§ 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

$$(D, p) = 0, = +1, \text{ oder } = -1 \tag{7}$$

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

$$(D, 1) = 1, \tag{8}$$

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

$$(D, m) = (D, p)\,(D, p')\,(D, p'')\ldots, \tag{9}$$

woraus der allgemeine Satz

$$(D, m'\,m'') = (D, m')\,(D, m'') \tag{10}$$

folgt*).

Indem wir die bei der allgemeinen Untersuchung über die Anzahl h der Idealklassen benutzten Bezeichnungen beibehalten (§ 184), setzen wir

$$\Omega(s) = \Sigma N(\mathfrak{a})^{-s} = \Pi(1 - N(\mathfrak{p})^{-s})^{-1}; \tag{11}$$

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

$$\begin{aligned}\Omega(s) &= \Pi(1 - p^{-s})^{-1}\ \Pi(1 - (D, p)\,p^{-s})^{-1} \\ &= \Sigma\frac{1}{m^s}\cdot\Sigma\frac{(D, m)}{m^s}\end{aligned} \tag{12}$$

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

$$gh = \lim \Sigma\frac{(D, m)}{m^s}, \tag{13}$$

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 Ω 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 $\frac{1}{4}D$, 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 des 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

$$\mathfrak{m} = [\alpha, \beta] \tag{1}$$

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

$$\mathfrak{m} = [m, m\omega] = m[1, \omega] \tag{2}$$

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

$$a\omega^2 - b\omega + c = 0, \tag{3}$$

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

$$m = m.1 + 0.a\omega, \ m\omega = 0.1 + \frac{m}{a}.a\omega$$

*) Vgl. die beiden folgenden Anmerkungen.

verbunden sind, so ergibt sich [nach § 175, (10)] das Resultat

$$N(\mathfrak{m}) = \begin{vmatrix} m, & 0 \\ 0, & \frac{m}{a} \end{vmatrix} = \frac{m^2}{a}. \tag{10}$$

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

$$a(\omega + \omega') = b, \ a\omega\omega' = c; \tag{11}$$

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

$$\mathfrak{m}' = m[1, -\omega'] \tag{12}$$

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

$$\mu = m(x + y\omega), \tag{13}$$

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

$$N(\mu) = N(\mathfrak{m})(ax^2 + bxy + cy^2); \tag{14}$$

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

$$(a_2\omega_2)^2 - b_2(a_2\omega_2) + a_2c_2 = 0,$$

so ergibt sich

$$e_2 = ef_1 + e_1f + ee_1b_2,\quad f_2 = ff_1 - ee_1a_2c_2; \tag{23}$$

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

$$k = ek_2,\quad k_1 = e_1k_2,\quad (\mathfrak{n}_1, \mathfrak{n}) = e,\quad (\mathfrak{n}, \mathfrak{n}_1) = e_1, \tag{24}$$

also auch

$$d = d_2e^2,\quad d_1 = d_2e_1^2, \tag{25}$$

und außerdem

$$f = \frac{b - b_2e}{2},\quad f_1 = \frac{b_1 - b_2e_1}{2}; \tag{26}$$

ebenso erhält man aus der letzten der Gleichungen (22), oder indem man die vorstehenden Ausdrücke in (23) substituiert,

$$e_2 = \frac{be_1 + b_1e}{2},\quad f_2 = \frac{bb_1 + d_2ee_1 - 2b_2e_2}{4}. \tag{27}$$

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 mm_1 in $\mathfrak{m}_2$ und folglich auch in $[m_2]$ enthalten ist, so kann man zunächst

$$mm_1 = pm_2,\quad m_2 = \frac{mm_1}{p} \tag{28}$$

setzen, wo p eine natürliche Zahl bedeutet; ersetzt man nun die im Satze (19) auftretenden Normen durch ihre Ausdrücke gemäß (10), so erhält man

$$aa_1 = p^2a_2,\quad a_2 = \frac{aa_1}{p^2}, \tag{29}$$

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 $\omega, \omega_1, \omega\omega_1$ 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

$$a e_1 = p q', \quad a_1 e = p q'', \quad e_2 = p q''', \tag{34}$$

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

$$\frac{a b_1}{p} - q' b_2 = 2 a_2 p', \quad \frac{a_1 b}{p} - q'' b_2 = 2 a_2 p'',$$

$$\frac{b b_1 + d_2 e e_1}{2p} - q''' b_2 = 2 a_2 p''',$$

also die Kongruenzen

$$\left.\begin{aligned} q' b_2 &\equiv \frac{a b_1}{p} \\ q'' b_2 &\equiv \frac{a_1 b}{p} \\ q''' b_2 &\equiv \frac{b b_1 + d_2 e e_1}{2p} \end{aligned}\right\} \pmod{2 a_2}, \tag{35}$$

durch welche die Zahl b_2 nach dem Modul $2a_2$ 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

$$\begin{aligned} x_2 &= p x x_1 + p' x y_1 + p'' y x_1 + p''' y y_1 \\ y_2 &= \quad\quad q' x y_1 + q'' y x_1 + q''' y y_1; \end{aligned} \tag{37}$$

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 $n_1 n_2 = n_2$ 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 $\mathfrak{m}_1 = \mathfrak{n}_1$ ist, und man braucht sich nur noch mit der Lösung der Gleichung $\mathfrak{m}\,\mathfrak{n}_1 = \mathfrak{m}_2$ 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 $n_2 = n\,n_1$ der größte gemeinschaftliche Teiler von n und n_1, also $k = e k_2$ wird, wo e relative Primzahl zu e_1 ist; nachdem man für den Modul $\mathfrak{m}$ eine solche Ordnung 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 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 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 n sind, es immer einen und nur einen Modul $\mathfrak{a} = \mathfrak{c}\mathfrak{b}^{-1}$ von derselben Ordnung 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 n zu finden, welche der Bedingung

$$(39)\qquad \mathfrak{m}\,\mathfrak{n}_2 = \mathfrak{n}_2$$

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

$$(40)\qquad \mathfrak{m}\,\mathfrak{o} = \mathfrak{o};$$

diese Moduln, zu welchen offenbar n selbst gehört, sind von besonderer Wichtigkeit, und wir wollen jeden Modul $\mathfrak{m}$ von der Ordnung n, welcher diese letzte Bedingung erfüllt, aus einem sogleich anzugebenden Grunde eine Wurzel der Ordnung n nennen; es ist zweckmäßig, zunächst alle diese Wurzeln von 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

$$(41)\qquad \mathfrak{m} > \mathfrak{o},$$

also besteht jede Wurzel $\mathfrak{m}$ aus lauter ganzen Zahlen. Da ferner $\mathfrak{n} = \mathfrak{m} : \mathfrak{m}$, und allgemein $(c : a) : b = c : ab$ 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, $3\varrho \ldots k\varrho$ 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

$$\varphi(k) = k\,\Pi\Big(1 - \frac{1}{p}\Big),$$

wo das Produkt über alle verschiedenen, in k aufgehenden rationalen Primzahlen p auszudehnen ist; andererseits ist [nach § 180, (26)]

$$\varphi(\mathfrak{o}\,k) = k^2\,\Pi\Big(1 - \frac{1}{N(\mathfrak{p})}\Big),$$

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

$$\varphi(\mathfrak{o}\,k) = k^2\,\Pi\Big(1 - \frac{1}{p}\Big)\Big(1 - \frac{(D, p)}{p}\Big)$$

und folglich

$$l = k\,\Pi\Big(1 - \frac{(D, p)}{p}\Big). \tag{53}$$

Nachdem hiermit die Anzahl aller Wurzeln $\mathfrak{m}$ der Ordnung $\mathfrak{n}$ bestimmt ist, findet man leicht die Anzahl aller derjenigen unter ihnen, welche der obigen Bedingung (39) genügen, wo $\mathfrak{n}_2$ eine gegebene, in $\mathfrak{n}$ aufgehende Ordnung bedeutet; multipliziert man nämlich alle l Wurzeln der Ordnung $\mathfrak{n}$ mit $\mathfrak{n}_2$, so werden alle l_2 Wurzeln von $\mathfrak{n}_2$, 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 $\mathfrak{n}$, welche der ursprünglich vorgelegten Bedingung $\mathfrak{m}\,\mathfrak{m}_1 = \mathfrak{m}_2$ genügen.

Die binären Formen $(a, \frac{1}{2}b, c) = (m^2, \frac{1}{2}m\,b_0, c)$, welche nach (14) den Wurzeln $\mathfrak{m} = [m, \alpha]$ der Ordnung $\mathfrak{n}$ 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

$$\eta = p + q\,\omega_1, \quad \eta\,\omega = r + s\,\omega_1, \quad \omega = \frac{r + s\,\omega_1}{p + q\,\omega_1}, \qquad p\,s - q\,r = +1 \tag{54}$$

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 $M\,O$; 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.]

XLVII.

Über die Komposition der binären quadratischen Formen.

[Supplement X von Dirichlets Vorlesungen über Zahlentheorie, 2. Auflage, S. 423—462 (1871).]

Inhalt.

§ 159.

Die Theorie der binären quadratischen Formen, ihrer Äquivalenz und Komposition bildet nur einen speziellen Fall von der Theorie derjenigen homogenen Formen $n$ten Grades mit n Veränderlichen, welche sich in lineare Faktoren mit algebraischen Koeffizienten zerlegen lassen. Diese Formen sind zuerst von Lagrange*) betrachtet; später hat Dirichlet**) sich vielfach mit diesem Gegenstande beschäftigt, aber er hat von seinen weitgehenden Untersuchungen nur diejenige veröffentlicht, welche die Transformationen solcher Formen in sich selbst (vgl. §§ 61, 62) oder, was dasselbe ist, die Theorie der Einheiten für die entsprechenden algebraischen Zahlen behandelt; endlich hat Kummer***) durch die Schöpfung der idealen Zahlen einen neuen Weg betreten, welcher nicht nur zu einer sehr bequemen Ausdrucksweise, sondern auch zu einer tieferen Einsicht in die wahre Natur der algebraischen Zahlen führt. Indem wir versuchen, den

*) 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 Éléments d'Algèbre par L. Euler. § IX.

**) Vgl. Anm. zu § 141.

***) Vgl. Anm. zu § 16.

Leser in diese neuen Ideen einzuführen, stellen wir uns auf einen etwas höheren Standpunkt und beginnen damit, einen Begriff einzuführen, welcher wohl geeignet scheint, als Grundlage für die höhere Algebra und die mit ihr zusammenhängenden Teile der Zahlentheorie zu dienen.

I. Unter einem Körper wollen wir jedes System von unendlich vielen reellen oder komplexen Zahlen verstehen, welches in sich so abgeschlossen und vollständig ist, daß die Addition, Subtraktion, Multiplikation und Division von je zwei dieser Zahlen immer wieder eine Zahl desselben Systems hervorbringt. Der einfachste Körper wird durch alle rationalen, der größte Körper durch alle Zahlen gebildet. Wir nennen einen Körper A einen Divisor des Körpers M, diesen ein Multiplum von jenem, wenn alle in A enthaltenen Zahlen sich auch in M vorfinden; man findet leicht, daß der Körper der rationalen Zahlen ein Divisor von jedem andern Körper ist. Der Inbegriff aller Zahlen, welche gleichzeitig in zwei Körpern A, B enthalten sind, bildet wieder einen Körper D, welcher der größte gemeinschaftliche Divisor der beiden Körper A, B genannt werden kann, weil offenbar jeder gemeinschaftliche Divisor von A und B notwendig ein Divisor von D ist; ebenso existiert immer ein Körper M, welcher das kleinste gemeinschaftliche Multiplum von A und B heißen soll, weil er ein Divisor von jedem andern gemeinschaftlichen Multiplum der beiden Körper ist. Entspricht ferner einer jeden Zahl a des Körpers A eine Zahl $b = \varphi(a)$ in der Weise, daß $\varphi(a+a') = \varphi(a)+\varphi(a')$, und $\varphi(aa') = \varphi(a)\varphi(a')$ ist, so bilden die Zahlen b (falls sie nicht sämtlich verschwinden) ebenfalls einen Körper $B = \varphi(A)$, welcher mit A konjugiert ist und durch die Substitution φ aus A hervorgeht; dann ist rückwärts auch $A = \psi(B)$ mit B konjugiert. Zwei mit einem dritten konjugierte Körper sind auch miteinander konjugiert, und jeder Körper ist mit sich selbst konjugiert. Korrespondierende Zahlen in zwei konjugierten Körpern A und B, wie a und $b = \varphi(a)$, sollen konjugierte Zahlen heißen.

Die einfachsten Körper sind diejenigen, welche nur eine endliche Anzahl von Divisoren besitzen. Nennt man m bestimmte Zahlen $\alpha_1, \alpha_2, \ldots, \alpha_m$ voneinander abhängig oder unabhängig, je nachdem die Gleichung $x_1\alpha_1 + x_2\alpha_2 + \cdots + x_m\alpha_m = 0$ in rationalen Zahlen $x_1, x_2, \ldots, x_m$, die nicht sämtlich verschwinden, lösbar ist oder nicht, so

findet man durch sehr einfache Betrachtungen, auf die wir aber hier nicht eingehen wollen, daß aus einem Körper Ω von der angegebenen Art*) nur eine endliche Anzahl n von unabhängigen Zahlen $\omega_1, \omega_2, \ldots, \omega_n$ sich auswählen läßt, daß also jede Zahl ω des Körpers stets und nur auf eine einzige Art durch die Form

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

darstellbar ist, wo $h_1, h_2, \ldots, h_n$ rationale Zahlen bedeuten. Wir wollen die Zahl n den Grad, ferner den Komplex der n unabhängigen Zahlen ω_i eine Basis des Körpers Ω, und die n Zahlen h_i die dieser Basis entsprechenden Koordinaten der Zahl ω nennen; offenbar bilden je n Zahlen von der Form (1) wieder eine solche Basis, wenn die aus den entsprechenden n^2 Koordinaten gebildete Determinante von Null verschieden ist; einer solchen Transformation der Basis durch eine lineare Substitution entspricht eine Transformation der Koordinaten durch die sogenannte transponierte Substitution.

Die Forderung, daß die Zahlen ω des Körpers Ω durch Addition und Subtraktion sich reproduzieren sollen, wird durch ihre gemeinsame Form (1) schon erfüllt; für die Reproduktion durch Multiplikation ist ferner erforderlich und hinreichend, daß jedes Produkt $\omega_i\omega_{i'}$ wieder in der Form (1) enthalten ist; diese Bedingungen, deren Anzahl gleich $\frac{1}{2}n(n+1)$ ist, lassen sich am einfachsten zusammenfassen, indem man die Koordinaten h_i als veränderlich ansieht und

$$\omega^2 = 2\Sigma H_i\omega_i \tag{2}$$

setzt, wo nun $H_1, H_2, \ldots, H_n$ bestimmte, mit rationalen Koeffizienten behaftete, ganze homogene quadratische Funktionen der Koordinaten bedeuten. Durch diese n Funktionen H_i, auf deren analytische Eigenschaften wir unten zurückkommen werden, ist die Konstitution des Körpers Ω vollständig bestimmt, und es läßt sich zunächst zeigen, daß die Zahlen von der Form (1) auch durch Division sich wieder erzeugen. Durch totale Differentiation von (2) erhält man

$$\omega\, d\omega = \Sigma\, dH_i\omega_i; \tag{3}$$

legt man den Koordinaten h_i und ihren Differentialen dh_i beliebige rationale Werte bei, so ist durch die vorstehende Gleichung das

*) Ersetzt man die rationalen Zahlen überall durch Zahlen eines Körpers R, so gelten die nachfolgenden Betrachtungen auch für einen Körper Ω, welcher nur eine endliche Anzahl solcher Divisoren besitzt, die zugleich Multipla von R sind.

Produkt aus zwei beliebigen Zahlen ω und $d\omega$ des Körpers Ω auf die Form (1) zurückgeführt. Speziell ergibt sich aus (3)

$$\omega\,\omega_r = \sum \frac{\partial H_\iota}{\partial h_r}\,\omega_\iota; \tag{4}$$

legt man nun den Koordinaten h_ι beliebige rationale Werte bei, welche aber nicht sämtlich verschwinden, so kann auch der entsprechende Wert der Funktional-Determinante

$$H = \sum \pm \frac{\partial H_1}{\partial h_1}\frac{\partial H_2}{\partial h_2}\cdots\frac{\partial H_n}{\partial h_n} \tag{5}$$

nicht verschwinden; denn sonst ließen sich bekanntlich n rationale Zahlen dh_ι, die nicht sämtlich verschwinden, so bestimmen, daß für jeden Index r

$$dH_r = \sum \frac{\partial H_r}{\partial h_\iota}\,dh_\iota = 0,$$

und folglich auch $\omega\,d\omega = 0$ würde, während doch keine der beiden Zahlen ω und $d\omega$ verschwindet. Hieraus folgt weiter durch Umkehrung der n Gleichungen (4), daß die n Quotienten $\omega_\iota : \omega$ wieder Zahlen von der Form (1) sind; dasselbe gilt daher auch von jedem Quotienten $\alpha : \omega$, wo α irgendeine Zahl von der Form (1) bedeutet. Mithin bilden alle Zahlen von der Form (1) wirklich einen Körper.

Durch Elimination der n Zahlen ω_ι aus den n Gleichungen (4) ergibt sich die Gleichung

$$\begin{vmatrix} \frac{\partial H_1}{\partial h_1} - \omega, & \frac{\partial H_2}{\partial h_1} & \cdots & \frac{\partial H_n}{\partial h_1} \\ \frac{\partial H_1}{\partial h_2}, & \frac{\partial H_2}{\partial h_2} - \omega & \cdots & \frac{\partial H_n}{\partial h_2} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{\partial H_1}{\partial h_n}, & \frac{\partial H_2}{\partial h_n} & \cdots & \frac{\partial H_n}{\partial h_n} - \omega \end{vmatrix} = 0 \tag{6}$$

mithin ist jede Zahl ω des Körpers Ω die Wurzel einer (von der Wahl der Basis unabhängigen) Gleichung $n$ten Grades mit rationalen Koeffizienten, also eine algebraische Zahl, und es läßt sich leicht zeigen, daß in dem Körper Ω auch Zahlen existieren, welche keiner Gleichung mit rationalen Koeffizienten von niedrigerem als dem $n$ten Grade genügen, für welche also die vorstehende Gleichung irreduktibel

ist*). Bedeutet θ eine solche Zahl, so bilden offenbar die Potenzen $1, \theta, \theta^2, \ldots, \theta^{n-1}$ ebenfalls eine Basis des Körpers Ω, und Ω ist das System aller Zahlen, welche sich durch beliebige Wiederholung der vier arithmetischen Grundoperationen aus θ ableiten lassen. Substituiert man nun für θ der Reihe nach alle Wurzeln derselben irreduktiblen Gleichung, so entstehen ebensoviele entsprechende Körper, welche offenbar mit Ω und folglich auch miteinander konjugiert sind, und es ließe sich leicht zeigen, daß außer diesen Körpern kein anderer

*) Der Beweis dieser Behauptung kann z. B. auf das folgende Lemma gestützt werden:

Genügt eine homogene lineare Funktion $\omega = \Sigma h_\iota \omega_\iota$ der n Variablen h_ι einer Identität von der Form

$$A\,\omega^m + A_1\,\omega^{m-1} + \cdots + A_m = 0, \tag{1}$$

wo $A, A_1, \ldots, A_m$ ganze Funktionen der Variablen h_ι mit rationalen Koeffizienten bedeuten, die nicht sämtlich identisch verschwinden, und ist der Grad m kleiner als die Anzahl n der Variablen, so sind die n Größen ω_ι voneinander abhängig.

