutationen $\varphi_1, \varphi_2 \ldots \varphi_n$ desselben Körpers A voneinander verschieden, so gibt es in A ein System von n Zahlen $a', a'' \ldots a^{(n)}$ der Art, daß die aus den Elementen $a^{(s)}\varphi_r$ gebildete Determinante nicht verschwindet.

§ 162.

Nach diesen Betrachtungen, welche sich auf Permutationen eines und desselben Körpers beziehen, gehen wir zu der Zusammensetzung*) von zwei Permutationen φ, ψ über, die aber nur dann möglich ist, wenn ψ eine Permutation des durch φ erzeugten Körpers $A\varphi$ ist; im Anschluß an die einzuführende Zeichensprache kann man zweckmäßig ψ einen rechten Nachbar von φ, und φ einen linken Nachbar von ψ nennen. Jede bestimmte Zahl a des Körpers A geht durch die Permutation φ in eine bestimmte Zahl $a\varphi$ des Körpers $A\varphi$, und diese geht durch ψ in eine bestimmte Zahl $(a\varphi)\psi$ über; man kann daher eine Abbildung π des Körpers A dadurch definieren, daß man allgemein $a\pi = (a\varphi)\psi$ setzt. Wendet man nun die Gesetze (1) und (3) des vorigen Paragraphen erst auf φ, dann auf ψ an, so ergibt sich, wie der Leser leicht finden wird, daß dieselben Gesetze auch für diese Abbildung π gelten, und da die Bilder $a\pi$ offenbar nicht alle verschwinden (weil z. B. $1\pi = 1$ ist), so ist π eine Permutation des Körpers A. Wir nennen sie die Resultante der Komponenten φ, ψ und bezeichnen sie durch das Symbol $\varphi\psi$, wobei der Einfluß der linken oder ersten Komponente φ von dem der rechten oder zweiten Komponente ψ durch die Stellung wohl zu unterscheiden ist. Die Definition dieser Resultante $\varphi\psi$ besteht nach dem obigen darin, daß das aus jeder in A enthaltenen Zahl a erzeugte Bild

$$a(\varphi\psi) = (a\varphi)\psi$$

*) Dieselbe bildet nur einen speziellen Fall der Zusammensetzung von Abbildungen beliebiger Systeme; vgl. den Schluß in § 2 meiner oben zitierten Schrift, wo aber die Bezeichnungsweise eine andere ist.

ist; man kann daher unbedenklich die Klammern weglassen und dieses Bild kurz durch $a\,\varphi\,\psi$ bezeichnen. Ebenso leicht erkennt man, daß, wenn T irgendein Teil von A ist, die beiden Systeme $T(\varphi\,\psi)$ und $(T\,\varphi)\,\psi$ vollständig identisch sind und daher kurz durch $T\,\varphi\,\psi$ bezeichnet werden können. Hieraus ergibt sich unmittelbar der Satz:

Wenn zwei Körper A, A'' mit einem dritten A' konjugiert sind, so sind sie auch miteinander konjugiert.

Denn zufolge der Annahme gibt es eine Permutation φ von A, und eine Permutation ψ von A', für welche $A\,\varphi = A'$, und $A'\,\psi = A''$ wird; mithin ist $A(\varphi\,\psi) = (A\,\varphi)\,\psi = A'\,\psi = A''$, was zu beweisen war.

Nachdem die Zusammensetzung benachbarter Permutationen ausführlich beschrieben ist, heben wir noch die folgenden, darauf bezüglichen wichtigen Sätze hervor, deren Beweise der Leser leicht finden wird.

Ist φ eine Permutation des Körpers A, so ist $\varphi\,\varphi^{-1}$ die identische Permutation von A. Ist ψ ein rechter Nachbar von φ, so ist ψ^{-1} ein linker Nachbar von φ^{-1}, und $(\varphi\,\psi)^{-1} = \psi^{-1}\,\varphi^{-1}$. Ist ferner ψ_1 ebenfalls ein rechter Nachbar von φ, und φ_1 ein linker Nachbar von ψ, so folgt aus $\varphi\,\psi = \varphi\,\psi_1$, daß $\psi = \psi_1$, und aus $\varphi\,\psi = \varphi_1\,\psi$, daß $\varphi = \varphi_1$ ist. Wenn außerdem die Permutation χ ein rechter Nachbar von ψ ist, so ist $(\varphi\,\psi)\chi = \varphi(\psi\,\chi)$, und man kann daher diese Resultante kurz durch $\varphi\,\psi\,\chi$ bezeichnen; hieraus ergibt sich, wenn man dieselbe Schlußweise wie in § 2 anwendet, die vollständig bestimmte Bedeutung der Resultante $\varphi_1\,\varphi_2 \cdots \varphi_{n-1}\,\varphi_n$ von n Komponenten φ_1, $\varphi_2 \cdots \varphi_{n-1}$, φ_n, deren jede ein rechter Nachbar der vorhergehenden ist; da die Komponenten nicht miteinander vertauscht werden dürfen, und jede immer nur mit der nächstfolgenden zu einer Resultante verbunden werden kann, so ist die Anzahl der verschiedenen Herstellungsarten dieser Resultante $= (n-1)(n-2) \ldots 2.1$.

§ 163.

Außer der eben beschriebenen Zusammensetzung benachbarter Permutationen haben wir nun noch die ebenso wichtigen Beziehungen zu betrachten, welche zwischen den Permutationen eines Körpers und denen seiner Divisoren stattfinden. Ist der Körper A ein Divisor des

Körpers M, und π eine Permutation des letzteren, so ist in ihr immer eine vollständig bestimmte Abbildung φ von A enthalten, welche darin besteht, daß für jede in A, also auch in M enthaltene Zahl a das Bild $a\varphi = a\pi$ ist, und es leuchtet aus den Grundgesetzen in § 161 unmittelbar ein, daß diese Abbildung φ eine Permutation von A ist; wir wollen sie den auf A bezüglichen Divisor von π, und umgekehrt π ein Multiplum von φ nennen. Offenbar ist φ^{-1} zugleich ein Divisor von π^{-1}. Wenn $A = M$ ist, so ist natürlich auch $\varphi = \pi$; in jedem anderen Falle, d. h. wenn A ein echter Divisor von M ist, wird man aber φ von π streng unterscheiden müssen*). Ist π wieder ein Divisor einer Permutation ϱ, so leuchtet ein, daß φ auch ein Divisor von ϱ ist. Ist π die identische Permutation von M, so ist φ die identische Permutation von A. Die einzige — nämlich die identische — Permutation des Körpers R der rationalen Zahlen ist (nach § 161) gemeinsamer Divisor aller Körper-Permutationen. Allgemein gilt der folgende Fundamentalsatz:

Bedeutet Π irgendein System von Permutationen π beliebiger Körper M, so bildet die Gesamtheit A aller zu Π einwertigen Zahlen a einen Körper, der ein gemeinsamer Divisor der Körper M ist; die Permutationen π haben alle einen und denselben auf A bezüglichen Divisor φ, und jeder gemeinsame Divisor ψ der Permutationen π ist Divisor dieser Permutation φ.

Denn das Wesen einer zu Π einwertigen Zahl a besteht (nach § 161) darin, daß die den sämtlichen Permutationen π entsprechenden Bilder $a\pi$ einen und denselben Wert besitzen, mithin folgt aus den Grundgesetzen (in § 161), daß die Summen, Differenzen, Produkte und Quotienten von je zwei solchen einwertigen Zahlen u, v ebenfalls einwertig zu Π sind; also ist A ein Körper. Definiert man ferner die Abbildung φ von A, indem man $a\varphi = a\pi$ setzt, so ist φ offenbar der auf A bezügliche Divisor von jeder einzelnen Permutation π. Wenn endlich eine Permutation ψ eines Körpers B gemeinsamer Divisor der Permutationen π, und b irgendeine Zahl in B ist, so muß $b\psi$ mit jedem der Bilder $b\pi$ übereinstimmen, d. h. b ist eine zu Π einwertige Zahl; folglich ist B Divisor von A, und zugleich ψ Divisor von φ, was zu beweisen war.

*) Auf diese Unterscheidung brauchte in der oben zitierten Schrift (§ 2) kein Gewicht gelegt zu werden.

Da dieser Körper A, welcher ein gemeinsamer, aber keineswegs immer der größte gemeinsame Divisor der Körper M ist, durch das System Π vollständig bestimmt ist, so wollen wir sagen, A gehöre zu Π oder sei der zu Π gehörige Körper, oder wir wollen kurz A den Körper des Systems Π nennen, und man sieht sofort, daß diese Ausdrucksweise, falls Π nur aus einer einzigen Permutation besteht, vollständig mit der in § 161 eingeführten übereinstimmt. Die Permutation φ kann unbedenklich der größte gemeinsame Divisor der Permutationen π genannt werden; der Kürze halber wollen wir aber φ auch den Rest des Systems Π oder der Permutationen π nennen. —

Ganz anders verhält es sich dagegen mit der Existenz eines gemeinsamen Multiplum von gegebenen Permutationen; denn es leuchtet z. B. ein, daß zwei verschiedene Permutationen eines und desselben Körpers gewiß kein gemeinsames Multiplum haben. Hierauf gründet sich eine sehr wichtige Unterscheidung: die Permutationen φ, ψ ... sollen einig (harmonisch) oder uneinig heißen, je nachdem sie ein gemeinsames Multiplum besitzen oder nicht. Beschränken wir uns auf die Betrachtung von zwei einigen Permutationen φ, ψ der Körper A, B, und bezeichnen mit ϱ ein gemeinsames Multiplum von φ, ψ, so ist der zu ϱ gehörige Körper ein gemeinsames Multiplum von A, B und folglich auch von AB; bedeutet ferner a jede in A, b jede in B enthaltene Zahl, und π den auf AB bezüglichen Divisor von ϱ, so ist $a\varphi = a\varrho = a\pi$, $b\psi = b\varrho = b\pi$, und folglich ist π ebenfalls ein gemeinsames Multiplum von φ, ψ. Da nun jede bestimmte Zahl m des Körpers AB (nach § 160) durch eine endliche Menge von Zahlen a, b rational darstellbar ist, und das Bild $m\pi$ (nach den Grundgesetzen jeder Permutation) auf dieselbe Weise aus den Bildern $a\pi$, $b\pi$, also aus den Zahlen $a\varphi$, $b\psi$ abgeleitet wird, so ergibt sich, daß die Permutation π des Produktes AB durch die Permutationen φ, ψ der Faktoren A, B vollständig bestimmt, also gänzlich unabhängig von der Auswahl der obigen Permutation ϱ ist. Diese Permutation π, welche folglich Divisor von jedem gemeinsamen Multiplum ϱ der Permutationen φ, ψ ist, kann daher ihr kleinstes gemeinsames Multiplum oder kürzer ihre Union*) genannt werden.

*) Ich würde das Wort Produkt vorziehen, wenn dasselbe nicht von manchen Schriftstellern schon bei der Zusammensetzung von Substitutionen in dem Sinne benutzt wäre, wofür ich oben (§ 162) den ebenfalls gebräuchlichen Namen Resultante gewählt habe.

Umgekehrt, wenn π eine Permutation eines Produktes AB, und φ, ψ die auf A, B bezüglichen Divisoren von π bedeuten, so sind diese Permutationen φ, ψ offenbar einig, und π ist ihre Union. Zugleich leuchtet ein, daß $(AB)\pi = (A\pi)(B\pi) = (A\varphi)(B\psi)$, und daß π^{-1} die Union von φ^{-1}, ψ^{-1} ist. Sind außerdem φ_1, ψ_1 zwei einige Permutationen der Körper $A\varphi$, $B\psi$, und π_1 ihre Union, so erkennt man leicht, daß die Resultanten $\varphi\varphi_1$, $\psi\psi_1$ ebenfalls einig sind, und daß die Resultante $\pi\pi_1$ ihre Union ist.

Auf diesen Betrachtungen, die genau ebenso für Systeme von mehr als zwei, ja von unendlich vielen einigen Permutationen gelten, beruht endlich noch der folgende Begriff. Ein System von beliebigen (einigen oder uneinigen) Permutationen

$$\varphi_1, \varphi_2, \varphi_3 \cdots$$

und ein System von korrespondierenden Permutationen

$$\varphi_1', \varphi_2', \varphi_3' \cdots$$

sollen konjugierte Systeme heißen, wenn je zwei korrespondierende Glieder φ_r, φ_r' Permutationen eines und desselben Körpers A_r sind, und wenn zugleich die resultierenden Permutationen

$$\varphi_1^{-1}\varphi_1', \varphi_2^{-1}\varphi_2', \varphi_3^{-1}\varphi_3' \cdots$$

einig sind. Aus dem Vorhergehenden ergibt sich dann sofort der Satz, daß zwei mit einem dritten konjugierte Systeme von Permutationen auch miteinander konjugiert sind. Der Nutzen, welchen diese und die früher entwickelten Begriffe gewähren, würde freilich erst bei einer ausführlicheren, ins einzelne gehenden Darstellung der Algebra deutlich erkennbar werden.

§ 164.

Für die genaue Untersuchung der Verwandtschaft zwischen den verschiedenen Körpern — und hierin besteht der eigentliche Gegenstand der heutigen Algebra — bildet der folgende Begriff*) die allgemeinste und zugleich einfachste Grundlage:

*) Vgl. Dirichlet: Verallgemeinerung eines Satzes aus der Lehre von den Kettenbrüchen nebst einigen Anwendungen auf die Theorie der Zahlen. (Berliner Monatsberichte, April 1842, oder Dirichlets Werke, Bd. 1, S. 633.)

Ein System T von m Zahlen $\omega_1, \omega_2, \ldots, \omega_m$ heißt reduzibel in bezug auf einen Körper A, wenn es m Zahlen $a_1, a_2, \ldots, a_m$ in A gibt, die der Bedingung

$$a_1\omega_1 + a_2\omega_2 + \cdots + a_m\omega_m = 0$$

genügen und nicht alle verschwinden; im entgegengesetzten Falle heißt das System T irreduzibel nach A. Je nachdem der erstere oder letztere Fall stattfindet, werden wir auch sagen, die m Zahlen $\omega_1, \omega_2, \ldots, \omega_m$ seien voneinander abhängig oder unabhängig (in bezug auf A).

Ist A ein Divisor des Körpers B, so leuchtet ein, daß jedes in bezug auf A reduzible System auch reduzibel nach B, und jedes nach B irreduzible System auch irreduzibel in bezug auf A ist. Bei den zunächst folgenden Bemerkungen werden aber alle Systeme T immer auf einen und denselben Körper A bezogen, und es wird deshalb erlaubt sein, diese Beziehung unerwähnt zu lassen.

Jedes irreduzible System besteht aus lauter voneinander und von Null verschiedenen Zahlen, und ein aus einer einzigen Zahl bestehendes System ist dann und nur dann irreduzibel, wenn diese Zahl von Null verschieden ist.

Ein reduzibles oder irreduzibles System behält diesen Charakter, wenn die Zahlen desselben mit einem beliebigen gemeinsamen, von Null verschiedenen Faktor multipliziert werden.

Fügt man zu einem reduziblen Systeme noch eine oder mehrere Zahlen hinzu, so bleibt das System reduzibel; jeder Teil eines irreduziblen Systems ist irreduzibel.

Von besonderem Interesse ist die folgende Anwendung des obigen Begriffes. Wir sagen, eine Zahl θ sei algebraisch in bezug auf den Körper A, wenn sie die Wurzel einer endlichen algebraischen Gleichung von der Form

$$\theta^n + a_1\theta^{n-1} + \cdots + a_{n-1}\theta + a_n = 0$$

ist, deren Koeffizienten a_r dem Körper A angehören. Dieselbe Eigenschaft können wir jetzt so aussprechen, daß die $n+1$ Potenzen $\theta^n, \theta^{n-1}, \ldots, \theta, 1$ ein nach A reduzibles System bilden. Unter allen positiven Exponenten n, für welche diese Reduzibilität besteht, muß es nun einen kleinsten n geben, in der Weise, daß das System der n Potenzen $\theta^{n-1}, \ldots, \theta, 1$ irreduzibel ist, aber durch Hinzufügung von θ^n reduzibel wird; diese natürliche Zahl n wollen wir den Grad

der Zahl θ in bezug auf A nennen, und wir sagen kurz, θ sei eine (algebraische) Zahl $n$ten Grades in bezug auf A. Ist $n = 1$, so ist θ offenbar in A enthalten, und umgekehrt ist jede Zahl des Körpers A algebraisch vom ersten Grade in bezug auf A.

Kehren wir jetzt zu dem allgemeinen Falle zurück und nehmen wir an, das obige System der m Zahlen $\omega_1, \omega_2, \ldots, \omega_m$ (die nicht alle verschwinden) sei reduzibel, so wird offenbar ein Teil dieses Systems, der etwa aus den n Zahlen $\omega_1, \omega_2, \ldots, \omega_n$ bestehen mag, irreduzibel sein, während jede der übrigen $m - n$ Zahlen ω_{n+1}, $\omega_{n+2}, \ldots, \omega_m$ mit jenen ein reduzibles System bildet. Wir wollen nun allgemein mit ω jede Zahl bezeichnen, welche von den Zahlen $\omega_1, \omega_2, \ldots, \omega_n$ abhängig ist, d. h. welche mit diesen Zahlen ein reduzibles System bildet; es leuchtet ein, daß jede solche Zahl ω stets und nur auf eine einzige Art in der Form

$$\omega = h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n \tag{1}$$

darstellbar ist, wo die Koeffizienten $h_1, h_2, \ldots, h_n$ Zahlen des Körpers A bedeuten, und daß umgekehrt jede in dieser Form darstellbare Zahl abhängig ist von den n Zahlen $\omega_1, \omega_2, \ldots, \omega_n$. Die Gesamtheit Ω aller dieser Zahlen ω nennen wir eine Schar (in bezug auf A); das System der n bestimmten Zahlen $\omega_1, \omega_2, \ldots, \omega_n$ heißt eine (irreduzible) Basis der Schar Ω, und diese n Zahlen ω_r selbst heißen die Glieder oder Elemente dieser Basis. Zu jeder in Ω enthaltenen Zahl ω gehören dann n völlig bestimmte Zahlen $h_1, h_2, \ldots, h_n$ des Körpers A, die in der Darstellung (1) von ω auftreten und die Koordinaten von ω in bezug auf diese Basis heißen sollen. Die charakteristischen Eigenschaften einer solchen Schar Ω sind die folgenden:

I. Die Zahlen in Ω reproduzieren sich durch Addition und Subtraktion, d. h. die Summen und Differenzen von je zwei solchen Zahlen sind ebenfalls Zahlen in Ω.

II. Jedes Produkt aus einer Zahl in Ω und einer Zahl in A ist eine Zahl in Ω.

III. Es gibt n voneinander unabhängige Zahlen in Ω, aber je $n + 1$ solche Zahlen sind voneinander abhängig.

Nur der zweite Teil dieser letzten Eigenschaft bedarf noch einer Begründung, und wir dürfen dabei annehmen, daß sie für jede ähnliche Schar, deren Basis aus weniger als n Gliedern besteht, schon be-

wiesen sei. Nimmt man nun $n+1$ beliebige Zahlen $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_n$ aus $\mathfrak{Q}$, so sind sie, falls eine von ihnen, z. B. $\alpha = 0$ ist, gewiß voneinander abhängig; im entgegengesetzten Falle dürfen wir voraussetzen, daß z. B. die erste Koordinate der Zahl α nicht verschwindet; dann kann man offenbar n Zahlen $c_1, c_2, \ldots, c_n$ in A so bestimmen, daß die erste Koordinate von jeder der n Zahlen

$$\alpha_1 + c_1\alpha,\ \alpha_2 + c_2\alpha,\ \ldots,\ \alpha_n + c_n\alpha$$

verschwindet*); diese n Zahlen gehören dann einer Schar an, deren Basis aus nur $n-1$ Zahlen $\omega_2, \omega_3, \ldots, \omega_n$ besteht, und sind folglich voneinander abhängig; es gibt daher n Zahlen $a_1, a_2, \ldots, a_n$ in A, die nicht alle verschwinden, und welche der Bedingung

$$a_1(\alpha_1 + c_1\alpha) + a_2(\alpha_2 + c_2\alpha) + \cdots + a_n(\alpha_n + c_n\alpha) = 0$$

genügen, und da auch die Summe $a = a_1c_1 + a_2c_2 + \cdots + a_nc_n$ in A enthalten ist, so folgt hieraus, daß die $n+1$ Zahlen $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_n$ wirklich voneinander abhängig sind, was zu beweisen war.

Umgekehrt, wenn ein Zahlensystem $\mathfrak{Q}$ die obigen drei Eigenschaften I, II, III besitzt, so folgt aus der letzteren, daß, nachdem man n voneinander unabhängige Zahlen $\omega_1, \omega_2, \ldots, \omega_n$ aus $\mathfrak{Q}$ gewählt hat, jede in $\mathfrak{Q}$ enthaltene Zahl ω gewiß von der Form (1) ist; sodann folgt aus II und I, daß auch jede in der Form (1) enthaltene Zahl ω dem System $\mathfrak{Q}$ angehört. Also sind wirklich diese drei Eigenschaften charakteristisch für die aus allen Zahlen ω von der Form (1) bestehende Schar $\mathfrak{Q}$.

Zugleich leuchtet hieraus ein, daß jedes aus n solchen Zahlen ω bestehende irreduzible System ebenfalls als eine Basis von $\mathfrak{Q}$ angesehen und benutzt werden kann; mit jedem Übergange von einer Basis zu einer anderen ist offenbar eine Transformation der Koordinaten aller Zahlen ω verbunden, ähnlich wie in der analytischen Geometrie. Auf die Auswahl einer solchen neuen Basis bezieht sich der folgende wichtige Satz, von dem wir, wenn auch erst später, oft Gebrauch zu machen haben werden.

IV. Ein beliebiges System von n Zahlen der Schar $\mathfrak{Q}$ ist reduzibel oder irreduzibel, je nachdem die aus ihren Koordinaten gebildete Determinante verschwindet oder nicht verschwindet.

---

*) Im Falle $n = 1$ ist hierdurch allein die Behauptung schon erwiesen.

Um dies zu beweisen, betrachten wir ein beliebiges System von n Zahlen $\alpha_1, \alpha_2, \ldots, \alpha_n$, die in Ω enthalten, also von der Form

$$\alpha_r = a_{r,1}\,\omega_1 + a_{r,2}\,\omega_2 + \cdots + a_{r,n}\,\omega_n$$

sind, und bezeichnen mit a die aus den Koordinaten $a_{r,s}$ gebildete Determinante. Bilden nun diese n Zahlen α_r ein reduzibles System, so gibt es n Zahlen $x_1, x_2, \ldots, x_n$ in A, die nicht alle verschwinden und die der Bedingung

$$x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n = 0$$

genügen; ersetzt man hierin die n Zahlen α_r durch die vorstehenden Ausdrücke, so müssen, weil die n Zahlen ω_s voneinander unabhängig sind, die in A enthaltenen n Summen

$$a_{1,s}\,x_1 + a_{2,s}\,x_2 + \cdots + a_{n,s}\,x_n = 0$$

sein, und hieraus folgt bekanntlich, daß jedes der Produkte $a\,x_1$, $a\,x_2, \ldots, a\,x_n$, also auch a selbst verschwindet. Bilden aber die n Zahlen α_r ein irreduzibles System, also auch eine neue Basis von Ω, so sind die n Zahlen ω_s darstellbar in der Form

$$\omega_s = b_{1,s}\,\alpha_1 + b_{2,s}\,\alpha_2 + \cdots + b_{n,s}\,\alpha_n,$$

wo wieder alle Koeffizienten $b_{r,s}$, deren Determinante wir mit b bezeichnen, in A enthalten sind. Substituiert man diese Darstellungen der Zahlen ω_s in den obigen Ausdruck für α_r, so folgt, daß jede der in A enthaltenen n^2 Summen

$$a_{r,1}\,b_{s,1} + a_{r,2}\,b_{s,2} + \cdots + a_{r,n}\,b_{s,n} = 1 \quad \text{oder} \quad = 0$$

ist, je nachdem r, s gleich oder verschieden sind; nach dem bekannten Satze über die Multiplikation der Determinanten folgt hieraus $ab = 1$, mithin ist a von Null verschieden, was zu beweisen war. —

Wir wenden uns nun zu der wichtigen Frage: Wann ist eine solche, durch die Eigenschaften I, II, III charakterisierte Schar Ω ein Körper? Soll dies der Fall sein, so müssen alle Produkte $\omega_r\,\omega_s$ aus je zwei Elementen der Basis ebenfalls in Ω enthalten, also muß

$$\omega_r\,\omega_s = a_1^{r,s}\,\omega_1 + a_2^{r,s}\,\omega_2 + \cdots + a_n^{r,s}\,\omega_n$$

sein, wo alle Koeffizienten $a_m^{r,s}$ Zahlen des Körpers A bedeuten*). Sind diese Bedingungen erfüllt, so leuchtet ein, daß die Zahlen ω

*) Zufolge der allgemeinen Gesetze $\omega_r\,\omega_s = \omega_s\,\omega_r$ und $(\omega_r\,\omega_s)\,\omega_t = \omega_r\,(\omega_s\,\omega_t)$ müssen diese Koeffizienten gewisse Bedingungen erfüllen, die wir aber hier nicht weiter zu verfolgen brauchen. Vgl. § 159 der zweiten Auflage (1871) dieses Werkes [wiedergegeben unter XLVII] und meinen Aufsatz: Zur Theorie der aus n Haupteinheiten gebildeten komplexen Größen (Nachrichten von der Göttinger Ges. d. W. 1885, S. 141).

der Schar $\mathfrak{Q}$ sich nicht nur (zufolge I) durch Addition und Subtraktion, sondern auch durch Multiplikation reproduzieren; ist ferner α eine beliebige, aber von Null verschiedene Zahl in $\mathfrak{Q}$, so bilden die n Produkte $\alpha\omega_r$ gewiß ein irreduzibles System, und da sie ebenfalls in $\mathfrak{Q}$ enthalten sind, so können sie als eine neue Basis von $\mathfrak{Q}$ dienen; mithin ist jede Zahl ω auch darstellbar in der Form:

$$\omega = \alpha(k_1\omega_1 + k_2\omega_2 + \cdots + k_n\omega_n),$$

wo die n neuen Koordinaten k_r wieder dem Körper A angehören, und folglich ist auch jeder Quotient von zwei Zahlen ω, α der Schar $\mathfrak{Q}$ wieder eine Zahl in $\mathfrak{Q}$. Wir haben daher folgenden Satz gewonnen:

V. Die erforderlichen und hinreichenden Bedingungen dafür, daß die Schar $\mathfrak{Q}$ ein Körper ist, bestehen darin, daß alle Produkte aus zwei Elementen einer Basis von $\mathfrak{Q}$ wieder in $\mathfrak{Q}$ enthalten sind.

Jede Basis der Schar $\mathfrak{Q}$ nennen wir nun auch eine Basis des Körpers $\mathfrak{Q}$ in bezug auf A. Da dieser Körper $\mathfrak{Q}$ gewiß die Zahl 1 enthält, so ergibt sich aus II der Satz:

VI. Ist die Schar $\mathfrak{Q}$ ein Körper, so ist A ein Divisor von $\mathfrak{Q}$.

Da ferner, wenn ω eine beliebige Zahl dieses Körpers $\mathfrak{Q}$ bedeutet, auch alle Potenzen ω^2, ω^3, ... in $\mathfrak{Q}$ enthalten sind, so bilden zufolge III die $n+1$ Zahlen ω^n, ω^{n-1}, ..., ω, 1 gewiß ein reduzibles System, was wir so aussprechen können:

VII. Ist die Schar $\mathfrak{Q}$ ein Körper, so ist jede darin enthaltene Zahl algebraisch in bezug auf A, und zwar höchstens vom Grade n.

Wir betrachten jetzt zwei Körper A, B und nehmen an, es gebe n Zahlen ω_1, ω_2, ..., ω_n in B, die ein nach A irreduzibles System bilden, aber jedes System von $n+1$ Zahlen des Körpers B sei reduzibel; da jeder Teil eines irreduziblen Systems ebenfalls irreduzibel ist, so kann es nur eine einzige solche Anzahl n geben; in diesem Falle sagen wir, der Körper B sei endlich und vom Grade n in bezug auf A, und bezeichnen dies durch die Gleichung *)

$$(B, A) = n.$$

*) In dieser Bedeutung habe ich das Symbol (B, A) zuerst benutzt auf S. 21 der Literaturzeitung im Jahrgang 18 von Schlömilchs Zeitschrift für Mathematik und Physik (1873).

Zunächst leuchtet ein, daß der Fall $n = 1$ dann und nur dann eintritt, wenn B Divisor von A ist; die beiden Gleichungen

$$(B, A) = 1, \quad AB = A$$

sind daher gleichbedeutend. Für einen beliebigen Grad n ergibt sich, daß B in der Schar $\mathfrak{Q}$ enthalten ist, welche aus allen Zahlen ω von der Form (1) besteht, und da alle Produkte $\omega_r \omega_s$ in B, mithin auch in $\mathfrak{Q}$ enthalten sind, so ist $\mathfrak{Q}$ (nach V, VI) ein Körper, und zwar ein Multiplum von AB; da ferner jede Zahl ω rational aus Zahlen h_r des Körpers A und Zahlen ω_r des Körpers B gebildet und folglich in AB enthalten ist, so ergibt sich, daß $\mathfrak{Q}$ auch ein Divisor von AB, mithin $\mathfrak{Q} = AB$ ist. Wir können also folgenden Satz aussprechen:

VIII. Ist B ein Körper n^{ten} Grades in bezug auf den Körper A, so ist auch

$$(AB, A) = (B, A) = n \tag{2}$$

und jedes nach A irreduzible System von n Zahlen in B oder in AB bildet eine Basis der Schar AB in bezug auf A.

Zugleich ergibt sich (aus VII), daß alle Zahlen in AB, also auch alle Zahlen in B algebraisch in bezug auf A sind, und zwar höchstens vom Grade n; daß es in B auch Zahlen n^{ten} Grades gibt, könnte zwar schon jetzt bewiesen werden, doch wollen wir, weil dies später (in § 165, VI) sich ganz von selbst ergeben wird, für jetzt darauf verzichten und nur die folgende Umkehrung beweisen:

IX. Ist θ eine algebraische Zahl n^{ten} Grades in bezug auf A, und B der Körper $R(\theta)$, welcher aus allen durch θ rational darstellbaren Zahlen besteht, also $AB = A(\theta)$, so ist $(B, A) = n$, und die n Potenzen $\theta^{n-1}, \theta^{n-2}, \ldots, \theta, 1$ bilden eine Basis von $A(\theta)$ in bezug auf A.

Hierzu betrachten wir die Schar $\mathfrak{Q}$ aller Zahlen ω von der Form

$$\omega = h_1 \theta^{n-1} + h_2 \theta^{n-2} + \cdots + h_{n-1}\theta + h_n,$$

deren Koordinaten h_r beliebige Zahlen in A sind. Da (nach Annahme) die Potenz θ^n in $\mathfrak{Q}$ enthalten ist, so gilt dasselbe (nach II, I) von $h_1 \theta^n$ und von jedem Produkte $\omega\theta$, also auch von allen höheren Potenzen $\theta^{n+1}, \theta^{n+2}, \ldots$; mithin sind alle Produkte aus je zwei Gliedern der Basis ebenfalls in $\mathfrak{Q}$ enthalten, und folglich ist $\mathfrak{Q}$ (nach V) ein Körper. Da dieser Körper $\mathfrak{Q}$ ein Multiplum von A

ist und die Zahl θ enthält, so ist er auch ein Multiplum von $A(\theta)$ und folglich $= A(\theta)$, weil umgekehrt jede Zahl ω gewiß in $A(\theta)$ enthalten ist. Der Körper $A(\theta)$ oder AB ist daher vom Grade n in bezug auf A, und dasselbe gilt folglich auch von B, was zu beweisen war.

Hieran knüpfen wir die folgenden Bemerkungen. Bedeutet t eine Variable, und bezeichnen wir mit $F(t)$, $f(t)$, $f_1(t)$, $f_2(t)$ ... ausschließlich solche ganze Funktionen von t, deren Koeffizienten im Körper A enthalten sind, so sind die Summen, Differenzen, Produkte derselben ebenfalls solche Funktionen, und durch Division von $f_1(t)$ durch $f(t)$ entspringt eine Identität von der Form $f_1(t) = f(t) f_2(t) + F(t)$, wo der Rest $F(t)$ von niedrigerem Grade als $f(t)$, oder identisch $= 0$ wird, falls $f_1(t)$ durch $f(t)$ teilbar ist. Hat nun θ dieselbe Bedeutung wie im vorstehenden Satze, so gibt es eine und nur eine Funktion n^{ten} Grades

$$f(t) = t^n + a_1 t^{n-1} + \cdots + a_{n-1} t + a_n, \tag{3}$$

welche zugleich mit $t - \theta$ verschwindet und folglich durch die Zahl θ (und A) vollständig bestimmt ist. Bezeichnet man mit $F(t)$ jede Funktion, deren Grad $< n$ ist, so wird nur dann $F(\theta) = 0$, wenn identisch $F(t) = 0$ ist. Ist daher $f_1(\theta) = 0$, so muß $f_1(t)$ durch $f(t)$ teilbar sein. Die Funktion $f(t)$ selbst kann durch keine Funktion $F(t)$ teilbar sein, weil aus $f(t) = F(t) F_1(t)$ und $f(\theta) = 0$ entweder $F(\theta) = 0$ oder $F_1(\theta) = 0$ folgen würde, was unmöglich ist. Eine solche Funktion $f(t)$, deren Koeffizienten in A enthalten sind, und welche durch keine ähnliche Funktion niedrigeren Grades teilbar ist, heißt irreduzibel oder eine Primfunktion in bezug auf A, und ebenso heißt auch die Gleichung $f(\theta) = 0$ irreduzibel. Der Körper $A(\theta)$ besteht aus allen Zahlen ω von der Form $F(\theta)$, und jede solche Zahl ω kann auch nur auf eine einzige Weise in der Form $F(\theta)$ dargestellt werden.

Hierauf gehen wir zur Betrachtung von drei Körpern A, B, C über und stellen folgenden Satz*) auf:

X. Ist B endlich in bezug auf A, und C endlich in bezug auf AB, so ist auch BC endlich in bezug auf A, und

$$(BC, A) = (C, AB)(B, A). \tag{4}$$

*) Vgl. das vorhergehende Zitat.

Bilden nämlich, wenn $(B, A) = n$ und $(C, AB) = p$ gesetzt wird, die n Zahlen ω_r in B ein irreduzibles System nach A, und die p Zahlen τ_s in C ein irreduzibles System nach AB, so bilden, wie man leicht sieht, die np Produkte $\omega_r \tau_s$ eine irreduzible Basis des Körpers ABC in bezug auf A, was zu beweisen war.

Am häufigsten tritt der Fall auf, wo B Multiplum von A und zugleich Divisor von C, also $AB = B$, $BC = C$, und folglich

$$(5) \qquad (C, A) = (C, B)(B, A)$$

ist. Außerdem folgt aus dem Satze X, daß jedes Produkt aus zwei oder mehreren, in bezug auf A endlichen Körpern wieder ein solcher Körper ist. Sind nun θ, η irgend zwei algebraische Zahlen in bezug auf A, so sind (nach IX) die Körper $R(\theta)$, $R(\eta)$ endlich in bezug auf A, und folglich gilt dasselbe von ihrem Produkte $R(\theta, \eta)$; mithin sind auch die in dem letzteren enthaltene Summe, die Differenz, das Produkt und der Quotient von θ, η algebraisch in bezug auf A, und folglich ist der Inbegriff aller in bezug auf A algebraischen Zahlen ein Körper.

Es ist vorteilhaft, dem Symbol (B, A) auch dann eine Bedeutung beizulegen, und zwar $(B, A) = 0$ zu setzen*), wenn B nicht endlich in bezug auf A ist. Hierdurch erreicht man nämlich, wie der Leser leicht finden wird, daß die in den beiden Gleichungen (2), (4) enthaltenen Sätze ohne jede Voraussetzung für beliebige Körper A, B, C gelten. Vertauscht man nun die letzteren miteinander, so erhält man gewisse Reziprozitäten und andere Beziehungen, wie z. B.

$$(6) \qquad (B, C)\,(C, A)\,(A, B) = (C, B)\,(A, C)\,(B, A),$$

deren tiefere Bedeutung aber erst durch die nachfolgenden Untersuchungen erkannt werden kann.

§ 165.

Wir verbinden jetzt die in den vorhergehenden Paragraphen erklärten Begriffe miteinander und nehmen an, der Körper A sei ein Divisor des Körpers M, und π sei eine Permutation des letzteren; der Kürze wegen bezeichnen wir, wenn ω irgendeine Zahl in M bedeutet, mit ω' die konjugierte Zahl $\omega\pi$. Bilden nun die in M enthaltenen m

*) Wenn man es vorzieht, so mag man $(B, A) = \infty$ setzen, was im wesentlichen denselben Erfolg hat.

Zahlen $\omega_1, \omega_2, \ldots, \omega_m$ ein nach A reduzibles System T, gibt es also m Zahlen $a_1, a_2, \ldots, a_m$ in A, die der Bedingung

$$a_1\omega_1 + a_2\omega_2 + \cdots + a_m\omega_m = 0$$

genügen und nicht alle verschwinden, so folgt hieraus, weil $0' = 0$ ist, auch

$$a_1'\omega_1' + a_2'\omega_2' + \cdots + a_m'\omega_m' = 0,$$

und da einer von Null verschiedenen Zahl a in A immer eine von Null verschiedene Zahl a' in $A\pi$ entspricht, so ist das in $M\pi$ enthaltene, aus den m Zahlen $\omega_1', \omega_2', \ldots, \omega_m'$ bestehende System $T\pi$ reduzibel in bezug auf $A\pi$. Da ferner jede Zahl ω' des Körpers $M\pi$ durch die inverse Permutation π^{-1} in eine Zahl ω des Körpers M übergeht, so ist umgekehrt das System T gewiß reduzibel nach A, wenn das System $T\pi$ reduzibel nach $A\pi$ ist. Wir können daher folgenden Satz aussprechen:

I. Ist der Körper M ein Multiplum des Körpers A, und π eine Permutation von M, so wird, je nachdem das in M enthaltene System T reduzibel oder irreduzibel nach A ist, das System $T\pi$ auch reduzibel oder irreduzibel nach $A\pi$ sein.

Wenden wir dies auf den Fall an, wo M das Produkt der beiden Körper A, B ist, so ergibt sich unmittelbar der Satz:

II. Ist π eine Permutation des Produktes AB der beiden Körper A, B, so ist

$$(B, A) = (B\pi, A\pi).$$

Hierauf schreiten wir zum Beweise des folgenden Fundamentalsatzes:

III. Ist der Körper B endlich in bezug auf den Körper A und φ eine Permutation von A, so ist der Grad (B, A) die Anzahl aller derjenigen verschiedenen Permutationen π des Produktes AB, welche Multipla von φ sind. Zugleich ist A der Körper und φ der Rest des Systems Π dieser Permutationen π.

Derselbe leuchtet für den Fall $(B, A) = 1$ unmittelbar ein, weil dann B ein Divisor von A, also $AB = A$, mithin notwendig $\pi = \varphi$ sein muß. Um ihn allgemein zu beweisen, wenden wir die vollständige Induktion an; wir nehmen an, er sei schon

für alle Fälle bewiesen, wo der Grad $(B, A) < n$ ist, und zeigen, daß er dann auch für $(B, A) = n$ gilt.

Hierbei müssen wir zwei Fälle unterscheiden, deren erster dann eintritt, wenn es einen dritten Körper K gibt, der ein echter Divisor von AB und zugleich ein echtes Multiplum von A ist. Setzen wir $(AB, K) = p$, $(K, A) = q$, so ist (nach den Sätzen VIII und X in § 164) $n = (B, A) = (AB, A) = (AB, K)\ (K, A) = pq$, und da K verschieden von AB und A ist, so ist jeder der beiden Grade p, $q > 1$ und folglich auch $< n$. Nach unserer Annahme gibt es daher q und nur q verschiedene Permutationen

$$\chi_1, \chi_2, \cdots, \chi_q$$

des Körpers $AK = K$, welche Multipla von φ sind, und wenn χ_r irgendeine dieser Permutationen ist, so gibt es p und nur p verschiedene Permutationen

$$\pi_{r,1}, \pi_{r,2}, \cdots, \pi_{r,p}$$

des Körpers $ABK = AB$, welche Multipla von χ_r sind, und jede dieser Permutationen $\pi_{r,s}$ ist (nach § 163) zugleich Multiplum von φ. Da ferner jeder Permutation π des Körpers AB, welche Multiplum von φ ist, immer eine und nur eine Permutation χ von K entspricht, welche Divisor von π und folglich ebenfalls Multiplum von φ ist, so sind die oben erhaltenen n Permutationen $\pi_{r,s}$, welche den q Werten r und den p Werten s entsprechen, alle voneinander verschieden, und außer diesen n Permutationen $\pi_{r,s}$ kann es keine andere Permutation π von AB geben, die ein Multiplum von φ wäre. Also ist in diesem Falle unser Satz über die Anzahl der Permutationen π bewiesen.

Im entgegengesetzten zweiten Falle, wo es keinen Körper K von der obigen Beschaffenheit gibt, wählen wir aus B (oder auch aus AB) eine nicht in A enthaltene Zahl θ, was stets möglich ist, weil $n > 1$, also B nicht Divisor von A ist. Dann muß der aus A durch Adjunktion von θ erzeugte Körper $A(\theta) = AB$ sein, weil er Divisor von AB und zugleich Multiplum von A, aber verschieden von A ist, und die in bezug auf A algebraische Zahl θ ist (nach IX in § 164) gewiß vom Grade $n = (B, A)$; der Körper $A(\theta)$ besteht aus allen Zahlen α von der Form

$$(1) \qquad \alpha = F(\theta) = x_1\theta^{n-1} + x_2\theta^{n-2} + \cdots + x_{n-1}\theta + x_n,$$

wo die n Koeffizienten oder Koordinaten x willkürliche Zahlen in A bedeuten, und zwar ist jede Zahl α nur auf eine einzige Art so darstellbar, weil die n Potenzen $\theta^{n-1}, \ldots, \theta, 1$ ein nach A irreduzibles System bilden. Die Zahl θ ist die Wurzel einer bestimmten, nach A irreduziblen Gleichung

$$(2) \quad f(\theta) = \theta^n + a_1\theta^{n-1} + a_2\theta^{n-2} + \cdots + a_{n-1}\theta + a_n = 0,$$

deren Koeffizienten a_r zugleich die Koordinaten der Zahl $-\theta^n$ sind*).

Wir suchen nun alle etwa vorhandenen Permutationen π dieses Körpers $A(\theta)$, welche Multipla von der gegebenen Permutation φ des Körpers A sind. Der Einfachheit halber setzen wir, wenn x irgendeine Zahl in A bedeutet, die aus ihr durch φ erzeugte, also gegebene Zahl

$$(3) \quad x\varphi = x';$$

dann muß, weil π ein Multiplum von φ sein soll, auch

$$(4) \quad x\pi = x'$$

sein, und da alle Zahlen α des Körpers AB rational aus Zahlen x und der einzigen Zahl θ gebildet sind, so wird die Permutation π vollständig bestimmt sein, sobald auch $\theta\pi$ bekannt ist; setzen wir der Kürze halber diese Zahl

$$(5) \quad \theta\pi = \eta,$$

so folgt aus (1) und (2), daß jede in der Form (1) dargestellte Zahl α durch π in die zugehörige Zahl

$$(6) \quad \alpha\pi = \mathfrak{F}(\eta) = x_1'\eta^{n-1} + x_2'\eta^{n-2} + \cdots + x_{n-1}'\eta + x_n'$$

übergeht, und daß η eine Wurzel der bestimmten Gleichung

$$(7) \quad \mathfrak{f}(\eta) = \eta^n + a_1'\eta^{n-1} + a_2'\eta^{n-2} + \cdots + a_{n-1}'\eta + a_n' = 0$$

sein muß. Umgekehrt, wenn η eine bestimmte Wurzel dieser Gleichung (7) bedeutet, so ist, weil jede Zahl α des Körpers $A(\theta)$ stets und nur auf eine einzige Weise in der Form (1) darstellbar ist, durch das Gesetz (6), worin (4) und (5) als spezielle Fälle enthalten sind, eine Abbildung π dieses Körpers vollständig bestimmt, und wir wollen jetzt beweisen, daß dieselbe wirklich eine Permu-

*) Es ist gut, zu bemerken, daß alles Folgende für jeden solchen Körper $A(\theta)$ gilt, der aus einer Zahl θ vom Grade n entspringt.

tation ist. Hierzu brauchen wir (nach § 161) nur zu zeigen, daß für je zwei Zahlen α, β des Körpers AB die beiden Gesetze

$$(8) \qquad (\alpha + \beta)\pi = \alpha\pi + \beta\pi$$

$$(9) \qquad (\alpha\beta)\pi = (\alpha\pi)(\beta\pi)$$

gelten. Bezeichnet man mit y_r die Koordinaten von β, so sind $x_r + y_r$ diejenigen von $\alpha + \beta$; da nun φ eine Permutation von A, also $(x_r + y_r)' = x_r' + y_r'$ ist, so ergibt sich aus (6) unmittelbar das Gesetz (8). Da dasselbe natürlich auch für Summen von mehr als zwei Gliedern gilt, und da jede Zahl β eine Summe von Produkten ist, deren Faktoren teils in A enthalten, teils $= \theta$ sind, so erkennt man leicht, daß das Gesetz (9) nur noch für die beiden Fälle zu beweisen ist, wo β entweder eine beliebige Zahl y des Körpers A oder $= \theta$ ist. Da nun die Koordinaten $y x_r$ des Produktes αy durch die Permutation φ in $(y x_r)' = y' x_r'$ übergehen, so folgt aus (6) der erste Fall $(\alpha y)\pi = (\alpha\pi) y'$, und ebenso leicht ergibt sich der zweite Fall $(\alpha\theta)\pi = (\alpha\pi)\eta$, wenn man bedenkt, daß zufolge (2), (6), (7) auch $(\theta^n)\pi = \eta^n$ ist. Hiermit ist der Beweis geliefert, daß jeder Wurzel η der Gleichung (7) wirklich eine durch (6) definierte Permutation π des Körpers AB entspricht, welche ein Multiplum von φ ist*).

Zugleich folgt aus dem Satze I, daß die n Potenzen $\eta^{n-1}, \ldots, \eta, 1$ ein irreduzibles System in bezug auf den Körper $A\pi = A\varphi$ bilden. Nun gibt es nach dem zuerst von Gauß bewiesenen Hauptsatze der Algebra im allgemeinen n verschiedene Wurzeln η der Gleichung (7), und ihre Anzahl ist bekanntlich nur dann kleiner als n, wenn wenigstens eine dieser Zahlen η zugleich der Bedingung

$$f'(\eta) = n\eta^{n-1} + (n-1)a_1'\eta^{n-2} + (n-2)a_2'\eta^{n-3} + \cdots + a_{n-1}' = 0$$

genügt; da dies aber mit der eben bewiesenen Irreduzibilität im Widerspruch stehen würde, so hat die Gleichung (7) wirklich n verschiedene Wurzeln η, und es gibt folglich genau n ver-

*) Bedeuten (wie in § 164) $f(t)$, $F(t)$, $f_1(t)\ldots$ ganze Funktionen der Variablen t, deren Koeffizienten c in A enthalten sind, und gehen aus ihnen bzw. die Funktionen $\mathfrak{f}(t)$, $\mathfrak{F}(t)$, $\mathfrak{f}_1(t)\ldots$ dadurch hervor, daß jeder Koeffizient c durch $c' = c\varphi$ ersetzt wird, so folgen, weil φ eine Permutation von A ist, aus den Identitäten $F(t) + F_1(t) = F_2(t)$, $F(t)F_1(t) = f(t)f_1(t) + F_3(t)$ immer die Identitäten $\mathfrak{F}(t) + \mathfrak{F}_1(t) = \mathfrak{F}_2(t)$, $\mathfrak{F}(t)\mathfrak{F}_1(t) = \mathfrak{f}(t)\mathfrak{f}_1(t) + \mathfrak{F}_3(t)$. Hierin liegt offenbar ein Beweis der Gesetze (8) und (9), von welchem der oben im Text gegebene nur eine Umschreibung ist.

schiedene Permutationen π des Körpers AB, welche Multipla von φ sind, was zu beweisen war.

Nachdem hiermit der Satz III, soweit er von der Anzahl der Permutationen π handelt, allgemein bewiesen ist, können wir auch seinen letzten Teil leicht erledigen. Denn wenn K den Körper, und χ den Rest des Systems Π bedeutet, so besteht K (nach § 163) aus allen zu Π einwertigen Zahlen, ist also Multiplum von A und Divisor von AB, und seine Permutation χ ist Multiplum von φ; setzt man wieder $(AB, K) = p$, $(K, A) = q$, so ist $n = pq$, und nach dem schon bewiesenen Teile des Satzes ist p die genaue Anzahl derjenigen verschiedenen Permutationen von AB, welche Multipla von χ sind; unter diesen befinden sich aber gewiß die n Permutationen π, und folglich ist $p \geqq n$, mithin $p = n$, $q = 1$, $K = A$, $\chi = \varphi$, was zu beweisen war. —

Nachdem der Fundamentalsatz III vollständig bewiesen ist, bemerken wir zunächst, daß die auf B bezüglichen Divisoren ψ der n Permutationen π ebenfalls voneinander verschieden sind, weil (nach § 163) jede Permutation π des Produktes AB umgekehrt durch ihre auf A, B bezüglichen Divisoren φ, ψ vollständig bestimmt ist. Der Körper des Systems Ψ dieser n mit φ einigen Permutationen ψ ist, wie unmittelbar einleuchtet, der größte gemeinsame Divisor D von A, B, und der Rest von Ψ ist der auf D bezügliche Divisor von φ.

Ist ferner φ' ebenfalls eine Permutation von A, also $\varphi^{-1}\varphi'$ eine Permutation von $A\varphi$, und Π' das System derjenigen n Permutationen π' von AB, welche Multipla von φ' sind, so sind, wenn π eine bestimmte Permutation in Π bedeutet, die n Permutationen $\pi^{-1}\pi'$ des Körpers $(AB)\pi$ verschieden und zugleich Multipla von $\varphi^{-1}\varphi'$ (nach § 163), und da der Körper $(AB)\pi$ zufolge II vom Grade n in bezug auf $A\varphi$ ist, so kann es zufolge III außer diesen n Permutationen $\pi^{-1}\pi'$, durch welche $(AB)\pi$ in die n Körper $(AB)\pi'$ übergeht, und deren Komplex zweckmäßig durch $\pi^{-1}\Pi'$ bezeichnet wird, keine andere Permutation von $(AB)\pi$ geben, die zugleich Multiplum von $\varphi^{-1}\varphi'$ wäre; es ist also $A\varphi$ der Körper, $\varphi^{-1}\varphi'$ der Rest des Systems $\pi^{-1}\Pi'$. —

Von jetzt ab wollen wir nur noch den speziellen Fall betrachten, in welchem φ die identische Permutation von A ist; dann sind in den Systemen Π, Ψ offenbar auch die identischen Permutationen

von AB, B enthalten; A ist der Inbegriff aller Zahlen in AB, welche durch jede Permutation π in sich selbst übergehen, und ebenso ist D der Inbegriff aller Zahlen in B, welche durch jede Permutation ψ in sich selbst übergehen. Bedeutet nun T irgendeine in AB enthaltene Reihe von n Zahlen $\omega_1, \omega_2, \ldots, \omega_n$, und sind $\pi_1, \pi_2, \ldots, \pi_n$ die in einer bestimmten Folge geordneten Permutationen in Π, so wollen wir die aus den n^2 Elementen $\omega_r \pi_s$ gebildete Determinante

$$(10) \qquad \begin{vmatrix} \omega_1\pi_1, & \omega_2\pi_1, & \ldots, & \omega_n\pi_1 \\ \omega_1\pi_2, & \omega_2\pi_2, & \ldots, & \omega_n\pi_2 \\ \ldots & \ldots & \ldots & \ldots \\ \omega_1\pi_n, & \omega_2\pi_n, & \ldots, & \omega_n\pi_n \end{vmatrix} = (T)$$

setzen und kurz die Determinante des Systems T nennen. Dann gilt folgender Satz:

IV. Die erforderliche und hinreichende Bedingung dafür, daß das System T irreduzibel nach A ist und folglich eine Basis von AB bildet, besteht darin, daß die Determinante (T) nicht verschwindet; und der Quotient von je zwei solchen Determinanten (T) ist in A enthalten.

Denn wenn T irreduzibel ist, so kann jede Zahl α der Schar AB in der Form

$$(11) \qquad \alpha = x_1\omega_1 + x_2\omega_2 + \cdots + x_n\omega_n$$

dargestellt werden, wo die Zahlen x_r die in A enthaltenen Koordinaten von α bedeuten, und folglich ist zugleich

$$(12) \qquad \alpha\pi_s = x_1(\omega_1\pi_s) + x_2(\omega_2\pi_s) + \cdots + x_n(\omega_n\pi_s).$$

Ist nun U ein System von n solchen Zahlen $\alpha_1, \alpha_2, \ldots, \alpha_n$, und $a_{r,s}$ die s^{te} Koordinate von α_r, so ist

$$(13) \qquad \alpha_r = a_{r,1}\omega_1 + a_{r,2}\omega_2 + \cdots + a_{r,n}\omega_n$$
$$\alpha_r\pi_s = a_{r,1}(\omega_1\pi_s) + a_{r,2}(\omega_2\pi_s) + \cdots + a_{r,n}(\omega_n\pi_s)$$

und folglich nach dem bekannten Satze der Determinantentheorie

$$(14) \qquad (U) = a(T),$$

wo a die aus den Koordinaten $a_{r,s}$ gebildete Determinante

$$(15) \qquad a = \begin{vmatrix} a_{1,1}, & a_{1,2}, & \ldots, & a_{1,n} \\ a_{2,1}, & a_{2,2}, & \ldots, & a_{2,n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n,1}, & a_{n,2}, & \ldots, & a_{n,n} \end{vmatrix}$$

bedeutet, also in A enthalten ist. Da nun nach einem früheren Satze (am Schlusse von § 161) in AB gewiß ein System U existiert, dessen Determinante (U) nicht verschwindet, so folgt aus (14), daß (T) von Null verschieden ist*). Wenn aber zweitens T reduzibel ist, so gibt es n Zahlen x_r in A, welche nicht sämtlich verschwinden, für welche aber die Summe α in (11), also auch alle n Summen $\alpha\pi_s$ in (12) verschwinden, und hieraus folgt bekanntlich, daß auch $(T) = 0$ ist, was zu beweisen war.

Unter der in bezug auf A genommenen Norm des Körpers B verstehen wir das Produkt P der n konjugierten Körper $B\pi$ oder $B\psi$, in welche B durch die n Permutationen ψ des Systems Ψ übergeht; da unter diesen sich auch die identische Permutation von B befindet, so ist die Norm P immer ein Multiplum von B. Offenbar ist AP zugleich die Norm von AB, weil $A\pi = A$, also $(AB)\pi = A(B\psi)$ ist, und aus dem Beweise des vorhergehenden Satzes ergibt sich leicht der folgende:

V. Ist P die Norm des Körpers B in bezug auf A, und Q der größte gemeinsame Divisor von P und A, so ist $(B, A) = (B, Q)$.

Denn wenn man aus B ein nach A irreduzibles System T von n Zahlen $\omega_1, \omega_2, \ldots, \omega_n$ wählt, so ist jede Zahl α des Körpers B in der Form (11) darstellbar; da nun die Determinante (T) nicht verschwindet, und da alle in (12) auftretenden Zahlen $\alpha\pi$, $\omega_r\pi$ in P enthalten sind, so gilt dasselbe von den Koordinaten x_r, welche mithin gewiß dem Körper Q angehören; das nach A, und folglich auch nach Q irreduzible System T wird daher durch Hinzufügung jeder in B enthaltenen Zahl α reduzibel nach Q, und folglich ist $(B, Q) = n$, was zu beweisen war.

Bedeutet ferner θ eine beliebige Zahl in AB, und T das System der n Potenzen $\theta^{n-1}, \theta^{n-2}, \ldots, \theta, 1$, so ist die Determinante (T), wie wir schon früher (am Schlusse von § 161) bemerkt haben, das Produkt der sämtlichen Differenzen $\theta\pi_r - \theta\pi_s$, wo $r < s$, und folglich wird das System T stets und nur dann irreduzibel nach A, wenn θ eine n-wertige Zahl zu Π ist; da nun jede in AB enthaltene Zahl (nach § 164, VIII) algebraisch in bezug auf A und höchstens vom Grade n ist, so folgt hieraus, daß jede n-wer-

*) Man vergleiche hiermit den Satz IV in § 164.

tige Zahl θ und keine andere vom Grade n ist. Da ferner das System Ψ aus n verschiedenen Permutationen ψ des Körpers B besteht, so gibt es in B (nach § 161) unendlich viele Zahlen θ, welche n-wertig zu Ψ, also auch zu Π sind, und wir können daher folgenden Satz aussprechen:

VI. Ist B ein Körper n^{ten} Grades in bezug auf A, so gibt es in B auch unendlich viele Zahlen θ vom Grade n in bezug auf A, und zugleich ist $A(\theta) = AB$.

Wenn umgekehrt ein Körper B aus lauter Zahlen besteht, die algebraisch in bezug auf A sind, und deren Grade eine endliche Höhe nicht überschreiten, so ergibt sich aus den vorhergehenden Sätzen ohne Schwierigkeit, daß B endlich in bezug auf A ist. Ein anderes, ebenfalls charakteristisches Kriterium dieser Endlichkeit besteht darin, daß die Anzahl aller der verschiedenen Körper K, welche Multipla von A und zugleich Divisoren von AB sind, endlich ist. Wir wollen hier aber nur auf den einen Teil dieses Satzes eingehen, indem wir wieder annehmen, B sei vom Grade n in bezug auf A, und mit Π das System der n Permutationen π von AB bezeichnen, welche Multipla der identischen Permutation φ von A sind; setzt man $(AB, K) = p$, $(K, A) = q$, so ist $n = pq$, und K ist (nach VI) von der Form $A(\alpha)$, wo α eine in K, also auch in AB enthaltene Zahl vom Grade q bedeutet, und umgekehrt erzeugt jede Zahl α in AB einen solchen Körper $K = A(\alpha)$. Nun gibt es (nach III) q verschiedene Permutationen χ von K, welche Multipla von φ sind, und durch welche α in q verschiedene Werte $\alpha\chi$ übergeht; jede bestimmte solche Permutation χ ist wieder der Rest eines Systems Π' von p Permutationen π', welche einen und denselben Wert $\alpha\pi' = \alpha\chi$ erzeugen, und das System Π besteht aus diesen q Komplexen Π'. Da nun umgekehrt K durch jeden einzelnen Komplex Π' als zugehöriger Körper (nach § 163) vollständig bestimmt ist, so leuchtet ein, daß die Anzahl solcher Körper K endlich ist, weil ein endliches System Π auch nur eine endliche Anzahl von Teilen Π' besitzt. — Auf den Beweis der Umkehrung, welcher zwar nicht schwierig ist, aber doch einige Hilfssätze erfordert, müssen wir der Kürze halber hier verzichten.

Für die Algebra bildet nun die vollständige Bestimmung aller dieser Körper K und die Untersuchung ihrer gegenseitigen Be-

ziehungen die wichtigste Aufgabe, deren Lösung von Lagrange*) begonnen und endlich von Galois**) zu einem systematischen Abschluß durch die Theorie der Gruppen gebracht ist. Obgleich wir auf die letztere selbst nicht näher eingehen können, so wollen wir doch von unserem Standpunkte aus noch andeuten, worin diese Zurückführung besteht.

§ 166.

Ein System Π von n verschiedenen Körperpermutationen π heißt eine Gruppe, wenn jede mit jeder zusammensetzbar, und wenn die Resultante immer in Π enthalten ist.

Aus dieser Erklärung folgt zunächst, daß die in einer Gruppe Π enthaltenen Permutationen π sich alle auf einen und denselben Körper beziehen, und daß dieser Körper M durch jede Permutation π in sich selbst übergeht. Bedeutet ferner π' eine bestimmte dieser n Permutationen, während π sie alle durchläuft, so sind die n Resultanten $\pi\pi'$ (nach § 162) alle verschieden, mithin ist ihr Komplex identisch mit Π; es gibt daher, wenn π', π'' zwei bestimmte Permutationen sind, immer eine und nur eine Permutation π, welche der Bedingung $\pi\pi' = \pi''$ genügt. Nimmt man $\pi' = \pi''$, so ergibt sich, daß in Π auch die identische Permutation von M enthalten ist. Auf diesen Eigenschaften einer Gruppe beruht der folgende Fundamentalsatz:

I. Besteht eine Gruppe Π aus n verschiedenen Permutationen π des Körpers M, und ist A der Körper von Π, so ist $(M, A) = n$, und der Rest von Π ist die identische Permutation von A.

Um dies zu beweisen, wählen wir (nach § 161) aus M ein System von n Zahlen α_r so aus, daß die aus den n^2 Zahlen $\alpha_r\pi$ gebildete Determinante nicht verschwindet; dann gibt es, wenn ω irgendeine bestimmte Zahl in M bedeutet, ein und nur ein System von n Zahlen x_r, welche den n linearen Gleichungen

$$(1) \qquad \omega\pi = x_1(\alpha_1\pi) + x_2(\alpha_2\pi) + \cdots + x_n(\alpha_n\pi)$$

*) Réflexions sur la résolution algébrique des équations (Mém. de l'Acad. de Berlin, 1770, 1771. — Œuvres de L. Tome III).

**) Sur les conditions de résolubilité des équations par radicaux (Liouvilles Journal, t. XI, 1846).

genügen; da alle hier auftretenden Zahlen $\omega\pi$, $\alpha\pi$ in M enthalten sind, so gilt dasselbe auch von diesen n Zahlen x_r, und folglich entspringt, wenn π' eine bestimmte Permutation in Π bedeutet, aus dem vorstehenden System (1) das folgende

$$\omega\pi\pi' = (x_1\pi')(\alpha_1\pi\pi') + (x_2\pi')(\alpha_2\pi\pi') + \cdots + (x_n\pi')(\alpha_n\pi\pi'),$$

welches, weil $\pi\pi'$ zugleich mit π das ganze System Π durchläuft, auch in der Form

$$\omega\pi = (x_1\pi')(\alpha_1\pi) + (x_2\pi')(\alpha_2\pi) + \cdots + (x_n\pi')(\alpha_n\pi)$$

dargestellt werden kann; durch Vergleichung mit (1) ergibt sich hieraus $x_r\pi' = x_r$, und folglich sind die n Zahlen x_r in dem Körper A enthalten, welcher (nach § 163) aus allen zu Π einwertigen Zahlen besteht. Da unter den Permutationen π sich auch die identische Permutation von M befindet, so folgt aus (1), daß jede Zahl ω des Körpers M in der Form

$$\omega = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n$$

darstellbar ist, wo die Koeffizienten x_r dem Körper A angehören; mithin ist M endlich in bezug auf A, und zwar $(M, A) \leqq n$; da es aber n verschiedene Permutationen π von M gibt, welche Multipla der identischen Permutation von A sind, so folgt (nach § 165, III), daß $(M, A) = n$, und daß das System der n Zahlen α_r irreduzibel nach A ist, was zu beweisen war.

Bildet nun ein Teil der Gruppe Π ebenfalls eine Gruppe Π', welche aus p Permutationen π' besteht, so ist der zu Π' gehörige Körper A' Divisor von M und Multiplum von A, weil jede zu Π einwertige Zahl auch einwertig zu Π' ist, und zugleich ist $n = pq$, wo $p = (M, A')$, $q = (A', A)$; bezeichnet man ferner, wenn π eine bestimmte Permutation in Π bedeutet, π' aber alle Permutationen der Gruppe Π' durchläuft, mit $\Pi'\pi$ den Komplex der p Resultanten $\pi'\pi$, und mit φ' den Rest von $\Pi'\pi$, so besteht die Gruppe Π aus q verschiedenen Komplexen $\Pi'\pi$, und deren Reste φ' stimmen überein mit denjenigen q Permutationen des Körpers A', welche Multipla der identischen Permutation von A sind. Umgekehrt, wenn ein Körper A' Divisor von M und Multiplum von A ist, so bilden, wie man leicht sieht, diejenigen Permutationen von M, welche Multipla der identischen Permutation von A' sind, eine in Π enthaltene Gruppe Π', und A' ist der zu Π' gehörige Körper. Ist ferner Π'' ebenfalls eine in Π enthaltene Gruppe, und A'' der zugehörige Körper,

so bilden die den beiden Gruppen Π', Π'' gemeinsamen Permutationen wieder eine Gruppe; und der zugehörige Körper ist das Produkt $A'A''$.

Hieraus erkennt man, daß die vollständige Bestimmung aller dieser Körper A', A'', ... und die Untersuchung ihrer gegenseitigen Beziehungen vollständig erledigt wird durch die Bestimmung aller in der Gruppe Π enthaltenen Gruppen Π', Π'', ..., und diese Aufgabe gehört in die allgemeine*) Theorie der Gruppen.

Nun läßt sich der allgemeine Fall (§ 165), wo $(B, A) = n > 0$, und wo es sich um die Bestimmung aller Körper K handelt, die Multipla von A und zugleich Divisoren von AB sind, leicht auf den eben besprochenen zurückführen. Bedeutet φ wieder die identische Permutation von A, und Π das System der n Permutationen π von AB, welche Multipla von φ sind, so haben wir schon bemerkt, daß die Norm von B, d. h. das Produkt P der n Körper $B\pi$, ein Multiplum von B ist. Wenn nun $P = B$, also B seine eigene Norm ist, soll B ein Normalkörper in bezug auf A heißen; dieser Fall tritt stets und auch nur**) dann ein, wenn alle Körper $B\pi$ identisch mit B sind, und offenbar ist dann auch AB normal in bezug auf A. Ist nun das letztere der Fall — was, wie wir doch bemerken wollen, auch eintreten kann, ohne daß B normal in bezug auf A ist —, so überzeugt man sich leicht, daß Π eine Gruppe ist, und daß alles, was oben von dem Körper M gesagt ist, für diesen Körper AB gilt. Ist aber AB (und folglich auch B) nicht

*) Schon in meinen Göttinger Vorlesungen (1857—1858) habe ich diese Theorie in der Weise vorgetragen, daß sie für Gruppen Π von beliebigen Elementen π gilt.

**) Zunächst folgt allerdings nur, daß jeder Körper $B\pi$ Divisor von B sein muß; da aber (nach § 164) jede Zahl ω in B algebraisch in bezug auf A ist, und da die Zahlen der unendlichen Kette ω, $\omega' = \omega\pi$, $\omega'' = \omega'\pi$, $\omega''' = \omega''\pi$ ... in B enthalten und Wurzeln einer und derselben, nach A irreduziblen Gleichung sind, so müssen in ihr Wiederholungen von der Form $\omega^{(r)} = \omega^{(r+s)}$ auftreten, wo $s > 0$, und da aus $\alpha\pi = \beta\pi$ stets $\alpha = \beta$ folgt, so ergibt sich $\omega = \omega^{(s)}$, und folglich ist jede in B enthaltene Zahl ω auch in $B\pi$ enthalten, also $B\pi = B$. — Um diese Betrachtung in das rechte Licht zu setzen, bemerken wir noch folgendes. Sind τ, τ' irgend zwei transzendente, d. h. nicht algebraische Zahlen in bezug auf A, so geht der Körper $A(\tau)$ durch unendlich viele Permutationen, welche Multipla der identischen Permutation von A sind, in $A(\tau')$ über, und unter ihnen ist eine einzige π, für welche $\tau\pi = \tau'$ wird; nimmt man nun z. B. $\tau' = \tau^2$, so leuchtet leicht ein, daß der mit $A(\tau)$ konjugierte Körper $A(\tau^2)$ ein echter Divisor von $A(\tau)$ ist.

normal in bezug auf A, so ist doch immer die Norm P von B und folglich auch AP normal in bezug auf A; ist nämlich χ eine bestimmte Permutation von AP, und zwar Multiplum von φ, so sind (nach § 165) die auf die n Körper $AB\pi$ bezüglichen Divisoren von χ von der Form $\pi^{-1}\pi'$, wo π' gleichzeitig mit π alle in Π enthaltenen Permutationen durchläuft*), und folglich ist $(AP)\chi = AP$, d. h. AP (und ebenso auch P) ist normal in bezug auf A, das System X aller Permutationen χ ist eine Gruppe, φ deren Rest, und die obigen Prinzipien gelten für den Körper $M = AP$.

Hieraus folgt beiläufig auch noch der wichtige Satz, daß, wenn ω irgendeine in AB enthaltene Zahl bedeutet, jede aus den n Zahlen $\omega\pi$ auf rationale und symmetrische Weise abgeleitete Zahl gewiß in A enthalten ist, weil sie offenbar einwertig zu X ist.

§ 167.

Wir bezeichnen wieder mit φ die identische Permutation eines Körpers A, mit B einen in bezug auf A endlichen Körper vom Grade n, mit Π das System der n verschiedenen Permutationen π von AB, welche Multipla von φ sind, und führen folgende Begriffe ein. Ist α eine beliebige Zahl in AB, so verstehen wir unter ihrer Spur $S(\alpha)$ die Summe, unter ihrer Norm $N(\alpha)$ das Produkt der n mit α konjugierten Zahlen $\alpha\pi$; da (nach § 161) das Bild $\alpha\pi$ einer von Null verschiedenen Zahl α niemals verschwindet, so ist nur dann $N(\alpha) = 0$, wenn $\alpha = 0$ ist. Ist x eine einwertige, also in A enthaltene Zahl, so ergibt sich

$$S(x) = nx,\ S(x\alpha) = xS(\alpha) \tag{1}$$

$$N(x) = x^n,\ N(x\alpha) = x^n N(\alpha), \tag{2}$$

und wenn β ebenfalls eine in AB enthaltene Zahl ist, so folgt aus den Gesetzen $(\alpha \pm \beta)\pi = \alpha\pi \pm \beta\pi$ und $(\alpha\beta)\pi = (\alpha\pi)(\beta\pi)$, daß

$$S(\alpha \pm \beta) = S(\alpha) \pm S(\beta) \tag{3}$$

$$N(\alpha\beta) = N(\alpha)\ N(\beta), \tag{4}$$

*) Denn wählt man aus AB irgendeine n-wertige Zahl θ, so müssen die n verschiedenen, in AP enthaltenen Zahlen $\theta\pi$ durch die Permutation χ (nach § 161) auch in n verschiedene Bilder $\theta\pi'$ übergehen, und folglich sind auch die n Permutationen π' verschieden; die Permutation χ erzeugt also eine gewisse Vertauschung (Permutation) der n Werte $\theta\pi$ untereinander.

daß also die Spur einer Summe von Zahlen gleich der Summe ihrer Spuren, und die Norm eines Produktes gleich dem Produkte aus den Normen der Faktoren ist.

Bedeutet T irgendein System von n Zahlen $\omega_1, \omega_2, \ldots, \omega_n$ in AB, so haben wir schon (in § 165, (10)) die aus den n^2 Zahlen $\omega_r \pi_s$ gebildete Determinante mit (T) bezeichnet, und wir wollen jetzt das Quadrat von (T), welches von der Reihenfolge der Zahlen ω_r und der Permutationen π_s gänzlich unabhängig ist, die Diskriminante des Systems T nennen und kurz mit ΔT oder $\Delta(\omega_1, \omega_2, \ldots, \omega_n)$ bezeichnen; dieselbe ist (nach § 165, IV) stets und nur dann von Null verschieden, wenn das System T irreduzibel ist und folglich eine Basis von AB bildet; und wenn ein System U von n Zahlen $\alpha_1, \alpha_2, \ldots, \alpha_n$ mit T durch n Gleichungen von der Form

$$\alpha_r = a_{r,1}\omega_1 + a_{r,2}\omega_2 + \cdots + a_{r,n}\omega_n \tag{5}$$

verbunden ist, wo alle Koeffizienten $a_{r,s}$ in A enthalten sind, so folgt

$$(U) = a\,(T),\ \Delta U = a^2 \Delta T, \tag{6}$$

wo a die aus diesen Koeffizienten $a_{r,s}$ gebildete Determinante bedeutet [§ 165, (13) bis (15)].

Zwischen den Determinanten (T), den Spuren und Normen bestehen ferner die folgenden Beziehungen. Bezeichnet man das System der n Produkte $\alpha\omega_1, \alpha\omega_2, \ldots, \alpha\omega_n$ kurz mit αT, so folgt aus $(\alpha\omega_r)\pi_s = (\alpha\pi_s)(\omega_r\pi_s)$, daß die zugehörige Determinante

$$(\alpha T) = N(\alpha)(T) \tag{7}$$

ist. Wenn ferner U ein System von n Zahlen α_r, und V ein System von n Zahlen β_s ist, so folgt bekanntlich aus

$$S(\alpha_r\beta_s) = (\alpha_r\pi_1)(\beta_s\pi_1) + \cdots + (\alpha_r\pi_n)(\beta_s\pi_n),$$

daß das Produkt

$$(U)(V) = \begin{vmatrix} S(\alpha_1\beta_1) & \ldots & S(\alpha_1\beta_n) \\ \cdots & \cdots & \cdots \\ S(\alpha_n\beta_1) & \ldots & S(\alpha_n\beta_n) \end{vmatrix} \tag{8}$$

und folglich die Diskriminante

$$\Delta T = \begin{vmatrix} S(\omega_1\omega_1) & \ldots & S(\omega_1\omega_n) \\ \cdots & \cdots & \cdots \\ S(\omega_n\omega_1) & \ldots & S(\omega_n\omega_n) \end{vmatrix} \tag{9}$$

ist.

Aus der Schlußbemerkung des vorigen Paragraphen folgt unmittelbar, daß alle Spuren und Normen Zahlen des Körpers A

sind, und da (nach § 165, VI) alle Zahlen des Körpers AB rational durch die des Körpers A und durch eine einzige n-wertige Zahl θ darstellbar sind, so folgt dasselbe [ohne Zuziehung von (8) und (9)] auch für jedes Produkt von zwei Determinanten (T), also auch für jede Diskriminante ΔT, weil diese Größen ebenfalls symmetrisch aus den n konjugierten Zahlen $\theta\pi$ gebildet sind. Es ist aber von Wichtigkeit, diese Voraussagungen der allgemeinen Theorie durch die Rechnung zu bestätigen. Zu diesem Zwecke wählen wir aus AB ein irreduzibles System T von n Zahlen ω_r; dann ergibt sich schon aus (6) und (7), daß die Norm $N(\alpha)$ als Quotient der beiden Determinanten (αT) und (T) gewiß in A enthalten ist. Wir wollen dies etwas näher ausführen. Da T eine Basis von AB bildet, so kann man

$$\alpha = x_1\omega_1 + x_2\omega_2 + \cdots + x_n\omega_n \tag{10}$$

und ebenso

$$\alpha\omega_r = x_{r,1}\omega_1 + x_{r,2}\omega_2 + \cdots + x_{r,n}\omega_n \tag{11}$$

setzen, wo die Koordinaten x_r und $x_{r,s}$ sämtlich in A enthalten sind, und zufolge (6) und (7) ist die aus den letzteren*) gebildete Determinante

$$\Sigma \pm x_{1,1}x_{2,2}\ldots x_{n,n} = N(\alpha). \tag{12}$$

Jeder Zahl α entspricht nun, wenn t eine Variable bedeutet, eine ganze Funktion n^{ten} Grades

$$f(t) = \Pi(t - \alpha\pi) = t^n + a_1t^{n-1} + \cdots + a_{n-1}t + a_n, \tag{13}$$

wo sich das Produktzeichen Π auf alle n Permutationen π bezieht. Dieselbe ist offenbar dadurch völlig bestimmt, daß für jeden in A enthaltenen Wert t

$$f(t) = N(t - \alpha) \tag{14}$$

wird; ersetzt man aber in (11) die Zahl α durch $\alpha - t$, so bleiben die Koordinaten $x_{r,s}$ ungeändert mit Ausnahme derjenigen $x_{r,r}$, welche in der Diagonale liegen und durch $x_{r,r} - t$ zu ersetzen sind, und folglich entspringt aus (12) die Gleichung

$$\begin{vmatrix} x_{1,1} - t & \ldots & x_{1,n} \\ \cdots & \cdots & \cdots \\ x_{n,1} & \ldots & x_{n,n} - t \end{vmatrix} = (-1)^n f(t), \tag{15}$$

*) Diese sind offenbar homogene lineare Funktionen der n Koordinaten x_r, und die Koeffizienten dieser Funktionen sind die Koordinaten der Produkte $\omega_r\omega_s$. Vgl. § 182.

welche identisch für jeden Wert von t gilt, weil auch die linke Seite eine ganze Funktion n^{ten} Grades von t ist; mithin sind die Koeffizienten a_r der Funktion $f(t)$ in A enthalten. Dies gilt also insbesondere von der Spur

$$S(\alpha) = x_{1,1} + x_{2,2} + \cdots + x_{n,n} = -a_1 \tag{16}$$

und zufolge (8) und (9) auch von allen Produkten $(U)(V)$ und von allen Diskriminanten ΔT, was zu beweisen war.

Ist α eine n-wertige und folglich (nach § 165) eine Zahl n^{ten} Grades in bezug auf A, so ist die zugehörige Funktion $f(t)$ irreduzibel in bezug auf A, d. h. sie kann nicht in Faktoren niedrigeren Grades zerlegt werden, deren Koeffizienten ebenfalls in A enthalten sind (§ 164); allgemein, wenn α eine q-wertige Zahl ist, so ist (nach § 165) $n = pq$, und $f(t)$ ist die p^{te} Potenz einer irreduziblen Funktion vom Grade q. Da die Funktion $f(t)$, also auch ihre Derivierte $f'(t)$ durch die Zahl α vollständig bestimmt ist, so gehört zu jeder Zahl α eine bestimmte Zahl α^*, welche durch

$$\alpha^* = f'(\alpha) = n\alpha^{n-1} + \cdots + a_{n-1} \tag{17}$$

definiert wird und ebenfalls in AB enthalten ist, und wenn π eine bestimmte Permutation in Π bedeutet, so folgt aus (13), daß

$$\alpha^*\pi = f'(\alpha\pi) = \Pi'(\alpha\pi - \alpha\pi') \tag{18}$$

ist, wo das Produktzeichen Π' sich auf alle $n - 1$ von π verschiedenen Permutationen π' bezieht, und hieraus ergibt sich

$$N(\alpha^*) = (-1)^{1/2\,n(n-1)}\,\Pi''(\alpha\pi_r - \alpha\pi_s)^2, \tag{19}$$

wo die Multiplikation Π'' auf alle Kombinationen r, s auszudehnen ist, in denen $r < s$ ist. Offenbar ist die Zahl α^* dann und nur dann von Null verschieden, wenn α eine n-wertige, also eine Zahl n^{ten} Grades ist, und folglich das aus den n Potenzen $\alpha^{n-1}, \alpha^{n-2}, \ldots, \alpha, 1$ bestehende System T_α eine Basis von AB bildet. In dieser Annahme folgt aus

$$f(\alpha) = \alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0, \tag{20}$$

daß a_r die r^{te} Koordinate der Zahl $-\alpha^n$ ist; bedeuten ferner x, y willkürliche Variable, so können wir

$$\frac{f(x) - f(y)}{x - y} = f_1(x)y^{n-1} + f_2(x)y^{n-2} + \cdots + f_n(x) \tag{21}$$

setzen, wo

$$f_r(x) = x^{r-1} + a_1x^{r-2} + \cdots + a_{r-2}x + a_{r-1},$$

und hieraus entspringt wieder ein bestimmtes System U_α von n Zahlen $\alpha_1, \alpha_2, \ldots, \alpha_n$, welche durch

(22) $\alpha_r = f_r(\alpha) = \alpha^{r-1} + a_1\alpha^{r-2} + \cdots + a_{r-2}\alpha + a_{r-1}$

definiert sind und den Bedingungen

(23) $\alpha_1 = 1; \quad \alpha_{r+1} = \alpha\alpha_r + a_r; \quad 0 = \alpha\alpha_n + a_n$

genügen. Da die aus ihren Koordinaten gebildete Determinante $= (-1)^{1/2\,n(n-1)}$ ist, so folgt aus (6):

(24) $(U_\alpha) = (-1)^{1/2\,n(n-1)}(T_\alpha).$

Wählt man ferner irgend zwei Permutationen π, π' und setzt $x = \alpha\pi$, $y = \alpha\pi'$, so ergibt sich aus (21), daß die Summe

(25) $(\alpha_1\pi)(\alpha^{n-1}\pi') + (\alpha_2\pi)(\alpha^{n-2}\pi') + \cdots + (\alpha_n\pi)(1\pi')$
$= \alpha^*\pi$ oder $= 0$

ist, je nachdem π, π' gleich oder verschieden sind; läßt man π und π' unabhängig voneinander alle n Permutationen durchlaufen, und bildet man die Determinante aus den entsprechenden n^2 Summen, so ist dieselbe bekanntlich das Produkt aus den Determinanten (U_α), (T_α), und man erhält daher

(26) $(U_\alpha)(T_\alpha) = N(\alpha^*),$

also mit Rücksicht auf (24) auch

(27) $N(\alpha^*) = (-1)^{1/2\,n(n-1)}\,\Delta\,T_\alpha;$

da nach einem sehr bekannten, schon öfter (z. B. in § 161) von uns benutzten Satze die Determinante (T_α) gleich dem Produkte aller Differenzen $\alpha\pi_r - \alpha\pi_s$ ist, wo $r < s$, so stimmt (27) völlig mit (19) überein.

