Richard Dedekind

Gesammelte mathematische Werke

Herausgegeben von

Robert Fricke †
in Braunschweig

Emmy Noether
in Göttingen

Öystein Ore
in New Haven

Dritter Band

Druck und Verlag von Friedr. Vieweg & Sohn Akt.-Ges.
Braunschweig 1932

Nachwort der Herausgeber.

Der Abschluß der Herausgabe von Dedekinds Werken fällt fast genau in das Jahr seines hundertsten Geburtstags (6. Oktober 1931). Es ist ein Zeichen, wie Dedekind seiner Zeit voraus war, daß seine Werke noch heute lebendig sind, ja daß sie vielleicht erst heute ganz lebendig geworden sind.

Die Ausgabe sollte mit einem Lebenslauf schließen, den R. Fricke aus persönlicher Erinnerung beisteuern wollte, als Ergänzung zu den „Erläuterungen", die in ihrer Gesamtheit so etwas wie einen wissenschaftlichen Lebenslauf darstellen möchten. Mit dem Tod Frickes ist dieser Lebenslauf weggefallen; an Stelle dessen haben wir versucht, möglichst Dedekind selbst auch persönlich zu Worte kommen zu lassen, in Vorworten, Selbstanzeigen, vor allem in seinen Briefen. Auch der Nachlaß*) gibt ein Stück Lebenslauf. Im übrigen sei auf die Würdigung von Landau (Gött. Nachr. 1917) verwiesen.

Der Notgemeinschaft der Deutschen Wissenschaft haben wir für ihre großzügige Unterstützung zu danken, die das Erscheinen dieser Gesamtausgabe erst ermöglichte. Auch der Yale University sind wir für einen Beitrag zur Assistentenhilfe zu Dank verpflichtet. Die Korrekturen des dritten und des größten Teils des zweiten Bandes hat W. Weber mit bekannter Sorgfalt gelesen.

Göttingen und New Haven, im Mai 1932.

E. Noether. **Ö. Ore.**

*) Der Nachlaß soll vollständig in der Universitätsbibliothek Göttingen deponiert werden, wo er zum größten Teil schon liegt.

Inhaltsverzeichnis.

XLVI.

Über die Theorie der ganzen algebraischen Zahlen.

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

Inhalt.

§ 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

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

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:

$$(\alpha \pm \beta)' = \alpha' \pm \beta'$$
$$(\alpha\beta)' = \alpha'\beta'$$
$$\left(\frac{\alpha}{\beta}\right)' = \frac{\alpha'}{\beta'}.$$

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

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

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 gemeinschaftlicher 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, $\gamma \ldots$ eine Primzahl π auftritt, was nach einer endlichen Anzahl von Zerlegungen geschehen muß, weil die Reihe der beständig abnehmenden natürlichen Zahlen $N(\alpha)$, $N(\beta)$, $N(\gamma) \ldots$ 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 $\alpha_1, \alpha_2 \ldots$ 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

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

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 $\varrho, \varrho_1, \varrho_2 \ldots \varrho_m$, also

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

so muß nach dem oben bewiesenen Satze die in diesem Produkte α aufgehende Primzahl π notwendig in einem der Faktoren ϱ, ϱ_1, $\varrho_2 \ldots \varrho_m$, 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Man setze nun

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

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

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

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

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

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 $g', g'' \ldots$ 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 $AA = A$.