Durch totale Differentiation der Identität (1) ergibt sich zunächst

$$M\,d\omega + \omega^m\,dA + \omega^{m-1}\,dA_1 + \cdots + dA_m = 0, \tag{2}$$

wo zur Abkürzung

$$M = m\,A\,\omega^{m-1} + (m-1)\,A_1\,\omega^{m-2} + \cdots + A_{m-1}$$

gesetzt ist. Man kann nun offenbar annehmen, daß keine solche Identität (1) von noch niedrigerem Grade als m existiert, daß also das Produkt AM nicht identisch verschwindet; nun lege man, was stets möglich ist, den Variablen h_ι solche rationale Werte bei, für welche AM einen von Null verschiedenen Wert erhält; hierauf kann man, weil $m < n$ ist, den n Differentialen dh_ι solche rationale Werte beilegen, welche den m homogenen linearen Gleichungen

$$A\,dA_1 = A_1\,dA,\ A\,dA_2 = A_2\,dA\ \ldots\ A\,dA_m = A_m\,dA$$

genügen und nicht sämtlich verschwinden; multipliziert man nun (1) mit dA, (2) mit A, und subtrahiert, so folgt $A\,M\,d\omega = 0$, also auch $d\omega = \Sigma\,dh_\iota\,\omega_\iota = 0$, was zu beweisen war.

Hieraus folgt zunächst, daß, wenn die Größen ω_ι und ω wieder ihre alte Bedeutung erhalten, die aus den Koordinaten der n Größen $1, \omega, \omega^2, \ldots, \omega^{n-1}$ gebildete Determinante D, welche eine homogene Funktion der Variablen h_ι vom Grade $\frac{1}{2}n\,(n-1)$ ist, nicht identisch verschwinden kann, weil sonst ω einer Identität von der obigen Form (1) und von niedrigerem Grade als n genügte, und folglich die Größen ω_ι voneinander abhängig wären. Gibt man nun den Koordinaten h_ι solche rationale Werte, für welche D einen von Null verschiedenen Wert erhält, so folgt unmittelbar, daß die entsprechende Zahl ω des Körpers Ω die Wurzel einer irreduktiblen Gleichung $n$ten Grades ist.

Jeder Lösung der Gleichung $D = 0$ in rationalen Zahlen h_ι entspricht eine Zahl ω, welche einem Divisor des Körpers Ω von niedrigerem als dem $n$ten Grade angehört; der Grad eines solchen Divisors ist immer ein Divisor von n.

mit Ω konjugiert ist. Dabei bemerken wir aber, um Mißverständnissen vorzubeugen, daß diese n Körper, was ihren gesamten Zahleninhalt anbetrifft, sehr wohl teilweise oder auch sämtlich identisch sein können, obgleich sie durch n verschiedene Substitutionen aus einem von ihnen hervorgehen*).

Da nun vermöge des Begriffes konjugierter Körper die Gleichungen (4) gültig bleiben, wenn die Zahlen des Körpers Ω durch die entsprechenden Zahlen eines konjugierten Körpers ersetzt werden, so folgt leicht, daß die sämtlichen Wurzeln der Gleichung (6) die mit ω konjugierten Zahlen sind. Bezeichnet man daher mit $N(\omega)$ die sogenannte Norm der Zahl ω, d. h. das Produkt aus allen n konjugierten Wurzeln, die auch gruppenweise einander gleich sein können, so ist zufolge (6)

$$N(\omega) = H, \tag{7}$$

d. h. die homogene Funktion H ist das Produkt aus n konjugierten Faktoren ersten Grades mit algebraischen Koeffizienten. Aus dieser Definition geht unmittelbar der Satz hervor: die Norm eines Produktes ist immer gleich dem Produkt aus den Normen der Faktoren. Setzt man ferner

$$N(\omega) = \omega\,\omega', \tag{8}$$

so ist ω', weil $N(\omega)$ als rationale Zahl in Ω enthalten ist, ebenfalls eine Zahl des Körpers Ω, was auch aus (6) hervorgeht, und zwar ist

$$N(\omega') = N(\omega)^{n-1}; \tag{9}$$

nennen wir ω' die zu ω adjungierte Zahl**), so ist die zu ω' adjungierte Zahl $= \omega\, N(\omega)^{n-2}$.

Sind $\alpha_1, \alpha_2, \ldots, \alpha_n$ beliebige Zahlen des Körpers Ω, und bedeuten $\beta_\iota, \gamma_\iota, \ldots, \lambda_\iota$ die übrigen $(n-1)$ mit α_ι konjugierten Zahlen, so setzen wir zur Abkürzung

$$(\Sigma \pm \alpha_1 \beta_2 \ldots \lambda_n)^2 = \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) \tag{10}$$

*) Durch die weitere Verfolgung dieses Gegenstandes gelangt man unmittelbar zu den von Galois in die Algebra eingeführten Prinzipien (Sur les conditions de résolubilité des équations par radicaux; Journ. de Math. p. p. Liouville. T. XI. 1846); hierbei ist es zweckmäßig, zunächst die einfachen Reziprozitätsgesetze aufzusuchen, welche zwischen irgend zwei solchen Körpern wie Ω, ihrem größten gemeinschaftlichen Divisor und ihrem kleinsten gemeinschaftlichen Multiplum herrschen.

**) Dieser Ausdruck wird hier in ganz anderer Bedeutung gebraucht wie von Galois.

und nennen dieses Determinantenquadrat die Diskriminante der n Zahlen $\alpha_1, \alpha_2, \ldots, \alpha_n$; sie ist eine symmetrische Funktion der n mit θ konjugierten Zahlen und folglich eine rationale Zahl, und zwar ist

$$\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = m^2 \Delta(\omega_1, \omega_2, \ldots, \omega_n), \tag{11}$$

wo m die aus den Koordinaten der Zahlen $\alpha_1, \alpha_2, \ldots, \alpha_n$ gebildete Determinante bedeutet; da die Diskriminante $\Delta(1, \theta, \theta^2, \ldots, \theta^{n-1})$ bekanntlich das Produkt aller Differenzen zwischen den mit θ konjugierten Zahlen und folglich von Null verschieden ist (weil eine irreduktible Gleichung nur ungleiche Wurzeln haben kann), so ist $\Delta(\alpha_1 \ldots \alpha_n)$ stets und nur dann $= 0$, wenn die Zahlen $\alpha_1, \alpha_2, \ldots, \alpha_n$ voneinander abhängig sind. Endlich ist allgemein

$$\Delta(\omega\,\alpha_1, \omega\,\alpha_2, \ldots, \omega\,\alpha_n) = N(\omega)^2 \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n). \tag{12}$$

II. Im vorhergehenden sind die Begriffe und Sätze entwickelt, deren wir in der Folge bedürfen; zur Erläuterung mögen aber hier noch die wichtigsten und nächstliegenden Resultate aus dem großen Reichtume analytischer Entwicklungen mitgeteilt werden, welche sich an die Betrachtung der Funktionen H_ι anknüpfen. Zwischen diesen n Funktionen bestehen fundamentale Relationen, welche man erhält, wenn man das Produkt aus drei beliebigen Zahlen des Körpers Ω auf alle möglichen Arten bildet (vgl. §§ 1, 2). Bedeutet d' wieder eine beliebige Variation, so ist zufolge (4)

$$d'\,\omega\,\omega_r = \sum d'\left(\frac{\partial H_\iota}{\partial h_r}\right)\omega_\iota;$$

multipliziert man nun (3) mit $d'\omega$, und ersetzt die Produkte $d'\omega\,\omega_\iota$ der vorstehenden Gleichung gemäß durch Summen, so folgt

$$\omega\, d\omega\, d'\omega = \sum d H_\iota\, d'\left(\frac{\partial H_{\iota'}}{\partial h_\iota}\right)\omega_{\iota'};$$

da die linke Seite symmetrisch in bezug auf d und d' ist, und da die n Zahlen $\omega_{\iota'}$ unabhängig sind, so ergibt sich, daß die Funktionen H_ι den n Differentialgleichungen

$$\sum d H_\iota\, d'\left(\frac{\partial H_r}{\partial h_\iota}\right) = \sum d' H_\iota\, d\left(\frac{\partial H_r}{\partial h_\iota}\right) \tag{13}$$

genügen, wo r irgendeinen der Indizes $1, 2, \ldots, n$ bedeutet. Um die Bedeutung dieser Relationen mehr hervortreten zu lassen, wollen wir sie den folgenden Entwicklungen zugrunde legen, ohne den Zusammenhang der Funktionen H_ι mit dem Körper Ω zu benutzen.

Zunächst wollen wir zeigen, daß die Funktionaldeterminante H, welche zufolge ihrer Definition (5) eine ganze homogene Funktion $n$ten Grades mit rationalen Koeffizienten ist, sich durch Multiplikation reproduziert; gehen die Formen K und L dadurch aus H hervor, daß die Koordinaten h_ι bzw. durch dh_ι und durch dH_ι ersetzt werden, so ist

$$L = HK; \tag{14}$$

denn wenn man die Koordinaten h_ι durch dh_ι ersetzt, so geht jede homogene lineare Funktion

$$\frac{\partial H_r}{\partial H_s} \text{ in } d\left(\frac{\partial H_r}{\partial h_s}\right),$$

und folglich H in

$$K = \sum \pm d\left(\frac{\partial H_1}{\partial h_1}\right) d\left(\frac{\partial H_2}{\partial h_2}\right) \cdots d\left(\frac{\partial H_n}{\partial h_n}\right)$$

über; werden aber die Koordinaten h_ι durch die bilinearen Funktionen dH_ι ersetzt, so geht zufolge (13)

$$\frac{\partial H_r}{\partial h_s} \text{ in } \sum \frac{\partial}{\partial h_s}\left(\frac{\partial H_r}{\partial h_\iota}\right) dH_\iota = \sum \frac{\partial H_\iota}{\partial h_s} d\left(\frac{\partial H_r}{\partial h_\iota}\right),$$

und folglich H in $L = HK$ über, was zu beweisen war. Dies ist der schon oben angeführte Satz über die Norm eines Produktes.

Bedeutet φ eine willkürliche Funktion der Koordinaten h_ι, und definiert man die Variation δ dadurch, daß

$$\delta\varphi = \sum \frac{\partial \varphi}{\partial H_\iota} h_\iota, \text{ also } \delta H_\iota = h_\iota \tag{15}$$

wird, so ergibt sich aus (13), wenn man d' durch δ ersetzt,

$$\sum dH_\iota \delta\left(\frac{\partial H_r}{\partial h_\iota}\right) = \sum h_\iota d\left(\frac{\partial H_r}{\partial h_\iota}\right) = dH_r,$$

weil H_r eine homogene Funktion zweiten Grades ist, mithin

$$\delta\left(\frac{\partial H_r}{\partial h_s}\right) = 1 \text{ oder } = 0, \tag{16}$$

je nachdem r und s gleich oder ungleich sind; hieraus folgt, daß die n Variationen δh_ι konstante, rationale Zahlen sind. Wird ferner die Variation δ' durch

$$\delta'\varphi = H \sum \frac{\partial \varphi}{\partial H_\iota} \delta h_\iota, \text{ also } \delta' H_\iota = H \delta h_\iota \tag{17}$$

definiert, so ergibt sich, wenn man in (13) d' durch δ' ersetzt,

$$\sum dH_\iota \delta'\left(\frac{\partial H_r}{\partial h_\iota}\right) = H \sum \delta h_\iota d\left(\frac{\partial H_r}{\partial h_\iota}\right) = Hd \sum \frac{\partial H_r}{\partial h_\iota} \delta h_\iota$$
$$= Hd\delta H_r = Hdh_r,$$

folglich

$$\delta'\left(\frac{\partial H_r}{\partial h_s}\right) = H \frac{\partial h_r}{\partial H_s}; \tag{18}$$

da nun der Ausdruck rechter Hand der Koeffizient des Elementes

$$\frac{\partial H_s}{\partial h_r}$$

in der Determinante H, also eine ganze homogene Funktion $(n-1)$ten Grades der Koordinaten h_ι mit rationalen Koeffizienten ist, so gilt dasselbe von den Größen

$$h'_r = \delta' h_r = H \sum \frac{\partial h_r}{\partial H_\iota} \delta h_\iota, \tag{19}$$

und umgekehrt geht aus (18) hervor, daß die Koeffizienten der einzelnen n^2 Elemente in der Determinante H sich als homogene lineare Funktionen der soeben definierten n Größen h'_ι darstellen lassen. Wir wollen, wenn φ eine beliebige Funktion der Koordinaten h_ι bedeutet, mit φ' dieselbe Funktion der Größen h'_ι bezeichnen; dann lautet die Gleichung (18)

$$\frac{\partial H'_r}{\partial h'_s} = H \frac{\partial h_r}{\partial H_s}, \tag{20}$$

und hieraus folgt zugleich

$$H' = H^{n-1}; \quad H \frac{\partial h'_s}{\partial H'_r} = \frac{\partial H_s}{\partial h_r}. \tag{21}$$

Da H eine Funktionaldeterminante ist, so ist bekanntlich*)

$$d \log H = \sum \frac{\partial dH_\iota}{\partial H_\iota} - \sum \frac{\partial dh_\iota}{\partial h_\iota},$$

*) Jacobi: De determinantibus functionalibus § 9 (Crelles Journal XXII); in der obigen Form ist auch der Fall berücksichtigt, daß die Differentiale dh_ι Funktionen von den Veränderlichen h_ι sind. Ersetzt man d durch δ', so folgt aus (17) und (19) unmittelbar

$$\sum \frac{\partial h'_\iota}{\partial h_\iota} = 0.$$

und folglich ergibt sich unter Berücksichtigung von (13)

$$\sum \frac{\partial \log H}{\partial h_\iota} d H_\iota = \sum \frac{\partial}{\partial H_{\iota'}} \left(\frac{\partial H_{\iota'}}{\partial h_\iota}\right) d H_\iota$$
$$= \sum d\left(\frac{\partial H_{\iota'}}{\partial h_\iota}\right) \frac{\partial H_\iota}{\partial H_{\iota'}} = d \sum \frac{\partial H_\iota}{\partial h_\iota};$$

führt man daher die homogene lineare Funktion

$$S = \sum \frac{\partial H_\iota}{\partial h_\iota} \tag{22}$$

ein, so ist

$$\sum \frac{\partial \log H}{\partial h_\iota} d H_\iota = d S; \quad \frac{\partial \log H}{\partial h_r} = \frac{\partial S}{\partial H_r}, \tag{23}$$

also mit Rücksicht auf (20)

$$\frac{\partial H}{\partial h_r} = H \sum \frac{\partial S}{\partial h_\iota} \frac{\partial h_\iota}{\partial H_r} = \sum \frac{\partial S}{\partial h_\iota} \frac{\partial H'_\iota}{\partial h'_r};$$

man führe daher die ganze homogene Funktion zweiten Grades

$$T = \sum \frac{\partial S}{\partial h_\iota} H_\iota \tag{24}$$

ein, so wird

$$\frac{\partial H}{\partial h_r} = \frac{\partial T}{\partial h'_r}; \quad d H = \sum \frac{\partial T}{\partial h'_\iota} d h_\iota, \tag{25}$$

mithin sind auch die Derivierten der Form H darstellbar als homogene lineare Funktionen der in (19) definierten Größen h'_ι, und rückwärts diese durch jene. Da ferner zufolge (20)

$$\sum \frac{\partial H'_\iota}{\partial h'_s} \frac{\partial H_r}{\partial h_\iota} = H \quad \text{oder} \quad = 0$$

ist, je nachdem r und s gleich oder ungleich sind, so folgt durch Multiplikation mit h'_s oder $d h'_s$ und Summation in bezug auf s

$$2 \sum H'_\iota \frac{\partial H_r}{\partial h_\iota} = H h'_r; \quad \sum d H'_\iota \frac{\partial H_r}{\partial h_\iota} = H d h'_r$$

und hieraus durch Differentiation

$$h'_r d H - H d h'_r = 2 \sum H'_\iota d\left(\frac{\partial H_r}{\partial h_\iota}\right). \tag{26}$$

Mit Hilfe von (25) und (26) ist man imstande, auch die Differentiale höherer Ordnung von H zu bilden; auf diese Weise findet man

$$H d d' H - d H d' H = 2 H \sum \frac{\partial H}{\partial h_\iota} d d' h_\iota - 2 \sum \frac{\partial^2 T}{\partial h_\iota \partial h_{\iota'}} H'_\iota d d' H_{\iota'}; \tag{27}$$

außerdem ergibt sich aus Gleichung (26), welcher man mit Hilfe von (13) auch die Form

$$h'_r d H - H d h'_r = \sum \frac{\partial H'_\iota}{\partial h'_{\iota'}} \frac{\partial H'_r}{\partial h'_\iota} d h_{\iota'}$$

geben kann, die Funktionaldeterminante

$$\sum \pm \frac{\partial h'_1}{\partial h_1} \frac{\partial h'_2}{\partial h_2} \cdots \frac{\partial h'_n}{\partial h_n} = (-1)^{n-1} (n-1) H^{n-2} \tag{28}$$

und folglich aus (25) die Hessesche Determinante der Form H, nämlich

$$\sum \pm \frac{\partial^2 H}{\partial h_1^2} \cdots \frac{\partial^2 H}{\partial h_n^2} = (-1)^{n-1} (n-1) H^{n-2} \sum \pm \frac{\partial^2 T}{\partial h_1^2} \cdots \frac{\partial^2 T}{\partial h_n^2}. \tag{29}$$

Aus den Gleichungen (16), (22), (24), (25), (26), (27) ergeben sich unmittelbar folgende auf die Variation δ bezüglichen Resultate:

$$\begin{gathered} \delta S = n; \quad \delta T = S; \quad h'_r \delta H - H \delta h'_r = 2 H'_r; \\ \delta H = S'; \; \delta' H = \delta H^2 - H \delta^2 H = 2 T'. \end{gathered} \tag{30}$$

III. Alle diese Sätze sind abgeleitet aus der Voraussetzung, daß das System der n ganzen homogenen Funktionen H_ι vom zweiten Grade den Bedingungen (13) genügt, und daß ihre Funktionaldeterminante H nicht identisch verschwindet; fügt man noch die Voraussetzung hinzu, daß die Koeffizienten dieser Funktionen rationale Zahlen sind, und daß die Form H irreduktibel, d. h. nicht zerlegbar ist in Faktoren niedrigeren Grades, deren Koeffizienten ebenfalls rationale Zahlen sind, so läßt sich umgekehrt beweisen, daß zu diesem Funktionensystem ein algebraischer Zahlkörper Ω von der oben betrachteten Art gehört. Der Kürze halber führen wir eine Charakteristik ε ein, welche folgenden Sinn hat: ist φ irgendeine Funktion der Koordinaten h_ι, und ersetzt man die letzteren durch $h_\iota - \omega \delta h_\iota$, wo ω vorläufig eine willkürliche Funktion bedeutet, so geht φ in eine neue Funktion über, welche mit $\varepsilon(\varphi)$ bezeichnet werden soll. Aus dieser Definition folgt sofort

$$d \varepsilon(\varphi) = \varepsilon(d \varphi) - \varepsilon(\delta \varphi) d \omega; \tag{31}$$

unter der Voraussetzung, daß die Differentiale $d h_\iota$ konstant sind. Hierauf definiere man die Funktion ω als Wurzel der Gleichung $n$ten Grades

$$\varepsilon(H) = 0, \tag{32}$$

welche zufolge (16) vollständig mit der Gleichung (6) übereinstimmt, so läßt sich beweisen, daß ω eine ganze (homogene) Funktion ersten

Grades, d. h. daß $d\,d'\omega = 0$ ist, wenn die Differentiale dh_ι, $d'h_\iota$ als konstant vorausgesetzt werden. In der Tat ergibt sich durch sukzessive Differentiation der Identität (32) nach der in (31) ausgesprochenen Regel

(33) $$\varepsilon(\delta H)\,d\omega = \varepsilon(dH)$$

und

(34) $$\varepsilon(\delta H)^3\,d\,d'\omega = \varepsilon(R),$$

wo zur Abkürzung die homogene Funktion $(3n-4)$ten Grades

$$\left\{\begin{array}{l} \delta H^3\,d\,d'H + \delta^2 H\,d H\,d'H \\ -\delta H\,d H\,d'\delta H - \delta H\,d'H\,d\delta H \end{array}\right\} = R$$

gesetzt ist. Daß diese Funktion R durch H teilbar, in Zeichen, daß $R \equiv 0$ ist*), ergibt sich auf folgende Weise.