Das Vorhergehende hängt nahe zusammen mit der folgenden allgemeinen Betrachtung *). Bedeutet wieder T irgendein irreduzibles System von n Zahlen ω_r, so gibt es, weil die in (9) dargestellte Diskriminante $\Delta\,T$ von Null verschieden ist, immer ein und nur ein System T' von n korrespondierenden Zahlen ω'_r, welches den n linearen Gleichungen

(28) $\omega_r = S(\omega_r\omega_1)\,\omega'_1 + S(\omega_r\omega_2)\,\omega'_2 + \cdots + S(\omega_r\omega_n)\,\omega'_n$

genügt und offenbar ebenfalls in AB enthalten ist, weil dies von allen anderen hier auftretenden Zahlen ω_r, $S(\omega_r\omega_s)$ gilt. Setzt man

*) Vgl. meine Abhandlung Über die Diskriminanten endlicher Körper (1882, Bd. 29 der Abhandlungen der Ges. d. Wissensch. zu Göttingen).

diese Ausdrücke (28) in die Gleichung (10) ein, so geht die letztere mit Rücksicht auf (1) und (3) in die Gleichung

$$(29) \qquad \alpha = S(\alpha\omega_1)\omega'_1 + S(\alpha\omega_2)\omega'_2 + \cdots + S(\alpha\omega_n)\omega'_n$$

über, in welcher umgekehrt die Gleichungen (28) als spezielle Fälle enthalten sind. Zugleich leuchtet ein, daß das System T' ebenfalls eine Basis von AB bildet, und daß die ihr entsprechenden Koordinaten einer beliebigen Zahl α die n Spuren $S(\alpha\omega_r)$ sind. Wir wollen T' die zu T komplementäre Basis oder das Komplement von T nennen, wobei wohl zu beachten ist, daß jedem Elemente ω_r der Basis T ein bestimmtes Element ω'_r der Basis T' entspricht. Setzt man nun $\alpha = \omega'_s$, so ergibt sich aus (29), daß

$$(30) \qquad S(\omega_r\omega'_s) = 1 \quad \text{oder} \quad = 0$$

ist, je nachdem r, s gleich oder verschieden sind, und aus (8) folgt daher

$$(31) \qquad (T)(T') = 1, \ \Delta T \cdot \Delta T' = 1.$$

Umgekehrt, wenn zwei Systeme T und T' von je n Zahlen ω_r und ω'_r des Körpers AB den n^2 Gleichungen (30) genügen, so folgt zunächst aus (31), daß beide Systeme Basen von AB sind; jede Zahl α in AB ist daher von der Form

$$\alpha = y_1\omega'_1 + y_2\omega'_2 + \cdots + y_n\omega'_n,$$

wo die Koeffizienten y_r in A enthalten sind; multipliziert man mit ω_r, so ergibt sich mit Rücksicht auf (1), (3) und (30), daß $y_r = S(\alpha\omega_r)$ ist; mithin gilt (29), also auch (28), und folglich ist T' das Komplement von T. Da aber die Gleichungen (30) durchaus symmetrisch in bezug auf die beiden Systeme T und T' sind, so ist zugleich T das Komplement von T'. Aus denselben Gleichungen (30) und aus der Bedeutung einer Spur ergibt sich ferner nach bekannten Sätzen, daß $\omega'_r\pi_s \cdot (T)$ der Koeffizient des Elementes $\omega_r\pi_s$ in der Determinante (T) ist; zugleich folgt, daß auch die Summe

$$(32) \qquad (\omega_1\pi)(\omega'_1\pi') + \cdots + (\omega_n\pi)(\omega'_n\pi') = 1 \quad \text{oder} \quad = 0$$

ist, je nachdem die Permutationen π, π' gleich oder verschieden sind, und umgekehrt folgt (30) aus (32). Nimmt man für π und π' die identische Permutation von AB, so ergibt sich die Beziehung

$$(33) \qquad \omega_1\omega'_1 + \omega_2\omega'_2 + \cdots + \omega_n\omega'_n = 1,$$

welche man auch auf anderem Wege aus (29) und (16) ableiten kann.

Vergleicht man die Gleichungen (25) mit (32), so ergibt sich, daß das dort mit U_α bezeichnete System $= \alpha^* T'_\alpha$ ist, wo T'_α das Komplement des dortigen Systems T_α bedeutet; hieraus folgt zugleich mit Rücksicht auf (30), daß

$$S\left(\frac{\alpha_r \alpha^{n-s}}{\alpha^*}\right) = 1 \quad \text{oder} \quad = 0 \tag{34}$$

ist, je nachdem r, s gleich oder verschieden sind; das letztere ergibt sich aber auch unmittelbar aus dem bekannten Satze über die Zerlegung echt gebrochener Funktionen mit dem Nenner $f(t)$ in Partialbrüche.

Durch Vertauschung von T mit T' ergibt sich aus (29), daß jede Zahl α auch in der Form

$$\alpha = S(\alpha\omega'_1)\,\omega_1 + S(\alpha\omega'_2)\,\omega_2 + \cdots + S(\alpha\omega'_n)\,\omega_n \tag{35}$$

darstellbar, also $S(\alpha\omega'_s)$ die s^{te} Koordinate von α in bezug auf die Basis T ist. Verstehen wir jetzt unter $\alpha_1, \alpha_2, \ldots, \alpha_n$ nicht mehr die in (22) definierten Zahlen, sondern die in (5) dargestellten Elemente einer beliebigen Basis U, so ist die Zahl $a_{r,s} = S(\alpha_r\omega'_s)$ die s^{te} Koordinate von α_r in bezug auf die Basis T und folglich zugleich die r^{te} Koordinate von ω'_s in bezug auf die Basis U'; hieraus ergibt sich, daß gleichzeitig mit den n Gleichungen (5) auch die n Gleichungen

$$\omega'_s = a_{1,s}\,\alpha'_1 + a_{2,s}\,\alpha'_2 + \cdots + a_{n,s}\,\alpha'_n \tag{36}$$

gelten. —

Zum Schlusse der in den §§ 160 bis 167 enthaltenen Darstellung algebraischer Grundlagen bemerken wir, daß in dem weiteren Verlaufe des vorliegenden Werkes der Körper, auf welchen sich die Begriffe der reduziblen und irreduziblen Systeme, der algebraischen Zahlen, der endlichen Körper usw. beziehen, ausschließlich der Körper R der rationalen Zahlen sein wird. Ein System von m Zahlen $\omega_1, \omega_2, \ldots, \omega_m$ heißt daher reduzibel, wenn es m rationale Zahlen $a_1, a_2, \ldots, a_m$ gibt, die der Bedingung $a_1\omega_1 + a_2\omega_2 + \cdots + a_m\omega_m = 0$ genügen und nicht alle verschwinden; im entgegengesetzten Falle heißt das System schlechthin irreduzibel. Eine Zahl θ heißt algebraisch*) und vom Grade n, wenn die n Potenzen $1, \theta, \theta^2, \ldots, \theta^{n-1}$

*) Aus dem Satze X in § 164 und dessen unmittelbaren Folgerungen geht hervor, daß der Inbegriff $\mathfrak{A}$ aller dieser algebraischen Zahlen ein (nicht endlicher) Körper, und daß jede in bezug auf $\mathfrak{A}$ algebraische Zahl notwendig in $\mathfrak{A}$ selbst enthalten ist. Daß aber mit $\mathfrak{A}$ das Reich aller Zahlen noch nicht erschöpft ist,

ein irreduzibles System bilden, das durch Hinzufügung von θ^n reduzibel wird. Aus jeder solchen Zahl θ entspringt ein endlicher Körper $R(\theta)$, und umgekehrt ist jeder endliche Körper n^{ten} Grades von dieser Form; er besitzt, weil es nur eine einzige Permutation von R gibt, n und nur n verschiedene Permutationen, von denen eine die identische Permutation ist.

§ 168.

Wir wenden uns jetzt zu einer anderen allgemeinen Untersuchung, welche eine wichtige Grundlage unserer Zahlentheorie bildet und auch auf andere Teile der Mathematik sich mit Nutzen anwenden läßt. Sie beruht auf dem folgenden einfachen Begriffe:

Ein System $\mathfrak{a}$ von beliebigen reellen oder komplexen Zahlen soll ein Modul heißen, wenn dieselben sich durch Subtraktion reproduzieren, d. h. wenn die Differenzen von je zwei solchen Zahlen demselben System $\mathfrak{a}$ angehören.

Zufolge dieser Erklärung ist jeder Zahlenkörper (§ 160) gewiß auch ein Modul; aber wir wollen von vornherein bemerken, daß in der folgenden allgemeinen Theorie auf diesen Umstand nicht das geringste Gewicht zu legen ist, weil diejenigen besonderen Moduln, welche wir später (§ 172) ausschließlich zu betrachten haben, niemals zugleich Körper sind.

---

daß es also noch andere, sogenannte transzendente Zahlen gibt, ist meines Wissens zuerst von Liouville bewiesen (Sur des classes très-étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationnelles algébriques. Journal de Math. t. XVI, 1851). Einen anderen Beweis findet man in der Abhandlung von G. Cantor: Über eine Eigenschaft des Inbegriffes aller reellen algebraischen Zahlen (Crelles Journal, Bd. 77, 1874). Dann hat Ch. Hermite (in der Abhandlung Sur la fonction exponentielle, 1874) zuerst den strengen Beweis geliefert, daß die Basis e des natürlichen Logarithmensystems eine transzendente Zahl ist, und durch die hieran sich anschließenden Untersuchungen von Lindemann (Über die Zahl π; Math. Annalen, Bd. 20) und Weierstraß (Sitzungsberichte der Berliner Ak. 1885) ist endlich der allgemeinere Satz bewiesen, daß, wenn α irgendwelche verschiedene Zahlen in $\mathfrak{A}$ durchläuft, die entsprechenden Potenzen e^{α} immer ein nach $\mathfrak{A}$ irreduzibles System bilden, woraus als spezieller Fall die Transzendenz der Ludolphschen Zahl π, also auch die vorher noch nicht erwiesene Unmöglichkeit der Quadratur des Zirkels hervorgeht. Vgl. auch Hurwitz: Über arithmetische Eigenschaften gewisser transzendenter Funktionen (Math. Annalen, Bd. 22 und 32), ferner die neuesten, sehr einfachen Beweise für die Transzendenz der Zahlen e und π von Hilbert und Hurwitz (Nachr. v. d. Göttinger Ges. d. W., 1893).

In jedem Modul $\mathfrak{a}$ ist die Zahl Null enthalten; denn wenn α irgendeine Zahl in $\mathfrak{a}$ bedeutet, so muß auch die Differenz $\alpha - \alpha$ in $\mathfrak{a}$ enthalten sein. Zugleich leuchtet ein, daß die Zahl Null für sich allein schon einen Modul, den Modul 0, bildet.

Hieraus folgt weiter, daß mit α auch stets die entgegengesetzte Zahl $-\alpha = 0 - \alpha$ in $\mathfrak{a}$ enthalten ist. Sind ferner α_1, α_2 und folglich auch $-\alpha_2$ Zahlen in $\mathfrak{a}$, so gilt dasselbe von der Differenz $\alpha_1 - (-\alpha_2)$, d. h. von der Summe $\alpha_1 + \alpha_2$, und ebenso von jeder aus mehreren Zahlen des Moduls $\mathfrak{a}$ gebildeten Summe. Die Zahlen eines Moduls reproduzieren sich daher nicht bloß durch Subtraktion, sondern auch durch Addition*), und folglich besteht jeder von 0 verschiedene Modul immer aus unendlich vielen verschiedenen Zahlen; denn wenn α in $\mathfrak{a}$ enthalten ist, so müssen auch alle Zahlen von der Form $x\alpha$ in $\mathfrak{a}$ enthalten sein, wo x alle ganzen rationalen Zahlen durchläuft.

Hieran schließt sich die Bemerkung, daß jedes endliche oder unendliche System T von Zahlen α, falls es nicht selbst schon ein Modul ist, durch Hinzufügung der Zahlen $-\alpha$ und aller Summen von mehreren Zahlen $\pm\alpha$ offenbar zu einem Modul $\mathfrak{a}$ ergänzt wird; diesen durch das System T vollständig bestimmten Modul $\mathfrak{a}$ kann man zweckmäßig durch das Symbol $[T]$ bezeichnen, und wir wollen T eine Basis des Moduls $\mathfrak{a}$ nennen. Zugleich leuchtet ein, daß jeder Modul $\mathfrak{b}$, welcher alle Zahlen α des Systems T enthält, auch alle Zahlen des Moduls $[T]$ enthalten muß.

Ist T ein endliches System, welches aus den n Zahlen α_1, α_2, $\ldots$, α_n besteht, so bezeichnen wir den zugehörigen Modul $\mathfrak{a}$ durch das Symbol

$$[\alpha_1, \alpha_2, \ldots, \alpha_n];$$

derselbe besteht offenbar aus allen Zahlen von der Form

$$x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n,$$

wo x_1, x_2, $\ldots$, x_n willkürliche ganze rationale Zahlen bedeuten. Jeden solchen Modul $\mathfrak{a}$ wollen wir einen endlichen Modul nennen; die n Zahlen α_1, α_2, $\ldots$, α_n heißen die Elemente oder Glieder seiner Basis, und $\mathfrak{a}$ selbst heißt danach ein n-gliedriger Modul.

*) In § 161 der zweiten Auflage dieses Werkes (1871) [wiedergegeben unter XLVII], wo der Begriff des Moduls zuerst in die Zahlentheorie eingeführt ist, und ebenso in § 165 der dritten Auflage (1879) war diese Eigenschaft in die Erklärung selbst aufgenommen.

Offenbar ist es stets erlaubt, diese Basis in der Weise abzuändern, daß man zu ihren Gliedern noch irgendwelche in dem Modul $\mathfrak{a}$ enthaltene Zahlen als neue Glieder hinzufügt; derselbe Modul $\mathfrak{a}$ ist daher auch ein $(n+1)$-gliedriger Modul*). Der eingliedrige Modul [1], den wir immer durch $\mathfrak{z}$ bezeichnen wollen, ist nichts anderes als das System aller ganzen rationalen Zahlen; ebenso ist [2] oder auch [2, 6, 10] das System aller geraden Zahlen, und der zweigliedrige Modul [1, i] ist das System aller ganzen komplexen Zahlen von Gauß (§ 159).

§ 169.

Sehr häufig wird, wie z. B. in der vorstehenden Betrachtung, der Fall auftreten, daß alle Zahlen eines Moduls $\mathfrak{m}$ auch in einem Modul $\mathfrak{b}$ enthalten sind; dann heißt $\mathfrak{m}$ teilbar durch $\mathfrak{b}$, oder wir sagen, $\mathfrak{m}$ sei ein Vielfaches oder Multiplum von $\mathfrak{b}$, $\mathfrak{b}$ sei ein Teiler oder Divisor von $\mathfrak{m}$, oder $\mathfrak{b}$ gehe in $\mathfrak{m}$ auf, und wir bezeichnen dies symbolisch**) auf doppelte Weise durch

$$\mathfrak{m} > \mathfrak{b} \quad \text{oder} \quad \mathfrak{b} < \mathfrak{m}.$$

Diese Ausdrucks- und Bezeichnungsweise mag auf den ersten Blick Anstoß erregen, weil das Vielfache $\mathfrak{m}$ in Wahrheit einen Teil des Teilers $\mathfrak{b}$ bildet, doch wird dieselbe sich in der Folge hinreichend rechtfertigen durch die Analogie mit der Teilbarkeit der Zahlen***); so ist z. B. [4] ein Vielfaches von [2], weil alle durch 4 teilbaren ganzen rationalen Zahlen auch gerade Zahlen sind. Allgemein bemerken wir, daß der Modul 0 ein gemeinschaftliches Vielfaches, und das System aller Zahlen ein gemeinsamer Teiler aller Moduln ist. Der im vorigen Paragraphen betrachtete Modul $[T]$ ist teilbar durch jeden Modul, welcher alle Zahlen der Basis T enthält. Ist jeder der Moduln $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \ldots$ durch den zunächst folgenden teilbar, so ist jeder auch ein Multiplum von allen folgenden. Jeder Modul ist durch sich selbst teilbar, und wenn jeder der beiden Moduln $\mathfrak{m}$, $\mathfrak{b}$ durch

*) Erst später (§ 172) kann es zweckmäßig erscheinen, diese Ausdrucksweise abzuändern.

**) Diese und die später folgenden Zeichen $\mathfrak{a}+\mathfrak{b}$, $\mathfrak{a}-\mathfrak{b}$ usw. habe ich schon benutzt in der Festschrift: Über die Anzahl der Ideal-Klassen in den verschiedenen Ordnungen eines endlichen Körpers (Braunschweig 1877).

***) Selbst der Umstand, daß bei den Körpern, die doch auch Moduln sind, die entgegengesetzte Ausdrucksweise gebraucht ist, kann hier nicht ins Gewicht fallen, weil bei einiger Aufmerksamkeit eine Verwechslung nicht möglich ist.

den anderen teilbar, also $\mathfrak{m} > \mathfrak{b}$ und $\mathfrak{b} > \mathfrak{m}$ ist, so folgt $\mathfrak{m} = \mathfrak{b}$, d. h. $\mathfrak{m}$ und $\mathfrak{b}$ sind nur verschiedene Zeichen für einen und denselben Modul. Wenn dagegen $\mathfrak{m}$ teilbar durch $\mathfrak{b}$, aber verschieden von $\mathfrak{b}$ ist, so soll $\mathfrak{b}$ ein echter Teiler von $\mathfrak{m}$, und $\mathfrak{m}$ ein echtes Vielfaches von $\mathfrak{b}$ heißen; es gibt dann in $\mathfrak{b}$ mindestens eine und folglich, wie leicht zu sehen, auch unendlich viele Zahlen, die nicht in $\mathfrak{m}$ enthalten sind.

Sind nun $\mathfrak{a}$, $\mathfrak{b}$ irgend zwei Moduln, und bedeutet α jede Zahl in $\mathfrak{a}$, ebenso β jede Zahl in $\mathfrak{b}$, so bezeichnen wir mit

$$\mathfrak{a} + \mathfrak{b}$$

das System aller in der Form $\alpha + \beta$ darstellbaren Zahlen; dasselbe ist ebenfalls ein Modul, weil die Differenz von je zwei solchen Zahlen $\alpha_1 + \beta_1$, $\alpha_2 + \beta_2$, nämlich $(\alpha_1 - \alpha_2) + (\beta_1 - \beta_2)$ wieder in $\mathfrak{a} + \mathfrak{b}$ enthalten ist. Dieser Modul, den wir kurz die Summe der beiden Moduln $\mathfrak{a}$, $\mathfrak{b}$ nennen, ist offenbar ein gemeinsamer Teiler von $\mathfrak{a}$, $\mathfrak{b}$, weil er alle Zahlen $\alpha + 0$ des Moduls $\mathfrak{a}$ und alle Zahlen $0 + \beta$ des Moduls $\mathfrak{b}$ enthält. Ist ferner der Modul $\mathfrak{d}$ irgendein gemeinsamer Teiler von $\mathfrak{a}$, $\mathfrak{b}$, also $\mathfrak{d} < \mathfrak{a}$ und $\mathfrak{d} < \mathfrak{b}$, so sind alle Zahlen α, β, also auch alle Summen $\alpha + \beta$ in $\mathfrak{d}$ enthalten, mithin ist $\mathfrak{d} < \mathfrak{a} + \mathfrak{b}$. Aus diesem Grunde nennen wir der Analogie wegen die Summe $\mathfrak{a} + \mathfrak{b}$ auch den größten gemeinsamen Teiler von $\mathfrak{a}$, $\mathfrak{b}$, obgleich er unter allen Moduln $\mathfrak{d}$ den kleinsten Zahleninhalt besitzt.

Aus dieser Erklärung folgen unmittelbar die für beliebige Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, ... geltenden Sätze:

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

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

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

und wendet man auf (2) und (3) die in § 2 vorgetragene Schlußweise an, so ergibt sich die Bedeutung der in beliebiger Ordnung gebildeten Summe

(4) $$\Sigma\, \mathfrak{a} = \mathfrak{a}_1 + \mathfrak{a}_2 + \cdots + \mathfrak{a}_n$$

von beliebigen Moduln $\mathfrak{a}$, deren Anzahl endlich ist; diese Summe ist der größte gemeinsame Teiler aller n Moduln $\mathfrak{a}$, d. h. sie geht in jedem Modul $\mathfrak{a}$ auf und ist zugleich teilbar durch jeden gemeinsamen Teiler aller $\mathfrak{a}$. Offenbar ist z. B.

(5) $$[\alpha_1, \alpha_2, \ldots, \alpha_n] = [\alpha_1] + [\alpha_2] + \cdots + [\alpha_n],$$

und die Summe von mehreren endlichen Moduln ist wieder ein endlicher Modul. Außerdem leuchtet ein, daß die Teilbarkeit eines Moduls $\mathfrak{m}$ durch einen Modul $\mathfrak{b}$ vollständig durch

$$\mathfrak{m} + \mathfrak{b} = \mathfrak{b} \tag{6}$$

ausgedrückt wird, und daß aus $\mathfrak{a} > \mathfrak{a}'$ und $\mathfrak{b} > \mathfrak{b}'$ auch $\mathfrak{a} + \mathfrak{b} > \mathfrak{a}' + \mathfrak{b}'$ folgt.

Der Begriff der Summe $\Sigma\mathfrak{a}$ oder des größten gemeinsamen Teilers von beliebigen Moduln $\mathfrak{a}$ läßt sich aber von vornherein auch so erklären, daß er einen vollständig bestimmten Sinn, und zwar die oben ausgesprochene Bedeutung behält, mag die Anzahl der Moduln $\mathfrak{a}$ endlich oder unendlich groß sein, welcher letztere Fall auch bei unseren Untersuchungen gelegentlich auftreten wird. Hierzu führt am kürzesten die im vorigen Paragraphen betrachtete Bildung des Moduls $[T]$ aus einem gegebenen System T; in der Tat, nimmt man in T jede und nur jede solche Zahl α auf, welche in wenigstens einem der Moduln $\mathfrak{a}$ enthalten ist*), so besteht der zugehörige Modul $[T]$ aus diesen Zahlen α und allen Summen von mehreren Zahlen α, und es leuchtet ein, daß dieser Modul $[T]$, den wir nun auch durch $\Sigma\mathfrak{a}$ bezeichnen, im obigen Sinne auch der größte gemeinsame Teiler aller Moduln $\mathfrak{a}$ ist.

Ein besonderer Fall, welcher uns später (§§ 172, 173) wirklich begegnen wird, ist der, wo die Moduln $\mathfrak{a}$ eine einfach unendliche Reihe $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3 \ldots$ von der Art bilden, daß jeder Modul $\mathfrak{a}_n$ durch den nächstfolgenden $\mathfrak{a}_{n+1}$ und also durch alle folgenden teilbar ist. Dann ist offenbar ihr größter gemeinsamer Teiler $[T] = T$; bedeuten nämlich ϱ, σ irgend zwei Zahlen in T, so gehört ϱ einem Modul $\mathfrak{a}_r$, ebenso σ einem Modul $\mathfrak{a}_s$ an; ist nun $r \leqq s$, so sind beide Zahlen ϱ, σ in $\mathfrak{a}_s$ enthalten, und da $\mathfrak{a}_s$ ein Modul ist, so ist die Differenz $\varrho - \sigma$ in $\mathfrak{a}_s$ und folglich auch in T enthalten, mithin ist T ein Modul und folglich $= [T]$, wie behauptet war. Offenbar kann der größte gemeinsame Teiler $[T]$ oder $\Sigma\mathfrak{a}$ in diesem Falle zweckmäßig mit $\mathfrak{a}_\infty$ bezeichnet werden.

Ist z. B. $\mathfrak{a}_n = [2^{-n}]$, so besteht $\mathfrak{a}_n$ aus allen ganzen und denjenigen gebrochenen rationalen Zahlen, welche, auf die kleinste Benennung gebracht, zum Nenner eine Potenz von 2 haben, deren

*) Nach der Ausdrucksweise der in § 161 mehrmals zitierten Schrift (§ 1) ist T das aus den Systemen $\mathfrak{a}$ zusammengesetzte System.

Exponent $\leqq n$ ist; offenbar ist $\mathfrak{a}_{n+1}$ ein echter Teiler von $\mathfrak{a}_n$; der größte gemeinsame Teiler $\mathfrak{a}_\infty$ aller dieser Moduln $\mathfrak{a}_n$ ist das System aller derjenigen rationalen Zahlen, deren Nenner irgendeine Potenz von 2 ist; alle Moduln $\mathfrak{a}_n$ sind endliche, eingliedrige Moduln, aber $\mathfrak{a}_\infty$ ist kein endlicher Modul. —

Auf der Erklärung der Teilbarkeit der Moduln, aus welcher der Begriff des größten gemeinsamen Teilers von beliebigen Moduln $\mathfrak{a}$ hervorgegangen ist, beruht ebenso der Begriff ihres kleinsten gemeinsamen Vielfachen; wir verstehen darunter das System $\mathfrak{m}$ aller derjenigen Zahlen μ, welche (wie z. B. die Zahl 0) allen Moduln $\mathfrak{a}$ gemeinsam angehören, deren jede also in jedem dieser Moduln $\mathfrak{a}$ enthalten ist*). Da, wenn μ_1, μ_2 zwei solche Zahlen in $\mathfrak{m}$ sind, auch ihre Differenz $\mu_1 - \mu_2$ in jedem der Moduln $\mathfrak{a}$ und folglich auch in $\mathfrak{m}$ enthalten ist, so ist $\mathfrak{m}$ ein Modul, und zwar ein gemeinsames Vielfaches dieser Moduln $\mathfrak{a}$. Da ferner jedes gemeinsame Vielfache $\mathfrak{m}'$ der Moduln $\mathfrak{a}$ nur aus solchen Zahlen besteht, welche in jedem dieser Moduln $\mathfrak{a}$ und folglich in $\mathfrak{m}$ enthalten sind, so ist $\mathfrak{m}' > \mathfrak{m}$; aus diesem Grunde haben wir der Analogie wegen $\mathfrak{m}$ das kleinste gemeinsame Vielfache der Moduln $\mathfrak{a}$ genannt, obgleich $\mathfrak{m}$ unter allen Moduln $\mathfrak{m}'$ den größten Zahleninhalt besitzt.

Bezeichnet man das kleinste gemeinsame Vielfache zweier Moduln $\mathfrak{a}$, $\mathfrak{b}$ durch das Symbol

$$\mathfrak{a} - \mathfrak{b},$$

so ergeben sich folgende Sätze, deren Beweise wir wieder übergehen dürfen:

(1′) $\qquad \mathfrak{a} - \mathfrak{a} = \mathfrak{a}$

(2′) $\qquad \mathfrak{a} - \mathfrak{b} = \mathfrak{b} - \mathfrak{a}$

(3′) $\qquad (\mathfrak{a} - \mathfrak{b}) - \mathfrak{c} = \mathfrak{a} - (\mathfrak{b} - \mathfrak{c}).$

Zugleich leuchtet ein, daß die Teilbarkeit eines Moduls $\mathfrak{m}$ durch einen Modul $\mathfrak{b}$ vollständig durch

(6′) $\qquad \mathfrak{m} - \mathfrak{b} = \mathfrak{m}$

ausgedrückt wird, und daß aus $\mathfrak{a} > \mathfrak{a}'$ und $\mathfrak{b} > \mathfrak{b}'$ auch $\mathfrak{a} - \mathfrak{b} > \mathfrak{a}' - \mathfrak{b}'$ folgt.

Zwischen den Begriffen des größten gemeinsamen Teilers und des kleinsten gemeinsamen Vielfachen beliebiger Moduln besteht ein

*) Nach der Ausdrucksweise der eben wieder zitierten Schrift (§ 1) ist $\mathfrak{m}$ die Gemeinheit der Systeme $\mathfrak{a}$.

eigentümlicher Dualismus, dessen letzter Grund schwer zu erkennen sein mag. Wir führen hier nur folgenden besonders charakteristischen Satz an:

Ist $\mathfrak{m}$ teilbar durch $\mathfrak{b}$, und $\mathfrak{a}$ ein beliebiger Modul, so ist*)

$$(7) \qquad \mathfrak{m} + (\mathfrak{a} - \mathfrak{b}) = (\mathfrak{m} + \mathfrak{a}) - \mathfrak{b}.$$

Um dies zu beweisen, bezeichnen wir den Modul linker Hand mit $\mathfrak{p}$, den rechter Hand mit $\mathfrak{q}$, und wir haben zu zeigen, daß sie gegenseitig durch einander teilbar sind. Die Teilbarkeit von $\mathfrak{p}$ durch $\mathfrak{q}$ ergibt sich ohne Mühe aus den früheren Sätzen, weil jeder der beiden Moduln $\mathfrak{m}$ und $\mathfrak{a} - \mathfrak{b}$ teilbar durch jeden der beiden Moduln $\mathfrak{m} + \mathfrak{a}$ und $\mathfrak{b}$, und folglich der größte gemeinsame Divisor $\mathfrak{p}$ der beiden ersteren auch teilbar durch das kleinste gemeinsame Vielfache $\mathfrak{q}$ der beiden letzteren ist. Um aber die Teilbarkeit von $\mathfrak{q}$ durch $\mathfrak{p}$ darzutun, genügen die früheren Sätze durchaus nicht, sondern es ist erforderlich, noch einmal auf den Begriff des Moduls zurückzugehen und die in $\mathfrak{q}$ enthaltenen Zahlen zu betrachten; da jede solche Zahl gleichzeitig in $\mathfrak{m} + \mathfrak{a}$ und $\mathfrak{b}$ enthalten ist, so ist sie von der Form $\mu + \alpha = \delta$, wo μ, α, δ bzw. in $\mathfrak{m}$, $\mathfrak{a}$, $\mathfrak{b}$ enthalten sind; da nun $\mathfrak{m} > \mathfrak{b}$, also μ auch in $\mathfrak{b}$ enthalten ist, so gilt dasselbe von der Zahl $\alpha = \delta - \mu$, welche folglich auch in $\mathfrak{a} - \mathfrak{b}$ enthalten ist, und hieraus folgt, daß die Zahl $\mu + \alpha$ wirklich in $\mathfrak{p}$ enthalten ist, was zu beweisen war.

Bedeuten nun $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ willkürliche Moduln, und setzt man in dem eben bewiesenen Satze einmal $\mathfrak{m} = \mathfrak{b}$, $\mathfrak{b} = \mathfrak{b} + \mathfrak{c}$, hierauf $\mathfrak{m} = \mathfrak{b} - \mathfrak{c}$, $\mathfrak{b} = \mathfrak{b}$, so ist die Bedingung $\mathfrak{m} > \mathfrak{b}$ erfüllt, und man erhält die beiden Sätze

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

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

in welchen sich der erwähnte Dualismus recht auffällig ausspricht**). Aus jedem dieser beiden Sätze folgt rückwärts der Satz (7), aus dem ersten, wenn man $\mathfrak{b} = \mathfrak{m}$, $\mathfrak{c} = \mathfrak{b}$, aus dem zweiten, wenn man $\mathfrak{b} = \mathfrak{b}$, $\mathfrak{c} = \mathfrak{m}$ setzt und wieder $\mathfrak{m} > \mathfrak{b}$ voraussetzt. Der Satz (7) entspricht dualistisch sich selbst.

---

*) Daß umgekehrt, wenn drei Moduln $\mathfrak{m}$, $\mathfrak{b}$, $\mathfrak{a}$ die Gleichung (7) erfüllen, $\mathfrak{m}$ durch $\mathfrak{b}$ teilbar ist, leuchtet unmittelbar ein.

**) Leitet man aus drei beliebigen Moduln neue Moduln ab, indem man immer wieder die gemeinsamen größten Teiler und kleinsten Vielfachen bildet, so gelangt man zu einer endlichen Modulgruppe, welche im allgemeinen aus 28 verschiedenen Moduln besteht. Die merkwürdigen Gesetze jeder Gruppe, welche mit je zwei

§ 170.

Während die eben betrachteten Modulbildungen auf dem Begriffe der Teilbarkeit beruhten, gehen wir jetzt zu der hiervon durchaus unabhängigen Multiplikation der Moduln über. Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei beliebige Moduln, und bedeutet α jede Zahl in $\mathfrak{a}$, ebenso β jede Zahl in $\mathfrak{b}$, so verstehen wir unter dem Produkte $\mathfrak{a}\mathfrak{b}$ der Faktoren $\mathfrak{a}, \mathfrak{b}$ den Inbegriff aller Zahlen μ, welche als ein Produkt $\alpha\beta$ oder als Summe von mehreren solchen Produkten $\alpha\beta$ darstellbar sind. Da auch jede Zahl $-\alpha$ in $\mathfrak{a}$ enthalten ist, so leuchtet ein, daß jede Differenz von zwei Zahlen μ ebenfalls eine solche Zahl μ, daß also das Produkt $\mathfrak{a}\mathfrak{b}$ wieder ein Modul ist; aber man darf, wie kaum bemerkt zu werden braucht, das Produkt $\mathfrak{a}\mathfrak{b}$ nicht mit einem Vielfachen von $\mathfrak{a}$, $\mathfrak{b}$ verwechseln.

Aus dieser Erklärung ergibt sich ohne weiteres, daß

$$(1) \qquad \mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$$

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

ist; wir bezeichnen dieses letztere Produkt kurz mit $\mathfrak{a}\mathfrak{b}\mathfrak{c}$, und aus der schon oft angewendeten Schlußweise (§ 2) geht hervor, daß das mit $\mathfrak{a}_1\mathfrak{a}_2\ldots\mathfrak{a}_m$ zu bezeichnende Produkt aus m beliebigen Moduln $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_m$ eine vollständig bestimmte, von der Anordnung der aufeinander folgenden Multiplikationen gänzlich unabhängige Bedeutung hat. Man könnte dieses Produkt auch unmittelbar als den Modul $[T]$ erklären (§ 168), dessen Basis T aus allen Produkten $\alpha_1\alpha_2\ldots\alpha_m$ besteht, wo $\alpha_1, \alpha_2, \ldots, \alpha_m$ resp. beliebige Zahlen der Moduln $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_m$ bedeuten. Sind alle diese m Moduln miteinander identisch $= \mathfrak{a}$, so bezeichnen wir ihr Produkt mit $\mathfrak{a}^m$, und nennen es die m^{te} Potenz von $\mathfrak{a}$; m heißt der Exponent derselben, und wir dehnen diese Erklärung auch auf den Fall $m = 1$ aus, indem wir $\mathfrak{a}^1 = \mathfrak{a}$ setzen; dann gelten allgemein die Sätze

$$(3) \qquad \mathfrak{a}^r\mathfrak{a}^s = \mathfrak{a}^{r+s},\ (\mathfrak{a}^r)^s = \mathfrak{a}^{rs},\ (\mathfrak{a}\mathfrak{b})^r = \mathfrak{a}^r\mathfrak{b}^r.$$

Moduln $\mathfrak{a}$, $\mathfrak{b}$ zugleich die Moduln $\mathfrak{a} \pm \mathfrak{b}$ enthält, sollen an einem anderen Orte [vgl. XXX] besprochen werden; hier mag nur der folgende, oft anzuwendende Satz erwähnt werden: sind $\mathfrak{a}$, $\mathfrak{b}$ zwei beliebige Moduln, so findet zwischen der Gruppe aller Moduln $\mathfrak{a}'$, welche Teiler von $\mathfrak{a}$, und zugleich Vielfache von $\mathfrak{a} + \mathfrak{b}$ sind, und der Gruppe aller Moduln $\mathfrak{b}_1$, welche Vielfache von $\mathfrak{b}$ und zugleich Teiler von $\mathfrak{a} - \mathfrak{b}$ sind, eine gegenseitige eindeutige Korrespondenz statt, welche durch jede der beiden, wechselseitig auseinander folgenden Beziehungen $\mathfrak{b}_1 = \mathfrak{b} - \mathfrak{a}'$, $\mathfrak{a}' = \mathfrak{a} + \mathfrak{b}_1$ ausgedrückt wird.

Wir bemerken zunächst, daß ein Produkt aus zwei oder mehreren Moduln dann und nur dann $= 0$ ist, wenn unter den Faktoren sich auch der Modul Null befindet. Sodann leuchtet ein, daß, wenn $\mathfrak{z}$ wieder das System [1] aller ganzen rationalen Zahlen bedeutet, immer

$$\mathfrak{a}\,\mathfrak{z} = \mathfrak{a} \tag{4}$$

ist; und zwar ist $\mathfrak{z}$ auch der einzige Modul $\mathfrak{b}$, welcher als Faktor jeden Modul $\mathfrak{a}$ ungeändert läßt, weil $\mathfrak{b}\,\mathfrak{z} = \mathfrak{b} = \mathfrak{z}$ sein muß.

Sehr häufig wird der Fall auftreten, wo der eine Faktor $\mathfrak{b}$ eines Produktes $\mathfrak{a}\,\mathfrak{b}$ ein eingliedriger Modul $[\eta]$ ist; dann setzen wir zur Abkürzung das Produkt

$$\mathfrak{a}[\eta] = \mathfrak{a}\,\eta = \eta\,\mathfrak{a}; \tag{5}$$

dasselbe besteht offenbar aus allen Produkten $\alpha\,\eta$, wo α alle Zahlen in $\mathfrak{a}$ durchläuft, und insbesondere ist stets

$$[\eta] = \mathfrak{z}\,\eta. \tag{6}$$

Ferner ergibt sich, daß das Produkt $(\mathfrak{a}\,\eta)\,\eta_1 = (\mathfrak{a}\,\eta_1)\,\eta = \mathfrak{a}\,(\eta\,\eta_1)$ ist und deshalb kurz durch $\mathfrak{a}\,\eta\,\eta_1$ bezeichnet werden darf.

Sodann leuchtet ein, daß ein Produkt aus zwei oder mehreren endlichen Moduln (§ 168) wieder ein endlicher Modul ist; bilden z. B. die m Zahlen α_r eine Basis von $\mathfrak{a}$, und die n Zahlen β_s eine Basis von $\mathfrak{b}$, so bilden die $m\,n$ Produkte $\alpha_r\,\beta_s$ eine Basis des Produktes $\mathfrak{a}\,\mathfrak{b}$. Insbesondere ist

$$\eta\,[\alpha_1, \alpha_2, \ldots, \alpha_m] = [\eta\,\alpha_1, \eta\,\alpha_2, \ldots, \eta\,\alpha_m]. \tag{7}$$

Nach diesen, allein auf die Multiplikation der Moduln bezüglichen Bemerkungen lassen wir zunächst einige Sätze folgen, in welchen es sich um eine Verbindung mit dem Begriffe der Teilbarkeit handelt:

I. Ist $\mathfrak{a} > \mathfrak{a}'$, so ist auch $\mathfrak{a}\,\mathfrak{b} > \mathfrak{a}'\,\mathfrak{b}$, und wenn außerdem $\mathfrak{b} > \mathfrak{b}'$ ist, so ist $\mathfrak{a}\,\mathfrak{b} > \mathfrak{a}'\,\mathfrak{b}'$.

Denn weil jede Zahl α des Moduls $\mathfrak{a}$ auch in $\mathfrak{a}'$, und jede Zahl β des Moduls $\mathfrak{b}$ auch in $\mathfrak{b}'$ enthalten ist, so ist jedes Produkt $\alpha\,\beta$ und folglich auch jede Summe solcher Produkte $\alpha\,\beta$ zugleich in $\mathfrak{a}'\,\mathfrak{b}'$ enthalten, was zu beweisen war.

Mit Rücksicht auf (4), oder auch unmittelbar aus den Begriffen selbst, ergibt sich der besondere Satz:

II. Ist die Zahl 1 in dem Modul $\mathfrak{o}$ enthalten, also $\mathfrak{z} > \mathfrak{o}$, so ist allgemein $\mathfrak{a} > \mathfrak{a}\,\mathfrak{o}$.

Wir wollen noch bemerken, daß umgekehrt aus der Teilbarkeit von $\mathfrak{a}\,\mathfrak{b}$ durch $\mathfrak{a}'\mathfrak{b}$ nicht allgemein die Teilbarkeit von $\mathfrak{a}$ durch $\mathfrak{a}'$ folgt*); doch ist dies offenbar der Fall, wenn $\mathfrak{b}$ ein von Null verschiedener eingliedriger Modul $[\eta]$ ist, d. h. es besteht der Satz:

III. Ist η eine von Null verschiedene Zahl, und $\mathfrak{a}\,\eta > \mathfrak{a}'\,\eta$, so ist $\mathfrak{a} > \mathfrak{a}'$; und aus $\mathfrak{a}\,\eta = \mathfrak{a}'\,\eta$ folgt $\mathfrak{a} = \mathfrak{a}'$.

Von der größten Wichtigkeit ist aber der folgende Satz:

IV. Sind $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ drei beliebige Moduln, so ist immer

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

Bezeichnen wir den Modul linker Hand mit $\mathfrak{p}$, den rechter Hand mit $\mathfrak{q}$, so haben wir zu zeigen, daß $\mathfrak{p} > \mathfrak{q}$, und $\mathfrak{q} > \mathfrak{p}$ ist. Das letztere folgt ohne weiteres aus dem Satze I; da nämlich $\mathfrak{a} + \mathfrak{b}$ ein gemeinsamer Teiler von $\mathfrak{a}$, $\mathfrak{b}$ ist, so muß das Produkt $\mathfrak{p}$ auch ein gemeinsamer Teiler der Produkte $\mathfrak{a}\,\mathfrak{c}$, $\mathfrak{b}\,\mathfrak{c}$, also ein Teiler von deren größtem gemeinsamen Teiler $\mathfrak{q}$ sein. Um aber das erstere zu beweisen, müssen wir alle in den Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ enthaltenen Zahlen α, β, γ betrachten; nun ist jede Zahl des Produktes $\mathfrak{p}$ ein Produkt $(\alpha + \beta)\gamma$ oder eine Summe von mehreren solchen Produkten, und da $(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$ die Summe einer in $\mathfrak{a}\,\mathfrak{c}$ enthaltenen Zahl $\alpha\gamma$ und einer in $\mathfrak{b}\,\mathfrak{c}$ enthaltenen Zahl $\beta\gamma$ ist, so ist jedes Produkt $(\alpha + \beta)\gamma$ und folglich jede Zahl des Moduls $\mathfrak{p}$ in der Summe $\mathfrak{q}$ der Moduln $\mathfrak{a}\,\mathfrak{c}$, $\mathfrak{b}\,\mathfrak{c}$ enthalten, d. h. $\mathfrak{p} > \mathfrak{q}$, was zu beweisen war.

Wir bemerken, daß es keinen ebenso bestimmten Satz für das kleinste gemeinsame Vielfache gibt; aus dem Satze I folgt lediglich, daß

$$(9) \qquad (\mathfrak{a} - \mathfrak{b})\,\mathfrak{c} > \mathfrak{a}\,\mathfrak{c} - \mathfrak{b}\,\mathfrak{c}$$

ist, und mehr läßt sich im allgemeinen nicht beweisen**). Wenn aber $\mathfrak{c}$ z. B. ein eingliedriger Modul $[\eta]$ ist, so ergibt sich leicht

$$(10) \qquad (\mathfrak{a} - \mathfrak{b})\,\eta = \mathfrak{a}\,\eta - \mathfrak{b}\,\eta.$$

Der Satz IV läßt sich, wie man leicht erkennt, auf Produkte von beliebig vielen Faktoren (in endlicher Anzahl) ausdehnen, deren jeder eine Summe von beliebig vielen (auch unendlich vielen) Moduln ist; als spezieller Fall ergibt sich z. B. wieder, daß jedes Produkt aus

---

*) Nimmt man z. B. $\mathfrak{a} = [1]$, $\mathfrak{a}' = [i]$, $\mathfrak{b} = [1, i]$, wo $i^2 = -1$, so ist $\mathfrak{a}\,\mathfrak{b} = \mathfrak{a}'\,\mathfrak{b} = \mathfrak{b}$, aber keiner der beiden Moduln $\mathfrak{a}$, $\mathfrak{a}'$ ist durch den anderen teilbar.

**) Ist z. B. $\mathfrak{a} = [1]$, $\mathfrak{b} = [i]$, $\mathfrak{c} = [1, i]$, wo $i^2 = -1$, so ist $\mathfrak{a} - \mathfrak{b} = (\mathfrak{a} - \mathfrak{b})\,\mathfrak{c} = 0$, hingegen $\mathfrak{a}\,\mathfrak{c} = \mathfrak{b}\,\mathfrak{c} = \mathfrak{a}\,\mathfrak{c} - \mathfrak{b}\,\mathfrak{c} = \mathfrak{c}$.

zwei endlichen Moduln $\Sigma[\alpha_r]$ und $\Sigma[\beta_s]$ ebenfalls ein endlicher Modul $\Sigma[\alpha_r \beta_s]$ ist. Zugleich leuchtet ein, daß sehr viele Identitäten der gewöhnlichen Buchstabenrechnung, in denen nur die Addition und Multiplikation der Zahlen auftritt, sich unmittelbar auf unsere Moduln übertragen lassen. So ist z. B.:

$$(11) \qquad \begin{aligned}&(\mathfrak{a}+\mathfrak{b}_1)(\mathfrak{a}+\mathfrak{b}_2)\ldots(\mathfrak{a}+\mathfrak{b}_n)\\ &= \mathfrak{a}^n + \mathfrak{c}_1\mathfrak{a}^{n-1} + \mathfrak{c}_2\mathfrak{a}^{n-2} + \cdots + \mathfrak{c}_{n-1}\mathfrak{a} + \mathfrak{c}_n,\end{aligned}$$

wo $\mathfrak{c}_1, \mathfrak{c}_2, \ldots, \mathfrak{c}_{n-1}, \mathfrak{c}_n$ die einfachsten, auf symmetrische Weise aus $\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_n$ gebildeten Moduln (Summen von Produkten) bedeuten. Allein viele dieser Sätze erleiden doch, weil $\mathfrak{a}+\mathfrak{a} = \mathfrak{a}$ und nicht $= 2\mathfrak{a}$ ist, eine wesentliche Änderung. Sind z. B. in der vorstehenden Gleichung die n Moduln $\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_n$ alle $= \mathfrak{b}$, so wird $\mathfrak{c}_r = \mathfrak{b}^r$, und man erhält

$$(12) \qquad (\mathfrak{a}+\mathfrak{b})^n = \mathfrak{a}^n + \mathfrak{a}^{n-1}\mathfrak{b} + \mathfrak{a}^{n-2}\mathfrak{b}^2 + \cdots + \mathfrak{b}^n.$$

Unter diesen der Modultheorie eigentümlichen Identitäten müssen wir wenigstens eine hier noch besonders hervorheben, weil sie uns später (§ 173) von sehr großem Nutzen sein wird, nämlich

$$(13) \qquad (\mathfrak{a}+\mathfrak{b}+\mathfrak{c})(\mathfrak{b}\mathfrak{c}+\mathfrak{c}\mathfrak{a}+\mathfrak{a}\mathfrak{b}) = (\mathfrak{b}+\mathfrak{c})(\mathfrak{c}+\mathfrak{a})(\mathfrak{a}+\mathfrak{b}).$$

Ihre Wahrheit ergibt sich unmittelbar durch Auflösung aller Klammern, worauf beide Produkte dieselbe Form

$$\mathfrak{a}\mathfrak{b}\mathfrak{c} + \mathfrak{a}\mathfrak{b}^2 + \mathfrak{a}\mathfrak{c}^2 + \mathfrak{b}\mathfrak{c}^2 + \mathfrak{b}\mathfrak{a}^2 + \mathfrak{c}\mathfrak{a}^2 + \mathfrak{c}\mathfrak{b}^2$$

annehmen. Das Charakteristische dieses Satzes*) besteht darin, daß ein und derselbe Modul auf zwei wesentlich verschiedene Arten als Produkt von Faktoren dargestellt wird, und daß eine Summe von drei beliebigen Moduln $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ durch Multiplikation mit einem Modul, dessen Zahlen auf rationale Weise aus denen von $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$

*) Derselbe ist nur ein spezieller Fall des folgenden allgemeinen, nicht ganz leicht zu beweisenden Satzes, in welchem wir die oben in (11) gebrauchte Bezeichnung beibehalten: Wenn $n > r > 0$, so ist das Produkt aller Summen von je $(r+1)$ mit verschiedenen Zeigern behafteten Moduln aus der Reihe $\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_n$ identisch mit dem Produkte

$$\mathfrak{c}_1^{e_1}\mathfrak{c}_2^{e_2}\ldots\mathfrak{c}_{n-r}^{e_{n-r}},$$

wo die Exponenten die Binomialkoeffizienten

$$e_s = \frac{\Pi(n-1-s)}{\Pi(r-1)\,\Pi(n-r-s)}$$

bedeuten. Für $r = 1$ wird dieses Produkt $= \mathfrak{c}_1\mathfrak{c}_2\ldots\mathfrak{c}_{n-2}\mathfrak{c}_{n-1}$, und hieraus folgt unser obiger Satz (13) für $n = 3$.

gebildet sind, in ein Produkt verwandelt wird, dessen Faktoren die Summen von je zwei dieser Moduln sind. —

Wir wenden uns endlich zu einer letzten Art von Modulbildung, der Division. Unter dem Quotienten

$$\frac{\mathfrak{b}}{\mathfrak{a}} \text{ oder } \mathfrak{b} : \mathfrak{a}$$

zweier Moduln, des Nenners $\mathfrak{a}$ und des Zählers $\mathfrak{b}$ verstehen wir den Inbegriff $\mathfrak{n}$ aller derjenigen Zahlen ν (z. B. 0), für welche $\mathfrak{a}\nu > \mathfrak{b}$ wird. Sind ν_1, ν_2 solche Zahlen, während α jede Zahl in $\mathfrak{a}$ bedeutet, so sind alle Produkte $\alpha\nu_1$, $\alpha\nu_2$, also auch alle Produkte $\alpha(\nu_1 - \nu_2)$ in dem Modul $\mathfrak{b}$ enthalten, also ist $\mathfrak{a}(\nu_1 - \nu_2) > \mathfrak{b}$, und folglich gehört die Differenz $\nu_1 - \nu_2$ ebenfalls dem Quotienten $\mathfrak{n}$ an, welcher mithin ein Modul ist*). Offenbar ist jede der beiden Aussagen

$$(14) \qquad \mathfrak{a}\mathfrak{m} > \mathfrak{b} \text{ und } \mathfrak{m} > \frac{\mathfrak{b}}{\mathfrak{a}}$$

eine Folge der anderen, mithin könnte der Quotient $\mathfrak{n}$ auch erklärt werden als der größte gemeinsame Teiler (die Summe) aller der Moduln $\mathfrak{m}$, welche der Bedingung $\mathfrak{a}\mathfrak{m} > \mathfrak{b}$ genügen. Hierauf beruhen die leicht zu findenden Beweise der folgenden Sätze, in denen sich eine gewisse Fortsetzung des in § 169 erwähnten Dualismus offenbart:

$$(15) \qquad \text{Aus } \mathfrak{a} > \mathfrak{a}',\ \mathfrak{b} > \mathfrak{b}' \text{ folgt } \frac{\mathfrak{b}}{\mathfrak{a}'} > \frac{\mathfrak{b}'}{\mathfrak{a}}.$$

$$(16) \qquad \text{Allgemein ist } \mathfrak{a}\left(\frac{\mathfrak{b}}{\mathfrak{a}}\right) > \mathfrak{b} > \frac{\mathfrak{a}\mathfrak{b}}{\mathfrak{a}},$$

aber der erste Modul ist gleich dem zweiten, wenn $\mathfrak{a}$ ein Faktor von $\mathfrak{b}$, d. h. wenn $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$, und der zweite Modul ist gleich dem dritten, wenn $\mathfrak{b} = \mathfrak{c} : \mathfrak{a}$ ist. Ferner ergibt sich

$$(17) \qquad \frac{\mathfrak{a}}{\mathfrak{d}} = \mathfrak{a};\ \frac{\mathfrak{c}}{\mathfrak{a}\mathfrak{b}} = \left(\frac{\mathfrak{c}}{\mathfrak{a}}\right) : \mathfrak{b};\ \mathfrak{b}\left(\frac{\mathfrak{a}}{\mathfrak{c}}\right) > \frac{\mathfrak{a}\mathfrak{b}}{\mathfrak{c}}$$

$$(18) \qquad \frac{\mathfrak{a} - \mathfrak{b}}{\mathfrak{c}} = \frac{\mathfrak{a}}{\mathfrak{c}} - \frac{\mathfrak{b}}{\mathfrak{c}};\ \frac{\mathfrak{c}}{\mathfrak{a} + \mathfrak{b}} = \frac{\mathfrak{c}}{\mathfrak{a}} - \frac{\mathfrak{c}}{\mathfrak{b}}$$

$$(19) \qquad \frac{\mathfrak{c}}{\mathfrak{a} - \mathfrak{b}} < \frac{\mathfrak{c}}{\mathfrak{a}} + \frac{\mathfrak{c}}{\mathfrak{b}};\ \frac{\mathfrak{a} + \mathfrak{b}}{\mathfrak{c}} < \frac{\mathfrak{a}}{\mathfrak{c}} + \frac{\mathfrak{b}}{\mathfrak{c}}.$$

In den Untersuchungen, auf welche wir uns hier beschränken müssen, wird vorzugsweise der besondere Fall auftreten, wo Zähler

*) Ist der Nenner $\mathfrak{a} = 0$, so ist der Quotient der Inbegriff aller Zahlen.

und Nenner eines Quotienten miteinander identisch sind. Wenn $\mathfrak{a}$ ein beliebiger Modul ist, so setzen wir

$$\mathfrak{a}^0 = \frac{\mathfrak{a}}{\mathfrak{a}} \tag{20}$$

und nennen $\mathfrak{a}^0$ die Ordnung von $\mathfrak{a}$; nach (14) ist dann jede der beiden Aussagen

$$\mathfrak{a}\,\mathfrak{m} > \mathfrak{a} \quad \text{und} \quad \mathfrak{m} > \mathfrak{a}^0 \tag{21}$$

eine Folge der anderen. Hieraus ergibt sich nach (4) zunächst

$$\mathfrak{z} > \mathfrak{a}^0, \text{ also allgemein } \mathfrak{b} > \mathfrak{b}\,\mathfrak{a}^0, \tag{22}$$

d. h. in jeder Ordnung sind alle ganzen rationalen Zahlen enthalten. Da mithin $\mathfrak{a} > \mathfrak{a}\,\mathfrak{a}^0$, und zufolge (21) auch $\mathfrak{a}\,\mathfrak{a}^0 > \mathfrak{a}$ ist, so ergibt sich

$$\mathfrak{a}\,\mathfrak{a}^0 = \mathfrak{a}, \tag{23}$$

und hieraus ebenso leicht

$$\frac{\mathfrak{a}}{\mathfrak{a}^0} = \mathfrak{a}. \tag{24}$$

Aus (23) folgt $\mathfrak{a}\,\mathfrak{a}^0\,\mathfrak{a}^0 = \mathfrak{a}$, also nach (21) auch $\mathfrak{a}^0\,\mathfrak{a}^0 > \mathfrak{a}^0$, und da aus (22) ebenso $\mathfrak{a}^0 > \mathfrak{a}^0\,\mathfrak{a}^0$ folgt, so ist

$$\mathfrak{a}^0\,\mathfrak{a}^0 = \mathfrak{a}^0, \tag{25}$$

mithin reproduzieren sich die Zahlen einer jeden Ordnung nicht bloß durch Addition und Subtraktion, sondern auch durch Multiplikation.

Umgekehrt, wenn ein Modul $\mathfrak{o}$ die Zahl 1 enthält, und wenn seine Zahlen sich durch Multiplikation reproduzieren, wenn also

$$\mathfrak{z} > \mathfrak{o},\ \mathfrak{o}^2 > \mathfrak{o} \tag{26}$$

ist, so folgt leicht, daß $\mathfrak{o}$ eine Ordnung, nämlich

$$\mathfrak{o} = \mathfrak{o}^0 \tag{27}$$

ist; denn zufolge der zweiten Annahme (26) ist $\mathfrak{o} > \mathfrak{o}^0$, und aus der ersten folgt durch Multiplikation mit $\mathfrak{o}^0$ und mit Rücksicht auf (23) auch $\mathfrak{o}^0 > \mathfrak{o}$, woraus sich (27) ergibt.

Da nun zufolge (22), (25) jede Ordnung $\mathfrak{a}^0$ die beiden Eigenschaften (26) besitzt, so folgt

$$(\mathfrak{a}^0)^0 = \mathfrak{a}^0, \tag{28}$$

und ebenso findet man, daß das kleinste gemeinsame Vielfache $\mathfrak{a}^0 - \mathfrak{b}^0$ von zwei Ordnungen $\mathfrak{a}^0$, $\mathfrak{b}^0$, und ihr Produkt $\mathfrak{a}^0\,\mathfrak{b}^0$, welches

auch $= (\mathfrak{a}^0 + \mathfrak{b}^0)^2$ und $< \mathfrak{a}^0 + \mathfrak{b}^0$ ist, wieder Ordnungen sind. Offenbar ist

(29) $$\mathfrak{a}\,\mathfrak{b} = \mathfrak{a}^0(\mathfrak{a}\,\mathfrak{b}) = \mathfrak{b}^0(\mathfrak{a}\,\mathfrak{b}) = \mathfrak{a}^0\mathfrak{b}^0(\mathfrak{a}\,\mathfrak{b}),$$

und aus (14), (16), (22), (23) folgt ebenso

(30) $$\frac{\mathfrak{b}}{\mathfrak{a}} = \mathfrak{a}^0\left(\frac{\mathfrak{b}}{\mathfrak{a}}\right) = \mathfrak{b}^0\left(\frac{\mathfrak{b}}{\mathfrak{a}}\right) = \mathfrak{a}^0\mathfrak{b}^0\left(\frac{\mathfrak{b}}{\mathfrak{a}}\right),$$

mithin

(31) $$\mathfrak{a}^0 + \mathfrak{b}^0 > \mathfrak{a}^0\mathfrak{b}^0 > (\mathfrak{a}\,\mathfrak{b})^0,\ \mathfrak{a}^0\mathfrak{b}^0 > \left(\frac{\mathfrak{b}}{\mathfrak{a}}\right)^0.$$

Es liegt nun nahe, den Begriff der Potenz eines Moduls $\mathfrak{a}$ auch auf den Fall negativer Exponenten auszudehnen, indem man

(32) $$\mathfrak{a}^{-n} = \frac{\mathfrak{a}^0}{\mathfrak{a}^n}$$

setzt, wenn $n > 0$ ist. Allein es ist im allgemeinen unmöglich, die Gesetze der Multiplikation und Division von Zahlenpotenzen auf die Modulpotenzen zu übertragen; vielmehr zerfallen die Moduln hinsichtlich ihres Verhaltens zu ihrer Ordnung in zwei wesentlich verschiedene Arten. Aus (16) und (30) folgt jedenfalls

(33) $$\mathfrak{a}\,\mathfrak{a}^{-1} > \mathfrak{a}^0,\ \mathfrak{a}^0\mathfrak{a}^{-1} = \mathfrak{a}^{-1},\ \mathfrak{a}^0 > (\mathfrak{a}^{-1})^0,\ \mathfrak{a} > (\mathfrak{a}^{-1})^{-1};$$

wir wollen aber $\mathfrak{a}$ einen eigentlichen Modul nennen,

(34) $$\text{wenn } \mathfrak{a}\,\mathfrak{a}^{-1} = \mathfrak{a}^0,$$

oder, was nach (4), (23), (33) hiermit gleichwertig ist,

(34′) $$\text{wenn } \mathfrak{z} > \mathfrak{a}\,\mathfrak{a}^{-1}$$

ist. Aus dieser Erklärung ergeben sich die folgenden Sätze:

V. Ein Modul $\mathfrak{a}$ ist gewiß (und auch nur dann) ein eigentlicher Modul, wenn er ein Faktor seiner Ordnung $\mathfrak{a}^0$ ist, d. h. wenn es einen Modul $\mathfrak{n}$ gibt, welcher der Bedingung $\mathfrak{a}\,\mathfrak{n} = \mathfrak{a}^0$ genügt; und hieraus folgt $\mathfrak{a}^{-1} = \mathfrak{n}\,\mathfrak{a}^0$.

Denn nach (23) ist $\mathfrak{a}(\mathfrak{n}\,\mathfrak{a}^0) = \mathfrak{a}^0$, also $\mathfrak{n}\,\mathfrak{a}^0 > \mathfrak{a}^{-1}$, und aus (33) folgt $\mathfrak{a}^{-1} = \mathfrak{a}^0\mathfrak{a}^{-1} = \mathfrak{n}\,\mathfrak{a}\,\mathfrak{a}^{-1} > \mathfrak{n}\,\mathfrak{a}^0$; mithin ist $\mathfrak{a}^{-1} = \mathfrak{n}\,\mathfrak{a}^0$, und folglich $\mathfrak{a}\,\mathfrak{a}^{-1} = \mathfrak{n}\,\mathfrak{a}\,\mathfrak{a}^0 = \mathfrak{n}\,\mathfrak{a} = \mathfrak{a}^0$, was zu beweisen war.

VI. Ist $\mathfrak{a}$ ein eigentlicher Modul, so gilt dasselbe von $\mathfrak{a}^{-1}$, und es ist

(35) $$(\mathfrak{a}^{-1})^0 = \mathfrak{a}^0,\ (\mathfrak{a}^{-1})^{-1} = \mathfrak{a}.$$

Denn da nach (31) die Ordnung eines Produktes ein Teiler von der Ordnung jedes Faktors ist, so folgt aus (34) mit Rück-

sicht auf (28), daß $a^0 < (a^{-1})^0$, und hieraus mit Rücksicht auf (33), daß $a^0 = (a^{-1})^0$ ist. Da nun zufolge (34) der Modul a^{-1} ein Faktor seiner Ordnung a^0 ist, so ist er zufolge V ein eigentlicher Modul, und zugleich ergibt sich die zweite Gleichung (35), was zu beweisen war.

VII. Ist a ein eigentlicher, b ein beliebiger Modul, so ist

$$\frac{ab}{a} = b a^0, \quad \frac{b a^0}{a} = b a^{-1}. \tag{36}$$

Diese beiden Sätze gehen auseinander hervor, wenn man b durch $b a^{-1}$ oder durch $b a$ ersetzt und (34), (33), (23) berücksichtigt. Bezeichnet man die linke und rechte Seite der ersten Gleichung bzw. mit p und q, so ist zufolge (17) immer $q > p$. Ist aber a ein eigentlicher Modul (34), so ist zufolge (22) $p > p a a^{-1}$, und da nach (16) $p a > b a$, also $p a a^{-1} > b a a^{-1}$ ist, so folgt $p > q$, mithin $p = q$, was zu beweisen war.

VIII. Sind a, b eigentliche Moduln, so gilt dasselbe von ihrem Produkte ab, und es ist

$$(ab)^0 = a^0 b^0, \quad (ab)^{-1} = a^{-1} b^{-1}. \tag{37}$$

Die erste Gleichung ergibt sich aus dem zweiten Satze (17), wenn man $c = ab$ setzt und den ersten Satz (36) zweimal anwendet. Da ferner $a a^{-1} = a^0$, $b b^{-1} = b^0$, mithin $(ab)(a^{-1} b^{-1}) = a^0 b^0 = (ab)^0$, also das Produkt ab ein Faktor seiner Ordnung $(ab)^0$ ist, so ist es nach V ein eigentlicher Modul, und zugleich ergibt sich mit Rücksicht auf (33), daß $(ab)^{-1} = (ab)^0 (a^{-1} b^{-1}) = a^0 b^0 a^{-1} b^{-1} = a^{-1} b^{-1}$ ist, was zu beweisen war.

Mit Hilfe dieser Sätze wird man leicht finden, daß die Multiplikation und Division aller Potenzen eines eigentlichen Moduls, ebenso aller eigentlichen Moduln, welche dieselbe Ordnung haben, genau nach denselben Regeln geschieht wie bei Produkten und Quotienten von Zahlen.

§ 171.

Wir gehen nun zu derjenigen Betrachtung über, die uns veranlaßt hat, für die hier untersuchten Zahlengebiete den Namen Moduln zu wählen, obgleich derselbe schon in so vielen anderen Bedeutungen gebraucht wird. Wenn m ein beliebiger Modul ist, so

nennen wir zwei Zahlen α, β kongruent nach $\mathfrak{m}$, wenn ihre Differenz $\alpha - \beta$ in $\mathfrak{m}$ enthalten ist, und wir bezeichnen dies durch die Kongruenz

$$\alpha \equiv \beta \pmod{\mathfrak{m}}, \tag{1}$$

in welcher offenbar die beiden Zahlen α, β, deren jede auch ein Rest der anderen heißt, stets miteinander vertauscht werden dürfen. Wir nennen dagegen die Zahlen α, β, γ, ... inkongruent nach $\mathfrak{m}$, wenn keine von ihnen mit einer der übrigen kongruent ist*). Aus dem Begriffe eines Moduls und aus den früheren Sätzen folgt, daß man beliebig viele solche Kongruenzen, die sich auf einen und denselben Modul $\mathfrak{m}$ beziehen, addieren und subtrahieren darf, wie Gleichungen; auch darf man beide Seiten einer solchen Kongruenz mit derselben ganzen rationalen Zahl, allgemeiner mit jeder in der Ordnung $\mathfrak{m}^0$ des Moduls $\mathfrak{m}$ enthaltenen Zahl multiplizieren. Aus der Kongruenz zweier Zahlen in bezug auf einen Modul $\mathfrak{m}$ folgt auch ihre Kongruenz in bezug auf jeden Teiler von $\mathfrak{m}$, und wenn eine Kongruenz in bezug auf mehrere Moduln gilt, so gilt sie auch für deren kleinstes gemeinsames Vielfaches.

Ferner leuchtet ein, daß jede Zahl sich selbst kongruent, und daß zwei mit einer dritten Zahl γ kongruente Zahlen α, β auch einander kongruent sind; denn wenn $\alpha - \gamma$, $\beta - \gamma$ Zahlen des Moduls $\mathfrak{m}$ sind, so ist auch ihre Differenz $\alpha - \beta$ in $\mathfrak{m}$ enthalten. Hierauf beruht die Möglichkeit, alle Zahlen in bezug auf einen Modul $\mathfrak{m}$ in Zahlklassen einzuteilen, in der Weise, daß je zwei beliebige Zahlen in dieselbe oder in verschiedene Klassen aufgenommen werden, je nachdem sie kongruent oder inkongruent sind; ist α eine bestimmte Zahl, während μ alle Zahlen des Moduls $\mathfrak{m}$ durchläuft, so bilden die Zahlen $\alpha + \mu$ eine solche Klasse, die wir mit $\alpha + \mathfrak{m}$ oder $\mathfrak{m} + \alpha$ bezeichnen wollen, und man kann α oder jede andere dieser Zahlen als Repräsentant oder auch als Rest der Klasse ansehen. Die Gleichung $\mathfrak{m} + \alpha = \mathfrak{m} + \beta$ ist dann gleichbedeutend mit der Kongruenz (1); findet sie nicht statt, so sind die Klassen $\alpha + \mathfrak{m}$, $\beta + \mathfrak{m}$ verschieden und

*) Der von Gauß zuerst eingeführte Begriff der Kongruenz bildet offenbar einen besonderen Fall des obigen; denn wenn a, b, m ganze rationale Zahlen sind, so ist die Kongruenz $a \equiv b \pmod{m}$ gleichbedeutend mit der Kongruenz der Zahlen a, b nach dem Modul $[m] = m\,[1]$; und wenn α, β, μ ganze Zahlen des Körpers J sind (§ 159), so ist die Kongruenz $\alpha \equiv \beta \pmod{\mu}$ gleichbedeutend mit der Kongruenz der Zahlen α, β nach dem Modul $[\mu, \mu i] = \mu\,[1, i]$.

besitzen keine einzige gemeinsame Zahl. Offenbar bildet der Modul $\mathfrak{m}$ selbst die durch die Zahl 0 repräsentierte Klasse.

Auf diesem Begriffe beruhen die folgenden Betrachtungen. Ist $\mathfrak{a}$ ein Teiler von $\mathfrak{m}$, und α' eine bestimmte Zahl in $\mathfrak{a}$, so sind alle Zahlen der Klasse $\alpha' + \mathfrak{m}$ auch in $\mathfrak{a}$ enthalten, und folglich besteht der Modul $\mathfrak{a}$ aus einer endlichen oder unendlichen Anzahl verschiedener Klassen $\alpha' + \mathfrak{m}$, von denen je zwei keine gemeinsame Zahl besitzen. Ist ferner ϱ eine beliebige Zahl, so besteht zugleich die auf den Modul $\mathfrak{a}$ bezügliche Klasse $\varrho + \mathfrak{a}$ aus den sämtlichen entsprechenden, ebenfalls verschiedenen Zahlklassen $(\varrho + \alpha') + \mathfrak{m}$.

Allgemeiner, sind $\mathfrak{a}$, $\mathfrak{b}$ zwei beliebige Moduln, deren kleinstes gemeinsames Vielfaches $\mathfrak{a} - \mathfrak{b}$ zur Abkürzung mit $\mathfrak{m}$ bezeichnet werden möge, und ist α' eine bestimmte Zahl in $\mathfrak{a}$, so bilden alle diejenigen in $\mathfrak{a}$ enthaltenen Zahlen α, welche $\equiv \alpha' \pmod{\mathfrak{b}}$ sind, die auf $\mathfrak{m}$ bezügliche, durch α' repräsentierte Klasse $\alpha' + \mathfrak{m}$; da nämlich $\alpha - \alpha'$ sowohl in $\mathfrak{a}$ als auch in $\mathfrak{b}$ enthalten ist, so ist $\alpha = \alpha' + \mu$, wo μ eine Zahl des Moduls $\mathfrak{m}$ bedeutet, und umgekehrt, wenn μ in $\mathfrak{m}$, also auch in $\mathfrak{a}$ und in $\mathfrak{b}$ enthalten ist, so ist die Summe $\alpha = \alpha' + \mu$ in $\mathfrak{a}$ enthalten und zugleich $\equiv \alpha' \pmod{\mathfrak{b}}$. Wählt man daher aus jeder der verschiedenen Klassen $\alpha' + \mathfrak{m}$, aus denen $\mathfrak{a}$ besteht, einen bestimmten Rest α' aus, so besitzt das System aller dieser in $\mathfrak{a}$ enthaltenen Zahlen α' offenbar die charakteristische Eigenschaft, daß jede beliebige in $\mathfrak{a}$ enthaltene Zahl α mit einer, aber auch nur mit einer einzigen Zahl α' kongruent ist nach dem Modul $\mathfrak{b}$; ein solches System von Zahlen α' nennen wir daher ein Repräsentanten-System oder ein Restsystem von $\mathfrak{a}$ nach $\mathfrak{b}$. Ist die Anzahl dieser in $\mathfrak{a}$ enthaltenen, nach $\mathfrak{b}$ inkongruenten Zahlen α' endlich, so wollen wir dieselbe durch das Symbol

$$(\mathfrak{a}, \mathfrak{b})$$

bezeichnen*), und dies ist zugleich die Anzahl der Klassen $\alpha' + \mathfrak{m}$, aus denen $\mathfrak{a}$ besteht; ist sie aber unendlich, so ist es zweckmäßig, unter dem Symbol $(\mathfrak{a}, \mathfrak{b})$ die Zahl Null zu verstehen, weil dann die meisten Sätze allgemein gültig bleiben**). Ist $(\mathfrak{a}, \mathfrak{b}) = 1$, sind also

*) Dasselbe habe ich zuerst in § 169 der zweiten Auflage benutzt. Sollten die Moduln $\mathfrak{a}$, $\mathfrak{b}$ zugleich Körper sein, was aber bei unseren Untersuchungen niemals vorkommen wird, so würde die dem Symbol $(\mathfrak{a}, \mathfrak{b})$ jetzt beigelegte Bedeutung von der in § 164 wohl zu unterscheiden sein.

**) Vgl. z. B. die Sätze im folgenden § 172.

alle Zahlen α des Moduls $\mathfrak{a}$ einander kongruent, mithin alle $\alpha \equiv 0 \pmod{\mathfrak{b}}$, so ist $\mathfrak{a}$ teilbar durch $\mathfrak{b}$, und aus dieser Teilbarkeit folgt umgekehrt $(\mathfrak{a}, \mathfrak{b}) = 1$.

Aus dem Obigen leuchtet unmittelbar ein, daß dieselben Zahlen α' zugleich ein Restsystem von $\mathfrak{a}$ nach $\mathfrak{m}$ bilden, und folglich ist in allen Fällen

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

Dieselben Zahlen α' bilden aber auch ein Restsystem von $\mathfrak{a} + \mathfrak{b}$ nach $\mathfrak{b}$, d. h. $\mathfrak{a} + \mathfrak{b}$ besteht aus den sämtlichen Klassen $\alpha' + \mathfrak{b}$, und folglich ist

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

denn die Zahlen α' sind auch in $\mathfrak{a} + \mathfrak{b}$ enthalten und inkongruent nach $\mathfrak{b}$, und jede in $\mathfrak{a} + \mathfrak{b}$ enthaltene Zahl $\alpha + \beta$ ist $\equiv \alpha \pmod{\mathfrak{b}}$, also auch kongruent mit einer der Zahlen α', was zu beweisen war.

Auf dieselbe Weise ergibt sich, daß, wenn η eine von Null verschiedene Zahl ist, die Produkte $\eta\alpha'$ ein Restsystem von $\mathfrak{a}\eta$ nach $\mathfrak{b}\eta$ bilden, und folglich ist

$$(4) \qquad (\mathfrak{a}\eta, \mathfrak{b}\eta) = (\mathfrak{a}, \mathfrak{b}).$$

Ist ferner $\mathfrak{a}$ ein Teiler von $\mathfrak{b}$, und $\mathfrak{b}$ ein Teiler von $\mathfrak{c}$, also $(\mathfrak{b}, \mathfrak{a}) = (\mathfrak{c}, \mathfrak{b}) = 1$, so bilden, wenn α' ein Restsystem von $\mathfrak{a}$ nach $\mathfrak{b}$, und β' ein Restsystem von $\mathfrak{b}$ nach $\mathfrak{c}$ durchläuft, die sämtlichen Summen $\alpha' + \beta'$ ein Restsystem von $\mathfrak{a}$ nach $\mathfrak{c}$, und folglich ist

$$(5) \qquad (\mathfrak{a}, \mathfrak{c}) = (\mathfrak{a}, \mathfrak{b})(\mathfrak{b}, \mathfrak{c}), \text{ wenn } \mathfrak{a} < \mathfrak{b} < \mathfrak{c}.$$

Denn $\mathfrak{a}$ besteht aus allen Klassen $\alpha' + \mathfrak{b}$, und jede dieser Klassen wieder aus den allen β' entsprechenden Klassen $(\alpha' + \beta') + \mathfrak{c}$, mithin besteht $\mathfrak{a}$ aus allen Klassen $(\alpha' + \beta') + \mathfrak{c}$, wo α' und β' alle ihre Werte durchlaufen.

Zu diesen Sätzen, durch deren Verbindung sich viele andere*) ableiten lassen, fügen wir noch die folgenden hinzu.

---

*) Aus drei beliebigen Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ entspringt, wie in der Anmerkung auf S. 66 erwähnt ist, eine Gruppe von 28 Moduln $\mathfrak{m}$, $\mathfrak{n}$, ...; die sämtlichen Klassenanzahlen $(\mathfrak{m}, \mathfrak{n})$ lassen sich aus sieben von ihnen bestimmen; bezeichnet man diese mit a, b, c, a_1, b_1, c_1 und d, so ist z. B.:

$$(\mathfrak{b}, \mathfrak{c}) = b\,c_1\,d, \quad (\mathfrak{c}, \mathfrak{a}) = c\,a_1\,d, \quad (\mathfrak{a}, \mathfrak{b}) = a\,b_1\,d,$$
$$(\mathfrak{c}, \mathfrak{b}) = c\,b_1\,d, \quad (\mathfrak{a}, \mathfrak{c}) = a\,c_1\,d, \quad (\mathfrak{b}, \mathfrak{a}) = b\,a_1\,d.$$

Hieraus folgt der schon in der zweiten Auflage dieses Werkes (S. 490) angeführte Satz

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

welcher sich aber auch leicht auf kürzerem Wege beweisen läßt.

I. Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei beliebige Moduln, so genügt jede in $\mathfrak{a}$ enthaltene Zahl α der Kongruenz

$$(6) \qquad (\mathfrak{a}, \mathfrak{b})\, \alpha \equiv 0 \pmod{\mathfrak{a} - \mathfrak{b}},$$

also ist $(\mathfrak{a}, \mathfrak{b})\, \mathfrak{a} > \mathfrak{a} - \mathfrak{b}$.

Dies leuchtet, wenn $(\mathfrak{a}, \mathfrak{b}) = 0$ ist, unmittelbar ein. Ist aber $(\mathfrak{a}, \mathfrak{b}) = n > 0$, und durchläuft α' ein Restsystem von $\mathfrak{a}$ nach $\mathfrak{a} - \mathfrak{b}$, während α eine bestimmte Zahl in $\mathfrak{a}$ bedeutet, so bilden die n Zahlen $\alpha + \alpha'$, weil sie in $\mathfrak{a}$ enthalten und inkongruent nach $\mathfrak{a} - \mathfrak{b}$ sind, ebenfalls ein solches Restsystem; jede dieser Zahlen $\alpha + \alpha'$ ist daher mit einer der Zahlen α', umgekehrt jede der letzteren mit einer der ersteren kongruent; mithin ist auch die Summe σ der Zahlen α' kongruent der Summe $n\alpha + \sigma$, woraus (6) folgt, was zu beweisen war.

II. Ist $\mathfrak{c} > \mathfrak{a}$, und $(\mathfrak{a}, \mathfrak{c}) > 0$, so gibt es nur eine endliche Anzahl solcher Moduln $\mathfrak{b}$, welche $> \mathfrak{a}$ und zugleich $< \mathfrak{c}$ sind*).

Da nämlich jeder solche Modul $\mathfrak{b}$ aus gewissen Zahlklassen $\beta' + \mathfrak{c}$ bestehen muß, welche in $\mathfrak{a}$ enthalten sind, und unter denen sich immer $\mathfrak{c}$ selbst befindet, und da die Anzahl m aller in $\mathfrak{a}$ enthaltenen Klassen $\alpha' + \mathfrak{c}$ endlich, nämlich $= (\mathfrak{a}, \mathfrak{c})$ ist, so kann die Anzahl der Moduln $\mathfrak{b}$ höchstens gleich 2^{m-1} sein, was zu beweisen war.