Aus (30) folgt

$$h'_r\delta H = 2H'_r + H\delta h'_r \equiv 2H'_r$$

ferner

$$h'_r\delta^2 H = 2\delta H'_r + H\delta^2 h'_r \equiv 2\delta H'_r$$

und hieraus durch Elimination von h'_r

$$\delta^2 H H'_r - \delta H \delta H'_r \equiv 0;$$

da nun zufolge (27) $dHd'H - Hdd'H$ eine homogene lineare Funktion der n Größen H'_ι ist, so folgt auch, daß

$$\delta^2 H(dHd'H - Hdd'H) - \delta H\delta(dHd'H - Hdd'H) \equiv 0$$

ist; die linke Seite unterscheidet sich aber von R nur um Bestandteile, welche durch H teilbar sind. Mithin ist $R = PH$, wo P eine ganze Funktion bedeutet, und folglich $\varepsilon(R) = \varepsilon(P)\varepsilon(H) = 0$. Da sich nun aus den Voraussetzungen über H beweisen läßt, daß $\varepsilon(\delta H)$ nicht identisch verschwindet, so folgt aus (34) $d\,d'\omega = 0$, d. h. die Wurzel ω der Gleichung (32) ist eine ganze Funktion ersten Grades; daß sie zugleich homogen ist, versteht sich von selbst, weil H, $\delta H, \ldots, \delta^{n-1}H$ und folglich auch ω gleichzeitig mit den Koordinaten h_ι verschwinden. Setzt man nun

(1) $$\frac{\partial\omega}{\partial h_\iota} = \omega_\iota, \quad \omega = \sum h_\iota\omega_\iota,$$

*) Dies gilt allgemein von dem Ausdruck
$d'Hd'''Hd''Hd''H + dHd''Hd'd'''H - d'''HdHd'd''H - d'Hd''Hdd'''H.$

so ergibt sich aus (33), daß

(35) $$\Sigma\delta h_\iota\omega_\iota = \delta\omega = 1$$

und

(36) $$\varepsilon\left(\frac{\partial H}{\partial h_\iota}\right) = \varepsilon(\delta H)\omega_\iota$$

ist. Da ferner zufolge (23)

$$\sum\frac{\partial H}{\partial h_\iota}dH_\iota = HdS \equiv 0$$

und

$$\varepsilon(dH_\iota) = dH_\iota - \omega\,d\delta H_\iota = dH_\iota - \omega\,dh_\iota$$

ist, so folgt

$$0 = \varepsilon(H)\,dS = \sum\varepsilon\left(\frac{\partial H}{\partial h_\iota}\right)\varepsilon(dH_\iota)$$

$$= \varepsilon(\delta H)\Sigma\omega_\iota(dH_\iota - \omega\,dh_\iota),$$

mithin

(3) $$\omega\,d\omega = \Sigma\,dH_\iota\omega_\iota,$$

also auch

(2) $$\omega^2 = 2\Sigma H_\iota\omega_\iota,$$

wodurch wir rückwärts zu unseren ursprünglichen Annahmen zurückgekehrt sind; und man kann auch beweisen — worauf wir hier nicht eingehen wollen —, daß aus den Voraussetzungen über H die Unabhängigkeit der n Zahlen ω_ι folgt.

Wir fügen diesen Entwicklungen endlich noch folgende leicht zu beweisende Bemerkungen hinzu. Die ausgeführte Form der Gleichung (32) oder (6) ist folgende

(37) $$0 = H - \delta H\frac{\omega}{1} + \delta^2 H\frac{\omega^2}{1\cdot 2} - \delta^3 H\frac{\omega^3}{1\cdot 2\cdot 3} + \cdots;$$

es ist ferner

(7) $$H = \Pi\omega = N(\omega),$$

wo das Produktzeichen Π sich auf alle n Wurzeln ω bezieht; ebenso findet man [wenn man in (3) d durch δ' ersetzt]

(8) $$H = \omega\omega',$$

wo

(38) $$\omega' = \delta'\omega = \Sigma h'_\iota\omega_\iota$$

zu ω adjungiert ist, und

(39) $$S = \Sigma\omega, \quad 2T = \Sigma\omega^2,$$

wo die Summenzeichen sich ebenfalls auf alle n Wurzeln beziehen. Die quadratische Form T ist charakteristisch für die Anzahl der reellen Wurzeln; bildet man ferner die Hessesche Determinante des Produktes $H = \Pi\omega$, so ergibt sich durch Vergleichung mit (29) die Diskriminante

$$(40) \qquad \Delta(\omega_1, \omega_2, \ldots, \omega_n) = \sum \pm \frac{\partial^2 T}{\partial h_1^2} \cdots \frac{\partial^2 T}{\partial h_n^2},$$

was auch unmittelbar aus (39) folgt.

§ 160.

Der Inbegriff aller algebraischen Zahlen bildet offenbar ebenfalls einen Körper*). Wir wollen nun, indem wir unserem eigentlichen Gegenstande näher treten, eine Zahl α eine ganze algebraische Zahl nennen, wenn sie die Wurzel einer Gleichung ist, deren Koeffizienten rationale ganze Zahlen sind, wobei wir ein für allemal bemerken, daß wir unter den Koeffizienten einer Funktion $m$ten Grades

$$F(x) = c\,x^m + c_1\,x^{m-1} + c_2\,x^{m-2} + \cdots + c_m$$

oder der Gleichung $F(x) = 0$ stets die m Quotienten

$$-\frac{c_1}{c}, \quad +\frac{c_2}{c} \cdots (-1)^m \frac{c_m}{c}$$

verstehen. Aus dieser Erklärung folgt zunächst, daß eine rationale Zahl stets und nur dann eine ganze algebraische Zahl ist, wenn sie eine ganze Zahl im gewöhnlichen Sinne des Wortes ist (vgl. § 5, 4.); diese Zahlen wollen wir von jetzt ab rationale ganze Zahlen, alle algebraischen ganzen Zahlen aber kurz ganze Zahlen nennen. Dieses vorausgeschickt, schreiten wir zum Beweise der folgenden Fundamentalsätze.

1. Die Summe, die Differenz und das Produkt zweier ganzen Zahlen α, β sind wieder ganze Zahlen.

*) Daß es außer den algebraischen 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; Journ. de Math. T. XVI, 1851). Man vermutet, daß die Ludolphsche Zahl π eine solche transzendente Zahl ist; allein selbst die als spezieller Fall hierin enthaltene Behauptung, daß die Quadratur des Zirkels unmöglich sei, ist bis auf den heutigen Tag noch nicht erwiesen. (Vgl. Euler: De relatione inter ternas pluresve quantitates instituenda. § 10. Opusc. anal. T. II, 1785.)

Sind a, b bzw. die Grade der Gleichungen $\varphi(\alpha) = 0$, $\psi(\beta) = 0$, deren Koeffizienten rationale ganze Zahlen sind, und bezeichnet man mit $\omega_1, \omega_2, \ldots, \omega_n$ die sämtlichen ab Produkte von der Form $\alpha^{a'}\beta^{b'}$, wo a' irgendeine der Zahlen 0, 1, 2, …, $(a-1)$, und b' irgendeine der Zahlen 0, 1, 2, …, $(b-1)$ bedeutet, so wird, wenn $\omega = \alpha + \beta$, oder $= \alpha - \beta$, oder $= \alpha\beta$ ist, jedes der n Produkte $\omega\omega_1, \omega\omega_2, \ldots, \omega\omega_n$ mit Zuziehung der Gleichungen $\varphi(\alpha) = 0$, $\psi(\beta) = 0$ auf die Form $r_1\omega_1 + r_2\omega_2 + \cdots + r_n\omega_n$ gebracht werden können, wo $r_1, r_2, \ldots, r_n$ rationale ganze Zahlen sind. Eliminiert man die n Größen $\omega_1, \omega_2, \ldots, \omega_n$ aus diesen n Gleichungen, so ergibt sich für ω eine Gleichung vom $n$ten Grade [wie (6) in § 159], deren Koeffizienten rationale ganze Zahlen sind, was zu beweisen war (vgl. § 139).

2. Die ganze Zahl α heißt teilbar durch die ganze Zahl β, oder ein Multiplum von β, wenn der Quotient $\alpha : \beta$ ebenfalls eine ganze Zahl ist; umgekehrt heißt β ein Divisor oder Teiler von α (vgl. § 3). Ebenso setzen wir $\alpha \equiv \beta \pmod{\gamma}$, wenn $\alpha - \beta$ durch γ teilbar ist, und nennen α, β kongruent nach dem Modul γ (vgl. § 17). Man erkennt sofort (zufolge 1.), daß die Sätze des § 3 und auch die des § 17 (mit vorläufiger Ausnahme von 6. und 8.; vgl. § 164, 3.) ihre Gültigkeit behalten.

3. Jede Wurzel ω einer Gleichung, deren Koeffizienten ganze Zahlen sind, ist ebenfalls eine ganze Zahl.

Ist ω die Wurzel einer Gleichung $m$ten Grades $F(\omega) = 0$, deren Koeffizienten α, β … ganze Zahlen sind, sind ferner a, b … bzw. die Grade der mit rationalen ganzen Koeffizienten behafteten Gleichungen $\varphi(\alpha) = 0$, $\psi(\beta) = 0$ …, so führe man die sämtlichen $mab\ldots$ Produkte $\omega_1, \omega_2, \ldots, \omega_n$ von der Form $\omega^{m'}\alpha^{a'}\beta^{b'}\ldots$ ein, wo die ganzen rationalen Exponenten den Bedingungen $0 \leqq m' < m$, $0 \leqq a' < a$, $0 \leqq b' < b$ … genügen; dann läßt sich vermöge der Gleichungen $F(\omega) = 0$, $\varphi(\alpha) = 0$, $\psi(\beta) = 0$ … jedes der n Produkte $\omega\omega_1, \omega\omega_2, \ldots, \omega\omega_n$ wieder in die Form $r_1\omega_1 + r_2\omega_2 + \cdots + r_n\omega_n$ bringen, wo $r_1, r_2, \ldots, r_n$ rationale ganze Zahlen bedeuten, und hieraus folgt unmittelbar die Richtigkeit des Satzes.

Ist daher z. B. α eine ganze Zahl, und r eine beliebige (ganze oder gebrochene) positive rationale Zahl, so ist auch α^r eine ganze Zahl (vgl. § 5, 4.).

4. Bekanntlich lassen sich die Begriffe der Teilbarkeit und des Vielfachen von den ganzen rationalen Zahlen unmittelbar auf die ganzen rationalen Funktionen übertragen, und es gibt einen Algorithmus zur Auffindung des größten gemeinschaftlichen Divisors $\varphi(x)$ zweier gegebenen Funktionen $F(x)$, $f(x)$, welcher demjenigen der Zahlentheorie (§ 4) vollständig analog ist. Sind die Koeffizienten von $F(x)$ und $f(x)$ sämtlich in einem Körper K enthalten, so werden auch die Koeffizienten von $\varphi(x)$ Zahlen des Körpers K sein, weil sie durch Addition, Multiplikation, Subtraktion und Division aus den Koeffizienten von $F(x)$ und $f(x)$ entstehen. Hieraus folgt leicht, daß, wenn α die Wurzel einer solchen Gleichung $F(\alpha) = 0$ ist, deren Koeffizienten Zahlen des Körpers K sind, notwendig auch eine solche Gleichung $\varphi(\alpha) = 0$ von niedrigstem Grade existieren muß, welche irreduktibel in K heißen soll und welche offenbar keine anderen Wurzeln besitzen kann als die Gleichung $F(\alpha) = 0$. Hieraus folgt der Satz:

Ist α eine ganze Zahl, und K ein bestimmter Körper, so sind alle Koeffizienten der in K irreduktiblen Gleichung $\varphi(\alpha) = 0$ ganze Zahlen.

Denn weil α eine ganze Zahl, also die Wurzel einer Gleichung $F(\alpha) = 0$ ist, deren Koeffizienten rationale ganze Zahlen und folglich auch Zahlen des Körpers K sind (§ 159), so kann die in K irreduktible Gleichung $\varphi(\alpha) = 0$, welcher α genügt, nur ganze Zahlen zu Wurzeln haben; da aber die Koeffizienten einer Gleichung durch Addition und Multiplikation aus ihren Wurzeln entstehen, so sind (zufolge 1.) auch die Koeffizienten der Gleichung $\varphi(\alpha) = 0$ ganze Zahlen, was zu beweisen war.

Der einfachste Fall, in welchem K der Körper der rationalen Zahlen ist, findet sich bei Gauß*).

5. Ist ϱ irgendeine algebraische Zahl, so gibt es immer unendlich viele (von Null verschiedene) rationale ganze Zahlen h von der Beschaffenheit, daß $h\varrho$ eine ganze Zahl wird, und zwar stimmen diese sämtlichen Zahlen h mit den sämtlichen rationalen Vielfachen der kleinsten unter ihnen überein.

*) D. A. art. 42.

Da ϱ eine algebraische Zahl, also die Wurzel einer Gleichung von der Form

$$c\varrho^m + c_1\varrho^{m-1} + c_2\varrho^{m-2} + \cdots + c_m = 0$$

ist, wo c, c_1, c_2, …, c_m rationale ganze Zahlen bedeuten, so ergibt sich durch Multiplikation mit c^{m-1}, daß $c\varrho$ eine ganze Zahl ist. Sind ferner $a\varrho$, $b\varrho$ ganze Zahlen, wo a, b rationale ganze Zahlen bedeuten, deren größter gemeinschaftlicher Teiler $= h$ ist, so folgt leicht (aus 1. und § 4), daß auch $h\varrho$ eine ganze Zahl ist. Hieraus ergibt sich unmittelbar der zu beweisende Satz.

6. Versteht man unter einer Einheit eine ganze Zahl ε, welche in allen ganzen Zahlen aufgeht, so ist zunächst erforderlich, daß sie auch in 1 aufgeht, daß also $1 = \varepsilon\varepsilon'$, und ε' eine ganze Zahl ist; wenn nun

$$\varepsilon^m + c_1\varepsilon^{m-1} + \cdots + c_m = 0$$

die im Körper der rationalen Zahlen irreduktible Gleichung ist, welcher ε genügt, so muß (zufolge 4.) $c_m = \pm 1$ sein, weil ε' der ebenfalls irreduktiblen Gleichung

$$c_m\varepsilon'^m + c_{m-1}\varepsilon'^{m-1} + \cdots + c_1\varepsilon' + 1 = 0$$

genügt; umgekehrt, ist dies der Fall, so geht ε in 1 und folglich in allen ganzen Zahlen auf, ist also eine Einheit. Die Anzahl der Einheiten ist offenbar unbegrenzt.

Ist α teilbar durch α', und sind ε, ε' irgendwelche Einheiten, so ist offenbar auch $\varepsilon\alpha$ durch $\varepsilon'\alpha'$ teilbar; hinsichtlich der Teilbarkeit verhalten sich daher alle Zahlen $\varepsilon\alpha$, welche den sämtlichen Einheiten ε entsprechen, genau wie α. Zwei ganze Zahlen, deren Quotient keine Einheit ist, wollen wir wesentlich verschieden nennen.

7. Will man nun den Begriff der Primzahl so fassen, daß sie außer sich selbst und den Einheiten keine wesentlich verschiedene Teiler besitzt und auch selbst keine Einheit ist, so erkennt man sofort, daß gar keine solche Zahl existiert; ist nämlich α eine ganze Zahl, aber keine Einheit, so besitzt sie immer unendlich viele wesentlich verschiedene Divisoren, z. B. die Zahlen $\sqrt{\alpha}$, $\sqrt[3]{\alpha}$, $\sqrt[4]{\alpha}$ usf., welche (zufolge 3.) ganze Zahlen sind.

Dagegen läßt sich der Begriff von relativen Primzahlen vollständig definieren, und diese Frage wird uns überhaupt auf den richtigen Weg leiten, welcher bei den ferneren Untersuchungen einzuschlagen ist. Da von einem größten gemeinschaftlichen Teiler

zweier ganzen Zahlen vorläufig (vgl. § 164, 3.) nicht gesprochen werden kann, so ist es auch unmöglich, die Definition von relativen Primzahlen so zu fassen, wie sie in der Theorie der rationalen Zahlen aufgestellt wird (§ 5); aber aus dieser Definition ergaben sich mehrere Sätze, deren jeder umgekehrt das Verhalten zweier relativen Primzahlen vollständig charakterisiert, ohne die Kenntnis ihrer sämtlichen Divisoren vorauszusetzen. Ein solcher Satz ist z. B. der folgende (§ 7): Sind a, b relative Primzahlen, so ist jede durch a und b teilbare Zahl auch durch ab teilbar. Dieser Satz läßt sich in der Tat umkehren: Ist jede durch a und b teilbare Zahl auch durch ab teilbar, so sind a, b relative Primzahlen. Hätten nämlich die beiden Zahlen $a = ha'$, $b = hb'$ einen gemeinschaftlichen Teiler $h > 1$, so wäre $ha'b'$ eine durch a und b, aber nicht durch ab teilbare Zahl.

Diese Betrachtung veranlaßt uns, folgende für das Gebiet aller ganzen algebraischen Zahlen gültige Erklärung aufzustellen:

Zwei von Null verschiedene ganze Zahlen α, β heißen relative Primzahlen, wenn jede durch α und β teilbare Zahl auch durch $\alpha\beta$ teilbar ist.