Wir schließen diese Betrachtungen mit der Verallgemeinerung zweier in § 25 und § 11 bewiesenen Sätze.

III. Sind ϱ, σ gegebene Zahlen, und $\mathfrak{a}$, $\mathfrak{b}$ irgend zwei Moduln, so haben die beiden gleichzeitigen Kongruenzen

$$(7) \qquad \omega \equiv \varrho \pmod{\mathfrak{a}}, \quad \omega \equiv \sigma \pmod{\mathfrak{b}}$$

stets und nur dann gemeinsame Wurzeln ω, wenn

$$(8) \qquad \varrho \equiv \sigma \pmod{\mathfrak{a} + \mathfrak{b}}$$

ist, und alle diese Wurzeln, d. h. alle den beiden Klassen $\mathfrak{a} + \varrho$, $\mathfrak{b} + \sigma$ gemeinsamen Zahlen ω bilden eine bestimmte Klasse in bezug auf den Modul $\mathfrak{a} - \mathfrak{b}$.

---

*) Daß auch die Umkehrung dieses Satzes wahr ist, wird man leicht beweisen, z. B. durch die Betrachtung aller Moduln von der Form $\mathfrak{c}$, $\mathfrak{c} + [\alpha]$, $\mathfrak{c} + [2\alpha]$, $\mathfrak{c} + [3\alpha] \ldots$, wo α jede beliebige Zahl in $\mathfrak{a}$ bedeutet. Man kann auch von dem Begriffe eines unmittelbaren oder nächsten Teilers von $\mathfrak{c}$ ausgehen; so soll ein echter Teiler $\mathfrak{b}$ von $\mathfrak{c}$ heißen, wenn es außer $\mathfrak{b}$ und $\mathfrak{c}$ keinen Modul gibt, der $> \mathfrak{b}$ und zugleich $< \mathfrak{c}$ ist; die erforderliche und hinreichende Bedingung hierfür besteht darin, daß $(\mathfrak{b}, \mathfrak{c})$ eine Primzahl ist. Man vergleiche hiermit die Betrachtungen im folgenden § 172.

In der Tat, wenn eine Zahl ω den Kongruenzen (7) genügt, so sind die Zahlen $\omega - \varrho$, $\omega - \sigma$, also auch ihre Differenz in $\mathfrak{a} + \mathfrak{b}$ enthalten, d. h. die Bedingung (8) ist erfüllt. Umgekehrt, wenn dies der Fall ist, so gibt es zufolge der Definition von $\mathfrak{a} + \mathfrak{b}$ eine Zahl α in $\mathfrak{a}$ und eine Zahl β in $\mathfrak{b}$, deren Summe $\alpha + \beta = \varrho - \sigma$ ist, und dann erfüllt die Zahl $\omega = \varrho - \alpha = \sigma + \beta$ die Kongruenzen (7). Genügt ferner ω' denselben Kongruenzen (7), so ist $\omega' - \omega$ in $\mathfrak{a}$ und $\mathfrak{b}$, also in $\mathfrak{a} - \mathfrak{b}$ enthalten, mithin $\omega' \equiv \omega \pmod{\mathfrak{a} - \mathfrak{b}}$, und umgekehrt leuchtet ein, daß jede Zahl ω' der Klasse $\omega + (\mathfrak{a} - \mathfrak{b})$ auch den Kongruenzen (7) genügt, was zu beweisen war*).

IV. Ist $(\mathfrak{a}, \mathfrak{m}) > 0$, und $\mathfrak{a} - \mathfrak{m}$ teilbar durch jeden der r Moduln $\mathfrak{n}$, so ist die Anzahl aller derjenigen nach $\mathfrak{m}$ inkongruenten Zahlen α in $\mathfrak{a}$, die in keinem Modul $\mathfrak{n}$ enthalten sind, gleich der Summendifferenz

$$\Sigma(\mathfrak{n}', \mathfrak{m}) - \Sigma(\mathfrak{n}'', \mathfrak{m}), \tag{9}$$

wo für $\mathfrak{n}'$ der Modul $\mathfrak{a}$ und jedes aus $\mathfrak{a}$ und einer geraden Anzahl, für $\mathfrak{n}''$ jedes aus $\mathfrak{a}$ und einer ungeraden Anzahl von Moduln $\mathfrak{n}$ gebildete kleinste Vielfache zu setzen ist.

Denn wenn ω irgendeine Zahl in $\mathfrak{a}$ bedeutet, so ist nach dem Obigen die Klasse $(\mathfrak{a} - \mathfrak{m}) + \omega$ der Inbegriff aller der Zahlen in $\mathfrak{a}$, welche $\equiv \omega \pmod{\mathfrak{m}}$ sind, und $\mathfrak{a}$ besteht aus $(\mathfrak{a}, \mathfrak{m})$ solchen Klassen. Ist nun $\mathfrak{a} - \mathfrak{m} > \mathfrak{n}$, und ω in $\mathfrak{n}$, also auch in $\mathfrak{a} - \mathfrak{n}$ enthalten, so gilt dasselbe von allen Zahlen der Klasse $(\mathfrak{a} - \mathfrak{m}) + \omega$, und da $\mathfrak{a} - \mathfrak{n}$ aus $(\mathfrak{a} - \mathfrak{n}, \mathfrak{m})$ solchen Klassen besteht, so ist $(\mathfrak{a}, \mathfrak{m}) - (\mathfrak{a} - \mathfrak{n}, \mathfrak{m})$ die Anzahl derjenigen nach $\mathfrak{m}$ inkongruenten Zahlen in $\mathfrak{a}$, welche nicht in $\mathfrak{n}$ enthalten sind. Mithin gilt unser Satz für den Fall $r = 1$, weil es dann nur einen Modul $\mathfrak{n}' = \mathfrak{a}$, und nur einen Modul $\mathfrak{n}'' = \mathfrak{a} - \mathfrak{n}$ gibt. Nimmt man an, er sei für eine bestimmte Anzahl r von Moduln $\mathfrak{n}$ allgemein bewiesen, und der Modul $\mathfrak{p}$ gehe ebenfalls in $\mathfrak{a} - \mathfrak{m}$ auf, so darf man $\mathfrak{a}$ auch durch $\mathfrak{a} - \mathfrak{p}$ ersetzen, weil $(\mathfrak{a} - \mathfrak{p}, \mathfrak{m}) > 0$, und weil der Modul $(\mathfrak{a} - \mathfrak{p}) - \mathfrak{m} = \mathfrak{a} - \mathfrak{m}$, also durch jeden Modul $\mathfrak{n}$ teilbar ist; zufolge (9) ist daher die Differenz

$$\Sigma(\mathfrak{n}' - \mathfrak{p}, \mathfrak{m}) - \Sigma(\mathfrak{n}'' - \mathfrak{p}, \mathfrak{m})$$

*) Schwieriger gestaltet sich die Untersuchung, ob drei oder mehr gegebene Zahlklassen $\mathfrak{a} + \varrho$, $\mathfrak{b} + \sigma$, $\mathfrak{c} + \tau$ ... gemeinsame Zahlen besitzen oder nicht; im ersteren Falle kann man diese Klassen einig nennen, und es leuchtet ein, daß ihre Gemeinheit, d. h. der Inbegriff aller ihnen gemeinsamen Zahlen, eine auf den Modul $\mathfrak{a} - \mathfrak{b} - \mathfrak{c}$ ... bezügliche Klasse ist.

die Anzahl derjenigen, im Satze mit α bezeichneten Zahlen, welche in $\mathfrak{p}$ enthalten sind; zieht man dieselbe von der in (9) angegebenen Anzahl aller Zahlen α ab, so erhält man die Differenz

$$\{\Sigma(\mathfrak{n}', \mathfrak{m}) + \Sigma(\mathfrak{n}'' - \mathfrak{p}, \mathfrak{m})\} - \{\Sigma(\mathfrak{n}'', \mathfrak{m}) + \Sigma(\mathfrak{n}' - \mathfrak{p}, \mathfrak{m})\}$$

als Anzahl aller nicht in $\mathfrak{p}$ enthaltenen Zahlen α, d. h. aller nach $\mathfrak{m}$ inkongruenten Zahlen in $\mathfrak{a}$, welche in keinem der $(r+1)$ Moduln $\mathfrak{n}$, $\mathfrak{p}$ enthalten sind. Vergleicht man diesen Ausdruck mit (9), so ergibt sich, daß unser Satz auch für die nächstfolgende Anzahl $(r+1)$, mithin allgemein gilt, was zu beweisen war.

Statt die vollständige Induktion anzuwenden (wie in § 11), kann man unseren Satz auch unmittelbar auf folgende Art beweisen. Wir schicken die Bemerkung voraus, daß die Anzahl der Moduln $\mathfrak{n}'$ immer gleich der der Moduln $\mathfrak{n}''$, nämlich $= 2^{r-1}$ ist; sondert man nämlich einen bestimmten Modul $\mathfrak{n}$ aus, und bezeichnet mit $\mathfrak{o}'$, $\mathfrak{o}''$ bzw. diejenigen $\mathfrak{n}'$, $\mathfrak{n}''$, zu deren Bildung $\mathfrak{n}$ nicht mitwirkt, so besteht das System der Moduln $\mathfrak{n}'$ aus den Moduln $\mathfrak{o}'$, $\mathfrak{o}'' - \mathfrak{n}$, ebenso das System der Moduln $\mathfrak{n}''$ aus den Moduln $\mathfrak{o}' - \mathfrak{n}$, $\mathfrak{o}''$, wodurch unsere Behauptung erwiesen ist*). Läßt man nun ω ein Restsystem von $\mathfrak{a}$ nach $\mathfrak{m}$ durchlaufen, und bezeichnet mit ω', ω'' bzw. die Anzahl der Moduln $\mathfrak{n}'$, $\mathfrak{n}''$, denen ω angehört, so ist offenbar $\Sigma\omega' = \Sigma(\mathfrak{n}', \mathfrak{m})$, $\Sigma\omega'' = \Sigma(\mathfrak{n}'', \mathfrak{m})$, also die in (9) angegebene Differenz $= \Sigma(\omega' - \omega'')$. Da nun die Anzahl der Zahlen α offenbar $= \Sigma(\alpha' - \alpha'')$ ist, weil $\alpha' = 1$, $\alpha'' = 0$, so wird unser Satz bewiesen sein, wenn wir zeigen, daß für jede andere Zahl ω die Differenz $\omega' - \omega'' = 0$, also $\omega' = \omega''$ ist (vgl. § 138). Bezeichnet man mit $\mathfrak{p}$ diejenigen s Moduln $\mathfrak{n}$, denen ω angehört, und mit $\mathfrak{p}'$, $\mathfrak{p}''$ bzw. diejenigen Moduln $\mathfrak{n}'$, $\mathfrak{n}''$, welche aus $\mathfrak{a}$ und nur diesen Moduln $\mathfrak{p}$ gebildet sind, so gehört ω allen diesen Moduln $\mathfrak{p}'$, $\mathfrak{p}''$ und keinem anderen Modul $\mathfrak{n}'$, $\mathfrak{n}''$ an, und hieraus folgt nach der obigen Bemerkung $\omega' = \omega'' = 2^{s-1}$, w. z. b. w.

§ 172.

Von diesen allgemeinen Sätzen über die Beziehungen zwischen beliebigen Moduln wenden wir uns jetzt zur Betrachtung der be-

*) Wenn $\mathfrak{n}$ in $\mathfrak{a}$ aufgeht, also $\mathfrak{o}' - \mathfrak{n} = \mathfrak{o}'$, $\mathfrak{o}'' - \mathfrak{n} = \mathfrak{o}''$ ist, so fällt das System der Moduln $\mathfrak{n}'$ mit dem der Moduln $\mathfrak{n}''$ zusammen, und folglich verschwindet die Differenz in (9), was damit übereinstimmt, daß es in diesem Falle selbstverständlich gar keine Zahl α gibt. Aber man darf nicht umgekehrt aus der letzteren Tatsache schließen, daß mindestens einer der Moduln $\mathfrak{n}$ in $\mathfrak{a}$ aufgeht (vgl. § 178, IX).

sonderen Erscheinungen, welche dann auftreten, wenn diese Moduln zum Teil oder alle endlich sind (§ 168). Da jeder endliche Modul entweder eingliedrig oder [nach (5) in § 169] eine Summe von mehreren eingliedrigen Moduln ist, so gehen wir von dem folgenden Satze aus:

I. Jedes Vielfache $\mathfrak{m}$ eines eingliedrigen Moduls $\mathfrak{n}$ ist ebenfalls eingliedrig, und zwar ist

$$\mathfrak{m} = (\mathfrak{n}, \mathfrak{m})\,\mathfrak{n}. \tag{1}$$

Um dies zu beweisen, setzen wir $\mathfrak{z} = [1]$, $\mathfrak{n} = \mathfrak{z}\omega$ und bemerken, daß jede in $\mathfrak{m}$, also auch in $\mathfrak{n}$ enthaltene Zahl ein Produkt $x\omega$ ist, wo x eine Zahl in $\mathfrak{z}$ bedeutet, und daß der Inbegriff $\mathfrak{x}$ aller dieser Zahlen x, welche durch Multiplikation mit ω in Zahlen des Moduls $\mathfrak{m}$ verwandelt werden, offenbar ein durch $\mathfrak{z}$ teilbarer Modul ist; zugleich ist $\mathfrak{m} = \mathfrak{x}\omega$. Schließen wir zunächst den Fall aus, wo $\mathfrak{x} = 0$ ist, und bezeichnen wir mit a die kleinste positive Zahl in $\mathfrak{x}$, so ergibt sich leicht, daß $\mathfrak{x} = a\mathfrak{z}$, also $\mathfrak{m} = a\mathfrak{n}$ ist; denn wenn z jede Zahl in $\mathfrak{z}$ bedeutet, so ist az in $\mathfrak{x}$ enthalten, also $a\mathfrak{z} > \mathfrak{x}$; umgekehrt läßt sich jede in $\mathfrak{x}$ enthaltene Zahl x (nach § 4 oder § 17) in die Form $x = az + y$ setzen*), wo y eine der a Zahlen $0, 1, 2 \ldots (a-1)$ bedeutet, und da $y = x - az$ in $\mathfrak{x}$ enthalten ist, so muß $y = 0$, $x = az$, $\mathfrak{x} > a\mathfrak{z}$, also wirklich $\mathfrak{x} = a\mathfrak{z}$ sein**). Da ferner irgend zwei Zahlen $z_1\omega$, $z_2\omega$ des Moduls $\mathfrak{n}$ dann und nur dann kongruent nach $\mathfrak{m}$ sind, wenn ihre Differenz $(z_1 - z_2)\omega$ in $\mathfrak{m}$, also die Differenz $z_1 - z_2$ in $\mathfrak{x} = a\mathfrak{z}$ enthalten ist, so bilden die a Zahlen

$$0,\ \omega,\ 2\omega,\ \ldots,\ (a-1)\,\omega \tag{2}$$

ein Restsystem von $\mathfrak{n}$ nach $\mathfrak{m}$; mithin ist

$$a = (\mathfrak{n}, \mathfrak{m}), \tag{3}$$

und da, wie wir oben gesehen haben, $\mathfrak{m} = \mathfrak{x}\omega = a\mathfrak{n}$ ist, so ergibt sich hieraus unser Satz (1). Offenbar gilt derselbe aber auch in dem bisher ausgeschlossenen Falle, wo $\mathfrak{x} = 0$ ist; dann ist nämlich $\mathfrak{m} = \mathfrak{x}\omega = 0$, und da je zwei verschiedenen ganzen rationalen Zahlen z_1, z_2 zwei Zahlen $z_1\omega$, $z_2\omega$ des Moduls $\mathfrak{n}$ entsprechen, welche inkongruent nach $\mathfrak{m}$ sind, so ist (nach § 171) auch $(\mathfrak{n}, \mathfrak{m}) = 0$, w. z. b. w.

*) Dies ist die Grundlage aller Zahlentheorie.

**) Offenbar ist dies selbst nur ein spezieller Fall unseres Satzes.

Um zu zeigen, wie nützlich dieser Satz schon in den ersten Anfangsgründen der Zahlentheorie verwendet werden kann, leiten wir aus ihm zunächst den folgenden ab:

II. Jeder endliche, aus lauter rationalen Zahlen bestehende Modul $\mathfrak{c}$ ist darstellbar als eingliedriger Modul.

Besteht nämlich eine Basis von $\mathfrak{c}$ aus m ganzen oder gebrochenen rationalen Zahlen $c_1, c_2, \ldots, c_m$, die nicht alle verschwinden*), so kann man bekanntlich eine natürliche Zahl b immer so wählen, daß die m Produkte $bc_1, bc_2, \ldots, bc_m$ ganze Zahlen werden; da dieselben eine Basis des von Null verschiedenen Moduls $b\mathfrak{c}$ bilden, so ist letzterer teilbar durch den eingliedrigen Modul $\mathfrak{z}$, also $b\mathfrak{c} = a\mathfrak{z} = [a]$, wo a eine natürliche Zahl bedeutet; setzt man noch $a = bc$, so ist c eine positive rationale Zahl, und man erhält $\mathfrak{c} = [c]$, w. z. b. w.

Nach der Bedeutung unserer Symbole besagt nun die eben bewiesene Gleichung

$$[c_1, c_2, \ldots, c_m] = [c] \tag{4}$$

erstens, daß es m ganze rationale Zahlen $q_1, q_2, \ldots, q_m$ gibt, welche der Bedingung

$$c_1 q_1 + c_2 q_2 + \cdots + c_m q_m = c \tag{5}$$

genügen, und zweitens, daß

$$c_1 = c\,p_1, \; c_2 = c\,p_2, \ldots, c_m = c\,p_m, \tag{6}$$

also

$$p_1 q_1 + p_2 q_2 + \cdots + p_m q_m = 1 \tag{7}$$

ist, wo $p_1, p_2, \ldots, p_m$ ebenfalls ganze rationale Zahlen bedeuten. Da der Modul $[c]$ der größte gemeinsame Teiler der m Moduln $[c_r]$ ist, so nennen wir die Zahl c auch den größten gemeinsamen Teiler der m Zahlen c_r, und offenbar ist die gewöhnliche Bedeutung dieses Wortes (§§ 6 und 24) hierin als spezieller Fall enthalten. Ja es ist zweckmäßig, diese Ausdrucksweise selbst auf den oben ausgeschlossenen Fall zu übertragen, wo die m Zahlen c_r sämtlich verschwinden, und unter deren größtem gemeinsamen Teiler die Zahl $c = 0$ zu verstehen, wodurch die Gleichung (4) erhalten bleibt. —

Da, wenn $\mathfrak{a}$, $\mathfrak{n}$ irgendwelche Moduln bedeuten, immer $(\mathfrak{n}, \mathfrak{a}) = (\mathfrak{n}, \mathfrak{a} - \mathfrak{n}) = (\mathfrak{a} + \mathfrak{n}, \mathfrak{a})$ ist (§ 171), so können wir den in (1) enthaltenen Satz auch so aussprechen:

---

*) Im entgegengesetzten Falle ist offenbar $\mathfrak{c} = 0 = [0]$.

III. Ist $\mathfrak{n}$ ein eingliedriger, und $\mathfrak{a}$ ein beliebiger Modul, so ist

(8) $$\mathfrak{a} - \mathfrak{n} = (\mathfrak{n}, \mathfrak{a})\ \mathfrak{n} = (\mathfrak{a} + \mathfrak{n}, \mathfrak{a})\ \mathfrak{n}.$$

Derselbe dient zum Beweise des folgenden:

IV. Ist der letzte der drei Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{n}$ eingliedrig $= [\omega]$, so kann man einen eingliedrigen Modul $\mathfrak{n}' = [\alpha']$ so wählen, daß

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

wird.

Dies läßt sich in der Tat immer auf folgende Weise erreichen. Setzen wir zur Abkürzung

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

so ist zufolge (8)

(11) $$(\mathfrak{a} + \mathfrak{b}) - \mathfrak{n} = \mathfrak{a}\mathfrak{n} = [\mathfrak{a}\omega];$$

da nun $\mathfrak{a}\omega$ in $\mathfrak{a} + \mathfrak{b}$ enthalten ist, so kann man eine Zahl α' in $\mathfrak{a}$ und eine Zahl β' in $\mathfrak{b}$ so wählen, daß

(12) $$\mathfrak{a}\omega = \alpha' - \beta', \text{ also } \alpha' = \beta' + \mathfrak{a}\omega$$

wird, und wir wollen beweisen, daß der eingliedrige Modul $\mathfrak{n}' = [\alpha']$ die Gleichung (9) erfüllt. Hierzu bezeichnen wir deren linke und rechte Seite bzw. mit $\mathfrak{p}$, $\mathfrak{q}$, und wir haben zu zeigen, daß $\mathfrak{p}$ durch $\mathfrak{q}$, und $\mathfrak{q}$ durch $\mathfrak{p}$ teilbar ist. Das Erstere ergibt sich daraus, daß jede in $\mathfrak{p}$ enthaltene Zahl von der Form $\alpha = \beta + \nu$ ist, wo α, β, ν bzw. Zahlen der Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{n}$ bedeuten; denn hieraus folgt zunächst, daß die Zahl $\alpha - \beta = \nu$ in $(\mathfrak{a} + \mathfrak{b}) - \mathfrak{n}$ enthalten, also zufolge (11) und (12) auch $= x\,(\alpha' - \beta')$ ist, wo x eine ganze rationale Zahl bedeutet, und folglich ist die Zahl $\mu = \alpha - x\alpha' = \beta - x\beta'$ in $\mathfrak{a} - \mathfrak{b}$ enthalten; mithin ergibt sich, daß jede in $\mathfrak{p}$ enthaltene Zahl $\alpha = \mu + x\alpha'$ auch in $\mathfrak{q}$ enthalten, also wirklich $\mathfrak{p}$ durch $\mathfrak{q}$ teilbar ist. Umgekehrt leuchtet ein, daß $\mathfrak{a} - \mathfrak{b}$ durch jeden der beiden Moduln $\mathfrak{a}$ und $\mathfrak{b} + \mathfrak{n}$, also auch durch $\mathfrak{p}$ teilbar, und da dasselbe zufolge (12) von dem Modul $\mathfrak{n}' = [\alpha']$ gilt, so muß auch der größte gemeinsame Teiler von $\mathfrak{a} - \mathfrak{b}$ und $\mathfrak{n}'$, d. h. $\mathfrak{q}$ durch $\mathfrak{p}$ teilbar sein. Mithin ist $\mathfrak{p} = \mathfrak{q}$, was zu beweisen war. Hieraus folgt der Satz:

V. Jedes Vielfache eines n-gliedrigen Moduls ist ein n-gliedriger Modul.

Für eingliedrige Moduln ergibt sich derselbe aus (1) oder (8). Da ferner, wenn $n > 1$, jeder n-gliedrige Modul $\mathfrak{o} = \mathfrak{b} + \mathfrak{n}$ gesetzt

werden kann, wo $\mathfrak{n}$ eingliedrig, $\mathfrak{b}$ aber $(n-1)$-gliedrig ist, und da wir annehmen dürfen, der Satz sei schon für jedes Vielfache $\mathfrak{a} - \mathfrak{b}$ von $\mathfrak{b}$ bewiesen, so folgt aus (9), daß er auch für jedes Vielfache $\mathfrak{a} - \mathfrak{o}$ von $\mathfrak{o}$, also allgemein gilt, w. z. b. w.

Es ist aber von Wichtigkeit, wenn irgendein n-gliedriger Modul

$$\mathfrak{o} = [\omega_1, \omega_2, \ldots, \omega_n] \tag{13}$$

gegeben ist, die Basis des Vielfachen $\mathfrak{a} - \mathfrak{o}$ nach den in (10) und (12) enthaltenen Vorschriften wirklich herzustellen. Zu diesem Zweck setzen wir, wenn r irgendeine Zahl aus der Reihe $1, 2, \ldots, n$ ist,

$$\mathfrak{o}_r = [\omega_1, \omega_2, \ldots, \omega_r], \tag{14}$$

und wenden den Satz (9) auf das Beispiel $\mathfrak{b} = \mathfrak{o}_{r-1}$, $\omega = \omega_r$ an, woraus $\mathfrak{n} = [\omega_r]$, $\mathfrak{b} + \mathfrak{n} = \mathfrak{o}_r$ folgt; bezeichnen wir zugleich die Basis α' des Moduls $\mathfrak{n}'$ mit α_r, so erhalten wir:

$$\mathfrak{a} - \mathfrak{o}_r = (\mathfrak{a} - \mathfrak{o}_{r-1}) + [\alpha_r],$$

und da $\mathfrak{o}_n = \mathfrak{o}$, $\mathfrak{o}_0 = 0$ zu setzen ist, so ergibt sich:

$$\mathfrak{a} - \mathfrak{o} = \Sigma[\alpha_r] = [\alpha_1, \alpha_2, \ldots, \alpha_n]. \tag{15}$$

Um die Zahlen α_r zu bestimmen, setzen wir nach (10):

$$(\mathfrak{a} + \mathfrak{o}_r, \mathfrak{a} + \mathfrak{o}_{r-1}) = a_r^{(r)}; \tag{16}$$

dann folgt aus (12), weil β' in $\mathfrak{b}$, d. h. in $\mathfrak{o}_{r-1}$ enthalten ist, die Darstellung:

$$\alpha_r = a_1^{(r)}\omega_1 + a_2^{(r)}\omega_2 + \cdots + a_{r-1}^{(r)}\omega_{r-1} + a_r^{(r)}\omega_r, \tag{17}$$

wo alle Koeffizienten $a_s^{(r)}$ ganze rationale Zahlen bedeuten, und $a_s^{(r)} = 0$ ist, wenn $s > r$. Multipliziert man die n Gleichungen (16) miteinander und bedenkt, daß $\mathfrak{a} + \mathfrak{o}_r$ ein Teiler von $\mathfrak{a} + \mathfrak{o}_{r-1}$ ist, so ergibt sich mit Rücksicht auf die Sätze (5), (3), (2) in § 171 die wichtige Beziehung:

$$(\mathfrak{a} + \mathfrak{o}, \mathfrak{a}) = (\mathfrak{o}, \mathfrak{a}) = (\mathfrak{o}, \mathfrak{a} - \mathfrak{o}) = a_1' a_2'' \ldots a_n^{(n)}, \tag{18}$$

wo das Produkt rechter Hand zugleich die Determinante der n^2 Koeffizienten $a_s^{(r)}$ ist. Diese Zahl $(\mathfrak{o}, \mathfrak{a})$ ist von Null verschieden, wenn keine der n Zahlen $a_r^{(r)}$ in (16) verschwindet, und bedeutet dann die Anzahl der in $\mathfrak{o}$ enthaltenen, nach $\mathfrak{a}$ inkongruenten Zahlen ω'; erinnert man sich der Bedeutung des obigen Restsystems (2), und läßt $x_1, x_2, \ldots, x_n$ alle ganzen Zahlen durchlaufen, welche den Bedingungen

$$0 \leqq x_r < a_r^{(r)} \tag{19}$$

genügen, so folgt aus den genannten Sätzen des vorigen Paragraphen leicht, daß die entsprechenden Zahlen

$$\omega' = x_1\omega_1 + x_2\omega_2 + \cdots + x_n\omega_n \tag{20}$$

ein Restsystem von $\mathfrak{o}$ nach $\mathfrak{a}$ bilden*). —

Die in (4) enthaltene Zurückführung einer mehrgliedrigen Basis auf eine eingliedrige bildet nur einen besonderen Fall eines sehr wichtigen allgemeinen Satzes, in welchem der Begriff des endlichen Moduls sich mit dem des irreduziblen Systems (§ 164) verbindet; wir bemerken aber (wie schon am Schluß von § 167), daß dieser letztere Begriff hier und in der Folge stets auf den Körper der rationalen Zahlen zu beziehen ist. Unser Satz lautet:

VI. Jeder endliche, von Null verschiedene Modul besitzt eine irreduzible Basis.

Um dies zu beweisen, nehmen wir an, es liege ein m-gliedriger Modul

$$\mathfrak{a} = [\mu_1, \mu_2, \ldots, \mu_m] \tag{21}$$

mit einer reduziblen Basis vor, welche aus m Zahlen μ_s besteht, die nicht alle verschwinden. Bedeutet nun n die größte Anzahl voneinander unabhängiger Zahlen, die man aus diesen m Zahlen μ_s und folglich (nach § 164) aus dem Modul $\mathfrak{a}$ auswählen kann, so lassen sie sich sämtlich in der Form

$$\mu_s = c_1^{(s)}\omega_1 + c_2^{(s)}\omega_2 + \cdots + c_n^{(s)}\omega_n \tag{22}$$

darstellen, wo die n Zahlen ω_r ein irreduzibles System bilden, und die $m\,n$ Koeffizienten $c_r^{(s)}$ ganze rationale Zahlen sind; denn da wir annehmen dürfen, daß z. B. die ersten n Zahlen $\mu_1, \mu_2, \ldots, \mu_n$ ein irreduzibles System bilden, so ist jede der m Zahlen μ_s, weil sie mit jenen ein reduzibles System bildet, von der Form

$$\mu_s = e_1^{(s)}\mu_1 + e_2^{(s)}\mu_2 + \cdots + e_n^{(s)}\mu_n,$$

wo die $m\,n$ Koeffizienten $e_r^{(s)}$ rationale, im allgemeinen gebrochene Zahlen bedeuten; nun kann man immer eine natürliche Zahl c so wählen, daß alle Produkte $c\,e_r^{(s)}$ ganze Zahlen $c_r^{(s)}$ werden, und wenn man

$$\mu_1 = c\,\omega_1, \quad \mu_2 = c\,\omega_2, \ldots, \quad \mu_n = c\,\omega_n$$

setzt, so nehmen die vorhergehenden Gleichungen wirklich die Form (22) an, und die n Zahlen ω_r bilden ebenfalls ein irreduzibles System.

*) Vgl. das Beispiel in § 159, S. 13 bis 15.

Nachdem dies nachgewiesen ist, leuchtet ein, daß der Modul $\mathfrak{a}$ durch den n-gliedrigen Modul (13) teilbar und folglich selbst ein n-gliedriger Modul von der Form (15) ist, dessen Basis aus n Zahlen α_r von der Form (17) besteht und gewiß irreduzibel ist, weil sonst je n Zahlen in $\mathfrak{a}$ ein reduzibles System bilden würden, w. z. b. w.

An den Beweis des vorstehenden Satzes knüpfen wir die folgende Beschreibung eines einfachen Verfahrens*), durch welches man die aus m gegebenen Zahlen μ_s von der Form (22) bestehende Basis des Moduls $\mathfrak{a}$ in eine irreduzible, aus n Zahlen α_r von der Form (17) bestehende Basis überführen kann. Die m Koeffizienten c'_n, c''_n, ..., $c_n^{(m)}$, mit welchen die letzte Zahl ω_n in den m Gleichungen (22) multipliziert ist, können gewiß nicht alle verschwinden, weil sonst (nach § 164, III) schon je n der m Zahlen μ_s ein reduzibles System bilden würden; sind nun von diesen m Koeffizienten $c_n^{(s)}$ mindestens zwei von Null verschieden, z. B. c'_n und c''_n, und ist (absolut genommen) $c'_n \geqq c''_n$, so kann man (nach § 4) die ganze rationale Zahl x so wählen, daß $c'_n + x\,c''_n < c''_n$, also auch $< c'_n$ wird. Nun bleibt offenbar der Modul $\mathfrak{a}$ in (21) ungeändert, wenn man das erste Glied μ_1 seiner Basis durch $\mu_1 + x\,\mu_2$ ersetzt, alle anderen μ_2, μ_3, ..., μ_m aber beibehält, d. h. es ist

$$(23) \qquad \mathfrak{a} = [\mu_1, \mu_2, \ldots, \mu_m] = [\mu_1 + x\,\mu_2, \mu_2, \ldots, \mu_m];$$

hiermit ist das System der $m\,n$ Koeffizienten $c_r^{(s)}$ in (22) nur insofern abgeändert, als an Stelle der n Koeffizienten c'_r die Koeffizienten $c'_r + x\,c''_r$ getreten sind, und von diesen ist der letzte $c'_n + x\,c''_n$ absolut kleiner als der frühere c'_n. Durch wiederholte Anwendung solcher elementaren Transformationen (23) wird man endlich zu einer neuen Basis von m Gliedern gelangen, von denen $m - 1$ in dem nach (14) mit $\mathfrak{o}_{n-1}$ zu bezeichnenden Modul enthalten sind, während ein einziges Glied α_n von der Form (17) ist, und zwar kann man den Koeffizienten $a_n^{(n)}$, welcher offenbar der größte gemeinsame Teiler der m Koeffizienten $c_n^{(s)}$ ist, positiv annehmen, weil α_n auch durch $-\alpha_n$ ersetzt werden darf. In derselben Weise kann man nun, indem man α_n ungeändert läßt, die übrigen, in $\mathfrak{o}_{n-1}$ enthaltenen $m - 1$ Glieder der neuen Basis transformieren, bis alle Koeffizienten von ω_{n-1} mit Ausnahme eines einzigen $a_{n-1}^{(n-1)}$ verschwinden, welcher in einem Gliede α_{n-1}

*) Die Kenntnis desselben ist unerläßlich für diejenigen, welche bestimmte Beispiele in der Theorie der Moduln und Ideale zu berechnen haben. Vgl. § 176.

auftritt. Durch Fortsetzung dieses Verfahrens gelangt man endlich zu einer Basis von m Gliedern, unter denen sich n Zahlen α_r von der Form (17) befinden, während die übrigen $m - n$ Glieder $= 0$ sind und deshalb gänzlich unterdrückt werden dürfen.

Nachdem auf diese Weise die Basis (22) wirklich durch eine Kette elementarer Transformationen (23), von denen sich mehrere auch gleichzeitig ausführen lassen, in eine Basis (17) übergeführt ist, in welcher die n Koeffizienten $a_r^{(r)}$ (nach § 164, III) von Null verschieden sind und als positiv angenommen werden dürfen, während alle Koeffizienten $a_s^{(r)} = 0$ sind, in denen $s > r$, kann man offenbar durch fernere Anwendung von elementaren Transformationen (23) noch erreichen, daß alle anderen Koeffizienten, in denen $s < r$, der Bedingung $0 \leqq a_s^{(r)} < a_s^{(s)}$ genügen, und man überzeugt sich leicht, daß hierdurch das System der Koeffizienten $a_s^{(r)}$ vollständig bestimmt ist, daß also der Modul $\mathfrak{a}$ nur eine einzige solche Basis besitzt. Außerdem leuchtet ein, daß das ganze Verfahren auch auf den Fall anwendbar ist, wo $m = n$, also der Modul $\mathfrak{a}$ schon in (21) durch eine irreduzible Basis dargestellt ist. Ein Beispiel, auf welches wir später (in § 176) zurückkommen werden, möge zur Erläuterung dienen:

$$\begin{aligned}
&[21\,\omega_1,\ 12\,\omega_1 + 3\,\omega_2,\ 14\,\omega_1 + 7\,\omega_2,\ 3\,\omega_1 + 6\,\omega_2] \\
&= [21\,\omega_1,\ 12\,\omega_1 + 3\,\omega_2,\ -10\,\omega_1 + \omega_2,\ -21\,\omega_1] \\
&= [21\,\omega_1,\ 42\,\omega_1,\ -10\,\omega_1 + \omega_2,\ -21\,\omega_1] \\
&= [21\,\omega_1,\ 0,\ -10\,\omega_1 + \omega_2,\ 0] \\
&= [21\,\omega_1,\ -10\,\omega_1 + \omega_2] = [21\,\omega_1,\ 11\,\omega_1 + \omega_2].
\end{aligned}$$

Ähnlich findet man:

$$[21\,\omega_1, 7\,\omega_1 + 7\,\omega_2, 9\,\omega_1 + 3\,\omega_2, -2\,\omega_1 + 4\,\omega_2] = [21\,\omega_1,\ 10\,\omega_1 + \omega_2]$$
$$[3\,\omega_1,\ \omega_1 + \omega_2,\ 2\,\omega_1 + \omega_2,\ -\omega_1 + \omega_2] = [\omega_1,\ \omega_2]$$
$$[7\,\omega_1,\ 3\,\omega_1 + \omega_2,\ 4\,\omega_1 + \omega_2,\ \omega_1 + \omega_2] = [\omega_1,\ \omega_2]$$
$$[\omega_1 + 2\,\omega_2, -10\,\omega_1 + \omega_2] = [21\,\omega_1,\ 11\,\omega_1 + \omega_2]$$
$$[\omega_1 - 2\,\omega_2,\ 10\,\omega_1 + \omega_2] = [21\,\omega_1,\ 10\,\omega_1 + \omega_2].$$

Wenn nun ein Modul $\mathfrak{a}$, welcher durch (21) und (22) als Vielfaches des Moduls $\mathfrak{o}$ in (13) dargestellt wird, durch das angegebene Verfahren in die Form (15) übergeführt ist, so folgt aus (18) auch der Wert der Klassenanzahl $(\mathfrak{o}, \mathfrak{a})$; aber es ist sehr wichtig, daß man dieselbe auch unmittelbar aus den Koeffizienten $c_r^{(s)}$ in (22), nämlich durch die aus ihnen gebildeten Determinanten n^{ten} Grades bestimmen kann. Bedeutet σ irgendeine Kombination von n der m

Zahlen $s = 1, 2 \ldots m$, so wollen wir mit $C(\sigma)$ die entsprechende Determinante bezeichnen, welche aus den n^2 zugehörigen Koeffizienten $c_r^{(s)}$ gebildet und natürlich eine ganze rationale Zahl ist; die Anzahl dieser Kombinationen σ und Determinanten $C(\sigma)$ ist bekanntlich

$$= \frac{m(m-1)\ldots(m-n+1)}{1 \cdot 2 \quad \ldots \quad n}.$$

Wie verändern sich nun diese Determinanten bei der in (23) dargestellten Transformation der Basis? Bezeichnet man mit σ_1 alle diejenigen Kombinationen σ, in denen die Zahl 1, aber nicht 2 auftritt, und mit σ_2 alle anderen Kombinationen, so leuchtet ein, daß, wenn μ_1 durch $\mu_1 + x\mu_2$ ersetzt wird, alle Determinanten $C(\sigma_2)$ ungeändert bleiben, während $C(\sigma_1)$ in eine Summe von der Form $C(\sigma_1) + xC(\sigma_2)$ übergeht. Hieraus folgt offenbar, daß der größte gemeinsame Teiler C aller Determinanten $C(\sigma)$ vor wie nach der Transformation (23) derselbe ist und folglich bis zum Schlusse des ganzen Verfahrens ungeändert erhalten bleibt. Da nun die letzte Basis aus den n Zahlen α_r in (17) und aus $m - n$ Nullen besteht, so gibt es nur noch eine einzige von Null verschiedene Determinante (18), und folglich ist

$$(\mathfrak{o}, \mathfrak{a}) = C. \tag{24}$$

Bei dem Beweise dieses Satzes haben wir eben nur die einfachsten Sätze über Determinanten benutzt; zu demselben Resultate gelangt man auch auf folgendem Wege, der etwas tiefere Kenntnisse voraussetzt. Die doppelte Darstellung desselben Moduls $\mathfrak{a}$ durch (21) und (15) ist nach der Bedeutung unserer Symbole nur ein kurzer Ausdruck dafür, daß m Gleichungen

$$\mu_s = p_1^{(s)}\alpha_1 + p_2^{(s)}\alpha_2 + \cdots + p_n^{(s)}\alpha_n \tag{25}$$

und n Gleichungen

$$\alpha_r = q_r'\mu_1 + q_r''\mu_2 + \cdots + q_r^{(m)}\mu_m \tag{26}$$

bestehen, wo alle Koeffizienten $p_r^{(s)}$ und $q_r^{(s)}$ ganze rationale Zahlen bedeuten*). Da nun die n Zahlen α_r ein irreduzibles System bilden, so ergibt sich durch Substitution von (25) in (26), daß die Summe

$$p_t'q_r' + p_t''q_r'' + \cdots + p_t^{(m)}q_r^{(m)} = 1 \text{ oder } = 0 \tag{27}$$

*) Das oben beschriebene Verfahren liefert durch Zusammensetzung aller Transformationen (23) und deren Umkehrung immer ein solches System von Koeffizienten p, q; die allgemeinste Lösung der Aufgabe, alle solche Systeme zu finden,

ist, je nachdem die in der Reihe 1, 2...n enthaltenen Zahlen t, r gleich oder verschieden sind. Hieraus folgt nach einem bekannten Satze der Determinanten-Theorie die Gleichung

$$\Sigma P(\sigma) Q(\sigma) = 1, \tag{28}$$

wo σ jede Kombination von n der m Zahlen $s = 1, 2 \ldots m$ durchläuft, und $P(\sigma)$, $Q(\sigma)$ die zugehörigen, aus den Koeffizienten $p_r^{(s)}$, $q_r^{(s)}$ gebildeten Determinanten n^{ten} Grades bedeuten; mithin sind die Determinanten $P(\sigma)$ — und ebenso die Determinanten $Q(\sigma)$ — Zahlen ohne gemeinsamen Teiler. Substituiert man ferner (17) in (25), so folgt durch Vergleichung mit (22):

$$c_r^{(s)} = p_1^{(s)} a_r' + p_2^{(s)} a_r'' + \cdots + p_n^{(s)} a_r^{(n)}, \tag{29}$$

und hieraus mit Rücksicht auf (18):

$$C(\sigma) = (\mathfrak{o}, \mathfrak{a}) P(\sigma), \tag{30}$$

wodurch unser Satz (24) abermals bewiesen ist.

Wir wenden uns nun noch zu dem wichtigen Fall $m = n$ und sprechen den besonderen, in (24) enthaltenen Satz*) so aus:

VII. Sind die irreduziblen Basen zweier n-gliedrigen Moduln

$$\mathfrak{o} = [\omega_1, \omega_2, \ldots, \omega_n], \quad \mathfrak{a} = [\mu_1, \mu_2, \ldots, \mu_n]$$

durch n Gleichungen von der Form

$$\mu_s = c_1^{(s)} \omega_1 + c_2^{(s)} \omega_2 + \cdots + c_n^{(s)} \omega_n$$

miteinander verbunden, wo die Koeffizienten $c_r^{(s)}$ ganze rationale Zahlen bedeuten, so ist deren Determinante

$$C = \pm (\mathfrak{o}, \mathfrak{a}). \tag{31}$$

Wir schließen diesen, der Modultheorie gewidmeten Abschnitt mit der folgenden Betrachtung. Es leuchtet ein, daß jeder von Null

---

besteht in der Verallgemeinerung einer Methode, welche von Gauß in einigen besonderen Fällen angewendet ist (D. A. artt. 234, 236, 279). Der Fall $n = 1$ ist oben schon in den Gleichungen (4) bis (7) behandelt.

*) Wenn unter den Elementen $c_r^{(s)}$ der Determinante C sich auch gebrochene rationale Zahlen befinden, also $\mathfrak{a}$ nicht teilbar durch $\mathfrak{o}$ ist, so gilt der allgemeinere Satz $(\mathfrak{o}, \mathfrak{a}) = \pm (\mathfrak{a}, \mathfrak{o})\, C$, und zwar ist der umgekehrte Wert von $(\mathfrak{a}, \mathfrak{o})$ vollständig bestimmt als der größte gemeinsame Teiler der Determinante C und aller ihrer Unterdeterminanten, zu denen auch die Zahl 1 als Determinante 0ten Grades zu rechnen ist; dies ergibt sich leicht aus den obigen Sätzen durch Betrachtung des Moduls $\mathfrak{a} + \mathfrak{o}$. Ist endlich $C = 0$, so bilden die n Zahlen μ_s ein reduzibles System, und die Gleichung (31) bleibt gültig.

verschiedene Modul n — mag er endlich sein oder nicht — unendlich viele verschiedene Vielfache m besitzt, und daß man sogar unendliche Ketten von solchen Vielfachen m, m_1, m_2 ... bilden kann, deren jedes ein echter Teiler des nächstfolgenden ist; denn wenn ω eine beliebige, von Null verschiedene Zahl in n bedeutet, so bilden die Moduln $[\omega]$, $[2\omega]$, $[4\omega]$, $[8\omega]$ ... offenbar eine solche Kette. Es wird daher auf den ersten Blick vielleicht auffallen, daß ein endlicher Modul n keine unendliche Kette von Vielfachen a_1, a_2, a_3 ... besitzen kann, in welcher jeder Modul ein echtes Vielfaches des nächstfolgenden wäre. In der Tat besteht folgender Satz, von welchem wir bald (in § 173) eine wichtige Anwendung machen werden:

VIII. Sind alle Moduln der unendlichen Kette a_1, a_2, a_3 ... teilbar durch den endlichen Modul n, und ist jeder von ihnen teilbar durch den nächstfolgenden, so sind von einer bestimmten Stelle an alle folgenden Moduln a_n, a_{n+1}, a_{n+2} ... miteinander identisch.

Denn der größte gemeinsame Teiler aller dieser Moduln a, den man (nach § 169) zweckmäßig durch a_∞ bezeichnen kann, ist teilbar durch ihren gemeinsamen Teiler n, mithin ebenfalls ein endlicher Modul $[\alpha_1, \alpha_2, \ldots, \alpha_m]$, und da jede in a_∞ enthaltene Zahl auch in einem Modul a_r und folglich in allen folgenden a_{r+1}, a_{r+2} ... enthalten ist, so muß es auch einen solchen Modul a_n geben, welcher die sämtlichen m Zahlen α_1, α_2, ..., α_m enthält, aus denen die Basis von a_∞ besteht; dann ist a_∞ teilbar durch a_n, und da umgekehrt a_n durch a_∞ teilbar ist, so muß a_n und ebenso jeder folgende Modul a_{n+1}, a_{n+2} ... mit a_∞ identisch sein, w. z. b. w.

§ 173.

Wir nennen, wie schon früher (am Schluß von § 167) bemerkt ist, eine Zahl ω eine algebraische Zahl schlechthin, wenn die hinreichend weit fortgesetzte Reihe der Potenzen $1, \omega, \omega^2, \ldots, \omega^{n-1}, \omega^n$ ein reduzibles System bildet, d. h. wenn ω einer Gleichung von der Form

$$\omega^n + a_1\omega^{n-1} + \cdots + a_{n-1}\omega + a_n = 0 \tag{1}$$

genügt, deren Koeffizienten a_r rationale Zahlen sind. Indem wir uns jetzt dem eigentlichen Gegenstande unserer Untersuchung zuwenden, teilen wir den unendlichen Körper aller algebraischen Zahlen in zwei

wesentlich verschiedene Teile ein: wir nennen eine solche Zahl ω eine ganze algebraische Zahl oder kürzer eine ganze Zahl*), wenn sie einer Gleichung von der Form (1) genügt, deren höchster Koeffizient $= 1$, und deren übrige Koeffizienten a_r ganze rationale Zahlen sind; jede andere algebraische Zahl soll eine gebrochene Zahl heißen.

Vor allem müssen wir uns versichern, daß der neue, erweiterte Begriff der ganzen Zahl mit dem alten, engeren Sinne desselben Wortes niemals in Widerspruch geraten kann. Bezeichnen wir auch ferner mit $\mathfrak{z}$ den Inbegriff [1] aller ganzen rationalen Zahlen, so leuchtet zunächst ein, daß jede solche Zahl a auch eine ganze algebraische Zahl ω, nämlich die Wurzel der Gleichung $\omega - a = 0$ ist; wir müssen aber auch umgekehrt beweisen, daß jede ganze algebraische Zahl ω, welche zugleich dem Körper R der rationalen Zahlen angehört, auch in $\mathfrak{z}$ enthalten ist. Dies geschieht leicht auf folgende Weise. Da ω eine ganze algebraische Zahl ist, so genügt sie einer Gleichung von der Form (1) mit ganzen rationalen Koeffizienten a_r; da sie zugleich rational, also ein Quotient ist, dessen Zähler b und Nenner c in $\mathfrak{z}$ enthalten und zwar relative Primzahlen sind, so ergibt sich durch Multiplikation der Gleichung (1) mit c^n, daß die Potenz b^n, welche ebenfalls relative Primzahl zu c ist, durch c teilbar ist; mithin muß $c = \pm 1$, also $\omega = \pm b$ sein, w. z. b. w.

Genau auf dieselbe Weise würde sich zeigen lassen, daß jede ganze algebraische Zahl ω, welche dem in § 159 behandelten Körper J angehört, notwendig eine ganze komplexe Zahl, d. h. in dem Modul $[1, i]$ enthalten ist, und umgekehrt leuchtet ein, daß jede solche ganze komplexe Zahl $\omega = x + y\,i$ eine Wurzel der Gleichung

$$\omega^2 - 2\,x\,\omega + (x^2 + y^2) = 0$$

und folglich eine ganze algebraische Zahl ist.

Um jedes Mißverständnis zu verhüten, bemerken wir ferner, daß, wenn unter den rationalen Koeffizienten a_r in (1) sich auch gebrochene Zahlen befinden, dennoch ω eine ganze Zahl sein, also einer anderen Gleichung mit lauter ganzen Koeffizienten genügen kann. So z. B. genügt die Zahl $\omega = \sqrt{2} = 1,414\ldots$ der Gleichung

$$\omega^3 + {}^1/_2\,\omega^2 - 2\,\omega - 1 = 0,$$

*) Vgl. § 160 der zweiten Auflage dieses Werkes (1871, vgl. XLVII); ob dieselben Benennungen schon früher in diesem Sinne gebraucht sind, ist mir nicht bekannt.

in welcher ein Koeffizient gebrochen ist; sie genügt aber auch der Gleichung $\omega^2 - 2 = 0$ und ist folglich eine ganze Zahl. Doch werden wir am Schlusse dieses Paragraphen beweisen, daß die Gleichung (1), wenn sie eine ganze Wurzel ω besitzt und zugleich irreduzibel ist, notwendig lauter ganze Koeffizienten a_r haben muß; und aus diesem Satze folgt offenbar wieder das, was wir eben über die ganzen Zahlen der Körper R und J bemerkt haben.

Wenn aber ω eine gebrochene Zahl ist, und folglich die Koeffizienten a_r der Gleichung (1) nicht alle ganz sind, so kann man eine natürliche Zahl c so wählen, daß die Produkte $c a_r$, also auch die Produkte $b_r = a_r c^r$ ganze Zahlen werden; multipliziert man nun (1) mit c^n und setzt $c\omega = \beta$, so erhält man

$$\beta^n + b_1 \beta^{n-1} + \cdots + b_{n-1}\beta + b_n = 0,$$

und folglich ist β eine ganze Zahl. Wir können daher folgenden Satz aussprechen:

I. Jede gebrochene Zahl läßt sich durch Multiplikation mit einer natürlichen Zahl in eine ganze Zahl verwandeln.

Unsere obige Erklärung einer ganzen Zahl läßt sich nun, wenn man die Begriffe und Bezeichnungen der vorausgeschickten Theorie der Moduln zuzieht, in mehrere Formen bringen, die für die nächsten Beweisführungen von großem Nutzen sind. Setzen wir zur Abkürzung den aus einer beliebigen Zahl ω gebildeten m-gliedrigen Modul

$$[\omega^{m-1}, \omega^{m-2}, \ldots, \omega, 1] = (\omega)_m, \tag{2}$$

so ist $(\omega)_m$ stets teilbar durch $(\omega)_{m+1} = [\omega^m] + (\omega)_m$; ist aber ω eine ganze Zahl, also eine Wurzel einer Gleichung von der Form (1) mit ganzen rationalen Koeffizienten a_r, so ist ω^n in $(\omega)_n$ enthalten, also $(\omega)_{n+1}$ teilbar durch $(\omega)_n$, und folglich

$$(\omega)_n = (\omega)_{n+1}; \tag{3}$$

umgekehrt folgt aus einer solchen Identität (3) offenbar, daß ω einer Gleichung (1) mit ganzen rationalen Koeffizienten a_r genügt, also eine ganze Zahl ist. Zugleich leuchtet ein, daß dann auch alle folgenden Moduln $(\omega)_{n+2}, (\omega)_{n+3}, \ldots$ mit $(\omega)_n$ identisch sind.

Ein endlicher, von Null verschiedener Modul $\mathfrak{a}$ soll im folgenden eine Hülle der Zahl ω heißen, wenn $\mathfrak{a}\omega > \mathfrak{a}$, also ω in der Ordnung $\mathfrak{a}^0$ enthalten ist (§ 170); dann wird der Charakter einer ganzen

Zahl auf die einfachste Weise durch den folgenden Satz*) ausgesprochen:

II. Eine Zahl ist dann und nur dann eine ganze Zahl, wenn sie eine Hülle besitzt.

Der Beweis des zweiten Teils ergibt sich leicht aus dem Vorhergehenden; denn wenn ω eine ganze Zahl ist, so besteht eine Identität von der Form (3), und da $(\omega)_{n+1} = \omega(\omega)_n + \zeta$ stets ein Teiler des Produktes $\omega(\omega)_n$ ist, so ist $(\omega)_n$ eine Hülle von ω. Um auch den ersten Teil zu beweisen, nehmen wir an, der von Null verschiedene Modul

$$\mathfrak{a} = [\alpha_1, \alpha_2, \ldots, \alpha_n]$$

sei eine Hülle der Zahl ω, d. h. es bestehen n Gleichungen von der Form

$$\omega\,\alpha_r = a_{r,1}\alpha_1 + a_{r,2}\alpha_2 + \cdots + a_{r,n}\alpha_n,$$

wo alle Koeffizienten $a_{r,s}$ ganze rationale Zahlen bedeuten; da nun die n Zahlen α_r nicht alle verschwinden, so ergibt sich durch ihre Elimination bekanntlich die Determinanten-Gleichung

$$\begin{vmatrix} a_{1,1} - \omega & \ldots & a_{1,n} \\ \cdot & \cdots & \cdot \\ a_{n,1} & \ldots & a_{n,n} - \omega \end{vmatrix} = 0,$$

deren Entwicklung offenbar zu einer Gleichung von der Form (1) mit ganzen rationalen Koeffizienten a_r führt, und folglich ist ω eine ganze Zahl, w. z. b. w.

So kurz sich dieser Beweis durch die Zuziehung der Theorie der Determinanten gestaltet, so muß man doch zugestehen, daß diese Theorie dem eigentlichen Inhalte des Satzes gänzlich fern steht; es wird daher hoffentlich nicht überflüssig erscheinen, wenn wir diesen Teil des Satzes und seinen Beweis in die folgende Form einkleiden:

III. Die Ordnung $\mathfrak{a}^0$ eines jeden endlichen, von Null verschiedenen Moduls $\mathfrak{a}$ ist ebenfalls ein solcher Modul und besteht aus lauter ganzen Zahlen ω.

Wählt man aus $\mathfrak{a}$ irgendeine von Null verschiedene Zahl α und bedenkt, daß nach dem Satze (23) in § 170 immer $\mathfrak{a}\,\mathfrak{a}^0 = \mathfrak{a}$ ist, so folgt $\alpha\,\mathfrak{a}^0 > \mathfrak{a}$, mithin ist $\mathfrak{a}^0$ teilbar durch den endlichen Modul $\mathfrak{a}\,\alpha^{-1}$ und folglich (nach § 172) ebenfalls ein endlicher Modul. Da

*) Vgl. die Anmerkung zu S. 481 — 482 in der dritten Auflage dieses Werkes (1879).

(nach § 170) jede Ordnung ein Teiler des Moduls $\mathfrak{z}$ ist, und die in ihr enthaltenen Zahlen sich auch durch Multiplikation reproduzieren, so sind, wenn ω eine Zahl in $\mathfrak{a}^0$ bedeutet, alle in (2) definierten Moduln $(\omega)_m$ teilbar durch $\mathfrak{a}^0$, und da zugleich jeder solche Modul $(\omega)_m$ durch den nächstfolgenden $(\omega)_{m+1}$ teilbar ist, so muß nach dem Schlußsatze des vorigen Paragraphen endlich eine Identität von der Form (3) eintreten, und folglich ist ω eine ganze Zahl, w. z. b. w.

Hieraus geht auch hervor, daß gleichzeitig mit dem Modul $\mathfrak{a}$ auch dessen Ordnung $\mathfrak{a}^0$ eine Hülle der Zahl ω ist, weil $\mathfrak{a}^0$ ein endlicher, von Null verschiedener Modul ist, dessen Zahlen sich durch Multiplikation reproduzieren, so daß auch $\omega\,\mathfrak{a}^0 > \mathfrak{a}^0$ ist. Wichtiger ist aber die andere Bemerkung, daß, wenn $\mathfrak{n}$ einen willkürlichen endlichen, von Null verschiedenen Modul bedeutet, auch das Produkt $\mathfrak{a}\,\mathfrak{n}$ eine Hülle von ω ist, weil aus $\mathfrak{a}\,\omega > \mathfrak{a}$ auch $\mathfrak{a}\,\mathfrak{n}\,\omega > \mathfrak{a}\,\mathfrak{n}$ folgt. Sind daher $\alpha_1, \alpha_2, \ldots, \alpha_n$ irgendwelche ganze Zahlen in endlicher Anzahl, die bzw. die Hüllen $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ besitzen, so ist das Produkt $\mathfrak{a} = \mathfrak{a}_1\,\mathfrak{a}_2 \ldots \mathfrak{a}_n$ eine gemeinsame Hülle dieser Zahlen. Hieraus ergeben sich unmittelbar die folgenden Sätze:

IV. Die ganzen Zahlen reproduzieren sich durch Addition, Subtraktion und Multiplikation.

Denn je zwei ganze Zahlen α_1, α_2 besitzen eine gemeinsame Hülle $\mathfrak{a}$ und sind folglich in deren Ordnung $\mathfrak{a}^0$ enthalten; da nun diese Ordnung $\mathfrak{a}^0$ (nach III) aus lauter ganzen Zahlen besteht, die sich (nach § 170) durch Addition, Subtraktion, Multiplikation reproduzieren, so sind auch die Zahlen $\alpha_1 + \alpha_2$, $\alpha_1 - \alpha_2$, $\alpha_1\,\alpha_2$ in $\mathfrak{a}^0$ enthalten und folglich ganze Zahlen, w. z. b. w.

V. Genügt eine Zahl ω einer Gleichung von der Form

$$\omega^n + \alpha_1\,\omega^{n-1} + \cdots + \alpha_{n-1}\,\omega + \alpha_n = 0, \tag{4}$$

deren höchster Koeffizient $= 1$, und deren übrige Koeffizienten α_r ganze Zahlen sind, so ist auch ω eine ganze Zahl.

Denn wenn $\mathfrak{a}$ eine gemeinsame Hülle der Koeffizienten α_r ist, so ergibt sich leicht, daß das Produkt $\mathfrak{a}\,(\omega)_n$ eine Hülle von ω ist. In der Tat, bedeutet α irgendeine Zahl in $\mathfrak{a}$, so sind die n Produkte $\alpha\,\alpha_r$ in $\mathfrak{a}$ enthalten, und hieraus folgt nach (4), daß $\alpha\,\omega^n$ in $\mathfrak{a}\,(\omega)_n$ enthalten, mithin $\mathfrak{a}\,\omega^n > \mathfrak{a}\,(\omega)_n$ ist; da ferner $\omega\,(\omega)_n > (\omega)_{n+1} = [\omega^n] + (\omega)_n$ ist, so folgt $\omega\,\mathfrak{a}\,(\omega)_n > \mathfrak{a}\,(\omega)_{n+1} = \mathfrak{a}\,\omega^n + \mathfrak{a}\,(\omega)_n$, also $\omega\,\mathfrak{a}\,(\omega)_n > \mathfrak{a}\,(\omega)_n$, w. z. b. w.

Als einen speziellen Fall, von welchem oft Gebrauch zu machen ist, erwähnen wir, daß jede Wurzel $\sqrt[n]{\alpha}$ aus einer ganzen Zahl α eine ganze Zahl ist. Hierauf beweisen wir den folgenden wichtigen Satz:

VI. 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 aus lauter ganzen Zahlen besteht und ein Teiler des Moduls $\mathfrak{z}$ ist.

Ist $\mathfrak{m}$ eingliedrig $= [\alpha]$, so genügt der Modul $\mathfrak{n} = [\alpha^{-1}]$ dem Satze, weil $\mathfrak{m}\mathfrak{n} = \mathfrak{z}$ wird. Liegt ein zweigliedriger Modul

$$\mathfrak{m} = [\alpha, \beta] \tag{5}$$

vor, wo α, β algebraische Zahlen und von Null verschieden sind, so besteht, weil ihr Quotient ebenfalls algebraisch ist, eine homogene Gleichung von der Form

$$c_0 \alpha^n + c_1 \alpha^{n-1} \beta + \cdots + c_{n-1} \alpha \beta^{n-1} + c_n \beta^n = 0, \tag{6}$$

deren Koeffizienten c_s ganze rationale Zahlen ohne gemeinsamen Teiler sind, was nach unserer Bezeichnung kurz durch

$$[c_0, c_1, \ldots, c_{n-1}, c_n] = \mathfrak{z} \tag{7}$$

ausgedrückt wird. Es ist vorteilhaft, die Reihe dieser Koeffizienten nach beiden Seiten in der Weise fortzusetzen, daß immer $c_s = 0$ ist, wenn s größer als n oder negativ ist. Sodann bilden wir eine entsprechende Reihe von Zahlen ν_s, indem wir

$$\beta \nu_{s+1} - \alpha \nu_s = c_s \tag{8}$$

und das Anfangsglied

$$\nu_0 = 0 \tag{9}$$

setzen; hierdurch sind alle diese Zahlen ν_s vollständig bestimmt, und zwar sind sie auf rationale Weise aus α und β gebildet*). Zunächst ergibt sich, daß auch $\nu_s = 0$ ist, wenn s größer als n oder negativ ist; das letztere folgt unmittelbar aus (8) und (9), wenn man s die Zahlen $-1, -2, -3, \ldots$ durchlaufen läßt; setzt man ferner

$$\gamma_s = \alpha^{n-s+1} \beta^s \nu_s, \text{ also } \gamma_0 = 0,$$

so wird zufolge (8)

$$c_s \alpha^{n-s} \beta^s = \gamma_{s+1} - \gamma_s,$$

*) Die leicht herzustellenden Ausdrücke für die Zahlen ν_s sind hier völlig entbehrlich.

und hieraus ergibt sich mit Rücksicht auf (6), daß $\gamma_{n+1} = \gamma_0 = 0$, also auch $\nu_{n+1} = 0$ ist; setzt man weiter $s = n+1, n+2, \ldots$, so folgt aus (8), daß auch alle folgenden Zahlen $\nu_{n+2}, \nu_{n+3}, \ldots$ verschwinden. Nun ist leicht zu zeigen, daß der n-gliedrige Modul

$$\mathfrak{n} = [\nu_1, \nu_2, \ldots, \nu_n] \tag{10}$$

die im Satze angegebenen Eigenschaften besitzt. In der Tat folgt zunächst aus (7) und (8), daß der Modul $\mathfrak{z}$ durch $\mathfrak{m}\mathfrak{n}$ teilbar, also auch $\mathfrak{n}$ von Null verschieden ist. Multipliziert man ferner (8) mit ν_{r+1}, so folgt

$$\beta\nu_{r+1}\nu_{s+1} \equiv \alpha\nu_{r+1}\nu_s \pmod{\mathfrak{n}} \tag{11}$$

und hieraus durch Vertauschung von r mit s

$$\alpha\nu_{r+1}\nu_s \equiv \alpha\nu_r\nu_{s+1} \pmod{\mathfrak{n}};$$

mithin sind alle diejenigen Produkte $\alpha\nu_p\nu_q$, in denen die Summe $p+q$ einen und denselben Wert hat, einander kongruent nach $\mathfrak{n}$, und da unter diesen Produkten sich auch solche befinden, die $= 0$ sind (wie z. B. $\alpha\nu_0\nu_{p+q}$), so sind sie alle in $\mathfrak{n}$ enthalten, und zufolge (11) gilt dasselbe von allen Produkten $\beta\nu_p\nu_q$. Mithin ist der Modul $\mathfrak{m}\mathfrak{n}^2$ teilbar durch $\mathfrak{n}$, also $\mathfrak{m}\mathfrak{n}$ teilbar durch die Ordnung $\mathfrak{n}^0$ des endlichen, von Null verschiedenen Moduls $\mathfrak{n}$, und folglich besteht $\mathfrak{m}\mathfrak{n}$ aus lauter ganzen Zahlen, womit unser Satz auch für den Fall eines zweigliedrigen Moduls $\mathfrak{m}$ bewiesen ist.

Wir machen nun, wenn $m > 2$ ist, die Annahme, der Satz sei für jeden endlichen algebraischen Modul $\mathfrak{m}$ bewiesen, dessen Basis aus weniger als m Gliedern besteht, und brauchen nur zu zeigen, daß er dann auch für jeden m-gliedrigen Modul $\mathfrak{m}$ gilt. Zu diesem Zwecke bedienen wir uns der früher [§ 170, (13)] bewiesenen Identität:

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

in folgender Weise. Wir verteilen die (von Null verschiedenen) m Zahlen, aus denen die Basis von $\mathfrak{m}$ besteht, nach Belieben in drei Gruppen, doch so, daß jede Gruppe wenigstens eine dieser Zahlen enthält, und bezeichnen mit $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ die drei Moduln, deren Basen aus je einer dieser Gruppen bestehen, wodurch

$$\mathfrak{m} = \mathfrak{a}+\mathfrak{b}+\mathfrak{c}$$

wird. Da nun die von Null verschiedenen Moduln $\mathfrak{b}+\mathfrak{c}$, $\mathfrak{c}+\mathfrak{a}$, $\mathfrak{a}+\mathfrak{b}$ nur algebraische Zahlen, nämlich Zahlen des Moduls $\mathfrak{m}$ enthalten, und ihre Basen aus höchstens $m-1$ Gliedern bestehen, so kann man

nach unserer Annahme drei Moduln $\mathfrak{a}'$, $\mathfrak{b}'$, $\mathfrak{c}'$, deren Zahlen auf rationale Weise aus denen von $\mathfrak{m}$ gebildet sind, so wählen, daß jeder der drei Moduln $(\mathfrak{b}+\mathfrak{c})\mathfrak{a}'$, $(\mathfrak{c}+\mathfrak{a})\mathfrak{b}'$, $(\mathfrak{a}+\mathfrak{b})\mathfrak{c}'$ und folglich auch ihr Produkt

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

nur ganze Zahlen enthält und zugleich ein Teiler von $\mathfrak{z}$ wird. Mithin genügt der Modul

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

dessen Zahlen ebenfalls auf rationale Weise aus denen von $\mathfrak{m}$ gebildet sind, unserem Satze, w. z. b. w.

Derselbe Satz kann, wie man leicht findet, auch in folgender Weise ausgesprochen werden:

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

$$\mu_1\nu_1 + \mu_2\nu_2 + \cdots + \mu_m\nu_m = 1 \tag{12}$$

und außerdem der Bedingung genügen, daß alle m^2 Produkte $\mu_r\nu_s$ ganze Zahlen sind.

Wir bemerken zugleich, daß, wenn die gegebenen algebraischen Zahlen μ_r überhaupt eine Lösung der Gleichung

$$\mu_1\xi_1 + \mu_2\xi_2 + \cdots + \mu_m\xi_m = 1 \tag{13}$$

durch ganze Zahlen ξ_r zulassen, es gewiß auch eine solche Lösung innerhalb des Körpers $R(\mu_1, \mu_2, \ldots, \mu_m)$ gibt; denn wenn man (13) mit jeder der eben mit ν_r bezeichneten Zahlen multipliziert, so ergibt sich, daß diese Zahlen ν_r ebenfalls ganze Zahlen sind.

Wir schließen mit dem folgenden Satze:

VIII. Jede mit einer ganzen Zahl θ konjugierte Zahl ist eine ganze Zahl; bedeutet ferner A irgendeinen Körper, und t eine Variable, so hat die zu θ gehörige, nach A irreduzible Funktion

$$f(t) = t^n + a_1t^{n-1} + \cdots + a_{n-1}t + a_n,$$

welche mit $t-\theta$ verschwindet, lauter ganze Koeffizienten a_r.

Denn weil θ eine ganze Zahl ist, so gibt es eine ganze Funktion $f_1(t)$, welche mit $t-\theta$ verschwindet und lauter ganze rationale Koeffizienten c_s hat, deren höchster $= 1$ ist. Bedeutet nun π eine Permutation irgendeines Körpers M, in welchem θ enthalten ist, so folgt aus $f_1(\theta) = 0$, weil $c_s\pi = c_s$ ist, auch $f_1(\theta)\pi = f_1(\theta\pi) = 0$,

mithin ist jede mit θ konjugierte Zahl $\theta\pi$ eine ganze Zahl. Da ferner (nach den auf den Satz IX in § 164 folgenden Bemerkungen) $f_1(t)$ durch $f(t)$ teilbar ist, so genügt jede Wurzel η der Gleichung $f(\eta) = 0$ auch der Gleichung $f_1(\eta) = 0$ und ist folglich eine ganze Zahl; mithin müssen (nach IV) auch die in A enthaltenen Zahlen $\pm a_r$, welche bekanntlich durch Addition und Multiplikation aus diesen n Wurzeln η gebildet sind, ganze algebraische Zahlen sein, w. z. b. w.

§ 174.

Eine ganze Zahl α heißt teilbar durch eine ganze Zahl β, wenn $\alpha = \beta\gamma$, und γ ebenfalls eine ganze Zahl ist, und ebenso übertragen wir die anderen Ausdrucksarten, welche in der Theorie der rationalen Zahlen zur Bezeichnung der Teilbarkeit einer Zahl durch eine andere gebräuchlich sind, auf unser Gebiet aller ganzen Zahlen. Zunächst ergeben sich wieder dieselben beiden Elementarsätze:

I. Sind α und β teilbar durch μ, so sind auch die Zahlen $\alpha + \beta$ und $\alpha - \beta$ teilbar durch μ.

II. Ist $\varkappa$ teilbar durch λ, und λ teilbar durch μ, so ist auch $\varkappa$ teilbar durch μ.

Die Beweise derselben beruhen offenbar auf der im vorigen Paragraphen bewiesenen Reproduktion der ganzen Zahlen durch Addition, Subtraktion und Multiplikation (vgl. §§ 3, 159).

Unter einer Einheit verstehen wir jede ganze Zahl, welche in der Zahl 1 und folglich auch in jeder ganzen Zahl aufgeht. Offenbar ist ein Produkt von beliebig vielen Einheiten immer wieder eine Einheit, und da der reziproke Wert einer Einheit, ferner jede Wurzel aus einer Einheit ebenfalls eine Einheit ist, so reproduzieren sich die Einheiten durch Multiplikation, Division und Wurzelausziehung. Es gibt unendlich viele Einheiten; denn jede Wurzel einer Gleichung, deren höchster und niedrigster Koeffizient Einheiten, und deren übrige Koeffizienten beliebige ganze Zahlen sind, ist immer wieder eine Einheit.

Wenn zwei ganze, von Null verschiedene Zahlen α, β gegenseitig durch einander teilbar sind, so sind ihre beiden Quotienten ganze Zahlen, und zwar Einheiten, weil ihr Produkt $= 1$ ist. Es ist folglich $\beta = \alpha\varepsilon$, wo ε eine Einheit bedeutet; umgekehrt, wenn dies der Fall ist, so ist $1 = \varepsilon\varepsilon'$, wo ε' ebenfalls eine Einheit bedeutet, und

folglich $\alpha = \beta\varepsilon'$. Zwei solche Zahlen α, β sollen assoziierte Zahlen heißen; aus dieser Definition ergibt sich sofort, daß zwei mit einer dritten assoziierte Zahlen auch miteinander assoziiert sind, und hierauf beruht die Möglichkeit einer Einteilung aller ganzen Zahlen in Systeme von assoziierten Zahlen, in der Weise, daß zwei beliebige ganze Zahlen demselben oder zwei verschiedenen Systemen zugeteilt werden, je nachdem sie assoziiert sind oder nicht. Solange es sich nur um die Teilbarkeit der Zahlen handelt, verhalten sich alle miteinander assoziierten Zahlen wie eine einzige Zahl; denn wenn α durch μ teilbar ist, so ist auch jede mit α assoziierte Zahl teilbar durch jede mit μ assoziierte Zahl.

Die Definition von relativen Primzahlen kann auf verschiedene Arten gefaßt werden; diejenige, welche uns augenblicklich am weitesten führen wird, obwohl sie etwas formell ist und deshalb wohl nicht als die beste bezeichnet werden darf, lautet folgendermaßen: Zwei ganze Zahlen α, β heißen relative Primzahlen, wenn es zwei ganze Zahlen ξ, η gibt, welche der Bedingung

$$\alpha\xi + \beta\eta = 1$$

genügen*). In der Tat gewinnt man hieraus leicht die folgenden Sätze:

Ist α relative Primzahl zu β und zu γ, so ist α auch relative Primzahl zu dem Produkt $\beta\gamma$.

Denn zufolge der Annahme existieren ganze Zahlen ξ, η, ξ', η', welche den Bedingungen

$$\alpha\xi + \beta\eta = 1, \quad \alpha\xi' + \gamma\eta' = 1$$

genügen, und hieraus folgt durch Multiplikation die Existenz von zwei ganzen Zahlen

$$\xi'' = \alpha\xi\xi' + \beta\eta\xi' + \gamma\xi\eta', \quad \eta'' = \eta\eta',$$

welche der Bedingung

$$\alpha\xi'' + (\beta\gamma)\eta'' = 1$$

genügen, was zu beweisen war. Durch wiederholte Anwendung dieses Satzes ergibt sich seine Verallgemeinerung:

Ist jede der Zahlen α_1, α_2, α_3 ... relative Primzahl zu jeder der Zahlen β_1, β_2 ..., so sind die Produkte $\alpha_1\alpha_2\alpha_3\ldots$ und $\beta_1\beta_2\ldots$ relative Primzahlen.

---

*) Zufolge der bei (13) in § 173 gemachten Bemerkung können diese ganzen Zahlen ξ, η dem Körper $R(\alpha, \beta)$ entnommen werden.

Multipliziert man ferner die obige Gleichung, welche ausdrückt, daß α, β relative Primzahlen sind, mit einer beliebigen ganzen Zahl ω, so erhält man $\omega = \alpha\omega\xi + \beta\omega\eta$, woraus sich ohne weiteres die folgenden Sätze ergeben:

Sind α, β relative Primzahlen, und ist $\beta\omega$ teilbar durch α, so ist auch ω teilbar durch α.

Ist ω ein gemeinschaftliches Multiplum von zwei relativen Primzahlen α, β, so ist ω auch durch das Produkt $\alpha\beta$ teilbar.

Es leuchtet ferner ein, daß, wenn α, β relative Primzahlen sind, auch jeder Divisor von α relative Primzahl zu jedem Divisor von β ist, und so ließen sich noch sehr viele andere Sätze aus den vorhergehenden durch Kombination ableiten, die wir aber übergehen, weil sie uns doch keinen wesentlichen Dienst leisten würden. Auf einen Punkt müssen wir indessen hier noch aufmerksam machen. Offenbar ergibt sich aus der obigen Definition auch der folgende Satz:

Jeder gemeinschaftliche Divisor von zwei relativen Primzahlen ist notwendig eine Einheit.

Ob aber auch die Umkehrung dieses Satzes gilt, ob also zwei ganze Zahlen, welche außer den Einheiten keine gemeinschaftlichen Divisoren besitzen, immer relative Primzahlen im Sinne der obigen Definition sind, dies zu entscheiden sind wir mit den augenblicklich uns zu Gebote stehenden Hilfsmitteln noch nicht imstande. Erst später (§ 181) wird uns dies gelingen, und zwar werden wir folgenden allgemeinen Satz beweisen:

Zwei beliebige ganze Zahlen α, β besitzen immer einen gemeinschaftlichen Divisor δ, welcher in der Form $\alpha\xi + \beta\eta$ darstellbar ist, wo ξ, η ganze Zahlen bedeuten, und diese Zahl δ wird folglich durch jeden gemeinschaftlichen Teiler von α und β teilbar sein.

Hieraus ergibt sich dann sofort, daß die eben aufgeworfene Frage zu bejahen ist, und man wird die obige Definition, ohne ihren Inhalt zu ändern, durch folgende einfachere ersetzen können: Zwei ganze Zahlen heißen relative Primzahlen, wenn sie außer den Einheiten keinen gemeinschaftlichen Divisor besitzen.

Wenden wir uns bei dieser vorläufigen Orientierung im Gebiete aller ganzen Zahlen endlich noch zu dem Begriffe der Primzahl, so würden wir nach Analogie der Theorie der rationalen Zahlen

unter einer Primzahl eine solche ganze Zahl α verstehen, welche keine Einheit ist, und deren sämtliche Divisoren entweder Einheiten oder mit α assoziiert sind. Allein es folgt aus dem Satze V des vorigen Paragraphen, daß diese Bedingungen einen Widerspruch enthalten, daß also eine solche Zahl gar nicht existieren kann; denn wenn die ganze Zahl α keine Einheit ist, so ist auch die ganze Zahl $\sqrt{\alpha}$ keine Einheit, und sie ist auch nicht assoziiert mit α, aber sie ist ein Divisor von α. Überhaupt geht aus dem genannten Satze leicht hervor, daß jede ganze Zahl, die keine Einheit ist, immer, und zwar auf unendlich viele wesentlich verschiedene Arten in eine beliebig vorgeschriebene Anzahl von ganzen Faktoren zerlegt werden kann, von denen keiner eine Einheit ist. In dem von uns bis jetzt betrachteten, aus allen ganzen Zahlen bestehenden Gebiete findet daher eine unbeschränkte Zerlegbarkeit statt.

Das System aller ganzen Zahlen ist ein Teil des Körpers aller algebraischen Zahlen; um nun von diesem Körper, in welchem die ganzen Zahlen eine unbeschränkte Zerlegbarkeit besitzen, zu solchen Gebieten zu gelangen, innerhalb deren die Zerlegbarkeit eine begrenzte ist, müssen wir diejenigen Körper betrachten, welche wir (am Schlusse von § 167) schlechthin endliche Körper genannt haben. Mit diesen werden wir uns von jetzt ab ausschließlich beschäftigen.

§ 175.

Es sei Ω ein endlicher Körper n^{ten} Grades; derselbe besitzt, wie schon früher (am Schlusse von § 167) bemerkt ist, n und nur n verschiedene Permutationen $\pi_1, \pi_2, \ldots, \pi_n$, unter denen sich auch die identische Permutation befindet, und wir wollen, wenn ω irgendeine Zahl in Ω bedeutet, die konjugierten Zahlen $\omega\pi_1, \omega\pi_2, \ldots, \omega\pi_n$ kurz mit $\omega', \omega'', \ldots, \omega^{(n)}$ bezeichnen. Nach den in § 167 aufgestellten Definitionen ist dann

$$(1) \qquad S(\omega) = \omega' + \omega'' + \cdots + \omega^{(n)},$$

$$(2) \qquad N(\omega) = \omega'\,\omega'' \ldots \omega^{(n)},$$

$$(3) \qquad \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = (\Sigma \pm \alpha_1' \alpha_2'' \ldots \alpha_n^{(n)})^2,$$

$$(4) \qquad \Delta(\omega\alpha_1, \omega\alpha_2, \ldots, \omega\alpha_n) = N(\omega)^2\, \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n),$$

wo $\alpha_1, \alpha_2, \ldots, \alpha_n$ irgendwelche n Zahlen des Körpers bedeuten, und alle diese Spuren, Normen und Diskriminanten sind rationale Zahlen.