Vor allem bemerken wir, daß zwei relative Primzahlen im alten Sinne des Wortes, d. h. zwei rationale ganze Zahlen a, b, deren größter gemeinschaftlicher Divisor $= 1$ ist, auch im neuen Sinne relative Primzahlen bleiben; ist nämlich eine ganze algebraische Zahl γ teilbar durch a und b, so ist der Quotient $\varrho = \gamma : ab$ eine algebraische Zahl der Art, daß $a\varrho$ und $b\varrho$ ganze Zahlen sind; mithin muß (zufolge 5.) auch ϱ eine ganze Zahl, also γ teilbar durch ab sein, was zu beweisen war. Daß ferner umgekehrt zwei relative Primzahlen im neuen Sinne des Wortes, welche zugleich rational sind, auch relative Primzahlen im alten Sinne sind, versteht sich zufolge der der neuen Erklärung vorausgeschickten Erörterung von selbst.

Wir nennen ferner die ganzen Zahlen α, β, γ, δ ... kurz relative Primzahlen, wenn jede von ihnen relative Primzahl zu jeder der anderen ist (vgl. § 6); ist dann eine ganze Zahl ω durch jede von ihnen teilbar, so ist sie auch durch ihr Produkt teilbar (vgl. § 7), weil, wie man leicht findet, auch der folgende Satz (§ 5, 3.) seine Gültigkeit behält: Ist jede der Zahlen α', β', γ' ... relative Primzahl zu jeder der Zahlen α'', β'', γ'', δ'' ..., so sind auch die Produkte $\alpha'\beta'\gamma'$ ... und $\alpha''\beta''\gamma''\delta''$ ... relative Primzahlen und umgekehrt.

Aber wie soll man definitiv entscheiden, ob zwei gegebene ganze Zahlen α, β relative Primzahlen sind? Man könnte versuchen, folgenden Weg einzuschlagen. Da α^{-1} und β^{-1} algebraische Zahlen sind, so gibt es (zufolge 5.) immer zwei kleinste positive ganze rationale Zahlen a, b von der Art, daß $a\alpha^{-1}$ und $b\beta^{-1}$ ganze Zahlen, d. h. daß a, b bzw. durch α, β teilbar werden; zeigt sich nun, daß a, b relative Primzahlen sind, so sind auch α, β gewiß relative Primzahlen. Aber man muß sich hüten zu glauben, daß auch das Umgekehrte stattfindet, daß also die kleinsten rationalen Multipla a, b von zwei relativen Primzahlen α, β notwendig selbst relative Primzahlen sein müssen. So z. B. sind in der Tat die beiden konjugierten Zahlen $\alpha = 2 + i$ und $\beta = 2 - i$ relative Primzahlen, und doch ist $a = b = 5$. Eine wesentliche Reduktion unserer Aufgabe wird aber durch den folgenden Satz bewirkt:

Wenn zwei ganze Zahlen α, β sich in einem Körper K, dem sie selbst angehören, als relative Primzahlen bewähren, d. h. wenn jede durch α und β teilbare Zahl des Körpers K auch durch $\alpha\beta$ teilbar ist, so sind α, β wirklich relative Primzahlen.

Ist nämlich ω irgendeine durch α und durch β teilbare ganze Zahl, und ist

$$\omega^m + \gamma_1\omega^{m-1} + \gamma_2\omega^{m-2} + \cdots + \gamma_m = 0$$

die in K irreduktible Gleichung, welcher ω genügt, so sind (zufolge 4.) die Zahlen $\gamma_1, \gamma_2, \ldots, \gamma_m$ ganze Zahlen des Körpers K; da ferner die ganzen Zahlen $\alpha' = \omega : \alpha$ und $\beta' = \omega : \beta$ bzw. den in K irreduktiblen Gleichungen

$$(\alpha\alpha')^m + \gamma_1(\alpha\alpha')^{m-1} + \cdots + \gamma_m = 0$$
$$(\beta\beta')^m + \gamma_1(\beta\beta')^{m-1} + \cdots + \gamma_m = 0$$

genügen, so sind (zufolge 4.) auch die Quotienten $\gamma_n : \alpha^n$ und $\gamma_n : \beta^n$ ganze Zahlen des Körpers K; da ferner nach Voraussetzung jede durch α und β teilbare Zahl des Körpers K auch durch $\alpha\beta$ teilbar ist, so ergibt sich leicht, daß auch jede durch α^n und β^n teilbare Zahl γ_n des Körpers K durch $\alpha^n\beta^n$ teilbar, also von der Form $\alpha^n\beta^n\gamma'_n$ ist, wo γ'_n eine ganze Zahl bedeutet; setzt man nun $\omega = \alpha\beta\omega'$, so genügt ω' der Gleichung

$$\omega'^m + \gamma'_1\omega'^{m-1} + \cdots + \gamma'_m = 0,$$

deren Koeffizienten ganze Zahlen sind; mithin ist ω' (zufolge 3.) eine ganze Zahl, d. h. ω ist auch teilbar durch $\alpha\beta$, was zu beweisen war.

Hieraus geht hervor, daß man, um das gegenseitige Verhalten zweier ganzen Zahlen α, β zu untersuchen, nur den kleinsten Körper K zu bilden braucht, welchem sie beide angehören; und dieser Körper ist, wie man leicht erkennt, immer von der im vorigen Paragraphen betrachteten Beschaffenheit.

§ 161.

Um den späteren Verlauf der Darstellung nicht zu unterbrechen, schalten wir hier eine sehr allgemeine Betrachtung ein, welche für die nachfolgenden, sowie für viele andere, unserem Gegenstande fremde Untersuchungen von großem Nutzen ist.

1. Ein System $\mathfrak{a}$ von reellen oder komplexen Zahlen α, deren Summen und Differenzen demselben System $\mathfrak{a}$ angehören, soll ein Modul heißen; wenn die Differenz zweier Zahlen ω, ω' in $\mathfrak{a}$ enthalten ist, so wollen wir sie kongruent nach $\mathfrak{a}$ nennen und dies durch die Kongruenz

$$\omega \equiv \omega' \pmod{\mathfrak{a}}$$

andeuten. Solche Kongruenzen können addiert, subtrahiert und folglich auch mit beliebigen ganzen rationalen Zahlen multipliziert werden, wie Gleichungen. Da je zwei einer dritten kongruente Zahlen auch einander kongruent sind, so kann man alle existierenden Zahlen in Klassen (mod $\mathfrak{a}$) einteilen, indem man je zwei kongruente Zahlen in dieselbe Klasse, je zwei inkongruente in zwei verschiedene Klassen aufnimmt.

2. Wenn alle Zahlen eines Moduls $\mathfrak{a}$ auch Zahlen eines Moduls $\mathfrak{b}$ sind, so heiße $\mathfrak{a}$ ein Vielfaches von $\mathfrak{b}$, und $\mathfrak{b}$ ein Teiler von $\mathfrak{a}$; oder wir sagen auch, $\mathfrak{b}$ gehe in $\mathfrak{a}$ auf, $\mathfrak{a}$ sei teilbar durch $\mathfrak{b}$. Aus jeder Kongruenz $\omega \equiv \omega' \pmod{\mathfrak{a}}$ folgt auch $\omega \equiv \omega' \pmod{\mathfrak{b}}$. Offenbar besteht $\mathfrak{b}$ aus einer endlichen oder unendlichen Anzahl von Klassen (mod $\mathfrak{a}$).

Sind $\mathfrak{a}$, $\mathfrak{b}$ irgend zwei Moduln, so bilden alle die Zahlen, welche gleichzeitig in $\mathfrak{a}$ und in $\mathfrak{b}$ enthalten sind, das kleinste gemeinschaftliche Vielfache $\mathfrak{m}$ von $\mathfrak{a}$ und $\mathfrak{b}$, weil jedes gemeinschaftliche Vielfache von $\mathfrak{a}$ und $\mathfrak{b}$ auch durch den Modul $\mathfrak{m}$ teilbar ist. Durchläuft α alle Zahlen des Moduls $\mathfrak{a}$, β alle Zahlen des Moduls $\mathfrak{b}$, so bilden die Zahlen $\alpha + \beta$ den größten gemeinschaftlichen Teiler von $\mathfrak{a}$ und $\mathfrak{b}$, weil jeder gemeinschaftliche Teiler von $\mathfrak{a}$ und $\mathfrak{b}$ auch in dem Modul $\mathfrak{b}$ aufgeht.

3. Sind $\omega_1, \omega_2, \ldots, \omega_n$ gegebene Zahlen, so bilden alle Zahlen von der Form

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

wo $h_1, h_2, \ldots, h_n$ alle ganzen rationalen Zahlen durchlaufen, einen endlichen Modul $\mathfrak{o}$, und wir wollen den Komplex der n Zahlen $\omega_1, \omega_2, \ldots, \omega_n$, mögen sie abhängig oder unabhängig voneinander sein, eine Basis des Moduls $\mathfrak{o}$ nennen. Dann besteht folgender Satz:

Wenn alle Zahlen ω eines endlichen Moduls $\mathfrak{o}$ durch Multiplikation mit rationalen, von Null verschiedenen Zahlen in Zahlen eines Moduls $\mathfrak{m}$ verwandelt werden können, so enthält $\mathfrak{o}$ nur eine endliche Anzahl inkongruenter Zahlen (mod $\mathfrak{m}$).

Da es nämlich n rationale, von Null verschiedene Zahlen $r_1, r_2, \ldots, r_n$ der Art gibt, daß die Produkte $r_1\omega_1, r_2\omega_2, \ldots, r_n\omega_n$ in $\mathfrak{m}$ enthalten sind, so gibt es auch eine ganze rationale, von Null verschiedene Zahl s der Art, daß alle Produkte $s\omega \equiv 0 \pmod{\mathfrak{m}}$ sind. Läßt man daher jede der n ganzen rationalen Zahlen $h_1, h_2, \ldots, h_n$ ein vollständiges Restsystem (mod s) durchlaufen, so entstehen s^n Zahlen ω von der Form (1), und jede Zahl des Moduls $\mathfrak{o}$ ist wenigstens einer derselben kongruent (mod $\mathfrak{m}$); mithin ist die Anzahl der in $\mathfrak{o}$ enthaltenen, nach $\mathfrak{m}$ inkongruenten Zahlen höchstens $= s^n$, was zu beweisen war.

Allein es ist wichtig, die Anzahl dieser inkongruenten Zahlen genau zu bestimmen. Zu diesem Zwecke betrachten wir das kleinste gemeinschaftliche Vielfache $\mathfrak{a}$ der beiden Moduln $\mathfrak{o}$ und $\mathfrak{m}$; da je zwei nach $\mathfrak{m}$ kongruente Zahlen ω, ω' des Moduls $\mathfrak{o}$ auch nach $\mathfrak{a}$ kongruent sind, und umgekehrt, so ist unsere Aufgabe die, die Anzahl der Klassen (mod $\mathfrak{a}$) zu bestimmen, aus welchen $\mathfrak{o}$ besteht. Wir suchen daher zunächst die allgemeine Form aller in $\mathfrak{a}$ enthaltenen Zahlen

$$\alpha = k_1\omega_1 + k_2\omega_2 + \cdots + k_n\omega_n \tag{2}$$

aufzustellen, wo $k_1, k_2, \ldots, k_n$ jedenfalls ganze rationale Zahlen bedeuten. Ist nun r ein bestimmter Index aus der Reihe $1, 2, \ldots, n$, so gibt es unter allen den Zahlen $\alpha = \theta_r$, in welchen $k_{r+1} = 0$, $k_{r+2} = 0$, $\ldots$, $k_n = 0$ ist, auch solche, in denen k_r von Null verschieden ist (z. B. $s\omega_r$), und unter diesen sei

$$\alpha_r = a_1^{(r)}\omega_1 + a_2^{(r)}\omega_2 + \cdots + a_r^{(r)}\omega_r \tag{3}$$

eine solche, in welcher k_r den kleinsten positiven Wert $a_r^{(r)}$ besitzt. Dann leuchtet ein, daß der Wert von k_r in jeder Zahl θ_r durch $a_r^{(r)}$

teilbar, also von der Form $a_r^{(r)} x_r$ ist, wo x_r eine ganze rationale Zahl bedeutet, und daß folglich $\theta_r - x_r \alpha_r = \theta_{r-1}$ eine Zahl α ist, in welcher $k_r, k_{r+1}, \ldots, k_n$ verschwinden. Hieraus folgt sofort, daß, nachdem man für jeden Index r eine solche partikuläre Zahl α_r des Moduls $\mathfrak{a}$ aufgestellt hat*), jede Zahl α gewiß in die Form

$$\alpha = x_1 \alpha_1 + x_2 \alpha_2 + \cdots + x_n \alpha_n \tag{4}$$

gebracht werden kann, wo $x_1, x_2, \ldots, x_n$ ganze rationale Zahlen bedeuten, aus welchen die in der Form (2) vorkommenden Zahlen $k_1, k_2, \ldots, k_n$ durch die Gleichungen

$$k_r = a_r^{(r)} x_r + a_r^{(r+1)} x_{r+1} + \cdots + a_r^{(n)} x_n \tag{5}$$

abgeleitet werden; und umgekehrt sind alle Zahlen α von der Form (4) in $\mathfrak{a}$ enthalten.

Ist nun eine Zahl ω von der Form (1) gegeben, sind also $h_1, h_2, \ldots, h_n$ gegebene rationale ganze Zahlen, so sind alle Zahlen ω' des Moduls $\mathfrak{o}$, welche ihr nach $\mathfrak{m}$ kongruent sind, welche also eine Klasse (mod $\mathfrak{a}$) bilden, von der Form

$$\omega' = \omega + \alpha = h_1' \omega_1 + h_2' \omega_2 + \cdots + h_n' \omega_n, \tag{6}$$

wo zufolge (5)

$$h_r' = h_r + a_r^{(r)} x_r + a_r^{(r+1)} x_{r+1} + \cdots + a_r^{(n)} x_n$$

ist, und hieraus folgt, daß man sukzessive die willkürlichen rationalen ganzen Zahlen $x_n, x_{n-1}, \ldots, x_2, x_1$ stets und nur auf eine einzige Art so bestimmen kann, daß die n Zahlen h_r' den Bedingungen

$$0 \leqq h_r' < a_r^{(r)} \tag{7}$$

genügen. In jeder Klasse existiert daher ein und nur ein Repräsentant ω' von der Form (6), welcher diesen Bedingungen (7) genügt; mithin ist die Anzahl der verschiedenen Klassen (mod $\mathfrak{a}$), aus welchen der Modul $\mathfrak{o}$ besteht, gleich dem Produkte $a_1' a_2'' \ldots a_n^{(n)}$, d. h. gleich der Determinante des Koeffizientensystems in den n partikulären Zahlen α_r von der Form (3), welche eine Basis von $\mathfrak{a}$ bilden**).

*) Das System dieser n partikulären Zahlen wird ein vollständig bestimmtes, wenn man die Bedingung hinzufügt, daß $0 \leq a_r^{(r')} < a_r^{(r)}$ sein soll, wenn $r' > r$ ist.

**) Die weitere Entwicklung der allgemeinen Theorie der Moduln würde uns hier zu weit führen (vgl. § 163); wir erwähnen nur noch folgenden Satz: Sind die Basiszahlen eines endlichen Moduls voneinander abhängig, so gibt es immer eine aus unabhängigen Zahlen bestehende Basis desselben Moduls. Die eleganteste Methode, die neue Basis aufzufinden, besteht in einer Verallgemeinerung der von Gauß angewandten Behandlung der partialen Determinanten (D. A. artt. 234, 236, 279).

§ 162.

Wir beschränken uns von jetzt an auf die Untersuchung der ganzen Zahlen, welche in einem endlichen Körper Ω (§ 159) enthalten sind.

1. Da jede algebraische Zahl (zufolge § 160, 5.) durch Multiplikation mit einer rationalen ganzen von Null verschiedenen Zahl in eine ganze Zahl verwandelt werden kann, so dürfen wir annehmen, daß die Zahlen $\omega_1, \omega_2, \ldots, \omega_n$, welche eine Basis des Körpers Ω bilden, sämtlich ganze Zahlen sind, und es wird dann (zufolge § 160, 1.) jede Zahl

$$\omega = \Sigma h_\iota \omega_\iota \tag{1}$$

gewiß eine ganze Zahl sein, wenn ihre Koordinaten h_ι rationale ganze Zahlen sind; aber dies läßt sich im allgemeinen nicht umkehren, d. h. es kann ω sehr wohl eine ganze Zahl sein, auch wenn ihre Koordinaten teilweise oder sämtlich gebrochene Zahlen sind. Dies ist einer der wichtigsten Punkte der Theorie und muß deshalb vor allem aufgeklärt werden.

Wir schicken zunächst die einleuchtende Bemerkung voraus, daß die Diskriminante [§ 159, (10)] eines jeden Systems von n unabhängigen ganzen Zahlen gewiß eine von Null verschiedene rationale, und zwar ganze Zahl ist, weil sie durch Addition, Subtraktion und Multiplikation aus lauter ganzen Zahlen gebildet ist. Gibt es nun wirklich in Ω eine ganze Zahl

$$\beta = \frac{\Sigma k_\iota \omega_\iota}{s}, \tag{2}$$

wo $s, k_1, k_2, \ldots, k_n$ ganze rationale Zahlen ohne gemeinschaftlichen Teiler bedeuten, deren erste $s > 1$ ist, so behaupten wir, daß s^2 in der Diskriminante $\Delta(\omega_1, \omega_2, \ldots, \omega_n)$ aufgeht, und daß man eine neue Basis von ganzen Zahlen $\beta_1, \beta_2, \ldots, \beta_n$ aufstellen kann, deren Diskriminante absolut genommen $< \Delta(\omega_1, \omega_2, \ldots, \omega_n)$ ist.

Um dies zu beweisen, bezeichnen wir mit $\mathfrak{m}$ den aus allen durch s teilbaren ganzen Zahlen bestehenden Modul, ebenso mit $\mathfrak{o}$ das System aller Zahlen ω von der Form (1), deren Koordinaten h_ι ganze Zahlen sind; da jedes Produkt $s\omega$ eine Zahl des Moduls $\mathfrak{m}$ ist, so können wir die allgemeine Untersuchung des vorigen Paragraphen auf unsern

Fall anwenden. Alle durch s teilbaren Zahlen α des Systems $\mathfrak{o}$ sind daher von der Form

$$\alpha = \Sigma x_\iota \alpha_\iota = s \Sigma x_\iota \beta_\iota,$$

wo die n Zahlen $\alpha_\iota = s\beta_\iota$ partikuläre Zahlen α, also die β_ι ganze Zahlen des Körpers Ω, und die x_ι willkürliche rationale ganze Zahlen bedeuten.

Da nun alle Zahlen $s\omega$ auch solche Zahlen α sind, so kann man

$$\omega_r = \Sigma b_\iota^{(r)} \beta_\iota, \quad \Delta(\omega_1, \omega_2, \ldots, \omega_n) = b^2 \Delta(\beta_1, \beta_2, \ldots, \beta_n)$$

setzen, wo die Koeffizienten $b_\iota^{(r)}$ rationale ganze Zahlen sind und b die aus ihnen gebildete Determinante bedeutet; durch Umkehrung ergibt sich, daß die n Produkte $b\beta_\iota$, mithin auch alle Quotienten $b\alpha : s$ Zahlen des Systems $\mathfrak{o}$ sind.

Wenden wir dies Resultat auf die obige Voraussetzung (2) an, daß die Zahl β eine ganze Zahl, ihr Zähler $\Sigma k_\iota \omega_\iota$ also eine Zahl α ist, obgleich die Zahlen $s, k_1, k_2, \ldots, k_n$ keinen gemeinschaftlichen Teiler haben, so folgt unmittelbar, daß b durch s teilbar ist, wodurch zugleich die obigen Behauptungen erwiesen sind.

Da nun die Diskriminante eines jeden Systems von n unabhängigen ganzen Zahlen des Körpers Ω eine von Null verschiedene ganze rationale Zahl ist, so gibt es unter allen diesen Diskriminanten eine solche, deren Wert — abgesehen vom Vorzeichen — ein Minimum ist, und aus der vorstehenden Untersuchung folgt unmittelbar, daß, wenn eine Basis aus solchen ganzen Zahlen $\omega_1, \omega_2, \ldots, \omega_n$ besteht, deren Diskriminante diesen Minimumwert besitzt, die entsprechenden Koordinaten h_ι einer jeden ganzen Zahl ω des Körpers notwendig ganze rationale Zahlen sein müssen. Eine solche Basis $\omega_1, \omega_2, \ldots, \omega_n$ wollen wir eine Grundreihe des Körpers Ω nennen; aus ihr ergeben sich alle anderen Grundreihen desselben Körpers, wenn man n ganze Zahlen ω von der Form (1) so wählt, daß die aus den n^2 zugehörigen Koordinaten gebildete Determinante $= \pm 1$ wird.

Die wichtigste Rolle spielt aber die Minimaldiskriminante selbst, sowohl hinsichtlich der inneren*) Konstitution des Körpers Ω, als

*) Vgl. Kronecker: Über die algebraisch auflösbaren Gleichungen (Monatsbericht der Berliner Ak. 14. April 1856).

auch hinsichtlich seiner Verwandtschaft mit anderen Körpern*); wir wollen daher diese positive oder negative ganze rationale Zahl die Grundzahl oder die Diskriminante des Körpers Ω nennen und mit $\Delta(\Omega)$ bezeichnen; sie ist offenbar zugleich die Grundzahl eines jeden mit Ω konjugierten Körpers.

Die Zahlen eines quadratischen Körpers sind z. B. von der Form $t + u\sqrt{D}$, wo t, u alle rationalen Zahlen durchlaufen und D eine ganze rationale Zahl bedeutet, welche kein Quadrat und auch durch kein Quadrat außer 1 teilbar ist. Ist $D \equiv 1 \pmod 4$, so bilden die Zahlen 1 und $\frac{1}{2}(1 + \sqrt{D})$ eine Grundreihe des Körpers, und seine Grundzahl ist $= D$; ist dagegen $D \equiv 2$ oder $\equiv 3 \pmod 4$, so bilden die Zahlen 1 und $\sqrt{D}$ eine Grundreihe des Körpers, und seine Grundzahl ist $= 4D$.

Ist ferner θ eine primitive Wurzel der Gleichung $\theta^m = 1$ (§ 139), wo $m > 2$, so bilden die Zahlen $1, \theta, \theta^2, \ldots, \theta^{n-1}$ die Grundreihe eines Körpers vom Grade $n = \varphi(m)$, dessen Grundzahl

$$\left(\frac{m\sqrt{-1}}{\sqrt[a-1]{a}\,\sqrt[b-1]{b}\,\sqrt[c-1]{c}\ldots} \right)^n$$

ist, wo $a, b, c \ldots$ alle verschiedenen in m aufgehenden Primzahlen bedeuten. Ist $m = 3$ (oder $= 6$), so ist dieser Körper ein quadratischer, seine Grundzahl $= -3$; ist $m = 4$, so ist die Grundzahl des quadratischen Körpers $= -4$.

2. Aus den vorstehenden Prinzipien ergibt sich leicht der folgende Fundamentalsatz:

Ist μ eine von Null verschiedene ganze Zahl des Körpers Ω, so ist die Anzahl der nach dem Modul μ inkongruenten ganzen Zahlen des Körpers gleich dem absoluten Wert der Norm des Moduls μ.

Es sei $\mathfrak{m}$ das System aller durch μ teilbaren ganzen Zahlen (welche sich durch Addition und Subtraktion reproduzieren) und $\mathfrak{o}$

*) Die erste Spur dieser Beziehungen hat sich bei einer schönen Untersuchung von Kronecker gezeigt (Mémoire sur les facteurs irréductibles de l'expression $x^n - 1$; Journ. de Math., p. p. Liouville; T. XIX, 1854). Um den Charakter dieser Gesetze, deren Entwicklung ich mir auf eine andere Gelegenheit erspare, näher anzudeuten, führe ich nur das einfachste Beispiel an: das kleinste gemeinschaftliche Multiplum zweier voneinander verschiedenen quadratischen Körper A, B ist ein biquadratischer Körper K, der noch einen dritten quadratischen Körper C zum Divisor hat; die Grundzahl von K ist gleich dem Produkt aus den Grundzahlen von A, B, C, und zwar eine Quadratzahl.

das System aller ganzen Zahlen des Körpers Ω, d. h. aller Zahlen ω von der Form (1), wo die Zahlen ω_i eine Grundreihe des Körpers bilden und die Koordinaten h_i beliebige ganze rationale Zahlen bedeuten; da jeder Quotient $\omega : \mu$ (zufolge § 160, 5.) durch Multiplikation mit einer von Null verschiedenen ganzen rationalen Zahl in eine ganze Zahl verwandelt werden kann, so ist die Untersuchung des vorigen Paragraphen auf unseren Fall anwendbar. Mithin sind alle durch μ teilbaren Zahlen α des Systems $\mathfrak{o}$ von der Form

$$\alpha = \Sigma x_i \alpha_i = \mu \Sigma x_i \beta_i,$$

wo die n Zahlen $\alpha_i = \mu \beta_i$ partikuläre Zahlen α bedeuten, also die Zahlen β_i in $\mathfrak{o}$ enthalten sind, und die Größen x_i alle rationalen ganzen Zahlwerte annehmen dürfen; die Anzahl der Klassen, in welche das System $\mathfrak{o}$ in bezug auf den Modul μ zerfällt, ist ferner gleich der aus den Koordinaten der n Zahlen $\alpha_1, \alpha_2, \ldots, \alpha_n$ gebildeten Determinante a. Zugleich ist [nach § 159, (11), (12)]

$$\Delta(\alpha_1 \ldots \alpha_n) = a^2 \Delta(\Omega) = N(\mu)^2 \Delta(\beta_1 \ldots \beta_n);$$

da nun jede durch μ teilbare Zahl $\alpha = \mu\omega$ des Systems $\mathfrak{o}$ die Form $\mu \Sigma x_i \beta_i$ besitzt, so ist jede Zahl ω des Systems $\mathfrak{o}$ auch von der Form $\Sigma x_i \beta_i$; mithin bilden die Zahlen β_i ebenfalls eine Grundreihe des Körpers, und folglich ist $\Delta(\beta_1 \ldots \beta_n) = \Delta(\Omega)$, also $a = \pm N(\mu)$, was zu beweisen war.

Zugleich leuchtet ein, daß nach der Methode des vorigen Paragraphen ein System von a inkongruenten Repräsentanten der verschiedenen Klassen, also ein vollständiges Restsystem für den Modul μ aufgestellt werden kann*).

3. Will man jetzt zwei gegebene ganze Zahlen θ, μ darauf prüfen, ob sie relative Primzahlen sind, so braucht man offenbar ω nur ein vollständiges Restsystem (mod μ) durchlaufen zu lassen und nachzusehen, wie oft $\theta\omega \equiv 0 \pmod{\mu}$ wird; zeigt sich, daß dies nur dann eintritt, wenn $\omega \equiv 0 \pmod{\mu}$ ist, so ist also jede durch θ und

*) Bilden die n Zahlen ω_i irgendeine Basis des Körpers Ω, und ist $\mathfrak{o}$ das System aller der Zahlen ω von der Form (1), deren Koordinaten ganze Zahlen sind, so reproduzieren sich die Zahlen des Systems $\mathfrak{o}$ durch Addition und Subtraktion; nimmt man ferner an, daß sie sich auch durch Multiplikation reproduzieren, woraus zugleich folgt, daß sie ganze Zahlen sind, und nennt man zwei solche Zahlen ω, ω' stets und nur dann kongruent in bezug auf eine dritte solche Zahl μ, wenn der Quotient $(\omega - \omega') : \mu$ wieder eine Zahl des Systems $\mathfrak{o}$ ist, so ist die Anzahl der in $\mathfrak{o}$ enthaltenen, nach μ inkongruenten Zahlen ebenfalls $= \pm N(\mu)$. Vgl. § 165, 4.

μ teilbare ganze Zahl $\theta\omega$ auch teilbar durch $\theta\mu$, mithin sind θ, μ relative Primzahlen; besitzt aber die Kongruenz $\theta\omega \equiv 0 \pmod{\mu}$ auch eine Wurzel ω, welche nicht $\equiv 0 \pmod{\mu}$ ist, so ist die entsprechende Zahl $\theta\omega$ durch θ und μ, aber nicht durch $\theta\mu$ teilbar, mithin sind θ, μ keine relative Primzahlen.

Ist θ relative Primzahl zu μ (z. B. $\theta = 1$), so durchläuft $\theta\omega$ gleichzeitig mit ω ein vollständiges Restsystem (mod μ); folglich hat jede Kongruenz $\theta\omega \equiv \theta' \pmod{\mu}$ immer eine und nur eine Wurzel ω (vgl. § 22); ist ferner $\psi(\mu)$ die Anzahl aller Klassen, deren Zahlen relative Primzahlen zum Modul μ sind, so durchläuft $\theta\omega$ gleichzeitig mit ω die Repräsentanten aller dieser Klassen, und da das Produkt dieser Zahlen ω auch relative Primzahl zu μ ist, so ergibt sich der Satz

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

welcher dem Fermatschen Satze (§ 19) entspricht.

4. Verfolgt man diese Analogie mit der rationalen Zahlentheorie weiter, so drängt sich immer wieder die Frage nach der Zusammensetzung der Zahlen des Systems $\mathfrak{o}$ (d. h. der ganzen Zahlen des Körpers Ω) aus Faktoren auf, welche demselben System $\mathfrak{o}$ angehören, und es zeigt sich zunächst, daß die unbegrenzte Zerlegbarkeit der ganzen Zahlen, wie sie in dem unendlichen Körper aller algebraischen Zahlen auftrat (§ 160, 7.), in einem endlichen Körper Ω wieder verschwindet. Dafür tritt aber bei unendlich vielen solchen Körpern Ω ein höchst eigentümliches Phänomen auf, das schon früher (§ 16) gelegentlich erwähnt ist*). Nennt man eine Zahl in $\mathfrak{o}$ zerlegbar, wenn sie das Produkt aus zwei Zahlen in $\mathfrak{o}$ ist, welche beide keine Einheiten sind, dagegen unzerlegbar, wenn dies nicht der Fall ist, so ist offenbar jede zerlegbare Zahl μ darstellbar als Produkt aus einer endlichen Anzahl von unzerlegbaren Zahlen (vgl. § 8), weil die Norm von μ gleich dem Produkte aus den Normen der einzelnen Faktoren ist (§ 159); aber es zeigt sich häufig, daß diese Zerlegung nicht

*) Das dortige Beispiel paßt freilich nicht ganz hierher, insofern die ganzen Zahlen des der Gleichung $\varrho^2 = -11$ entsprechenden quadratischen Körpers nicht durch die Form $t + u\varrho$, wohl aber durch die Form $t + u\theta$ erschöpft werden, wo $2\theta = 1 + \varrho$ ist; die Zahlen 3, 5, $2+\varrho$, $2-\varrho$ sind in der Tat zerlegbar: $3 = \theta(1-\theta)$, $5 = (1+\theta)(2-\theta)$, $2-\varrho = -\theta(1+\theta)$, $2+\varrho = -(1-\theta)(2-\theta)$; die vier Zahlen θ, $1-\theta$, $1+\theta$, $2-\theta$ sind Primzahlen in diesem Körper. Die in Rede stehende Erscheinung tritt aber in dem der Gleichung $x^2 = -5$ entsprechenden quadratischen Körper an dem Beispiel $3 \cdot 7 = (1+2x)(1-2x)$ wirklich auf (vgl. § 71; die beiden Zahlen 3, 7 sind durch die Hauptform der Determinante -5 nicht darstellbar).

eine vollkommen bestimmte ist, sondern daß mehrere wesentlich verschiedene Zerlegungen derselben Zahl in unzerlegbare Faktoren existieren (§ 160, 6.). Dies widerspricht so sehr dem in der rationalen Zahlentheorie herrschenden Begriffe des Primzahlcharakters (§ 8), daß wir deshalb eine unzerlegbare Zahl als solche noch nicht als Primzahl anerkennen wollen; wir suchen daher für den wahren Primzahlcharakter ein kräftigeres Kriterium als diese unzulängliche Unzerlegbarkeit aufzustellen, ähnlich wie früher bei dem Begriffe der relativen Primzahl (§ 160, 7.), indem wir die zu untersuchende Zahl μ nicht zerlegen, sondern ihr Verhalten als Modul betrachten:

Eine ganze Zahl μ, welche keine Einheit ist, soll eine Primzahl heißen, wenn jedes durch μ teilbare Produkt $\eta\varrho$ wenigstens einen durch μ teilbaren Faktor η oder ϱ besitzt.

Es ergibt sich dann sofort, daß die höchste in einem Produkte aufgehende Potenz einer Primzahl μ das Produkt aus den höchsten in den einzelnen Faktoren aufgehenden Potenzen von μ, und daß jede durch μ nicht teilbare Zahl relative Primzahl zu μ ist. Man erkennt ferner leicht, daß die kleinste durch μ teilbare rationale ganze Zahl p notwendig eine Primzahl (im Körper der rationalen Zahlen), und folglich die Norm von μ eine Potenz von p, nämlich ein rationaler Divisor von $N(p) = p^n$ sein muß. Es werden daher gewiß alle Primzahlen μ des Körpers Ω entdeckt, wenn die Divisoren aller rationalen Primzahlen p aufgesucht werden.

5. Ist aber μ keine Primzahl (und auch keine Einheit), existieren also zwei durch μ nicht teilbare Zahlen η, ϱ, deren Produkt $\eta\varrho$ durch μ teilbar ist, so schreiten wir zu einer Zerlegung von μ in wirkliche oder ideale, d. h. fingierte Faktoren. Gibt es nämlich in $\mathfrak{o}$ einen größten gemeinschaftlichen Teiler ν der beiden Zahlen η und $\mu = \nu\mu'$, der Art, daß die Quotienten $\eta : \nu$ und $\mu : \nu$ relative Primzahlen sind, so ist μ in die beiden Faktoren ν und μ' zerlegt, von denen keiner eine Einheit ist, weil weder ϱ noch η durch μ teilbar ist. Der Faktor μ' ist wesentlich dadurch bestimmt, daß alle Wurzeln α' der Kongruenz $\eta\alpha' \equiv 0 \pmod{\mu}$ durch μ' teilbar sind (z. B. auch $\alpha' = \varrho$), und daß ebenso jede durch μ' teilbare Zahl α' auch der vorstehenden Kongruenz genügt. Umgekehrt, gibt es in $\mathfrak{o}$ eine Zahl μ', welche in allen Wurzeln α' der Kongruenz $\eta\alpha' \equiv 0 \pmod{\mu}$ und nur in diesen aufgeht, so ist auch μ teilbar durch μ', und der Quotient $\nu = \mu : \mu'$ ist der größte gemeinschaftliche Teiler der beiden Zahlen η und μ.

Aber es kann sehr wohl der Fall eintreten, daß in $\mathfrak{o}$ keine solche Zahl μ' zu finden ist; als nun diese Erscheinung (bei den aus Einheitswurzeln gebildeten Zahlen) Kummer entgegentrat, so kam er auf den glücklichen Gedanken, trotzdem eine solche Zahl μ' zu fingieren und dieselbe als ideale Zahl einzuführen; die Teilbarkeit einer Zahl α' durch diese ideale Zahl μ' besteht lediglich darin, daß α' eine Wurzel der Kongruenz $\eta\alpha' \equiv 0 \pmod{\mu}$ ist, und da diese idealen Zahlen in der Folge immer nur als Teiler oder Moduln auftreten, so hat diese Art ihrer Einführung durchaus keine Bedenken. Allein die Befürchtung, daß die unmittelbare Übertragung der bei den wirklichen Zahlen üblichen Benennungen auf die idealen Zahlen im Anfang leicht Mißtrauen gegen die Sicherheit der Beweisführung einflößen könnte, veranlaßt uns, die Untersuchung dadurch in ein anderes Gewand einzukleiden, daß wir immer ganze Systeme von wirklichen Zahlen betrachten.

§ 163.

Wir gründen die Theorie der in $\mathfrak{o}$ enthaltenen Zahlen, d. h. aller ganzen Zahlen des Körpers Ω, auf den folgenden neuen Begriff.

1. Ein System $\mathfrak{a}$ von unendlich vielen in $\mathfrak{o}$ enthaltenen Zahlen soll ein Ideal heißen, wenn es den beiden Bedingungen genügt:

I. Die Summe und die Differenz je zweier Zahlen in $\mathfrak{a}$ sind wieder Zahlen in $\mathfrak{a}$.

II. Jedes Produkt aus einer Zahl in $\mathfrak{a}$ und einer Zahl in $\mathfrak{o}$ ist wieder eine Zahl in $\mathfrak{a}$.

Ist α in $\mathfrak{a}$ enthalten, so sagen wir, α sei teilbar durch $\mathfrak{a}$, $\mathfrak{a}$ gehe in α auf, weil die Ausdrucksweise hierdurch an Leichtigkeit gewinnt. Wir nennen ferner zwei in $\mathfrak{o}$ enthaltene Zahlen ω, ω', deren Differenz durch $\mathfrak{a}$ teilbar ist, kongruent nach $\mathfrak{a}$ (vgl. § 161), und bezeichnen dies durch die Kongruenz $\omega \equiv \omega' \pmod{\mathfrak{a}}$; solche Kongruenzen dürfen (zufolge I.) addiert, subtrahiert und (zufolge II.) multipliziert werden, wie Gleichungen. Da je zwei einer dritten kongruente Zahlen auch einander kongruent sind, so kann man alle Zahlen in Klassen (mod $\mathfrak{a}$) einteilen, indem man je zwei kongruente Zahlen in dieselbe, je zwei inkongruente Zahlen in zwei verschiedene Klassen wirft; da nun, wenn μ eine von Null verschiedene Zahl in $\mathfrak{a}$ bedeutet, je zwei nach μ kongruente Zahlen (zufolge II.) auch nach $\mathfrak{a}$ kongruent sind — woraus zugleich folgt, daß $\mathfrak{a}$ aus einer oder

mehreren Klassen (mod μ) besteht —, so ist (zufolge § 162, 2.) die Anzahl der Klassen (mod $\mathfrak{a}$), in welche $\mathfrak{o}$ zerfällt, endlich*). Wählt man aus jeder Klasse ein Individuum als Repräsentanten, so bilden dieselben ein vollständiges Restsystem (mod $\mathfrak{a}$); die Anzahl dieser Klassen oder inkongruenten Zahlen soll die Norm von $\mathfrak{a}$ heißen und mit $N(\mathfrak{a})$ bezeichnet werden.