Die Norm von ω verschwindet nur dann, wenn $\omega = 0$ ist, und die Diskriminante (3) ist stets und nur dann von Null verschieden, wenn die n Zahlen α_r ein irreduzibles System und folglich eine Basis von Ω bilden, durch welche jede in Ω enthaltene Zahl ω in der Form

$$\omega = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n \tag{5}$$

mit rationalen Koordinaten x_r darstellbar ist. Wenn ferner die n Zahlen $\beta_1, \beta_2, \ldots, \beta_n$ ebenfalls eine Basis von Ω bilden, so bestehen n Gleichungen von der Form:

$$\alpha_r = c_{r,1}\beta_1 + c_{r,2}\beta_2 + \cdots + c_{r,n}\beta_n \tag{6}$$

mit rationalen Koeffizienten $c_{r,s}$, und wenn deren Determinante mit C bezeichnet wird, so ist

$$\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = C^2\Delta(\beta_1, \beta_2, \ldots, \beta_n). \tag{7}$$

Hieran knüpfen wir die folgende Betrachtung. Setzen wir

$$\mathfrak{a} = [\alpha_1, \alpha_2, \ldots, \alpha_n],\ \mathfrak{b} = [\beta_1, \beta_2, \ldots, \beta_n], \tag{8}$$

so sind $\mathfrak{a}$, $\mathfrak{b}$ endliche, in Ω enthaltene Moduln, deren Basen zugleich Basen von Ω sind, und umgekehrt leuchtet ein (nach § 172, VI), daß jeder endliche, in Ω enthaltene Modul, unter dessen Zahlen sich auch n voneinander unabhängige befinden, gewiß von der Form (8) ist. Hieraus folgt leicht, daß

$$\mathfrak{a} + \mathfrak{b},\ \mathfrak{a}\,\mathfrak{b},\ \mathfrak{a} - \mathfrak{b},\ \mathfrak{b} : \mathfrak{a},\ \mathfrak{a}^0,\ \mathfrak{b}^0$$

ebenfalls solche Moduln sind; von den beiden ersten leuchtet dies unmittelbar ein; wählt man ferner eine natürliche Zahl m so, daß alle Produkte $m c_{r,s}$ ganze Zahlen werden, so sind die n voneinander unabhängigen Produkte $m\alpha_r$ in $\mathfrak{a} - \mathfrak{b}$ enthalten, mithin hat der Modul $\mathfrak{a} - \mathfrak{b}$ dieselbe Eigenschaft, weil er als Vielfaches von $\mathfrak{a}$ zugleich endlich ist; dasselbe gilt auch von dem Quotienten $\mathfrak{b} : \mathfrak{a}$, weil er das kleinste gemeinsame Vielfache der n Moduln $\mathfrak{b}\alpha_r^{-1}$ ist, mithin auch von den Ordnungen $\mathfrak{a}^0$, $\mathfrak{b}^0$.

Da die Moduln $\mathfrak{a}$, $\mathfrak{b}$ (nach § 172, VII) stets und nur dann miteinander identisch sind, wenn alle Koeffizienten $c_{r,s}$ in (6) ganze Zahlen sind, und außerdem ihre Determinante $C = \pm 1$ ist, so folgt aus (7), daß alle Basen eines und desselben Moduls $\mathfrak{a}$ eine und dieselbe Diskriminante besitzen; diese von der Wahl der Basis gänzlich unabhängige Zahl wollen wir daher die Diskriminante des Moduls $\mathfrak{a}$

nennen und mit $\Delta(\mathfrak{a})$ bezeichnen*). Nehmen wir jetzt nur noch an, $\mathfrak{a}$ sei teilbar durch $\mathfrak{b}$, so sind die Koeffizienten $c_{r,s}$ in (6) ganze Zahlen, und da (nach § 172, VII) ihre Determinante $C = \pm(\mathfrak{b}, \mathfrak{a})$ ist, so nimmt die Gleichung (7) die Form $\Delta(\mathfrak{a}) = (\mathfrak{b}, \mathfrak{a})^2 \Delta(\mathfrak{b})$ an. Sind endlich $\mathfrak{a}$, $\mathfrak{b}$ zwei beliebige Moduln von der Form (8), so ergibt sich hieraus, weil $(\mathfrak{a}, \mathfrak{a} - \mathfrak{b}) = (\mathfrak{a}, \mathfrak{b})$ ist, der allgemeinste Satz

$$\Delta(\mathfrak{a} - \mathfrak{b}) = (\mathfrak{a}, \mathfrak{b})^2 \Delta(\mathfrak{a}) = (\mathfrak{b}, \mathfrak{a})^2 \Delta(\mathfrak{b}), \tag{9}$$

zugleich folgen mit Rücksicht auf (7) und (4) die Sätze**):

$$\frac{(\mathfrak{b}, \mathfrak{a})}{(\mathfrak{a}, \mathfrak{b})} = \sqrt{\frac{\Delta(\mathfrak{a})}{\Delta(\mathfrak{b})}} = \pm C \tag{10}$$

$$(\mathfrak{b}, \mathfrak{c})(\mathfrak{c}, \mathfrak{a})(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{c}, \mathfrak{b})(\mathfrak{a}, \mathfrak{c})(\mathfrak{b}, \mathfrak{a}) \tag{11}$$

$$\frac{(\mathfrak{a}, \mathfrak{a}\omega)}{(\mathfrak{a}\omega, \mathfrak{a})} = \sqrt{\frac{\Delta(\mathfrak{a}\omega)}{\Delta(\mathfrak{a})}} = \pm N(\omega), \tag{12}$$

und wenn $(\mathfrak{a}\omega, \mathfrak{a}) = 1$, also $\mathfrak{a}\omega > \mathfrak{a}$, und folglich ω eine Zahl der Ordnung $\mathfrak{a}^0$ ist, so ist $(\mathfrak{a}, \mathfrak{a}\omega) = \pm N(\omega)$. —

Alle im Körper Ω enthaltenen Zahlen sind algebraisch und zerfallen daher in ganze und gebrochene Zahlen. Wir bezeichnen mit $\mathfrak{o}$ den Inbegriff aller ganzen Zahlen des Körpers Ω, und unsere Aufgabe besteht darin, die Gesetze der Teilbarkeit der Zahlen innerhalb dieses Gebietes $\mathfrak{o}$ zu entwickeln. Da die Summen, Differenzen und Produkte von je zwei solchen Zahlen (nach § 173, IV) wieder ganze Zahlen und in Ω, also auch in $\mathfrak{o}$ enthalten sind, so ist $\mathfrak{o}$ ein Modul, und $\mathfrak{o}^2 > \mathfrak{o}$, und da alle rationalen Zahlen in Ω enthalten sind, also auch $\mathfrak{z} > \mathfrak{o}$ ist, so ist dieser Modul $\mathfrak{o}$ (nach § 170) eine Ordnung, mithin

$$\mathfrak{o}^2 = \mathfrak{o}. \tag{13}$$

---

*) Auf dieselbe Weise ergibt sich aus den Gleichungen (5) und (36) in § 167, daß die zu allen Basen des Moduls $\mathfrak{a}$ komplementären Basen auch Basen eines und desselben Moduls sind, den man deshalb das Komplement von $\mathfrak{a}$ nennen und mit $\mathfrak{a}'$ bezeichnen kann; umgekehrt ist dann $\mathfrak{a}$ das Komplement von $\mathfrak{a}'$, und $\Delta(\mathfrak{a})\Delta(\mathfrak{a}') = 1$. Verbindet man ferner die dortigen Sätze über komplementäre Systeme ebenfalls mit dem Satze VII in § 172, so erhält man die wichtigen Sätze

$$(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{b}', \mathfrak{a}'), \quad (\mathfrak{a} + \mathfrak{b})' = \mathfrak{a}' - \mathfrak{b}', \quad (\mathfrak{a}\omega)' = \mathfrak{a}'\omega^{-1}, \quad (\mathfrak{a}\mathfrak{b})' = \mathfrak{a}' : \mathfrak{b},$$

welche in meiner (in § 167 zitierten) Abhandlung „Über die Diskriminanten endlicher Körper“ weiter verfolgt sind.

**) Vgl. die Anmerkungen auf S. 89, 77.

Es kommt nun vor allen Dingen darauf an, einen deutlichen Überblick über die Ausdehnung dieses Zahlengebietes $\mathfrak{o}$ zu gewinnen. Zunächst ergibt sich leicht, daß man immer, und zwar auf unendlich viele Arten, eine ganze Basis, d. h. eine Basis von Ω finden kann, welche aus lauter ganzen Zahlen besteht. Denn wenn man ein beliebiges irreduzibles System von n Zahlen $\omega_1, \omega_2, \ldots, \omega_n$ aus Ω gewählt hat, so gibt es (nach § 173, I) n natürliche Zahlen $c_1, c_2, \ldots, c_n$ von der Art, daß die n Produkte $\alpha_r = c_r \omega_r$ ganze Zahlen werden, und offenbar bilden dieselben ebenfalls ein irreduzibles System. Nimmt man dasselbe als Basis von Ω, so leuchtet ein, daß alle diejenigen Zahlen ω in (5), deren Koordinaten x_r ganze Zahlen sind, d. h. alle Zahlen des Moduls $\mathfrak{a}$ in (8) gewiß ganze Zahlen sind, also $\mathfrak{a}$ durch $\mathfrak{o}$ teilbar ist; jeden solchen Modul $\mathfrak{a}$ wollen wir einen ganzen Modul nennen.

Da ferner alle mit einer ganzen Zahl konjugierten Zahlen (nach § 173, VIII) ebenfalls ganze Zahlen sind, so ist die rationale und von Null verschiedene Diskriminante $\Delta(\mathfrak{a})$ notwendig eine ganze Zahl, weil sie nach (3) aus lauter ganzen Zahlen $\alpha_r^{(s)}$ durch Addition, Subtraktion und Multiplikation gebildet ist. Bedeutet nun ω irgendeine Zahl in $\mathfrak{o}$, so wird sie nach (5) immer in der Form

$$\omega = \frac{m_1 \alpha_1 + m_2 \alpha_2 + \cdots + m_n \alpha_n}{m} \tag{14}$$

darstellbar sein, wo $m, m_1, m_2, \ldots, m_n$ ganze rationale Zahlen ohne gemeinschaftlichen Teiler bedeuten, deren erste, m, positiv angenommen werden darf; dann ist (nach § 172, III) offenbar $\mathfrak{a} - [\omega] = [m\omega]$, und wenn man $\mathfrak{b} = \mathfrak{a} + [\omega]$ setzt, so ist $m = (\mathfrak{b}, \mathfrak{a})$, und $(\mathfrak{a}, \mathfrak{b}) = 1$, also zufolge (9):

$$\Delta(\mathfrak{a}) = m^2 \Delta(\mathfrak{b}); \tag{15}$$

da ferner der Modul $\mathfrak{b}$ gewiß wieder von der Form (8), und zwar ein ganzer Modul ist, so können wir folgenden Satz aussprechen:

I. Ist $\mathfrak{a}$ ein endlicher und ganzer Modul, dessen Basis zugleich eine Basis des Körpers Ω bildet, und ist m der kleinste natürliche Faktor, durch welchen eine ganze Zahl ω in eine Zahl $m\omega$ des Moduls $\mathfrak{a}$ verwandelt wird, so ist die Diskriminante $\Delta(\mathfrak{a})$ teilbar durch m^2, und der Quotient ist die Diskriminante $\Delta(\mathfrak{b})$ des ganzen Moduls $\mathfrak{b} = \mathfrak{a} + [\omega]$.

Da nun die Diskriminanten aller dieser Moduln $\mathfrak{a}, \mathfrak{b} \ldots$ ganze rationale Zahlen und von Null verschieden sind, so muß es auch

einen solchen Modul $\mathfrak{a}$ geben, dessen Diskriminante $\Delta(\mathfrak{a})$, absolut genommen, ein Minimum ist, und aus dem vorhergehenden Satze leuchtet ein, daß jede ganze Zahl ω notwendig in diesem ganzen Modul $\mathfrak{a}$ enthalten, und folglich $\mathfrak{a} = \mathfrak{o}$ sein muß. Wir haben daher den folgenden Fundamentalsatz gewonnen:

II. Der Inbegriff $\mathfrak{o}$ aller ganzen Zahlen eines endlichen Körpers Ω ist ein endlicher Modul, dessen Basis zugleich eine Basis von Ω bildet.

Nächst dem Grade n ist nun diese Minimal-Diskriminante von der größten Bedeutung für die Beschaffenheit des Körpers Ω; wir wollen sie deshalb die Grundzahl oder auch die Diskriminante von Ω nennen und immer mit D bezeichnen, also

$$D = \Delta(\mathfrak{o}) \tag{16}$$

setzen; für jeden ganzen Modul $\mathfrak{a}$ von der obigen Beschaffenheit gilt dann zufolge (9) der Satz:

$$\Delta(\mathfrak{a}) = D(\mathfrak{o}, \mathfrak{a})^2. \tag{17}$$

Im einfachsten Falle $n = 1$, wo Ω der Körper R der rationalen Zahlen, also $\mathfrak{o} = \mathfrak{z} = [1]$ ist, hat man $D = 1$ zu setzen.

Zur Erläuterung wollen wir das nächstliegende Beispiel, den Fall eines quadratischen Körpers Ω betrachten. Jede Wurzel θ einer irreduziblen quadratischen Gleichung läßt sich auf die Form $a + b\sqrt{d}$ bringen, wo d eine ganze rationale, positive oder negative Zahl bedeutet, welche durch kein Quadrat (außer 1) teilbar und auch nicht $= +1$ ist, während a, b rationale Zahlen sind, deren letztere nicht verschwindet. Alle in Ω enthaltenen, d. h. durch θ rational darstellbaren Zahlen sind dann von der Form $\alpha = t + u\sqrt{d}$, wo t, u willkürliche rationale Zahlen bedeuten. Durch die nicht identische Permutation des Körpers geht $\sqrt{d}$ in $-\sqrt{d}$, also α in die konjugierte Zahl $\alpha' = t - u\sqrt{d}$ über, welche ebenfalls in Ω enthalten ist; mithin ist Ω ein Normalkörper (§ 166). Die ganzen Zahlen 1 und $\sqrt{d}$ sind voneinander unabhängig, und da ihre Diskriminante

$$\Delta(1, \sqrt{d}) = \begin{vmatrix} 1, & \sqrt{d} \\ 1, & -\sqrt{d} \end{vmatrix}^2 = 4d$$

durch keine Quadratzahl m^2 außer 1 und 4 teilbar ist, so schließen wir aus den obigen Sätzen, daß die Grundzahl D des Körpers entweder $= 4d$ oder $= d$ ist, und das letztere wird stets und nur

dann eintreten, wenn es in Ω eine ganze Zahl $\omega = {}^1/_2(x + y\sqrt{d})$ gibt, wo x, y ganze rationale Zahlen bedeuten, die nicht beide gerade sind. Um diese Möglichkeit zu prüfen, dürfen wir uns diese Zahlen x, y schon auf ihre kleinsten Reste 0 oder 1 nach dem Modul 2 reduziert denken; offenbar kann y nicht $= 0$ sein, weil sonst auch $x = 0$ sein müßte, und von den beiden übrigen Zahlen $\omega = {}^1/_2\sqrt{d}$ und $\omega = {}^1/_2(1 + \sqrt{d})$ ist die erstere gebrochen, weil ihr Quadrat keine ganze Zahl ist; die letztere genügt der irreduziblen Gleichung

$$\omega^2 - \omega + {}^1/_4(1 - d) = 0$$

und ist folglich dann und nur dann eine ganze Zahl, wenn $d \equiv 1 \pmod 4$ ist. Hieraus ergibt sich also:

(18) $\mathfrak{o} = [1, \sqrt{d}]$, $D = 4d$, wenn $d \equiv 2$ oder $3 \pmod 4$,

(19) $\mathfrak{o} = \left[1, \frac{1 + \sqrt{d}}{2}\right]$, $D = d$, wenn $d \equiv 1 \pmod 4$

und in beiden Fällen

(20) $$\mathfrak{o} = \left[1, \frac{D + \sqrt{D}}{2}\right].$$

Es gibt 61 quadratische Körper, deren Grundzahlen D absolut genommen kleiner als 100 sind; unter diesen Zahlen D sind 30 positive Zahlen:

5, 8, 12, 13, 17, 21, 24, 28, 29, 33, 37, 40, 41, 44, 53,
56, 57, 60, 61, 65, 69, 73, 76, 77, 85, 88, 89, 92, 93, 97

und die absoluten Werte der 31 negativen Zahlen D sind:

3, 4, 7, 8, 11, 15, 19, 20, 23, 24, 31, 35, 39, 40, 43, 47,
51, 52, 55, 56, 59, 67, 68, 71, 79, 83, 84, 87, 88, 91, 95.

Die Grundzahl des Körpers J (§ 159) ist $= -4$*).

*) Um schon hier einen Begriff von der Bedeutung der Grundzahl D zu geben, wollen wir nur darauf aufmerksam machen, daß (zufolge § 52, I — IV) die natürlichen Primzahlen p, von welchen d quadratischer Rest ist, immer in arithmetischen Reihen von der kleinsten Differenz D enthalten sind; diese Zahlen p verlieren in dem quadratischen Körper Ω den eigentlichen Primzahl-Charakter, und dem in dieser Form ausgesprochenen Gesetze fügt sich auch die Zahl $p = 2$ (vgl. § 186). Dies aus dem Reziprozitätssatze abgeleitete Gesetz der Verteilung in arithmetische Reihen hängt wesentlich damit zusammen, daß Ω ein Divisor desjenigen Kreisteilungskörpers $R(\theta)$ ist, welcher aus der Gleichung $\theta^D = 1$ entspringt, während aus jeder Gleichung $\theta^m = 1$, deren Grad m absolut $< D$, immer ein Körper $R(\theta)$ entspringt, welcher die Zahl $\sqrt{d}$ nicht enthält.

§ 176.

Das Gebiet $\mathfrak{o}$ aller ganzen Zahlen ω, welche in einem Körper Ω vom Grade n enthalten sind, und mit denen wir uns im folgenden ausschließlich beschäftigen, besitzt einige allgemeine Eigenschaften, welche denen der früher behandelten speziellen Gebiete [1] und [1, i] genau entsprechen. Wir wollen diese Analogie zunächst verfolgen, um sodann diejenige wesentlich neue Erscheinung hervorzuheben, welche uns zur Einführung neuer Begriffe nötigen wird.

Wir wiederholen zunächst, daß die Zahlen ω, zu denen auch alle ganzen rationalen Zahlen gehören, sich durch Addition, Subtraktion und Multiplikation reproduzieren; wenn ferner von zwei solchen Zahlen λ, μ die erstere durch die letztere teilbar ist (§ 174), so ist $\lambda = \mu\nu$, und die Zahl ν gehört demselben Gebiete $\mathfrak{o}$ an. Zugleich leuchtet ein, daß in $\mathfrak{o}$ die beiden Elementarsätze der Teilbarkeit gelten, die wir früher (§ 174, I und II) für das Gebiet aller ganzen algebraischen Zahlen bewiesen haben.

Die Spur $S(\mu)$ und die Norm $N(\mu)$ einer Zahl μ des Gebietes $\mathfrak{o}$ sind ganze rationale Zahlen, weil sie aus den n mit μ konjugierten Zahlen, die (zufolge § 173, VIII) ebenfalls ganze Zahlen sind, durch Addition und Multiplikation gebildet sind. Zugleich folgt aus dem [in § 167, (4) bewiesenen] Satze

$$N(\mu\nu) = N(\mu)N(\nu) \tag{1}$$

der häufig anzuwendende, aber nicht umzukehrende Satz:

I. Ist λ teilbar durch μ, so ist auch $N(\lambda)$ teilbar durch $N(\mu)$.

Die Norm besitzt nun eine äußerst wichtige Bedeutung, welche mit dem folgenden Begriffe zusammenhängt. Zwei Zahlen α, β heißen kongruent in bezug auf die Zahl μ, den Modulus, wenn ihre Differenz $\alpha - \beta$ durch μ teilbar ist, und wir bezeichnen dies durch die Kongruenz

$$\alpha \equiv \beta \pmod{\mu}; \tag{2}$$

wir nennen dagegen die Zahlen α, β, γ ... inkongruent nach μ, wenn keine von ihnen mit einer der übrigen kongruent ist. Aus der oben erwähnten Reproduktion unserer Zahlen ω durch Addition, Subtraktion und Multiplikation folgt, daß man beliebig viele solche Kongruenzen, die sich auf einen und denselben Modul μ beziehen,

addieren, subtrahieren und multiplizieren darf, wie Gleichungen (vgl. § 17). Da nun der Inbegriff aller durch μ teilbaren Zahlen $\omega\mu$ offenbar identisch mit dem Modul $\mathfrak{o}\mu$ ist (§ 170), so stimmt die Kongruenz (2) gänzlich überein mit

$$\alpha \equiv \beta \pmod{\mathfrak{o}\mu}, \tag{3}$$

und folglich ist die Anzahl aller nach μ inkongruenten Zahlen zugleich die Anzahl $(\mathfrak{o}, \mathfrak{o}\mu)$ aller auf den Modul $\mathfrak{o}\mu$ bezüglichen Zahlklassen, aus welchen $\mathfrak{o}$ besteht; da ferner $\mathfrak{o}\mu > \mathfrak{o}$, also $(\mathfrak{o}\mu, \mathfrak{o}) = 1$ ist, so folgt aus (12) in § 175 der Satz:

II. Die Anzahl aller nach μ inkongruenten Zahlen ist

$$(\mathfrak{o}, \mathfrak{o}\mu) = \pm N(\mu). \tag{4}$$

Hierbei ist vorausgesetzt, daß μ und folglich auch $N(\mu)$ von Null verschieden ist; wenn aber μ verschwindet, so ist die Anzahl der inkongruenten Zahlen offenbar unendlich groß, und die Gleichung (4) bleibt richtig, wenn $(\mathfrak{o}, \mathfrak{o}\mu)$ wieder $= 0$ gesetzt wird (§ 171); doch wollen wir diesen uninteressanten Fall im folgenden ausschließen. Die Betrachtung der Moduln von der Form $\mathfrak{o}\mu$ wird uns auch in der Folge große Dienste leisten, und ihre Bedeutung für unsere Aufgabe spricht sich schon in dem folgenden Satze aus:

III. Die Teilbarkeit der Zahl λ durch die Zahl μ ist gleichbedeutend mit der Teilbarkeit des Moduls $\mathfrak{o}\lambda$ durch den Modul $\mathfrak{o}\mu$, also mit $\mathfrak{o}\lambda > \mathfrak{o}\mu$.

Dies leuchtet unmittelbar ein; denn wenn λ durch μ teilbar ist, so ist nach dem zweiten Elementarsatze der Teilbarkeit jede durch λ teilbare, d. h. in $\mathfrak{o}\lambda$ enthaltene Zahl $\varkappa$ auch teilbar durch μ, also in $\mathfrak{o}\mu$ enthalten, mithin $\mathfrak{o}\lambda > \mathfrak{o}\mu$; und umgekehrt, wenn $\mathfrak{o}\lambda > \mathfrak{o}\mu$, so ist jede in $\mathfrak{o}\lambda$ enthaltene Zahl, also z. B. λ selbst auch in $\mathfrak{o}\mu$ enthalten, d. h. teilbar durch μ, w. z. b. w.

Um hiervon sogleich eine Anwendung zu machen, erinnern wir an den für zwei beliebige Moduln $\mathfrak{a}$, $\mathfrak{b}$ geltenden Satz $(\mathfrak{a}, \mathfrak{b})\mathfrak{a} > \mathfrak{b}$ (§ 171, I); setzen wir $\mathfrak{a} = \mathfrak{o}$, $\mathfrak{b} = \mathfrak{o}\mu$, so folgt aus (4) der Satz:

IV. Die Norm der Zahl μ ist teilbar durch μ.

Derselbe ergibt sich aber auch unmittelbar daraus, daß $N(\mu)$ das Produkt aus den n mit μ konjugierten, also ganzen Zahlen, und daß eine derselben $= \mu$ ist; mithin ist

$$N(\mu) = \mu\nu, \tag{5}$$

wo ν das Produkt aus den übrigen $n-1$ Faktoren, also eine ganze Zahl bedeutet, welche wir das Supplement*) der Zahl μ nennen wollen. Da $N(\mu)$ eine rationale Zahl und folglich $NN(\mu) = N(\mu)^n$ ist, so folgt aus (1):

$$N(\nu) = N(\mu)^{n-1}. \tag{6}$$

Wir bemerken noch, daß jeder Zahl μ (nach § 167) eine bestimmte Funktion einer Variablen t entspricht, welche durch

$$\begin{aligned} f(t) &= (t-\mu')(t-\mu'')\dots(t-\mu^{(n)}) \\ &= t^n + a_1 t^{n-1} + \dots + a_{n-1} t + a_n \end{aligned} \tag{7}$$

definiert wird, und deren Koeffizienten a_r in unserem Falle ganze rationale Zahlen sind; insbesondere ist

$$S(\mu) = -a_1;\quad N(\mu) = (-1)^n a_n, \tag{8}$$

und da $f(\mu) = 0$ ist, so ergibt sich auch hieraus wieder der Satz IV und zugleich die Darstellung des Supplementes ν durch die Gleichung

$$(-1)^{n-1}\nu = \mu^{n-1} + a_1\mu^{n-2} + \dots + a_{n-1}. \tag{9}$$

Bedeutet ε irgendeine (in $\mathfrak{o}$ enthaltene) Einheit, also eine Zahl, welche in allen ganzen Zahlen aufgeht (§ 174), so ist $\mathfrak{o}$ teilbar durch $\mathfrak{o}\varepsilon$, und folglich

$$\mathfrak{o}\varepsilon = \mathfrak{o}, \tag{10}$$

weil $\mathfrak{o}\varepsilon$ auch teilbar durch $\mathfrak{o}$ ist; und umgekehrt, wenn eine Zahl ε dieser Bedingung (10) genügt, so ist sie offenbar in $\mathfrak{o}$ enthalten, und zwar eine Einheit, weil die in $\mathfrak{o}$ enthaltene Zahl 1, und folglich jede ganze Zahl durch ε teilbar ist**). Zufolge (4) ist diese, für jede in $\mathfrak{o}$ enthaltene Einheit ε charakteristische Bedingung (10) gänzlich gleichbedeutend mit der folgenden

$$N(\varepsilon) = \pm 1. \tag{11}$$

Dasselbe ergibt sich aber auch so: wenn ε eine Einheit ist, also in der Zahl 1 aufgeht, so geht (nach I) die ganze rationale Zahl $N(\varepsilon)$ auch in $N(1)$, d. h. in 1 auf und ist folglich $= \pm 1$; umgekehrt, wenn eine ganze Zahl ε der Bedingung (11) genügt, so geht sie (nach IV) auch in der Zahl 1 auf, und ist folglich eine Einheit.

---

*) In den früheren Auflagen habe ich ν die zu μ adjungierte Zahl genannt, was aber unzweckmäßig erscheint, weil diesem Worte von Galois eine ganz andere Bedeutung beigelegt ist (§ 160).

**) Allgemein, wenn $\mathfrak{a}$ irgendein endlicher, von Null verschiedener Modul, und $\mathfrak{a}\varepsilon = \mathfrak{a}$ ist, so ist ε eine in der Ordnung $\mathfrak{a}^0$ enthaltene Einheit, und umgekehrt genügt jede solche Einheit ε der Bedingung $\mathfrak{a}\varepsilon = \mathfrak{a}$.

Betrachten wir jetzt eine Zahl μ, welche von Null verschieden und auch keine Einheit ist, so ist $N(\mu)$ absolut $\geqq 2$, und umgekehrt; jede solche Zahl μ ist gewiß durch alle Einheiten ε, und außerdem durch alle mit μ assoziierten Zahlen $\varepsilon\mu$ teilbar. Nun sind zwei Fälle möglich: wenn die Zahl μ außer den eben genannten Zahlen ε und $\varepsilon\mu$ keinen anderen Divisor in $\mathfrak{o}$ besitzt, so heißt μ unzerlegbar (in $\mathfrak{o}$, was immer hinzuzudenken ist); sie soll dagegen zerlegbar heißen, wenn sie einen von den Zahlen ε und $\varepsilon\mu$ verschiedenen Divisor α besitzt. In dem letzteren Falle ist $\mu = \alpha\beta$, und es leuchtet ein, daß auch β weder eine Einheit, noch mit μ assoziiert sein kann, weil sonst α entweder mit μ oder mit 1 assoziiert wäre; da ferner $N(\mu) = N(\alpha)N(\beta)$ ist, so folgt, daß (absolut) $N(\mu) > N(\alpha) > 1$ ist. Zerlegt man nun α und β, falls es angeht, weiter in solche Faktoren, die keine Einheiten sind, und fährt man so fort, so ergibt sich aus der angeführten Beschaffenheit der Normen, daß diese Zerlegung nach einer endlichen Anzahl von Schritten ihr Ende finden muß; während also in dem aus allen algebraischen Zahlen bestehenden Körper eine unbeschränkte Zerlegbarkeit der ganzen Zahlen stattfindet (§ 174), gilt für jeden endlichen Körper Ω der folgende Satz:

V. Jede zerlegbare Zahl ist darstellbar als Produkt aus einer endlichen Anzahl von unzerlegbaren Faktoren.

Diese Operation der Zerlegung einer Zahl μ ist vollständig analog derjenigen, welche wir früher bei den Körpern R und J (§§ 8 und 159) beschrieben haben; aber in diesen beiden speziellen Fällen besaß das Schlußresultat eine größere Bestimmtheit als dasjenige, zu welchem wir hier gelangt sind, denn wir konnten damals beweisen, daß das System der unzerlegbaren Faktoren von μ ein im wesentlichen bestimmtes, einziges war, vorausgesetzt, daß zwei assoziierte Zahlen als nicht wesentlich verschieden angesehen wurden. Dieser Nachweis gründete sich bei beiden Körpern auf diejenige Eigenschaft ihrer unzerlegbaren Zahlen, welche wir den Primzahl-Charakter nennen wollen, die aber bei einem beliebigen endlichen Körper Ω mit der Unzerlegbarkeit keineswegs notwendig verbunden ist. Um diesen Unterschied kurz bezeichnen zu können, stellen wir der obigen Einteilung der Zahlen ω in zerlegbare und unzerlegbare Zahlen die folgende gegenüber:

Eine von Null verschiedene Zahl μ, welche keine Einheit ist, soll eine Primzahl (in $\mathfrak{o}$) heißen, wenn je zwei durch μ nicht teil-

bare Zahlen ω auch ein durch μ unteilbares Produkt besitzen*); gibt es aber zwei durch μ nicht teilbare Zahlen ω, deren Produkt durch μ teilbar ist, so soll μ eine zusammengesetzte Zahl heißen.

Es leuchtet unmittelbar ein, daß jede zerlegbare Zahl gewiß auch eine zusammengesetzte Zahl, also jede Primzahl gewiß eine unzerlegbare Zahl ist. In den beiden speziellen Fällen der Körper R und J decken sich nun beide Einteilungen vollständig, d. h. jede unzerlegbare Zahl ist auch eine Primzahl, und jede zusammengesetzte Zahl ist auch eine zerlegbare Zahl, und man erkennt sofort, daß gerade hierin der Grund liegt, weshalb die Zerlegung einer Zahl in unzerlegbare Faktoren eine einzige, völlig bestimmte war (§§ 8 und 159); dieselbe Bestimmtheit der Zerlegungen wird deshalb bei allen Körpern Ω vorhanden sein, bei welchen die Begriffe der unzerlegbaren Zahl und der Primzahl sich vollständig decken. Sobald aber eine unzerlegbare Zahl μ existiert, welche keine Primzahl, also eine zusammengesetzte Zahl ist, so gibt es zwei durch μ nicht teilbare Zahlen α, β, deren Produkt γ durch μ teilbar, also von der Form $\mu\nu$ ist; mag man nun die Zahlen α, β, ν, wenn sie zerlegbar sind, auf irgendwelche Weise in unzerlegbare Faktoren aufgelöst haben, so entspringen aus den Gleichungen

$$\gamma = \alpha\beta \quad \text{und} \quad \gamma = \mu\nu$$

zwei Zerlegungen derselben Zahl γ in unzerlegbare Faktoren, und diese beiden Zerlegungen sind wesentlich verschieden, weil unter den Faktoren der durch μ nicht teilbaren Zahlen α und β kein einziger mit μ assoziiert sein kann.

Auf eine solche Erscheinung ist Kummer bei seinen Untersuchungen über diejenigen Zahlengebiete o gestoßen, welche aus dem Problem der Kreisteilung entspringen; aber durch die Einführung seiner idealen Zahlen ist es ihm gelungen, die hiermit zusammenhängenden großen Schwierigkeiten zu überwinden. Diese Schöpfung neuer Zahlen beruht auf einem Gedanken, welcher für unseren obigen

*) Ist also $\alpha\beta$ teilbar durch die Primzahl μ, so ist wenigstens einer der beiden Faktoren α, β durch μ teilbar. — Aus dieser Definition folgt leicht, daß die kleinste, durch μ teilbare natürliche Zahl p eine Primzahl in R, und daß $\pm N(\mu) = p^f$ ist; der Exponent f, welcher immer > 0 und $\leq n$ ist, kann der Grad der Primzahl μ genannt werden. Die Umkehrung dieses Satzes ist im allgemeinen nicht gestattet, doch gilt der folgende, ebenfalls leicht zu beweisende Satz: ist $N(\mu)$ eine Primzahl in R, so ist μ eine Primzahl (ersten Grades) in Ω.

Fall sich etwa in folgender Weise darstellen läßt. Wären die Zahlen α, β, μ, ν, welche durch die Gleichung

$$\alpha\beta = \mu\nu \tag{12}$$

miteinander verbunden sind, ganze rationale Zahlen, und zwar ohne gemeinschaftlichen Teiler, so würde hieraus nach den in R herrschenden Gesetzen der Teilbarkeit eine Zerlegung dieser Zahlen in rationale Faktoren folgen, nämlich

$$\alpha = \alpha_1\alpha_2,\ \beta = \beta_1\beta_2,\ \mu = \alpha_1\beta_2,\ \nu = \beta_1\alpha_2, \tag{13}$$

und zwar würde α_1 relative Primzahl zu β_1, und ebenso α_2 relative Primzahl zu β_2 sein; selbst wenn man nun diese Zerlegung nicht wirklich ausgeführt hätte, wenn man also die vier ganzen rationalen Zahlen α_1, α_2, β_1, β_2 noch nicht kennte, so wären dieselben doch wesentlich bestimmt, und, was das Wichtigste ist, man wäre mit alleiniger Hilfe der gegebenen Zahlen α, β, μ, ν völlig imstande, zu entscheiden, ob eine beliebige ganze rationale Zahl ω durch eine der unbekannten Zahlen, z. B. durch α_1, teilbar ist oder nicht; denn offenbar ist die Kongruenz

$$\omega \equiv 0 \pmod{\alpha_1} \tag{14}$$

völlig gleichbedeutend mit jeder der beiden Kongruenzen

$$\beta\omega \equiv 0 \pmod{\mu},\ \nu\omega \equiv 0 \pmod{\alpha}. \tag{15}$$

Wir haben es nun in Wahrheit nicht mit rationalen, sondern mit Zahlen α, β, μ, ν zu tun, welche dem Gebiete $\mathfrak{o}$ angehören, und da die Zahl μ unzerlegbar, und keine der Zahlen α, β durch μ teilbar ist, so existiert innerhalb $\mathfrak{o}$ eine Zerlegung von der Form (13) in Wirklichkeit nicht; aber obgleich eine Zahl wie α_1 nicht in $\mathfrak{o}$ vorhanden ist, so kann man mit Kummer doch eine solche Zahl α_1 als einen idealen Faktor der wirklichen Zahl μ in die Untersuchung einführen; diese ideale Zahl α_1 tritt zwar niemals isoliert auf, aber in Verbindung mit anderen, ebenfalls idealen Zahlen α_2, β_2 kann sie wirkliche Zahlen α, μ des Gebietes $\mathfrak{o}$ erzeugen, und vor allen Dingen läßt sich die Teilbarkeit einer beliebigen wirklichen Zahl ω durch die ideale Zahl α_1 mit voller Klarheit, nämlich durch jede der beiden obigen Kongruenzen (15) definieren.

Eine solche fingierte Zahl α_1 wird man eine ideale Primzahl nennen, wenn je zwei durch α_1 nicht teilbare Zahlen ein Produkt geben, welches ebenfalls durch α_1 nicht teilbar ist; man kann auch

Potenzen solcher Primzahlen einführen und die Teilbarkeit einer beliebigen wirklichen Zahl ω durch α_1^r so definieren, daß die Kongruenz

$$\omega \equiv 0 \pmod{\alpha_1^r}$$

als gleichbedeutend mit jeder der beiden Kongruenzen

$$\beta^r \omega \equiv 0 \pmod{\mu^r}, \quad \nu^r \omega \equiv 0 \pmod{\alpha^r}$$

angesehen wird. Zur Erläuterung möge folgendes einfache, schon in §§ 16, 159 erwähnte Beispiel dienen*).

Der quadratische Körper Ω, welcher aus einer Wurzel θ der Gleichung

$$\theta^2 + 5 = 0 \tag{16}$$

entspringt, hat die Grundzahl $D = -20$, und der endliche Modul

$$\mathfrak{o} = [1, \theta] \tag{17}$$

ist (nach § 175) der Inbegriff aller in Ω enthaltenen ganzen Zahlen

$$\omega = x + y\theta, \tag{18}$$

wo x, y beliebige ganze rationale Zahlen bedeuten. Da hieraus

$$N(\omega) = \omega\omega' = (x + y\theta)(x - y\theta) = x^2 + 5y^2 \tag{19}$$

folgt, so sind die einzigen Einheiten die beiden Zahlen ± 1. Nun sind die vier Zahlen

$$\alpha = 3, \ \beta = 7, \ \mu = 1 + 2\theta, \ \nu = 1 - 2\theta \tag{20}$$

durch die Gleichung (12) miteinander verbunden, und zwar sind sie alle unzerlegbar; denn wäre z. B. $\alpha = 3 = \alpha_1\alpha_2$, und keine der beiden ganzen Zahlen α_1, α_2 eine Einheit, so würde aus $N(\alpha) = 9 = N(\alpha_1)N(\alpha_2)$ folgen, daß $N(\alpha_1) = N(\alpha_2) = 3$ sein müßte, was aber zufolge (19) unmöglich ist; und ebenso würde sich die Unzerlegbarkeit der drei anderen Zahlen β, μ, ν beweisen lassen**). Man wird daher vier ideale Zahlen α_1, α_2, β_1, β_2 einführen und so definieren, daß eine beliebige Zahl ω teilbar durch α_1, α_2, β_1, β_2 heißt, wenn die entsprechende Kongruenz

$$(\alpha_1) \qquad \nu\omega \equiv 0 \pmod{3}$$
$$(\alpha_2) \qquad \mu\omega \equiv 0 \pmod{3}$$
$$(\beta_1) \qquad \mu\omega \equiv 0 \pmod{7}$$
$$(\beta_2) \qquad \nu\omega \equiv 0 \pmod{7}$$

*) Dasselbe ist ausführlicher behandelt in meiner Abhandlung Sur la théorie des nombres entiers algébriques §§ 7—12 (Paris 1877; Abdruck aus dem Bulletin des Sciences math. et astron. von Darboux und Houël, 1re série, t. XI, et 2e série, t. I) [vgl. XLVIII].

**) Vgl. §§ 71, 159.

erfüllt ist. Zufolge (18) und (20) ist aber

$$(21) \qquad \begin{cases} \nu\omega = (x + 10y) + (y - 2x)\theta \\ \mu\omega = (x - 10y) + (y + 2x)\theta, \end{cases}$$

und die vorstehenden Kongruenzen gehen über in

$$(\alpha_1) \qquad x + y \equiv 0 \pmod 3$$
$$(\alpha_2) \qquad x - y \equiv 0 \pmod 3$$
$$(\beta_1) \qquad x - 3y \equiv 0 \pmod 7$$
$$(\beta_2) \qquad x + 3y \equiv 0 \pmod 7.$$

Setzt man ferner $\omega_1 = x_1 + y_1\theta$, so wird $\omega\omega_1 = x_2 + y_2\theta$, wo $x_2 = xx_1 - 5yy_1$, $y_2 = xy_1 + yx_1$, mithin z. B.:

$$x_2 + y_2 \equiv (x + y)(x_1 + y_1) \pmod 3;$$

hieraus folgt mit Rücksicht auf (α_1), daß das Produkt $\omega\omega_1$ dann und nur dann durch die ideale Zahl α_1 teilbar ist, wenn mindestens einer der beiden Faktoren ω, ω_1 durch α_1 teilbar ist, und folglich werden wir α_1 eine ideale Primzahl nennen; ganz dasselbe gilt, wie man leicht findet, auch für die drei anderen idealen Zahlen α_2, β_1, β_2. Da ferner die Zahl μ teilbar durch α_1, unteilbar durch α_2, und ebenso die Zahl ν teilbar durch α_2, unteilbar durch α_1 ist, so sind die beiden idealen Primzahlen α_1, α_2 als verschieden anzusehen, und in demselben Sinne sind die Zahlen β_1, β_2 voneinander und von α_1, α_2 verschieden. Nun geht aus (α_1) und (α_2) hervor, daß eine Zahl ω dann und nur dann durch die Zahl $\alpha = 3$ teilbar ist, wenn sie sowohl durch α_1 als auch durch α_2 teilbar ist, und da α_1, α_2 für zwei verschiedene ideale Primzahlen zu halten sind, so wird man nach Analogie der Theorie der rationalen Zahlen die Zahl $\alpha = 3$ als wesentlich identisch mit dem Produkte dieser Zahlen α_1, α_2 ansehen, also in diesem Sinne $\alpha = \alpha_1\alpha_2$ setzen; ebenso würden sich die drei anderen Gleichungen in (13) rechtfertigen lassen, und diese Zerlegungen der Zahlen α, β, μ, ν in ideale Faktoren α_1, α_2, β_1, β_2 würden in (12) eine schöne Bestätigung finden.

Durch die Einführung dieser und unendlich vieler anderen idealen Primzahlen, sowie ihrer Potenzen, gewinnt nun die Theorie dieses Zahlengebietes $\mathfrak{o}$ eine bewunderungswürdige Einfachheit; in der Tat gelangt man auf diese Weise zu dem überraschenden Resultate, daß die in der Theorie der rationalen (ebenso der komplexen) Zahlen herrschenden allgemeinen Gesetze der Teilbarkeit, welche in unserem Gebiete $\mathfrak{o}$ ihre Geltung zu verlieren drohten, nun vollständig wieder

hergestellt werden; jede Zahl ω des Gebietes $\mathfrak{o}$ kann wie ein Produkt von völlig bestimmten Potenzen von wirklichen oder idealen Primzahlen angesehen werden, und sie geht dann und nur dann in einer zweiten Zahl auf, wenn diese durch jede solche Potenz teilbar ist.

Mit diesem Versuche, den Grundgedanken der Kummerschen Schöpfung zu erläutern, müssen wir uns hier begnügen; es würde sich nämlich selbst bei dem einfachen, hier gewählten Beispiele bald zeigen, daß eine völlig klare und strenge Durchführung dieser Untersuchung einige Schwierigkeiten darbietet, die zwar nicht erheblich sind, deren Beseitigung aber doch etwas umständlich ist. In bei weitem höheren Maße treten solche Schwierigkeiten auf, wenn man zu Körpern höheren Grades übergehen oder gar, was unsere eigentliche Aufgabe ist, die allgemeinen Gesetze der Teilbarkeit ergründen will, welche für jeden endlichen Körper Ω gelten. Wegen dieser Schwierigkeiten, deren genauere Erörterung uns hier zu weit führen würde*), verzichten wir im folgenden gänzlich auf die Einführung idealer Zahlen und gründen unsere Theorie auf einen anderen Begriff, den Begriff des Ideals, worunter immer ein mit gewissen charakteristischen Eigenschaften begabtes System von unendlich vielen wirklichen Zahlen verstanden werden soll.

Es wird gut sein, diesen Begriff an unserem obigen Beispiele zu erläutern. Die erforderliche und hinreichende Bedingung dafür, daß eine ganze Zahl $\omega = x + y\theta$ durch die ideale Primzahl α_1 teilbar ist, besteht nach (α_1) darin, daß $x \equiv 2y \pmod 3$, also $x = 3z + 2y$ ist, wo z eine beliebige ganze rationale Zahl bedeutet; jede solche Zahl ω ist also von der Form $3z + (2 + \theta)y$. Bezeichnet man daher mit $\mathfrak{a}_1$ den Inbegriff aller durch α_1 teilbaren Zahlen ω, so ist

$$\mathfrak{a}_1 = [3,\ 2 + \theta], \tag{22}$$

und ebenso findet man, daß die Inbegriffe aller durch α_2, β_1, β_2 teilbaren Zahlen bzw. die Moduln

$$\mathfrak{a}_2 = [3,\ 1 + \theta],\ \mathfrak{b}_1 = [7,\ 3 + \theta],\ \mathfrak{b}_2 = [7,\ 4 + \theta] \tag{22}$$

sind. Bilden wir nun auch die Inbegriffe

$$\begin{cases} \mathfrak{o}\alpha = [3,\ 3\theta],\ \mathfrak{o}\beta = [7,\ 7\theta], \\ \mathfrak{o}\mu = [1 + 2\theta, -10 + \theta],\ \mathfrak{o}\nu = [1 - 2\theta,\ 10 + \theta] \end{cases} \tag{23}$$

*) Vgl. die Einleitung der Schrift Sur la théorie des nombres entiers algébriques [XLVIII].

der durch α, β, μ, ν teilbaren Zahlen, von denen die letzteren in (21) dargestellt sind, so ergibt sich leicht, daß diese acht Moduln durch die Gleichungen

$$(24) \qquad \mathfrak{o}\alpha = \mathfrak{a}_1\mathfrak{a}_2,\ \mathfrak{o}\beta = \mathfrak{b}_1\mathfrak{b}_2,\ \mathfrak{o}\mu = \mathfrak{a}_1\mathfrak{b}_2,\ \mathfrak{o}\nu = \mathfrak{b}_1\mathfrak{a}_2$$

miteinander verbunden sind. Zunächst freilich erscheinen die rechts befindlichen Produkte von je zwei zweigliedrigen Moduln als die viergliedrigen Moduln

$$\begin{aligned}
\mathfrak{a}_1\mathfrak{a}_2 &= [\ 9,\ 3\ +3\theta,\ 6\ +3\theta,\ -\ 3+3\theta],\\
\mathfrak{b}_1\mathfrak{b}_2 &= [49,\ 21+7\theta,\ 28+7\theta,\ 7+7\theta],\\
\mathfrak{a}_1\mathfrak{b}_2 &= [21,\ 12+3\theta,\ 14+7\theta,\ 3+6\theta],\\
\mathfrak{b}_1\mathfrak{a}_2 &= [21,\ 7\ +7\theta,\ 9\ +3\theta,\ -\ 2+4\theta],
\end{aligned}$$

aber diese und auch die Moduln $\mathfrak{o}\mu$, $\mathfrak{o}\nu$ lassen sich nach der in § 172 angegebenen Methode auf zweigliedrige Moduln von der Form $[a,\ b+c\theta]$ reduzieren, wo a, b, c ganze rationale Zahlen bedeuten; diese Reduktion ist in den dortigen Beispielen, wo man nur $\omega_1 = 1$, $\omega_2 = \theta$ zu setzen braucht, schon ausgeführt und ergibt als Resultat die Gleichungen (24). Offenbar bilden nun diese Zerlegungen (24), in welchen nur von wirklich in $\mathfrak{o}$ enthaltenen Zahlen die Rede ist, einen vollständigen Ersatz für die Zerlegungen (13), die innerhalb dieses Gebietes $\mathfrak{o}$ schlechterdings unausführbar sind.

§ 177.

Das soeben behandelte Beispiel läßt vermuten, daß die eigentümlichen Lücken, die bei der Untersuchung über die Teilbarkeit der Zahlen ω innerhalb eines Gebietes $\mathfrak{o}$ auftreten und eine gewisse Unvollständigkeit desselben erkennen lassen, dadurch ausgefüllt werden können, daß man statt der einzelnen Zahlen ω in $\mathfrak{o}$ ganze Systeme solcher Zahlen einführt. Am nächsten liegt, wenn μ eine bestimmte, von Null verschiedene Zahl in $\mathfrak{o}$ bedeutet, die Betrachtung des schon im vorigen Paragraphen besprochenen Systems $\mathfrak{m} = \mathfrak{o}\mu$ aller durch μ teilbaren Zahlen $\omega\mu$. Wir heben die dort erwähnten Elementarsätze der Teilbarkeit nochmals als Eigenschaften eines jeden solchen Systems $\mathfrak{m}$ in folgender Weise hervor:

I. Das System $\mathfrak{m}$ besteht aus lauter ganzen Zahlen des Körpers Ω, und diese Zahlen reproduzieren sich durch Addition und Subtraktion, d. h. $\mathfrak{m}$ ist ein durch $\mathfrak{o}$ teilbarer, also ganzer Modul.

II. Ist λ eine in $\mathfrak{m}$ enthaltene Zahl, so ist jede durch λ teilbare Zahl $\omega\lambda$ des Körpers Ω ebenfalls in $\mathfrak{m}$ enthalten, d. h. das Produkt $\mathfrak{o}\mathfrak{m}$ ist teilbar durch $\mathfrak{m}$.

Dieselben beiden Eigenschaften kommen aber nicht bloß solchen Systemen $\mathfrak{m}$ zu, welche von der Form $\mathfrak{o}\mu$ sind, sondern z. B. auch dem System $\mathfrak{m}$ aller in $\mathfrak{o}$ enthaltenen Wurzeln ω einer Kongruenz von der Form $\nu\omega \equiv 0 \pmod{\alpha}$, wo ν und α bestimmte Zahlen in $\mathfrak{o}$ bedeuten, und in dem eben behandelten Beispiel hat sich gezeigt, daß es solche Systeme $\mathfrak{m}$ gibt, welche schlechterdings nicht von der Form $\mathfrak{o}\mu$ sind, die aber doch einen wesentlichen Dienst leisten, indem sie bei den Untersuchungen über die Teilbarkeit einen gewissen Ersatz für die fehlende (ideale) Zahl μ liefern. Diese Erscheinung veranlaßt uns, von der Existenz einer Zahl μ, durch welche ein solches System $\mathfrak{m}$ erzeugt werden könnte, ganz abzusehen und lediglich an den Eigenschaften I und II festzuhalten, welche an sich einen vollkommen klaren und bestimmten, von der Existenz einer erzeugenden Zahl μ unabhängigen Sinn haben. Jedes System $\mathfrak{m}$, welches diese beiden Eigenschaften besitzt, wollen wir (wegen der im vorigen Paragraphen besprochenen Beziehung zu Kummers idealen Zahlen) ein Ideal des Körpers Ω oder des Gebietes $\mathfrak{o}$ nennen; ist aber $\mathfrak{m} = \mathfrak{o}\mu$, gibt es also eine Zahl μ, durch welche das Ideal $\mathfrak{m}$ in der angegebenen Weise erzeugt wird, so soll $\mathfrak{m}$ ein Hauptideal genannt werden, weil solche Ideale unter den übrigen eine ähnliche oder vielmehr dieselbe Stellung einnehmen, welche z. B. in der Theorie der binären quadratischen Formen den der Hauptklasse angehörigen Formen unter den übrigen zukommt.

Zufolge dieser Definition würde die Zahl Null für sich allein ein Ideal bilden, und manche der im folgenden zu entwickelnden Sätze würden ihre Gültigkeit auch für diesen besonderen Fall nicht verlieren; da es aber für die Ausdrucksweise lästig sein würde, die etwaigen Ausnahmen immer anzugeben, so wollen wir diesen Fall lieber gänzlich ausschließen. Die vollständige Definition lautet daher:

III. Ein Modul $\mathfrak{m}$ heißt ein Ideal (in $\mathfrak{o}$), wenn er von Null verschieden ist und den beiden Bedingungen $\mathfrak{m} > \mathfrak{o}$, $\mathfrak{o}\mathfrak{m} > \mathfrak{m}$ genügt.

Unsere Aufgabe besteht nun darin, aus dieser Erklärung alle Eigenschaften der in $\mathfrak{o}$ enthaltenen Ideale und alle ihre Beziehungen

zueinander abzuleiten. In dieser Theorie der Ideale sind (nach § 176, III) jedenfalls die Gesetze der Teilbarkeit der Zahlen innerhalb $\mathfrak{o}$ vollständig enthalten; aber es wird sich auch umgekehrt zeigen, daß diese Teilbarkeitsgesetze nur durch Zuziehung aller Ideale gewonnen werden können. Da jedes Ideal ein Modul ist, so benutzen wir hierbei alle Begriffe und Sätze der allgemeinen Theorie der Moduln (§§ 168 — 172); die Theorie der Ideale $\mathfrak{m}$ wird aber infolge der zweiten Eigenschaft, nach welcher $\mathfrak{o}\mathfrak{m} > \mathfrak{m}$ ist, eine bei weitem bestimmtere Gestalt erhalten.

Wir bemerken zunächst, daß jedes Ideal $\mathfrak{m}$ zufolge der ersten Eigenschaft $\mathfrak{m} > \mathfrak{o}$ ein endlicher Modul ist (§ 172, V), und da es zufolge der zweiten Eigenschaft $\mathfrak{o}\mathfrak{m} > \mathfrak{m}$ offenbar n voneinander unabhängige Zahlen enthält, so ist jedes Ideal $\mathfrak{m}$ ein Modul von der Form (8) in § 175. Sodann leuchtet ein, daß diese zweite Eigenschaft, weil $\mathfrak{z} > \mathfrak{o}$, also $\mathfrak{m} > \mathfrak{o}\mathfrak{m}$ ist, sich in der schärferen Form

$$\mathfrak{o}\mathfrak{m} = \mathfrak{m} \tag{1}$$

darstellen läßt, und hierin liegt, weil $\mathfrak{o}$ offenbar selbst ein Ideal ist, ein erster Satz über die Multiplikation der Ideale, mit welcher wir uns sogleich näher zu beschäftigen haben. Schon hieraus erkennt man, daß dieses in allen Idealen aufgehende Ideal $\mathfrak{o}$ hier dieselbe Stellung einnimmt, wie die Zahl 1 in der rationalen Zahlentheorie. Wir können hinzufügen, daß $\mathfrak{o}$ ein Hauptideal ist; denn wenn $\varepsilon = 1$ oder irgendeine andere Einheit ist, so ist $\mathfrak{o}\varepsilon = \mathfrak{o}$ [§ 176, (10)]. Ferner leuchtet ein, daß ein Hauptideal $\mathfrak{o}\mu$ stets und nur dann durch ein Ideal $\mathfrak{m}$ teilbar ist, wenn die Zahl μ in $\mathfrak{m}$ enthalten ist, weil $\mathfrak{o}\mathfrak{m} > \mathfrak{m}$, und μ in $\mathfrak{o}\mu$ enthalten ist. Aus diesem Grunde wollen wir von jeder in $\mathfrak{m}$ enthaltenen Zahl μ (selbst von der Zahl Null) auch sagen, sie sei teilbar durch $\mathfrak{m}$, oder $\mathfrak{m}$ gehe in μ auf, oder $\mathfrak{m}$ sei ein Teiler von μ. Offenbar ist $\mathfrak{o}$ das einzige Ideal, das in einer Einheit ε aufgeht, weil $\mathfrak{o}\varepsilon = \mathfrak{o}$ ist. Ebenso soll ein Ideal $\mathfrak{m}$ teilbar durch die Zahl α heißen, wenn $\mathfrak{m} > \mathfrak{o}\alpha$, also jede in $\mathfrak{m}$ enthaltene Zahl μ durch α teilbar ist; setzt man $\mu = \alpha\beta$, so erkennt man leicht, daß die Quotienten β, welche allen Zahlen μ entsprechen, ein Ideal $\mathfrak{b} = \mathfrak{m}\alpha^{-1}$ bilden, mithin $\mathfrak{m} = \alpha\mathfrak{b}$ ist (vgl. den unten folgenden Satz VII). Nach diesen vorläufigen Bemerkungen wenden wir uns zu den folgenden Hauptsätzen über die Multiplikation der Ideale.

IV. Das Produkt von zwei Idealen $\mathfrak{a}$, $\mathfrak{b}$ ist ein Ideal und zwar ein gemeinsames Vielfaches von $\mathfrak{a}$, $\mathfrak{b}$, mithin

$$\mathfrak{a}\mathfrak{b} > \mathfrak{a} - \mathfrak{b}. \tag{2}$$

Denn weil $\mathfrak{a}$ und $\mathfrak{b}$ von Null verschieden sind, so gilt dasselbe von $\mathfrak{a}\mathfrak{b}$; aus $\mathfrak{o}\mathfrak{a} = \mathfrak{a}$ folgt ferner $\mathfrak{o}(\mathfrak{a}\mathfrak{b}) = (\mathfrak{o}\mathfrak{a})\mathfrak{b} = \mathfrak{a}\mathfrak{b}$; da endlich $\mathfrak{a}$ und $\mathfrak{b}$ durch $\mathfrak{o}$ teilbar sind, so ist $\mathfrak{a}\mathfrak{b}$ (nach § 170, I) teilbar durch $\mathfrak{o}\mathfrak{b}$ und $\mathfrak{a}\mathfrak{o}$, d. h. durch $\mathfrak{b}$ und $\mathfrak{a}$, also auch durch $\mathfrak{o}$, w. z. b. w.

V. Jedes Ideal $\mathfrak{m}$ ist ein eigentlicher Modul, dessen Ordnung $= \mathfrak{o}$, mithin

$$\mathfrak{m}\mathfrak{m}^{-1} = \mathfrak{o}. \tag{3}$$

Denn $\mathfrak{m}$ ist ein endlicher, von Null verschiedener Modul, der aus lauter algebraischen Zahlen besteht; mithin läßt sich $\mathfrak{m}$ (nach § 173, VI) durch Multiplikation mit einem Modul $\mathfrak{n}$, dessen Zahlen im Körper Ω enthalten sind, in einen Modul $\mathfrak{m}\mathfrak{n}$ verwandeln, welcher $< \mathfrak{z}$ ist und aus lauter ganzen Zahlen des Körpers Ω besteht, also $> \mathfrak{o}$ ist; da nun $\mathfrak{o}\mathfrak{z} = \mathfrak{o}\mathfrak{o} = \mathfrak{o}$, und $\mathfrak{o}(\mathfrak{m}\mathfrak{n}) = (\mathfrak{o}\mathfrak{m})\mathfrak{n} = \mathfrak{m}\mathfrak{n}$ ist, so folgt aus $\mathfrak{z} > \mathfrak{m}\mathfrak{n} > \mathfrak{o}$ durch Multiplikation mit $\mathfrak{o}$, daß $\mathfrak{m}\mathfrak{n} = \mathfrak{o}$ ist, woraus alles übrige sich leicht ergibt. Denn wenn man mit der Ordnung $\mathfrak{m}^0$ multipliziert und berücksichtigt, daß stets $\mathfrak{m}\mathfrak{m}^0 = \mathfrak{m}$ ist [§ 170, (23)], so erhält man zunächst $\mathfrak{o}\mathfrak{m}^0 = \mathfrak{o}$, also $\mathfrak{m}^0 > \mathfrak{o}$, und da andererseits aus $\mathfrak{o}\mathfrak{m} > \mathfrak{m}$ auch $\mathfrak{o} > \mathfrak{m}^0$ folgt, so ist $\mathfrak{m}^0 = \mathfrak{o}$*). Jedes Ideal $\mathfrak{m}$ ist also ein Faktor seiner Ordnung $\mathfrak{o} = \mathfrak{m}\mathfrak{n}$, und hieraus folgt (§ 170, V), daß $\mathfrak{m}$ ein eigentlicher Modul, daß $\mathfrak{m}^{-1} = \mathfrak{o}\mathfrak{n}$, und $\mathfrak{m}\mathfrak{m}^{-1} = \mathfrak{o}$ ist, w. z. b. w.

VI. Sind $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{b}'$ Ideale, und ist $\mathfrak{a}\mathfrak{b} > \mathfrak{a}\mathfrak{b}'$, so ist $\mathfrak{b} > \mathfrak{b}'$; aus $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{b}'$ folgt $\mathfrak{b} = \mathfrak{b}'$, und wenn $\mathfrak{a} > \mathfrak{a}\mathfrak{b}$, so ist $\mathfrak{b} = \mathfrak{o}$.

Dies ergibt sich unmittelbar durch Multiplikation mit $\mathfrak{a}^{-1}$ mit Rücksicht auf (3) und (1).

VII. Ist das Ideal $\mathfrak{m}$ teilbar durch das Ideal $\mathfrak{a}$, so gibt es ein (und nur ein) Ideal $\mathfrak{b}$, welches der Bedingung $\mathfrak{a}\mathfrak{b} = \mathfrak{m}$ genügt, und zwar ist $\mathfrak{b} = \mathfrak{m} : \mathfrak{a} = \mathfrak{m}\mathfrak{a}^{-1}$.

Denn der Modul $\mathfrak{b} = \mathfrak{m}\mathfrak{a}^{-1}$, welcher (nach § 170, VII) auch $= \mathfrak{m} : \mathfrak{a}$ ist, erfüllt zufolge (3) und (1) die Forderung $\mathfrak{a}\mathfrak{b} = \mathfrak{m}$ und

*) Dies würde sich auch ohne Zuziehung des Satzes VI in § 173 leicht beweisen lassen.

ist daher auch von Null verschieden; aus $\mathfrak{m} > \mathfrak{a}$ folgt durch Multiplikation mit $\mathfrak{a}^{-1}$, daß $\mathfrak{b} > \mathfrak{o}$ ist, und da $\mathfrak{o}\,\mathfrak{b} = (\mathfrak{o}\,\mathfrak{m})\,\mathfrak{a}^{-1} = \mathfrak{m}\,\mathfrak{a}^{-1} = \mathfrak{b}$ ist, so ist $\mathfrak{b}$ ein Ideal, w. z. b. w.

Durch diesen Satz, welcher als eine Umkehrung des Satzes IV angesehen werden kann, ist der wichtige Zusammenhang zwischen den Begriffen der Teilbarkeit der Ideale und ihrer Multiplikation aufgedeckt*). Der Kürze halber wollen wir in der Folge unter einem Faktor eines Ideals $\mathfrak{m}$ ausschließlich jeden Teiler $\mathfrak{a}$ von $\mathfrak{m}$ verstehen, der selbst ein Ideal ist. Dann besteht folgender Satz:

VIII. Die Anzahl der Faktoren eines Ideals ist endlich.

Denn wählt man aus dem Ideal $\mathfrak{m}$ nach Belieben eine von Null verschiedene Zahl μ, so ist (nach § 176, II) die Klassenanzahl $(\mathfrak{o}, \mathfrak{o}\,\mu) = \pm N(\mu) > 0$, und folglich gibt es (nach § 171, II) nur eine endliche Anzahl von Moduln, welche $> \mathfrak{o}$ und zugleich $< \mathfrak{o}\,\mu$ sind; da aber $\mathfrak{o}\,\mu > \mathfrak{m}$, so ist jeder Faktor von $\mathfrak{m}$ ein solcher Modul, und folglich ist auch die Anzahl dieser Faktoren endlich, w. z. b. w.

IX. Jedes Ideal $\mathfrak{m}$ kann durch Multiplikation mit einem Ideal $\mathfrak{n}$ in ein Hauptideal $\mathfrak{o}\,\mu = \mathfrak{m}\,\mathfrak{n}$ verwandelt werden**).

Denn wenn μ wieder irgendeine von Null verschiedene Zahl in $\mathfrak{m}$ bedeutet, so ist $\mathfrak{o}\,\mu > \mathfrak{m}$, woraus der Satz (nach VII) folgt. Da ferner $N(\mu)$ (nach § 176, IV) durch μ, also auch durch $\mathfrak{m}$ teilbar und von Null verschieden ist, so ergibt sich (aus § 172, I) noch der folgende Satz:

X. In jedem Ideal $\mathfrak{m}$ gibt es unendlich viele rationale Zahlen, deren Inbegriff

$$\mathfrak{m} - \mathfrak{z} = [m]$$

ist, wo $m = (\mathfrak{z}, \mathfrak{m})$ die kleinste durch $\mathfrak{m}$ teilbare natürliche Zahl bedeutet.

---

*) Hierin bestand die größte Schwierigkeit, welche bei der ersten Begründung der Ideal-Theorie zu überwinden war. Um dieselbe zu würdigen, vergleiche man die zweite und dritte Auflage dieses Werkes [vgl. XLVII und XLIX] und § 23 meiner Schrift Sur la théorie des nombres entiers algébriques (Paris 1877); denn wenn jetzt durch Zuziehung des Satzes VI in § 173 dieser Kardinalpunkt schon im Anfange der Theorie gewonnen wird, so lassen die früheren Darstellungen das Wesen desselben deutlicher erkennen, was für gewisse Verallgemeinerungen der Ideal-Theorie sehr wichtig ist.

**) Vgl. § 178, XI.

§ 178.

Der größte gemeinsame Teiler $a + b$ und das kleinste gemeinsame Vielfache $a — b$ von zwei Idealen a, b sind ebenfalls Ideale. Denn jedenfalls sind die Moduln $a + b$ und $a — b$ teilbar durch o, weil dasselbe von a und b gilt; da nun $a — b$ teilbar ist durch a und b, so ist $o(a — b)$ teilbar durch oa und ob, d. h. durch a und b, also auch durch $a — b$; und da das von Null verschiedene Produkt ab (nach § 177, IV) durch $a — b$ teilbar ist, so ist $a — b$ auch von Null verschieden und folglich ein Ideal. Da ferner $o(a + b) = oa + ob = a + b$, und $a + b$ als Teiler des Ideals a oder b gewiß von Null verschieden ist, so ist $a + b$ ein Ideal. Dasselbe gilt offenbar von dem gemeinsamen größten Teiler und kleinsten Vielfachen von beliebig vielen Idealen, und es ergeben sich die folgenden Sätze:

I. Sind $a, b, c \ldots$ beliebige Ideale, so ist deren kleinstes gemeinsames Vielfaches

(1) $$a — b — c — \cdots = aa_1 = bb_1 = cc_1 = \cdots,$$

wo $a_1, b_1, c_1 \ldots$ Ideale bedeuten, deren größter gemeinsamer Teiler

(2) $$a_1 + b_1 + c_1 + \cdots = o$$

ist.

Denn wenn man der Kürze wegen $m = a — b — c — \cdots$ und $n = a_1 + b_1 + c_1 + \cdots$ setzt, so ist das Ideal m teilbar durch $a, b, c \ldots$, und folglich genügen (nach § 177, VII) die Ideale $a_1 = ma^{-1}$, $b_1 = mb^{-1}$, $c_1 = mc^{-1} \ldots$ den Bedingungen (1); da sie ferner alle durch das Ideal n teilbar sind, so sind auch die Produkte $a_1 n^{-1}$, $b_1 n^{-1}$, $c_1 n^{-1} \ldots$ Ideale, und hieraus folgt nach (1), daß mn^{-1} (zufolge § 177, IV) durch $a, b, c \ldots$ teilbar, also $mn^{-1} > m$, $m > mn$, mithin (nach § 177, VI) $n = o$ ist, w. z. b. w.

Aus dem Beweise folgt, daß der in (2) enthaltene Satz auch in der Form

(3) $$(a — b — c — \cdots)^{-1} = a^{-1} + b^{-1} + c^{-1} + \cdots$$

dargestellt werden kann; er bildet das dualistische Gegenstück zu dem Satze

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

welcher eine unmittelbare Folge des zweiten Modulsatzes (18) in § 170 ist.

II. Zu je zwei Idealen $\mathfrak{a}$, $\mathfrak{b}$ gehören zwei Ideale $\mathfrak{a}'$, $\mathfrak{b}'$, welche den Bedingungen

$$\mathfrak{a} - \mathfrak{b} = \mathfrak{a}\mathfrak{b}' = \mathfrak{b}\mathfrak{a}' \tag{5}$$

$$\mathfrak{a}' + \mathfrak{b}' = \mathfrak{o} \tag{6}$$

$$\mathfrak{a} = (\mathfrak{a} + \mathfrak{b})\mathfrak{a}', \quad \mathfrak{b} = (\mathfrak{a} + \mathfrak{b})\mathfrak{b}' \tag{7}$$

genügen; zugleich ist

$$(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} - \mathfrak{b}) = \mathfrak{a}\mathfrak{b}. \tag{8}$$

Die Gleichungen (5), (6) folgen als spezieller Fall aus (1), (2); multipliziert man (6) mit $\mathfrak{a}$ oder mit $\mathfrak{b}$, so folgt (7) aus (5), und wenn man (5) mit $\mathfrak{a} + \mathfrak{b}$ multipliziert, so folgt (8) aus (7), w. z. b. w.

Ersetzt man $\mathfrak{a}$ und $\mathfrak{b}$ in (8) durch $\mathfrak{a}\mathfrak{c}$ und $\mathfrak{b}\mathfrak{c}$, wo $\mathfrak{c}$ ein beliebiges Ideal bedeutet, und dividiert durch

$$\mathfrak{a}\mathfrak{c} + \mathfrak{b}\mathfrak{c} = (\mathfrak{a} + \mathfrak{b})\mathfrak{c}, \tag{9}$$

so folgt aus (8) auch der Satz*)

$$\mathfrak{a}\mathfrak{c} - \mathfrak{b}\mathfrak{c} = (\mathfrak{a} - \mathfrak{b})\mathfrak{c}; \tag{10}$$

derselbe ergibt sich auch aus (5), wenn man bedenkt, daß zufolge (7) und (9) die Ideale $\mathfrak{a}'$, $\mathfrak{b}'$ ungeändert bleiben, wenn man $\mathfrak{a}$, $\mathfrak{b}$ durch $\mathfrak{a}\mathfrak{c}$, $\mathfrak{b}\mathfrak{c}$ ersetzt.

Zwei Ideale $\mathfrak{a}$, $\mathfrak{b}$ heißen relative Primideale, wenn ihr größter gemeinsamer Teiler $\mathfrak{a} + \mathfrak{b} = \mathfrak{o}$ ist. In diesem Falle sind die eben mit $\mathfrak{a}'$, $\mathfrak{b}'$ bezeichneten Ideale [welche zufolge (6) immer relative Primideale sind] identisch mit $\mathfrak{a}$, $\mathfrak{b}$, und zufolge (8) oder (5) ist das kleinste gemeinsame Vielfache zweier relativen Primideale zugleich ihr Produkt; umgekehrt folgt aus $\mathfrak{a} - \mathfrak{b} = \mathfrak{a}\mathfrak{b}$, daß $\mathfrak{a} + \mathfrak{b} = \mathfrak{o}$, daß also $\mathfrak{a}$, $\mathfrak{b}$ relative Primideale sind. Offenbar ist $\mathfrak{o}$ relatives Primideal zu jedem Ideal, also auch zu sich selbst, und kein anderes Ideal hat diese Eigenschaft. Die zunächst folgenden Sätze stimmen vollständig mit denen der rationalen Zahlentheorie überein (§ 5), wobei wir ein für allemal bemerken, daß mehr als zwei Ideale dann und nur dann relative Primideale heißen sollen, wenn jedes von ihnen relatives Primideal zu jedem der übrigen ist.

*) Vgl. die Sätze (8), (9) in § 170. — Wir bemerken noch, daß die in der Anmerkung zu § 171 auf S. 77 erwähnte Gruppe von 28 Moduln, welche aus drei beliebigen Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ entspringt, auf eine Gruppe von 18 Moduln einschrumpft, falls $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ Ideale sind, weil gleichzeitig die dortige Klassenanzahl $d = 1$ wird.

III. Sind $\mathfrak{a}, \mathfrak{b}$ relative Primideale, und ist $\mathfrak{c}$ ein beliebiges Ideal, so ist der größte gemeinschaftliche Teiler der beiden Ideale $\mathfrak{a}, \mathfrak{b}\mathfrak{c}$ zugleich derjenige der beiden Ideale $\mathfrak{a}, \mathfrak{c}$, also $\mathfrak{a} + \mathfrak{b}\mathfrak{c} = \mathfrak{a} + \mathfrak{c}$.

Denn durch Multiplikation von $\mathfrak{a} + \mathfrak{b} = \mathfrak{o}$ mit $\mathfrak{c}$ folgt zunächst $\mathfrak{a}\mathfrak{c} + \mathfrak{b}\mathfrak{c} = \mathfrak{c}$; addiert man $\mathfrak{a}$ und bedenkt, daß $\mathfrak{a}\mathfrak{c} > \mathfrak{a}$, also $\mathfrak{a}\mathfrak{c} + \mathfrak{a} = \mathfrak{a}$ ist, so folgt $\mathfrak{a} + \mathfrak{b}\mathfrak{c} = \mathfrak{a} + \mathfrak{c}$, w. z. b. w.

IV. Ist $\mathfrak{a}$ relatives Primideal zu jedem der beiden Ideale $\mathfrak{b}, \mathfrak{c}$, so ist $\mathfrak{a}$ auch relatives Primideal zu deren Produkte $\mathfrak{b}\mathfrak{c}$.

Dies folgt unmittelbar aus dem vorhergehenden Satze, weil $\mathfrak{a} + \mathfrak{c} = \mathfrak{o}$ ist. Durch wiederholte Anwendung ergibt sich (wie in § 5) der Satz:

V. Ist jedes der Ideale $\mathfrak{a}, \mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3 \ldots$ relatives Primideal zu jedem der Ideale $\mathfrak{b}, \mathfrak{b}_1, \mathfrak{b}_2 \ldots$, so sind auch die beiden Produkte $\mathfrak{a}\mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3 \ldots$ und $\mathfrak{b}\mathfrak{b}_1\mathfrak{b}_2 \ldots$, und ebenso auch irgend zwei Potenzen $\mathfrak{a}^r, \mathfrak{b}^s$ relative Primideale.

VI. Sind $\mathfrak{a}, \mathfrak{b}$ relative Primideale, und ist $\mathfrak{b}\mathfrak{c} > \mathfrak{a}$, so ist auch $\mathfrak{c} > \mathfrak{a}$.

Dies folgt ebenfalls aus III, weil $\mathfrak{a} + \mathfrak{b}\mathfrak{c} = \mathfrak{a}$ ist.

VII. Sind $\mathfrak{a}, \mathfrak{b}$ relative Primideale, so ist jeder Faktor $\mathfrak{a}'$ von $\mathfrak{a}$ relatives Primideal zu jedem Faktor $\mathfrak{b}'$ von $\mathfrak{b}$.

Denn aus $\mathfrak{a} > \mathfrak{a}' > \mathfrak{o}$ und $\mathfrak{b} > \mathfrak{b}' > \mathfrak{o}$ folgt $\mathfrak{a} + \mathfrak{b} > \mathfrak{a}' + \mathfrak{b}' > \mathfrak{o}$, und da $\mathfrak{a} + \mathfrak{b} = \mathfrak{o}$ ist, so ist auch $\mathfrak{a}' + \mathfrak{b}' = \mathfrak{o}$, w. z. b. w.

VIII. Sind $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \ldots$ relative Primideale, so ist ihr kleinstes gemeinsames Vielfaches zugleich ihr Produkt, also

$$(11) \qquad \mathfrak{a} - \mathfrak{b} - \mathfrak{c} - \cdots = \mathfrak{a}\mathfrak{b}\mathfrak{c} \ldots$$

Für zwei relative Primideale $\mathfrak{a}, \mathfrak{b}$ ist dieser Satz schon oben aus II. abgeleitet. Nehmen wir an, er sei für r relative Primideale $\mathfrak{b}, \mathfrak{c} \ldots$ bewiesen, und $\mathfrak{a}$ sei relatives Primideal zu jedem von ihnen, also auch zu ihrem Produkte $\mathfrak{a}_1 = \mathfrak{b}\mathfrak{c} \cdots = \mathfrak{b} - \mathfrak{c} - \cdots$, so ist das kleinste gemeinsame Vielfache aller $(r + 1)$ Ideale $= \mathfrak{a} - \mathfrak{a}_1 = \mathfrak{a}\mathfrak{a}_1$, mithin gilt der Satz allgemein, w. z. b. w.

Zugleich leuchtet ein, daß die im Satze I auftretenden $(r + 1)$ Ideale $\mathfrak{a}_1, \mathfrak{b}_1, \mathfrak{c}_1 \ldots$ in unserem Falle die aus je r von den Idealen

$\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$... gebildeten Produkte sind. — Aus den vorhergehenden Sätzen ergibt sich nun der folgende wichtige Existenzsatz*):

IX. Ist das Ideal $\mathfrak{a}$ durch keins der Ideale $\mathfrak{c}_1$, $\mathfrak{c}_2$... teilbar, so gibt es in $\mathfrak{a}$ auch eine Zahl α, welche in keinem der Ideale $\mathfrak{c}$ enthalten ist.

Wenn nur ein einziges Ideal $\mathfrak{c}$ vorliegt (oder wenn $\mathfrak{a}$ ein Hauptideal ist), so versteht sich der Satz von selbst. Wir nehmen an, er sei schon für alle Fälle bewiesen, wo die Anzahl der Ideale $\mathfrak{c}$ kleiner als r ist, und zeigen, daß er dann auch für r Ideale $\mathfrak{c}_1, \mathfrak{c}_2 \ldots \mathfrak{c}_r$, mithin allgemein gilt. Jedem dieser Ideale $\mathfrak{c}_s$ entspricht ein Ideal $\mathfrak{b}_s$, welches der Bedingung $\mathfrak{a}\mathfrak{b}_s = \mathfrak{a} - \mathfrak{c}_s$ genügt und folglich von $\mathfrak{o}$ verschieden ist; das Ideal $\mathfrak{a}$ ist durch keins der r Produkte $\mathfrak{a}\mathfrak{b}_s$ teilbar, und es genügt, die Existenz einer in $\mathfrak{a}$ enthaltenen Zahl α nachzuweisen, welche durch keins dieser Produkte und folglich auch durch keins der Ideale $\mathfrak{c}_s$ teilbar ist. Gibt es nun unter den r Idealen $\mathfrak{b}_s$ ein Paar, z. B. $\mathfrak{b}_1$ und $\mathfrak{b}_2$, deren größter gemeinschaftlicher Teiler von $\mathfrak{o}$ verschieden ist, so ist $\mathfrak{a}$ auch nicht teilbar durch $\mathfrak{a}(\mathfrak{b}_1 + \mathfrak{b}_2)$, und folglich gibt es (nach unserer Annahme) in $\mathfrak{a}$ eine Zahl α, welche durch keins der $(r-1)$ Ideale $\mathfrak{a}(\mathfrak{b}_1 + \mathfrak{b}_2)$, $\mathfrak{a}\mathfrak{b}_3 \ldots \mathfrak{a}\mathfrak{b}_r$ teilbar ist, mithin die geforderte Eigenschaft besitzt, weil $\mathfrak{a}\mathfrak{b}_1$ und $\mathfrak{a}\mathfrak{b}_2$ durch $\mathfrak{a}(\mathfrak{b}_1 + \mathfrak{b}_2)$ teilbar sind. Es bleibt daher nur noch der Fall übrig, wo die r Ideale $\mathfrak{b}_s$ relative Primideale sind. Dann ist jedes dieser Ideale $\mathfrak{b}_s$ relatives Primideal zu dem aus allen übrigen gebildeten Produkte $\mathfrak{b}'_s$, und da $\mathfrak{b}_s$ von $\mathfrak{o}$ verschieden ist, so ist $\mathfrak{b}'_s$ nicht teilbar durch $\mathfrak{b}_s$, also $\mathfrak{a}\mathfrak{b}'_s$ auch nicht teilbar durch $\mathfrak{a}\mathfrak{b}_s$, und es gibt folglich in $\mathfrak{a}\mathfrak{b}'_s$ eine Zahl α_s, welche nicht durch $\mathfrak{a}\mathfrak{b}_s$ teilbar ist. Setzt man nun $\alpha = \alpha_1 + \alpha_2 + \cdots + \alpha_r$, so ist die Zahl α wie jede der r Zahlen α_s in $\mathfrak{a}$ enthalten, aber sie kann durch keins der r Produkte $\mathfrak{a}\mathfrak{b}_s$ teilbar sein; denn weil die Ideale $\mathfrak{b}'_2, \mathfrak{b}'_3 \ldots \mathfrak{b}'_r$ alle durch $\mathfrak{b}_1$, also die Zahlen $\alpha_2, \alpha_3 \ldots \alpha_r$ alle durch $\mathfrak{a}\mathfrak{b}_1$ teilbar sind, während das Gegenteil

*) Auf den ersten Blick könnte es scheinen, als müßte derselbe auch für beliebige Moduln gelten. Dies ist wirklich noch wahr, wenn nur zwei Moduln $\mathfrak{c}_1$, $\mathfrak{c}_2$ vorliegen; denn wählt man aus $\mathfrak{a}$ zwei Zahlen α_1, α_2, von denen die erste nicht in $\mathfrak{c}_1$, die zweite nicht in $\mathfrak{c}_2$ enthalten ist, so hat mindestens eine der drei Zahlen α_1, α_2, $\alpha_1 + \alpha_2$ offenbar die geforderte Eigenschaft. Daß aber schon für drei Moduln $\mathfrak{c}_1$, $\mathfrak{c}_2$, $\mathfrak{c}_3$ der Satz nicht allgemein gilt, ergibt sich leicht aus der Betrachtung des Beispiels

$$\mathfrak{a} = [1, \omega],\ \mathfrak{c}_1 = [2, \omega],\ \mathfrak{c}_2 = [1, 2\omega],\ \mathfrak{c}_3 = [2, 1+\omega],$$

wo ω irgendeine irrationale Zahl bedeutet (vgl. § 171, IV).

für α_1 gilt, so kann auch α nicht durch $\mathfrak{a}\mathfrak{b}_1$, und ebensowenig kann α durch eins der übrigen Produkte $\mathfrak{a}\mathfrak{b}_s$ teilbar sein. Mithin hat die Zahl α die geforderte Eigenschaft, w. z. b. w.

X. Sind $\mathfrak{a}$, $\mathfrak{b}$ irgend zwei Ideale, so kann man eine von Null verschiedene Zahl α immer so wählen, daß $\mathfrak{a}\mathfrak{b} + \mathfrak{o}\alpha = \mathfrak{a}$, also $\mathfrak{a}\mathfrak{b} - \mathfrak{o}\alpha = \mathfrak{b}\alpha$ wird.

Denn wenn $\mathfrak{b} = \mathfrak{o}$ ist, so genügt offenbar jede Zahl α des Ideals $\mathfrak{a}$ dieser Forderung. Ist aber $\mathfrak{b}$ von $\mathfrak{o}$ verschieden, und bezeichnet man mit $\mathfrak{c}$ alle Ideale, welche $< \mathfrak{a}\mathfrak{b}$ und zugleich $> \mathfrak{a}$, aber verschieden von $\mathfrak{a}$ sind, so gibt es, weil deren Anzahl (nach § 177, VIII) endlich ist, in $\mathfrak{a}$ eine Zahl α, welche durch keins der Ideale $\mathfrak{c}$ teilbar ist; mithin ist auch das Ideal $\mathfrak{a}\mathfrak{b} + \mathfrak{o}\alpha$ verschieden von allen $\mathfrak{c}$, und da es ebenfalls $< \mathfrak{a}\mathfrak{b}$ und $> \mathfrak{a}$ ist, so muß $\mathfrak{a}\mathfrak{b} + \mathfrak{o}\alpha = \mathfrak{a}$, und nach (8) zugleich $\mathfrak{a}\mathfrak{b} - \mathfrak{o}\alpha = \mathfrak{b}\alpha$ sein, w. z. b. w.

XI. Sind $\mathfrak{a}$, $\mathfrak{b}$ Ideale, so läßt sich $\mathfrak{a}$ in ein Hauptideal $\mathfrak{o}\alpha$ verwandeln durch Multiplikation mit einem Ideal $\mathfrak{m}$, welches relatives Primideal zu $\mathfrak{b}$ ist.

Denn setzt man in dem vorigen Satze das durch $\mathfrak{a}$ teilbare Hauptideal $\mathfrak{o}\alpha = \mathfrak{a}\mathfrak{m}$, so ist $\mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{m} = \mathfrak{a}(\mathfrak{b} + \mathfrak{m}) = \mathfrak{a}$, also $\mathfrak{b} + \mathfrak{m} = \mathfrak{o}$, w. z. b. w.

XII. Jedes Ideal $\mathfrak{a}$ ist darstellbar als größter gemeinsamer Teiler von zwei Hauptidealen.

Denn wählt man nach Belieben aus $\mathfrak{a}$ eine von Null verschiedene Zahl μ, so ist $\mathfrak{o}\mu = \mathfrak{a}\mathfrak{b}$, und man kann (nach X) die Zahl α so wählen, daß $\mathfrak{o}\mu + \mathfrak{o}\alpha = \mathfrak{a}$ wird, w. z. b. w.

XIII. Zwei von Null verschiedene Zahlen α, β in $\mathfrak{o}$ sind stets und nur dann relative Primzahlen, wenn die durch sie erzeugten Hauptideale $\mathfrak{o}\alpha$, $\mathfrak{o}\beta$ relative Primideale sind, und es gibt dann immer zwei Zahlen ξ, η in $\mathfrak{o}$, welche der Bedingung

$$\alpha\xi + \beta\eta = 1 \tag{12}$$

genügen.

Denn wenn $\mathfrak{o}\alpha + \mathfrak{o}\beta = \mathfrak{o}$ ist, so ist die in $\mathfrak{o}$ enthaltene Zahl 1 als Summe von zwei in $\mathfrak{o}\alpha$, $\mathfrak{o}\beta$ enthaltenen Zahlen, also in der Form (12) darstellbar, d. h. α, β sind relative Primzahlen (§ 174). Im entgegengesetzten Falle, wenn $\mathfrak{o}\alpha + \mathfrak{o}\beta$ verschieden von $\mathfrak{o}$, also $\mathfrak{o}\alpha - \mathfrak{o}\beta$

zufolge (8) ein echter Teiler von $\mathfrak{o}\alpha\beta$ ist, gibt es eine durch α und β teilbare, d. h. eine in $\mathfrak{o}\alpha - \mathfrak{o}\beta$ enthaltene Zahl ω, welche nicht durch $\alpha\beta$ teilbar ist, und folglich können α, β (nach § 174) nicht relative Primzahlen sein, w. z. b. w.

Der zweite Teil dieses Satzes ergibt sich auch unmittelbar aus der Anmerkung zu § 174; denn zufolge derselben gibt es, wenn α, β relative Primzahlen in $\mathfrak{o}$ sind, auch zwei in $\mathfrak{o}$ enthaltene Zahlen ξ, η, welche die Bedingung (12) erfüllen, und hieraus folgt offenbar $\mathfrak{o}\alpha + \mathfrak{o}\beta = \mathfrak{o}$. Aber beide Beweise fließen, wie man leicht sieht, aus derselben Quelle, nämlich aus dem Satze VI in § 173.

Wir bemerken noch, daß wir unter dem größten gemeinsamen Teiler eines Ideals $\mathfrak{m}$ und einer Zahl α (selbst wenn letztere $= 0$ sein sollte) immer das Ideal $\mathfrak{m} + \mathfrak{o}\alpha$ verstehen; und wir sagen, $\mathfrak{m}$ sei relatives Primideal zu α, oder α sei relative Primzahl zu $\mathfrak{m}$, wenn $\mathfrak{m} + \mathfrak{o}\alpha = \mathfrak{o}$ ist*). Dann besteht folgender Satz:

XIV. Ist $\mathfrak{m}$ relatives Primideal zu der natürlichen Zahl k, so ist die kleinste durch $\mathfrak{m}$ teilbare natürliche Zahl $m = (\mathfrak{z}, \mathfrak{m})$ auch relative Primzahl zu k.

Denn bedeutet e den größten gemeinsamen Teiler der Zahlen $m = em'$ und k, so ist ihr kleinstes gemeinsames Vielfaches km' teilbar durch $\mathfrak{m}$ und $\mathfrak{o}k$, also auch durch $\mathfrak{m} - \mathfrak{o}k = k\mathfrak{m}$; mithin ist m' teilbar durch $\mathfrak{m}$, folglich $m' = m$, $e = 1$, w. z. b. w.

§ 179.

Das Ideal $\mathfrak{o}$ hat nur den einzigen Faktor $\mathfrak{o}$. Jedes von $\mathfrak{o}$ verschiedene Ideal $\mathfrak{p}$ besitzt gewiß zwei verschiedene Faktoren, nämlich $\mathfrak{o}$ und $\mathfrak{p}$, und es soll ein (absolutes) Primideal heißen, wenn es keine anderen Faktoren hat. Ein Ideal, welches mehr als zwei ver-

*) Endlich erwähnen wir, daß jeder Idealbruch, d. h. jeder Quotient von zwei Idealen, immer ein im Körper Ω enthaltener endlicher Modul $\mathfrak{i}$ von der Ordnung $\mathfrak{o}$ ist, und daß umgekehrt jeder solche Modul $\mathfrak{i}$ auf unendlich viele Arten als Idealbruch, und nur auf eine einzige Weise als ein solcher Idealbruch dargestellt werden kann, dessen Zähler und Nenner relative Primideale sind. Jedes Ideal ist ein Idealbruch mit dem Nenner $\mathfrak{o}$. Der größte gemeinsame Teiler, das kleinste gemeinsame Vielfache, das Produkt und der Quotient von irgend zwei Idealbrüchen sind ebenfalls Idealbrüche, und die Gesetze ihrer Bildung stimmen genau mit denen der rationalen Zahlentheorie überein. Die Beweise, welche hauptsächlich auf den in § 170 bewiesenen Sätzen über eigentliche Moduln beruhen wird der Leser leicht finden.

schiedene Faktoren besitzt, heißt zusammengesetzt (vgl. § 8). Aus dieser Erklärung ergeben sich die folgenden Sätze.

I. Ist $\mathfrak{p}$ ein Primideal, und $\mathfrak{a}$ irgendein Ideal, so ist entweder $\mathfrak{a}$ teilbar durch $\mathfrak{p}$, oder $\mathfrak{a}$ und $\mathfrak{p}$ sind relative Primideale.

Denn das Ideal $\mathfrak{a} + \mathfrak{p}$ ist als Faktor von $\mathfrak{p}$ entweder $= \mathfrak{p}$, oder $= \mathfrak{o}$, und im ersteren Falle ist $\mathfrak{a} > \mathfrak{p}$, w. z. b. w.

II. Geht das Primideal $\mathfrak{p}$ in dem Produkte der Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \ldots$ auf, so ist mindestens eins derselben durch $\mathfrak{p}$ teilbar.

Denn wenn $\mathfrak{p}$ in keinem der Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \ldots$ aufgeht, so ist $\mathfrak{p}$ (nach I) relatives Primideal zu jedem derselben, also (nach § 178, V) auch zu ihrem Produkte $\mathfrak{a}\mathfrak{b}\mathfrak{c}\ldots$, und folglich kann letzteres (nach I) auch nicht durch $\mathfrak{p}$ teilbar sein, w. z. b. w.

III. Ist $\mathfrak{m}$ ein zusammengesetztes Ideal, so gibt es zwei durch $\mathfrak{m}$ nicht teilbare Zahlen α, β, deren Produkt $\alpha\beta$ durch $\mathfrak{m}$ teilbar ist.

Denn $\mathfrak{m}$ besitzt einen von $\mathfrak{o}$ und $\mathfrak{m}$ verschiedenen Faktor $\mathfrak{a}$ und ist folglich $= \mathfrak{a}\mathfrak{b}$, wo $\mathfrak{b}$ ein von $\mathfrak{o}$ verschiedenes Ideal bedeutet; da nun (nach § 177, VI) weder $\mathfrak{a}$ noch $\mathfrak{b}$ durch $\mathfrak{m}$, d. h. durch $\mathfrak{a}\mathfrak{b}$ teilbar ist, so kann man aus $\mathfrak{a}$, $\mathfrak{b}$ Zahlen α, β wählen, die nicht in $\mathfrak{m}$, deren Produkt $\alpha\beta$ aber in $\mathfrak{a}\mathfrak{b}$, d. h. in $\mathfrak{m}$ enthalten ist, w. z. b. w.

Mithin ist eine Zahl μ dann und nur dann eine Primzahl (S. 110), wenn $\mathfrak{o}\mu$ ein Primideal ist.

IV. Jedes von $\mathfrak{o}$ verschiedene Ideal $\mathfrak{a}$ ist durch mindestens ein Primideal teilbar.

Der Satz ist richtig, wenn $\mathfrak{a}$ selbst ein Primideal ist. Im entgegengesetzten Falle besitzt $\mathfrak{a}$ einen von $\mathfrak{a}$ und $\mathfrak{o}$ verschiedenen Faktor $\mathfrak{b}$, und wenn dieser noch kein Primideal ist, so besitzt er einen von $\mathfrak{b}$ und $\mathfrak{o}$ verschiedenen Faktor $\mathfrak{c}$, und wenn dieser kein Primideal ist, so kann man in derselben Weise fortfahren. Da nun die in dieser Kette auftretenden Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \ldots$, deren jedes ein echtes Vielfaches des folgenden ist, alle voneinander verschieden und zugleich Faktoren des Ideals $\mathfrak{a}$ sind, welches (nach § 177, VIII) nur eine endliche Anzahl von Faktoren besitzt, so muß diese Kette notwendig eine endliche sein, sie muß ein letztes Glied $\mathfrak{p}$ enthalten, und dieses muß, weil sonst die Kette sich noch weiter fortsetzen ließe, ein Primideal sein, w. z. b. w.

V. Jedes von o verschiedene Ideal $\mathfrak{a}$ ist entweder ein Primideal, oder es läßt sich, und zwar nur auf eine einzige Weise, als ein Produkt von Primidealen darstellen.

Denn $\mathfrak{a}$ ist durch ein Primideal $\mathfrak{p}_1$ teilbar, also von der Form $\mathfrak{p}_1\mathfrak{a}_1$, wo $\mathfrak{a}_1$ ein Ideal; ist dasselbe $= \mathfrak{o}$, so ist $\mathfrak{a} = \mathfrak{p}_1$ ein Primideal. Ist aber $\mathfrak{a}_1$ verschieden von $\mathfrak{o}$, so ist wieder $\mathfrak{a}_1 = \mathfrak{p}_2\mathfrak{a}_2$, wo das erste der beiden Ideale $\mathfrak{p}_2$, $\mathfrak{a}_2$ ein Primideal bedeutet, und wenn $\mathfrak{a}_2$ von $\mathfrak{o}$ verschieden ist, so kann man in derselben Weise fortfahren. Die Kette der Ideale $\mathfrak{a}$, $\mathfrak{a}_1$, $\mathfrak{a}_2$ ..., deren jedes ein echtes Vielfaches des folgenden ist, muß eine endliche sein, also ein letztes Glied $\mathfrak{a}_r$ enthalten, und dieses muß $= \mathfrak{o}$ sein, weil sonst die Kette sich noch fortsetzen ließe. Zugleich ergibt sich die gewünschte Darstellung

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r. \tag{1}$$

Um zu zeigen, daß es im wesentlichen, d. h. abgesehen von der Aufeinanderfolge der Faktoren, nur eine einzige solche Darstellung gibt, bemerken wir zunächst, daß jeder der r Primfaktoren $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_r$ offenbar in $\mathfrak{a}$ aufgeht, und daß umgekehrt jedes in $\mathfrak{a}$ aufgehende Primideal $\mathfrak{p}$ notwendig mit einem dieser r Primfaktoren identisch sein muß; denn da $\mathfrak{p}$ in dem Produkte $\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r$ aufgeht, so muß (nach II) mindestens einer der Faktoren, z. B. $\mathfrak{p}_1$, durch $\mathfrak{p}$ teilbar sein, und da $\mathfrak{p}_1$ als Primideal nur die beiden Faktoren $\mathfrak{p}_1$ und $\mathfrak{o}$ besitzt, so muß das Primideal $\mathfrak{p}$, weil es von $\mathfrak{o}$ verschieden ist, notwendig $= \mathfrak{p}_1$ sein. Die in einer solchen Darstellung (1) auftretenden Faktoren sind also die sämtlichen in dem Ideal $\mathfrak{a}$ aufgehenden Primideale $\mathfrak{p}$ und keine anderen. Ist ferner e die genaue Anzahl derjenigen von diesen r Faktoren, welche mit einem bestimmten Primideal $\mathfrak{p}$ identisch sind, so kann man $\mathfrak{a} = \mathfrak{b}\mathfrak{p}^e$ setzen, wo $\mathfrak{b}$ entweder $= \mathfrak{o}$ oder, falls $e < r$ ist, das Produkt der übrigen $r - e$ Primfaktoren ist; da die letzteren alle von $\mathfrak{p}$ verschieden sind, so ist $\mathfrak{b}$ keinesfalls durch $\mathfrak{p}$ teilbar, und hieraus folgt (nach § 177, VI), daß $\mathfrak{a}$ zwar durch $\mathfrak{p}^e$, aber durch keine höhere Potenz von $\mathfrak{p}$ teilbar, daß also die Anzahl e zugleich der Exponent der höchsten in dem Ideal $\mathfrak{a}$ aufgehenden Potenz des Primideals $\mathfrak{p}$ ist. Mithin sind die in der Darstellung (1) des Ideals $\mathfrak{a}$ erscheinenden Primfaktoren $\mathfrak{p}$ nicht nur an sich, sondern auch nach der Häufigkeit ihres Auftretens vollständig bestimmt durch $\mathfrak{a}$ allein, w. z. b. w.

An den Beweis dieses Fundamentalsatzes knüpfen wir noch folgende Bemerkungen. Bezeichnet man jetzt mit $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3 \ldots$ alle voneinander verschiedenen, in dem Ideal $\mathfrak{a}$ aufgehenden Primideale, so nimmt die Darstellung (1) die Form

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \mathfrak{p}_3^{e_3} \ldots \tag{2}$$

an, wo die natürlichen Zahlen $e_1, e_2, e_3 \ldots$ die Häufigkeit des Auftretens für die einzelnen Primfaktoren angeben. Es kann gelegentlich, bei der Vergleichung mehrerer Ideale, von Vorteil sein, auch den Exponenten Null zuzulassen, in welchem Falle (nach § 177, V) die Potenz $\mathfrak{p}^0 = \mathfrak{o}$ zu setzen ist; dies bedeutet natürlich, daß das Ideal $\mathfrak{a}$ durch das Primideal $\mathfrak{p}$ gar nicht teilbar ist. In jedem Falle erscheint das Ideal $\mathfrak{a}$ als das Produkt oder (nach § 178, VIII) auch als das kleinste gemeinschaftliche Vielfache aller in ihm aufgehenden höchsten Primideal-Potenzen $\mathfrak{p}_1^{e_1}, \mathfrak{p}_2^{e_2}, \mathfrak{p}_3^{e_3} \ldots$, welche ja zugleich auch relative Primideale sind, und es ergibt sich der Satz:

VI. Ein Ideal $\mathfrak{a}$ ist dann (und nur dann) durch ein Ideal $\mathfrak{b}$ teilbar, wenn jede in $\mathfrak{b}$ aufgehende Primideal-Potenz auch in $\mathfrak{a}$ aufgeht.

Denn wenn $\mathfrak{a}$ ein Vielfaches aller in $\mathfrak{b}$ aufgehenden Primideal-Potenzen ist, so ist $\mathfrak{a}$ auch teilbar durch deren kleinstes gemeinsames Vielfaches $\mathfrak{b}$, w. z. b. w.

Hieraus folgt zugleich, daß jeder Faktor $\mathfrak{b}$ des in (2) dargestellten Ideals $\mathfrak{a}$ gewiß in der Form

$$\mathfrak{b} = \mathfrak{p}_1^{r_1} \mathfrak{p}_2^{r_2} \mathfrak{p}_3^{r_3} \ldots \tag{3}$$

darstellbar ist, wo z. B. r_1 eine der Zahlen 0, 1, 2, ..., e_1 bedeutet; und da je zwei solche Ideale $\mathfrak{b}$ von der Form (3), die verschiedenen Systemen von Exponenten $r_1, r_2, r_3 \ldots$ entsprechen, auch verschieden sind (nach V), so ist das Produkt

$$(e_1 + 1)\,(e_2 + 1)\,(e_3 + 1) \ldots \tag{4}$$

die Anzahl aller verschiedenen Faktoren $\mathfrak{b}$ des Ideals $\mathfrak{a}$. Zugleich leuchtet ein, daß die Regeln zur Bestimmung des größten gemeinsamen Teilers und des kleinsten gemeinsamen Vielfachen von beliebig vielen in der Form (2) dargestellten Idealen vollständig übereinstimmen mit denen der rationalen Zahlentheorie (§ 10).

VII. Die kleinste durch das Primideal $\mathfrak{p}$ teilbare natürliche Zahl $p = (\mathfrak{z}, \mathfrak{p})$ ist eine natürliche Primzahl, und zwar ist p die einzige durch $\mathfrak{p}$ teilbare natürliche Primzahl.

Denn jedenfalls ist $p > 1$, weil sonst $\mathfrak{p} = \mathfrak{o}$ wäre, und wenn p ein Produkt aus zwei kleineren natürlichen Zahlen r, s wäre, so müßte das in dem Produkte $\mathfrak{o}r \,.\, \mathfrak{o}s$ aufgehende Primideal $\mathfrak{p}$ (zufolge II) auch in einem der Faktoren, also auch in einer der Zahlen r, s aufgehen, was der Definition von p widersprechen würde; mithin ist p eine Primzahl, und da $[p]$ der Inbegriff aller durch $\mathfrak{p}$ teilbaren rationalen Zahlen ist (§ 177, X), so kann keine andere natürliche Primzahl durch $\mathfrak{p}$ teilbar sein, w. z. b. w.

§ 180.

Nachdem in den §§ 177 bis 179 die Theorie der Teilbarkeit der Ideale und also auch der Zahlen in $\mathfrak{o}$ vollständig erledigt ist (vgl. §§ 1 bis 10), wenden wir uns zur Betrachtung der auf Ideale bezüglichen Zahlklassen und Kongruenzen von Zahlen in $\mathfrak{o}$. Ist μ von Null verschieden, so ist $\mathfrak{o}\mu$ ein Hauptideal, und wir haben schon (in § 176, II) bewiesen, daß

$$(1) \qquad (\mathfrak{o}, \mathfrak{o}\mu) = \pm N(\mu),$$

also von Null verschieden ist. Wählt man nun aus irgendeinem Ideal $\mathfrak{m}$ eine solche Zahl μ, so folgt aus $\mathfrak{o} < \mathfrak{m} < \mathfrak{o}\mu$ [nach § 171, (5)], daß $(\mathfrak{o}, \mathfrak{m})(\mathfrak{m}, \mathfrak{o}\mu) = (\mathfrak{o}, \mathfrak{o}\mu)$, mithin auch $(\mathfrak{o}, \mathfrak{m})$ von Null verschieden ist; wir wollen in Rücksicht auf (1) diese Klassenanzahl

$$(2) \qquad (\mathfrak{o}, \mathfrak{m}) = N(\mathfrak{m})$$

setzen und die Norm des Ideals $\mathfrak{m}$ nennen; offenbar ist $\mathfrak{o}$ das einzige Ideal, dessen Norm $= 1$ ist. Dann geht die Gleichung (1) in

$$(3) \qquad N(\mathfrak{o}\mu) = \pm N(\mu)$$

über, und für beliebige Ideale $\mathfrak{a}$, $\mathfrak{b}$ gelten die Sätze

$$(4) \qquad (\mathfrak{a}, \mathfrak{a}\mathfrak{b}) = N(\mathfrak{b})$$

$$(5) \qquad N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b}).$$

Denn wählt man (nach § 178, X) eine von Null verschiedene Zahl α so, daß $\mathfrak{a}\mathfrak{b} + \mathfrak{o}\alpha = \mathfrak{a}$, $\mathfrak{a}\mathfrak{b} - \mathfrak{o}\alpha = \mathfrak{b}\alpha$ wird, so folgt (4) aus den in § 171 bewiesenen Sätzen (3), (2), (4), weil $(\mathfrak{o}\alpha, \mathfrak{a}\mathfrak{b}) = (\mathfrak{a}, \mathfrak{a}\mathfrak{b}) = (\mathfrak{o}\alpha, \mathfrak{b}\alpha) = (\mathfrak{o}, \mathfrak{b})$ wird, und hieraus folgt (5), weil $\mathfrak{o} < \mathfrak{a} < \mathfrak{a}\mathfrak{b}$,

also $(\mathfrak{o}, \mathfrak{a}\mathfrak{b}) = (\mathfrak{o}, \mathfrak{a})(\mathfrak{a}, \mathfrak{a}\mathfrak{b}) = (\mathfrak{o}, \mathfrak{a})(\mathfrak{o}, \mathfrak{b})$ ist, was zu beweisen war. Setzt man ferner (wie in § 178, II):

$$(6) \qquad \frac{\mathfrak{b}}{\mathfrak{a}+\mathfrak{b}} = \frac{\mathfrak{a}-\mathfrak{b}}{\mathfrak{a}} = \mathfrak{b}',$$

so wird, wenn $\mathfrak{c}$ ein beliebiges Ideal bedeutet,

$$(7) \qquad (\mathfrak{a}\mathfrak{c}, \mathfrak{b}\mathfrak{c}) = (\mathfrak{a}, \mathfrak{b}) = N(\mathfrak{b}'),$$

weil $(\mathfrak{a}\mathfrak{c}, \mathfrak{b}\mathfrak{c}) = (\mathfrak{a}\mathfrak{c}+\mathfrak{b}\mathfrak{c}, \mathfrak{b}\mathfrak{c})$ und $\mathfrak{b}\mathfrak{c} = (\mathfrak{a}\mathfrak{c}+\mathfrak{b}\mathfrak{c})\mathfrak{b}'$ ist*).

Nach dem Satze I in § 171 ist $\mathfrak{o}(\mathfrak{o}, \mathfrak{m}) > \mathfrak{m}$, d. h. die Norm $N(\mathfrak{m})$ des Ideals $\mathfrak{m}$ ist teilbar durch $\mathfrak{m}$, und folglich kann man das Hauptideal

$$(8) \qquad \mathfrak{o}N(\mathfrak{m}) = \mathfrak{m}\mathfrak{n}$$

setzen, wo $\mathfrak{n}$ ein Ideal bedeutet; hierin liegt eine Verallgemeinerung des Satzes IV in § 176, und man kann das Ideal

$$(9) \qquad \mathfrak{n} = N(\mathfrak{m})\mathfrak{m}^{-1}$$

das Supplement von $\mathfrak{m}$ nennen; da die Norm der rationalen Zahl $N(\mathfrak{m})$ gleich $N(\mathfrak{m})^n$ ist, so folgt aus (8), (5) und (3), daß

$$(10) \qquad N(\mathfrak{n}) = N(\mathfrak{m})^{n-1},$$

mithin $\mathfrak{m}N(\mathfrak{m})^{n-2}$ das Supplement von $\mathfrak{n}$ ist.

Die kleinste durch $\mathfrak{m}$ teilbare natürliche Zahl $m = (\mathfrak{z}, \mathfrak{m})$ geht jedenfalls in $N(\mathfrak{m})$ auf, weil $[m]$ der Inbegriff aller in $\mathfrak{m}$ enthaltenen rationalen Zahlen ist (§ 177, X); da andererseits das Ideal $\mathfrak{o}m$ durch $\mathfrak{m}$ teilbar, also von der Form $\mathfrak{m}\mathfrak{q}$ ist, so folgt aus (5) und (3), daß $N(\mathfrak{m})$ in $N(\mathfrak{o}m)$, d. h. in m^n aufgeht, und hieraus ergibt sich (nach § 178, XIV) der Satz:

I. Ist $\mathfrak{m}$ relatives Primideal zu der natürlichen Zahl k, so ist $N(\mathfrak{m})$ auch relative Primzahl zu k.

---

*) Die vorstehenden Sätze gelten auch für die in der Anmerkung zu § 178, S. 126 besprochenen Idealbrüche $\mathfrak{i}$, wenn deren Norm durch

$$N(\mathfrak{i}) = \frac{(\mathfrak{o}, \mathfrak{i})}{(\mathfrak{i}, \mathfrak{o})}$$

erklärt wird. Wählt man die ganze Zahl α so, daß $\mathfrak{i}\alpha$ ein Ideal wird, so ergibt sich leicht aus $(\mathfrak{o}, \mathfrak{i}) = (\mathfrak{o}\alpha, \mathfrak{i}\alpha) = (\mathfrak{o}\alpha+\mathfrak{i}\alpha, \mathfrak{i}\alpha)$ und $(\mathfrak{i}, \mathfrak{o}) = (\mathfrak{i}\alpha, \mathfrak{o}\alpha) = (\mathfrak{o}\alpha+\mathfrak{i}\alpha, \mathfrak{o}\alpha)$, daß $N(\mathfrak{i})N(\mathfrak{o}\alpha) = N(\mathfrak{i}\alpha)$, und folglich allgemein

$$N(\mathfrak{i}) = \frac{N(\mathfrak{b})}{N(\mathfrak{a})} = \frac{(\mathfrak{a}, \mathfrak{b})}{(\mathfrak{b}, \mathfrak{a})}$$

ist, wo $\mathfrak{a}$, $\mathfrak{b}$ irgend zwei Ideale bedeuten, welche der Bedingung $\mathfrak{a}\mathfrak{i} = \mathfrak{b}$, d. h. $\mathfrak{b}:\mathfrak{a} = \mathfrak{i}$ genügen.

Da ferner die kleinste, durch ein Primideal $\mathfrak{p}$ teilbare natürliche Zahl

$$p = (\mathfrak{z}, \mathfrak{p}) \tag{11}$$

immer eine natürliche Primzahl ist (§ 179, VII), so ist $N(\mathfrak{p})$ als Divisor von p^n selbst eine Potenz von p; wir setzen

$$N(\mathfrak{p}) = p^f \tag{12}$$

und nennen den Exponenten f, der stets > 0 und $\leqq n$ ist, den Grad des Primideals $\mathfrak{p}$.

Allgemeiner verstehen wir unter dem Grade eines beliebigen Ideals $\mathfrak{m}$ die Anzahl der (gleichen oder verschiedenen) natürlichen Primzahlen, deren Produkt $= N(\mathfrak{m})$ ist; dann ist zufolge (5) der Grad eines Produktes gleich der Summe der Grade der Faktoren, und $\mathfrak{o}$ ist das einzige Ideal vom Grade Null.

Indem wir nun zu der Betrachtung der Kongruenz der Zahlen (in $\mathfrak{o}$) in bezug auf ein beliebiges Ideal $\mathfrak{m}$ übergehen, bemerken wir zunächst, daß zwei solche Kongruenzen

$$\alpha \equiv \alpha', \quad \beta \equiv \beta' \pmod{\mathfrak{m}} \tag{13}$$

nicht nur (wie in § 171) addiert und subtrahiert, sondern auch multipliziert (mithin auch potenziert) werden dürfen; denn weil $\mathfrak{o}\,\mathfrak{m} > \mathfrak{m}$ ist, so ist jedes der Produkte $(\alpha - \alpha')\beta$, $\alpha'(\beta - \beta')$, mithin auch deren Summe $\alpha\beta - \alpha'\beta'$ durch $\mathfrak{m}$ teilbar, also

$$\alpha\beta \equiv \alpha'\beta' \pmod{\mathfrak{m}}. \tag{14}$$

Setzt man ferner

$$\mathfrak{a} = \mathfrak{m} + \mathfrak{o}\alpha, \quad \mathfrak{m} = \mathfrak{a}\mathfrak{b}, \quad \mathfrak{o}\alpha = \mathfrak{a}\mathfrak{a}', \tag{15}$$

so sind $\mathfrak{b}$ und $\mathfrak{a}'$ (nach § 178) relative Primideale, und aus einer Kongruenz von der Form

$$\alpha\omega \equiv \alpha\omega' \pmod{\mathfrak{m}} \tag{16}$$

folgt stets die Kongruenz

$$\omega \equiv \omega' \pmod{\mathfrak{b}}; \tag{17}$$

denn weil $\alpha(\omega - \omega')$ in $\mathfrak{m}$ enthalten, also $\mathfrak{a}\mathfrak{a}'(\omega - \omega') > \mathfrak{a}\mathfrak{b}$ ist, so folgt $\mathfrak{a}'(\omega - \omega') > \mathfrak{b}$, also auch $\mathfrak{o}(\omega - \omega') > \mathfrak{b}$, was zu zeigen war. Daß umgekehrt aus (17) auch (16) folgt, leuchtet unmittelbar ein.

Ist α relative Primzahl zu $\mathfrak{m}$, also $\mathfrak{a} = \mathfrak{o}$, so ist $\mathfrak{b} = \mathfrak{m}$, mithin darf in diesem Falle die Kongruenz (16) ohne weiteres durch α dividiert werden. Dasselbe ergibt sich auch unmittelbar aus $\mathfrak{o} = \mathfrak{m} + \mathfrak{o}\alpha$;

denn da die in $\mathfrak{o}$ enthaltene Zahl $1 = \mu + \alpha\xi$ ist, wo μ in $\mathfrak{m}$ enthalten, so gibt es in diesem Falle eine Zahl ξ, welche der Kongruenz

$$\alpha\xi \equiv 1 \pmod{\mathfrak{m}} \tag{18}$$

genügt (und umgekehrt folgt hieraus offenbar, daß $\mathfrak{m} + \mathfrak{o}\alpha = \mathfrak{o}$, also α relative Primzahl zu $\mathfrak{m}$ ist); multipliziert man nun (16) mit ξ, so folgt $\omega \equiv \omega' \pmod{\mathfrak{m}}$, was zu zeigen war.

Die Anzahl aller in $\mathfrak{o}$ enthaltenen, auf das Ideal $\mathfrak{m}$ bezüglichen Zahlklassen $\mathfrak{m} + \alpha$ ist $= (\mathfrak{o}, \mathfrak{m}) = N(\mathfrak{m})$. Man sieht leicht ein, daß zwei beliebige, nach $\mathfrak{m}$ kongruente Zahlen α, α' mit $\mathfrak{m}$ einen und denselben größten gemeinsamen Teiler haben, daß also aus $\mathfrak{m} + \alpha = \mathfrak{m} + \alpha'$ auch $\mathfrak{m} + \mathfrak{o}\alpha = \mathfrak{m} + \mathfrak{o}\alpha'$ folgt; da nämlich $\alpha - \alpha'$ durch $\mathfrak{m}$ teilbar ist, so muß jeder Faktor von $\mathfrak{m}$, der in der einen Zahl α' aufgeht, auch in der anderen aufgehen, weil $\alpha = (\alpha - \alpha') + \alpha'$ ist. Jede bestimmte Zahlklasse $\mathfrak{m} + \alpha$ erzeugt daher ein bestimmtes, von der Wahl ihres Repräsentanten α gänzlich unabhängiges, in $\mathfrak{m}$ aufgehendes Ideal $\mathfrak{m} + \mathfrak{o}\alpha$, und wir stellen uns, wenn $\mathfrak{a}$ ein gegebener Faktor von $\mathfrak{m} = \mathfrak{a}\mathfrak{b}$ ist, die Aufgabe, die Anzahl aller Klassen $\mathfrak{m} + \alpha$ zu bestimmen, welche diesen Faktor $\mathfrak{a}$ erzeugen, also der Bedingung $\mathfrak{m} + \mathfrak{o}\alpha = \mathfrak{a}$ genügen. Im Falle $\mathfrak{a} = \mathfrak{m}$, $\mathfrak{b} = \mathfrak{o}$ ist diese Anzahl offenbar $= 1$; ist aber $\mathfrak{a}$ ein echter Faktor von $\mathfrak{m}$, also $\mathfrak{b}$ von $\mathfrak{o}$ verschieden, so wird unsere Frage sofort durch den Satz IV in § 171 beantwortet, wenn man dort $n = \mathfrak{a}\mathfrak{p}$ und für $\mathfrak{p}$ alle in $\mathfrak{b}$ aufgehenden Primideale setzt. Wir ziehen es aber vor, uns auf die folgenden Betrachtungen zu stützen, die ohnehin aus anderen Gründen unentbehrlich sind.

Zunächst läßt sich die Aufgabe auf den besonders wichtigen speziellen Fall $\mathfrak{a} = \mathfrak{o}$, $\mathfrak{b} = \mathfrak{m}$ zurückführen; es handelt sich dann um diejenigen Klassen $\mathfrak{m} + \alpha$, deren Zahlen relative Primzahlen zu $\mathfrak{m}$ sind, und deren Anzahl wir immer mit $\varphi(\mathfrak{m})$ bezeichnen wollen; offenbar hat diese Funktion genau dieselbe Bedeutung für unser Gebiet $\mathfrak{o}$, wie die in § 11 betrachtete Funktion φ für das Gebiet $\mathfrak{z}$ der ganzen rationalen Zahlen, und sie geht im Falle $n = 1$ in die letztere über*). Bedeutet nun $\mathfrak{a}$ wieder einen beliebigen Faktor von $\mathfrak{m} = \mathfrak{a}\mathfrak{b}$, so ist (in § 178, X) schon die Existenz einer Zahl α bewiesen, welche

*) Hieraus kann keine Zweideutigkeit entspringen, weil durch das Ideal $\mathfrak{m}$ auch der Körper Ω, also die Bedeutung von $\varphi(\mathfrak{m})$ vollständig bestimmt ist; aus diesem Grunde ersetze ich das in der dritten Auflage (§ 174) gewählte Zeichen ψ jetzt durch φ.

der Bedingung $\mathfrak{m} + \mathfrak{o}\alpha = \mathfrak{a}$ genügt, und es kommt nur darauf an, aus α alle Zahlen α' zu finden, welche die Bedingung $\mathfrak{m} + \mathfrak{o}\alpha' = \mathfrak{m} + \mathfrak{o}\alpha$ erfüllen. Da nun eine Modulgleichung von der Form $\mathfrak{m} + \mathfrak{p} = \mathfrak{m} + \mathfrak{q}$ nur den Inhalt hat, daß jede Zahl in $\mathfrak{p}$ mit einer Zahl in $\mathfrak{q}$ kongruent ist (mod. $\mathfrak{m}$) und umgekehrt, so wird eine Zahl α' dann und nur dann unsere Forderung erfüllen, wenn es zwei Zahlen ω, ω' gibt, welche den Kongruenzen $\alpha' \equiv \alpha\omega$, $\alpha \equiv \alpha'\omega'$ (mod $\mathfrak{m}$) genügen. Hieraus folgt $\alpha\omega\omega' \equiv \alpha$ (mod $\mathfrak{m}$), also nach (16) und (17) auch $\omega\omega' \equiv 1$ (mod $\mathfrak{b}$), mithin ist ω zufolge (18) relative Primzahl zu $\mathfrak{b}$; umgekehrt, wenn letzteres der Fall ist, und $\alpha' \equiv \alpha\omega$ (mod $\mathfrak{m}$) gesetzt wird, so kann man nach (18) eine Zahl ω' so wählen, daß $\omega\omega' \equiv 1$ (mod $\mathfrak{b}$) wird, woraus durch Multiplikation mit α auch $\alpha \equiv \alpha'\omega'$ (mod $\mathfrak{m}$) folgt. Man erhält daher alle von uns gesuchten Zahlen α' und nur solche, wenn man $\alpha' \equiv \alpha\omega$ (mod $\mathfrak{m}$) setzt, und ω alle relativen Primzahlen zu $\mathfrak{b}$ durchlaufen läßt. Da nun zufolge (16) und (17) die durch zwei solche Zahlen ω erzeugten Produkte $\omega\alpha$ dann und nur dann nach $\mathfrak{m}$ kongruent sind, wenn diese Zahlen ω nach $\mathfrak{b}$ kongruent sind, so ergibt sich, daß die Anzahl der Klassen $\mathfrak{m} + \alpha'$, welche der Bedingung $\mathfrak{m} + \mathfrak{o}\alpha' = \mathfrak{a}$ genügen, $= \varphi(\mathfrak{b})$ ist, wo $\mathfrak{a}\mathfrak{b} = \mathfrak{m}$ (vgl. § 13).

Da die Anzahl aller auf $\mathfrak{m}$ bezüglichen Zahlklassen $= N(\mathfrak{m})$ ist, so folgt hieraus offenbar (wie in § 13) der Satz

$$\sum \varphi(\mathfrak{b}) = N(\mathfrak{m}), \tag{19}$$

wo $\mathfrak{b}$ alle verschiedenen Faktoren von $\mathfrak{m}$ durchläuft. Überträgt man die in § 138 enthaltenen Betrachtungen auf unser Gebiet, was keine Schwierigkeit hat, so überzeugt man sich, daß die Funktion φ durch diesen Satz vollständig bestimmt ist, und ihr allgemeiner Ausdruck leicht gewonnen werden kann. Wir überlassen dies dem Leser und schlagen einen anderen Weg ein, welcher auf der Verallgemeinerung der in § 25 behandelten Aufgabe, nämlich auf dem folgenden, häufig anzuwendenden Satze beruht.

II. Ist $\mathfrak{m}$ das Produkt aus den relativen Primidealen $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$..., und sind ϱ, σ, τ... ebenso viele gegebene Zahlen, so gibt es immer Zahlen ω, welche den gleichzeitigen Kongruenzen

$$\omega \equiv \varrho \text{ (mod. } \mathfrak{a}\text{)}, \quad \omega \equiv \sigma \text{ (mod. } \mathfrak{b}\text{)}, \quad \omega \equiv \tau \text{ (mod. } \mathfrak{c}\text{)} \ldots \tag{20}$$

genügen, und alle diese Zahlen ω bilden eine bestimmte Zahlklasse in bezug auf $\mathfrak{m}$.

Handelt es sich nur um zwei relative Primideale $\mathfrak{a}$, $\mathfrak{b}$, so folgt dies unmittelbar aus dem Satze III in § 171, weil $\mathfrak{a} + \mathfrak{b} = \mathfrak{o}$, $\mathfrak{a} - \mathfrak{b} = \mathfrak{a}\mathfrak{b}$ ist, und hieraus ergibt sich durch Wiederholung derselben Schlüsse, weil $\mathfrak{a}\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{d}$ ... relative Primideale sind, leicht unser allgemeiner Satz. Derselbe läßt sich aber auch unmittelbar auf folgende Art beweisen. Setzt man (wie in § 178, I und VIII) $\mathfrak{m} = \mathfrak{a}\mathfrak{a}_1 = \mathfrak{b}\mathfrak{b}_1 = \mathfrak{c}\mathfrak{c}_1 \ldots$, so ist $\mathfrak{a}_1 + \mathfrak{b}_1 + \mathfrak{c}_1 + \cdots = \mathfrak{o}$, und folglich gibt es in den Idealen $\mathfrak{a}_1$, $\mathfrak{b}_1$, $\mathfrak{c}_1 \ldots$ bzw. Zahlen α_1, β_1, $\gamma_1 \ldots$, welche der Bedingung

$$\alpha_1 + \beta_1 + \gamma_1 + \cdots = 1 \tag{21}$$

genügen. Erfüllt nun eine Zahl ω die Kongruenzen (20), so folgen daraus durch Multiplikation mit α_1, β_1, γ_1 ... die auf $\mathfrak{m}$ bezüglichen Kongruenzen $\omega\alpha_1 \equiv \varrho\alpha_1$, $\omega\beta_1 \equiv \sigma\beta_1$, $\omega\gamma_1 \equiv \tau\gamma_1 \ldots$ und durch deren Addition zufolge (21) die Kongruenz

$$\omega \equiv \varrho\alpha_1 + \sigma\beta_1 + \tau\gamma_1 + \cdots \pmod{\mathfrak{m}}; \tag{22}$$

umgekehrt genügt jede in dieser Form (22) darstellbare Zahl ω allen Kongruenzen (20), z. B. der ersten von ihnen, weil die Zahlen β_1, $\gamma_1 \ldots$ alle durch $\mathfrak{a}$ teilbar, also zufolge (21) die Zahl $\alpha_1 \equiv 1 \pmod{\mathfrak{a}}$ ist, w. z. b. w.

Jeder Kombination von Klassen $\mathfrak{a} + \varrho$, $\mathfrak{b} + \sigma$, $\mathfrak{c} + \tau \ldots$ entspricht daher immer eine bestimmte Klasse $\mathfrak{m} + \omega$ als Inbegriff aller derjenigen Zahlen, welche jenen Klassen gemeinsam sind; umgekehrt leuchtet ein, daß jede Klasse $\mathfrak{m} + \omega$ immer aus einer und nur einer solchen Kombination entspringt. Da ferner zufolge (20) die Zahl ω dann und nur dann relative Primzahl zu $\mathfrak{m}$ wird, wenn die Zahlen ϱ, σ, $\tau \ldots$ bzw. relative Primzahlen zu $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c} \ldots$ sind, so ergibt sich der folgende Satz (vgl. § 12):

III. Sind $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c} \ldots$ relative Primideale, so ist

$$\varphi(\mathfrak{a}\mathfrak{b}\mathfrak{c} \ldots) = \varphi(\mathfrak{a})\varphi(\mathfrak{b})\varphi(\mathfrak{c}) \ldots \tag{23}$$

Da nun jedes von $\mathfrak{o}$ verschiedene Ideal entweder eine Potenz eines Primideals oder ein Produkt aus mehreren solchen Potenzen $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c} \ldots$ ist, die zugleich relative Primideale sind, während offenbar

$$\varphi(\mathfrak{o}) = 1 \tag{24}$$

ist, so kommt es nur noch darauf an, die Funktion $\varphi(\mathfrak{a})$ für den Fall zu bestimmen, daß $\mathfrak{a}$ durch ein und nur ein Primideal $\mathfrak{p}$ teilbar ist; da aber eine Zahl ϱ dann und nur dann relative Primzahl zu $\mathfrak{a}$ ist, wenn sie nicht durch $\mathfrak{p}$ teilbar ist, so hat man, um die Anzahl $\varphi(\mathfrak{a})$ aller dieser Klassen $\mathfrak{a} + \varrho$ zu erhalten, von der Anzahl $(\mathfrak{o}, \mathfrak{a})$ aller

Klassen die Anzahl $(\mathfrak{p}, \mathfrak{a})$ derjenigen Klassen abzuziehen, deren Zahlen durch $\mathfrak{p}$ teilbar sind, und da $(\mathfrak{o}, \mathfrak{p})(\mathfrak{p}, \mathfrak{a}) = (\mathfrak{o}, \mathfrak{a}) = N(\mathfrak{a})$ ist, so ergibt sich

$$\varphi(\mathfrak{a}) = N(\mathfrak{a})\left(1 - \frac{1}{N(\mathfrak{p})}\right) \tag{25}$$

und hieraus der allgemeine Satz

$$\varphi(\mathfrak{m}) = N(\mathfrak{m})\,\Pi\left(1 - \frac{1}{N(\mathfrak{p})}\right), \tag{26}$$

wo das Produktzeichen sich auf alle verschiedenen, in $\mathfrak{m}$ aufgehenden Primideale $\mathfrak{p}$ bezieht. Man erkennt leicht, wie hieraus rückwärts sich die Sätze (23) und (19) ableiten lassen (vgl. §§ 12, 14). Unsere Aufgabe ist hiermit gelöst. —

Bedeutet nun ϱ irgendeine bestimmte relative Primzahl zu $\mathfrak{m}$, während ϱ' ein System von $\varphi(\mathfrak{m})$ nach $\mathfrak{m}$ inkongruenten Zahlen durchläuft, die relative Primzahlen zu $\mathfrak{m}$ sind, so sind die Produkte $\varrho\,\varrho'$ inkongruent und ebenfalls relative Primzahlen zu $\mathfrak{m}$; jede dieser Zahlen $\varrho\,\varrho'$ ist daher mit einer der Zahlen ϱ', und jede der letzteren mit einer der ersteren kongruent; mithin ist auch das Produkt σ der Zahlen ϱ' kongruent dem Produkte $\sigma\,\varrho^{\varphi(\mathfrak{m})}$ der Zahlen $\varrho\,\varrho'$, und da σ ebenfalls relative Primzahl zu $\mathfrak{m}$ ist, so erhält man den Satz:

IV. Ist $\mathfrak{m}$ ein Ideal, und ϱ relative Primzahl zu $\mathfrak{m}$, so ist

$$\varrho^{\varphi(\mathfrak{m})} \equiv 1 \pmod{\mathfrak{m}}. \tag{27}$$

Derselbe entspricht offenbar dem verallgemeinerten Fermatschen Satze der rationalen Zahlentheorie (§ 19), und aus ihm folgt unmittelbar der Satz:

V. Ist $\mathfrak{p}$ ein Primideal, so genügt jede Zahl ω der Kongruenz

$$\omega^{N(\mathfrak{p})} \equiv \omega \pmod{\mathfrak{p}}. \tag{28}$$

Von der unerschöpflichen Reihe von Untersuchungen, welche von diesem Fundamentalsatze ausgehen, dürfen wir des Raumes wegen nur einige Andeutungen geben, die der Leser ohne Schwierigkeit ausführen kann*). Zunächst wird man alle in den §§ 26 bis 31

*) Vgl. meine von der Gesellschaft der Wissenschaften zu Göttingen herausgegebenen Abhandlungen Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen (Bd. 23, 1878) und Über die Diskriminanten endlicher Körper (Bd. 29, 1882), ferner die Abhandlung von Stickelberger: Über eine Verallgemeinerung der Kreisteilung (Math. Annalen, Bd. 37).

enthaltenen Sätze über Kongruenzen, Potenzreste, primitive Wurzeln auf solche Kongruenzen übertragen, deren Koeffizienten irgendwelche Zahlen unseres Gebietes o, und deren Modul ein Primideal $\mathfrak{p}$ ist. Behalten p und f die in (11) und (12) angegebene Bedeutung, so ergibt sich hieraus in Verbindung mit (28) die in bezug auf die Variable t identische Kongruenz

$$t^{p^f} - t \equiv \Pi(t - \omega) \pmod{\mathfrak{p}}, \tag{29}$$

wo das Produktzeichen Π sich auf alle inkongruenten Zahlen ω bezieht. Hierzu kommt eine Betrachtung, welche in der Theorie der rationalen Zahlen noch nicht auftreten konnte. Versteht man unter der Höhe einer Zahl α (in bezug auf $\mathfrak{p}$) die kleinste natürliche Zahl a, welche der Bedingung

$$\alpha^{p^a} \equiv \alpha \pmod{\mathfrak{p}} \tag{30}$$

genügt, so sind die a Zahlen

$$\alpha,\ \alpha^p,\ \alpha^{p^2},\ \ldots,\ \alpha^{p^{a-1}} \tag{31}$$

inkongruent, und die beiden Kongruenzen

$$\alpha^{p^r} \equiv \alpha^{p^s} \pmod{\mathfrak{p}} \quad \text{und} \quad r \equiv s \pmod{a} \tag{32}$$

sind gleichbedeutend, woraus zugleich folgt, daß die Höhe a ein Divisor des Grades f ist. Das System aller Zahlen, deren Höhe $= 1$ ist, fällt zusammen mit dem Modul $\mathfrak{p} + \mathfrak{z}$, d. h. mit dem System aller derjenigen Zahlen, welche einer rationalen Zahl kongruent sind. Zu den Zahlen von der Höhe f gehören z. B. alle primitiven Wurzeln von $\mathfrak{p}$.

Die a Zahlen (31) oder irgendwelche ihnen kongruente Zahlen bilden die Periode der Zahl α; jede von ihnen hat dieselbe Höhe und erzeugt dieselbe Periode. Nun gilt zufolge der in § 20 erwähnten Eigenschaft der Binomialkoeffizienten für je zwei ganze Zahlen μ, ν die Kongruenz

$$(\mu \pm \nu)^p \equiv \mu^p \pm \nu^p \pmod{p}; \tag{33}$$

hieraus folgt, daß jede durch Addition und Multiplikation gebildete symmetrische Funktion der Zahlen (31) die Höhe 1 besitzt, und daß folglich eine identische Kongruenz von der Form

$$(t - \alpha)\,(t - \alpha^p) \ldots (t - \alpha^{p^{a-1}}) \equiv P(t) \pmod{\mathfrak{p}} \tag{34}$$

besteht, wo $P(t)$ eine ganze Funktion von t mit ganzen rationalen Koeffizienten bedeutet. In der Theorie dieser auf den Modul p be-

zogenen Funktionen ist $P(t)$ eine sogenannte Primfunktion*), weil aus einer Kongruenz von der Form

$$P(\alpha) \equiv 0 \pmod{\mathfrak{p}} \tag{35}$$

durch Potenzieren auch $P(\alpha') \equiv 0 \pmod{\mathfrak{p}}$ folgt, wo α' jede Zahl der Periode (31) bedeutet. Verbindet man nun in (29) immer diejenigen Faktoren $t - \omega$, welche den zu einer Periode gehörenden Zahlen ω entsprechen, zu einer Funktion $P(t)$ und bedenkt, daß jede auf $\mathfrak{p}$ bezügliche Kongruenz zwischen rationalen Zahlen auch in bezug auf den Modul p gilt, so erhält man eine von der Beschaffenheit des Körpers Ω gänzlich unabhängige identische Kongruenz von der Form

$$t^{p^f} - t \equiv \Pi P(t) \pmod{p}; \tag{36}$$

die rechte Seite ist ein Produkt von lauter solchen Primfunktionen, deren Grade Divisoren von f sind, und in der Theorie dieser identischen Funktionen-Kongruenzen wird gezeigt**), daß in diesem Produkte auch jede solche Primfunktion einmal auftreten muß.

Bildet man aus einer Zahl α von der Höhe a und aus ganzen rationalen Koeffizienten x alle Zahlen ν von der Form

$$\nu \equiv x_1 \alpha^{a-1} + x_2 \alpha^{a-2} + \cdots + x_a \pmod{\mathfrak{p}}, \tag{37}$$

so überzeugt man sich leicht, daß dieselben mit allen Wurzeln der Kongruenz

$$\nu^{p^a} \equiv \nu \pmod{\mathfrak{p}}, \tag{38}$$

also mit allen denjenigen Zahlen zusammenfallen, deren Höhe ein Divisor von a ist. Der Inbegriff $\mathfrak{n}$ aller dieser Zahlen ν, welcher nach § 173 auch durch $\mathfrak{p} + (\alpha)_a$ bezeichnet werden kann, ist eine Ordnung (§ 170), und außer diesen, den sämtlichen Divisoren a von f entsprechenden Ordnungen gibt es in $\mathfrak{o}$ keine andere in $\mathfrak{p}$ aufgehende Ordnung. Der Führer der Ordnung $\mathfrak{n}$, worunter immer der Quotient $\mathfrak{n} : \mathfrak{o}$ zu verstehen ist***), ist $= \mathfrak{p}$ oder $= \mathfrak{o}$, je nachdem $a < f$ oder $a = f$ ist, weil im letzteren Falle offenbar $\mathfrak{n} = \mathfrak{o}$ ist. Daß es, wenn a irgendein Divisor von f ist, immer auch Zahlen α von der Höhe a gibt, folgt leicht aus den früheren Sätzen, und durch Anwendung

*) Vgl. meine auf S. 61 [von Dirichlets Vorlesungen über Zahlentheorie] zitierte Abhandlung art. 6 [V dieser Ausgabe].

**) A. a. O. art. 19.

***) Vgl. § 7 meiner Abhandlung Über die Diskriminanten endlicher Körper (Göttingen 1882).

der in § 138 enthaltenen Methode findet man auch den allgemeinen Ausdruck für die Anzahl aller inkongruenten solchen Zahlen.

Wir bemerken endlich, daß die obenerwähnte Theorie der identischen Kongruenzen, in welcher Funktionen einer Variablen mit rationalen Koeffizienten auf eine natürliche Primzahl p als Modulus bezogen werden, sich ebenfalls auf Funktionen übertragen läßt, deren Koeffizienten beliebige Zahlen unseres Gebietes o sind, während als Modulus irgendein Primideal $\mathfrak{p}$ auftritt, und da diese Übertragung für manche tiefere Untersuchung erfordert wird, so empfehlen wir dem Leser, dieselbe durchzuführen.

§ 181.

Wir haben gesehen, daß jedes Ideal $\mathfrak{a}$ durch Multiplikation mit einem geeigneten Ideal $\mathfrak{m}$ in ein Hauptideal $\mathfrak{a}\mathfrak{m}$ verwandelt werden kann (§ 177, IX), und wollen nun zwei Ideale $\mathfrak{a}$, $\mathfrak{a}'$ äquivalent nennen, wenn beide durch Multiplikation mit einem und demselben Faktor $\mathfrak{m}$ in Hauptideale $\mathfrak{a}\mathfrak{m} = o\mu$, $\mathfrak{a}'\mathfrak{m} = o\mu'$ übergehen; dann ist $\mathfrak{a}\mu' = \mathfrak{a}'\mu$, und wenn man die (ganze oder gebrochene) Zahl $\mu'\mu^{-1} = \eta$ setzt, so wird $\mathfrak{a}' = \mathfrak{a}\eta$. Umgekehrt, wenn es eine Zahl η gibt, welche dieser Bedingung genügt, so sind die Ideale $\mathfrak{a}$, $\mathfrak{a}'$ äquivalent, weil dann aus $\mathfrak{a}\mathfrak{m} = o\mu$ auch $\mathfrak{a}'\mathfrak{m} = o\mu'$ folgt, wo $\mu' = \mu\eta$ gewiß eine ganze Zahl ist. Zugleich ergibt sich hieraus, daß jeder Faktor $\mathfrak{m}$, welcher das eine von zwei äquivalenten Idealen $\mathfrak{a}$, $\mathfrak{a}'$ in ein Hauptideal verwandelt, gleiches auch für das andere Ideal leistet, und daß folglich je zwei Ideale $\mathfrak{a}'$, $\mathfrak{a}''$, die mit einem dritten Ideal $\mathfrak{a}$ äquivalent sind, stets auch miteinander äquivalent sein müssen. Auf diesem Satze beruht die Möglichkeit, alle Ideale in Idealklassen einzuteilen; ist $\mathfrak{a}$ ein bestimmtes Ideal, so hat der Inbegriff A aller mit $\mathfrak{a}$ äquivalenten Ideale $\mathfrak{a}$, $\mathfrak{a}'$, $\mathfrak{a}''$... die Eigenschaft, daß je zwei darin enthaltene Ideale $\mathfrak{a}'$, $\mathfrak{a}''$ einander äquivalent sind, und wenn $\mathfrak{a}'$ irgendein in A enthaltenes Ideal ist, so ist A zugleich der Inbegriff aller mit $\mathfrak{a}'$ äquivalenten Ideale. Ein solches System A von Idealen nennen wir eine Idealklasse oder auch kürzer eine Klasse, da eine Verwechslung mit Zahlklassen hier nicht zu befürchten ist; jede Klasse A ist durch ein beliebiges in ihr enthaltenes Ideal $\mathfrak{a}$ vollständig bestimmt, und letzteres kann daher immer als Repräsentant der ganzen Klasse A angesehen werden.

Die durch das Ideal $\mathfrak{o}$ repräsentierte Klasse wollen wir mit O bezeichnen und die Hauptklasse nennen, weil sie offenbar aus allen Hauptidealen $\mathfrak{o}\eta$ besteht.

Sind $\mathfrak{a}$, $\mathfrak{a}'$ äquivalent, so gilt dasselbe von $\mathfrak{a}\mathfrak{b}$, $\mathfrak{a}'\mathfrak{b}$, weil aus $\mathfrak{a}' = \mathfrak{a}\eta$ auch $\mathfrak{a}'\mathfrak{b} = (\mathfrak{a}\mathfrak{b})\eta$ folgt; sind außerdem $\mathfrak{b}$, $\mathfrak{b}'$ äquivalent, so folgt ebenso, daß $\mathfrak{a}'\mathfrak{b}$, $\mathfrak{a}'\mathfrak{b}'$, also auch $\mathfrak{a}\mathfrak{b}$, $\mathfrak{a}'\mathfrak{b}'$ äquivalent sind. Durchläuft daher $\mathfrak{a}$ alle Ideale der Klasse A, und ebenso $\mathfrak{b}$ alle Ideale der Klasse B, so gehören alle Produkte $\mathfrak{a}\mathfrak{b}$ einer und derselben Klasse K an, die aber noch unendlich viele andere Ideale enthalten kann; diese Klasse K wollen wir mit AB bezeichnen, und sie soll das Produkt aus A, B oder die aus A und B zusammengesetzte Klasse heißen. Offenbar ist $AB = BA$, wo das Gleichheitszeichen die Identität der beiden Klassen bedeutet, und aus $(\mathfrak{a}\mathfrak{b})\mathfrak{c} = \mathfrak{a}(\mathfrak{b}\mathfrak{c})$ folgt für drei beliebige Klassen der Satz $(AB)C = A(BC)$. Man kann daher dieselben Schlüsse anwenden wie bei der Multiplikation von Zahlen oder Idealen, und beweisen, daß bei der Zusammensetzung von beliebig vielen Klassen $A_1, A_2, \ldots, A_m$ die Anordnung der sukzessiven Multiplikationen, durch welche jedesmal zwei Klassen zu ihrem Produkte vereinigt werden, keinen Einfluß auf das Endresultat hat, welches kurz durch $A_1 A_2 \ldots A_m$ bezeichnet werden kann (vgl. § 2). Sind die Ideale $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_m$ Repräsentanten der Klassen $A_1, A_2, \ldots, A_m$, so ist das Ideal $\mathfrak{a}_1 \mathfrak{a}_2 \ldots \mathfrak{a}_m$ ein Repräsentant des Produktes $A_1 A_2 \ldots A_m$. Sind alle m Faktoren $= A$, so heißt ihr Produkt die m^{te} Potenz von A und wird mit A^m bezeichnet; außerdem setzen wir $A^1 = A$ und $A^0 = O$. Von besonderer Wichtigkeit sind die beiden folgenden Fälle.

Aus $\mathfrak{o}\mathfrak{a} = \mathfrak{a}$ folgt der für jede Klasse A gültige Satz $OA = A$.

Da ferner jedes Ideal $\mathfrak{a}$ durch Multiplikation mit einem Ideal $\mathfrak{m}$ in ein Hauptideal $\mathfrak{a}\mathfrak{m}$ verwandelt werden kann, so gibt es für jede Klasse A eine zugehörige Klasse M, welche der Bedingung $AM = O$ genügt, und zwar nur eine einzige; denn wenn die Klasse M' ebenfalls die Bedingung $AM' = O$ erfüllt, so folgt

$$M' = OM' = (AM)M' = (AM')M = OM = M.$$

Diese Klasse M heißt die entgegengesetzte oder die inverse Klasse von A, und sie soll durch A^{-1} bezeichnet werden; offenbar ist umgekehrt A die inverse Klasse von A^{-1}. Definiert man ferner

A^{-m} als die inverse Klasse von A^m, so gelten für beliebige ganze rationale Exponenten r, s die Sätze:

$$A^r A^s = A^{r+s}, \quad (A^r)^s = A^{rs}, \quad (AB)^r = A^r B^r.$$

Endlich leuchtet ein, daß aus $AB = AC$ durch Multiplikation mit A^{-1} stets $B = C$ folgt.

Um nun tiefer in die Natur der Idealklassen einzudringen, wählen wir eine beliebige, aus n ganzen Zahlen $\omega_1, \omega_2, \ldots, \omega_n$ bestehende Basis von $\mathfrak{o}$; dann wird jede Zahl

$$\omega = h_1 \omega_1 + h_2 \omega_2 + \cdots + h_n \omega_n, \tag{1}$$

welche ganze Koordinaten $h_1, h_2 \ldots h_n$ hat, ebenfalls eine ganze Zahl des Körpers. Legt man den Koordinaten alle ganzen Werte bei, welche, absolut genommen, einen bestimmten positiven Wert k nicht überschreiten, so werden offenbar die absoluten Werte der entsprechenden Zahlen ω, wenn sie reell sind, oder ihre analytischen Moduln, wenn sie imaginär sind, sämtlich $\leqq rk$ sein, wo r die Summe der absoluten Werte oder der Moduln von $\omega_1, \omega_2, \ldots, \omega_n$ bedeutet und folglich eine von k gänzlich unabhängige Konstante ist. Da ferner die Norm $N(\omega)$ ein Produkt aus n konjugierten Zahlen ω von der obigen Form ist, so wird gleichzeitig

$$\pm N(\omega) \leqq H k^n, \tag{2}$$

wo H ebenfalls eine lediglich von der Basis abhängige Konstante bedeutet. Dann gilt der folgende Satz:

I. Aus jedem endlichen Modul $\mathfrak{a}$, dessen Basis zugleich eine Basis des Körpers Ω ist, kann man eine ganze, von Null verschiedene Zahl α so auswählen, daß

$$\pm N(\alpha) \leqq H(\mathfrak{o}, \mathfrak{a}) \tag{3}$$

wird.

Denn bestimmt man, da $(\mathfrak{o}, \mathfrak{a}) > 0$ ist (§ 175), die natürliche Zahl k durch die Bedingungen

$$k^n \leqq (\mathfrak{o}, \mathfrak{a}) < (k+1)^n \tag{4}$$

und legt jeder der n Koordinaten in (1) die sämtlichen $(k+1)$ Werte 0, 1, 2, …, k bei, so entstehen lauter verschiedene Zahlen ω, und da ihre Anzahl $= (k+1)^n$, also $> (\mathfrak{o}, \mathfrak{a})$ ist, so gibt es unter ihnen mindestens zwei verschiedene β, γ, welche nach $\mathfrak{a}$ kongruent sind; mithin wird ihre Differenz $\beta - \gamma$ eine von Null verschiedene, ganze Zahl α in $\mathfrak{a}$. Da nun die Koordinaten der Zahlen β, γ in der

Reihe 0, 1, 2, ..., k enthalten sind, so überschreiten die Koordinaten dieser Zahl α, absolut genommen, den Wert k nicht, und hieraus ergibt sich mit Rücksicht auf (2) und (4) die Gleichung (3), w. z. b. w.

Als eine unmittelbare Folgerung ergibt sich hieraus der Fundamentalsatz:

II. In jeder Idealklasse M gibt es mindestens ein Ideal $\mathfrak{m}$, dessen Norm die Konstante H nicht überschreitet*), und folglich ist die Anzahl der Idealklassen endlich.

Denn wendet man den vorigen Satz auf ein Ideal $\mathfrak{a}$ an, welches nach Belieben aus der inversen Klasse M^{-1} gewählt ist, so wird $\mathfrak{o}\alpha > \mathfrak{a}$, also $\mathfrak{o}\alpha = \mathfrak{a}\mathfrak{m}$, wo $\mathfrak{m}$ ein Ideal der Klasse M bedeutet; zugleich wird $\pm N(\alpha) = N(\mathfrak{a})N(\mathfrak{m}) = (\mathfrak{o}, \mathfrak{a})N(\mathfrak{m})$, also $N(\mathfrak{m}) \leqq H$. Bedenkt man aber, daß es nur eine endliche Anzahl von natürlichen Zahlen gibt, die den Wert H nicht überschreiten, und daß jedes Ideal $\mathfrak{m}$ [nach § 180, (8)] ein Faktor seiner Norm ist, so ergibt sich (nach § 177, VIII), daß die Anzahl der Ideale $\mathfrak{m}$, welche der Bedingung $N(\mathfrak{m}) \leqq H$ genügen, und folglich auch die Anzahl der Idealklassen M endlich ist, w. z. b. w.

Es leuchtet nun unmittelbar ein, daß alles, was wir in der Theorie der quadratischen Formen über die Zusammensetzung der ursprünglichen Klassen erster Art gesagt haben (§ 149), sich Wort für Wort auf unsere Idealklassen übertragen läßt. Wir heben hier aber nur den einen Satz hervor, daß, wenn h die Anzahl aller Klassen bedeutet, jede Idealklasse A der Bedingung

$$A^h = O$$

genügt. Ist daher $\mathfrak{a}$ ein beliebiges Ideal, so ist $\mathfrak{a}^h$ immer ein Hauptideal; setzt man nun

$$\mathfrak{a}^h = \mathfrak{o}\mu$$

und

$$\alpha_0^h = \mu, \quad \alpha_0 = \sqrt[h]{\mu},$$

*) Vgl. H. Minkowski: Théorèmes arithmétiques (Compte rendu der Pariser Akademie vom 26. Januar 1891); Über die positiven quadratischen Formen und über kettenbruchähnliche Algorithmen (Crelles Journal, Bd. 107). Aus diesen wichtigen Untersuchungen, welche in weiterer Ausführung demnächst als besonderes Werk (Geometrie der Zahlen) erscheinen werden, geht unter anderem hervor, daß (wenn $n > 1$) die Konstante H kleiner angenommen werden darf als die Quadratwurzel aus dem absoluten Werte der Grundzahl D, woraus zugleich folgt, daß D absolut > 1 ist.

so ist α_0 eine ganze algebraische Zahl (§ 173, V); gehört dieselbe dem Körper Ω, also auch dem Gebiete $\mathfrak{o}$ an, so ist $\mathfrak{a}$ offenbar ein Hauptideal, nämlich $= \mathfrak{o}\,\alpha_0$, und es wird folglich, wenn $\mathfrak{a}$ kein Hauptideal ist, die Zahl α_0 dem Körper Ω gewiß nicht angehören. Nichtsdestoweniger findet auch im letzteren Falle zwischen dem Ideal $\mathfrak{a}$ und der Zahl α_0 der Zusammenhang statt, daß $\mathfrak{a}$ der Inbegriff aller derjenigen in $\mathfrak{o}$ enthaltenen Zahlen ist, welche durch α_0 teilbar sind (§ 174). Denn wenn α in $\mathfrak{a}$ enthalten, also α^h durch $\mathfrak{a}^h$, mithin auch durch μ teilbar ist, so ist α auch teilbar durch $\sqrt[h]{\mu} = \alpha_0$; und umgekehrt, ist α eine in $\mathfrak{o}$ enthaltene und durch α_0 teilbare Zahl, so ist α^h teilbar durch $\alpha_0^h = \mu$, also auch durch $\mathfrak{a}^h$, woraus (nach § 179) leicht folgt, daß α auch durch $\mathfrak{a}$ teilbar ist. Nennt man daher eine solche Zahl α_0 eine ideale Zahl des Körpers Ω im Gegensatze zu den in Ω enthaltenen wirklichen Zahlen, so kann jedes Ideal $\mathfrak{a}$ als der Inbegriff aller in $\mathfrak{o}$ enthaltenen, durch eine wirkliche oder ideale Zahl α_0 teilbaren Zahlen angesehen werden. Hieran knüpfen wir den Beweis des folgenden, schon früher (§ 174) angekündigten Satzes:

III. Zwei beliebige ganze algebraische Zahlen α, β besitzen immer einen gemeinschaftlichen Teiler δ_0, welcher in der Form $\alpha\xi_0 + \beta\eta_0$ darstellbar ist, wo ξ_0, η_0 ebenfalls ganze algebraische Zahlen bedeuten.

Wir nehmen an, daß beide Zahlen α, β von Null verschieden sind, weil im entgegengesetzten Falle der Satz evident ist. Es gibt nun (nach § 164) immer einen endlichen Körper Ω, welcher beide Zahlen α, β enthält, und es sei $\mathfrak{o}$ wieder das System aller ganzen Zahlen dieses Körpers, ferner h die Anzahl der Idealklassen. Ist $\mathfrak{d}$ der größte gemeinschaftliche Teiler der beiden Hauptideale

$$\mathfrak{o}\alpha = \mathfrak{a}\mathfrak{d}, \quad \mathfrak{o}\beta = \mathfrak{b}\mathfrak{d},$$

so sind $\mathfrak{a}$, $\mathfrak{b}$ relative Primideale, und dasselbe gilt folglich von ihren Potenzen $\mathfrak{a}^h$, $\mathfrak{b}^h$. Setzt man nun

$$\mathfrak{b}^h = \mathfrak{o}\gamma,$$

wo γ in $\mathfrak{o}$ enthalten, so wird, weil α^h und β^h durch $\mathfrak{b}^h$ teilbar sind,

$$\alpha^h = \mu\gamma, \quad \beta^h = \nu\gamma, \quad \mathfrak{o}\mu = \mathfrak{a}^h, \quad \mathfrak{o}\nu = \mathfrak{b}^h,$$

wo μ, ν ebenfalls in $\mathfrak{o}$ enthalten, und zwar relative Primzahlen sind (§ 178, XIII); es gibt daher in $\mathfrak{o}$ zwei Zahlen ϱ, σ, welche der Bedingung

$$\mu\varrho + \nu\sigma = 1$$

genügen. Man definiere jetzt die zu $\mathfrak{b}$ gehörige ideale Zahl δ_0 und ferner die Zahlen α_0, β_0 durch

$$\delta_0 = \sqrt[h]{\gamma}, \quad \alpha = \alpha_0 \delta_0, \quad \beta = \beta_0 \delta_0,$$

so wird

$$\gamma = \delta_0^h, \quad \mu = \alpha_0^h, \quad \nu = \beta_0^h,$$

mithin sind α_0, β_0 die zu $\mathfrak{a}$, $\mathfrak{b}$ gehörigen idealen ganzen Zahlen, und δ_0 ist ein gemeinsamer Divisor der beiden gegebenen Zahlen α, β. Setzt man endlich

$$\xi_0 = \alpha_0^{h-1} \varrho, \quad \eta_0 = \beta_0^{h-1} \sigma,$$

so sind ξ_0, η_0 ganze Zahlen, welche den Bedingungen

$$\alpha_0 \xi_0 + \beta_0 \eta_0 = 1, \quad \alpha \xi_0 + \beta \eta_0 = \delta_0$$

genügen, was zu beweisen war.

Diese Zahl δ_0, aber auch jede mit ihr assoziierte Zahl, verdient den Namen des größten gemeinschaftlichen Teilers von α, β, weil jeder gemeinschaftliche Teiler dieser beiden Zahlen in δ_0 aufgehen muß. Da ferner jedes Ideal $\mathfrak{b}$ als größter gemeinschaftlicher Teiler von zwei Hauptidealen $\mathfrak{o}\alpha$, $\mathfrak{o}\beta$ darstellbar ist (§ 178, XII), so kann unter einer idealen Zahl des Körpers Ω auch jede Zahl δ_0 verstanden werden, welche der größte gemeinschaftliche Teiler von zwei wirklichen, d. h. in $\mathfrak{o}$ enthaltenen Zahlen α, β ist.

Nach dieser Abschweifung kehren wir noch einmal zu der Einteilung aller Ideale in Klassen zurück; es gibt nämlich einen Fall, für welchen es zweckmäßig sein kann, an Stelle der oben beschriebenen Einteilung eine andere zu setzen, die noch etwas tiefer eingreift. Zwei Hauptideale $\mathfrak{o}\mu$, $\mathfrak{o}\nu$ sind offenbar stets und nur dann identisch, wenn die beiden Zahlen μ, ν assoziiert, d. h. wenn $\nu = \varepsilon\mu$ ist, wo ε eine Einheit bedeutet. Ist die Norm von μ positiv, so ist sie zugleich die Norm des Hauptideals $\mathfrak{o}\mu$. Es kann aber auch der Fall eintreten, daß die Normen aller mit einer bestimmten Zahl μ assoziierten Zahlen $\varepsilon\mu$ negativ sind; dies wird immer und nur dann geschehen, wenn es in dem Körper Ω Zahlen von negativer Norm, unter diesen aber keine Einheit gibt*). In diesem Falle ist es für manche Unter-

*) Der Grad n eines solchen Körpers Ω muß, wie leicht zu sehen, eine gerade Zahl, und unter den mit Ω konjugierten Körpern müssen auch solche sein, welche aus lauter reellen Zahlen bestehen. Ein solcher Körper ist z. B. der quadratische Körper, dessen Grundzahl $= +12$, während der von der Grundzahl $+8$ diese Eigenschaft nicht besitzt.

suchungen zweckmäßig, zwei Ideale $\mathfrak{a}$, $\mathfrak{a}'$ nur dann äquivalent zu nennen, wenn es eine Zahl η von positiver Norm gibt, welche der Bedingung $\mathfrak{a}\eta = \mathfrak{a}'$ genügt, und hierdurch verdoppelt sich offenbar die Anzahl der Idealklassen; die Hauptklasse O besteht nur noch aus denjenigen Hauptidealen $\mathfrak{o}\mu$, welche den Zahlen μ von positiver Norm entsprechen, während die übrigen Hauptideale eine besondere, sich selbst entgegengesetzte Klasse bilden*). Die allgemeinen Sätze über die Zusammensetzung der Klassen werden aber hierdurch nicht geändert. Man kann auch leicht beweisen, daß jedes Ideal $\mathfrak{a}$ in ein Ideal der jetzigen Hauptklasse O verwandelt werden kann durch Multiplikation mit einem Faktor $\mathfrak{m}$, welcher relatives Primideal zu einem beliebig gegebenen Ideal $\mathfrak{b}$ ist; denn hat man (nach § 178, X) aus $\mathfrak{a}$ eine Zahl α so ausgewählt, daß $\mathfrak{a}\mathfrak{b} + \mathfrak{o}\alpha = \mathfrak{a}$ wird, so hat (nach § 180) jede Zahl μ, welche $\equiv \alpha \pmod{\mathfrak{a}\mathfrak{b}}$ ist, dieselbe Eigenschaft, und es braucht nur noch gezeigt zu werden, daß es unter diesen Zahlen μ auch solche von positiver Norm gibt; dies erreicht man offenbar, wenn man $\mu = \alpha + m$ setzt und die durch $\mathfrak{a}\mathfrak{b}$ teilbare natürliche Zahl m so groß wählt, daß alle mit μ konjugierten reellen Zahlen positiv ausfallen; aus $\mathfrak{o}(\alpha + m) = \mathfrak{a}\mathfrak{m}$ ergibt sich dann der verlangte Faktor $\mathfrak{m}$. Den hiermit in erweitertem Umfange bewiesenen Satz kann man offenbar auch so aussprechen:

IV. In jeder Idealklasse M gibt es Ideale $\mathfrak{m}$, die mit einem beliebig gegebenen Ideale keinen gemeinschaftlichen Teiler außer $\mathfrak{o}$ haben.

Zum Schlusse bemerken wir, daß man die Einteilung der Ideale in Klassen auf alle Moduln von der Form (8) in § 175 übertragen kann, indem man zwei solche Moduln $\mathfrak{a}$, $\mathfrak{a}'$ äquivalent nennt und in dieselbe Modulklasse A aufnimmt, wenn es eine Zahl η gibt, welche der Bedingung $\mathfrak{a}\eta = \mathfrak{a}'$ genügt. Alle Moduln einer Klasse A haben dieselbe Ordnung $\mathfrak{n}$, und die Hauptklasse dieser Ordnung besteht aus allen Hauptmoduln $\mathfrak{n}\eta$, wo η jede von Null verschiedene Zahl des Körpers Ω bedeutet. Jede Klasse besteht aus unendlich vielen ganzen und gebrochenen Moduln; eine Klasse von der Ordnung $\mathfrak{o}$ besteht aus Idealen und Idealbrüchen (Anm. auf S. 126), und das System der ersteren ist eine Idealklasse im obigen Sinne. Durch-

*) Eine noch weitergehende Beschränkung erhält man durch die Forderung, daß jede mit der erzeugenden Zahl μ konjugierte reelle Zahl positiv sein soll.

laufen $\mathfrak{a}$, $\mathfrak{b}$ bzw. alle Moduln der Klassen A, B, so bilden die Produkte $\mathfrak{a}\mathfrak{b}$ eine Klasse AB, und die Quotienten $\mathfrak{b}:\mathfrak{a}$ eine Klasse $B:A$, woraus auch die Bedeutung der Zeichen A^0 und A^{-1} einleuchtet; ebenso bilden die Komplemente aller in einer Klasse enthaltenen Moduln eine Klasse (Anm. auf S. 103). Je nachdem eine Klasse aus lauter eigentlichen oder aus lauter uneigentlichen Moduln besteht (S. 73), heiße sie eine eigentliche oder uneigentliche Klasse. Durch das Auftreten der letzteren wird (schon bei Körpern dritten Grades) diese Theorie, welche für gewisse Untersuchungen (z. B. über höhere Reziprozitätsgesetze) doch unerläßlich scheint, nicht wenig erschwert*). Schon der Beweis, daß die Anzahl der zu einer bestimmten Ordnung $\mathfrak{n}$ gehörenden Klassen A endlich ist, muß etwas anders geführt werden, wie oben für die Ideale, etwa in folgender Weise. Greift man nach Belieben aus A einen durch die Ordnung $\mathfrak{n}$ teilbaren Modul $\mathfrak{a}$ heraus, und wendet auf ihn den Satz I an, so wird $\mathfrak{a}\alpha > \mathfrak{n}\alpha > \mathfrak{a} > \mathfrak{n} > \mathfrak{o}$, also $(\mathfrak{o}, \mathfrak{a}) = (\mathfrak{o}, \mathfrak{n})(\mathfrak{n}, \mathfrak{a})$, und da [nach § 175, (12)] zugleich $\pm N(\alpha) = (\mathfrak{a}, \mathfrak{a}\alpha) = (\mathfrak{a}, \mathfrak{n}\alpha)(\mathfrak{n}\alpha, \mathfrak{a}\alpha) = (\mathfrak{a}, \mathfrak{n}\alpha)(\mathfrak{n}, \mathfrak{a})$ ist, so folgt $(\mathfrak{a}, \mathfrak{n}\alpha) \leqq H(\mathfrak{o}, \mathfrak{n})$; also gibt es in jeder Klasse A der Ordnung $\mathfrak{n}$ mindestens einen Modul $\mathfrak{a}' = \mathfrak{a}\alpha^{-1}$, welcher den Bedingungen $\mathfrak{n} > \mathfrak{a}'$ und $(\mathfrak{a}', \mathfrak{n}) \leqq H(\mathfrak{o}, \mathfrak{n})$ genügt. Betrachtet man aber eine bestimmte der (in endlicher Anzahl vorhandenen) natürlichen Zahlen m, welche $\leqq H(\mathfrak{o}, \mathfrak{n})$ sind, und bedenkt, daß $(\mathfrak{n}m^{-1}, \mathfrak{n}) = (\mathfrak{n}, \mathfrak{n}m) = m^n > 0$ ist, so folgt aus den Sätzen I und II in § 171, daß die Anzahl aller Moduln $\mathfrak{a}'$, welche den Bedingungen $\mathfrak{n} > \mathfrak{a}'$ und $(\mathfrak{a}', \mathfrak{n}) = m$, also auch $\mathfrak{a}' > \mathfrak{n}m^{-1}$ genügen, endlich ist. Mithin ist auch die Anzahl der Klassen A von der Ordnung $\mathfrak{n}$ endlich, was zu beweisen war.