Ist η eine von Null verschiedene Zahl in $\mathfrak{o}$, so bilden alle durch η teilbaren Zahlen in $\mathfrak{o}$ ein Ideal, welches mit $\mathfrak{i}(\eta)$ bezeichnet werden soll; solche Ideale sind besonders ausgezeichnet und sollen Hauptideale heißen; die Norm von $\mathfrak{i}(\eta)$ ist $= \pm N(\eta)$; ist η eine Einheit, so ist $\mathfrak{i}(\eta) = \mathfrak{o}$, und umgekehrt.

2. Wenn alle Zahlen eines Ideals $\mathfrak{a}$ auch in einem Ideal $\mathfrak{b}$ enthalten sind, so besteht offenbar $\mathfrak{b}$ aus einer oder mehreren Klassen (mod $\mathfrak{a}$), und wir wollen sagen, $\mathfrak{a}$ sei ein Multiplum von $\mathfrak{b}$ oder teilbar durch $\mathfrak{b}$, $\mathfrak{b}$ sei ein Teiler von $\mathfrak{a}$ oder gehe in $\mathfrak{a}$ auf.

Besteht $\mathfrak{b}$ aus r Klassen (mod $\mathfrak{a}$), so ist $N(\mathfrak{a}) = rN(\mathfrak{b})$. Durchläuft nämlich δ die Repräsentanten dieser r Klassen und γ ein vollständiges Restsystem (mod $\mathfrak{b}$), so bilden die $rN(\mathfrak{b})$ Zahlen $\gamma + \delta$ ein vollständiges Restsystem (mod $\mathfrak{a}$); denn erstens ist jede Zahl in $\mathfrak{o}$ kongruent einer Zahl γ (mod $\mathfrak{b}$), also $\equiv \gamma + \delta$ (mod $\mathfrak{a}$), und zweitens folgt aus $\gamma + \delta \equiv \gamma' + \delta'$ (mod $\mathfrak{a}$), wo γ', δ' ähnliche Bedeutung haben wie γ, δ, sukzessive $\gamma + \delta \equiv \gamma' + \delta'$ (mod $\mathfrak{b}$), $\gamma \equiv \gamma'$ (mod $\mathfrak{b}$), $\gamma = \gamma'$, also $\delta \equiv \delta'$ (mod $\mathfrak{a}$), $\delta = \delta'$, d. h. die sämtlichen Zahlen $\gamma + \delta$ sind inkongruent (mod $\mathfrak{a}$).

Ein Ideal besitzt folglich nur eine endliche Anzahl von Teilern. Ist $\mathfrak{m}$ teilbar durch $\mathfrak{a}$, $\mathfrak{a}$ durch $\mathfrak{b}$, so ist auch $\mathfrak{m}$ durch $\mathfrak{b}$ teilbar. Das Hauptideal $\mathfrak{o}$ selbst geht in jedem Ideal auf und ist zugleich das einzige Ideal, welches die Zahl 1 oder überhaupt Einheiten enthält, und dessen Norm $= 1$ ist.

Das System aller derjenigen Zahlen, welche gleichzeitig in zwei Idealen $\mathfrak{a}$, $\mathfrak{b}$ enthalten sind, ist das kleinste gemeinschaftliche Multiplum $\mathfrak{m}$ von $\mathfrak{a}$, $\mathfrak{b}$, insofern jedes gemeinschaftliche Multiplum von $\mathfrak{a}$, $\mathfrak{b}$ durch das Ideal $\mathfrak{m}$ teilbar ist. Durchläuft α alle Zahlen in $\mathfrak{a}$, β alle Zahlen in $\mathfrak{b}$, so ist das System aller Zahlen $\alpha + \beta$ der

*) Dasselbe ergibt sich unmittelbar aus § 161; ist nämlich ω irgendeine Zahl in $\mathfrak{o}$, so kann durch Multiplikation mit einer von Null verschiedenen ganzen rationalen Zahl der Quotient $\omega : \mu$ in eine ganze Zahl, also ω (zufolge II.) in eine Zahl des Ideals $\mathfrak{a}$ verwandelt werden.

größte gemeinschaftliche Teiler $\mathfrak{d}$ der Ideale $\mathfrak{a}$, $\mathfrak{b}$, weil jeder gemeinschaftliche Teiler von $\mathfrak{a}$, $\mathfrak{b}$ in dem Ideale $\mathfrak{d}$ aufgeht*).

Ist r die Anzahl der in $\mathfrak{b}$ enthaltenen Zahlen, welche (mod $\mathfrak{a}$) inkongruent sind, so besteht $\mathfrak{b}$ aus r Klassen (mod $\mathfrak{m}$), und $\mathfrak{b}$ aus r Klassen (mod $\mathfrak{a}$); also ist $N(\mathfrak{m}) = rN(\mathfrak{b})$, $N(\mathfrak{a}) = rN(\mathfrak{d})$ und $N(\mathfrak{m})N(\mathfrak{d}) = N(\mathfrak{a})N(\mathfrak{b})$.

Ist $\mathfrak{b}$ ein Hauptideal $= \mathfrak{i}(\eta)$, so ist die Anzahl r der in $\mathfrak{b}$ enthaltenen Zahlen $\beta = \eta\omega$, welche (mod $\mathfrak{a}$) inkongruent sind, zugleich die Norm des aus allen Wurzeln ϱ der Kongruenz $\eta\varrho \equiv 0$ (mod $\mathfrak{a}$) bestehenden Ideals $\mathfrak{r}$, weil zwei Zahlen ω, ω' stets und nur dann kongruent (mod $\mathfrak{r}$) sind, wenn $\eta\omega \equiv \eta\omega'$ (mod $\mathfrak{a}$) ist. Mithin ist in diesem Falle $N(\mathfrak{a}) = N(\mathfrak{r})N(\mathfrak{b})$.

3. Ein von $\mathfrak{o}$ verschiedenes Ideal $\mathfrak{p}$, welches keinen von $\mathfrak{o}$ und $\mathfrak{p}$ verschiedenen Teiler besitzt, soll ein Primideal heißen. Dann gilt folgender Satz:

Ist $\eta\varrho \equiv 0$ (mod $\mathfrak{p}$), so ist wenigstens eine der beiden Zahlen η, ϱ durch $\mathfrak{p}$ teilbar. Ist nämlich η nicht $\equiv 0$ (mod $\mathfrak{p}$), so bilden die sämtlichen Wurzeln ϱ der Kongruenz $\eta\varrho \equiv 0$ (mod $\mathfrak{p}$) offenbar ein in $\mathfrak{p}$ aufgehendes Ideal, welches, da es die Zahl 1 nicht enthält, von $\mathfrak{o}$ verschieden und folglich mit $\mathfrak{p}$ identisch ist, was zu beweisen war.

Dieser Satz ist charakteristisch für ein Primideal, da er sich folgendermaßen umkehren läßt: Enthält jedes durch ein (von $\mathfrak{o}$ verschiedenes) Ideal $\mathfrak{p}$ teilbare Produkt mindestens einen durch $\mathfrak{p}$ teilbaren Faktor, so ist $\mathfrak{p}$ ein Primideal. Ist nämlich $\mathfrak{q}$ ein Teiler des Ideals $\mathfrak{p}$, aber verschieden von $\mathfrak{p}$, so gibt es in $\mathfrak{q}$ eine nicht in $\mathfrak{p}$ enthaltene Zahl ω; dann ist (zufolge der Annahme) auch keine der Potenzen $\omega^2, \omega^3 \ldots$ durch $\mathfrak{p}$ teilbar; da aber nur eine endliche Anzahl von inkongruenten Zahlen (mod $\mathfrak{p}$) existiert, so muß einmal für zwei verschiedene Exponenten m und $m + s > m$ notwendig $\omega^{m+s} \equiv \omega^m$ (mod $\mathfrak{p}$), also das Produkt $\omega^m(\omega^s - 1)$ durch $\mathfrak{p}$ teilbar sein; da nun ω^m nicht durch $\mathfrak{p}$ teilbar ist, so muß (zufolge der Annahme) der andere Faktor $\omega^s - 1$ durch $\mathfrak{p}$, und folglich auch durch $\mathfrak{q}$ teilbar sein; nun ist ω und, weil $s > 0$ ist, auch $\omega^s \equiv 0$ (mod $\mathfrak{q}$), mithin ist auch die Zahl 1 in $\mathfrak{q}$ enthalten, also $\mathfrak{q} = \mathfrak{o}$, was zu beweisen war.

*) Die Erweiterung dieser Definitionen von $\mathfrak{m}$ und $\mathfrak{d}$ für mehr als zwei Ideale $\mathfrak{a}$, $\mathfrak{b}$ ... liegt auf der Hand.

Nennt man ein von $\mathfrak{o}$ verschiedenes Ideal zusammengesetzt, wenn es kein Primideal ist, so läßt sich dieser Satz auch so aussprechen: Ist $\mathfrak{a}$ ein zusammengesetztes Ideal, so gibt es zwei durch $\mathfrak{a}$ nicht teilbare Zahlen η, ϱ, deren Produkt $\eta\varrho$ durch $\mathfrak{a}$ teilbar ist. Wir beweisen ihn zum zweiten Male auf folgende Art. Es sei $\mathfrak{e}$ ein von $\mathfrak{a}$ und $\mathfrak{o}$ verschiedener Teiler von $\mathfrak{a}$, so gibt es in $\mathfrak{e}$ eine durch $\mathfrak{a}$ nicht teilbare Zahl η, und der größte gemeinschaftliche Teiler $\mathfrak{b}$ von $\mathfrak{a}$ und $\mathfrak{i}(\eta)$ ist teilbar durch $\mathfrak{e}$, also von $\mathfrak{o}$ verschieden, mithin ist $N(\mathfrak{b}) > 1$. Das aus allen Wurzeln ϱ der Kongruenz $\eta\varrho \equiv 0 \pmod{\mathfrak{a}}$ bestehende Ideal $\mathfrak{r}$ ist ein Teiler von $\mathfrak{a}$, und da (zufolge 2.) $N(\mathfrak{a}) = N(\mathfrak{r})\,N(\mathfrak{b}) > N(\mathfrak{r})$ ist, so ist $\mathfrak{r}$ verschieden von $\mathfrak{a}$ und enthält folglich eine durch $\mathfrak{a}$ nicht teilbare Zahl ϱ, was zu beweisen war.

Es leuchtet nun ein, daß die kleinste (von Null verschiedene) rationale Zahl p, welche in einem Primideale $\mathfrak{p}$ enthalten ist, notwendig eine Primzahl (im rationalen Zahlkörper) sein muß; da ferner $\mathfrak{p}$ in $\mathfrak{i}(p)$ aufgeht, so ist $N(\mathfrak{p})$ ein Teiler von $N(p) = p^n$, also ebenfalls eine Potenz p^f der rationalen Primzahl p, und man findet leicht (vgl. § 162, 3.), daß jede in $\mathfrak{o}$ enthaltene Zahl ω der Kongruenz

$$\omega^{p^f} \equiv \omega \pmod{\mathfrak{p}}$$

genügt*). Auch hat es keine Schwierigkeit, die allgemeinen Sätze der §§ 26, 27, 29, 30, 31 auf Kongruenzen in bezug auf den Modul $\mathfrak{p}$ zu übertragen.

*) Hierauf beruht das Eingreifen der Theorie der höheren Kongruenzen (vgl. § 26), welche zur Bestimmung der Primideale dient. Für die Körper vom Grade $n = \varphi(m)$, welche aus den primitiven Wurzeln θ der Gleichung $\theta^m = 1$ entspringen, ist dieselbe zuerst ausgeführt, und zwar von Kummer, dem Schöpfer der Theorie der idealen Zahlen; den hierauf bezüglichen Teil seiner Untersuchungen findet man am vollständigsten zusammengestellt in den Abhandlungen: Mémoire sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers (Journ. de Math. p. p. Liouville, T. XVI, 1851). — 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. der Berliner Ak. 1856). Das Hauptresultat ergibt sich mit größter Leichtigkeit aus unserer Theorie und lautet in unserer Ausdrucksweise folgendermaßen: Ist p eine rationale Primzahl und m' der größte durch p nicht teilbare Divisor von $m = p'm'$, gehört ferner p zum Exponenten f (mod m'), wo $\varphi(m') = ef$ (§ 28), so ist $\mathfrak{i}(p) = (\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_e)^{\varphi(p')}$, wo $\mathfrak{p}_1$, $\mathfrak{p}_2$, …, $\mathfrak{p}_e$ voneinander verschiedene Primideale bedeuten, deren Normen $= p^f$ sind; wenn $p' > 1$, so ist $\mathfrak{i}(1-\theta^{m'}) = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_e$. — Für komplexe Zahlen einer höheren Stufe vgl. Kummer: Über die allgemeinen Reziprozitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist (Abh. der Berliner Ak. 1859). — Für diejenigen Körper Ω, deren konjugierte Körper mit Ω identisch sind, und welche ich Galoissche Körper nennen möchte, vgl. Selling: Über die idealen Primfaktoren der komplexen Zahlen, welche aus den Wurzeln einer beliebigen irreduktibelen Gleichung rational gebildet sind (Schlömilchs Zeitschr. für Math. u. Phys. Bd. 10. 1865). — Ein spezieller Fall biquadratischer Körper ist vollständig durchgeführt von Bachmann: Die Theorie der komplexen Zahlen, welche aus zwei Quadratwurzeln zusammengesetzt sind. 1867. — Für eine gewisse Klasse kubischer Körper vgl. Eisenstein: Allgemeine Untersuchungen über die Formen dritten Grades mit drei Variabeln, welche der Kreisteilung ihre Entstehung verdanken (Crelles Journ. XXVIII).

Ist das kleinste gemeinschaftliche Multiplum $\mathfrak{m}$ der Ideale $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, … durch das Primideal $\mathfrak{p}$ teilbar, so geht $\mathfrak{p}$ wenigstens in einem der Ideale $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, … auf. Ist nämlich keins dieser Ideale durch $\mathfrak{p}$ teilbar, gibt es also in $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, … bzw. Zahlen α, β, γ, …, die nicht durch $\mathfrak{p}$ teilbar sind, so ist das in $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, …, also auch in $\mathfrak{m}$ enthaltene Produkt $\alpha\beta\gamma\dots$ nicht teilbar durch das Primideal $\mathfrak{p}$, und folglich geht $\mathfrak{p}$ nicht in $\mathfrak{m}$ auf, was zu beweisen war.

Ist die Zahl η nicht teilbar durch das Ideal $\mathfrak{a}$, so gibt es immer eine durch η teilbare Zahl ν der Art, daß alle Wurzeln π der Kongruenz $\nu\pi \equiv 0 \pmod{\mathfrak{a}}$ ein Primideal bilden. Alle Wurzeln β der Kongruenz $\eta\beta \equiv 0 \pmod{\mathfrak{a}}$ bilden ein in $\mathfrak{a}$ aufgehendes Ideal $\mathfrak{b}$, welches von $\mathfrak{o}$ verschieden ist, weil es die Zahl 1 nicht enthält; ist $\mathfrak{b}$ ein Primideal, so ist der Satz bewiesen. Ist $\mathfrak{b}$ kein Primideal, gibt es also zwei durch $\mathfrak{b}$ nicht teilbare Zahlen η', ϱ', deren Produkt $\eta'\varrho' \equiv 0 \pmod{\mathfrak{b}}$ ist, so bilden alle Wurzeln γ der Kongruenz $\eta'\gamma \equiv 0 \pmod{\mathfrak{b}}$, d. h. der Kongruenz $\eta\eta'\gamma \equiv 0 \pmod{\mathfrak{a}}$, ein in $\mathfrak{b}$ aufgehendes Ideal $\mathfrak{c}$, und zwar ist (zufolge 2.) $N(\mathfrak{c}) < N(\mathfrak{b})$, weil ϱ' in $\mathfrak{c}$, aber nicht in $\mathfrak{b}$ enthalten ist; außerdem ist $\mathfrak{c}$ von $\mathfrak{o}$ verschieden, weil η' nicht in $\mathfrak{b}$ und folglich die Zahl 1 nicht in $\mathfrak{c}$ enthalten ist; ist $\mathfrak{c}$ ein Primideal, so ist der Satz bewiesen. Ist aber $\mathfrak{c}$ kein Primideal, so kann man in derselben Weise fortfahren; endlich muß in der Reihe der Ideale $\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{d}$, …, deren Normen immer kleiner werden, aber stets > 1 bleiben, ein Primideal $\mathfrak{p}$ auftreten, welches aus allen Wurzeln π der Kongruenz $\nu\pi \equiv 0 \pmod{\mathfrak{a}}$ besteht, wo $\nu = \eta\eta'\eta'' \dots$ durch η teilbar ist.

4. Ist μ eine von Null verschiedene Zahl in $\mathfrak{o}$ und keine Einheit, so existiert zufolge des zuletzt bewiesenen Satzes (in welchem man

$\eta = 1$ nehmen kann) jedenfalls eine Zahl ν der Art, daß alle Wurzeln π der Kongruenz $\nu\pi \equiv 0 \pmod{\mu}$ ein Primideal $\mathfrak{p}$ bilden; Primideale, welche aus den sämtlichen Wurzeln einer solchen Kongruenz bestehen, wollen wir vorläufig einfache Ideale nennen. Ist nun r irgendein ganzer rationaler, nicht negativer Exponent, so bilden alle Wurzeln ϱ der Kongruenz $\varrho\nu^r \equiv 0 \pmod{\mu^r}$ ein Ideal, welches die $r$te Potenz von $\mathfrak{p}$ heißen und mit $\mathfrak{p}^r$ bezeichnet werden soll. Diese Definition ist unabhängig von dem zur Definition von $\mathfrak{p}$ benutzten Zahlenpaar μ, ν; ist nämlich μ' irgendeine von Null verschiedene, durch $\mathfrak{p}$ teilbare Zahl, also $\nu\mu' = \mu\nu'$, so folgt aus $\varrho\nu^r \equiv 0 \pmod{\mu^r}$ durch Multiplikation mit μ'^r und Division durch μ^r auch $\varrho\nu'^r \equiv 0 \pmod{\mu'^r}$, und umgekehrt. Von der größten Wichtigkeit sind aber die folgenden Sätze über einfache Ideale $\mathfrak{p}$:

Ist $s \geqq r$, so ist $\mathfrak{p}^s$ teilbar durch $\mathfrak{p}^r$. Ist nämlich σ in $\mathfrak{p}^s$ enthalten, also $\sigma\nu^s = \tau\mu^s$, so folgt, daß

$$\left(\frac{\sigma\nu^r}{\mu^r}\right)^s = \tau^r\sigma^{s-r}$$

eine ganze Zahl ist; mithin ist (nach § 160, 3.) der jedenfalls dem Körper Ω angehörige Quotient $\sigma\nu^r : \mu^r$ ebenfalls eine ganze Zahl, also in $\mathfrak{o}$ enthalten, weil $\mathfrak{o}$ alle ganzen Zahlen des Körpers Ω umfaßt*); also ist jede Zahl σ des Ideals $\mathfrak{p}^s$ auch in $\mathfrak{p}^r$ enthalten.