§ 182.

Die Theorie der Ideale eines Körpers Ω hängt unmittelbar zusammen mit der Theorie der zerlegbaren Formen, welche demselben Körper entsprechen**); wir beschränken uns hier darauf, diesen Zusammenhang in seinen Grundzügen anzudeuten.

*) In einem gewissen Umfange ist sie behandelt in meiner Schrift: Über die Anzahl der Ideal-Klassen in den verschiedenen Ordnungen eines endlichen Körpers (Braunschweig 1877). Vgl. § 187.

**) Solche Formen sind zuerst von Lagrange betrachtet in der Abhandlung: Sur la solution des problèmes indéterminés du second degré. § VI. Mém. de l'Ac. de Berlin. T. XXIII, 1769. (Œuvres de L. T. II, 1868, p. 375.) — Additions aux Élémens d'Algèbre par L. Euler. § IX.

Es sei X eine ganze homogene Funktion n^{ten} Grades von n unabhängigen Variablen $x_1, x_2, \ldots, x_n$, und wir wollen annehmen, dieselbe sei eine zerlegbare Form, d. h. sie lasse sich als Produkt von n linearen Funktionen $u_1, u_2, \ldots, u_n$ darstellen. Alsdann verstehen wir unter der Diskriminante der Form X das Quadrat

$$(1) \qquad \left(\sum \pm \frac{\partial u_1}{\partial x_1} \frac{\partial u_2}{\partial x_2} \cdots \frac{\partial u_n}{\partial x_n}\right)^2 = \Delta(X)$$

der Funktional-Determinante, welche aus den in den Faktoren u auftretenden konstanten Koeffizienten gebildet ist*). Nun sind zwar, wenn

$$(2) \qquad X = u_1 u_2 \ldots u_n$$

eine solche gegebene zerlegbare Form ist, die Funktionen $u_1, u_2, \ldots, u_n$ nur bis auf konstante Faktoren bestimmt, und man könnte sie, ohne X zu ändern, durch $c_1 u_1, c_2 u_2, \ldots, c_n u_n$ ersetzen, wo $c_1, c_2, \ldots, c_n$ beliebige Konstanten bedeuten, die nur der Bedingung genügen müssen, daß ihr Produkt $= 1$ ist; hieraus ergibt sich aber, daß $\Delta(X)$ von der Wahl dieser Konstanten unabhängig, also durch die Form X allein vollständig bestimmt ist. Dasselbe folgt auch aus dem Satze

$$(3) \qquad X^2 \sum \pm \frac{\partial^2 \log X}{\partial x_1 \partial x_1} \frac{\partial^2 \log X}{\partial x_2 \partial x_2} \cdots \frac{\partial^2 \log X}{\partial x_n \partial x_n} = (-1)^n \Delta(X),$$

welcher aus

$$-\frac{\partial^2 \log X}{\partial x_r \partial x_s} =$$

$$\frac{\partial \log u_1}{\partial x_r} \frac{\partial \log u_1}{\partial x_s} + \frac{\partial \log u_2}{\partial x_r} \frac{\partial \log u_2}{\partial x_s} + \cdots + \frac{\partial \log u_n}{\partial x_r} \frac{\partial \log u_n}{\partial x_s}$$

hervorgeht und leicht in verschiedene andere Formen, z. B.

$$(4) \qquad \begin{vmatrix} X & \frac{\partial X}{\partial x_1} & \cdots & \frac{\partial X}{\partial x_n} \\ \frac{\partial X}{\partial x_1} & \frac{\partial^2 X}{\partial x_1 \partial x_1} & \cdots & \frac{\partial^2 X}{\partial x_1 \partial x_n} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{\partial X}{\partial x_n} & \frac{\partial^2 X}{\partial x_n \partial x_1} & \cdots & \frac{\partial^2 X}{\partial x_n \partial x_n} \end{vmatrix} = (-1)^n X^{n-1} \Delta(X)$$

*) Hermite: Sur la théorie des formes quadratiques (Crelles Journal, Bd. 47, S. 331). — Die Diskriminante der binären quadratischen Form $a x^2 + b x y + c y^2$ ist $= b^2 - 4 a c$.

umgewandelt werden kann. Besitzt X lauter ganze rationale Koeffizienten, so wollen wir deren größten gemeinschaftlichen Teiler t auch den Teiler der Form X nennen (vgl. § 61); da sich nun leicht allgemein zeigen läßt, daß der Teiler eines Produktes aus beliebigen Formen mit ganzen rationalen Koeffizienten gleich dem Produkte aus den Teilern der einzelnen Formen ist*), so folgt aus der vorstehenden Gleichung, daß $\Delta(X)$ eine ganze rationale, durch t^2 teilbare Zahl ist. Wir bemerken ferner, daß $\Delta(aX) = a^2\Delta(X)$ ist, wenn a irgendeinen konstanten Faktor bedeutet.

Wir beschränken uns nun auf die Betrachtung derjenigen zerlegbaren Formen X, welche den Idealen des Körpers Ω entsprechen und auf die folgende Weise entstehen. Zunächst wählen wir eine bestimmte Basis $\omega_1, \omega_2, \ldots, \omega_n$ für das aus allen ganzen Zahlen ω des Körpers bestehende Ideal

$$\mathfrak{o} = [\omega_1, \omega_2, \ldots, \omega_n] \tag{5}$$

und setzen (wie in § 175) die Grundzahl des Körpers, d. h. die Diskriminante

$$\Delta(\mathfrak{o}) = \Delta(\omega_1, \omega_2, \ldots, \omega_n) = D. \tag{6}$$

Nach § 177 (S. 118) ist jedes Ideal $\mathfrak{a}$ ein endlicher Modul von der Form

$$\mathfrak{a} = [\alpha_1, \alpha_2, \ldots, \alpha_n], \tag{7}$$

wo die Zahlen α_r zugleich eine Basis des Körpers Ω bilden. Da dieselben ganze Zahlen sind, so gelten n Gleichungen von der Form**)

$$\alpha_r = \sum a_{r,\iota}\,\omega_\iota, \tag{8}$$

wo die Koordinaten $a_{r,s}$ ganze rationale Zahlen sind, und zwar wollen wir die Basiszahlen stets, wie wir ein für allemal bemerken, so wählen, daß die aus diesen Koordinaten gebildete Determinante einen positiven Wert erhält, daß also

$$\sum \pm a_{1,1}\, a_{2,2} \ldots a_{n,n} = (\mathfrak{o}, \mathfrak{a}) = N(\mathfrak{a}) \tag{9}$$

*) Vgl. Gauß: D. A. art. 42 und meine Abhandlung: Über einen arithmetischen Satz von Gauß (Mitteilungen d. Deutschen math. Ges. in Prag. 1892).

**) Wir bezeichnen in der Folge mit ι, ι', ι'', ... ausschließlich Summationsbuchstaben, welche die n Werte $1, 2, \ldots, n$ durchlaufen sollen, und ein einfaches Summenzeichen Σ bezieht sich stets auf alle solche, hinter demselben auftretende ι, ι', ι'', ..., während r, s, ... konstante Indizes bedeuten.

wird (nach § 172, VII). Aus den vorstehenden Gleichungen folgt ferner [nach § 175, (7) oder (9)], daß die von der Wahl der Basis unabhängige Diskriminante

$$\Delta(\mathfrak{a}) = \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = D N(\mathfrak{a})^2 \tag{10}$$

ist.

Wir führen jetzt ein System von n unabhängigen Variablen $x_1, x_2, \ldots, x_n$ und die homogene lineare Funktion

$$\alpha = \sum x_\iota \alpha_\iota \tag{11}$$

ein; dann kann man, weil jedes Produkt $\alpha_r \omega_s$ in dem Ideal $\mathfrak{a}$ enthalten ist,

$$\alpha \omega_r = \sum x_{r,\iota} \alpha_\iota = \sum x_{r,\iota} a_{\iota,\iota'} \omega_{\iota'} \tag{12}$$

setzen, wo die n^2 Größen $x_{r,s}$ homogene lineare Funktionen der Veränderlichen $x_1, x_2, \ldots, x_n$ mit ganzen rationalen Koeffizienten bedeuten; setzt man daher die aus ihnen gebildete Determinante

$$\sum \pm x_{1,1} x_{2,2} \ldots x_{n,n} = X, \tag{13}$$

so ist X eine ganze homogene Funktion der n Variablen x_ι, deren Koeffizienten ganze rationale Zahlen sind, und wir wollen sagen, diese Form X entspreche der Basis $\alpha_1, \alpha_2, \ldots, \alpha_n$ des Ideals $\mathfrak{a}$. So oft nun die Variablen x_ι rationale Werte erhalten, wird α eine Zahl des Körpers Ω, und aus (12) folgt [nach § 167, (12)], daß die Norm von α durch Multiplikation der beiden aus den Größen $x_{\iota,\iota'}$ und $a_{\iota,\iota'}$ gebildeten Determinanten (9) und (13) entsteht, daß also

$$N(\alpha) = N(\mathfrak{a}) X \tag{14}$$

ist; da nun diese Norm das Produkt der n mit α konjugierten Zahlen, welche homogene lineare Funktionen der Variablen x_ι sind, und da zufolge (10) die Diskriminante dieses Produktes $= D N(\mathfrak{a})^2$ ist, so ergibt sich, daß X ebenfalls eine zerlegbare Form, und daß ihre Diskriminante

$$\Delta(X) = D \tag{15}$$

ist.

Legt man den Variablen x_ι ganze rationale Werte bei, so wird α teilbar durch $\mathfrak{a}$, und umgekehrt wird jede Zahl des Ideals $\mathfrak{a}$ durch ein und nur ein solches System von Werten x_ι erzeugt; dann ist

$$\mathfrak{o}\alpha = \mathfrak{a}\mathfrak{m}, \quad N(\alpha) = N(\mathfrak{a}) X = \pm N(\mathfrak{a}) N(\mathfrak{m}),$$

mithin

$$X = \pm N(\mathfrak{m}) = \pm (\mathfrak{a}, \mathfrak{o}\alpha). \tag{16}$$

Ist nun k eine beliebig gegebene natürliche Zahl, so kann man (nach § 178, XI) die Zahl α aus dem Ideal $\mathfrak{a}$ so auswählen, daß $\mathfrak{m}$ relatives Primideal zu k, also (nach § 180, I) der zugehörige Wert der Form X relative Primzahl zu k wird, woraus unmittelbar folgt, daß X eine ursprüngliche, d. h. eine solche Form ist, deren Koeffizienten keinen gemeinschaftlichen Teiler haben.

Verfährt man bei der Einteilung der Ideale in Klassen nach der schärferen Regel, welche auf S. 145 beschrieben ist — und dies soll im folgenden immer geschehen —, so wird, wenn $\mathfrak{a}$ der Klasse A angehört, und $\mathfrak{m}$ jedes beliebige Ideal der inversen Klasse A^{-1} bedeutet, immer eine Zahl α von positiver Norm existieren, welche der Bedingung $\mathfrak{o}\alpha = \mathfrak{a}\mathfrak{m}$ genügt, und gleichzeitig wird $X = +N(\mathfrak{m})$; mithin können durch die Form X die Normen aller in der Klasse A^{-1} enthaltenen Ideale $\mathfrak{m}$ dargestellt werden (vgl. § 60). Umgekehrt leuchtet ein, daß jeder durch die Form X darstellbare positive Wert, welcher ganzen rationalen Werten der Variablen x_ι entspricht, die Norm eines solchen Ideals $\mathfrak{m}$ ist.

Wählt man für dasselbe Ideal $\mathfrak{a}$ ein beliebiges anderes System von Basiszahlen $\beta_1, \beta_2, \ldots, \beta_n$, die aber ebenfalls der Bedingung genügen, daß die aus ihren Koordinaten gebildete Determinante positiv ist, so ist

$$(17) \qquad \beta_r = \sum c_{r,\iota}\alpha_\iota; \quad \sum \pm c_{1,1}c_{2,2}\ldots c_{n,n} = +1$$

und die der Basis $\alpha_1, \alpha_2, \ldots, \alpha_n$ entsprechende Form X geht durch die Substitution

$$(18) \qquad x_r = \sum c_{\iota,r}\, y_\iota,$$

deren Koeffizienten $c_{\iota,\iota'}$ ganze rationale Zahlen sind, in eine äquivalente Form Y über, welche der neuen Basis entspricht und eine ganze homogene Funktion der neuen Variablen y_ι ist. Umgekehrt, wenn Y mit X äquivalent ist, d. h. wenn X durch eine Substitution von der Form (18) mit ganzen rationalen Koeffizienten $c_{\iota,\iota'}$, deren Determinante $= +1$ ist, in Y übergeht, so gibt es offenbar eine Basis des Ideals $\mathfrak{a}$, welcher diese Form Y entspricht. Allen Basen desselben Ideals $\mathfrak{a}$ entspricht daher eine bestimmte Formenklasse, d. h. ein System von Formen $X, Y \ldots$ derart, daß je zwei von ihnen einander äquivalent sind, und wir wollen sagen, daß diese Formenklasse dem Ideale $\mathfrak{a}$ entspricht. Ist ferner $\mathfrak{a}'$ ein beliebiges mit $\mathfrak{a}$ äquivalentes Ideal, so gibt es eine Zahl η von positiver Norm, welche

der Bedingung $\mathfrak{a}\eta = \mathfrak{a}'$ genügt; dann bilden die n Produkte $\eta\alpha_\iota$ eine Basis von $\mathfrak{a}'$, und aus (12) geht durch Multiplikation mit η hervor, daß die Form X auch dem Ideal $\mathfrak{a}'$, mithin die Formenklasse auch allen Idealen der Klasse A entspricht. Jeder Idealklasse entspricht daher eine bestimmte Formenklasse. Die schwierigere Frage aber, ob mehreren verschiedenen Idealklassen eine und dieselbe Formenklasse entsprechen kann, müssen wir der Kürze halber hier unerörtert lassen. Dasselbe gilt von der Aufgabe, alle Transformationen der Form X in sich selbst zu finden, und wir beschränken uns auf die einleuchtende Bemerkung, daß durch jede Einheit ε, deren Norm positiv, also $= +1$ ist, eine solche Transformation erzeugt wird, weil die n Zahlen $\varepsilon\alpha_\iota$ ebenfalls eine Basis des Ideals $\mathfrak{a}$ bilden (vgl. §§ 62, 83—85).

Die Komposition der Formen X entspricht der Multiplikation der Ideale. Es seien zwei beliebige Ideale

(19) $$\mathfrak{a} = [\alpha_1, \alpha_2, \ldots, \alpha_n], \quad \mathfrak{b} = [\beta_1, \beta_2, \ldots, \beta_n]$$

mit bestimmten Basen α_ι, β_ι gegeben, so kann man ihr Produkt

(20) $$\mathfrak{a}\mathfrak{b} = \mathfrak{c} = [\gamma_1, \gamma_2, \ldots, \gamma_n]$$

setzen; aus dem Begriffe der Multiplikation der Moduln (§ 170) folgt aber unmittelbar, daß $\mathfrak{a}\mathfrak{b}$ ein endlicher Modul ist, welcher die n^2 Produkte $\alpha_\iota\beta_{\iota'}$ zu Basiszahlen hat; zwischen diesen und den n Basiszahlen γ_ι desselben Moduls müssen daher [zufolge § 172, (25) bis (30)] Relationen von der Form

(21) $$\alpha_r\beta_s = \sum p_\iota^{r,s}\gamma_\iota, \quad \gamma_r = \sum q_r^{\iota,\iota'}\alpha_\iota\beta_{\iota'}$$

stattfinden, wo die Koeffizienten p, q ganze rationale Zahlen sind; die sämtlichen Determinanten P, welche sich aus je n der n^2 Zeilen

(22) $$p_1^{r,s}, p_2^{r,s}, \ldots, p_{n-1}^{r,s}, p_n^{r,s}$$

bilden lassen, sind Zahlen ohne gemeinschaftlichen Teiler. Man führe jetzt drei Systeme von je n Variablen $x_\iota, y_\iota, z_\iota$ ein und setze

(23) $$\alpha = \sum x_\iota\alpha_\iota, \quad \beta = \sum y_\iota\beta_\iota, \quad \gamma = \sum z_\iota\gamma_\iota,$$

so wird

(24) $$N(\alpha) = N(\mathfrak{a})X, \quad N(\beta) = N(\mathfrak{b})Y, \quad N(\gamma) = N(\mathfrak{c})Z,$$

wo X, Y, Z die den obigen Basen der Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ entsprechenden Formen bedeuten. Macht man nun die Variablen z_ι durch die bilineare Substitution

(25) $$z_r = \sum p_r^{\iota,\iota'} x_\iota y_{\iota'}$$

zu Funktionen der Variablen x_ι, y_ι, so wird

$$\gamma = \alpha\beta, \quad \text{also} \quad N(\gamma) = N(\alpha)N(\beta), \tag{26}$$

und da außerdem $N(\mathfrak{c}) = N(\mathfrak{a})N(\mathfrak{b})$ ist, so folgt

$$Z = XY, \tag{27}$$

d. h. die Form Z geht durch die Substitution (25) in das Produkt der beiden Formen X, Y über, und wir wollen deshalb sagen, die Form Z sei aus den beiden Formen X, Y zusammengesetzt.

Diese Formen sind durch die Substitution (25) vollständig bestimmt. Aus (26) folgt nämlich zunächst

$$\alpha\beta_r = \sum \frac{\partial z_\iota}{\partial y_r}\gamma_\iota; \tag{28}$$

nun lassen sich die Zahlen γ_ι, weil sie in $\mathfrak{c}$ und also auch in $\mathfrak{b}$ enthalten sind, in der Form

$$\gamma_\iota = \sum c_{\iota,\iota'}\beta_{\iota'}$$

darstellen, wo die Koeffizienten $c_{\iota,\iota'}$ ganze rationale Zahlen bedeuten, deren Determinante

$$\sum \pm c_{1,1}c_{2,2}\ldots c_{n,n} = (\mathfrak{b},\mathfrak{c}) = N(\mathfrak{a})$$

ist; es wird mithin

$$\alpha\beta_r = \sum \frac{\partial z_\iota}{\partial y_r}c_{\iota,\iota'}\beta_{\iota'},$$

woraus

$$N(\alpha) = N(\mathfrak{a})\sum \pm \frac{\partial z_1}{\partial y_1}\frac{\partial z_2}{\partial y_2}\cdots\frac{\partial z_n}{\partial y_n},$$

also

$$X = \sum \pm \frac{\partial z_1}{\partial y_1}\frac{\partial z_2}{\partial y_2}\cdots\frac{\partial z_n}{\partial y_n} \tag{29}$$

folgt. Auf ganz ähnliche Weise ergibt sich natürlich aus den Gleichungen

$$\beta\alpha_r = \sum \frac{\partial z_\iota}{\partial x_r}\gamma_\iota \tag{30}$$

die Form

$$Y = \sum \pm \frac{\partial z_1}{\partial x_1}\frac{\partial z_2}{\partial x_2}\cdots\frac{\partial z_n}{\partial x_n}. \tag{31}$$

Unsere obigen Gleichungen (12) und (13) gehen offenbar durch die spezielle Annahme $\mathfrak{b} = \mathfrak{o}$ aus den allgemeinen Gleichungen (28) und (29) hervor. Die in den letzteren auftretenden n^2 Größen

$$\frac{\partial z_m}{\partial y_s} = \sum p_m^{\iota,s}x_\iota \tag{32}$$

sind homogene lineare Funktionen der n Variablen x_ι mit ganzen rationalen Koeffizienten $p_m^{r,s}$, und zwar sind

$$p_m^{1,s},\ p_m^{2,s} \dots p_m^{n-1,s},\ p_m^{n,s} \tag{33}$$

die in einer und derselben Zeile enthaltenen Koeffizienten. Es ist nun von Wichtigkeit, daß umgekehrt die n Variablen x_ι sich (auf unendlich viele Arten) als homogene lineare Funktionen der n^2 Größen (32) mit ganzen rationalen Koeffizienten darstellen lassen, oder, was offenbar auf dasselbe hinauskommt, daß die sämtlichen Determinanten R, welche aus je n von den n^2 Zeilen (33) gebildet und von den oben mit P bezeichneten Determinanten wohl zu unterscheiden sind, ebenfalls keinen gemeinschaftlichen Teiler haben. Um dies letztere zu beweisen, bemerken wir zunächst, daß die Determinanten R gewiß nicht alle verschwinden; denn betrachtet man z. B. solche n Zeilen (33), in welchen der Index s ungeändert bleibt, so ist, wie sich durch Vertauschung der Horizontal- und Vertikalreihen unter Berücksichtigung von (21) leicht ergibt, die entsprechende Determinante

$$\begin{vmatrix} p_1^{1,s} \dots p_1^{n,s} \\ \dots\dots\dots \\ p_n^{1,s} \dots p_n^{n,s} \end{vmatrix} = \begin{vmatrix} p_1^{1,s} \dots p_n^{1,s} \\ \dots\dots\dots \\ p_1^{n,s} \dots p_n^{n,s} \end{vmatrix} = \frac{N(\beta_s)}{N(\mathfrak{b})},$$

also von Null verschieden. Bedeutet nun e den größten gemeinschaftlichen Teiler aller Determinanten R, so folgt aus unserer allgemeinen Untersuchung über die Reduktion eines endlichen Moduls auf eine irreduzible Basis (§ 172), daß sich zwei Systeme von ganzen rationalen Zahlen $h_m^{r,s}$ und $e_{r,s}$ aufstellen lassen, welche den Bedingungen

$$p_m^{r,s} = \sum h_m^{\iota,s} e_{r,\iota}, \qquad \sum \pm e_{1,1} e_{2,2} \dots e_{n,n} = e$$

genügen*). Hierauf definiere man n Zahlen μ_ι durch die Gleichungen

$$e\,\alpha_r = \sum e_{r,\iota}\,\mu_\iota,$$

*) Man braucht nur n beliebige, aber voneinander unabhängige Zahlen α_ι' zu wählen und den Modul, dessen Basis aus den n^2 Summen

$$\varepsilon_m^{(s)} = \sum p_m^{\iota,s}\,\alpha_\iota'$$

besteht, auf eine irreduzible, also aus n Zahlen

$$\varepsilon_r = \sum e_{\iota,r}\,\alpha_\iota'$$

bestehende Basis zu reduzieren, so wird

$$\varepsilon_m^{(s)} = \sum h_m^{\iota,s}\,\varepsilon_\iota,$$

und hieraus ergeben sich die obigen Beziehungen. — Bedeuten $\mathfrak{a}$, $\mathfrak{b}$ beliebige Moduln von der Form (8) in § 175, und wählt man für die n Zahlen α die

aus denen durch Umkehrung

$$\mu_r = \sum e'_{\iota,r}\, \alpha_\iota$$

folgt, wo die Koeffizienten $e'_{\iota,\iota'}$ ganze rationale Zahlen sind, deren Determinante

$$\sum \pm e'_{1,1}\, e'_{2,2} \dots e'_{n,n} = e^{n-1}$$

ist, weil

$$\sum e'_{\iota,r}\, e_{\iota,s} = e \text{ oder } = 0$$

ist, je nachdem r, s gleich oder ungleich sind. Mit Rücksicht auf (21) folgt nun aus den vorstehenden Gleichungen

$$\begin{aligned} \mu_r \beta_s &= \sum e'_{\iota',r}\, \alpha_{\iota'}\, \beta_s = \sum e'_{\iota',r}\, p_\iota^{\iota',s}\, \gamma_\iota \\ &= \sum e'_{\iota',r}\, h_\iota^{\iota'',s}\, e_{\iota',\iota''}\, \gamma_\iota = e \sum h_\iota^{r,s}\, \gamma_\iota; \end{aligned}$$

mithin ist $\mathfrak{b}\,\mu_r$ teilbar durch $e\,\mathfrak{c} = e\,\mathfrak{a}\,\mathfrak{b}$, also μ_r teilbar durch $e\,\mathfrak{a}$, und hieraus folgt, daß alle Koeffizienten $e'_{\iota,\iota'}$ durch e teilbar sind, mithin $e = 1$ ist, was zu beweisen war.

Derselbe Satz gilt selbstverständlich auch für die Determinanten S, welche aus je n Zeilen von der Form

$$(34) \qquad p_m^{r,1},\ p_m^{r,2} \dots p_m^{r,n-1},\ p_m^{r,n}$$

gebildet sind; also lassen sich die n Variablen y_ι auch als homogene lineare Funktionen der n^2 Größen

$$(35) \qquad \frac{\partial z_m}{\partial x_r} = \sum p_m^{r,\iota}\, y_\iota,$$

und zwar mit ganzen rationalen Koeffizienten darstellen.

Ganz ähnliche Eigenschaften, wie die linearen Funktionen (32) und (35), besitzen auch die aus ihnen gebildeten Determinanten $(n-1)^{\text{ten}}$ Grades, d. h. die Koeffizienten, mit welchen sie in den Determinanten (29) und (31) behaftet sind. Das Ideal $\mathfrak{a}$ besitzt (nach § 180) ein durch die Bedingung $\mathfrak{o}\,N(\mathfrak{a}) = \mathfrak{a}\,\mathfrak{a}'$ bestimmtes Supplement*)

$$(36) \qquad \mathfrak{a}' = [\alpha'_1,\ \alpha'_2,\ \dots,\ \alpha'_n],$$

---

zu α_ι komplementären Zahlen (§ 167 und § 175 Anm.), so wird $\varepsilon_m^{(s)} = \beta_s \gamma'_m$, wo die Zahlen γ'_ι komplementär zu γ_ι sind, und hieraus ergibt sich (nach § 172), daß der größte gemeinsame Teiler $e = (\mathfrak{a}', \mathfrak{b}\,\mathfrak{c}')$ ist, wo $\mathfrak{a}'$, $\mathfrak{b}'$, $\mathfrak{c}'$ die zu $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ komplementären Moduln bedeuten; sind aber $\mathfrak{a}$, $\mathfrak{b}$ (also auch $\mathfrak{c}$) Idealbrüche (Anm. zu §§ 178, 180), so gilt dasselbe von $\mathfrak{a}'$, $\mathfrak{b}'$, $\mathfrak{c}'$, und aus § 170, VII folgt leicht, daß in diesem Falle $\mathfrak{a}' = \mathfrak{b}\,\mathfrak{c}'$, also $e = 1$ ist.

*) Dieses Ideal $\mathfrak{a}'$ und seine Basiszahlen α'_ι dürfen natürlich nicht verwechselt werden mit dem in der vorigen Anmerkung erwähnten Komplement von $\mathfrak{a}$ und mit den zu α_ι komplementären Zahlen.

dessen Basis wir beliebig wählen; bedeutet nun α wieder irgendeine Zahl des Ideals $\mathfrak{a}$, und setzt man, wie in (16), $\mathfrak{o}\alpha = \mathfrak{a}\mathfrak{m}$, so folgt, wenn man mit $\mathfrak{m}'$ das Supplement von $\mathfrak{m}$ bezeichnet,

$$\mathfrak{o}N(\alpha) = \mathfrak{o}N(\mathfrak{a})N(\mathfrak{m}) = \mathfrak{a}\mathfrak{a}'\mathfrak{m}\mathfrak{m}' = \alpha\mathfrak{a}'\mathfrak{m}';$$

es ergibt sich daher von neuem, daß $N(\alpha)$ durch α teilbar ist (§ 176, IV), und wenn α' das durch die Gleichung

$$N(\alpha) = \alpha\alpha' \tag{37}$$

definierte Supplement der Zahl α bedeutet, so folgt $\mathfrak{o}\alpha' = \mathfrak{a}'\mathfrak{m}'$, d. h. α' ist teilbar durch $\mathfrak{a}'$, also von der Form

$$\alpha' = \sum x_\iota' \alpha_\iota', \tag{38}$$

wo die n Koeffizienten x_ι' ganze rationale Zahlen sind, die in bestimmter Weise von den ganzen rationalen Zahlen x_ι in (11) oder (23) abhängen. Setzt man nun wieder $\mathfrak{a}\mathfrak{b} = \mathfrak{c}$ und behält alle hierauf bezüglichen, im vorhergehenden gebrauchten Bezeichnungen bei, so folgt $\mathfrak{a}'\mathfrak{c} = \mathfrak{b}N(\mathfrak{a})$; man kann daher, wenn man die Größen x_ι' in (38) als willkürliche Variable ansieht, n Gleichungen von der Form

$$\alpha'\gamma_r = N(\mathfrak{a}) \sum x_{r,\iota}' \beta_\iota \tag{39}$$

aufstellen, welche den Gleichungen (28) entsprechen; die n^2 Größen $x_{\iota,\iota'}'$ sind homogene lineare Funktionen der n Variablen x_ι' mit ganzen rationalen Koeffizienten, und umgekehrt lassen sich, wie oben gezeigt ist, die Variablen x_ι' (auf unendlich viele Arten) als ebensolche Funktionen von den Größen $x_{\iota,\iota'}'$ darstellen. Multipliziert man aber (39) mit α unter Berücksichtigung von (37) und (24), so ergibt sich

$$X\gamma_r = \alpha \sum x_{r,\iota}' \beta_\iota, \tag{40}$$

und hieraus geht mit Rücksicht auf (28) hervor, daß $x_{m,s}'$ der Koeffizient ist, mit welchem das Element (32) in der Determinante (29) multipliziert wird. Die sämtlichen Größen $x_{\iota,\iota'}'$ und folglich auch die Größen x_ι', welche letzteren offenbar von der Wahl der Basis des Ideals $\mathfrak{a}'$ abhängen, sind daher ganze homogene Funktionen $(n-1)^{\text{ten}}$ Grades von den Variablen x_ι mit ganzen rationalen Koeffizienten, und hiermit ist unsere obige Behauptung bewiesen. —

Auf diese kurze Darstellung der wichtigsten Eigenschaften der Formen X müssen wir uns hier beschränken; allein wir dürfen nicht unterlassen, darauf aufmerksam zu machen, daß diese Formen X, deren Diskriminante $= D$ ist, nur einen unendlich kleinen Teil aller

zerlegbaren Formen bilden, welche dem Körper Ω entsprechen, und wir wollen hierüber wenigstens noch folgendes bemerken. Bedeutet $\mathfrak{a}$ in (7) einen beliebigen Modul, dessen Basis zugleich eine Basis des Körpers Ω ist, und verfährt man mit $\mathfrak{a}$ genau ebenso, wie oben in den Gleichungen (11) bis (16) mit dem Ideal $\mathfrak{a}$, indem man nur an Stelle von $\mathfrak{o}$ die Ordnung $\mathfrak{n}$ des Moduls $\mathfrak{a}$ eintreten läßt, so gelangt man zu einer entsprechenden zerlegbaren Form $X = \pm(\mathfrak{a}, \mathfrak{n}\alpha)$, deren Diskriminante $= D(\mathfrak{o}, \mathfrak{n})^2 = \Delta(\mathfrak{n})$ ist. Wir nennen die Zahl $(\mathfrak{o}, \mathfrak{n})$ den Index und den Quotient $\mathfrak{n} : \mathfrak{o}$ den Führer der Ordnung $\mathfrak{n}$; der letztere ist immer ein Ideal, und zwar der größte gemeinsame Teiler aller durch $\mathfrak{n}$ teilbaren Ideale, und der Index ist immer teilbar durch den Führer*).

§ 183.

Von der größten Wichtigkeit für die Theorie der in einem endlichen Körper Ω enthaltenen ganzen Zahlen ist die Frage nach dem Inbegriff aller unter ihnen befindlichen Einheiten (§§ 174, 176). Im Körper R der rationalen Zahlen gibt es nur die beiden Einheiten ± 1, und dasselbe gilt für alle quadratischen Körper von negativer Grundzahl D, mit Ausnahme der beiden Fälle $D = -3$ und $D = -4$, in welchen sechs bzw. vier Einheiten vorhanden sind. Bei allen anderen Körpern ist aber die Anzahl der Einheiten stets unendlich groß, und es ist äußerst schwierig gewesen, den Zusammenhang zwischen allen diesen Einheiten genau zu ergründen und in der einfachsten Form darzustellen; für den Fall der quadratischen Körper von positiver Grundzahl D fällt diese Frage im wesentlichen zusammen mit der Auflösung der Pellschen Gleichung $t^2 - Du^2 = 4$, und wir haben schon früher bemerkt, daß die Existenz solcher Lösungen t, u, in welchen u nicht verschwindet, zuerst von Lagrange bewiesen ist. Die Prinzipien, welche diesem Beweise zugrunde liegen, sind endlich von Dirichlet zur höchsten Allgemeinheit erhoben, und ihm gebührt der Ruhm, zuerst eine strenge und vollständige, alle endlichen Körper umfassende Theorie der Einheiten aufgebaut zu haben (vgl. §§ 83, 141). Wir kleiden dieselbe in unsere Ausdrucksweise ein und heben die Hauptmomente im folgenden so kurz wie möglich hervor.

*) Vgl. meine auf S. 136 und 146 zitierten Schriften, wo das Wort Index in einer spezielleren Bedeutung gebraucht ist.

1. Wir bezeichnen, wie bisher, mit Ω einen Körper n^{ten} Grades und mit

$$\mathfrak{o} = [\omega_1, \omega_2, \ldots, \omega_n] \tag{1}$$

den Inbegriff aller in Ω enthaltenen ganzen Zahlen

$$\omega = h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n = \sum h_\iota\omega_\iota, \tag{2}$$

wo die n Koordinaten h_ι alle ganzen rationalen Zahlen durchlaufen. Durch die n Permutationen des Körpers, die wir wieder mit $\pi_1, \pi_2, \ldots, \pi_n$ bezeichnen, geht eine solche Zahl ω in die n konjugierten Zahlen

$$\omega^{(r)} = \sum h_\iota\omega_\iota^{(r)} \tag{3}$$

über, welche homogene lineare Funktionen der variablen Koordinaten h_ι sind. Die Koeffizienten derselben sind die n^2 Konstanten $\omega_s^{(r)}$, welche durch die Wahl der Basis von $\mathfrak{o}$ ein für allemal bestimmt sind. Wir bilden nun, indem wir unter $M(z)$ stets den analytischen Modul (oder absoluten Betrag) der komplexen Zahl z verstehen, für jede Permutation π_r die Summe

$$M(\omega_1^{(r)}) + M(\omega_2^{(r)}) + \cdots + M(\omega_n^{(r)})$$

und bezeichnen mit c die größte von diesen n Summen; dann leuchtet ein, daß, wenn k eine positive Größe und ω eine Zahl ist, deren Koordinaten absolut genommen den Wert k nicht überschreiten, immer

$$M(\omega^{(r)}) \leqq c\,k \tag{4}$$

sein wird.

2. Die aus den n^2 Koeffizienten $\omega_s^{(r)}$ gebildete Determinante

$$\sum \pm \omega_1' \omega_2'' \ldots \omega_n^{(n)} = \sqrt{D} \tag{5}$$

ist von Null verschieden (§ 175), und wenn man mit $\varkappa_1, \varkappa_2, \ldots, \varkappa_n$ die zu $\omega_1, \omega_2, \ldots, \omega_n$ komplementären Zahlen bezeichnet (§ 167), so erhält man durch Umkehrung der Gleichungen (3) die n Koordinaten

$$h_s = S(\omega\varkappa_s) = \varkappa_s'\omega' + \cdots + \varkappa_s^{(n)}\omega^{(n)} \tag{6}$$

als homogene lineare Funktionen der n Konjugierten $\omega^{(r)}$; da die Koeffizienten $\varkappa_s^{(r)}$ ebenfalls durch die Basis von $\mathfrak{o}$ vollständig bestimmt sind, so schließt man ebenso wie vorher, daß, wenn die n Moduln $M(\omega^{(r)})$ eine gegebene Konstante C nicht überschreiten, auch die absoluten Werte der Koordinaten h_s eine entsprechende Konstante nicht überschreiten können, und da sie ganze rationale Zahlen sind, so folgt hieraus offenbar der Satz:

I. Ist C eine positive Konstante, so gibt es in $\mathfrak{o}$ nur eine endliche Anzahl von solchen Zahlen ω, deren Konjugierte sämtlich der Bedingung $M(\omega^{(r)}) < C$ genügen.

3. Bedeutet θ eine Zahl n^{ten} Grades in Ω, so ist Ω der Inbegriff $R(\theta)$ aller durch θ rational darstellbaren Zahlen (§ 165, VI), und die n verschiedenen konjugierten Zahlen $\theta^{(r)}$ sind die Wurzeln einer irreduziblen Gleichung mit rationalen Koeffizienten. Durch die Permutation π_r geht der Körper Ω in den Körper $\Omega^{(r)} = R(\theta^{(r)})$ über, und wir nennen π_r eine reelle Permutation, wenn $\theta^{(r)}$ reell ist, also $\Omega^{(r)}$ aus lauter reellen Zahlen besteht; zugleich ist $\omega^{(r)}$ in (3) eine reelle, d. h. eine mit lauter reellen Koeffizienten $\omega_s^{(r)}$ behaftete, lineare Funktion der Koordinaten h_ι. Ist aber z. B. θ' imaginär $= p + qi$, so nennen wir π_1 eine imaginäre Permutation, weil Ω' außer reellen auch imaginäre Zahlen enthält; die n Konstanten ω_ι' können nicht alle reell sein, und es wird folglich die Funktion ω' die Form $u + vi$ annehmen, wo u, v reelle lineare Funktionen der Koordinaten h_ι bedeuten. In diesem Falle gibt es bekanntlich*) unter den konjugierten Zahlen $\theta^{(r)}$ immer eine zweite $\theta'' = p - qi$, und durch die entsprechende Permutation π_2 geht ω in $\omega'' = u - vi$ über; wir wollen zwei solche Permutationen π_1, π_2 (sowie die Körper Ω', Ω'' und die Funktionen ω', ω'') immer ein imaginäres Paar, und u, v das zugehörige reelle Funktionen-Paar nennen. Bezeichnen wir die Anzahl dieser Paare mit $(n - \nu)$, so ist $2(n - \nu)$ die Anzahl der imaginären, und $(2\nu - n)$ diejenige der reellen Permutationen, und ν ist die Gesamtanzahl aller imaginären Paare und aller reellen Permutationen. Diese Zahl ν, welche von der größten Bedeutung für die Theorie der Einheiten ist, wird offenbar nur dann $= 1$, wenn Ω der Körper R der rationalen Zahlen oder ein quadratischer Körper von negativer Grundzahl ist; da es aber in diesen Fällen, wie oben bemerkt, nur zwei (oder vier oder sechs) Einheiten gibt, so bieten sie kein weiteres Interesse dar, und wir setzen daher im folgenden voraus, es sei $\nu \geqq 2$. Verbindet man je zwei, einem imaginären Paar entsprechende Zeilen der Determinante (5) durch Addition und Subtraktion, so ergibt sich, daß immer

$$D = (-1)^{n-\nu}(D) \tag{7}$$

ist, wo (D) den absoluten Wert der Grundzahl bedeutet.

*) Dies beruht darauf, daß die Gleichung $i^2 + 1 = 0$ in bezug auf jeden reellen Körper irreduzibel ist.

4. Wir verteilen nun die n Permutationen π_r nach Belieben in zwei Klassen, doch so, daß jede dieser Klassen wenigstens eine Permutation enthält, und daß die beiden Permutationen eines imaginären Paares in dieselbe Klasse fallen*); dann gilt, wenn c die obige Bedeutung behält, und allgemein mit α die zur ersten, mit β die zur zweiten Klasse gehörenden Funktionen $\omega^{(r)}$ bezeichnet werden, der folgende Satz:

II. Ist a ein beliebig kleiner, b ein beliebig großer positiver gegebener Wert, so kann man in $\mathfrak{o}$ eine Zahl ω so wählen, daß alle $M(\alpha) < a$, alle $M(\beta) > b$ ausfallen, und daß absolut $N(\omega) < (3c)^n$ wird.

Um dies zu beweisen, betrachten wir zunächst nur die Funktionen α der ersten Klasse, deren Anzahl wir mit μ bezeichnen wollen; indem wir jedes unter ihnen befindliche imaginäre Paar durch das zugehörige reelle Paar ersetzen, jede reelle Funktion α aber beibehalten, gelangen wir offenbar zu μ reellen homogenen linearen Funktionen w, die wir in bestimmter Ordnung mit $w_1, w_2, \ldots, w_\mu$ bezeichnen wollen. Ist nun k eine bestimmte natürliche Zahl, und legt man den Koordinaten h_ι alle Werte aus der Reihe der $(k+1)$ Zahlen $0, 1, 2, \ldots, k$ bei, so erhält man $(k+1)^n$ verschiedene Zahlen ω in $\mathfrak{o}$, für welche alle $M(\alpha) \leqq ck$ ausfallen, und folglich liegen alle zugehörigen Werte der μ Funktionen w zwischen $-ck$ und $+ck$. Das durch diese beiden Zahlen $\pm ck$ begrenzte reelle Zahlengebiet wollen wir auf folgende Weise in kleinere Intervalle einteilen. Da $n > \mu > 0$, und $k > 0$ ist, so ergibt sich leicht**), daß die Differenz

$$(k+1)^{\frac{n}{\mu}} - k^{\frac{n}{\mu}} > 1$$

ist, und daß folglich zwischen Minuend und Subtrahend mindestens eine natürliche Zahl m liegt, welche mithin den Bedingungen

$$(8) \qquad (k+1)^n > m^\mu > k^n$$

genügt; setzt man nun zur Abkürzung

$$(9) \qquad d = \frac{2ck}{m} < 2ck^{1-\frac{n}{\mu}},$$

*) Diese Bedingungen würden nur in dem ausgeschlossenen Falle $\nu = 1$ sich nicht vereinigen lassen.

**) Ist die Konstante $s > 1$, so hat die Funktion $\varphi(x) = (x+1)^s - x^s - 1$, welche zugleich mit x verschwindet, eine Derivierte $\varphi'(x)$, die für $x \geqq 0$ stets positiv ist, und folglich ist $\varphi(x) > 0$ für $x > 0$.

so zerfällt das obige Zahlgebiet durch Einschaltung der $(m-1)$ Zahlen

$$-ck+d, \quad -ck+2d \ldots \quad -ck+(m-1)d$$

in m Intervalle von gleicher Breite d, wobei man diese $(m-1)$ Zahlen selbst nach Belieben dem einen oder anderen der beiden benachbarten Intervalle zurechnen kann. Schreiben wir ferner einem reellen Werte w die bestimmte Intervallzahl s zu, wenn w dem von den beiden Zahlen $-ck+(s-1)d$ und $-ck+sd$ begrenzten Intervall angehört, so besitzen die zu einer bestimmten Zahl ω gehörenden μ Werte $w_1(\omega), w_2(\omega), \ldots, w_\mu(\omega)$ ihre entsprechenden Intervallzahlen $s_1, s_2, \ldots, s_\mu$, und wir dürfen dies kurz so ausdrücken, daß der Zahl ω diese bestimmte Folge $s_1, s_2, \ldots, s_\mu$ entspricht. Da jede Intervallzahl s eine der m Zahlen $1, 2, \ldots, m$ ist, so ist m^μ die Anzahl aller überhaupt denkbaren Folgen, und da dieselbe zufolge (8) kleiner ist als die Anzahl $(k+1)^n$ aller voneinander verschiedenen Zahlen ω, welche auf die obige Weise gebildet werden können, so muß es unter den letzteren mindestens zwei verschiedene $\varkappa, \lambda$ geben, denen eine und dieselbe Folge von Intervallzahlen $s_1, s_2, \ldots, s_\mu$ entspricht; es werden daher, wenn man die von Null verschiedene, in $\mathfrak{o}$ enthaltene Zahl $\varkappa - \lambda = \omega$ setzt, die absoluten Werte der μ Differenzen

$$w_1(\varkappa) - w_1(\lambda) = w_1(\omega) \ldots w_\mu(\varkappa) - w_\mu(\lambda) = w_\mu(\omega)$$

sämtlich $\leqq d$ sein, weil jedesmal der Minuend und Subtrahend in dasselbe Intervall fallen. Hieraus folgt für die Werte der zur ersten Klasse gehörigen, mit dieser Zahl ω konjugierten Zahlen α, welche entweder mit einer Größe $w(\omega)$ übereinstimmen oder von der Form $w_1(\omega) \pm i\, w_2(\omega)$ sind, daß $M(\alpha) \leqq d\sqrt{2}$, also zufolge (9) auch

$$M(\alpha) < 3\, c\, k^{1-\frac{n}{\mu}} \tag{10}$$

ist. Bedeuten nun A, B bzw. die absoluten Werte der beiden Produkte aus den μ Konjugierten α und aus den $(n-\mu)$ Konjugierten β, welche zu der zweiten Klasse gehören, so ist $\pm N(\omega) = AB$, und $A < (3\,c)^\mu\, k^{\mu-n}$; da ferner die Koordinaten der Differenz $\omega = \varkappa - \lambda$ absolut genommen den Wert k nicht überschreiten, also $M(\beta) \leqq c\,k$, $B \leqq (c\,k)^{n-\mu}$ ist, so folgt

$$\pm N(\omega) < (3\,c)^n. \tag{11}$$

Da endlich $N(\omega)$ eine von Null verschiedene ganze rationale Zahl ist, so wird $AB \geqq 1$, also $B > (3\,c)^{-\mu}\, k^{n-\mu}$; greift man nun aus der

zweiten Klasse eine beliebige Zahl β heraus und setzt $B = B_1 M(\beta)$, so ist $B_1 \leqq (c\,k)^{n-u-1}$, mithin

$$M(\beta) > (3\,c)^{1-n} k. \tag{12}$$

Offenbar kann nun, wie klein auch a, und wie groß auch b gegeben sein mag, die Zahl k zufolge (10) und (12) stets so groß gewählt werden, daß alle $M(\alpha) < a$, alle $M(\beta) > b$ ausfallen, während zufolge (11) immer $N(\omega)$ absolut $< (3\,c)^n$ wird, w. z. b. w.

5. Aus dem soeben bewiesenen Satze II ergibt sich, indem man dieselbe Einteilung der Permutationen π_r in zwei Klassen beibehält, daß man eine nie abreißende Kette von aufeinanderfolgenden, von Null verschiedenen ganzen Zahlen

$$\omega = \eta_1,\ \eta_2,\ \eta_3,\ \cdots,\ \eta_s,\ \eta_{s+1},\ \cdots \tag{13}$$

bilden kann, deren Normen absolut $< (3\,c)^n$ sind, und welche außerdem noch die zweite Eigenschaft besitzen, daß, wenn mit a_s der kleinste, mit b_s der größte der n Moduln

$$M(\eta_s'),\ M(\eta_s'') \ldots M(\eta_s^{(n)}) \tag{14}$$

bezeichnet wird, die zunächst folgenden Moduln

$$M(\eta_{s+1}'),\ M(\eta_{s+1}'') \ldots M(\eta_{s+1}^{(n)})$$

stets $< a_s$ oder $> b_s$ ausfallen, je nachdem sie zu der ersten oder zweiten Klasse gehören; da hieraus $a_{s+1} < a_s$ und $b_{s+1} > b_s$ folgt, so leuchtet ein, daß bei einer so gebildeten Kette (13) die einem beliebigen Gliede η_s entsprechenden Moduln (14), je nachdem sie zu der ersten oder zweiten Klasse gehören, kleiner bzw. größer sind als alle Moduln aller vorausgehenden Glieder $\eta_1, \eta_2, \ldots, \eta_{s-1}$. Da ferner die Normen aller dieser Zahlen η ganze rationale Zahlen und absolut kleiner als die endliche Konstante $(3\,c)^n$ sind, so müssen unendlich viele solche Zahlen η eine und dieselbe, von Null verschiedene Norm m haben; da (nach § 176, II bis IV) zugleich m durch η teilbar, also $\mathfrak{o}\,m > \mathfrak{o}\,\eta > \mathfrak{o}$, und $(\mathfrak{o}, \mathfrak{o}\,m) = \pm m^n > 0$ ist, so ist (nach § 171, II) die Anzahl dieser Moduln $\mathfrak{o}\,\eta$ endlich, und folglich muß es in der Kette (13) auch unendlich viele solche Zahlen η geben, welche einen und denselben Modul $\mathfrak{o}\,\eta$ erzeugen; sind $\varkappa, \lambda$ irgend zwei solche Zahlen, von denen $\varkappa$ den früheren, λ den späteren Platz in der Kette (13) einnimmt, und setzt man $\varkappa = \lambda\,\varepsilon$, so folgt aus $\mathfrak{o}\,\varkappa = \mathfrak{o}\,\lambda$ auch $\mathfrak{o}\,\varepsilon = \mathfrak{o}$; mithin ist ε eine Einheit, und da zugleich $\varkappa^{(r)} = \lambda^{(r)}\varepsilon^{(r)}$, also auch $M(\varkappa^{(r)}) = M(\lambda^{(r)})\,M(\varepsilon^{(r)})$ ist, so ergibt sich mit Rücksicht

auf die obige Bemerkung über die konjugierten Moduln der in der Kette (13) enthaltenen Zahlen der folgende Satz:

III. Es gibt in $\mathfrak{o}$ eine Einheit von der Art, daß die Moduln der mit ihr konjugierten Zahlen in der ersten Klasse > 1, in der zweiten Klasse < 1 ausfallen.

6. Von jetzt ab wollen wir, wenn unter den Permutationen π_r imaginäre Paare vorhanden sind, von jedem solchen Paar nur die eine beibehalten, die andere gänzlich fallen lassen; es bleiben dann ν Permutationen

$$\pi_1, \pi_2, \ldots, \pi_\nu, \tag{15}$$

und je nachdem eine solche Permutation π_s reell oder imaginär ist, wollen wir

$$c_s = 1 \quad \text{oder} \quad c_s = 2 \tag{16}$$

setzen, so daß

$$c_1 + c_2 + \cdots + c_\nu = n \tag{17}$$

wird. Bedeutet ferner α irgendeine von Null verschiedene Zahl des Körpers Ω, so soll, wenn π_s eine der Permutationen (15) ist, mit $l_s(\alpha)$ der reelle Bestandteil von $c_s \log \alpha^{(s)}$ bezeichnet werden, woraus offenbar

$$l_1(\alpha) + l_2(\alpha) + \cdots + l_\nu(\alpha) = \log N((\alpha)) \tag{18}$$

folgt, wo $N((\alpha))$ den absoluten Wert von $N(\alpha)$ bedeutet; zugleich ist allgemein

$$l_s(\alpha\beta) = l_s(\alpha) + l_s(\beta). \tag{19}$$

Für jede Einheit ε ergibt sich aus (18) speziell

$$l_1(\varepsilon) + l_2(\varepsilon) + \cdots + l_\nu(\varepsilon) = 0, \tag{20}$$

und der obige Satz III kann offenbar so ausgesprochen werden:

IV. Verteilt man die ν Permutationen (15) nach Belieben in zwei Klassen, doch so, daß jede von ihnen mindestens eine Permutation enthält, so gibt es in $\mathfrak{o}$ immer eine Einheit ε von der Art, daß $l_s(\varepsilon)$ positiv oder negativ ausfällt, je nachdem π_s zu der ersten oder zweiten Klasse gehört.

Betrachtet man jetzt ein System S von $(\nu - 1)$ Einheiten $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\nu-1}$ und setzt zur Abkürzung $l_s(\varepsilon_m) = l_{s,m}$, während $u_1, u_2, \ldots, u_\nu$ willkürliche Größen bedeuten, so ist die Determinante

$$\begin{vmatrix} l_{1,1}, \ldots, l_{1,\nu-1}, u_1 \\ \cdots\cdots\cdots\cdots \\ l_{\nu,1}, \ldots, l_{\nu,\nu-1}, u_\nu \end{vmatrix} = (u_1 + \cdots + u_\nu) S', \tag{21}$$

wo

$$S' = \Sigma \pm l_{1,1}\, l_{2,2} \ldots l_{\nu-1,\,\nu-1}; \tag{22}$$

denn wenn man zu der letzten Zeile alle vorhergehenden addiert, so verschwinden zufolge (20) alle ihre Elemente mit Ausnahme des letzten, welches gleich der Summe der Größen u_s wird. Die Determinante S' oder auch deren absoluter Wert, welcher durch das System S vollständig bestimmt ist, soll der Regulator dieses Systems heißen*). Fügt man zu S noch eine Einheit ε_ν hinzu und setzt $u_s = l_s(\varepsilon_\nu)$, so verschwindet zufolge (20) die aus ν Einheiten gebildete Determinante (21). Von der größten Wichtigkeit ist aber der folgende Satz:

V. Es gibt ein aus $(\nu - 1)$ Einheiten $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\nu-1}$ bestehendes System S, dessen Regulator von Null verschieden ist.

In der Tat, da $\nu \geqq 2$ ist, so folgt aus dem obigen Satze IV, wenn man π_1 in die erste, alle anderen Permutationen aber in die zweite Klasse aufnimmt, die Existenz einer Einheit ε_1, für welche $l_{1,1}$ positiv ausfällt, womit der Fall $\nu = 2$ erledigt ist. Wenn aber $\nu > 2$ ist, und m eine natürliche Zahl bedeutet, die $< \nu$, aber > 1 ist, so wollen wir annehmen, man habe schon $(m - 1)$ Einheiten ε_1, $\varepsilon_2, \ldots, \varepsilon_{m-1}$ gefunden, die eine positive Determinante

$$D_m = \Sigma \pm l_{1,1}\, l_{2,2} \ldots l_{m-1,\,m-1}$$

erzeugen, und wir wollen mit Hilfe desselben Satzes IV die Existenz einer Einheit ε_m beweisen, für welche auch die Determinante

$$E_{m+1} = \Sigma \pm l_{1,1}\, l_{2,2} \ldots l_{m-1,\,m-1}\, l_{m,m}$$

positiv ausfällt. Hierzu ordnen wir die letztere nach den aus ε_m entspringenden Elementen, wodurch sie die Form

$$E_{m+1} = D_1 l_{1,m} + \cdots + D_{m-1} l_{m-1,\,m} + D_m l_{m,m}$$

annimmt, wo D_m nach unserer Annahme positiv ist, während die übrigen aus $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{m-1}$ gebildeten Determinanten $D_1, D_2, \ldots, D_{m-1}$ positiv, negativ oder auch $= 0$ sein können. Bildet man nun wieder zwei Klassen und nimmt von den m Permutationen $\pi_1, \pi_2, \ldots, \pi_m$ alle diejenigen in die erste Klasse auf, denen positive Werte $D_1, D_2,$

*) Dieser Ausdruck findet sich in verwandter, freilich etwas anderer Bedeutung in § 4 der Abhandlung von Eisenstein: Allgemeine Untersuchungen über die Formen dritten Grades mit drei Variabeln, welche der Kreisteilung ihre Entstehung verdanken (Crelles Journal, Bd. 28, 29).

..., D_m entsprechen, also jedenfalls die Permutation π_m, während die übrigen und die Permutationen $\pi_{m+1}, \ldots, \pi_\nu$, also jedenfalls π_ν, in die zweite Klasse fallen, so gibt es nach dem obigen Satze IV eine Einheit ε_m, für welche $l_{s,m}$ positiv oder negativ ausfällt, je nachdem π_s zu der ersten oder zweiten Klasse gehört; mithin wird die Summe E_{m+1}, da sie mindestens ein positives Glied $D_m l_{m,m}$ und kein einziges negatives Glied enthält, gewiß positiv, was zu zeigen war. Auf diese Weise kann man offenbar von $m = 2$ bis $m = \nu - 1$ fortschließen, wodurch man zuletzt ein System S von $\nu - 1$ Einheiten erhält, dessen Regulator S' von Null verschieden ist, w. z. b. w.

7. Ein solches, aus $\nu - 1$ unabhängigen Einheiten $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\nu-1}$ bestehendes System S, dessen Regulator S' von Null verschieden ist, nennen wir ein vollständiges System, und wir bilden aus dieser Basis S, indem wir die Exponenten $m_1, m_2, \ldots, m_{\nu-1}$ alle ganzen rationalen Zahlen von $-\infty$ bis $+\infty$ durchlaufen lassen, eine zugehörige Gruppe (S) von unendlich vielen Einheiten

$$\sigma = \varepsilon_1^{m_1} \varepsilon_2^{m_2} \ldots \varepsilon_{\nu-1}^{m_{\nu-1}}, \tag{23}$$

welche sich durch Multiplikation und Division reproduzieren*); daß je zwei verschiedenen Systemen von Exponenten $m_1, m_2, \ldots, m_{\nu-1}$ auch zwei verschiedene Einheiten σ entsprechen, daß also nur dann $\sigma = 1$ wird, wenn alle diese Exponenten verschwinden, wird sich aus dem Folgenden beiläufig ergeben.

Ist α irgendeine von Null verschiedene Zahl des Körpers Ω, so bezeichnen wir mit $\alpha(S)$ den Komplex aller Produkte $\alpha\sigma$, welche den sämtlichen Einheiten σ der Gruppe (S) entsprechen, und es leuchtet ein, daß zwei solche Komplexe $\alpha(S)$, $\beta(S)$ entweder keine einzige gemeinsame Zahl besitzen oder vollständig identisch sind; jede in $\alpha(S)$ enthaltene Zahl kann an Stelle von α treten und als Repräsentant dieses Komplexes angesehen werden. Um nun von allen diesen Zahlen $\alpha\sigma$ eine einzige durch besondere Bedingungen herauszuheben, verfahren wir auf folgende Weise (vgl. § 87). Da die Determinante (21), wenn man die Größen u_s durch die in (16), (17) eingeführten Zahlen c_s ersetzt, den von Null verschiedenen Wert

*) Die jetzt folgenden Betrachtungen bieten eine vollständige und auf leicht ersichtlichen Gründen beruhende Analogie mit der Theorie der endlichen Moduln dar (§ 172).

$n S'$ annimmt, so entspricht jeder von Null verschiedenen Zahl α des Körpers Ω ein vollständig bestimmtes System von ν reellen Größen $e_1(\alpha)$, $e_2(\alpha)$, ..., $e_{\nu-1}(\alpha)$ und $f(\alpha)$, welche den ν linearen Gleichungen

$$\begin{aligned} &l_{1,1}e_1(\alpha) + \cdots + l_{1,\nu-1}e_{\nu-1}(\alpha) + c_1 f(\alpha) = l_1(\alpha) \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &l_{\nu,1}e_1(\alpha) + \cdots + l_{\nu,\nu-1}e_{\nu-1}(\alpha) + c_\nu f(\alpha) = l_\nu(\alpha) \end{aligned} \tag{24}$$

genügen und zufolge (19) die Eigenschaften

$$e_s(\alpha\beta) = e_s(\alpha) + e_s(\beta),\ f(\alpha\beta) = f(\alpha) + f(\beta) \tag{25}$$

besitzen. Die $(\nu - 1)$ Größen $e_s(\alpha)$ wollen wir die Exponenten der Zahl α in bezug auf die Basis S nennen, und α soll eine in bezug auf S reduzierte Zahl heißen, wenn ihre Exponenten sämtlich < 1 und nicht negativ sind. Die Bedeutung der Größe $f(\alpha)$ ergibt sich unmittelbar durch Addition der Gleichungen (24), woraus mit Rücksicht auf (17), (18), (20)

$$n f(\alpha) = \log N((\alpha)) \tag{26}$$

folgt; ist ε irgendeine Einheit, so ist $f(\varepsilon) = 0$. Da ferner zufolge (19) und (23)

$$l_s(\sigma) = l_{s,1}m_1 + l_{s,2}m_2 + \cdots + l_{s,\nu-1}m_{\nu-1}$$

und außerdem $f(\sigma) = 0$ ist, so lehrt die Vergleichung mit (24), daß die in (23) dargestellte Einheit σ der Gruppe (S) die ganzen rationalen Exponenten

$$e_s(\sigma) = m_s \tag{27}$$

besitzt; hieraus folgt zugleich, daß σ wirklich nur auf eine einzige Weise in der Form (23) darstellbar ist, und daß die einzige in (S) enthaltene reduzierte Einheit $= 1$ ist, weil ihre Exponenten m_s sämtlich verschwinden müssen. Betrachtet man nun irgendeine in dem Komplex $\alpha(S)$ enthaltene Zahl $\alpha\sigma$, so sind zufolge (25) und (27) ihre Exponenten $e_s(\alpha\sigma) = e_s(\alpha) + m_s$, und da die ganzen rationalen Zahlen m_s immer und nur auf eine einzige Weise so gewählt werden können, daß die Exponenten $e_s(\alpha\sigma) < 1$ und nicht negativ werden, so ergibt sich der Satz:

VI. In jedem Komplex $\alpha(S)$ gibt es eine und auch nur eine einzige reduzierte Zahl.

Die wichtigste Grundlage für alles Folgende ergibt sich aber aus den Gleichungen (24), wenn man alle diejenigen reduzierten

Zahlen α betrachtet, deren absolute Norm einen gegebenen positiven Wert t nicht überschreitet; da nämlich die $\nu - 1$ Exponenten $e_s(\alpha)$ zwischen 0 und 1 liegen, und zufolge (26) im algebraischen Sinne $nf(\alpha) \leqq \log t$ ist, so sind die ν Größen $l_s(\alpha)$ algebraisch kleiner als eine endliche, nur von t und der Basis S abhängige Größe, und folglich sind auch die Moduln aller mit einer solchen Zahl α konjugierten Zahlen kleiner als eine endliche positive Größe C, welche ebenfalls nur von t und S abhängt. Fügt man jetzt noch die Bedingung hinzu, daß α eine ganze Zahl sein soll, so ergibt sich hieraus mit Rücksicht auf I. der Satz:

VII. Ist t eine gegebene positive Größe, so gibt es nur eine endliche Anzahl solcher ganzen Zahlen, welche in bezug auf S reduziert, und deren absolute Normen $\leqq t$ sind.

Mithin ist auch die Anzahl aller reduzierten Einheiten ϱ endlich, und das System aller Einheiten ε des Körpers besteht (zufolge VI) aus ebenso vielen verschiedenen Komplexen von der Form $\varrho(S)$. Hieraus folgt leicht der Satz:

VIII. Bedeutet r die Anzahl aller in bezug auf S reduzierten Einheiten ϱ, und ε irgendeine Einheit, so ist ε^r in der Gruppe (S) enthalten.

Denn wenn $\varrho_1, \varrho_2, \ldots, \varrho_r$ die r reduzierten Einheiten sind, so kann man die Einheiten

$$\varepsilon\varrho_1 = \eta_1\sigma_1, \quad \varepsilon\varrho_2 = \eta_2\sigma_2, \quad \ldots, \quad \varepsilon\varrho_r = \eta_r\sigma_r \tag{28}$$

setzen, wo $\sigma_1, \sigma_2, \ldots, \sigma_r$ der Gruppe (S) angehören, während $\eta_1, \eta_2, \ldots, \eta_r$ reduzierte Einheiten sind; wäre nun z. B. $\eta_1 = \eta_2$, also auch $\varrho_1\sigma_2 = \varrho_2\sigma_1$, so gehörten die beiden verschiedenen Einheiten ϱ_1, ϱ_2 einem und demselben Komplex $\varrho_1(S) = \varrho_2(S)$ an, was (nach VI) unmöglich ist; mithin sind die r reduzierten Einheiten η sämtlich voneinander verschieden, und sie fallen daher in ihrer Gesamtheit, wenn auch in anderer Ordnung, mit den r Einheiten ϱ zusammen; multipliziert man nun die obigen r Gleichungen (28) und dividiert durch das Produkt der reduzierten Einheiten ϱ oder η, so ergibt sich $\varepsilon^r = \sigma_1\sigma_2 \ldots \sigma_r$, w. z. b. w.

8. Die Exponenten von ε^r sind daher zufolge (27) immer ganze rationale Zahlen, und da zufolge (25) diese Exponenten $e_s(\varepsilon^r) = r\,e_s(\varepsilon)$ sind, so ergibt sich, daß die Exponenten $e_s(\varepsilon)$ einer jeden Einheit ε rationale Zahlen mit dem gemeinsamen Nenner r sind. Ist nun

K irgendein System von $\nu - 1$ Einheiten $\varkappa$, und setzt man dieselben in (24) für α ein, so ergibt sich, weil $f(\varkappa) = 0$ ist, aus der Definition (22) der Regulator

$$K' = k S', \tag{29}$$

wo k die aus den Exponenten der Einheiten $\varkappa$ gebildete Determinante, also eine rationale Zahl mit dem Nenner $r^{\nu-1}$ bedeutet; mithin ist K dann und nur dann ein vollständiges System, wenn k, also auch die ganze Zahl $k r^{\nu-1}$ von Null verschieden ist. Hieraus folgt zugleich, daß es unter allen vollständigen Systemen auch ein sogenanntes Fundamentalsystem, d. h. ein System von absolut kleinstem Regulator geben muß, und wir wollen jetzt annehmen, unser obiges System S sei selbst ein solches Fundamentalsystem. Dann folgt zunächst, daß die Exponenten einer jeden reduzierten Einheit ϱ sämtlich verschwinden; denn ersetzt man eine der in S enthaltenen Einheiten, z. B. ε_s durch ϱ, während man die übrigen beibehält, so entsteht aus S ein System K, welches zufolge (29) den Regulator $K' = e_s(\varrho) S'$ besitzt; wäre nun der Exponent $e_s(\varrho)$ von Null verschieden und folglich ein positiver echter Bruch, so wäre K ein vollständiges System, und sein Regulator K' absolut kleiner als S', was unmöglich ist; mithin ist $e_s(\varrho) = 0$. Aus dieser Eigenschaft, welche, wie man leicht zeigen könnte, für jedes Fundamentalsystem S auch charakteristisch ist, folgt zunächst, daß die Exponenten einer jeden Einheit ε, weil sie in einem Komplexe ϱ (S) enthalten ist, sämtlich ganze rationale Zahlen sind. Ferner folgt hieraus, daß jedes Produkt aus zwei reduzierten Einheiten ϱ, weil seine Exponenten zufolge (25) sämtlich verschwinden, ebenfalls eine reduzierte Einheit ist; behält daher r die obige Bedeutung, so ist ϱ^r eine reduzierte Einheit, welche (nach VIII) der Gruppe (S) angehört, und hieraus folgt nach einer früheren Bemerkung

$$\varrho^r = 1. \tag{30}$$

Da umgekehrt jede in $\mathfrak{o}$ enthaltene Einheitswurzel $\varepsilon = \sqrt[m]{1}$ immer eine reduzierte Einheit ist, weil die Größen $l_s(\varepsilon)$ und $e_s(\varepsilon)$ sämtlich verschwinden, so fallen die r reduzierten Einheiten ϱ mit allen in $\mathfrak{o}$ enthaltenen Einheitswurzeln zusammen; unter diesen befinden sich immer die beiden Zahlen ± 1, und hieraus folgt offenbar, daß r stets eine gerade Zahl ist, die aber, wie man leicht erkennt, nur dann > 2 sein kann, wenn $n = 2\nu$ ist. Da endlich das System aller

Einheiten ε aus den r Komplexen $\varrho(S)$ besteht, so haben wir hiermit den folgenden großen Satz von Dirichlet*) bewiesen:

IX. Bezeichnet v die Gesamtanzahl der reellen, sowie der Paare von imaginären Permutationen des Körpers Ω, so gibt es in $\mathfrak{o}$ immer $v-1$ Fundamentaleinheiten von solcher Beschaffenheit, daß, wenn man dieselben beliebig oft ineinander multipliziert und dividiert und dem so gebildeten allgemeinen Produkt die sämtlichen in $\mathfrak{o}$ enthaltenen Einheitswurzeln ϱ, deren Anzahl r stets endlich ist, einzeln als Faktor zugesellt, alle Einheiten in $\mathfrak{o}$ und zwar jede nur einmal dargestellt werden.

Wir fügen diesem Resultate noch einige Bemerkungen hinzu. Es leuchtet ein, daß allen Fundamentalsystemen S nicht bloß derselbe absolute Minimal-Regulator S', sondern auch dieselbe Anzahl r der reduzierten Einheiten entspricht; bei den meisten Untersuchungen tritt der aus beiden gebildete Quotient

$$E = \frac{S'}{r} \tag{31}$$

auf**), und diese Größe besitzt für den Körper Ω eine Bedeutung von ähnlicher Wichtigkeit wie seine Grundzahl D. Durch Betrachtungen, welche den in der Theorie der endlichen Moduln angewendeten analog sind (§ 172), kann man leicht beweisen, daß dieser Quotient auch denselben Wert E besitzt, wenn S ein beliebiges vollständiges System, und r die Anzahl der in bezug auf S reduzierten Einheiten bedeutet; dasselbe wird sich aber auch beiläufig aus der im folgenden Paragraphen enthaltenen Untersuchung ergeben.

Ganz ähnliche Resultate erhält man, wenn man nicht alle Einheiten betrachtet, sondern nur diejenigen, deren Norm positiv***) ist, oder gar nur diejenigen, welche durch alle reellen Permutationen in positive Werte übergehen; man kann dieselbe Untersuchung ent-

*) Monatsbericht der Berliner Akademie vom 30. März 1846, oder Dirichlets Werke, Bd. 1, S. 642.

**) Im Falle $v = 1$ ist $S' = 1$, und r gleich der Anzahl aller Einheiten in $\mathfrak{o}$ zu setzen.

***) Vgl. die dritte Auflage S. 561; bei dem dortigen Ausspruche des Schlußsatzes (S. 567) hätte aber ausdrücklich bemerkt werden sollen, daß im Falle eines ungeraden n von den beiden einzigen reduzierten Einheiten $+1$ und -1 nur die erstere beizubehalten ist.

weder von vornherein mit Rücksicht auf solche Nebenbedingungen führen, oder man kann auch nachträglich die etwaigen Modifikationen des obigen Resultats leicht ableiten, wenn man bedenkt, daß jedes Quadrat einer Einheit diesen Bedingungen genügt.

Die obige Untersuchung ist ferner so dargestellt, daß sie auch dann gültig bleibt, wenn das Gebiet o aller in Ω enthaltenen ganzen Zahlen überall durch irgendeine endliche Ordnung n ersetzt wird, deren Basis zugleich eine Basis von Ω ist*); aber auch für diesen Fall kann man die eintretenden Modifikationen leicht nachträglich ableiten, wenn man den Führer der Ordnung, d. h. das Ideal $\mathfrak{f} = \mathfrak{n} : \mathfrak{o}$ betrachtet und bedenkt, daß jede Einheit durch Potenzierung mit dem Exponenten $\varphi(\mathfrak{f})$ in eine Einheit dieser Ordnung verwandelt wird (§ 180, IV).

§ 184.

Der eben bewiesene Satz bildet neben der Theorie der Ideale die wichtigste Grundlage für das tiefere Studium der ganzen Zahlen des Körpers Ω, und er ist unentbehrlich für die wirkliche Bestimmung der Anzahl der Idealklassen nach Dirichlets Prinzipien. Die vollständige und allgemeine Lösung dieser großen Aufgabe, von welcher die Bestimmung der Klassenanzahl der binären quadratischen Formen nur den einfachsten Fall bildet, scheint nach dem heutigen Stande der Wissenschaft noch in weiter Ferne zu liegen, allein mit Hilfe des genannten Satzes gelingt es doch, einen wesentlichen Teil derselben allgemein zu erledigen und die Klassenanzahl als Grenzwert einer unendlichen Reihe darzustellen. Da die entsprechenden Sätze über die quadratischen Formen (§§ 95, 96, 98) hierdurch abermals in ein helleres Licht gesetzt werden, so wollen wir diese Untersuchung im folgenden ausführen; hierbei kommt es vorzüglich darauf an, den folgenden Hauptsatz zu beweisen, in welchem die Bezeichnungen des vorigen Paragraphen beibehalten sind:

I. Ist $\mathfrak{m}$ ein gegebenes Ideal, und bezeichnet man, wenn t ein beliebiger positiver Wert ist, mit T die zugehörige Anzahl aller derjenigen verschiedenen, durch $\mathfrak{m}$ teilbaren

*) Vgl. die zweite Auflage (§ 166) und meine auf S. 146 zitierte Festschrift: Über die Anzahl der Ideal-Klassen in den verschiedenen Ordnungen eines endlichen Körpers (1877).

Hauptideale, deren Normen nicht größer als t sind, so wird für unendlich große Werte von t

$$\lim \frac{T}{t} = \frac{2^r \pi^{n-r} E}{N(\mathfrak{m}) \sqrt{(D)}}. \tag{1}$$

Wir bemerken zunächst, daß wir hier den Begriff des Hauptideals in seiner ursprünglichen Bedeutung nehmen (§ 177), also unter einem Hauptideal jeden Modul von der Form $\mathfrak{o}\alpha$ verstehen, wo α jede von Null verschiedene Zahl in $\mathfrak{o}$ bedeutet, mag ihre Norm positiv oder negativ sein. Um unseren Satz zu beweisen, wählen wir nach Belieben eine bestimmte Basis des Ideals

$$\mathfrak{m} = [\mu_1, \mu_2, \ldots, \mu_n], \tag{2}$$

ebenso irgendein vollständiges System S von $\nu - 1$ Einheiten

$$\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\nu-1}, \tag{3}$$

und behalten für dasselbe alle im vorigen Paragraphen benutzten Bezeichnungen bei. Wir erhalten nun gewiß alle durch $\mathfrak{m}$ teilbaren Hauptideale $\mathfrak{m}'$, deren Normen den Wert t nicht überschreiten, wenn wir $\mathfrak{m}' = \mathfrak{o}\alpha$ und

$$\alpha = a_1 \mu_1 + a_2 \mu_2 + \cdots + a_n \mu_n \tag{4}$$

setzen, wo die n Koordinaten $a_1, a_2, \ldots, a_n$ alle diejenigen ganzen rationalen Zahlen durchlaufen, welche der Bedingung

$$0 < N((\alpha)) \leqq t \tag{5}$$

genügen. Auf diese Weise würde aber (abgesehen von dem Falle $\nu = 1$) jedes solche Ideal $\mathfrak{m}'$ durch unendlich viele verschiedene Zahlen $\alpha = \varepsilon \alpha_0$ (und nur durch diese) erzeugt werden, wo α_0 eine bestimmte solche Zahl ist, ε aber alle Einheiten durchläuft. Bedeutet nun r wieder die Anzahl der in bezug auf S reduzierten Einheiten ϱ, so besteht das System aller dieser Zahlen α aus r verschiedenen Komplexen $\varrho\alpha_0 (S)$, und da es in jedem solchen Komplex eine und nur eine reduzierte Zahl α gibt, so wird, wenn wir zu (4) und (5) noch die $\nu - 1$ Bedingungen

$$0 \leqq e_s(\alpha) < 1 \tag{6}$$

hinzufügen, jedes Ideal $\mathfrak{m}'$ genau r-mal erzeugt werden; mithin ist die Anzahl aller derjenigen Zahlen α, welche diesen Bedingungen (4), (5), (6) genügen, $= rT$, wo T die im Satze angegebene Bedeutung hat.

Hierauf wenden wir uns zur Betrachtung des stetigen, n-fach ausgedehnten arithmetischen Raumes $\mathfrak{R}$; unter einem Punkte desselben verstehen wir jede Folge x von n reellen Werten $x_1, x_2, \ldots, x_n$, welche umgekehrt die Koordinaten des Punktes x heißen sollen*). Aus diesem unendlichen Raume $\mathfrak{R}$ wollen wir durch gewisse Bedingungen, welche den obigen nachgebildet sind, ein durch endliche Grenzen eingeschlossenes Gebiet $\mathfrak{A}$ ausscheiden. Zunächst bilden wir die allen n Permutationen entsprechenden Funktionen

$$\begin{aligned} \xi' &= x_1 \mu_1' + x_2 \mu_2' + \cdots + x_n \mu_n' \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ \xi^{(n)} &= x_1 \mu_1^{(n)} + x_2 \mu_2^{(n)} + \cdots + x_n \mu_n^{(n)} \end{aligned} \tag{7}$$

und unterwerfen den Punkt x, indem wir mit u den absoluten Wert des reellen Produktes

$$\xi' \xi'' \ldots \xi^{(n)} = \pm u \tag{8}$$

bezeichnen, der ersten Bedingung

$$0 < u \leqq 1. \tag{9}$$

Ist ferner π_s eine der ν Permutationen (15) in § 183, so bezeichnen wir mit y_s den reellen Teil von $c_s \log \xi^{(s)}$ und bestimmen aus $y_1, y_2, \ldots, y_\nu$ abermals ν reelle Größen $z_1, z_2, \ldots, z_{\nu-1}$ und v durch die ν linearen Gleichungen

$$\begin{aligned} l_{1,1} z_1 + \cdots + l_{1,\nu-1} z_{\nu-1} + c_1 v &= y_1 \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ l_{\nu,1} z_1 + \cdots + l_{\nu,\nu-1} z_{\nu-1} + c_\nu v &= y_\nu, \end{aligned} \tag{10}$$

aus welchen durch Addition offenbar

$$n v = y_1 + y_2 + \cdots + y_\nu = \log u \tag{11}$$

folgt. Hiernach verstehen wir unter dem Gebiete $\mathfrak{A}$ den Inbegriff aller derjenigen Punkte x, welche der Bedingung (9) und außerdem den $\nu - 1$ Bedingungen

$$0 \leqq z_s < 1 \tag{12}$$

genügen; mit Rücksicht auf (10) und (11) folgt hieraus, daß die ν Größen y_s algebraisch kleiner, also die Moduln der n Größen $\xi^{(s)}$ absolut kleiner als eine nur von S abhängige Konstante sind, und aus (7) ergibt sich weiter, daß auch die Koordinaten x_s aller in $\mathfrak{A}$ gelegenen

*) Nach der Ausdrucksweise meiner in § 161 zitierten Schrift ist jeder Punkt x eine bestimmte Abbildung des Systems Z_n der ersten n natürlichen Zahlen im Körper aller reellen Zahlen, und der Raum $\mathfrak{R}$ ist der Inbegriff aller dieser Abbildungen x.

Punkte x absolut kleiner sind, als eine Konstante, welche teils von S, teils von der obigen Basis des Ideals $\mathfrak{m}$ abhängt.