Ist ϱ eine von Null verschiedene Zahl in $\mathfrak{o}$, so gibt es immer eine höchste in ϱ aufgehende Potenz von $\mathfrak{p}$. Wäre nämlich für unendlich viele Exponenten r das Produkt $\varrho\nu^r$ teilbar durch μ^r, so müßte, da nur eine endliche Anzahl inkongruenter Zahlen (mod ϱ) existiert, für zwei verschiedene solche Exponenten r s notwendig einmal

$$\frac{\varrho\nu^r}{\mu^r} \equiv \frac{\varrho\nu^s}{\mu^s} \pmod{\varrho}, \quad \left(\frac{\nu}{\mu}\right)^r = \left(\frac{\nu}{\mu}\right)^s + \omega$$

werden, wo ω eine ganze Zahl; hieraus würde aber (nach § 160, 3.) folgen, daß ν durch μ teilbar wäre, was nicht der Fall ist, weil sonst $\mathfrak{p} = \mathfrak{o}$ wäre.

Sind $\mathfrak{p}^r$, $\mathfrak{p}^s$ bzw. die höchsten in ϱ, σ aufgehenden Potenzen, so ist $\mathfrak{p}^{r+s}$ die höchste in $\varrho\sigma$ aufgehende Potenz von $\mathfrak{p}$.

*) Sobald diese Bedingung nicht erfüllt ist, verlieren auch die obigen Sätze ihre allgemeine Gültigkeit; dies ist von Wichtigkeit für die Erweiterung der Definition der Ideale (vgl. § 165, 4.).

Denn da $\varrho\nu^r = \varrho'\mu^r$, $\sigma\nu^s = \sigma'\mu^s$ und keins der Produkte $\nu\varrho'$, $\nu\sigma'$ durch μ teilbar ist, so folgt $\varrho\sigma\nu^{r+s} = \varrho'\sigma'\mu^{r+s}$, und $\nu\varrho'\sigma'$ kann nicht durch μ teilbar sein, weil $\mathfrak{p}$ ein Primideal ist.

Ist $e \geqq 1$ der Exponent der höchsten in μ selbst aufgehenden Potenz von $\mathfrak{p}$, also $\mu\nu^e = \varkappa\mu^e$, wo $\nu\varkappa$ nicht teilbar durch μ, so folgt $\nu^e = \varkappa\mu^{e-1}$, d. h. der Exponent der höchsten in ν aufgehenden Potenz von $\mathfrak{p}$ ist $= e - 1$. Das Ideal $\mathfrak{p}^e$ besteht aus den sämtlichen Wurzeln θ der Kongruenz $\varkappa\theta \equiv 0 \pmod{\mu}$. Die ganze Zahl $\lambda = \varkappa\mu : \nu = \sqrt[e]{\mu\varkappa^{e-1}}$ ist durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbar; mithin ist λ^r durch $\mathfrak{p}^r$, aber nicht durch $\mathfrak{p}^{r+1}$ teilbar, woraus beiläufig folgt, daß die Ideale $\mathfrak{p}^r$ und $\mathfrak{p}^{r+1}$ wirklich verschieden sind. Endlich leuchtet folgender Satz ein:

Jede Potenz $\mathfrak{p}^r$ eines einfachen Ideals $\mathfrak{p}$ ist durch kein von $\mathfrak{p}$ verschiedenes Primideal teilbar. Ist nämlich π irgendeine Zahl in $\mathfrak{p}$, so muß ein in $\mathfrak{p}^r$ aufgehendes Primideal in π^r, also (zufolge 3.) in π selbst, d. h. in $\mathfrak{p}$ aufgehen und folglich mit $\mathfrak{p}$ identisch sein.

5. Die Wichtigkeit der einfachen Ideale und ihre Analogie mit den rationalen Primzahlen tritt unmittelbar hervor in dem folgenden Hauptsatz:

Wenn alle in einer von Null verschiedenen Zahl μ aufgehenden Potenzen einfacher Ideale auch in einer Zahl η aufgehen, so ist η durch μ teilbar. Ist η nicht teilbar durch μ, so gibt es (zufolge 3.) eine durch η teilbare Zahl ν der Art, daß alle Wurzeln π der Kongruenz $\nu\pi \equiv 0 \pmod{\mu}$ ein in μ aufgehendes einfaches Ideal $\mathfrak{p}$ bilden; ist $\mathfrak{p}^e$ die höchste in μ aufgehende Potenz, so ist (nach 4.) $\mathfrak{p}^{e-1}$ die höchste in ν aufgehende Potenz, und da ν durch η teilbar ist, so kann η nicht durch $\mathfrak{p}^e$ teilbar sein, was zu beweisen war. Derselbe Satz läßt sich offenbar auch so aussprechen: Jedes Hauptideal $\mathfrak{i}(\mu)$ ist das kleinste gemeinschaftliche Multiplum aller in μ aufgehenden Potenzen von einfachen Idealen. Es folgt zunächst:

Jedes Primideal $\mathfrak{p}$ ist ein einfaches Ideal. Es sei μ irgendeine von Null verschiedene Zahl in $\mathfrak{p}$, so muß $\mathfrak{p}$ (zufolge 3.) in einer der Potenzen einfacher Ideale aufgehen, deren kleinstes gemeinschaftliches Multiplum $\mathfrak{i}(\mu)$ ist; mithin ist $\mathfrak{p}$ selbst (zufolge 4.) ein ein-

faches Ideal. — Wir sprechen daher künftig nur noch von Primidealen, nicht mehr von einfachen Idealen.

Wenn alle in einem Ideal $\mathfrak{m}$ aufgehenden Potenzen von Primidealen auch in einer Zahl η aufgehen, so ist η teilbar durch $\mathfrak{m}$. Ist η nicht teilbar durch $\mathfrak{m}$, so gibt es (nach 3.) eine durch η teilbare Zahl ν der Art, daß alle Wurzeln π der Kongruenz $\nu\pi \equiv 0 \pmod{\mathfrak{m}}$ ein Primideal $\mathfrak{p}$ bilden; ist $\mathfrak{p}^e$ die höchste in $\mathfrak{m}$ aufgehende Potenz von $\mathfrak{p}$, so gibt es in $\mathfrak{m}$ eine nicht durch $\mathfrak{p}^{e+1}$ teilbare Zahl μ, und das aus allen Wurzeln ϱ der Kongruenz $\nu\varrho \equiv 0 \pmod{\mu}$ bestehende Ideal $\mathfrak{r}$ ist teilbar durch $\mathfrak{p}$, weil $\nu\varrho \equiv 0 \pmod{\mathfrak{m}}$ ist. Sind nun $\mathfrak{p}^e$, $\mathfrak{p}'^{e'}$, $\mathfrak{p}''^{e''}$, ... die sämtlichen höchsten in μ aufgehenden Potenzen verschiedener Primideale $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$, ..., so besteht $\mathfrak{r}$ zufolge des obigen Hauptsatzes aus allen gemeinschaftlichen Wurzeln ϱ der Kongruenzen $\nu\varrho \equiv 0 \pmod{\mathfrak{p}^e}$, $\nu\varrho \equiv 0 \pmod{\mathfrak{p}'^{e'}}$, $\nu\varrho \equiv 0 \pmod{\mathfrak{p}''^{e''}}$ usw., d. h. $\mathfrak{r}$ ist das kleinste gemeinschaftliche Multiplum der Ideale $\mathfrak{q}$, $\mathfrak{q}'$, $\mathfrak{q}''$, ..., welche bzw. aus den Wurzeln jeder einzelnen dieser Kongruenzen bestehen; da nun die Ideale $\mathfrak{q}'$, $\mathfrak{q}''$, ... als Teiler von $\mathfrak{p}'^{e'}$, $\mathfrak{p}''^{e''}$, ... nicht durch $\mathfrak{p}$ teilbar sind, so muß, weil $\mathfrak{r}$ durch $\mathfrak{p}$ teilbar ist, auch $\mathfrak{q}$ (zufolge 3.) durch $\mathfrak{p}$ teilbar sein; es kann folglich $\mathfrak{p}^e$ nicht in ν aufgehen (weil sonst $\mathfrak{q} = \mathfrak{o}$, also nicht durch $\mathfrak{p}$ teilbar wäre), und da ν durch η teilbar ist, so kann $\mathfrak{p}^e$ auch nicht in η aufgehen, was zu beweisen war.

Dieser Fundamentalsatz läßt sich offenbar auch so aussprechen: Jedes Ideal ist das kleinste gemeinschaftliche Multiplum aller in ihm aufgehenden Potenzen von Primidealen. Er entspricht durchaus dem Fundamentalsatze der rationalen Zahlentheorie über die Zusammensetzung der Zahlen aus Primzahlen (§ 8); denn ihm zufolge ist jedes Ideal $\mathfrak{m}$ vollständig bestimmt, sobald die höchsten in $\mathfrak{m}$ aufgehenden Potenzen $\mathfrak{p}^e$, $\mathfrak{p}'^{e'}$, $\mathfrak{p}''^{e''}$, ... von Primidealen gegeben sind; aus ihm ergibt sich auch ohne weiteres der folgende Satz: Ein Ideal $\mathfrak{m}$ ist stets und nur dann durch ein Ideal $\mathfrak{b}$ teilbar, wenn alle in $\mathfrak{b}$ aufgehenden Potenzen von Primidealen auch in $\mathfrak{m}$ aufgehen. Dies folgt unmittelbar aus dem Begriffe des kleinsten gemeinschaftlichen Multiplums.

Ist $\mathfrak{m}$ das kleinste gemeinschaftliche Multiplum von $\mathfrak{p}^e$, $\mathfrak{p}'^{e'}$, $\mathfrak{p}''^{e''}$, ..., wo $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$, ... voneinander verschiedene Primideale bedeuten, so ist $N(\mathfrak{m}) = N(\mathfrak{p})^e N(\mathfrak{p}')^{e'} N(\mathfrak{p}'')^{e''} \ldots$ Es

gibt immer (zufolge 4.) eine durch $\mathfrak{p}^{e-1}$, aber nicht durch $\mathfrak{a} = \mathfrak{p}^e$ teilbare Zahl η; das aus allen Wurzeln ϱ der Kongruenz $\eta\varrho \equiv 0 \pmod{\mathfrak{a}}$ bestehende Ideal $\mathfrak{r}$ ist verschieden von $\mathfrak{o}$ (weil es die Zahl 1 nicht enthält) und ein Teiler von $\mathfrak{p}$ (zufolge 4.), folglich identisch mit $\mathfrak{p}$; da ferner der größte gemeinschaftliche Teiler $\mathfrak{d}$ der Ideale $\mathfrak{a} = \mathfrak{p}^e$ und $\mathfrak{i}(\eta)$ zufolge des eben bewiesenen Fundamentalsatzes $= \mathfrak{p}^{e-1}$ ist, so folgt (aus 2.) $N(\mathfrak{a}) = N(\mathfrak{r})N(\mathfrak{d})$, d. h. $N(\mathfrak{p}^e) = N(\mathfrak{p})N(\mathfrak{p}^{e-1})$, und hieraus allgemein $N(\mathfrak{p}^e) = N(\mathfrak{p})^e$. — Nun ist (zufolge der Definition 2.) das kleinste gemeinschaftliche Multiplum $\mathfrak{m}$ der Ideale $\mathfrak{p}^e$, $\mathfrak{p}'^{e'}$, $\mathfrak{p}''^{e''}$, ... zugleich auch das der Ideale $\mathfrak{a} = \mathfrak{p}^e$ und $\mathfrak{b}$, wo $\mathfrak{b}$ das kleinste gemeinschaftliche Multiplum der Ideale $\mathfrak{p}'^{e'}$, $\mathfrak{p}''^{e''}$, ... bedeutet; da ferner (zufolge des Fundamentalsatzes) $\mathfrak{o}$ der größte gemeinschaftliche Teiler von $\mathfrak{a}$ und $\mathfrak{b}$ ist, so folgt (aus 2.) $N(\mathfrak{m}) = N(\mathfrak{a})N(\mathfrak{b})$, d. h. $N(\mathfrak{m}) = N(\mathfrak{p})^e N(\mathfrak{b})$, und hieraus ergibt sich offenbar der zu beweisende Satz.

6. Multipliziert man alle Zahlen eines Ideals $\mathfrak{a}$ mit allen Zahlen eines Ideals $\mathfrak{b}$, so bilden diese Produkte und deren Summen ein durch $\mathfrak{a}$ und $\mathfrak{b}$ teilbares Ideal, welches das Produkt aus den Faktoren $\mathfrak{a}$ und $\mathfrak{b}$ heißen und mit $\mathfrak{a}\mathfrak{b}$ bezeichnet werden soll. Aus dieser Erklärung leuchtet sofort ein, daß $\mathfrak{a}\mathfrak{o} = \mathfrak{a}$, $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$, ferner $(\mathfrak{a}\mathfrak{b})\mathfrak{c} = \mathfrak{a}(\mathfrak{b}\mathfrak{c})$ ist (vgl. §§ 1, 2, 147). Zugleich gilt folgender Satz:

Sind $\mathfrak{p}^a$, $\mathfrak{p}^b$ bzw. die höchsten in $\mathfrak{a}$, $\mathfrak{b}$ aufgehenden Potenzen des Primideals $\mathfrak{p}$, so ist $\mathfrak{p}^{a+b}$ die höchste in $\mathfrak{a}\mathfrak{b}$ aufgehende Potenz von $\mathfrak{p}$; und es ist $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$.

Aus der Erklärung folgt nämlich unmittelbar (mit Rücksicht auf 4.), daß $\mathfrak{a}\mathfrak{b}$ durch $\mathfrak{p}^{a+b}$ teilbar ist; da ferner in $\mathfrak{a}$ eine durch $\mathfrak{p}^{a+1}$ nicht teilbare Zahl α, in $\mathfrak{b}$ eine durch $\mathfrak{p}^{b+1}$ nicht teilbare Zahl β existiert, so gibt es in $\mathfrak{a}\mathfrak{b}$ eine durch $\mathfrak{p}^{a+b+1}$ nicht teilbare Zahl $\alpha\beta$, womit der erste Teil des Satzes bewiesen ist. Ist also $\mathfrak{a}$ das kleinste gemeinschaftliche Multiplum der Potenzen $\mathfrak{p}^a$, $\mathfrak{p}'^{a'}$, $\mathfrak{p}''^{a''}$, ... der voneinander verschiedenen Primideale $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$, ..., und $\mathfrak{b}$ das kleinste gemeinschaftliche Multiplum der Potenzen $\mathfrak{p}^b$, $\mathfrak{p}'^{b'}$, $\mathfrak{p}''^{b''}$, ..., so ist $\mathfrak{a}\mathfrak{b}$ dasjenige der Potenzen $\mathfrak{p}^{a+b}$, $\mathfrak{p}'^{a'+b'}$, $\mathfrak{p}''^{a''+b''}$, ..., woraus (mit Rücksicht auf 5.) auch der zweite Teil des Satzes folgt.

Da aus diesem Satze auch $\mathfrak{p}^a\mathfrak{p}^b = \mathfrak{p}^{a+b}$ folgt, so ist die oben (in 4.) gewählte Ausdrucks- und Bezeichnungsweise gerechtfertigt. Sind ferner $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$, ... voneinander verschiedene Primideale, so ist $\mathfrak{p}^a\mathfrak{p}'^{a'}\mathfrak{p}''^{a''}\ldots$ das kleinste gemeinschaftliche Multiplum der Potenzen

$\mathfrak{p}^a$, $\mathfrak{p}'^{a'}$, $\mathfrak{p}''^{a''}$, ... Auch leuchtet ein, daß der Begriff der Potenz durch die Definition $\mathfrak{a}^{r+1} = \mathfrak{a}\,\mathfrak{a}^r$ auf jedes Ideal $\mathfrak{a}$ ausgedehnt werden kann. Ist endlich $\mathfrak{a}$ teilbar durch $\mathfrak{b}$, so gibt es immer ein und nur ein Ideal $\mathfrak{r}$ der Art, daß $\mathfrak{a} = \mathfrak{r}\,\mathfrak{b}$ wird; sind nämlich $\mathfrak{p}^a$, $\mathfrak{p}^d$ die höchsten bzw. in $\mathfrak{a}$, $\mathfrak{b}$ aufgehenden Potenzen eines Primideals $\mathfrak{p}$, so ist $d \leqq a$, und $\mathfrak{r}$ ist das Produkt aus allen Potenzen $\mathfrak{p}^{a-d}$. Mit Rücksicht hierauf erkennt man leicht, daß die früheren Sätze (in 2.) sich jetzt einfacher aussprechen lassen.

7. Wir nennen nun $\mathfrak{a}$ und $\mathfrak{b}$ relative Primideale, wenn ihr größter gemeinschaftlicher Teiler $= \mathfrak{o}$ ist; ebenso soll η relative Primzahl zum Ideal $\mathfrak{a}$ heißen, wenn $\mathfrak{a}$ und $\mathfrak{i}(\eta)$ relative Primideale sind. Es leuchtet dann ein, daß die Sätze der rationalen Zahlentheorie über relative Primzahlen sich leicht auf die Theorie der Ideale übertragen lassen; wir begnügen uns aber hier, folgenden wichtigen Satz zu beweisen (vgl. § 25):

Sind $\mathfrak{a}$, $\mathfrak{b}$ relative Primideale, und μ, ν zwei gegebene Zahlen, so gibt es immer eine und nur eine Klasse von Zahlen η (mod $\mathfrak{a}\,\mathfrak{b}$), welche den Bedingungen $\eta \equiv \mu$ (mod $\mathfrak{a}$), $\eta \equiv \nu$ (mod $\mathfrak{b}$) genügen. Durchlaufen nämlich μ, ν, η vollständige Restsysteme bzw. für die drei Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{a}\,\mathfrak{b}$, so entspricht jeder Zahl η eine und nur eine Kombination μ, ν der Art, daß $\mu \equiv \eta$ (mod $\mathfrak{a}$), $\nu \equiv \eta$ (mod $\mathfrak{b}$) ist; entspräche ferner zwei verschiedenen Zahlen η, η' des Restsystems für den Modul $\mathfrak{a}\,\mathfrak{b}$ eine und dieselbe Kombination μ, ν, so wäre $\eta - \eta'$ teilbar sowohl durch $\mathfrak{a}$ als durch $\mathfrak{b}$, also auch durch $\mathfrak{a}\,\mathfrak{b}$ (weil $\mathfrak{a}$, $\mathfrak{b}$ relative Primideale sind), mithin wäre $\eta \equiv \eta'$ (mod $\mathfrak{a}\,\mathfrak{b}$), was gegen die Voraussetzung streitet. Durchläuft daher η alle seine Werte, deren Anzahl $= N(\mathfrak{a}\,\mathfrak{b}) = N(\mathfrak{a})\,N(\mathfrak{b})$ ist, so entstehen ebensoviele verschiedene Kombinationen μ, ν; und da genau ebensoviele verschiedene Kombinationen μ, ν wirklich existieren, so muß auch umgekehrt jede Kombination μ, ν einer Zahl η entsprechen, was zu beweisen war.