Zwischen diesem Gebiete $\mathfrak{A}$ und den vorher betrachteten Größen t und T besteht nun folgende Beziehung. Setzen wir zur Abkürzung die positive Größe

$$t^{-\frac{1}{n}} = \delta, \tag{13}$$

so erzeugt jede Zahl α, welche den Bedingungen (4), (5), (6) genügt, einen Punkt x, dessen Koordinaten

$$x_1 = \delta a_1, \quad x_2 = \delta a_2, \quad \ldots, \quad x_n = \delta a_n \tag{14}$$

aus den ganzen Koordinaten $a_1, a_2, \ldots, a_n$ der Zahl α durch Multiplikation mit δ entstehen, also dem Modul $[\delta]$ angehören; da nun zufolge (7), (8), (10), (11) gleichzeitig mit (14) auch

$$\begin{aligned} &\xi^{(s)} = \delta\, \alpha^{(s)}, \qquad y_s = c_s \log \delta + l_s(\alpha), \\ &u = \delta^n N((\alpha)), \quad v = \log \delta + f(\alpha), \quad z_s = e_s(\alpha) \end{aligned} \tag{15}$$

wird, so folgt aus (5) und (6) auch (9) und (12), mithin liegt der Punkt x im Gebiete $\mathfrak{A}$; und umgekehrt leuchtet ein, daß jeder Punkt x des Gebietes $\mathfrak{A}$, dessen Koordinaten in $[\delta]$ enthalten sind, auf diese Weise (14) durch eine und nur eine solche Zahl α erzeugt wird, welche den Bedingungen (4), (5), (6) genügt. Mithin ist die Anzahl $r\,T$ dieser Zahlen α zugleich die Anzahl T' dieser Punkte x.

Um nun hieraus den gesuchten Grenzwert abzuleiten, berufen wir uns auf das folgende allgemeine Prinzip*), welches seinen unmittelbaren Grund in dem Begriffe eines vielfachen Integrals findet und deshalb keines besonderen Beweises bedarf:

Setzt man das über ein reelles, in endliche Grenzen eingeschlossenes Gebiet $\mathfrak{A}$ ausgedehnte, aus lauter positiven Elementen gebildete n-fache Integral

$$\int \partial x_1\, \partial x_2 \ldots \partial x_n = (\mathfrak{A}), \tag{16}$$

und bezeichnet man, wenn δ eine beliebig kleine positive Größe ist, mit T' die zugehörige Anzahl aller derjenigen verschiedenen in $\mathfrak{A}$ liegenden Punkte x, deren Koordinaten $x_1, x_2, \ldots, x_n$ ganze rationale Vielfache von δ sind, so wird für unendlich kleine Werte von δ

$$\lim (T'\, \delta^n) = (\mathfrak{A}). \tag{17}$$

*) Für den Fall $n = 2$ fällt dasselbe mit dem in § 120 besprochenen geometrischen Satze zusammen.

Da in unserem Falle $T' = r\,T$ und $\delta^n = t^{-1}$ ist, so erhalten wir

$$\lim\left(\frac{T}{t}\right) = \frac{(\mathfrak{A})}{r}, \tag{18}$$

und es kommt nur noch darauf an, den Wert des Integrals $(\mathfrak{A})$ zu ermitteln. Zu diesem Zweck führen wir an Stelle der Koordinaten $x_1, x_2, \ldots, x_n$ ein neues System von n unabhängigen reellen Variablen ein, und zwar erwählen wir als solche die schon oben definierten ν Größen $u, z_1, z_2, \ldots, z_{\nu-1}$ und außerdem noch $(n - \nu)$ Größen $\varphi_{\nu+1}, \varphi_{\nu+2}, \ldots, \varphi_n$, welche dadurch vollständig bestimmt sind, daß sie, mit i multipliziert, die imaginären Bestandteile der Logarithmen von $\xi^{(\nu+1)}, \xi^{(\nu+2)}, \ldots, \xi^{(n)}$ bilden und zugleich den Bedingungen

$$0 \leqq \varphi_m < 2\pi \tag{19}$$

genügen, wo m jede der Zahlen $\nu + 1, \nu + 2, \ldots, n$ bedeutet.

Zu jedem Punkte x des Gebietes $\mathfrak{A}$ gehört offenbar ein einziges, den Bedingungen (9), (12), (19) genügendes System der neuen Variablen u, z_s, φ_m. Umgekehrt leuchtet ein, daß durch ein solches Wertsystem u, z_s, φ_m die unter den n Größen $\xi', \xi'', \ldots, \xi^{(n)}$ befindlichen imaginären Paare vollständig bestimmt sind, während für die übrigen $\xi^{(s)}$, welche den $(2\nu - n)$ reellen Permutationen π_s entsprechen, nur die absoluten Werte gegeben werden. Aus diesem Grunde zerfällt unser Gebiet $\mathfrak{A}$ offenbar in $2^{2\nu-n}$ Stücke $\mathfrak{B}$, deren jedes aus allen denjenigen Punkten x besteht, für welche jede der letztgenannten Größen $\xi^{(s)}$ ein unveränderliches Vorzeichen besitzt; betrachtet man daher ein bestimmtes solches Stück $\mathfrak{B}$, so entspricht zufolge (7) jedem Wertsystem u, z_s, φ_m ein und nur ein bestimmter Punkt x in $\mathfrak{B}$. Das Integral $(\mathfrak{A})$ ist die Summe aller, den einzelnen Stücken $\mathfrak{B}$ entsprechenden Integrale $(\mathfrak{B})$, und um für ein bestimmtes solches Stück $\mathfrak{B}$ die Transformation des Integrals $(\mathfrak{B})$ auszuführen, müssen wir bekanntlich den absoluten Wert der mit

$$\frac{d(x_1, \ldots, x_{\nu-1}, x_\nu, x_{\nu+1}, \ldots, x_n)}{d(z_1, \ldots, z_{\nu-1}, u, \varphi_{\nu+1}, \ldots, \varphi_n)}$$

zu bezeichnenden Funktional-Determinante der alten Variablen in bezug auf die neuen bestimmen. Dies führen wir nach bekannten Sätzen so aus, daß wir bei dem Übergange von jenen zu diesen noch andere Systeme von Variablen, und zwar zunächst das der n Größen $\xi', \xi'', \ldots, \xi^{(n)}$ einschalten; da zufolge (7) das Quadrat der Funktional-

Determinante der Größen ξ in bezug auf die Größen x die Diskriminante des Ideals $\mathfrak{m}$, also $= \Delta(\mathfrak{m}) = DN(\mathfrak{m})^2$ ist, so folgt

$$\frac{d(x_1, \ldots, x_n)}{d(\xi', \ldots, \xi^{(n)})} = \frac{1}{N(\mathfrak{m})\sqrt{D}}.$$

Hierauf führen wir die ν Größen y_s und die $(n - \nu)$ Größen φ_m ein; ist π_s eine reelle Permutation, so ist $y_s = \log(\pm \xi^{(s)})$, wo $\pm$ das in diesem Stück $\mathfrak{B}$ herrschende Vorzeichen von $\xi^{(s)}$ bedeutet, mithin

$$d\xi^{(s)} = \xi^{(s)} dy_s;$$

bilden aber π_s und π_m ein imaginäres Paar, so ist

$$\log \xi^{(s)} = {}^1/_2 y_s - \varphi_m i, \quad \log \xi^{(m)} = {}^1/_2 y_s + \varphi_m i,$$

also

$$\frac{d(\xi^{(s)}, \xi^{(m)})}{d(y_s, \varphi_m)} = i\,\xi^{(s)}\xi^{(m)},$$

und hieraus folgt mit Rücksicht auf (8)

$$\frac{d(\xi', \ldots, \xi^{(\nu)}, \xi^{(\nu+1)}, \ldots, \xi^{(n)})}{d(y_1, \ldots, y_\nu, \varphi_{\nu+1}, \ldots, \varphi_n)} = \pm u\, i^{n-\nu}.$$

Führt man endlich statt der Größen y_s die Größen z_s und u ein, so folgt aus (10) und (11) mit Rücksicht auf die Gleichungen (17) und (21) des vorigen Paragraphen

$$\frac{d(y_1, \ldots, y_{\nu-1}, y_\nu)}{d(z_1, \ldots, z_{\nu-1}, u)} = \frac{S'}{u}.$$

Durch Verbindung dieser Übergänge erhält man

$$\frac{d(x_1, \ldots, x_{\nu-1}, x_\nu, x_{\nu+1}, \ldots, x_n)}{d(z_1, \ldots, z_{\nu-1}, u, \varphi_{\nu+1}, \ldots, \varphi_n)} = \frac{S'}{N(\mathfrak{m})\sqrt{(D)}},$$

mithin

$$(\mathfrak{B}) = \frac{S'}{N(\mathfrak{m})\sqrt{(D)}} \int \partial z_1 \ldots \partial z_{\nu-1} \partial u \, \partial \varphi_{\nu+1} \ldots \partial \varphi_n,$$

oder wenn man die Integrationen in den durch (9), (12), (19) angegebenen Grenzen ausführt,

$$(\mathfrak{B}) = \frac{(2\pi)^{n-\nu} S'}{N(\mathfrak{m})\sqrt{(D)}},$$

wo der Regulator S' und $\sqrt{(D)}$ absolut zu nehmen sind. Da jedem der $2^{2\nu-n}$ Stücke $\mathfrak{B}$, aus welchen $\mathfrak{A}$ besteht, ein und derselbe Integralwert $(\mathfrak{B})$ entspricht, so folgt

$$(\mathfrak{A}) = \frac{2^\nu \pi^{n-\nu} S'}{N(\mathfrak{m})\sqrt{(D)}},$$

und zufolge (18) ergibt sich hieraus der gesuchte Grenzwert

$$\lim\left(\frac{T}{t}\right) = \frac{2^{r}\pi^{n-r}}{N(\mathfrak{m})\sqrt{(D)}} \cdot \frac{S'}{r}.$$

Da dieser Grenzwert seiner Bedeutung nach von der Auswahl des bei unserem Beweise benutzten vollständigen Einheits-Systems S gänzlich unabhängig ist, so ergibt sich beiläufig der auch auf elementare Weise leicht zu beweisende Satz, daß der Quotient $S' : r$ für alle vollständigen Systeme S einen und denselben absoluten Wert hat; bezeichnet man denselben mit E, so nimmt die letzte Gleichung die Form (1) an, w. z. b. w.

Mit Hilfe dieses Fundamentes lassen sich die nachfolgenden Sätze ohne jede Schwierigkeit ableiten; wir bemerken vorher, daß wir den Begriff der Idealklasse (§ 181) im ursprünglichen Sinne nehmen, also zwei Ideale $\mathfrak{a}$, $\mathfrak{a}'$ äquivalent nennen und derselben Klasse zuteilen, wenn es eine Zahl η (von positiver oder negativer Norm) gibt, welche der Bedingung $\mathfrak{a}\eta = \mathfrak{a}'$ genügt. Dann gilt folgender Satz:

II. Ist A irgendeine Idealklasse, und bezeichnet man, wenn t ein beliebiger positiver Wert ist, mit T die Anzahl aller derjenigen in A enthaltenen Ideale, deren Normen nicht größer als t sind, so wird für unendlich große Werte von t

$$\lim\frac{T}{t} = \frac{2^{r}\pi^{n-r}E}{\sqrt{(D)}} = g. \tag{20}$$

Um dies zu beweisen, wählen wir aus der inversen Klasse A^{-1} nach Belieben ein bestimmtes Ideal $\mathfrak{m}$; ist nun $\mathfrak{a}$ ein beliebiges Ideal in A, so ist $\mathfrak{a}\mathfrak{m}$ ein durch $\mathfrak{m}$ teilbares Hauptideal $\mathfrak{m}'$, und umgekehrt ist jedes solches Hauptideal $\mathfrak{m}'$ von der Form $\mathfrak{a}\mathfrak{m}$, wo $\mathfrak{a}$ der Klasse A angehört; da ferner je zwei verschiedenen Idealen $\mathfrak{a}$ auch zwei verschiedene Ideale $\mathfrak{a}\mathfrak{m}$ entsprechen und umgekehrt, so folgt aus $N(\mathfrak{a}\mathfrak{m}) = N(\mathfrak{a})N(\mathfrak{m})$, daß T zugleich die Anzahl aller derjenigen verschiedenen, durch $\mathfrak{m}$ teilbaren Hauptideale $\mathfrak{a}\mathfrak{m}$ ist, deren Normen nicht größer als $tN(\mathfrak{m})$ sind; ersetzt man daher t in dem Satze I durch $tN(\mathfrak{m})$, so geht die Gleichung (1) in (20) über, w. z. b. w.

Da dieser Grenzwert von der Klasse A gänzlich unabhängig ist, und da jedes Ideal einer und nur einer Klasse angehört, so folgt hieraus ohne weiteres der nachstehende Satz:

III. Bedeutet h die Anzahl aller Idealklassen, und bezeichnet man, wenn t ein beliebiger positiver Wert ist, mit T die Anzahl aller derjenigen verschiedenen Ideale, deren Normen nicht größer als t sind, so wird für unendlich große Werte von t

$$\lim \frac{T}{t} = \frac{2^r \pi^{n-r} E h}{\sqrt{(D)}} = gh. \tag{21}$$

Verbindet man hiermit das allgemeine, in § 118 aufgestellte Prinzip, so ergibt sich folgendes:

IV. Bedeutet s eine Variable, und setzt man die über alle Ideale $\mathfrak{a}$ ausgedehnte unendliche Reihe

$$\sum \frac{1}{N(\mathfrak{a})^s} = \Omega(s), \tag{22}$$

so konvergiert dieselbe für alle Werte $s > 1$, und für unendlich kleine Werte von $(s-1)$ wird

$$\lim (s-1)\Omega(s) = gh. \tag{23}$$

Hiermit ist, wenn die Werte von D und E schon gefunden sind, die Klassenanzahl h als Grenzwert einer unendlichen Reihe dargestellt. Gelingt es, denselben Grenzwert noch auf eine andere Weise, nämlich unmittelbar aus der Beschaffenheit der im Körper Ω auftretenden Ideale $\mathfrak{a}$ zu bestimmen, so ist damit auch die Klassenanzahl h gefunden; dies ist aber bis jetzt nur in sehr wenigen Fällen geglückt, von denen wir einige in den folgenden Paragraphen betrachten wollen, und vermutlich befinden wir uns noch sehr weit von einer allgemeinen Lösung dieses großen Problems. Hier wollen wir nur noch die folgenden Bemerkungen hinzufügen.

Aus den Gesetzen, nach welchen alle Ideale $\mathfrak{a}$ aus den sämtlichen Primidealen $\mathfrak{p}$ durch Multiplikation gebildet werden (§ 179), ergibt sich als unmittelbare Folgerung die Identität

$$\Sigma \psi(\mathfrak{a}) = \prod \frac{1}{1 - \psi(\mathfrak{p})}, \tag{24}$$

wenn die Funktion ψ die Eigenschaft

$$\psi(\mathfrak{a}\mathfrak{b}) = \psi(\mathfrak{a})\psi(\mathfrak{b}) \tag{25}$$

besitzt, und wenn außerdem die Summe linker Hand einen von der Anordnung ihrer Glieder unabhängigen endlichen Wert besitzt; der Beweis für diese Identität zwischen der Summe und dem unendlichen

Produkte stimmt vollständig mit demjenigen überein, welchen wir früher (§ 132) für den speziellen Fall $n = 1$ gegeben haben, und kann deshalb hier unterdrückt werden. Für unsere, in (22) definierte Funktion $\Omega(s)$ ergibt sich hieraus die folgende zweite Darstellung

$$\Omega(s) = \prod \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}}; \tag{26}$$

bedeuten nun, wenn p eine beliebige natürliche Primzahl ist, $\mathfrak{p}_1$, $\mathfrak{p}_2, \ldots, \mathfrak{p}_e$ die voneinander verschiedenen, in p aufgehenden Primideale, und $n_1, n_2, \ldots, n_e$ deren Grade (§ 180), so nimmt diese Gleichung die folgende Gestalt an

$$\Omega(s) = \prod \left(\frac{1}{1 - p^{-sn_1}} \cdot \frac{1}{1 - p^{-sn_2}} \cdots \frac{1}{1 - p^{-sn_e}} \right), \tag{27}$$

wo das Produkt über alle Primzahlen p zu erstrecken ist. Bezeichnet man ferner, wenn m eine beliebige natürliche Zahl ist, mit $F(m)$ die Anzahl aller derjenigen verschiedenen Ideale, deren Norm $= m$ ist, so ist offenbar

$$\Omega(s) = \sum \frac{F(m)}{m^s}, \tag{28}$$

und man erkennt leicht, daß für je zwei relative Primzahlen m', m'' stets

$$F(m'm'') = F(m')F(m'') \tag{29}$$

ist, während die unendliche Reihe

$$1 + \frac{F(p)}{p^s} + \frac{F(p^2)}{p^{2s}} + \frac{F(p^3)}{p^{3s}} + \cdots \tag{30}$$

mit dem allgemeinen Faktor des Produktes (27) übereinstimmt. Außerdem geht aus (21) hervor, daß für unendlich große Werte von m

$$\lim \frac{F(1) + F(2) + \cdots + F(m)}{m} = gh \tag{31}$$

ist.

Tiefere Untersuchungen, zu denen z. B. die über die Geschlechter der quadratischen Formen (Supplement IV) und die über die Verteilung der Primideale auf die verschiedenen Idealklassen gehören *),

*) Vgl. die schon in § 137 zitierte Abhandlung von Dirichlet (Crelles Journal, Bd. 21, S. 98).

knüpfen sich an die Betrachtung allgemeinerer Reihen und Produkte, welche aus (24) hervorgehen, wenn man

$$\psi(\mathfrak{a}) = \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s}$$

setzt, wo die Funktion $\chi(\mathfrak{a})$ außer der Eigenschaft (25) noch die andere besitzt, für alle derselben Klasse A angehörenden Ideale $\mathfrak{a}$ denselben Wert anzunehmen, welcher mithin zweckmäßig durch $\chi(A)$ bezeichnet wird und offenbar immer eine h^{te} Wurzel der Einheit ist. Solche Funktionen χ, die man im erweiterten Sinne Charaktere nennen kann, existieren immer, und zwar geht aus den am Schlusse des § 149 erwähnten Sätzen leicht hervor, daß die Klassenanzahl h zugleich die Anzahl aller verschiedenen Charaktere $\chi_1, \chi_2, \ldots, \chi_h$ ist, und daß jede Klasse A durch die ihr entsprechenden h Werte $\chi_1(A)$, $\chi_2(A), \ldots, \chi_h(A)$ vollständig charakterisiert, d. h. von allen anderen Klassen unterschieden wird. Setzt man noch die über alle Ideale $\mathfrak{a}$ der Klasse A ausgedehnte Summe

$$\sum \frac{1}{N(\mathfrak{a})^s} = A(s),$$

und bezeichnet mit $A_1, A_2, \ldots, A_h$ alle verschiedenen Klassen, so nimmt für den Charakter χ die Gleichung (24) die Form

$$\chi(A_1) A_1(s) + \cdots + \chi(A_h) A_h(s) = \prod \frac{1}{1 - \chi(\mathfrak{p}) N(\mathfrak{p})^{-s}}$$

an; auf die Folgerungen, welche sich aus der Betrachtung dieser h Ausdrücke und deren Logarithmen ergeben, können wir aber hier nicht mehr eingehen.

§ 185.

Um den Nutzen und die Bedeutung unserer bisherigen Untersuchungen erkennen zu lassen, deren Resultate nur die ersten Elemente einer allgemeinen Zahlentheorie bilden, wollen wir dieselben auf zwei bestimmte Beispiele anwenden, die zugleich in unmittelbarem Zusammenhange mit dem Hauptgegenstande dieses Werkes stehen. Als erstes Beispiel wählen wir den klassischen Fall der Kreisteilung, an welchem Kummer zuerst seine Schöpfung der idealen Zahlen mit dem schönsten Erfolge durchgeführt hat *).

*) Die bezüglichen, zuerst in Crelles Journal (Bd. 35, 40) veröffentlichten Untersuchungen sind zusammengestellt in der Abhandlung: Sur la théorie des nombres complexes composés de racines de l'unité et de nombres

Es sei m eine natürliche ungerade Primzahl, θ eine primitive Wurzel der Gleichung

$$\theta^m = 1, \tag{1}$$

und n der Grad des Körpers Ω, der aus allen durch θ rational darstellbaren Zahlen besteht. Setzen wir (nach § 139)

$$f(t) = \frac{t^m - 1}{t - 1} = (t - \theta)(t - \theta^2) \dots (t - \theta^{m-1}), \tag{2}$$

wo t eine Variable bedeutet, so ist $f(\theta) = 0$, und da die Koeffizienten dieser Gleichung rational sind, so ist $n \leqq m - 1$. Um n genau zu bestimmen, setzen wir $t = 1$, wodurch wir

$$m = (1 - \theta)(1 - \theta^2) \dots (1 - \theta^{m-1}) \tag{3}$$

erhalten; da θ eine ganze Zahl ist, so gilt dasselbe von den $(m - 1)$ Faktoren $1 - \theta^r$, und man erkennt leicht, daß dieselben miteinander assoziiert sind; denn wählt man die positive ganze Zahl s so, daß $rs \equiv 1 \pmod{m}$, also $1 - \theta = 1 - \theta^{rs}$ wird, so ist gleichzeitig

$$\frac{1 - \theta^r}{1 - \theta} = 1 + \theta + \theta^2 + \dots + \theta^{r-1}$$

und

$$\frac{1 - \theta}{1 - \theta^r} = 1 + \theta^r + \theta^{2r} + \dots + \theta^{(s-1)r};$$

mithin ist jede der beiden Zahlen $1 - \theta$ und $1 - \theta^r$ durch die andere teilbar. Setzt man daher

$$1 - \theta = \mu, \tag{4}$$

so geht die Gleichung (3) in

$$m = \varepsilon \mu^{m-1} \tag{5}$$

über, wo ε eine Einheit bedeutet, woraus zugleich hervorgeht, daß μ keine Einheit, und folglich jede durch μ teilbare rationale Zahl auch durch die Primzahl m teilbar ist. Da alle mit Ω konjugierten Körper zufolge (2) imaginär, und folglich alle Normen positiv sind, so folgt hieraus

$$m^n = N(\mu)^{m-1},$$

---

entiers (Liouvilles Journal, Bd. 16, 1851), und eine Ergänzung derselben findet sich in der Abhandlung: Über die den Gaußischen Perioden der Kreisteilung entsprechenden Kongruenzwurzeln (Crelles Journal, Bd. 53). — Vgl. Bachmann: Die Lehre von der Kreisteilung (Vorl. 17, 18) und meine Anzeige dieses Werkes in Schlömilchs Zeitschrift für Math. u. Phys., Jahrgang 18 (1873), Literaturzeitung S. 14 bis 24, 43.

mithin ist die natürliche Zahl $N(\mu)$ selbst eine Potenz der Primzahl m; setzt man nun $N(\mu) = m^a$, so folgt $n = a\,(m-1)$, und da, wie oben bemerkt, $n \leqq m-1$ ist, so ergibt sich $a = 1$, mithin

$$n = m-1,\ N(\mu) = m. \tag{6}$$

Die in (2) definierte Funktion $f(t)$ ist daher irreduzibel*), also bilden die $m-1$ Potenzen $1, \theta, \theta^2, \ldots, \theta^{m-2}$ eine Basis des Körpers Ω, und wir wollen jetzt zeigen, daß

$$\mathfrak{o} = [1, \theta, \ldots, \theta^{m-2}] = [1, \mu, \ldots, \mu^{m-2}] \tag{7}$$

ist, wo $\mathfrak{o}$ wieder das System aller ganzen Zahlen des Körpers Ω bedeutet. Zunächst leuchtet aus (4) ein, daß die Potenzen von θ und diejenigen der Zahl μ jedenfalls Basen eines und desselben ganzen Moduls bilden, den wir vorläufig mit $\mathfrak{a}$ bezeichnen wollen; um seine Diskriminante $\Delta(\mathfrak{a})$ zu bestimmen, multiplizieren wir (2) mit $t-1$, differentiieren nach t und setzen $t = \theta$, $f'(\theta) = \theta^*$, wodurch wir $(\theta-1)\,\theta^* = m\theta^{m-1}$ erhalten; da $N(\theta-1) = m$, und θ zufolge (1) eine Einheit ist, so ergibt sich $N(\theta^*) = m^{m-2}$ und hieraus [nach § 167, (27)]

$$\Delta(\mathfrak{a}) = (-1)^{\frac{m-1}{2}}\, m^{m-2}. \tag{8}$$

Sodann bemerken wir, daß jede durch m teilbare Zahl des Moduls $\mathfrak{a}$ auch in $m\mathfrak{a}$ enthalten ist; denn wenn die in $\mathfrak{a}$ enthaltene Zahl

$$a_0 + a_1\mu + a_2\mu^2 + \cdots + a_{m-2}\mu^{m-2}$$

durch m, also durch $\mu, \mu^2, \ldots, \mu^{m-1}$ teilbar sein soll, so ergibt sich schrittweise, daß die ganzen rationalen Zahlen $a_0, a_1, a_2, \ldots, a_{m-2}$ durch μ, also auch durch m teilbar sein müssen. Hieraus folgt unmittelbar, daß der kleinste natürliche Faktor k, durch welchen irgendeine ganze Zahl ω in eine Zahl $k\omega$ des Moduls $\mathfrak{a}$ verwandelt wird, nicht durch m teilbar sein kann; denn wäre $k = mh$, so wäre die in $\mathfrak{a}$ enthaltene Zahl $k\omega = mh\omega$ zugleich teilbar durch m, also in $m\mathfrak{a}$ enthalten, mithin wäre das Produkt $h\omega$ in $\mathfrak{a}$ enthalten, was der Bedeutung von k widerspricht, weil $h < k$ wäre. Da nun andererseits k^2 (nach dem Satze I in § 175) in der Diskriminante $\Delta(\mathfrak{a})$ aufgehen muß, so folgt aus (8), daß stets $k = 1$, also jede ganze Zahl ω in $\mathfrak{a}$ enthalten, mithin $\mathfrak{o} = \mathfrak{a}$ ist, w. z. b. w. Zugleich ergibt sich aus (8) die Grundzahl

$$D = \Delta(\mathfrak{o}) = (-1)^{\frac{m-1}{2}}\, m^{m-2}. \tag{9}$$

*) Gauß: D. A. art. 341.

Aus (6) folgt ferner, daß μ eine Primzahl, $\mathfrak{o}\mu$ ein Primideal ersten Grades ist; bedeutet nämlich $\mathfrak{a}$ irgendein in μ aufgehendes Primideal, so ist $\mathfrak{o}\mu = \mathfrak{a}\mathfrak{b}$, also $N(\mathfrak{a})N(\mathfrak{b}) = N(\mu) = m$; da aber m eine natürliche Primzahl und $N(\mathfrak{a}) > 1$ ist, so muß $N(\mathfrak{a}) = m$, $N(\mathfrak{b}) = 1$, mithin $\mathfrak{b} = \mathfrak{o}$ und $\mathfrak{a} = \mathfrak{o}\mu$ sein, wie behauptet war. Zufolge (5) ist ferner

$$\mathfrak{o}m = (\mathfrak{o}\mu)^{m-1}, \tag{10}$$

und hiermit ist die Zerlegung von $\mathfrak{o}m$ in Primfaktoren gefunden.

Die mit θ konjugierten Zahlen sind zufolge (2) die $m-1$ Potenzen $\theta, \theta^2, \ldots, \theta^{m-1}$, d. h. alle primitiven Wurzeln der Gleichung (1); da dieselben ebenfalls dem Körper Ω angehören, so sind alle mit Ω konjugierten Körper identisch mit Ω, d. h. Ω ist ein Normalkörper (§ 166); seine Permutationen lassen sich miteinander zusammensetzen und bilden daher eine Gruppe; geht ferner θ durch die Permutationen ϱ, σ bzw. in θ^r, θ^s über, so geht θ sowohl durch $\varrho\sigma$ als auch durch $\sigma\varrho$ in θ^{rs} über, und folglich ist $\varrho\sigma = \sigma\varrho$; Normalkörper, deren Permutationen diese Eigenschaft besitzen, werden zweckmäßig Abelsche Körper genannt*). Um eine für das Folgende geeignete Bezeichnung dieser Permutationen zu gewinnen, wählen wir nach Belieben eine bestimmte primitive Wurzel c der Primzahl m als Basis eines Systems von Indizes (§ 30); ist r eine durch m nicht teilbare ganze rationale Zahl, so setzen wir der Kürze halber

$$\text{Ind.}\, r = r', \quad \text{also} \quad r \equiv c^{r'} \pmod{m} \tag{11}$$

und bezeichnen mit $\pi_{r'}$ diejenige Permutation, durch welche θ in θ^r übergeht; hierbei darf der Index r', den wir auch den Index dieser Permutation nennen, durch jede beliebige Zahl ersetzt werden, welche $\equiv r' \pmod{m-1}$ ist. Gleichzeitig soll die Zahl, in welche eine beliebige Zahl ω des Körpers durch $\pi_{r'}$ übergeht, durch $\omega_{r'}$ bezeichnet werden; bedeutet daher $\varphi(t)$ irgendeine ganze Funktion von t mit rationalen Koeffizienten, so ist gleichzeitig

$$\omega = \varphi(\theta) \text{ und } \omega_{r'} = \varphi(\theta^r); \tag{12}$$

*) Mémoire sur une classe particulière d'équations résolubles algébriquement (Œuvres complètes de Abel, t. 1, oder Crelles Journal, Bd. 4). Der wichtige Satz von Kronecker (Monatsber. der Berliner Akademie 1853), daß jeder Abelsche Körper auf rationale Weise aus Einheitswurzeln entsteht, ist vollständig bewiesen von H. Weber (Theorie der Abelschen Zahlkörper, Acta Mathematica, Bd. 8 und 9).

offenbar ist π_0 die identische Permutation, also $\omega_0 = \omega$, und der obige Satz über die Zusammensetzung der Permutationen wird durch $\pi_{r'}\,\pi_{s'} = \pi_{s'}\,\pi_{r'} = \pi_{(r\,s)'} = \pi_{r'+s'}$, also durch die Gleichung

$$(\omega_{r'})_{s'} = (\omega_{s'})_{r'} = \omega_{(r\,s)'} = \omega_{r'+s'} \tag{13}$$

ausgedrückt; zugleich leuchtet ein, daß alle Permutationen durch Wiederholung aus der einzigen Permutation $\pi_{c'} = \pi_1$ entstehen. Setzen wir ferner

$$n = m - 1 = 2\nu, \tag{14}$$

so ist

$$(-1)' \equiv \nu,\ (-r)' \equiv r' + \nu \pmod{2\nu}, \tag{15}$$

und es bilden je zwei Permutationen $\pi_{r'}$ und $\pi_{r'+\nu}$, durch welche θ in θ^r und θ^{-r} übergeht, ein imaginäres Paar (§ 183, 3).

Wir gehen jetzt zur Bestimmung aller von $\mathfrak{o}\,\mu$ verschiedenen Primideale $\mathfrak{p}$ über und bemerken zunächst, daß aus

$$\theta^r \equiv \theta^s \pmod{\mathfrak{p}} \text{ stets } r \equiv s \pmod{m}, \tag{16}$$

also $\theta^r = \theta^s$ folgt, weil sonst die Zahl $\theta^r - \theta^s = \theta^r(1 - \theta^{s-r})$ assoziiert mit μ und folglich nicht teilbar durch $\mathfrak{p}$ wäre; es sind daher die m Potenzen

$$1,\ \theta,\ \theta^2, \ldots, \theta^{m-1},$$

oder, was dasselbe sagt, die Zahlen

$$1,\ \theta_1,\ \theta_2, \ldots, \theta_{m-1}$$

sämtlich inkongruent nach $\mathfrak{p}$. Bezeichnen wir nun mit p die durch $\mathfrak{p}$ teilbare natürliche Primzahl (§ 179, VII), so ist p verschieden von m, weil m nur durch das einzige Primideal $\mathfrak{o}\,\mu$ teilbar ist; es sei ferner f der Exponent, zu welchem p nach dem Modul m gehört (§ 28), d. h. es sei f die kleinste natürliche Zahl, welche der Kongruenz

$$p^f \equiv 1 \pmod{m}, \tag{17}$$

also auch der Kongruenz

$$f p' \equiv 0 \pmod{2\nu} \tag{18}$$

genügt, so ist

$$2\nu = m - 1 = ef, \tag{19}$$

und e ist der größte gemeinschaftliche Teiler von p' und 2ν (§§ 29, 30).

Sind nun $\alpha, \beta, \gamma, \ldots$ beliebige ganze Zahlen, so folgt aus einer bekannten Eigenschaft der Binomialkoeffizienten (§ 20), daß immer

$$(\alpha + \beta + \gamma + \cdots)^p \equiv \alpha^p + \beta^p + \gamma^p + \cdots \pmod{p}$$

ist; bezeichnet man daher mit $\varphi(t)$ eine beliebige ganze Funktion der Variablen t mit ganzen rationalen Koeffizienten a und bedenkt, daß nach dem Fermatschen Satze (§ 19) immer $a^p \equiv a \pmod p$ ist, so erhält man den für jede ganze Zahl α gültigen Satz

$$\varphi(\alpha)^p \equiv \varphi(\alpha^p) \pmod p. \tag{20}$$

Wenden wir denselben auf den Fall $\alpha = \theta$ an, so ergibt sich mit Rücksicht auf (7) und (12), daß für jede in unserem Gebiete $\mathfrak{o}$ enthaltene Zahl ω die Kongruenz

$$\omega^p \equiv \omega_{p'} \pmod p \tag{21}$$

gilt, aus welcher durch fortgesetzte Erhebung zur p^{ten} Potenz nach (13) die allgemeinere Kongruenz

$$\omega^{p^r} \equiv \omega_{rp'} \pmod p \tag{22}$$

folgt; da nun fp' zufolge (18) durch 2ν teilbar, also $\omega_{fp'} = \omega$ ist, so erhält man das Resultat

$$\omega^{p^f} \equiv \omega \pmod p. \tag{23}$$

Hieraus schließen wir zunächst, daß $\mathfrak{o}\,p$ entweder ein Primideal oder ein Produkt von lauter verschiedenen Primidealen ist; nehmen wir nämlich im Gegenteil an, es sei p durch das Quadrat eines Primideals $\mathfrak{p}$ teilbar, so ist $\mathfrak{o}\,p = \mathfrak{p}^2\mathfrak{q}$, und da $\mathfrak{p}\mathfrak{q}$ ein echter Teiler von $\mathfrak{o}\,p$ ist, so gibt es eine Zahl ω, welche durch $\mathfrak{p}\mathfrak{q}$, aber nicht durch p teilbar ist; dann ist ω^2 und folglich auch ω^{p^f} teilbar durch $\mathfrak{p}^2\mathfrak{q}^2 = p\mathfrak{q}$, also auch durch p; allein dies widerspricht der Kongruenz (23), weil ω nicht durch p teilbar ist. Unsere Annahme ist daher unzulässig.

Da ferner $\mathfrak{p}$ in p aufgeht, so genügt jede ganze Zahl ω auch der Kongruenz

$$\omega^{p^f} \equiv \omega \pmod{\mathfrak{p}}, \tag{24}$$

d. h. die Anzahl der inkongruenten Wurzeln ω dieser Kongruenz vom Grade p^f ist $= (\mathfrak{o}, \mathfrak{p}) = N(\mathfrak{p})$, und folglich ist

$$N(\mathfrak{p}) \leq p^f, \tag{25}$$

weil in bezug auf ein Primideal eine Kongruenz r^{ten} Grades niemals mehr als r inkongruente Wurzeln haben kann (vgl. §§ 26, 180). Nach dem verallgemeinerten Fermatschen Satze (§ 180, V) ist ferner

$$\theta^{N(\mathfrak{p})} \equiv \theta \pmod{\mathfrak{p}},$$

woraus wir nach (16) folgern, daß

$$N(\mathfrak{p}) \equiv 1 \pmod m \tag{26}$$

ist. Nun wissen wir [nach § 180, (12)], daß $N(\mathfrak{p})$ eine Potenz von p mit positivem Exponenten ist, und da unter allen solchen Potenzen, welche durch m dividiert den Rest 1 lassen, p^f die kleinste ist, so muß $N(\mathfrak{p}) \geqq p^f$ sein, woraus mit Rücksicht auf (25) folgt, daß

$$N(\mathfrak{p}) = p^f \tag{27}$$

ist. Mithin ist der Exponent f, zu welchem die Primzahl p nach dem Modul m gehört, zugleich der Grad eines jeden in p aufgehenden Primideals $\mathfrak{p}$; da ferner

$$N(p) = p^{m-1} = p^{ef}$$

ist, so erhalten wir die Zerlegung

$$\mathfrak{o}\, p = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_e, \tag{28}$$

wo $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_e$ voneinander verschiedene Primideale vom Grade f bedeuten*).

Hiermit ist die Natur aller in unserem Körper Ω auftretenden Primideale erkannt, und dies Resultat reicht aus für die Bestimmung der Anzahl der Idealklassen; bevor wir aber zu dieser Untersuchung übergehen, wollen wir im Anschluß an § 180 noch einige Bemerkungen

---

*) Ist m eine beliebige natürliche Zahl, so hat der aus einer primitiven Wurzel θ der Gleichung (1) entspringende Körper Ω den Grad $\varphi(m)$; ist p eine Primzahl, p' die höchste in $m = p'm'$ aufgehende Potenz von p, und gehört p zum Exponenten f (mod m'), so ist $\varphi(m') = ef$ (§ 28), und

$$\mathfrak{o}\, p = (\mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_e)^{\varphi(p')},$$

wo $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_e$ voneinander verschiedene Primideale vom Grade f bedeuten; ist ferner $p' > 1$, so ist

$$\mathfrak{o}\,(1 - \theta^{m'}) = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_e.$$

Vgl. Kummer: Theorie der idealen Primfaktoren der komplexen Zahlen, welche aus den Wurzeln der Gleichung $\omega^n = 1$ gebildet sind, wenn n eine zusammengesetzte Zahl ist (Abh. d. Berliner Ak. 1856). — Für alle in einem solchen Körper Ω als Divisoren enthaltenen Körper, zu denen auch die quadratischen Körper gehören, habe ich die Bestimmung der Primideale als Resultat einer allgemeinen Untersuchung mitgeteilt, welche ich demnächst zu veröffentlichen gedenke (Sur la théorie des nombres entiers algébriques, § 27, und Compte rendu der Pariser Ak. vom 24. Mai 1880); über spezielle Fälle solcher Divisoren vgl. Eisenstein: Allgemeine Untersuchungen über die Formen dritten Grades mit drei Variabeln, welche der Kreisteilung ihre Entstehung verdanken (Crelles Journ., Bd. 28); Fuchs: Über die aus Einheitswurzeln gebildeten komplexen Zahlen von periodischem Verhalten, insbesondere die Bestimmung der Klassenanzahl derselben (Crelles Journ., Bd. 65); Bachmann: Die Theorie der komplexen Zahlen, welche aus zwei Quadratwurzeln zusammengesetzt sind (Berlin 1867).

über die Zerlegungen (10) und (28) hinzufügen, aus welchen sich die Zerlegung der Funktion (2) in rationale Primfunktionen nach den Moduln m und p ergibt.

Da die Zahl θ und alle ihre Potenzen $\equiv 1 \pmod{\mu}$ sind, und da jede auf μ bezügliche Kongruenz zwischen rationalen Zahlen auch für den Modul m gilt, so folgt aus (2) die ohnehin evidente identische Kongruenz

$$f(t) \equiv (t-1)^{m-1} \pmod{m}. \tag{29}$$

Für jede andere natürliche Primzahl p und deren Primfaktoren $\mathfrak{p}$ folgt zunächst aus (16), daß der Grad f von $\mathfrak{p}$ zugleich die Höhe jeder mit θ konjugierten Zahl θ_r ist, und daß folglich die f Zahlen $\theta_{r+p'}, \theta_{r+2p'}, \ldots, \theta_{r+fp'}$, deren Komplex mit dem der Zahlen $\theta_{r+e}, \theta_{r+2e}, \ldots, \theta_{r+fe}$ zusammenfällt, eine Periode in bezug auf $\mathfrak{p}$ bilden (S. 137). Setzt man daher

$$F_r(t) = F_{r+e}(t) = (t-\theta_{r+e})(t-\theta_{r+2e})\ldots(t-\theta_{r+fe}), \tag{30}$$

so wird

$$F_r(t) \equiv P_r(t) \pmod{\mathfrak{p}}, \tag{31}$$

wo $P_r(t)$ eine mit ganzen rationalen Koeffizienten behaftete Primfunktion in bezug auf den Modul p bedeutet. Zufolge (2) ist nun

$$f(t) = F_1(t)F_2(t)\ldots F_e(t), \tag{32}$$

und da jede auf $\mathfrak{p}$ bezügliche Kongruenz zwischen rationalen Zahlen auch für den Modul p gilt, so ergibt sich die identische Kongruenz*)

$$f(t) \equiv P_1(t)P_2(t)\ldots P_e(t) \pmod{p}; \tag{33}$$

zugleich folgt aus (16), daß diese e Primfunktionen wesentlich verschieden sind. Man findet auch leicht, daß $\mathfrak{p}$ der größte gemeinsame Teiler der durch die Zahlen p und $P_e(\theta)$ erzeugten Hauptideale ist.

Mit dieser Zerlegung hängt die folgende algebraische Betrachtung nahe zusammen. Die f Permutationen

$$\pi_e, \pi_{2e}, \ldots, \pi_{fe}, \tag{34}$$

deren Indizes durch e teilbar sind, und welche alle durch Wiederholung der einzigen Permutation π_e entstehen, bilden eine Gruppe (§ 166), und der zugehörige Körper H besteht aus allen denjenigen

*) Schönemann: Grundzüge einer allgemeinen Theorie der höheren Kongruenzen, deren Modul eine reelle Primzahl ist. § 50. (Crelles Journal, Bd. 31). — Gauß: Disquisitiones generales de congruentiis, artt. 360—367 (Werke, Bd. II, 1863).

in Ω enthaltenen Zahlen ω, welche der Bedingung $\omega_e = \omega$ genügen; zugleich ist $(H, R) = e$, $(\Omega, H) = f$. Die Darstellung aller dieser Zahlen ω ergibt sich sehr leicht, wenn man bedenkt, daß auch die n Potenzen $\theta, \theta^2, \ldots, \theta^{m-1}$, d. h. alle mit θ konjugierten Zahlen $\theta_1, \theta_2, \ldots, \theta_n$ eine Basis von Ω, ja auch eine Basis von $\mathfrak{o}$ bilden, weil θ eine Einheit, also $\mathfrak{o}\,\theta = \mathfrak{o}$ ist. Jede Zahl ω des Körpers Ω ist daher von der Form

$$\omega = x^{(1)}\theta_1 + x^{(2)}\theta_2 + \cdots + x^{(n)}\theta_n,$$

wo die Koordinaten $x^{(r)}$ willkürliche rationale Zahlen bedeuten, deren Zeiger r auch durch jede nach n kongruente Zahl ersetzt werden darf. Soll nun ω dem Körper H angehören, also der Bedingung $\omega_e = \omega$ genügen, so folgt $x^{(r)} = x^{(r+e)}$, also

$$\omega = x^{(1)}\eta_1 + x^{(2)}\eta_2 + \cdots + x^{(e)}\eta_e, \tag{35}$$

wo die e konjugierten Zahlen

$$\eta_r = \eta_{r+e} = \theta_{r+e} + \theta_{r+2e} + \cdots + \theta_{r+fe} \tag{36}$$

die sogenannten f-gliedrigen Perioden bedeuten*). Zugleich ergibt sich, daß der Modul

$$\mathfrak{e} = [\eta_1, \eta_2, \ldots, \eta_e] \tag{37}$$

der Inbegriff aller ganzen Zahlen des Körpers H ist, und hieraus folgt nach später zu erwähnenden Sätzen**), daß seine Grundzahl $\Delta(\mathfrak{e}) = \pm m^{e-1}$ ist, wo das untere Zeichen gilt, wenn f ungerade und $e \equiv 2 \pmod 4$ ist. Bedeutet y eine Variable, so ist

$$G(y) = (y - \eta_1)(y - \eta_2)\ldots(y - \eta_e) \tag{38}$$

eine irreduzible Funktion mit ganzen rationalen Koeffizienten, und die Koeffizienten der in (30) definierten e Funktionen

$$F_r(t) = t^f - \eta_r t^{f-1} + \cdots \tag{39}$$

sind ganze Zahlen des Körpers H, also in $\mathfrak{e}$ enthalten***).

Hieraus ergibt sich durch Vergleichung mit der Kongruenz (31), daß jede der e Perioden η_r und folglich jede in $\mathfrak{e}$ enthaltene Zahl in bezug auf $\mathfrak{p}$ einer rationalen Zahl kongruent ist; setzen wir die Primfunktion

$$P_r(t) \equiv t^f - \eta_r^0 t^{f-1} + \cdots \pmod p, \tag{40}$$

wo $\eta_r^0 = \eta_{r+e}^0$ rational, so wird

$$\eta_r \equiv \eta_r^0 \pmod{\mathfrak{p}}, \tag{41}$$

*) Gauß: D. A. artt. 343, 348.

**) Vgl. unten (59) und die Anmerkung auf S. 197.

***) Gauß: D. A. artt. 348, 351.

und da jede auf $\mathfrak{p}$ bezügliche Kongruenz zwischen rationalen Zahlen auch für den Modul p gilt, so ergibt sich aus (38) die identische Kongruenz

$$(42) \qquad G(y) \equiv (y - \eta_1^0)(y - \eta_2^0) \ldots (y - \eta_e^0) \pmod{p},$$

auf welche Kummer seine Theorie der idealen Zahlen gegründet hat.

Um endlich noch den inneren Zusammenhang zwischen den e verschiedenen, in p aufgehenden Primidealen $\mathfrak{p}$ zu ergründen, schalten wir folgende allgemeine Bemerkungen ein. Ist Ω ein beliebiger endlicher Körper, welcher durch die Permutation π in Ω' übergeht, und ist $\mathfrak{a}$ ein beliebiges Ideal in Ω, so geht aus den Begriffen des Körpers und des Ideals unmittelbar hervor, daß das System $\mathfrak{a}'$ aller Zahlen, in welche die sämtlichen Zahlen des Ideals $\mathfrak{a}$ durch π übergehen, ein Ideal in Ω' ist, und daß $\mathfrak{a}'$ durch die inverse Permutation in $\mathfrak{a}$ übergeht; zwei solche Ideale $\mathfrak{a}, \mathfrak{a}'$ nennen wir konjugierte Ideale. Dann leuchtet ferner ein, daß $(\mathfrak{a}\mathfrak{b})' = \mathfrak{a}'\mathfrak{b}'$ ist, daß folglich ein Primideal $\mathfrak{p}$ in ein Primideal $\mathfrak{p}'$ übergeht, und daß, wenn p die durch $\mathfrak{p}$ teilbare natürliche Primzahl bedeutet, p auch durch $\mathfrak{p}'$ teilbar ist. Wenden wir dies auf unseren Kreiskörper Ω an, der durch alle seine Permutationen π_s in sich selbst übergeht, so folgt, daß jedes der e Primideale $\mathfrak{p}$ durch eine solche Permutation π_s immer wieder in eins von diesen Idealen übergehen muß. Nun ergibt sich zunächst aus (21), daß jede durch $\mathfrak{p}$ teilbare Zahl ω durch die Permutation $\pi_{p'}$ in eine ebenfalls durch $\mathfrak{p}$ teilbare Zahl $\omega_{p'}$ übergeht; mithin geht $\mathfrak{p}$ durch $\pi_{p'}$, und folglich durch jede der f Permutationen (34) in ein Primideal über, welches durch $\mathfrak{p}$ teilbar, also auch mit $\mathfrak{p}$ identisch ist. Umgekehrt, wenn $\mathfrak{p}$ durch die Permutation π_s in sich selbst übergeht, so muß, weil $P_e(\theta)$ durch $\mathfrak{p}$ teilbar ist, auch $P_e(\theta_s) \equiv 0 \pmod{\mathfrak{p}}$ sein; da aber die Kongruenz $P_e(\alpha) \equiv 0 \pmod{\mathfrak{p}}$ nur die Wurzeln $\theta_e, \theta_{2e}, \ldots, \theta_{fe}$ hat, so muß eine von ihnen mit θ_s kongruent, also zufolge (16) auch mit θ_s identisch sein, woraus sich ergibt, daß die oben genannten f Permutationen die einzigen sind, durch welche $\mathfrak{p}$ in sich selbst übergeht. Sodann leuchtet ein, daß $\mathfrak{p}$ durch je f Permutationen, deren Indizes nach e kongruent sind, in ein und dasselbe Primideal übergeht; umgekehrt, wenn $\mathfrak{p}$ durch π_r und π_s in dasselbe Primideal übergeht, so geht $\mathfrak{p}$ durch $\pi_r \pi_s^{-1} = \pi_{r-s}$ offenbar in sich selbst über, und folglich ist $r \equiv s \pmod{e}$. Hieraus folgt, daß die e Ideale $\mathfrak{p}$ sämtlich miteinander konjugiert sind, und daß

jedes von ihnen in jedes durch f bestimmte Permutationen übergeht; durch die e Permutationen $\pi_1, \pi_2, \ldots, \pi_e$ geht jedes dieser Ideale in e verschiedene Ideale über, und wir werden daher am zweckmäßigsten mit $\mathfrak{p}_r$ dasjenige Ideal bezeichnen, in welches $\mathfrak{p}$ durch π_r übergeht; demgemäß ist $\mathfrak{p}_{r+e} = \mathfrak{p}_r$ zu setzen, und aus (31) und (41) folgen die Kongruenzen

$$F_{r+s}(t) \equiv P_r(t) \pmod{\mathfrak{p}_s} \tag{43}$$

$$\eta_{r+s} \equiv \eta_r^0 \pmod{\mathfrak{p}_s}. \tag{44}$$

Es wird gut sein, die vorstehenden Sätze an einem bestimmten Zahlenbeispiele*) zu bestätigen; wählen wir zu diesem Zweck $m = 13$, $p = 3$, so ist $f = 3$, $e = 4$. Legen wir ferner die primitive Wurzel $c = 2$ zugrunde, so wird

$$\theta_0 = \theta\ , \quad \theta_1 = \theta^2\ , \quad \theta_2 = \theta^4, \quad \theta_3 = \theta^8, \quad \theta_4 = \theta^3\ , \quad \theta_5 = \theta^6,$$
$$\theta_6 = \theta^{12}, \quad \theta_7 = \theta^{11}, \quad \theta_8 = \theta^9, \quad \theta_9 = \theta^5, \quad \theta_{10} = \theta^{10}, \quad \theta_{11} = \theta^7,$$

also

$$\eta = \theta + \theta^3 + \theta^9\ , \quad \eta_1 = \theta^2 + \theta^6 + \theta^5,$$
$$\eta_2 = \theta^4 + \theta^{12} + \theta^{10}, \quad \eta_3 = \theta^8 + \theta^{11} + \theta^7,$$

und

$$F_r(t) = t^3 - \eta_r t^2 + \eta_{r+2}\, t - 1.$$

Man findet ferner leicht die Gleichungen**)

$$\eta\,\eta = \eta_1 + 2\,\eta_2$$
$$\eta\,\eta_1 = \eta + \eta_1 + \eta_3 = -1 - \eta_2$$
$$\eta\,\eta_2 = -3\,\eta - 2\,\eta_1 - 3\,\eta_2 - 2\,\eta_3 = 3 + \eta_1 + \eta_3$$
$$\eta\,\eta_3 = \eta + \eta_2 + \eta_3 = -1 - \eta_1$$

und hieraus

$$G(y) = y^4 + y^3 + 2\,y^2 - 4\,y + 3.$$

Die Wurzeln der Kongruenz $G(y) \equiv 0 \pmod 3$ ergeben sich am kürzesten durch Versuche, und man findet auf diese Weise in Übereinstimmung mit (42) die identische Kongruenz

$$G(y) \equiv y\,(y-1)\,(y+1)^2 \pmod 3.$$

---

*) Ein überaus reiches Material findet man in dem Werke von Reuschle: Tafeln komplexer Primzahlen, welche aus Wurzeln der Einheit gebildet sind. 1875.

**) Gauß: D. A. art. 345.

Da eine der Wurzeln $\equiv 0 \pmod 3$ ist, so dürfen wir das in 3 aufgehende Primideal $\mathfrak{p}$ durch die Kongruenz $\eta \equiv 0 \pmod{\mathfrak{p}}$ definieren*), woraus durch Substitution in die vorstehenden Ausdrücke für η^2, $\eta\eta_1$, $\eta\eta_2$, $\eta\eta_3$ sich $\eta_1 \equiv -1$, $\eta_2 \equiv -1$, $\eta_3 \equiv 1 \pmod{\mathfrak{p}}$ ergibt; zufolge (41) wird daher

$$\eta_0^0 \equiv 0, \quad \eta_1^0 \equiv -1, \quad \eta_2^0 \equiv -1, \quad \eta_3^0 \equiv +1 \pmod 3.$$

Ersetzt man ferner die in $F_r(t)$ auftretenden Koeffizienten η_r, η_{r+2} bzw. durch die nach $\mathfrak{p}$ kongruenten rationalen Zahlen η_r^0, η_{r+2}^0, so folgt aus (31)

$$P_r(t) \equiv t^3 - \eta_r^0 t^2 + \eta_{r+2}^0 t - 1 \pmod 3,$$

und durch wirkliche Ausführung der Multiplikation bestätigt sich die Kongruenz (33). Setzt man endlich

$$\varrho = \theta^3 - \theta - 1 \equiv P_0(\theta) \pmod 3,$$

so ist $\mathfrak{p}$ der größte gemeinschaftliche Teiler von 3 und $\mathfrak{o}\varrho$; allein in unserem Falle erkennt man leicht (nach § 180), daß $\mathfrak{p} = \mathfrak{o}\eta$, also auch $\mathfrak{p}_r = \mathfrak{o}\eta_r$ ist, weil η durch $\mathfrak{p}$ teilbar und außerdem $\eta\eta_1\eta_2\eta_3 = 3$, mithin $N(\eta) = 3^3 = N(\mathfrak{p})$ ist. Es muß folglich ϱ durch η teilbar sein; in der Tat findet man

$$\varrho = \eta\theta^3(\theta+1)(\theta^4+1),$$

woraus sich sogar ergibt, daß zufällig ϱ mit η assoziiert, also auch $\mathfrak{o}\varrho = \mathfrak{p}$ ist. —

Nach dieser Abschweifung kehren wir zu unserem obigen, in den Gleichungen (6), (10), (27), (28) enthaltenen Hauptresultate zurück, welches ausreicht, um mit Hilfe der im vorigen Paragraphen entwickelten Prinzipien einen geschlossenen Ausdruck für die Anzahl h der Idealklassen zu gewinnen. Diese Untersuchung ist ebenfalls von Kummer zuerst durchgeführt**), und sie bietet die überraschendsten

*) Ebenso folgt aus der Annahme $\eta \equiv 1 \pmod{\mathfrak{p}}$ mit Bestimmtheit $\eta_1 \equiv 0$, $\eta_2 \equiv -1$, $\eta_3 \equiv -1 \pmod{\mathfrak{p}}$. Dagegen entsprechen der Annahme $\eta \equiv -1 \pmod{\mathfrak{p}}$ zwei verschiedene Systeme, wie aus $\eta_2\eta_3 = -1-\eta \equiv 0 \pmod{\mathfrak{p}}$ hervorgeht; entweder ist $\eta_1 \equiv 1$, $\eta_2 \equiv 0$, $\eta_3 \equiv -1$, oder es ist $\eta_1 \equiv -1$, $\eta_2 \equiv -1$, $\eta_3 \equiv 0 \pmod{\mathfrak{p}}$.

**) Daß auch Dirichlet dieselbe Aufgabe, aber in anderer Einkleidung gelöst hat, berichtet Kummer in seiner ausgezeichneten Gedächtnisrede auf Gustav Peter Lejeune-Dirichlet (1860, S. 21 bis 22) mit den Worten: „Für diejenigen zerlegbaren Formen höherer Grade, deren lineäre Faktoren keine anderen Irrationalitäten, als Einheitswurzeln für einen Primzahl-Exponenten, enthalten, hat Dirichlet während seines Aufenthalts in Italien die Klassenanzahl bestimmt, aber er hat von dieser Arbeit leider nichts veröffentlicht."

Beziehungen zu dem Satze über die arithmetische Progression dar (Supplement VI). Wir setzen, wie im vorigen Paragraphen,

$$\Omega(s) = \Sigma N(\mathfrak{a})^{-s} = \Pi(1 - N(\mathfrak{p})^{-s})^{-1} \tag{45}$$

und untersuchen das Verhalten dieser Funktion für unendlich kleine positive Werte der Variablen $s - 1$. Da m nur durch ein einziges Primideal ersten Grades, und jede andere Primzahl p, wenn sie zum Exponenten f gehört, durch e verschiedene Primideale vom Grade f teilbar ist, wo $ef = m - 1$, so erhalten wir

$$\Omega(s) = (1 - m^{-s})^{-1} \Pi(1 - p^{-sf})^{-e},$$

wo das Produkt auf alle von m verschiedenen Primzahlen p zu erstrecken ist. Der allgemeine Faktor dieses Produktes läßt sich in folgender Weise umformen. Bezeichnet man, wenn $m - 1$ wieder $= 2\nu$ gesetzt wird, mit α alle Wurzeln der Gleichung

$$\alpha^{2\nu} = 1, \tag{46}$$

ferner mit γ eine primitive Wurzel derselben Gleichung, so ist

$$\alpha = 1, \gamma, \gamma^2, \ldots, \gamma^{2\nu-1};$$

da nun der Index p' mit 2ν den größten gemeinschaftlichen Teiler e hat, so ist $\gamma^{p'}$ eine Wurzel δ der Gleichung $\delta^f = 1$, und zwar eine primitive; mithin tritt jede Wurzel δ dieser Gleichung unter den 2ν Zahlen

$$\alpha^{p'} = 1, \quad \gamma^{p'}, \quad \gamma^{2p'}, \ldots, \gamma^{(2\nu-1)p'}$$

genau $e$mal auf, und hieraus folgt unmittelbar, daß

$$(1 - p^{-sf})^e = \Pi(1 - \alpha^{p'} p^{-s})$$

ist, wo das Produktzeichen sich auf alle α bezieht. Man erhält daher

$$\Omega(s) = (1 - m^{-s})^{-1} \Pi(1 - \alpha^{p'} p^{-s})^{-1},$$

und dieses Produkt, in welchem α und p alle ihre Werte durchlaufen müssen, hat, solange $s > 1$ ist, einen von der Anordnung der Faktoren unabhängigen Wert. Bezeichnet man mit $L(\alpha)$ das Produkt aller derjenigen Faktoren, welche allen Werten von p, aber einem bestimmten Werte α entsprechen, so ist folglich

$$\Omega(s) = (1 - m^{-s})^{-1} \Pi L(\alpha), \tag{47}$$

wo das Produktzeichen sich auf alle α bezieht, und hierin ist nach früheren Sätzen (§§ 132, 133)

$$L(\alpha) = \Pi(1 - \alpha^{p'} p^{-s})^{-1} = \Sigma \alpha^{z'} z^{-s}, \tag{48}$$

wo z alle natürlichen Zahlen durchläuft, die nicht durch m teilbar sind, und wo z' wieder den Index von z bedeutet.

Wenn nun die Variable s abnehmend sich dem Grenzwerte 1 nähert, so wächst die Funktion $L(1)$ über alle Grenzen, und zwar so, daß

$$\lim (s-1)(1-m^{-s})^{-1} L(1) = 1 \tag{49}$$

wird (§ 117). Ist aber α verschieden von 1, also eine Wurzel der Gleichung

$$\frac{\alpha^{2\nu}-1}{\alpha-1} = 1+\alpha+\alpha^2+\cdots+\alpha^{2\nu-1} = 0, \tag{50}$$

so nähert sich, wie wir früher (§ 134) gesehen haben, die Funktion $L(\alpha)$ einem endlichen Grenzwert; da nämlich, wenn die Glieder der Reihe (48) nach wachsenden z geordnet werden, die Summe von je 2ν aufeinanderfolgenden Koeffizienten $\alpha^{z'}$ zufolge (50) verschwindet, so konvergiert (nach § 101) diese Reihe für alle positiven Werte von s, und sie ist zugleich eine stetige Funktion von s; setzt man daher bei dieser Anordnung der Glieder

$$L^0(\alpha) = \Sigma \alpha^{z'} z^{-1}, \tag{51}$$

so ist $L^0(\alpha)$ endlich und zugleich der Grenzwert von $L(\alpha)$. Bis zu diesem Punkte war es leicht, das Verhalten der Reihen $L(\alpha)$ an der Stelle $s = 1$ zu ergründen; bei dem Beweise des Satzes über die arithmetische Progression mußte aber außerdem gezeigt werden, daß der Grenzwert $L^0(\alpha)$ stets von Null verschieden ist, und dies verursachte damals erhebliche Schwierigkeiten. Es ist daher von hohem Interesse, daß dieselbe Tatsache jetzt als eine unmittelbare Folge unserer Untersuchung über die Anzahl h der Idealklassen erscheint *). In der Tat, da im vorigen Paragraphen allgemein gezeigt ist, daß

$$\lim (s-1)\,\Omega(s) = g\,h$$

ist, wo g einen bestimmten, von Null verschiedenen Wert bedeutet, so erhalten wir zufolge (47) und (49) für unseren Fall

$$g\,h = \Pi L^0(\alpha), \tag{52}$$

und da h immer eine positive ganze Zahl, niemals $= 0$ ist, so kann auch keiner der endlichen Faktoren $L^0(\alpha)$ verschwinden, w. z. b. w.

*) Genau dasselbe gilt auch, wenn die Differenz m der arithmetischen Progression eine zusammengesetzte Zahl ist.

Nachdem wir auf diesen Zusammenhang unserer Untersuchung mit dem Beweise des Satzes über die arithmetische Progression aufmerksam gemacht haben, wollen wir, was für den letzteren kein weiteres Interesse darbot, die Werte $L^0(\alpha)$ in geschlossener Form darstellen. Setzt man, wenn x eine Variable bedeutet, zur Abkürzung

$$(\alpha, x) = \Sigma \alpha^{r'} x^r, \tag{53}$$

wo r die Werte 1, 2, 3 ... $m-1$ durchlaufen soll, und verfährt man wie damals (§ 134 oder § 103), indem man in (51) die Größen z^{-1} durch bestimmte Integrale ersetzt und die mit (50) übereinstimmende Gleichung

$$(\alpha, 1) = 0 \tag{54}$$

berücksichtigt, so erhält man zunächst

$$L^0(\alpha) = \int_0^1 \frac{(\alpha, x)}{1 - x^m} \frac{dx}{x}. \tag{55}$$

Da nun

$$x^m - 1 = (x-1)\,\Pi(x - \theta_s)$$

ist, wo s ein vollständiges Restsystem nach dem Modul 2ν durchläuft, so ergibt sich mit Rücksicht auf (54) durch Zerlegung in Partialbrüche

$$\frac{(\alpha, x)}{x(1-x^m)} = -\frac{1}{m} \Sigma \frac{(\alpha, \theta_s)}{x - \theta_s}.$$

Hierin lassen sich die Zähler sämtlich auf (α, θ) zurückführen; da nämlich $\theta_s^r = \theta_{s+r'}$ ist, so folgt

$$(\alpha, \theta_s) = \Sigma \alpha^{r'} \theta_{s+r'},$$

wo r' ein beliebiges Restsystem nach dem Modul 2ν zu durchlaufen hat; man darf daher r' durch $r' - s$ ersetzen, und erhält so die in der Theorie der Kreisteilung wohlbekannte Relation

$$(\alpha, \theta_s) = \alpha^{-s} \Sigma \alpha^{r'} \theta_{r'} = \alpha^{-s} (\alpha, \theta). \tag{56}$$

Mithin ist

$$\frac{(\alpha, x)}{x(1-x^m)} = -\frac{(\alpha, \theta)}{m} \Sigma \frac{\alpha^{-s}}{x - \theta_s},$$

und hierdurch geht die Gleichung (55) in die folgende über

$$L^0(\alpha) = -\frac{(\alpha, \theta)}{m} \Sigma \alpha^{-s} \int_0^1 \frac{dx}{x - \theta_s};$$

es ist ferner

$$\int_0^1 \frac{dx}{x - \theta_s} = \log\left(\frac{1 - \theta_s}{-\theta_s}\right) = \log(1 - \theta_s^{-1}) = \log \mu_{s+\nu},$$

und dieser Logarithme ist (nach § 103, S. 262 [von Dirichlet-Dedekind]) dadurch vollständig bestimmt, daß sein imaginärer Bestandteil zwischen den Grenzen $\pm {}^1/_2 \pi i$ liegt. Setzen wir daher zur Abkürzung

$$\psi(\alpha) = -\Sigma \alpha^{-s} \log \mu_{s+\nu}, \tag{57}$$

wo s ein vollständiges Restsystem nach dem Modul 2ν durchläuft, so erhalten wir das Resultat

$$L^0(\alpha) = \frac{1}{m}(\alpha, \theta)\, \psi(\alpha). \tag{58}$$

Um nun, wie es die Gleichung (52) verlangt, das Produkt der Größen $L^0(\alpha)$ für alle Wurzeln α der Gleichung (50) zu bilden, beginnen wir mit dem Faktor (α, θ) und benutzen hierbei den Hilfssatz

$$(\alpha, \theta)(\alpha^{-1}, \theta) = m\alpha^{\nu} = \pm m; \tag{59}$$

derselbe ergibt sich leicht aus (56), wenn man mit θ_s multipliziert, s ein Restsystem nach dem Modul 2ν durchlaufen läßt und die Summe bildet; man erhält auf diese Weise zunächst

$$(\alpha, \theta)(\alpha^{-1}, \theta) = \Sigma(\alpha, \theta_s)\theta_s = \Sigma \alpha^u \theta_{s+u} \theta_s = \Sigma \alpha^u (\theta\, \theta_u)_s,$$

wo u ebenfalls ein solches Restsystem durchläuft; je nachdem nun u mit ν kongruent ist oder nicht, ist $\theta\, \theta_u = 1$ oder konjugiert mit θ, und folglich ist die nach s genommene Summe $\Sigma(\theta\, \theta_u)_s$ im ersten Falle $= 2\nu = m - 1$, in allen übrigen Fällen aber $= \Sigma \theta_s = -1$, woraus mit Rücksicht auf (50) der zu beweisende Satz (59) unmittelbar folgt. Für $\alpha = -1$ ergibt sich

$$(-1, \theta)^2 = m(-1)^{\nu},$$

also

$$(-1, \theta) = \Sigma(-1)^{r'} \theta^r = \Sigma\left(\frac{r}{m}\right)\theta^r = i^{\nu^2} \sqrt{m}, \tag{60}$$

und hierin ist (nach § 115) die Quadratwurzel positiv, wenn, was wir von jetzt ab festsetzen wollen,

$$\theta = e^{\frac{2\pi i}{m}} \tag{61}$$

genommen wird. Da nun die Wurzeln α der Gleichung (50) aus der Zahl -1 und $(\nu - 1)$ Paaren von der Form α, α^{-1} bestehen, so folgt aus (59) und (60) bei gehöriger Beachtung der Faktoren α^{ν} das Resultat

$$\Pi(\alpha, \theta) = i^{\nu} m^{\nu-1} \sqrt{m}. \tag{62}$$

Wir wenden uns jetzt zu der näheren Betrachtung des in (58) ferner auftretenden Faktors $\psi(\alpha)$, welcher einen wesentlich verschiedenen Charakter besitzt, je nachdem $\alpha^{\nu} = +1$ oder $= -1$ ist; wir behandeln zuerst den Fall

$$\alpha^{\nu} = -1. \tag{63}$$

Ersetzt man in (57) den Summations-Buchstaben s durch $s - \nu$ und nimmt das Mittel aus dem so entstehenden und dem ursprünglichen Ausdruck, so erhält man

$$\psi(\alpha) = \frac{1}{2} \Sigma \alpha^{-s} \log\left(\frac{\mu_s}{\mu_{s+\nu}}\right),$$

wo zufolge der obigen Bemerkung die Logarithmen so zu nehmen sind, daß ihr imaginärer Teil zwischen den Grenzen $\pm \pi i$ liegt; setzt man nun wieder $s = r'$ und unterwirft r der Bedingung $0 < r < m$, so ist

$$\frac{\mu_s}{\mu_{s+\nu}} = \frac{1 - \theta^r}{1 - \theta^{-r}} = -\theta^r = e^{\pi i\left(\frac{2r}{m} - 1\right)},$$

mithin

$$\log\left(\frac{\mu_s}{\mu_{s+\nu}}\right) = \pi i\left(\frac{2r}{m} - 1\right).$$

Setzt man daher zur Abkürzung

$$\varphi(\alpha) = -\Sigma r \alpha^{-r'}, \tag{64}$$

wo r die Werte $1, 2, 3 \ldots (m-1)$ zu durchlaufen hat, so erhält man mit Rücksicht auf (50) das Resultat

$$\psi(\alpha) = -\frac{\pi i}{m} \varphi(\alpha). \tag{65}$$

Offenbar ist $\varphi(\alpha)$ eine ganze algebraische Zahl; bezieht man daher das Produktzeichen Π' auf alle Wurzeln α der Gleichung (63), so ist $\Pi' \varphi(\alpha)$ als symmetrische Funktion dieser Wurzeln*) eine ganze rationale Zahl, und wir wollen zeigen, daß dieselbe positiv

*) Will man sich hierauf nicht berufen, so leuchtet doch ein, daß das fragliche Produkt rational ist, weil man es als eine Norm oder als ein Produkt mehrerer Normen in denjenigen Körpern ansehen kann, welche den Wurzeln der Gleichung (63) entsprechen.

und außerdem durch $(2m)^{\nu-1}$ teilbar ist. Das erstere leuchtet sofort ein, wenn ν gerade ist, weil in diesem Falle die Wurzeln der Gleichung (63) aus imaginären Paaren von der Form α, α^{-1} bestehen; ist ferner ν ungerade, also $m \equiv 3 \pmod 4$, so tritt außer solchen Paaren noch die reelle Wurzel $\alpha = -1$ auf, also auch der reelle Faktor

$$\varphi(-1) = -\Sigma r(-1)^{-r'} = -\Sigma\left(\frac{r}{m}\right)r,$$

welcher aber nach einer früheren Untersuchung (§ 104, S. 264 [von Dirichlet-Dedekind]) einen positiven Wert hat. Um auch die zweite Behauptung zu erweisen, bilden wir das Produkt

$$c\,\varphi(\alpha) = -\alpha\,\Sigma(cr)\alpha^{-(cr)'},$$

wo c wieder die Basis unseres Index-Systems bedeutet; reduziert man hierin die Produkte cr auf ihre kleinsten positiven Reste nach m, so stimmen dieselben im Komplex wieder mit den Zahlen r überein, woraus offenbar folgt, daß $(c-\alpha)\varphi(\alpha)$ durch m teilbar, mithin

$$\Pi'(c-\alpha).\,\Pi'\varphi(\alpha) \equiv 0 \pmod{m^{\nu}}$$

ist; hierin ist der erste Faktor

$$\Pi'(c-\alpha) = c^{\nu}+1 \equiv 0 \pmod m;$$

wählt man aber die Zahl c so, daß sie eine primitive Wurzel auch von m^2 wird (§ 128), so ist $c^{2\nu}-1$ und folglich auch $c^{\nu}+1$ nicht durch m^2 teilbar, und hieraus folgt, daß $\Pi'\varphi(\alpha)$ durch $m^{\nu-1}$ teilbar ist*). Ganz ähnlich ergibt sich die Teilbarkeit durch $2^{\nu-1}$; durchläuft nämlich u diejenigen ν Werte r, deren Indizes $u' \equiv 0, -1, -2, \cdots, -(\nu-1) \pmod{2\nu}$ sind, so durchläuft die Zahl $(m-u)$, deren Index $\equiv u'+\nu \pmod{2\nu}$, die übrigen Werte r, und man erhält

$$\varphi(\alpha) = -\Sigma(2u-m)\alpha^{-u'};$$

da aber

$$\Sigma\alpha^{-u'} = 1+\alpha+\cdots+\alpha^{\nu-1} = \frac{1-\alpha^{\nu}}{1-\alpha} = \frac{2}{1-\alpha},$$

also

$$\varphi(\alpha) = \frac{2m}{1-\alpha} - 2\,\Sigma u\,\alpha^{-u'}$$

ist, so folgt, daß $(1-\alpha)\varphi(\alpha)$ durch 2 teilbar ist, und hieraus ergibt sich, daß $\Pi'\varphi(\alpha)$ durch $2^{\nu-1}$ teilbar ist, weil $\Pi'(1-\alpha) = 1^{\nu}+1 = 2$ ist. Nachdem hiermit unsere obigen Behauptungen bewiesen sind, können wir

(66) $$\Pi'\varphi(\alpha) = (2m)^{\nu-1}a$$

*) Natürlich ist dies Resultat von der bei dem Beweise gemachten speziellen Annahme über c gänzlich unabhängig.

setzen, wo a eine natürliche Zahl*) bedeutet, und hiermit ergibt sich zugleich

$$\Pi' \psi(\alpha) = \frac{(-2\pi i)^\nu a}{2m}. \tag{67}$$

Wir haben jetzt den Ausdruck $\psi(\alpha)$ für den zweiten Fall zu untersuchen, in welchem $\alpha^\nu = +1$ oder vielmehr

$$\frac{\alpha^\nu - 1}{\alpha - 1} = 1 + \alpha + \alpha^2 + \cdots + \alpha^{\nu-1} = 0 \tag{68}$$

ist [im Falle $m = 3$, $\nu = 1$ gibt es keine solche Zahl α, also auch keinen solchen Faktor $\psi(\alpha)$]. Läßt man u ein vollständiges Restsystem nach dem Modul ν durchlaufen, so bilden diese Zahlen u in Verbindung mit den Zahlen $u + \nu$ ein vollständiges System von inkongruenten Zahlen s in bezug auf den Modul 2ν, und aus der Definition (57) folgt daher in unserem Falle

$$\psi(\alpha) = -\Sigma \alpha^{-u} \log(\mu_u \mu_{u+\nu}), \tag{69}$$

wo die imaginären Teile der Logarithmen wieder zwischen den Grenzen $\pm \pi i$ liegen; da aber die Produkte $\mu_u \mu_{u+\nu}$ positiv sind, so folgt hieraus, daß die Logarithmen reell sind. Bezieht sich nun das Produktzeichen Π'' auf alle Wurzeln α der Gleichung (68), so ergibt sich zunächst, daß $\Pi'' \psi(\alpha)$ positiv ist; dies leuchtet sofort ein, wenn ν ungerade ist, weil in diesem Falle die genannten Wurzeln aus imaginären Paaren von der Form α, α^{-1} bestehen; ist ferner ν gerade, also $m \equiv 1 \pmod 4$, so tritt außer solchen Paaren noch die reelle Wurzel $\alpha = -1$ auf, also auch der reelle Faktor

$$\psi(-1) = -\Sigma(-1)^{-s} \log \mu_{s+\nu} = -\Sigma\left(\frac{r}{m}\right) \log(1 - \theta^{-r}),$$

welcher aber nach einer früheren Untersuchung (§ 104, S. 267 [von Dirichlet-Dedekind]) einen positiven Wert hat. Setzt man nun nach Belieben

$$\tau = \frac{\mu_1}{\mu} \quad \text{oder} \quad = \frac{(\mu\theta^\nu)_1}{\mu\theta^\nu}, \tag{70}$$

welcher letztere Wert der Bedingung $\tau_\nu = \tau$ genügt, also reell ist, so ist τ eine Einheit in Ω, weil μ und μ_1 assoziiert sind, und wir wollen beweisen, daß das positive Produkt

$$\Pi'' \psi(\alpha) = T' \tag{71}$$

*) Dieselbe ist von Kummer mit $P'(m)$ bezeichnet.

ist, wo T' den Regulator des aus den $\nu - 1$ konjugierten Einheiten

(72) $$\tau_0, \tau_1, \ldots, \tau_{\nu-2}$$

bestehenden Systems T bedeutet (S. 163).

Hierzu setzen wir im Anschluß an die in § 183 (S. 162) eingeführte Bezeichnung den reellen Logarithmus

(73) $$\log(\omega_u \omega_{u+v}) = l_u(\omega),$$

wo u auch durch jede nach ν kongruente Zahl ersetzt werden darf; dann ist allgemein

$$l_u(\omega_v) = l_{u+v}(\omega),$$

und wenn man zur Abkürzung

$$l_u(\mu) = \lambda_u$$

setzt, so folgt aus (70)

$$l_u(\tau_v) = l_{u+v}\left(\frac{\mu_1}{\mu}\right) = \lambda_{u+v+1} - \lambda_{u+v}.$$

Multipliziert man nun das Produkt der $\nu - 1$ Faktoren

$$\psi(\alpha) = -\Sigma \lambda_u \alpha^{-u}$$

noch mit dem von Null verschiedenen Faktor

$$\psi(1) = -(\lambda_0 + \lambda_1 + \cdots + \lambda_{\nu-1}) = -\log N(\mu) = -\log m,$$

so wird nach einem sehr bekannten Satze*) der Determinanten-Theorie das Produkt

$$\psi(1)\,\Pi''\psi(\alpha) = (-1)^\nu \begin{vmatrix} \lambda_0, & \lambda_1, \ldots, \lambda_{\nu-2}, & \lambda_{\nu-1} \\ \lambda_{\nu-1}, & \lambda_0, \ldots, \lambda_{\nu-3}, & \lambda_{\nu-2} \\ \cdots & \cdots & \cdots \\ \lambda_2, & \lambda_3, \ldots, \lambda_0, & \lambda_1 \\ \lambda_1, & \lambda_2, \ldots, \lambda_{\nu-1}, & \lambda_0 \end{vmatrix}$$

$$= \begin{vmatrix} \lambda_1 - \lambda_0, & \lambda_2 - \lambda_1, \ldots, \lambda_{\nu-1} - \lambda_{\nu-2}, & -\lambda_{\nu-1} \\ \lambda_0 - \lambda_{\nu-1}, & \lambda_1 - \lambda_0, \ldots, \lambda_{\nu-2} - \lambda_{\nu-3}, & -\lambda_{\nu-2} \\ \cdots & \cdots & \cdots \\ \lambda_3 - \lambda_2, & \lambda_4 - \lambda_3, \ldots, \lambda_1 - \lambda_0, & -\lambda_1 \\ \lambda_2 - \lambda_1, & \lambda_3 - \lambda_2, \ldots, \lambda_0 - \lambda_{\nu-1}, & -\lambda_0 \end{vmatrix}$$

$$= \begin{vmatrix} l_0(\tau_0), & l_0(\tau_1), & \ldots, l_0(\tau_{\nu-2}), & -\lambda_{\nu-1} \\ l_{\nu-1}(\tau_0), & l_{\nu-1}(\tau_1), \ldots, & l_{\nu-1}(\tau_{\nu-2}), & -\lambda_{\nu-2} \\ \cdots & \cdots & \cdots & \cdots \\ l_2(\tau_0), & l_2(\tau_1), & \ldots, l_2(\tau_{\nu-2}), & -\lambda_1 \\ l_1(\tau_0), & l_1(\tau_1), & \ldots, l_1(\tau_{\nu-2}), & -\lambda_0 \end{vmatrix}$$

*) Vgl. Baltzer: Theorie und Anwendung der Determinanten, § 11, 2. (vierte Auflage, 1875).

und da diese Determinante (nach § 183, S. 162) gleich $\psi(1)\,T'$ ist, so ergibt sich hieraus die zu beweisende Gleichung (71).

Bezeichnet man nun wieder mit S ein System von $\nu - 1$ Fundamentaleinheiten, und mit σ die in der entsprechenden Gruppe (S) enthaltenen Einheiten, so läßt sich jede Einheit $\tau_0, \tau_1, \ldots, \tau_{\nu-2}$ in die Form $\varrho\,\sigma$ setzen, wo ϱ eine der r reduzierten Einheiten bedeutet und eine Wurzel der Gleichung $\varrho^r = 1$ ist; man kann folglich die positive Größe

$$T' = b\,S' \tag{74}$$

setzen, wo S' den positiven Regulator des Systems S, und b eine natürliche Zahl*) bedeutet (§ 183, 8). Unter den r reduzierten Einheiten ϱ befinden sich jedenfalls die $2m$ Einheiten

$$\pm 1, \pm\theta, \pm\theta^2 \ldots \pm\theta^{m-1},$$

weil ihre in bezug auf S genommenen Exponenten sämtlich verschwinden, und da $(-\theta)^r = 1$ sein muß, so ist r jedenfalls teilbar durch $2m$. Wir wollen nun zeigen, daß $r = 2m$ ist, daß also außer den genannten keine andere Einheitswurzel ϱ in Ω existiert. Dies ist eigentlich eine unmittelbare Folge der allgemeinen Gesetze, welche die algebraische Verwandtschaft der Körper beherrschen, auf die wir uns hier jedoch nicht berufen wollen. Zu demselben Ziele gelangt man leicht, wenn man gemäß (7) die ganze Zahl $\varrho = F(\theta)$ setzt, woraus $\varrho^{-1} = F(\theta^{-1})$ folgt, und die Gleichung $F(\theta)F(\theta^{-1}) = 1$ nach Ausführung der Multiplikation näher untersucht. Wir ziehen hier aber folgenden Weg vor, bei welchem wir uns auf die Theorie der Ideale stützen. Ist p irgendeine in r aufgehende Primzahl, und pq die höchste Potenz von p, welche in r aufgeht, so befinden sich unter den Wurzeln ϱ der Gleichung $\varrho^r = 1$ auch die primitiven Wurzeln ϱ der Gleichung $\varrho^{pq} = 1$; bezeichnet man eine bestimmte von ihnen mit ϱ, so sind alle in der Form ϱ^s enthalten, wo s alle durch p nicht teilbaren Zahlen durchläuft, die nach dem Modul pq inkongruent sind, und wenn t eine Variable bedeutet, so ist (nach § 139)

$$\frac{t^{pq} - 1}{t^q - 1} = \Pi(t - \varrho^s).$$

*) Zur Bestimmung dieser Zahl nach (74) ist die Kenntnis eines Fundamentalsystems S erforderlich, welches aber bis jetzt, selbst in den einfachsten Fällen, nur durch äußerst beschwerliche Rechnungen zu erlangen ist.

Setzt man hierin $t = 1$, so ergibt sich, wie im Anfange dieses Paragraphen, daß

$$p = \delta(1 - \varrho)^{(p-1)q}$$

ist, wo δ eine Einheit bedeutet; ist daher $\mathfrak{p}$ ein in p aufgehendes Primideal, so geht $\mathfrak{p}$ auch in $1 - \varrho$ auf, und folglich ist p durch $\mathfrak{p}^{(q-1)q}$ teilbar. Wenn nun p von m verschieden ist, so ist p, wie wir oben gesehen haben, durch kein Quadrat eines Primideals teilbar, und folglich muß $(p-1)q = 1$, also $p = 2$, $q = 1$ sein; mithin ist r durch keine von m verschiedene ungerade Primzahl, und auch nicht durch 4 teilbar; und ebenso ergibt sich für den Fall $p = m$, daß $q = 1$ ist, also r nicht durch m^2 teilbar sein kann, weil $\mathfrak{o}m$ die $(m-1)^{\text{te}}$ Potenz eines Primideals ist. Da nun r, wie oben bemerkt, durch $2m$ teilbar ist, so folgt hieraus offenbar, daß

$$r = 2m \tag{75}$$

ist, wie behauptet war. Behält daher E dieselbe Bedeutung, wie in den beiden vorhergehenden Paragraphen, so ist

$$S' = 2mE, \tag{76}$$

und folglich*)

$$\Pi'' \psi(\alpha) = 2mbE. \tag{77}$$

Durch Zusammensetzung der in (58), (62), (67) und (77) erhaltenen Resultate ergibt sich nun leicht der Wert des auf alle Wurzeln α der Gleichung (50) ausgedehnten Produktes

$$\Pi L^0(\alpha) = \frac{1}{m^{2\nu-1}} \Pi(\alpha, \theta) \Pi' \psi(\alpha) \Pi'' \psi(\alpha),$$

und hierdurch nimmt die Gleichung (52) mit Rücksicht auf (9) folgende Form an

$$gh = \frac{(2\pi)^\nu E a b}{m^{\nu-1}\sqrt{m}} = \frac{(2\pi)^\nu E a b}{\sqrt{(D)}}; \tag{78}$$

da ferner (nach § 184, II)

$$g = \frac{(2\pi)^\nu E}{\sqrt{(D)}} \tag{79}$$

ist, so erhalten wir das von Kummer gefundene Endresultat

$$h = ab, \tag{80}$$

wo a, b natürliche Zahlen bedeuten, die durch die Gleichungen (66) und (74) definiert sind.

*) Offenbar ist $2mb$ die Anzahl der in bezug auf das System T reduzierten Einheiten.

§ 186.

Als zweites und letztes Beispiel, auf welches wir unsere allgemeine Idealtheorie anwenden wollen, wählen wir das der quadratischen Körper, weil dasselbe mit dem Hauptgegenstande dieses Werkes, der Theorie der binären quadratischen Formen, im engsten Zusammenhange steht. Wir haben schon früher (§ 175) die Grundzahl D eines solchen Körpers Ω bestimmt und gezeigt, daß, wenn

$$\theta = \frac{D + \sqrt{D}}{2}, \quad \mathfrak{o} = [1, \theta] \tag{1}$$

gesetzt wird, $\mathfrak{o}$ das System aller in Ω enthaltenen ganzen Zahlen ist. Um nun alle Primideale dieses Körpers zu finden, erinnern wir wieder daran, daß zu jedem solchen Ideal $\mathfrak{p}$ eine bestimmte, durch $\mathfrak{p}$ teilbare natürliche Primzahl p gehört, welche von allen durch $\mathfrak{p}$ teilbaren natürlichen Zahlen die kleinste ist, woraus unmittelbar folgt, daß die p Zahlen $0, 1, 2, \ldots, (p-1)$ jedenfalls inkongruent nach $\mathfrak{p}$ sind; da ferner $N(\mathfrak{p})$ ein Divisor von $p^2 = N(p)$, also entweder $= p$ oder $= p^2$ ist, so ist $\mathfrak{p}$ ein Ideal ersten oder zweiten Grades, und es leuchtet ein, daß im ersten Falle $\mathfrak{o}\,p = \mathfrak{p}\,\mathfrak{p}'$, also ein Produkt von zwei Primidealen ersten Grades, im zweiten Falle aber $\mathfrak{o}\,p = \mathfrak{p}$ ein Primideal zweiten Grades ist, also p auch im Körper Ω den Charakter einer Primzahl behält. Wir wollen nun beweisen, daß der erste oder zweite Fall eintritt, je nachdem D quadratischer Rest oder Nichtrest von $4p$ ist.

In der Tat, nehmen wir an, es finde der erste Fall $\mathfrak{o}\,p = \mathfrak{p}\,\mathfrak{p}'$ statt, so bilden, weil $(\mathfrak{o}, \mathfrak{p}) = N(\mathfrak{p}) = p$ ist, die Zahlen $0, 1, 2, \ldots, (p-1)$ ein vollständiges Restsystem nach $\mathfrak{p}$, und folglich gibt es eine rationale Zahl t, welche der Bedingung

$$t \equiv \theta \pmod{\mathfrak{p}} \tag{2}$$

genügt; setzt man daher, indem man (wie in § 175) die zu einer Zahl ω konjugierte Zahl mit ω' bezeichnet,

$$\pi = \theta - t = \frac{r + \sqrt{D}}{2}, \quad \pi' = \theta' - t = \frac{r - \sqrt{D}}{2}, \tag{3}$$

$$N(\pi) = \pi\,\pi' = \frac{r^2 - D}{4}, \tag{4}$$

wo

$$r = D - 2t \tag{5}$$

ebenfalls eine ganze rationale Zahl bedeutet, so ist π durch $\mathfrak{p}$, mithin $N(\pi)$ durch $N(\mathfrak{p})$, also durch p teilbar, und hieraus folgt, daß

$$r^2 \equiv D \pmod{4p}, \tag{6}$$

also D quadratischer Rest von $4p$ ist. Umgekehrt, wenn die vorstehende Kongruenz durch eine ganze rationale Zahl r befriedigt wird, so ist $r \equiv D \pmod 2$, und folglich sind die obigen, aus r oder t gebildeten Zahlen π, π' ganze Zahlen, deren Produkt durch p teilbar ist; da aber zufolge (1) keiner der beiden Faktoren π, π' durch p teilbar ist, so kann $\mathfrak{o}\,p$ kein Primideal sein, und folglich ist $\mathfrak{o}\,p$ gewiß ein Produkt von zwei Primidealen ersten Grades, womit unser Satz vollständig bewiesen ist.

Wir können noch hinzufügen, daß, wenn wir für den Fall $\mathfrak{o}\,p = \mathfrak{p}\,\mathfrak{p}'$ die vorstehenden Bezeichnungen beibehalten, die Zahl π' immer durch $\mathfrak{p}'$ teilbar ist. Da nämlich π durch $\mathfrak{p}$, aber nicht durch p teilbar ist, so kann man $\mathfrak{o}\,\pi = \mathfrak{p}\,\mathfrak{q}$ setzen, wo das Ideal $\mathfrak{q}$ nicht durch $\mathfrak{p}'$ teilbar ist; da ferner $\pi\,\pi'$ durch p, also $\mathfrak{p}\,\mathfrak{q}\,\pi'$ durch $\mathfrak{p}\,\mathfrak{p}'$, mithin $\mathfrak{q}\,\pi'$ durch $\mathfrak{p}'$ teilbar ist, so muß π' durch das Primideal $\mathfrak{p}'$ teilbar sein, wie behauptet war*).

Es ist nun noch von Wichtigkeit zu untersuchen, unter welcher Bedingung die in diesem Falle auftretenden Faktoren $\mathfrak{p}$, $\mathfrak{p}'$ miteinander identisch sind, also $\mathfrak{o}\,p = \mathfrak{p}^2$ wird; da unter dieser Annahme beide Zahlen π, π' durch $\mathfrak{p}$ teilbar sind, so gilt dasselbe von der Zahl $r = \pi + \pi'$, und da r rational ist, so muß r auch durch p teilbar sein, woraus mit Rücksicht auf (6) folgt, daß p in D aufgeht. Umgekehrt, wenn p eine in der Grundzahl D aufgehende Primzahl ist, so folgt zunächst, daß D auch quadratischer Rest von $4p$ ist; ist nämlich $p = 2$, so ist D (nach § 175) durch 4 teilbar, und folglich wird die Kongruenz (6) durch $r = 0$ oder durch $r = 2$ befriedigt; ist aber p ungerade, so geschieht dasselbe durch $r = 0$ oder $r = p$, je nachdem $D \equiv 0$ oder $\equiv 1 \pmod 4$ ist. Mithin ist $\mathfrak{o}\,p$ ein Produkt von zwei Primidealen ersten Grades $\mathfrak{p}$, $\mathfrak{p}'$; behält man die obigen Bezeichnungen bei und berücksichtigt, daß r jedenfalls durch p teilbar ist, so folgt, daß die durch $\mathfrak{p}$ teilbare Zahl $\pi = r - \pi'$ auch durch $\mathfrak{p}'$ teilbar ist; wäre nun $\mathfrak{p}'$ verschieden von

*) Man findet auch leicht, daß $\mathfrak{p} = [p, \pi]$, $\mathfrak{p}' = [p, \pi']$ ist, und wir empfehlen dem Leser, die Gleichung $\mathfrak{p}\,\mathfrak{p}' = \mathfrak{o}\,p$ durch wirkliche Ausführung der Multiplikation zu verifizieren, wobei es darauf ankommt, den viergliedrigen Modul $[p^2, p\,\pi, p\,\pi', \pi\,\pi']$ nach § 172 auf einen zweigliedrigen zu reduzieren (vgl. § 187).

$\mathfrak{p}$, so müßte π durch $\mathfrak{p}\,\mathfrak{p}'$, also auch durch p teilbar sein, was nicht der Fall ist; mithin ist $\mathfrak{p}' = \mathfrak{p}$, und folglich $\mathfrak{o}\,p = \mathfrak{p}^2$. Wir können daher das Resultat unserer bisherigen Untersuchung so aussprechen:

Bedeutet p eine natürliche Primzahl, so ist $\mathfrak{o}\,p$ stets und nur dann das Quadrat eines Primideals vom ersten Grade, wenn p in der Grundzahl D aufgeht; ist aber D nicht teilbar durch p, so ist $\mathfrak{o}\,p$ ein Produkt von zwei verschiedenen Primidealen ersten Grades, oder $\mathfrak{o}\,p$ ist selbst ein Primideal zweiten Grades, je nachdem D quadratischer Rest oder Nichtrest von $4\,p$ ist*).

Die Zahl $p = 2$ bietet den ersten, zweiten oder dritten Fall dar, je nachdem $D \equiv 0 \pmod 4$, $\equiv 1 \pmod 8$, oder $\equiv 5 \pmod 8$ ist, und hieraus erklärt sich das eigentümliche Verhalten der Zahl 2 in der Theorie der quadratischen Reste (§ 36). Ist p ungerade, so kommt, weil stets $D^2 \equiv D \pmod 4$ ist, die Bedingung (6) darauf hinaus, daß D quadratischer Rest von p ist, und folglich wird der erste, zweite oder dritte Fall eintreten, je nachdem

$$\left(\frac{D}{p}\right) = 0, = +1, \text{ oder } = -1$$

ist. Um aber alle Fälle zusammenzufassen, wollen wir ein anderes Symbol einführen und

(7) $$(D, p) = 0, = +1, \text{ oder } = -1$$

setzen, je nachdem die Primzahl p den ersten, zweiten oder dritten Fall darbietet; für jede ungerade Primzahl p ist daher

$$(D, p) = \left(\frac{D}{p}\right).$$

Wir definieren ferner

(8) $$(D, 1) = 1,$$

und wenn

$$m = p\,p'\,p'' \ldots$$

*) Hierzu bemerken wir folgendes. Sind die Primideale eines Normalkörpers bekannt, so gilt dasselbe, wie demnächst an einem anderen Orte [XXIV dieser Ausgabe] gezeigt werden soll, auch für jeden Divisor dieses Körpers. Nun ist, wie wir schon in der Schlußbemerkung zu § 175 gesagt haben, unser quadratischer Körper Ω ein Divisor desjenigen Normalkörpers, welcher aus einer primitiven D^{ten} Wurzel der Einheit entspringt, und da die Ideale dieses Kreisteilungs-Körpers nach den in § 185 (S. 184) angegebenen Sätzen bekannt sind, so folgt daraus auch die Bestimmung der Ideale des quadratischen Körpers Ω, aber in einer anderen

ein Produkt von beliebig vielen Primzahlen $p, p', p'' \ldots$ ist, so setzen wir entsprechend

$$(9) \qquad (D, m) = (D, p)\ (D, p')\ (D, p'') \ldots,$$

woraus der allgemeine Satz

$$(10) \qquad (D, m'\ m'') = (D, m')\ (D, m'')$$

folgt*).

Indem wir die bei der allgemeinen Untersuchung über die Anzahl h der Idealklassen benutzten Bezeichnungen beibehalten (§ 184), setzen wir

$$(11) \qquad \Omega(s) = \Sigma N(\mathfrak{a})^{-s} = \Pi(1 - N(\mathfrak{p})^{-s})^{-1};$$

fassen wir die Faktoren des Produktes zusammen, welche von den verschiedenen in einer und derselben natürlichen Primzahl p aufgehenden Primidealen $\mathfrak{p}$ herrühren, so ist dieser Beitrag gleich

$$(1 - p^{-s})^{-1},\ (1 - p^{-s})^{-2},\ (1 - p^{-2s})^{-1},$$

je nachdem der erste, zweite oder dritte der obigen Fälle eintritt; mit Benutzung des eben eingeführten Symbols (7) kann man aber diese drei Ausdrücke in der gemeinschaftlichen Form des Produktes

$$(1 - p^{-s})^{-1}\ (1 - (D, p)\ p^{-s})^{-1}$$

zusammenfassen, und hieraus folgt mit Rücksicht auf (10), daß

$$\Omega(s) = \Pi(1 - p^{-s})^{-1}\ \Pi(1 - (D, p)\ p^{-s})^{-1}$$

$$(12) \qquad = \Sigma \frac{1}{m^s} \cdot \Sigma \frac{(D, m)}{m^s}$$

ist, wo m in jeder der beiden Summen alle natürlichen Zahlen durchlaufen muß. Multipliziert man mit der positiven Größe $s - 1$ und läßt dieselbe unendlich klein werden, so ergibt sich hieraus

$$(13) \qquad g h = \lim \Sigma \frac{(D, m)}{m^s},$$

wo g die frühere Bedeutung hat; ordnet man die Glieder der Reihe nach wachsenden m, so folgt aus dem Reziprozitätssatze (vgl. § 52),

---

als der obigen Form, nämlich so, daß die Zerlegung von $\mathfrak{o}p$ in Primideale sich unmittelbar aus der Zahlklasse ergibt, welcher die Zahl p nach dem Modul D angehört. Aus der Vergleichung beider Formen ergibt sich abermals ein Beweis des Reziprozitätssatzes.

*) Eine erfolgreiche Verallgemeinerung dieses Symbols findet sich in der Abhandlung von H. Weber: Zahlentheoretische Untersuchungen aus dem Gebiete der elliptischen Funktionen (Nachr. v. d. Göttinger Ges. d. W., 18. Januar 1893).

daß die Summe von je (D) aufeinanderfolgenden Koeffizienten (D, m) verschwindet; mithin konvergiert die Reihe für alle positiven Werte s, und da sie zugleich eine stetige Funktion von s ist (§ 101), so erhalten wir

$$g h = \Sigma \frac{(D, m)}{m}. \tag{14}$$

Den Wert von g haben wir früher allgemein bestimmt (§ 184), aber er nimmt je nach dem Vorzeichen der Grundzahl D verschiedene Formen an. Ist D negativ, so ist $\nu = 1$, und E ist der umgekehrte Wert der Anzahl r aller in $\mathfrak{Q}$ enthaltenen Einheiten, welche $= 6$ für $D = -3$, $= 4$ für $D = -4$, und $= 2$ in allen anderen Fällen ist; es wird daher

$$g = \frac{2\pi}{r\sqrt{-D}},$$

mithin

$$h = \frac{r\sqrt{-D}}{2\pi} \Sigma \frac{(D, m)}{m}. \tag{15}$$

Ist aber D positiv, so ist $\nu = 2$; die Anzahl r der reduzierten Einheiten ± 1 ist $= 2$, mithin

$$E = \frac{1}{2} \log \varepsilon = \frac{1}{2} \log \left(\frac{T + U\sqrt{D}}{2}\right),$$

wo ε die Fundamentaleinheit bedeutet, also T, U die kleinsten natürlichen Zahlen sind, welche der Pellschen Gleichung

$$T^2 - D U^2 = \pm 4$$

genügen; es wird daher

$$g = \frac{2 \log \varepsilon}{\sqrt{D}}$$

und folglich

$$h = \frac{\sqrt{D}}{2 \log \varepsilon} \Sigma \frac{(D, m)}{m}. \tag{16}$$

Nimmt man aber für diesen Fall die auf S. 145 beschriebene feinere Einteilung in Idealklassen an, nach welcher zwei Ideale $\mathfrak{a}$, $\mathfrak{a}_1$ nur dann derselben Klasse zugeteilt werden, wenn es eine Zahl η von positiver Norm gibt, welche der Bedingung $\mathfrak{a}\eta = \mathfrak{a}_1$ genügt, so bestimmt sich die Anzahl h_1 dieser Idealklassen auf folgende Weise. Bedeuten T_1, U_1 die kleinsten natürlichen Zahlen, welche der Bedingung

$$T_1^2 - D U_1^2 = +4$$

genügen, so ist

$$\varepsilon_1 = \frac{T_1 + U_1\sqrt{D}}{2}$$

die kleinste unter allen denjenigen Einheiten von positiver Norm, welche positiv und > 1 sind. Ist nun $N(\varepsilon) = -1$, also $\varepsilon_1 = \varepsilon^2$, so stimmt die jetzige Einteilung in Idealklassen mit der früheren völlig überein, also ist $h_1 = h$; ist aber $N(\varepsilon) = +1$, also $\varepsilon_1 = \varepsilon$, so gibt es gar keine Einheit von negativer Norm, und folglich ist $h_1 = 2h$, weil z. B. die Zahl $\sqrt{D}$ eine negative Norm besitzt. Für beide Fälle ergibt sich daher aus (16) die gemeinsame Bestimmung

$$h_1 = \frac{\sqrt{D}}{\log \varepsilon_1} \Sigma \frac{(D, m)}{m}. \tag{17}$$

Vergleicht man die so gewonnenen Resultate (15) und (17) mit denen des fünften Abschnitts (§§ 97, 99), so wird man sich bei genauer Berücksichtigung der damals und jetzt angewendeten Bezeichnungen leicht überzeugen, daß, je nachdem die Grundzahl $D \equiv 0$ oder $\equiv 1 \pmod 4$ ist, die Anzahl unserer Idealklassen vollständig übereinstimmt mit der Klassenanzahl der (positiven) ursprünglichen Formen erster Art für die Determinante $^1/_4 D$, oder mit derjenigen der (positiven) ursprünglichen Formen zweiter Art für die Determinante D. Diese Übereinstimmung ist eine notwendige Folge des Umstandes, daß in unserem Falle der quadratischen Körper, wie man leicht finden wird, jede bestimmte Klasse von eigentlich äquivalenten Formen der Diskriminante D auch nur einer einzigen Idealklasse entspricht (vgl. § 182, S. 150 bis 151 und den Schluß von § 187).

Die Einteilung der binären quadratischen Formen in Geschlechter (Supplement IV) läßt sich ebenfalls leicht auf die Ideale übertragen, und sowohl diese Untersuchung wie der auf die Abzählung der zweiseitigen Klassen gestützte Beweis des Reziprozitätssatzes (§§ 152 bis 154) gewinnt in der neuen Einkleidung eine weit einfachere Gestalt, deren Herstellung wir jedoch dem Leser überlassen müssen. Dagegen wollen wir im folgenden noch die allgemeine Theorie der Moduln für quadratische Körper hinzufügen, weil dieselbe die Komposition der binären quadratischen Formen in sich schließt und für viele andere Untersuchungen, z. B. für die Theorie der komplexen Multiplikation der elliptischen Funktionen*) von großer Bedeutung ist.

*) Dieselbe ist im wesentlichen von Kronecker geschaffen und in zahlreichen Schriften behandelt, deren Sammlung bevorsteht. Vgl. die Abhandlung von Hermite: Sur la théorie dès équations modulaires et la résolution de l'équation du cinquième degré (1859), ferner die Werke von H. Weber: Ellip-

§ 187.

Jeder endliche Modul, dessen Zahlen sämtlich dem quadratischen Körper Ω angehören, läßt sich (nach § 172, VI) immer auf eine Basis zurückführen, welche aus höchstens zwei Zahlen besteht, und wir wollen im folgenden unter einem Modul, falls das Gegenteil nicht ausdrücklich bemerkt wird, immer einen solchen zweigliedrigen Modul

(1) $$\mathfrak{m} = [\alpha, \beta]$$

verstehen, dessen Basiszahlen α, β wirklich voneinander unabhängig sind und folglich zugleich eine Basis des Körpers Ω bilden. Es ist nun zweckmäßig, jede solche beliebig gegebene Basis so umzuformen, daß die eine der beiden Basiszahlen eine positive rationale Zahl m wird. Um die Möglichkeit dieser Umformung darzutun, bemerken wir, daß, weil die Zahl 1 in Ω enthalten ist, es immer zwei bestimmte rationale Zahlen x, y gibt, welche der Bedingung $x\alpha + y\beta = 1$ genügen; stellt man dieselben als Brüche mit demselben Nenner dar und sondert aus den Zählern den größten gemeinschaftlichen Teiler ab, so nimmt diese Gleichung die Form

$$m = p\alpha + q\beta$$

an, wo p, q relative Primzahlen bedeuten, und m eine positive, ganze oder gebrochene rationale Zahl ist; bestimmt man ferner zwei ganze rationale Zahlen r, s so, daß

$$ps - qr = \pm 1$$

wird, und setzt hierauf

$$m\omega = r\alpha + s\beta,$$

so leuchtet ein, daß die Zahlen m, $m\omega$ ebenfalls eine irreduzible Basis von $\mathfrak{m}$ bilden und daß folglich

(2) $$\mathfrak{m} = [m, m\omega] = m[1, \omega]$$

ist. Da ω gewiß irrational ist, so ist $[m]$ der Inbegriff aller in $\mathfrak{m}$ enthaltenen rationalen Zahlen, und m ist als die kleinste positive unter ihnen vollständig bestimmt.

Die Zahl ω ist die eine Wurzel einer irreduziblen quadratischen Gleichung

(3) $$a\omega^2 - b\omega + c = 0,$$

---

tische Funktionen und algebraische Zahlen (1890) und von F. Klein und R. Fricke: Vorlesungen über die Theorie der elliptischen Modulfunktionen (1890 bis 1892).

wo a, b, c ganze rationale Zahlen ohne gemeinschaftlichen Teiler bedeuten, und diese sind durch ω vollständig bestimmt, wenn wir festsetzen, daß a immer positiv sein soll. Bedeutet D wieder die Grundzahl des Körpers Ω, und setzen wir, wie im vorigen Paragraphen,

$$\theta = \frac{D + \sqrt{D}}{2}, \quad \mathfrak{o} = [1, \theta], \tag{4}$$

so ist $a\omega$ als ganze Zahl von der Form

$$a\omega = h + k\theta = \frac{b + k\sqrt{D}}{2} = \frac{b + \sqrt{d}}{2}, \tag{5}$$

wo h, k ganze rationale Zahlen bedeuten, und

$$d = b^2 - 4ac = \Delta(1, a\omega) = Dk^2 \tag{6}$$

ist. Da ω ohne Änderung von $\mathfrak{m}$ durch $-\omega$ ersetzt werden kann, so wollen wir für die Folge immer festsetzen, daß k positiv sein soll. Man sieht leicht, daß hierdurch, wenn ein gegebener Modul $\mathfrak{m}$ vorliegt, die Zahl ω so weit und nur so weit bestimmt ist, daß sie durch $\omega_0 = \omega + z$ ersetzt werden kann, wo z jede beliebige ganze rationale Zahl bedeutet; dies hat aber keinen Einfluß auf die Zahlen a, k und d, die mithin vollständig bestimmt sind, während b in $b_0 = 2az + b$, und c in $c_0 = az^2 + bz + c$ übergeht; da mithin b_0 alle Individuen einer bestimmten rationalen Zahlklasse nach dem Modul $2a$ durchläuft, so kann man, wenn man will, ω_0 durch die Bedingung vollständig bestimmen, daß $0 \leqq b_0 < 2a$ sein soll, was aber keinen wesentlichen Nutzen gewährt. Dagegen ist es bisweilen vorteilhaft, ω_0 so zu wählen, daß c_0 relative Primzahl zu a wird; um dies zu erreichen, kann man, wenn r das Produkt aller gleichzeitig in a und in c aufgehenden Primzahlen, und s das Produkt aller übrigen in a aufgehenden Primzahlen bedeutet, z so wählen, daß $z \equiv 1 \pmod{r}$ und zugleich $z \equiv 0 \pmod{s}$ wird, was (nach § 25) stets möglich ist.

Unter der Ordnung $\mathfrak{m}^0$ des Moduls $\mathfrak{m}$, die wir kürzer mit $\mathfrak{n}$ bezeichnen wollen, verstehen wir, wie früher (§ 170), den Inbegriff aller Zahlen ν, für welche $\mathfrak{m}\nu$ durch $\mathfrak{m}$ teilbar wird. Aus dieser Definition folgt offenbar, daß, wenn η eine beliebige von Null verschiedene Zahl bedeutet, $\mathfrak{n}$ zugleich die Ordnung des Moduls $\eta\mathfrak{m}$ ist; behalten wir daher die vorhergehenden Bezeichnungen bei, so sind die gesuchten Zahlen ν alle diejenigen, für welche $[\nu, \nu\omega]$ durch $[1, \omega]$ teilbar wird, und hierzu ist erforderlich und hinreichend, daß

die beiden Zahlen ν und $\nu\omega$ in $[1, \omega]$ enthalten sind. Es muß daher zunächst $\nu = x + y\omega$ sein, wo x, y ganze rationale Zahlen bedeuten; dann ist $\nu\omega = x\omega + y\omega^2$, und da $x\omega$ in $[1, \omega]$ enthalten ist, so muß dasselbe auch von $y\omega^2$ gelten; zufolge (3) ist aber

$$y\omega^2 = \frac{y(b\omega - c)}{a},$$

mithin müssen die beiden Produkte by, cy durch a teilbar sein; da aber die Zahlen a, b, c keinen gemeinschaftlichen Teiler haben, so folgt hieraus, daß y durch a teilbar, also $y = az$, $\nu = x + za\omega$ sein muß, wo z ebenfalls eine ganze rationale Zahl bedeutet; und da umgekehrt jede solche Zahl $x + za\omega$ die geforderte Eigenschaft besitzt, so erhalten wir das Resultat

$$\mathfrak{n} = [1, a\omega] = [1, k\theta] = \mathfrak{o}k + [1]. \tag{7}$$

Jede Ordnung $\mathfrak{n}$ ist daher ein Modul, welcher nur ganze Zahlen und unter diesen auch die Zahl 1, mithin alle ganzen rationalen Zahlen enthält (vgl. § 173, III); umgekehrt leuchtet ein, daß ein jeder solche Modul $\mathfrak{n}$ (in unserem Falle der quadratischen Körper) auch gewiß eine Ordnung, nämlich die Ordnung von $\mathfrak{n}$ selbst ist. Für die Diskriminante, den Index und Führer der Ordnung $\mathfrak{n}$ (S. 156) ergeben sich ferner aus (4), (6) und (7) leicht die Ausdrücke

$$\Delta(\mathfrak{n}) = d, \ (\mathfrak{o}, \mathfrak{n}) = k, \ \frac{\mathfrak{n}}{\mathfrak{o}} = \mathfrak{o}k, \tag{8}$$

und es leuchtet ein, daß jede Ordnung $\mathfrak{n}$ durch ihren Index k vollständig bestimmt ist.

Offenbar ist der Modul $\mathfrak{m}$ stets und nur dann ein Ideal, wenn er durch $\mathfrak{o}$ teilbar, und $\mathfrak{n} = \mathfrak{o}$, also $k = 1$, und m eine ganze, durch a teilbare Zahl ist. Dies führt dazu, den Begriff der Norm auch auf beliebige Moduln $\mathfrak{m}$ zu übertragen, und zwar wollen wir hier*) darunter den Quotienten

$$N(\mathfrak{m}) = \frac{(\mathfrak{n}, \mathfrak{m})}{(\mathfrak{m}, \mathfrak{n})} \tag{9}$$

verstehen, welcher sich in der Tat, wenn $\mathfrak{m}$ ein Ideal ist, auf den der früheren Definition entsprechenden Wert $(\mathfrak{o}, \mathfrak{m})$ reduziert (§ 180). Da die Basiszahlen von $\mathfrak{m}$ mit denen von $\mathfrak{n}$ durch die linearen Gleichungen

$$m = m \cdot 1 + 0 \cdot a\omega, \ m\omega = 0 \cdot 1 + \frac{m}{a} \cdot a\omega$$

*) Vgl. die beiden folgenden Anmerkungen.

verbunden sind, so ergibt sich [nach § 175, (10)] das Resultat

$$(10) \qquad N(\mathfrak{m}) = \begin{vmatrix} m, 0 \\ 0, \frac{m}{a} \end{vmatrix} = \frac{m^2}{a}.$$

Bezeichnet man allgemein, wenn α eine beliebige Zahl des Körpers Ω ist, mit α' die konjugierte Zahl, in welche α durch die nicht identische Permutation des Körpers übergeht, so ist

$$(11) \qquad a(\omega + \omega') = b, \; a\omega\omega' = c;$$

durchläuft μ alle Zahlen des Moduls $\mathfrak{m}$, so bilden die Zahlen μ' einen mit $\mathfrak{m}$ konjugierten Modul $m[1, \omega']$, den wir mit $\mathfrak{m}'$ bezeichnen wollen; halten wir aber an der obigen Vorschrift für die Wahl der Basiszahlen fest, so haben wir

$$(12) \qquad \mathfrak{m}' = m[1, -\omega']$$

zu setzen, und da

$$a(-\omega')^2 - (-b)(-\omega') + c = 0$$

ist, so geschieht der Übergang von $\mathfrak{m}$ zu $\mathfrak{m}'$ lediglich dadurch, daß b durch $-b$ ersetzt wird, während m, a, c, k, d unverändert bleiben. Ebenso ist natürlich $\mathfrak{m}$ konjugiert mit $\mathfrak{m}'$, und beide Moduln haben dieselbe Ordnung $\mathfrak{n} = \mathfrak{n}'$ und dieselbe Norm; sie sind aber nur dann miteinander identisch, wenn b durch a teilbar, also $b \equiv 0$ oder $\equiv a \pmod{2a}$ ist, und in diesem Falle kann $\mathfrak{m}$ ein zweiseitiger Modul genannt werden (vgl. § 58).

Jede in dem Modul $\mathfrak{m}$ enthaltene Zahl μ ist von der Form

$$(13) \qquad \mu = m(x + y\omega),$$

wo x, y ganze rationale Zahlen bedeuten; hieraus folgt

$$N(\mu) = \mu\mu' = m^2(x + y\omega)(x + y\omega'),$$

und wenn man die Multiplikation ausführt, so ergibt sich

$$(14) \qquad N(\mu) = N(\mathfrak{m})(ax^2 + bxy + cy^2);$$

jedem Modul $\mathfrak{m}$ entspricht daher, wenn man die obigen Regeln für die Wahl der Basis festhält, eine ursprüngliche binäre quadratische Form $(a, \frac{1}{2}b, c)$ oder vielmehr eine bestimmte Schar von unendlich vielen solchen parallelen Formen, in welchen b alle Individuen einer bestimmten Zahlklasse nach dem positiven Modul $2a$ durchläuft, und deren Diskriminante $b^2 - 4ac$ zugleich die Diskriminante d der Ordnung $\mathfrak{n}$ ist; dem konjugierten Modul $\mathfrak{m}'$ entspricht die entgegen-

gesetzte Schar $(a, -\frac{1}{2}b, c)$. Offenbar entspricht dieselbe Schar $(a, \frac{1}{2}b, c)$ allen und nur allen Moduln von der Form $\mathfrak{m}n$, wo n jede von Null verschiedene rationale Zahl bedeutet. Da ferner die Zahlen 1, $a\omega$ eine Basis der Ordnung $\mathfrak{n}$ bilden, und

$$a\omega\mu = m(-cy + (ax + by)\omega)$$

$$\begin{vmatrix} x, & y \\ -cy, & ax + by \end{vmatrix} = ax^2 + bxy + cy^2$$

ist, so stimmt diese Form $(a, \frac{1}{2}b, c)$ genau mit derjenigen überein, welche nach der auf S. 156 gegebenen Vorschrift dem Modul $\mathfrak{m}$ entspricht.

Indem wir uns jetzt zur Multiplikation der Moduln wenden, erinnern wir zunächst an die beiden allgemeinen, in § 170 (S. 72) bewiesenen Sätze

$$\mathfrak{m}\mathfrak{n} = \mathfrak{m}, \quad \mathfrak{n}^2 = \mathfrak{n}, \tag{15}$$

welche sich auch leicht durch die wirkliche Multiplikation aus (2) und (7) ergeben. Von besonderer Wichtigkeit ist die Bildung des Produktes $\mathfrak{m}\mathfrak{m}'$ aus zwei konjugierten Moduln; durch Multiplikation von (2) und (12) erhält man zunächst

$$\mathfrak{m}\mathfrak{m}' = m^2[1, \omega, \omega', \omega\omega'];$$

addiert man die zweite Basiszahl zur dritten, so folgt aus (11)

$$\mathfrak{m}\mathfrak{m}' = \frac{m^2}{a}[a, a\omega, b, c],$$

und da $[a, b, c] = [1]$ ist, so erhalten wir das Resultat*)

$$\mathfrak{m}\mathfrak{m}' = \frac{m^2}{a}[1, a\omega] = \mathfrak{n}N(\mathfrak{m}); \tag{16}$$

mithin ist $\mathfrak{m}$ (nach § 170, V) ein eigentlicher Modul, und zugleich ergibt sich

$$\mathfrak{m}' = \mathfrak{m}^{-1}N(\mathfrak{m}). \tag{17}$$

Wir betrachten jetzt ein Produkt aus zwei beliebigen Moduln $\mathfrak{m}$, $\mathfrak{m}_1$ und setzen

$$\mathfrak{m}\mathfrak{m}_1 = \mathfrak{m}_2; \tag{18}$$

*) Es ist wohl von Nutzen, hier zu bemerken, daß schon bei Körpern dritten Grades ein ähnlicher Satz nicht in voller Allgemeinheit gilt, und dasselbe ist von mehreren der nachfolgenden Sätze zu sagen.

da $\mathfrak{m}_2$ aus allen Zahlen μ_2 von der Form $\Sigma \mu \mu_1$ besteht, so besteht der konjugierte Modul $\mathfrak{m}_2'$ aus allen Zahlen μ_2' von der Form $\Sigma \mu' \mu_1'$, und folglich ist

$$\mathfrak{m}' \mathfrak{m}_1' = \mathfrak{m}_2' = (\mathfrak{m}\mathfrak{m}_1)'.$$

Durch Multiplikation dieser beiden Gleichungen erhält man zufolge (16)

$$\mathfrak{n}\mathfrak{n}_1 N(\mathfrak{m}) N(\mathfrak{m}_1) = \mathfrak{n}_2 N(\mathfrak{m}_2),$$

wo $\mathfrak{n}_1$, $\mathfrak{n}_2$ die Ordnungen von $\mathfrak{m}_1$, $\mathfrak{m}_2$ bedeuten; da nun das Produkt $\mathfrak{n}\mathfrak{n}_1$ nur ganze Zahlen und offenbar auch die Zahl 1 enthält, so ist es nach dem Obigen wieder eine Ordnung; die vorstehende Gleichung liefert daher, wenn man auf die beiderseits auftretenden rationalen Zahlen achtet, zunächst den Satz*)

$$N(\mathfrak{m}) N(\mathfrak{m}_1) = N(\mathfrak{m}_2) = N(\mathfrak{m}\mathfrak{m}_1), \tag{19}$$

mithin auch den folgenden

$$\mathfrak{n}\mathfrak{n}_1 = \mathfrak{n}_2; \tag{20}$$

die Norm eines Produktes ist daher gleich dem Produkte aus den Normen der Faktoren, und ebenso ist die Ordnung eines Produktes gleich dem Produkte aus den Ordnungen der Faktoren (vgl. § 170, VIII).

Da die Zahl 1 in jeder Ordnung enthalten ist, so ist das Produkt $\mathfrak{n}\mathfrak{n}_1$ ein gemeinschaftlicher Teiler von $\mathfrak{n}$ und $\mathfrak{n}_1$, und zwar, wie

*) Will man auch bei Körpern höheren Grades den Begriff der Norm $N(\mathfrak{m})$ jedes endlichen Moduls $\mathfrak{m}$, dessen Basis zugleich eine Basis des Körpers ist, so fassen, daß der Satz (19) allgemein gilt, und daß, falls $\mathfrak{m}$ ein Ideal ist, $N(\mathfrak{m})$ die alte Bedeutung $(\mathfrak{o}, \mathfrak{m})$ behält, so muß man, weil $N(\mathfrak{o}) = 1$ und $\mathfrak{o}\mathfrak{m}$ ein Idealbruch ist, die obige Definition (9) durch

$$N(\mathfrak{m}) = N(\mathfrak{o}\mathfrak{m}) = \frac{(\mathfrak{o}, \mathfrak{o}\mathfrak{m})}{(\mathfrak{o}\mathfrak{m}, \mathfrak{o})}$$

ersetzen (vgl. die Anm. auf S. 131). Daß schon bei Körpern dritten Grades diese beiden Definitionen nicht übereinstimmen, lehrt folgendes einfache Beispiel. Ist $\alpha^3 = 2$, so ist $\mathfrak{o} = [1, \alpha, \alpha^2]$ der Inbegriff aller ganzen Zahlen des aus α gebildeten Körpers $R(\alpha)$; ist nun m eine ungerade Zahl und > 1, ferner $\mathfrak{m} = [m, \alpha, \alpha^2]$, so wird $\mathfrak{o}\mathfrak{m} = \mathfrak{o}$, also $(\mathfrak{o}, \mathfrak{o}\mathfrak{m}) = (\mathfrak{o}\mathfrak{m}, \mathfrak{o}) = 1$; andererseits ist die Ordnung $\mathfrak{m}^0 = [1, m\alpha, m\alpha^2]$, also $\mathfrak{m} + \mathfrak{m}^0 = \mathfrak{o}$, $(\mathfrak{m}^0, \mathfrak{m}) = (\mathfrak{o}, \mathfrak{m}) = m$, $(\mathfrak{m}, \mathfrak{m}^0) = (\mathfrak{o}, \mathfrak{m}^0) = m^2$, woraus unsere Behauptung einleuchtet; die dem Modul $\mathfrak{m}$ entsprechende zerlegbare Form (S. 156) ist auch nicht ursprünglich, sondern sie besitzt den Teiler m. Man findet ferner $\mathfrak{m}^{-1} = \mathfrak{m}\mathfrak{m}^{-1} = \mathfrak{m}^0 : \mathfrak{o} = \mathfrak{o}m$, also ist $\mathfrak{m}$ ein uneigentlicher Modul (S. 73). Da zugleich $\mathfrak{m}^2 = \mathfrak{o}$, also $(\mathfrak{m}\mathfrak{m})^0$ nicht $= \mathfrak{m}^0\mathfrak{m}^0 = \mathfrak{m}^0$, sondern $= \mathfrak{o}$ ist, so gilt auch der obige Satz (20) nicht allgemein für Körper höheren Grades.

wir jetzt zeigen wollen, ihr größter gemeinschaftlicher Teiler. Bedeuten k, k_1, k_2 die Indizes der Ordnungen $\mathfrak{n}$, $\mathfrak{n}_1$, $\mathfrak{n}_2$, so ist $\mathfrak{n} = [1, k\theta]$, $\mathfrak{n}_1 = [1, k_1\theta]$, und folglich

$$\mathfrak{n}\mathfrak{n}_1 = [1, k\theta, k_1\theta, kk_1\theta^2];$$

da aber $\theta^2 = D\theta - D_1$ ist, wo D_1 eine ganze rationale Zahl, so kann die letzte Basiszahl $kk_1\theta^2$, weil sie eine Summe von Vielfachen der beiden ersten ist, weggelassen werden, und man erhält

$$\mathfrak{n}\mathfrak{n}_1 = [1, k\theta, k_1\theta] = \mathfrak{n} + \mathfrak{n}_1, \tag{21}$$

wie behauptet war. Da nun dasselbe Produkt zufolge (20) auch $= [1, k_2\theta]$ ist, so folgt, daß der Index k_2 des Produktes der größte gemeinschaftliche Teiler der Indizes k, k_1 der Faktoren ist. Bedeuten ferner d, d_1, d_2 die Diskriminanten von $\mathfrak{n}$, $\mathfrak{n}_1$, $\mathfrak{n}_2$, so ist $d = Dk^2$, $d_1 = Dk_1^2$, $d_2 = Dk_2^2$, und folglich ist die Diskriminante des Produktes auch der größte gemeinschaftliche Teiler von den Diskriminanten der Faktoren.

Die letzten Sätze ergeben sich auch auf folgende Weise, wobei wir den Buchstaben m_1, ω_1, a_1, b_1, c_1 und m_2, ω_2, a_2, b_2, c_2 dieselbe Bedeutung für die Moduln $\mathfrak{m}_1$ und $\mathfrak{m}_2$ beilegen, welche m, ω, a, b, c für $\mathfrak{m}$ haben. Dann ist zufolge (20)

$$[1, a_2\omega_2] = [1, a\omega]\,[1, a_1\omega_1] = [1, a\omega, a_1\omega_1, aa_1\omega\omega_1],$$

und es gelten daher (nach § 172) vier Gleichungen von der Form

$$\begin{aligned} 1 &= 1\cdot 1 + 0\cdot a_2\omega_2 \\ a\omega &= f\cdot 1 + e\cdot a_2\omega_2 \\ a_1\omega_1 &= f_1\cdot 1 + e_1\cdot a_2\omega_2 \\ aa_1\omega\omega_1 &= f_2\cdot 1 + e_2\cdot a_2\omega_2, \end{aligned} \tag{22}$$

wo die acht Koeffizienten rechts solche ganze rationale Zahlen sind, daß die sechs aus ihnen gebildeten Determinanten

$$e,\ e_1,\ e_2,\ fe_1 - ef_1,\ fe_2 - ef_2,\ f_1e_2 - e_1f_2$$

keinen gemeinschaftlichen Teiler haben; da aber jeder gemeinschaftliche Teiler der drei ersten auch in den folgenden aufgeht, so folgt, daß e, e_1, e_2 keinen gemeinschaftlichen Teiler haben. Zufolge (22) ist ferner

$$(f + ea_2\omega_2)(f_1 + e_1a_2\omega_2) = f_2 + e_2a_2\omega_2,$$

also

$$ee_1(a_2\omega_2)^2 - (e_2 - ef_1 - e_1f)(a_2\omega_2) + ff_1 - f_2 = 0;$$

vergleicht man dies mit der Gleichung

$$(a_2\,\omega_2)^2 - b_2\,(a_2\,\omega_2) + a_2\,c_2 = 0,$$

so ergibt sich

(23) $$e_2 = e\,f_1 + e_1\,f + e\,e_1\,b_2,\quad f_2 = f\,f_1 - e\,e_1\,a_2\,c_2;$$

aus der ersten dieser beiden Gleichungen folgt, daß jeder gemeinschaftliche Teiler von e, e_1 auch in e_2 aufgeht; da aber oben gezeigt ist, daß diese drei Zahlen keinen gemeinschaftlichen Teiler haben, so sind e, e_1 relative Primzahlen. Ersetzt man nun in (22) die Größen $a\,\omega$, $a_1\,\omega_1$, $a_2\,\omega_2$ gemäß (5) durch

$$\frac{b + k\sqrt{D}}{2},\quad \frac{b_1 + k_1\sqrt{D}}{2},\quad \frac{b_2 + k_2\sqrt{D}}{2},$$

so ergibt sich

(24) $$k = e\,k_2,\quad k_1 = e_1\,k_2,\quad (\mathfrak{n}_1,\,\mathfrak{n}) = e,\quad (\mathfrak{n},\,\mathfrak{n}_1) = e_1,$$

also auch

(25) $$d = d_2\,e^2,\quad d_1 = d_2\,e_1^2,$$

und außerdem

(26) $$f = \frac{b - b_2\,e}{2},\quad f_1 = \frac{b_1 - b_2\,e_1}{2};$$

ebenso erhält man aus der letzten der Gleichungen (22), oder indem man die vorstehenden Ausdrücke in (23) substituiert,

(27) $$e_2 = \frac{b\,e_1 + b_1\,e}{2},\quad f_2 = \frac{b\,b_1 + d_2\,e\,e_1 - 2\,b_2\,e_2}{4}.$$

Aus (24) und (25) folgt abermals, daß k_2 der größte gemeinschaftliche Teiler von k, k_1, und ebenso d_2 derjenige von d, d_1 ist.

Sind also die beiden Moduln $\mathfrak{m}$, $\mathfrak{m}_1$ gegeben, so findet man die Zahlen e, e_1, k_2, d_2 aus (24) und (25) durch die Bedingung, daß e, e_1 relative Primzahlen sein müssen, und hiermit ist auch e_2 zufolge (27) gefunden. Wir wollen nun dazu übergehen, den Modul $\mathfrak{m}_2$ vollständig zu bestimmen, indem wir auch die Zahlen m_2, a_2, b_2, c_2 aus den Daten ableiten. Da das Produkt $m\,m_1$ in $\mathfrak{m}_2$ und folglich auch in $[m_2]$ enthalten ist, so kann man zunächst

(28) $$m\,m_1 = p\,m_2,\quad m_2 = \frac{m\,m_1}{p}$$

setzen, wo p eine natürliche Zahl bedeutet; ersetzt man nun die im Satze (19) auftretenden Normen durch ihre Ausdrücke gemäß (10), so erhält man

(29) $$a\,a_1 = p^2\,a_2,\quad a_2 = \frac{a\,a_1}{p^2},$$

mithin ist die Bestimmung von m_2 und a_2 auf diejenige von p zurückgeführt. Ersetzt man ferner die Moduln $\mathfrak{m}$, $\mathfrak{m}_1$, $\mathfrak{m}_2$ durch ihre Ausdrücke gemäß (2), so nimmt die Gleichung $\mathfrak{m}_2 = \mathfrak{m}\mathfrak{m}_1$ die Form

$$[1, \omega_2] = p[1, \omega][1, \omega_1] = p[1, \omega_1, \omega, \omega\omega_1] \tag{30}$$

an; man kann daher (nach § 172)

$$\begin{aligned} p &= p \cdot 1 + 0 \cdot \omega_2 \\ p\omega_1 &= p' \cdot 1 + q' \cdot \omega_2 \\ p\omega &= p'' \cdot 1 + q'' \cdot \omega_2 \\ p\omega\omega_1 &= p''' \cdot 1 + q''' \cdot \omega_2 \end{aligned} \tag{31}$$

setzen, wo die acht Koeffizienten rechter Hand solche ganze rationale Zahlen sind, daß die sechs aus ihnen gebildeten Determinanten

$$pq', \; pq'', \; pq''', \; p'q'' - q'p'', \; p'q''' - q'p''', \; p''q''' - q''p''',$$

also jedenfalls auch die drei Zahlen q', q'', q''' keinen gemeinschaftlichen Teiler haben*). Substituiert man nun in (31) für ω, ω_1, $\omega\omega_1$ die aus (22) folgenden Ausdrücke, so erhält man die Gleichungen

$$\begin{aligned} p(f_1 + e_1 a_2 \omega_2) &= a_1(p' + q'\omega_2) \\ p(f + e a_2 \omega_2) &= a(p'' + q''\omega_2) \\ p(f_2 + e_2 a_2 \omega_2) &= a a_1(p''' + q'''\omega_2), \end{aligned}$$

welche, weil ω_2 irrational ist, in die folgenden zerfallen

$$pe_1 a_2 = a_1 q', \quad pe a_2 = a q'', \quad pe_2 a_2 = a a_1 q''' \tag{32}$$

$$pf_1 = a_1 p', \quad pf = a p'', \quad pf_2 = a a_1 p'''. \tag{33}$$

Substituiert man in (32) für a_2 den in (29) angegebenen Ausdruck, so erhält man

$$a e_1 = pq', \quad a_1 e = pq'', \quad e_2 = pq''', \tag{34}$$

und da q', q'', q''', wie oben bemerkt, keinen gemeinschaftlichen Teiler haben, so ist p offenbar als größter (positiver) gemeinschaftlicher Teiler der drei bekannten Zahlen $a e_1$, $a_1 e$, e_2 vollständig bestimmt, und dasselbe gilt mithin von den drei Zahlen q', q'', q''', sowie von den beiden Zahlen m_2, a_2, welche sich aus (28) und (29) ergeben. Multipliziert man ferner die Gleichungen (33) mit $2a$, $2a_1$, 2, und ersetzt $a a_1$ durch $p^2 a_2$, so erhält man mit Rücksicht auf (34), wenn

*) Hieraus folgt in Verbindung mit der aus (31) leicht abzuleitenden Gleichung $q'\omega + q''\omega_1' = q''' = q'\omega' + q''\omega_1$ ein für die Theorie der komplexen Multiplikation der elliptischen Funktionen sehr wichtiger Satz (vgl. meinen Aufsatz (§ 7) über die Theorie der elliptischen Modul-Funktionen in Crelles Journal, Bd. 83 [XIV dieser Ausgabe]).

man für f_1, f, f_2 die in (26) und (27) angegebenen Ausdrücke substituiert, die Gleichungen

$$\frac{a\,b_1}{p} - q'\,b_2 = 2\,a_2\,p', \quad \frac{a_1\,b}{p} - q''\,b_2 = 2\,a_2\,p'',$$
$$\frac{b\,b_1 + d_2\,e\,e_1}{2\,p} - q'''\,b_2 = 2\,a_2\,p''',$$

also die Kongruenzen

$$\left.\begin{aligned} q'\,b_2 &\equiv \frac{a\,b_1}{p} \\ q''\,b_2 &\equiv \frac{a_1\,b}{p} \\ q'''\,b_2 &\equiv \frac{b\,b_1 + d_2\,e\,e_1}{2\,p} \end{aligned}\right\} \pmod{2\,a_2}, \tag{35}$$

durch welche die Zahl b_2 nach dem Modul $2\,a_2$ vollständig bestimmt ist, weil q', q'', q''' keinen gemeinschaftlichen Teiler haben (vgl. § 145); und hieraus ergibt sich endlich auch c_2 durch die Gleichung

$$c_2 = \frac{b_2^2 - d_2}{4\,a_2}. \tag{36}$$

Hiermit ist die Bestimmung des Produktes $\mathfrak{m}_2$ aus den beiden Faktoren $\mathfrak{m}$, $\mathfrak{m}_1$ vollendet, und wir haben nur noch die folgende Bemerkung hinzuzufügen. Da die Existenz des Moduls $\mathfrak{m}_2 = \mathfrak{m}\,\mathfrak{m}_1$ von vornherein gewiß ist, so müssen wir schließen, daß die in (26), (27), (29), (35) und (36) in Form von Brüchen auftretenden Zahlen in Wahrheit ganze Zahlen, daß ferner die drei Kongruenzen (35) wirklich miteinander vereinbar sind, und daß die so erhaltenen Zahlen a_2, b_2, c_2 keinen gemeinschaftlichen Teiler haben; dies alles würde sich auch auf direktem Wege leicht beweisen lassen, was wir jedoch dem Leser überlassen wollen*).

Wir bezeichnen nun mit x, y und x_1, y_1 zwei Systeme von unabhängigen Variablen und bilden die bilinearen Funktionen

$$\begin{aligned} x_2 &= p\,x\,x_1 + p'\,x\,y_1 + p''\,y\,x_1 + p'''\,y\,y_1 \\ y_2 &= \qquad\quad q'\,x\,y_1 + q''\,y\,x_1 + q'''\,y\,y_1; \end{aligned} \tag{37}$$

setzt man ferner

$$\mu = m(x + y\,\omega), \quad \mu_1 = m_1(x_1 + y_1\,\omega_1), \quad \mu_2 = m_2(x_2 + y_2\,\omega_2),$$

*) Vgl. Arndt: Auflösung einer Aufgabe in der Komposition der quadratischen Formen (Crelles Journal, Bd. 56).

so folgt aus (28) und (31), daß $\mu_2 = \mu\mu_1$, also für rationale Werte der Variablen auch $N(\mu_2) = N(\mu)N(\mu_1)$ ist; ersetzt man diese Normen durch ihre Ausdrücke gemäß (14) und berücksichtigt (19), so ergibt sich

$$(38) \qquad \begin{aligned} &a_2 x_2^2 + b_2 x_2 y_2 + c_2 y_2^2 \\ &= (a x^2 + b x y + c y^2)(a_1 x_1^2 + b_1 x_1 y_1 + c_1 y_1^2); \end{aligned}$$

man sagt daher, die Form $(a_2, \frac{1}{2}b_2, c_2)$ gehe durch die bilineare Substitution (37) in das Produkt der beiden Formen $(a, \frac{1}{2}b, c)$ und $(a_1, \frac{1}{2}b_1, c_1)$ über, und nennt die erste Form zusammengesetzt aus den beiden letzteren*); offenbar ist (38) infolge von (37) eine Identität, welche für beliebige Werte der unabhängigen Variablen gilt. —

Die vorstehende Darstellung der Multiplikation der Moduln bildet zugleich die Grundlage für die Behandlung der umgekehrten Aufgabe, alle Moduln $\mathfrak{m}$ zu finden, welche der Bedingung $\mathfrak{m}\mathfrak{m}_1 = \mathfrak{m}_2$ genügen, wo $\mathfrak{m}_1$ und $\mathfrak{m}_2$ gegebene Moduln bedeuten. Wir beschränken uns aber hier darauf, einige Hauptpunkte dieser äußerst wichtigen Untersuchung hervorzuheben, und überlassen die weitere Ausführung dem Leser. Aus (20) folgt, daß, wenn die Aufgabe lösbar sein soll, die Ordnung n_1 des Moduls $\mathfrak{m}_1$ durch die Ordnung n_2 des Moduls $\mathfrak{m}_2$ teilbar sein muß; diese erforderliche Bedingung, welche im folgenden stets als erfüllt vorausgesetzt wird und auch durch $n_1 n = n_2$ oder $k_1 = e_1 k_2$ ausgedrückt werden kann, ist aber auch hinreichend, und es gibt dann immer unendlich viele Moduln $\mathfrak{m}$, welche die Bedingung $\mathfrak{m}\mathfrak{m}_1 = \mathfrak{m}_2$ erfüllen. Zunächst findet man nach (16) oder (17) durch Multiplikation mit $\mathfrak{m}_1'$ oder $\mathfrak{m}_1^{-1}$ leicht den Hauptsatz, daß es immer einen und nur einen solchen Modul $\mathfrak{m}$ gibt, dessen Ordnung $= n_2$ ist; bezeichnet man diesen gegebenen Modul $\mathfrak{m}_2\mathfrak{m}_1^{-1}$ der Kürze halber wieder mit $\mathfrak{m}_2$, so wird zugleich die allgemeine Aufgabe auf den speziellen Fall zurückgeführt, in welchem $\mathfrak{m}_1 = n_1$ ist, und man braucht sich nur noch mit der Lösung der Gleichung $\mathfrak{m} n_1 = \mathfrak{m}_2$ zu beschäftigen. Die Ordnung n des Moduls $\mathfrak{m}$ muß so

*) Vgl. § 146. Die allgemeinste Art der Komposition der binären quadratischen Formen, wie sie von Gauß dargestellt ist (D. A. artt. 235, 236), erhält man, wenn man statt der speziellen Darstellungsform (2) der Moduln die allgemeinere Form (1) zugrunde legt; dies ist in § 170 der zweiten Auflage dieses Werkes (1871) geschehen, wo ich auch für die quadratischen Formen schon den Ausdruck $(a, \frac{1}{2}b, c)$ statt (a, b, c) gewählt habe (vgl. die Anmerkung auf S. 388 [von Dirichlets Vorlesungen über Zahlentheorie] und eine Mitteilung von Kronecker im Sitzungsbericht der Berliner Akademie vom 30. Juli 1885).

beschaffen sein, daß $\mathfrak{n}_2 = \mathfrak{n}\mathfrak{n}_1$ der größte gemeinschaftliche Teiler von $\mathfrak{n}$ und $\mathfrak{n}_1$, also $k = ek_2$ wird, wo e relative Primzahl zu e_1 ist; nachdem man für den Modul $\mathfrak{m}$ eine solche Ordnung $\mathfrak{n}$, also auch eine solche Zahl e willkürlich gewählt hat, leuchtet ein, daß stets $\mathfrak{m}\mathfrak{n}_1 = \mathfrak{m}\mathfrak{n}_2$ ist, und es kommt daher nur darauf an, alle Moduln $\mathfrak{m}$ von dieser Ordnung $\mathfrak{n}$ zu finden, welche der Bedingung $\mathfrak{m}\mathfrak{n}_2 = \mathfrak{m}_2$ genügen. Um nachzuweisen, daß mindestens ein solcher Modul $\mathfrak{m}$ existiert, wähle man die in $\mathfrak{m}_2 = m_2\,[1, \omega_2]$ auftretende Zahl ω_2 so, daß c_2 relative Primzahl zu a_2 wird, was nach einer früheren Bemerkung stets möglich ist; setzt man alsdann die vorher gewählte Zahl $e = pq''$, wo q'' den größten Divisor von e bedeutet, welcher relative Primzahl zu a_2 ist, so findet man leicht, daß der Modul $\mathfrak{m} = m_2[p, q''\omega_2]$ der Bedingung $\mathfrak{m}\mathfrak{n}_2 = \mathfrak{m}_2$ genügt, und daß $\mathfrak{n}$ seine Ordnung ist. Um aus diesem einen Modul $\mathfrak{m}$ alle anderen zu finden, benutze man den schon vorher bewiesenen Satz, daß, wenn $\mathfrak{b}$, $\mathfrak{c}$ zwei beliebige Moduln von gleicher Ordnung $\mathfrak{n}$ sind, es immer einen und nur einen Modul $\mathfrak{a} = \mathfrak{c}\mathfrak{b}^{-1}$ von derselben Ordnung $\mathfrak{n}$ gibt, welcher der Bedingung $\mathfrak{a}\mathfrak{b} = \mathfrak{c}$ genügt; hierdurch wird die vollständige Lösung unserer Gleichung $\mathfrak{m}\mathfrak{n}_2 = \mathfrak{m}_2$ auf den speziellen Fall $\mathfrak{m}_2 = \mathfrak{n}_2$, also auf die Aufgabe zurückgeführt, alle Moduln $\mathfrak{m}$ von der Ordnung $\mathfrak{n}$ zu finden, welche der Bedingung

$$\mathfrak{m}\mathfrak{n}_2 = \mathfrak{n}_2 \tag{39}$$

genügen. Da nun, wenn $\mathfrak{o}$ die frühere Bedeutung hat, immer $\mathfrak{o}\mathfrak{n}_2 = \mathfrak{o}$ ist, so genügt ein solcher Modul $\mathfrak{m}$ gewiß auch der Bedingung

$$\mathfrak{m}\mathfrak{o} = \mathfrak{o}; \tag{40}$$

diese Moduln, zu welchen offenbar $\mathfrak{n}$ selbst gehört, sind von besonderer Wichtigkeit, und wir wollen jeden Modul $\mathfrak{m}$ von der Ordnung $\mathfrak{n}$, welcher diese letzte Bedingung erfüllt, aus einem sogleich anzugebenden Grunde eine Wurzel der Ordnung $\mathfrak{n}$ nennen; es ist zweckmäßig, zunächst alle diese Wurzeln von $\mathfrak{n}$ zu bestimmen, worauf es keine Schwierigkeit haben wird, diejenigen von ihnen auszusondern, welche auch die Bedingung (39) erfüllen.

Da die Zahl 1 in $\mathfrak{o}$ enthalten, also immer $\mathfrak{m} > \mathfrak{m}\mathfrak{o}$ ist [§ 170, (22)], so folgt aus (40) zunächst

$$\mathfrak{m} \geqq \mathfrak{o}, \tag{41}$$

also besteht jede Wurzel $\mathfrak{m}$ aus lauter ganzen Zahlen. Da ferner $\mathfrak{n} = \mathfrak{m} : \mathfrak{m}$, und allgemein $(\mathfrak{c} : \mathfrak{a}) : \mathfrak{b} = \mathfrak{c} : \mathfrak{a}\mathfrak{b}$ ist [§ 170, (17)], so folgt aus (8) und (40) auch $\mathfrak{o}k = \mathfrak{n} : \mathfrak{o} = (\mathfrak{m} : \mathfrak{m}) : \mathfrak{o} = \mathfrak{m} : \mathfrak{m}\mathfrak{o} = \mathfrak{m} : \mathfrak{o}$, also

$$\frac{\mathfrak{m}}{\mathfrak{o}} = \mathfrak{o}k, \tag{42}$$

mithin [nach § 170, (14)] auch

$$\mathfrak{o}k > \mathfrak{m}. \tag{43}$$

Da außerdem $(\mathfrak{o}, \mathfrak{o}k) = N(k) = k^2 > 0$ ist, so folgt aus (41) und (43), daß die Anzahl der Wurzeln $\mathfrak{m}$ der Ordnung $\mathfrak{n}$ endlich ist (§ 171, II); diese Anzahl wollen wir mit l bezeichnen. Aus der Definition (40) folgt ferner unmittelbar, daß diese l Wurzeln insofern eine Gruppe bilden, als jedes Produkt aus zwei solchen Wurzeln wieder eine Wurzel derselben Ordnung $\mathfrak{n}$ ist, und hieraus ergibt sich durch die schon oft angewendete Schlußweise (vgl. § 149), daß für jede Wurzel $\mathfrak{m}$ der Ordnung $\mathfrak{n}$ der Satz

$$\mathfrak{m}^l = \mathfrak{n} \tag{44}$$

gilt. Umgekehrt, sobald unter den Potenzen $\mathfrak{m}, \mathfrak{m}^2, \mathfrak{m}^3 \ldots$ eines Moduls $\mathfrak{m}$ sich eine Ordnung $\mathfrak{n} = \mathfrak{m}^r$ vorfindet, so ist $\mathfrak{n}$ zufolge (20) auch die Ordnung von $\mathfrak{m}$; da ferner die r^{te} Potenz einer jeden in $\mathfrak{m}$ enthaltenen Zahl auch in $\mathfrak{n}$ enthalten, also eine ganze Zahl ist, so besteht $\mathfrak{m}$ (nach § 173, V) aus lauter ganzen Zahlen; mithin ist $\mathfrak{m}\mathfrak{o}$ ein Ideal, und da $(\mathfrak{m}\mathfrak{o})^r = \mathfrak{n}\mathfrak{o}^r = \mathfrak{o}$ ist, so folgt auch $\mathfrak{m}\mathfrak{o} = \mathfrak{o}$, also ist $\mathfrak{m}$ eine Wurzel der Ordnung $\mathfrak{n}$, womit zugleich die eingeführte Benennung gerechtfertigt ist.

Der oben aus der allgemeinen Modultheorie (§ 170) abgeleitete Satz (43) bestätigt sich auch durch die Rechnung, wenn man für $\mathfrak{m}$ die in (2), (3), (5) eingeführten Bezeichnungen beibehält. Setzt man noch $m\omega = \alpha$, so sind die Basiszahlen des Moduls

$$\mathfrak{m} = [m, \alpha] \tag{45}$$

zufolge (41) ganze Zahlen, und aus (40), (19) und (10) ergibt sich $N(\mathfrak{m}) = 1$, also $a = m^2$; hieraus folgt weiter, daß b durch m teilbar, mithin c relative Primzahl zu m ist; da aber $c = aN(\omega) = N(\alpha) = \alpha\alpha'$ ist, so sind die Basiszahlen m, α ebenfalls relative Primzahlen, was auch unmittelbar aus (40), nämlich aus

$$\mathfrak{o}m + \mathfrak{o}\alpha = \mathfrak{o} \tag{46}$$

folgt; da nach (7) außerdem

$$\mathfrak{n} = [1, m\alpha] \tag{47}$$

ist, so geht m in dem Index k auf, und wenn

$$\alpha = t + u\theta \tag{48}$$

gesetzt wird, so ist $k = um$, $k\theta = -tm + m\alpha$, woraus wirklich (43) und zugleich

$$(\mathfrak{o}, \mathfrak{m}) = (\mathfrak{m}, \mathfrak{o}k) = k \tag{49}$$

folgt. Umgekehrt, wenn eine natürliche Zahl m relative Primzahl zu der irrationalen Zahl α (also auch zu deren Norm c) ist, so hat, wie man leicht findet, der Modul (45) die Ordnung (47), und aus (46) folgt (40), mithin ist $\mathfrak{m}$ eine Wurzel von $\mathfrak{n}$*).

Um nun die Anzahl l zu bestimmen, ist es zweckmäßig, die Darstellung (45) in eine andere Form zu bringen, aus welcher man die wahre Natur und die gegenseitigen Beziehungen der Wurzeln $\mathfrak{m}$ noch deutlicher erkennen wird. Hierzu bemerke man, daß unter den in $\mathfrak{m}$ enthaltenen Zahlen sich auch solche finden, die relative Primzahlen zu k sind; denn weil $\alpha = t + u\theta$ schon relative Primzahl zu m ist, und folglich m, t, u keinen gemeinschaftlichen Teiler haben, so kann man die ganze rationale Zahl z so wählen, daß $t + mz$ relative Primzahl zu u wird, und hieraus folgt, daß die Zahl $\alpha + mz$ (welche auch statt α als zweite Basiszahl von $\mathfrak{m}$ dienen könnte) relative Primzahl zu m und u, also auch zu $k = mu$ ist. Wählt man nun aus $\mathfrak{m}$ nach Belieben eine Zahl ϱ, welche relative Primzahl zu k ist, so sind auch die k Zahlen ϱ, 2ϱ, 3ϱ ... $k\varrho$ in $\mathfrak{m}$ enthalten, und da sie inkongruent nach k sind, so bilden sie zufolge (49) ein Restsystem von $\mathfrak{m}$ nach $\mathfrak{o}k$, und hieraus folgt mit Rücksicht auf (43) die neue Darstellung

$$\mathfrak{m} = [k, k\theta, \varrho] = \mathfrak{o}k + [\varrho]. \tag{50}$$

Umgekehrt, wenn $\varrho = r + s\theta$ eine beliebige relative Primzahl zu k ist, so findet man durch Reduktion des vorstehenden Moduls $\mathfrak{m}$ auf eine zweigliedrige Basis m, α, daß $k = mu$, und $\alpha = t + u\theta$ relative Primzahl zu m ist, woraus nach dem Obigen folgt, daß $\mathfrak{m}$ eine Wurzel der Ordnung $\mathfrak{n} = [1, k\theta]$ ist. Jede Wurzel $\mathfrak{m}$ der Ordnung $\mathfrak{n}$ ist also durch eine beliebige in ihr enthaltene Zahl ϱ vollständig be-

*) Zugleich ist $\mathfrak{m}[1, \alpha] = [1, \alpha]$, und damit $\mathfrak{m}$ auch der Bedingung (39) genüge, ist erforderlich und hinreichend, daß die Ordnung $[1, \alpha]$ durch die Ordnung $\mathfrak{n}_2$ teilbar sei.

stimmt, welche relative Primzahl zum Index k ist, und man kann daher diese Wurzel $\mathfrak{n}$ zweckmäßig durch das Symbol $\mathfrak{n}_\varrho$ bezeichnen; ist σ ebenfalls relative Primzahl zu k, so gilt dasselbe von $\varrho\,\sigma$, und da dieses Produkt in dem Produkte $\mathfrak{n}_\varrho\,\mathfrak{n}_\sigma$ enthalten ist, so ergibt sich

$$\mathfrak{n}_\varrho\,\mathfrak{n}_\sigma = \mathfrak{n}_{\varrho\sigma}, \tag{51}$$

worin das Gesetz der Multiplikation der Wurzeln von $\mathfrak{n}$ seinen einfachsten Ausdruck findet. Sollen ferner die beiden Zahlen ϱ und σ eine und dieselbe Wurzel $\mathfrak{n}_\varrho = \mathfrak{n}_\sigma$ erzeugen, so ist erforderlich und hinreichend, daß $\sigma \equiv r\,\varrho$, $\varrho \equiv s\,\sigma \pmod{k}$ sei, wo r, s ganze rationale Zahlen bedeuten; hieraus folgt aber $r\,s \equiv 1 \pmod{k}$, also muß r relative Primzahl zu k sein; und umgekehrt, wenn $\sigma \equiv r\,\varrho \pmod{k}$ ist, wo r eine ganze rationale Zahl bedeutet, welche relative Primzahl zu k ist, so ist gewiß $\mathfrak{n}_\sigma = \mathfrak{n}_\varrho$. Es gibt mithin (nach § 18) in bezug auf k immer genau $\varphi(k)$ verschiedene Zahlklassen, welche aus lauter Zahlen ϱ bestehen, die relative Primzahlen zu k sind und alle eine und dieselbe Wurzel $\mathfrak{n}_\varrho$ der Ordnung $\mathfrak{n}$ erzeugen; bezeichnet man daher (nach § 180) mit $\varphi(\mathfrak{o}\,k)$ die Anzahl aller nach k inkongruenten Zahlen ϱ in $\mathfrak{o}$, welche relative Primzahlen zu k sind, so ergibt sich für die Anzahl l aller verschiedenen Wurzeln $\mathfrak{n}_\varrho$ der Ordnung $\mathfrak{n}$ der Ausdruck

$$l = \frac{\varphi(\mathfrak{o}\,k)}{\varphi(k)}. \tag{52}$$

Hierin ist nun

$$\varphi(k) = k\,\Pi\left(1 - \frac{1}{p}\right),$$

wo das Produkt über alle verschiedenen, in k aufgehenden rationalen Primzahlen p auszudehnen ist; andererseits ist [nach § 180, (26)]

$$\varphi(\mathfrak{o}\,k) = k^2\,\Pi\left(1 - \frac{1}{N(\mathfrak{p})}\right),$$

wo das Produktzeichen sich auf alle verschiedenen, in k aufgehenden Primideale $\mathfrak{p}$ bezieht; ordnet man die Faktoren nach den rationalen Primzahlen p, in denen diese Primideale aufgehen, und legt dem Symbol (D, p) die im vorigen Paragraphen festgesetzte Bedeutung bei, so erhält man

$$\varphi(\mathfrak{o}\,k) = k^2\,\Pi\left(1 - \frac{1}{p}\right)\left(1 - \frac{(D, p)}{p}\right)$$

und folglich

$$l = k\,\Pi\left(1 - \frac{(D, p)}{p}\right). \tag{53}$$

Nachdem hiermit die Anzahl aller Wurzeln $\mathfrak{m}$ der Ordnung n bestimmt ist, findet man leicht die Anzahl aller derjenigen unter ihnen, welche der obigen Bedingung (39) genügen, wo n_2 eine gegebene, in n aufgehende Ordnung bedeutet; multipliziert man nämlich alle l Wurzeln der Ordnung n mit n_2, so werden alle l_2 Wurzeln von n_2, und zwar jede gleich oft erzeugt; mithin ist die gesuchte Anzahl $= l : l_2$, und nach der obigen Untersuchung ist dies zugleich die Anzahl aller verschiedenen Moduln $\mathfrak{m}$ von der Ordnung n, welche der ursprünglich vorgelegten Bedingung $\mathfrak{m}\mathfrak{m}_1 = \mathfrak{m}_2$ genügen.

Die binären Formen $(a, \frac{1}{2}b, c) = (m^2, \frac{1}{2}mb_0, c)$, welche nach (14) den Wurzeln $\mathfrak{m} = [m, \alpha]$ der Ordnung n entsprechen, stimmen offenbar mit denjenigen überein, auf welche wir früher (§§ 150, 151) bei der Bestimmung der Anzahl der Formenklassen von beliebiger Ordnung geführt sind. Den Grund dieser Übereinstimmung erkennt man leicht, wenn man nach § 181 (S. 145) die Moduln, ebenso wie die Ideale, in Klassen einteilt und die feinere Bestimmung hinzufügt, daß zwei Moduln $\mathfrak{m}$, $\mathfrak{m}_1$ nur dann äquivalent heißen und in dieselbe Klasse aufgenommen werden sollen, wenn es eine Zahl η von positiver Norm gibt, welche der Bedingung $\mathfrak{m}\eta = \mathfrak{m}_1$ genügt. Denn wenn man die oben festgesetzten Bezeichnungen und Regeln für die Wahl der Basis eines Moduls $\mathfrak{m} = m[1, \omega]$, sowie für die Bildung der zugehörigen Form $(a, \frac{1}{2}b, c)$ beibehält, so entsprechen je zwei äquivalenten Moduln auch zwei eigentlich äquivalente Formen (§ 56), und umgekehrt; beides ergibt sich leicht daraus, daß die Äquivalenz der Moduln $\mathfrak{m} = m[1, \omega]$, $\mathfrak{m}_1 = m_1[1, \omega_1]$ in der Existenz einer Zahl η von positiver Norm besteht, welche der Bedingung $[\eta, \eta\omega] = [1, \omega_1]$ genügt, und daß sowohl diese Bedingung wie die eigentliche Äquivalenz der zugehörigen Formen $(a, \frac{1}{2}b, c)$, $(a_1, \frac{1}{2}b_1, c_1)$ mit der Existenz von vier ganzen rationalen Zahlen p, q, r, s zusammenfällt, welche die Gleichungen

$$\eta = p + q\omega_1, \quad \eta\omega = r + s\omega_1, \quad \omega = \frac{r + s\omega_1}{p + q\omega_1}, \qquad ps - qr = +1 \tag{54}$$

befriedigen*). Mithin entsprechen die Modul- und Formenklassen sich gegenseitig und eindeutig. Bezeichnet man nun, wie früher, mit O die Hauptklasse der Ideale, so erzeugt jede Modulklasse M eine Idealklasse MO; umgekehrt, wenn A eine beliebige Idealklasse,

*) Vgl. meine auf S. 214 zitierte Schrift (§ 1).

und $\mathfrak{n}$ eine beliebige Ordnung ist, so folgt aus unserer obigen Untersuchung über die umgekehrte Aufgabe der Multiplikation der Moduln, daß es immer mindestens eine Klasse M von der Ordnung $\mathfrak{n}$ gibt, welche diese Idealklasse A erzeugt, und zwar findet man leicht, daß jede Idealklasse A durch gleich viele Modulklassen M von der Ordnung $\mathfrak{n}$ erzeugt wird. Bezeichnet man daher mit h' die Anzahl der verschiedenen Modulklassen M für die Ordnung $\mathfrak{n}$, mit h die Anzahl der Idealklassen, so ist $h' = rh$, wo r die Anzahl derjenigen Klassen M bedeutet, welche der Bedingung $MO = O$ genügen und folglich durch Wurzeln der Ordnung $\mathfrak{n}$ repräsentiert werden. Bezeichnet man nun mit λ die Anzahl aller derjenigen von diesen l Wurzeln, welche der Hauptklasse der Ordnung $\mathfrak{n}$ angehören, also mit $\mathfrak{n}$ äquivalent sind, so findet man ebenso leicht, daß jede solche Klasse M durch λ verschiedene Wurzeln repräsentiert wird, daß also $l = r\lambda$, mithin

$$\frac{h'}{h} = \frac{l}{\lambda} = \frac{k}{\lambda} \Pi\left(1 - \frac{(D, p)}{p}\right) \tag{55}$$

ist (vgl. § 151). Bedeutet aber $\mathfrak{m} = [m, \alpha]$ eine solche mit $\mathfrak{n}$ äquivalente Wurzel von $\mathfrak{n}$, so ist $\mathfrak{m} = \mathfrak{n}\eta$, woraus folgt, daß η in $\mathfrak{m}$ enthalten, also eine ganze Zahl, und zwar eine Einheit (von positiver Norm) ist, weil sie in den beiden relativen Primzahlen m, α aufgehen muß; und da umgekehrt einleuchtet, daß jeder Einheit η ein mit $\mathfrak{n}$ äquivalenter Modul $\mathfrak{n}\eta$ entspricht, welcher eine Wurzel von $\mathfrak{n}$ ist, so ist λ die Anzahl aller derjenigen Einheiten η, denen verschiedene Moduln $\mathfrak{n}\eta$ entsprechen. Da nun alle Einheiten η, mag ihre Anzahl endlich oder unendlich, also die Grundzahl D negativ oder positiv sein, in der Form $\pm\varepsilon^s$ enthalten sind, wo ε eine bestimmte Einheit, und s jede ganze rationale Zahl bedeutet, so ergibt sich leicht, daß λ der kleinste positive Exponent ist, welcher bewirkt, daß die Potenz ε^λ eine in der Ordnung $\mathfrak{n}$ enthaltene Zahl wird. Hiermit ist vermöge (55) für jede Ordnung $\mathfrak{n}$ das Verhältnis der Klassenanzahl h' zu der Anzahl h der Idealklassen gefunden, und man überzeugt sich leicht, daß die früher (in §§ 97, 99, 100, 151) gewonnenen Resultate mit dem jetzigen vollständig übereinstimmen*).

*) Dieselbe Aufgabe habe ich für beliebige Körper in der auf S. 146 zitierten Festschrift behandelt.

[Erläuterungen gemeinsam mit denen zu XLVII, XLVIII, XLIX am Schluß von XLIX.]