Bedeutet $\psi(\mathfrak{a})$ die Anzahl der (mod $\mathfrak{a}$) inkongruenten relativen Primzahlen zu $\mathfrak{a}$, so ist $\psi(\mathfrak{a}\,\mathfrak{b}) = \psi(\mathfrak{a})\,\psi(\mathfrak{b})$, wenn $\mathfrak{a}$, $\mathfrak{b}$ relative Primideale bedeuten. Ist ferner $\mathfrak{p}$ ein Primideal, und $e \geqq 1$, so ist $\psi(\mathfrak{p}^e) = N(\mathfrak{p}^e) - N(\mathfrak{p}^{e-1}) = N(\mathfrak{p})^{e-1}(N(\mathfrak{p}) - 1)$; denn, wenn δ alle r durch $\mathfrak{p}$ teilbaren und nach dem Modul $\mathfrak{p}^e$ inkongruenten Zahlen, wenn ferner γ ein vollständiges Restsystem (mod $\mathfrak{p}$) durchläuft, so bilden die Zahlen $\gamma + \delta$ (zufolge 2.) ein vollständiges Restsystem

(mod $\mathfrak{p}^e$), und es ist $N(\mathfrak{p}^e) = r\,N(\mathfrak{p})$, also $r = N(\mathfrak{p}^{e-1})$; nun ist aber eine solche Zahl $\gamma + \delta$ stets und nur dann relative Primzahl zu $\mathfrak{p}^e$, wenn γ nicht $\equiv 0$ (mod $\mathfrak{p}$) ist, und folglich ist die Anzahl der Zahlen $\gamma + \delta$, welche relative Primzahlen zu $\mathfrak{p}^e$ sind, gleich $r(N(\mathfrak{p}) - 1)$, was zu beweisen war.

Bedeutet $\mathfrak{p}$ ein Primideal, so gibt es (zufolge 4.) immer eine Zahl λ, welche durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbar ist, mithin auch eine Zahl λ^e, welche durch $\mathfrak{p}^e$, aber nicht durch $\mathfrak{p}^{e+1}$ teilbar ist. Sind nun $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$, ... voneinander verschiedene Primideale, und haben λ', λ'', ... ähnliche Bedeutung für $\mathfrak{p}'$, $\mathfrak{p}''$, ..., wie λ für $\mathfrak{p}$, so existiert immer, wenn e, e', e'', ... gegebene Exponenten bedeuten, eine Zahl η, welche den gleichzeitigen Kongruenzen

$$\eta \equiv \lambda^e \pmod{\mathfrak{p}^{e+1}}, \quad \eta \equiv \lambda'^{e'} \pmod{\mathfrak{p}'^{e'+1}},$$
$$\eta \equiv \lambda''^{e''} \pmod{\mathfrak{p}''^{e''+1}} \ \ldots$$

genügt, weil die Moduln relative Primideale sind. Dann ist offenbar $\mathfrak{i}(\eta) = \mathfrak{m}\,\mathfrak{p}^e\mathfrak{p}'^{e'}\mathfrak{p}''^{e''}\ldots$, und das Ideal $\mathfrak{m}$ ist durch keines der Primideale $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$, ... teilbar. Hieraus folgt unmittelbar der Satz:

Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei beliebige Ideale, so gibt es immer ein solches relatives Primideal $\mathfrak{m}$ zu $\mathfrak{b}$, daß $\mathfrak{a}\,\mathfrak{m}$ ein Hauptideal wird. Sind nämlich $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$, ... alle voneinander verschiedenen in $\mathfrak{a}\,\mathfrak{b}$ aufgehenden Primideale, und ist $\mathfrak{a} = \mathfrak{p}^e\mathfrak{p}'^{e'}\mathfrak{p}''^{e''}\ldots$ (wo die Exponenten e, e', e'', ... auch $= 0$ sein können), so gibt es, wie eben gezeigt ist, ein durch $\mathfrak{a}$ teilbares Hauptideal $\mathfrak{i}(\eta) = \mathfrak{a}\,\mathfrak{m}$ der Art, daß $\mathfrak{b}$ und $\mathfrak{m}$ relative Primideale sind.

Hieraus folgt auch, daß jedes Ideal $\mathfrak{a}$, welches kein Hauptideal ist, immer als der größte gemeinschaftliche Teiler von zwei Hauptidealen angesehen werden kann; hat man nämlich nach Belieben ein durch $\mathfrak{a}$ teilbares Hauptideal $\mathfrak{i}(\eta') = \mathfrak{a}\,\mathfrak{b}$ gewählt, so kann man immer ein zweites $\mathfrak{i}(\eta) = \mathfrak{a}\,\mathfrak{m}$ so wählen, daß $\mathfrak{b}$ und $\mathfrak{m}$ relative Primideale werden; die sämtlichen Zahlen des Ideals $\mathfrak{a}$ sind dann von der Form $\eta\,\omega + \eta'\,\omega'$, wo ω, ω' alle Zahlen in $\mathfrak{o}$ durchlaufen.

[Erläuterungen gemeinsam mit denen zu XLVI, XLVIII, XLIX am Schluß von XLIX.]

XLVIII.

Sur la Théorie des Nombres entiers algébriques.

[Paris, Gauthier-Villars, 1877, S. 1—121. Bulletin des Sciences mathématiques et astronomiques, 1re série, t. XI, 2e série, t. I, 1876, 1877.]

Table des Matières.

Introduction.

En réponse à l'invitation que l'on m'a fait l'honneur de m'adresser, je me propose, dans le présent Mémoire, de développer les principes fondamentaux de la théorie générale, échappant à toute exception des nombres entiers algébriques, principes que j'ai publiés dans la seconde édition des Leçons sur la Théorie des nombres de Dirichlet. Mais, à cause de l'étendue extraordinaire de ce champ de recherches mathématiques, je me bornerai ici à poursuivre un but unique, que je vais essayer de définir clairement par les remarques suivantes.

La théorie de la divisibilité des nombres, qui sert de fondement à l'arithmologie, a déjà été établie par Euclide dans ce qu'elle a d'essentiel; du moins, le théorème capital que tout nombre entier composé peut toujours se mettre, et cela d'une seule manière, sous la forme d'un produit de nombres tous premiers, est une conséquence immédiate de ce théorème démontré par Euclide*), qu'un produit de deux nombres ne peut être divisible par un nombre premier que si celui-ci divise au moins l'un des facteurs.

Deux mille ans plus tard, Gauss donna, pour la première fois, une extension à la notion du nombre entier; tandis que, jusqu'à lui, on ne désignait sous ce nom que les nombres $0, \pm 1, \pm 2, \ldots$, que j'appellerai dans tout ce qui va suivre nombres entiers rationnels, Gauss introduisit**) les nombres entiers complexes, de la forme $a + b\sqrt{-1}$, a et b désignant des nombres entiers rationnels quelconques, et il démontra que les lois générales de la divisibilité de ces nombres sont identiques avec celles qui régissent le domaine des nombres entiers rationnels.

La plus haute généralisation de la notion du nombre entier consiste dans ce qui suit. Un nombre θ est dit un nombre algébrique, lorsqu'il satisfait à une équation

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

de degré fini n et à coefficients rationnels $a_1, a_2, \ldots, a_{n-1}, a_n$; il est dit un nombre entier algébrique, ou plus brièvement un nombre entier, lorsqu'il satisfait à une équation de la forme ci-dessus, dans laquelle les coefficients $a_1, a_2, \ldots, a_{n-1}, a_n$ sont tous des nombres entiers rationnels. De cette définition il résulte immé-

*) Éléments, VII, 32.
**) Theoria residuorum biquadraticorum, II; 1832.

diatement que les sommes, les différences et les produits de nombres entiers sont tous aussi des nombres entiers; par suite, un nombre entier α sera dit divisible par un nombre entier β, si l'on a $\alpha = \beta\gamma$, γ étant également un nombre entier. Un nombre entier ε s'appellera une unité, lorsque tout nombre entier quelconque sera divisible par ε. Par analogie, on devrait entendre par nombre premier un nombre entier α qui ne serait pas une unité, et qui n'aurait pour diviseurs que les unités ε et les produits de la forme $\varepsilon\alpha$; mais il est facile de reconnaître que, dans le domaine de tous les nombres entiers que nous considérons ici, il n'existe pas de tels nombres premiers, puisque tout nombre entier qui n'est pas une unité peut toujours être mis sous la forme d'un produit de deux facteurs ou plutôt d'un nombre quelconque de facteurs, qui sont tous des nombres entiers, mais non des unités.

Toutefois, l'existence des nombres premiers et l'analogie avec les domaines des nombres entiers rationnels ou complexes commence à se montrer de nouveau, lorsque du domaine de tous les nombres entiers on sépare une partie infiniment petite, de la manière suivante. Si θ est un nombre algébrique déterminé, parmi les équations à coefficients rationnels, en nombre infini dont θ est racine, il y en a une et une seule,

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

qui est de degré moins élevé que toutes les autres, et que l'on nomme à cause de cela irréductible. Si $x_0, x_1, x_2, \ldots, x_{n-1}$ désignent des nombres rationnels pris à volonté, tous les nombres de la forme

$$\varphi(\theta) = x_0 + x_1\theta + x_2\theta^2 + \cdots + x_{n-1}\theta^{n-1},$$

dont nous représenterons le complexe par Ω, seront aussi des nombres algébriques, et ils jouiront de la propriété fondamentale que leurs sommes, leurs différences, leurs produits et leurs quotients appartiendront tous aussi au même complexe Ω; j'appellerai un tel complexe Ω un corps fini du degré n. Tous les nombres $\varphi(\theta)$ appartenant au corps Ω se partagent maintenant, conformément à la définition ci-dessus, en deux grandes classes, savoir, en nombres entiers dont nous désignerons le complexe par $\mathfrak{o}$, et en nombres non entiers ou nombres fractionnaires. Le problème que nous nous proposons consiste à établir les lois générales de la divisibilité qui régissent un tel système $\mathfrak{o}$.

Le système $\mathfrak{o}$ est évidemment identique avec le système de tous les nombres entiers rationnels, lorsqu'on a $n = 1$, ou avec celui des nombres entiers complexes, lorsqu'on a $n = 2$ et $\theta = \sqrt{-1}$. Certains phénomènes qui se présentent dans ces deux domaines $\mathfrak{o}$ spéciaux se reproduisent encore dans tout domaine $\mathfrak{o}$ de cette nature; il faut observer avant tout que la décomposition illimitée dont il a été question plus haut, et qui règne dans le domaine qui comprend tous les nombres algébriques entiers, ne se rencontre jamais dans un domaine $\mathfrak{o}$ de l'espèce indiquée, comme on peut aisément s'en assurer par la considération des normes. Si l'on entend, en effet, par norme d'un nombre quelconque $\mu = \varphi(\theta)$, appartenant au corps Ω, le produit

$$N(\mu) = \mu\,\mu_1\,\mu_2 \cdots \mu_{n-1},$$

dont les facteurs sont les nombres conjugués

$$\mu = \varphi(\theta), \quad \mu_1 = \varphi(\theta_1), \quad \mu_2 = \varphi(\theta_2), \quad \ldots, \quad \mu_{n-1} = \varphi(\theta_{n-1}),$$

$\theta, \theta_1, \theta_2, \ldots, \theta_{n-1}$ désignant toutes les racines de la même équation irréductible du $n^{\text{ième}}$ degré, $N(\mu)$ sera toujours, comme on sait, un nombre rationnel, et ne deviendra $= 0$ que si $\mu = 0$; en même temps, on a toujours

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

α et β étant deux nombres quelconques du corps Ω. Si maintenant μ est un nombre entier et par suite un nombre compris dans $\mathfrak{o}$, les autres nombres conjugués $\mu_1, \mu_2, \ldots, \mu_{n-1}$ seront pareillement des nombres entiers, et par suite $N(\mu)$ sera un nombre entier rationnel. Cette norme joue un rôle extrêmement important dans la théorie des nombres du domaine $\mathfrak{o}$; en effet, si deux nombres quelconques α, β de ce domaine sont dits congrus ou incongrus par rapport à un troisième μ, pris pour module, selon que leur différence $\pm(\alpha - \beta)$ est ou n'est pas divisible par μ, on pourra, exactement comme dans la théorie des nombres entiers rationnels ou complexes, partager tous les nombres du système $\mathfrak{o}$ en classes de nombres, de sorte que chaque classe comprenne l'ensemble de tous les nombres qui sont congrus à un nombre déterminé, lequel sera le représentant de cette classe, et une étude plus approfondie nous apprend que le nombre de ces classes (à l'exception du seul cas de $\mu = 0$) est toujours fini, et de plus égal à la valeur absolue de $N(\mu)$. Une conséquence immédiate de ce résultat, c'est que $N(\mu)$ sera toujours

$= \pm 1$ dans le cas, et seulement dans ce cas, où μ sera une unité. Si maintenant un nombre du système o est dit décomposable, lorsqu'il est le produit de deux nombres de ce système, dont aucun ne soit une unité, il suit évidemment de ce qui précède que tout nombre décomposable peut toujours être représenté comme le produit d'un nombre fini de facteurs indécomposables.

Ce résultat correspond encore complétement à la loi qui a lieu dans la théorie des nombres entiers rationnels ou complexes, savoir que tout nombre composé peut être représenté par le produit d'un nombre fini de facteurs premiers; mais en même temps c'est ici le point où l'analogie, observée jusqu'ici, avec l'ancienne théorie menace de se rompre pour toujours. Dans ses recherches sur le domaine des nombres qui appartiennent à la théorie de la division du cercle, et qui correspondent par suite aux équations de la forme $\theta^m = 1$, Kummer a remarqué l'existence d'un phénomène par lequel les nombres de ce domaine se distinguent en général de ceux qu'on a considérés auparavant, d'une manière si complète et si essentielle, qu'il restait à peine un espoir quelconque de conserver les lois simples qui régissent l'ancienne théorie des nombres. En effet, tandis que, dans le domaine des nombres entiers, tant rationnels que complexes, tout nombre composé ne peut se mettre que d'une seule manière sous la forme d'un produit de nombres premiers, on reconnaît que, dans les domaines numériques considérés par Kummer, un nombre décomposable peut souvent se représenter de plusieurs manières, entièrement différentes entre elles, sous la forme d'un produit de nombres indécomposables, ou, ce qui dans le fond revient au même, on reconnaît que les nombres indécomposables ne possèdent pas tous le caractère d'un nombre premier proprement dit, lequel consiste en ce qu'un nombre premier ne peut diviser un produit de deux ou de plusieurs facteurs, s'il ne divise au moins un de ces facteurs. Mais plus le succès des recherches ultérieures sur de tels domaines numériques devait sembler désespéré*), plus

*) Dans le Mémoire: De numeris complexis qui radicibus unitatis et numeris integri realibus constant (Vrastislaviæ, 1844, § 8), Kummer dit: «Maxime dolendum videtur, quod hæc numerorum realium virtus, ut in factores primos dissolvi possint qui pro eodem numero semper iidem sint, non eadem est numerorum complexorum, quæ si esset tota hæc doctrina, quæ magnis adhuc difficultatibus laborat, facile absolvi et ad finem perduci posset.»

on doit de reconnaissance aux efforts persévérants de Kummer, qui ont été enfin récompensés par une découverte vraiment grande et féconde. Ce géomètre est parvenu*) à ramener toutes les irrégularités apparentes à des lois rigoureuses, et en considérant les nombres indécomposables, mais dépourvus du caractère de véritables nombres premiers, comme des produits de facteurs premiers idéaux, qui n'apparaissent et ne manifestent leur effet que combinés ensemble, et non pas isolés, il a obtenu ce résultat surprenant, que les lois de la divisibilité dans les domaines de nombres étudiés par lui coïncident maintenant complétement avec celles qui régissent le domaine des nombres entiers rationnels. Tout nombre qui n'est pas une unité se comporte, dans toutes les questions de divisibilité, tant dans un rôle actif que dans un rôle passif, ou comme un nombre premier, ou comme un nombre formé par la multiplication de facteurs premiers, existants ou idéaux, complétement déterminés. Deux nombres idéaux, soit premiers, soit composés, qui se changent en deux nombres existants par la combinaison avec un seul et même nombre idéal, sont dits équivalents, et tous les nombres idéaux équivalents à un même nombre idéal déterminé forment une classe de nombres idéaux; l'ensemble de tous les nombres existants, qui sont considérés comme un cas spécial des nombres idéaux, forme la classe principale; à chaque classe correspond un système d'une infinité de formes homogènes équivalentes, à n variables et du degré n, qui sont décomposables en n facteurs linéaires à coefficients algébriques; le nombre de ces classes est fini, et Kummer est parvenu à étendre à la détermination de ce nombre les principes par lesquels Dirichlet a déterminé le nombre des classes des formes quadratiques binaires.

Le grand succès des recherches de Kummer, dans le domaine de la division du cercle, donnait lieu de présumer que les mêmes lois subsistaient dans tous les domaines numériques o de l'espèce la plus générale, dont il a été question plus haut. Dans mes recherches, qui avaient pour but d'amener la question à une solution définitive, j'ai commencé par m'appuyer sur la théorie des congruences d'ordre supérieur, parce que j'avais déjà précédemment remarqué que par l'application de cette théorie les recherches de Kummer pouvaient

*) Zur Theorie der complexen Zahlen (Journal de Crelle, t. 35).

être considérablement abrégées; mais, bien que ce moyen conduisit jusqu'à un point très-voisin du but de mes efforts, je n'ai pu toutefois réussir par cette voie à soumettre certaines exceptions apparentes aux lois constatées pour les autres cas. Je ne suis parvenu à la théorie générale et sans exceptions, que j'ai publiée pour la première fois au lieu indiqué plus haut, qu'après avoir entièrement abandonné l'ancienne marche plus formelle, et l'avoir remplacée par une autre partant de la conception fondamentale la plus simple, et fixant le regard immédiatement sur le but. Dans cette marche, je n'ai plus besoin d'aucune création nouvelle, comme celle du nombre idéal de Kummer, et il suffit complétement de la considération de ce système de nombres réellement existants, que j'appelle un idéal. La puissance de ce concept reposant sur son extrême simplicité, et mon dessein étant avant tout d'inspirer la confiance en cette notion, je vais essayer de développer la suite des idées qui m'ont conduit à ce concept.

Kummer n'a pas défini les nombres idéaux eux-mêmes, mais seulement la divisibilité par ces nombres. Si un nombre α possède une certaine propriété A, consistant toujours en ce que α satisfait à une ou plusieurs congruences, il dit que α est divisible par un nombre idéal déterminé, correspondant à la propriété A. Bien que cette introduction de nouveaux nombres soit tout à fait légitime, il est toutefois à craindre d'abord que, par le mode d'expression que l'on a choisi, dans lequel on parle de nombres idéaux déterminés et de leurs produits, et aussi par l'analogie présumée avec la théorie des nombres rationnels, on ne soit entraîné à des conclusions précipitées et par là à des démonstrations insuffisantes, et en effet cet écueil n'est pas toujours complétement évité. D'autre part, une définition exacte et qui soit commune à tous les nombres idéaux qu'il s'agit d'introduire dans un domaine numérique déterminé o, et en même temps une définition générale de leur multiplication paraissent d'autant plus nécessaires, que ces nombres idéaux n'existent nullement dans le domaine numérique considéré o. Pour satisfaire à ces exigences, il sera nécessaire et suffisant d'établir une fois pour toutes le caractère commun de toutes les propriétés A, B, C, ..., qui toujours, et elles seules, servent à l'introduction de nombres idéaux déterminés, et ensuite d'indiquer généralement comment de deux de ces propriétés A, B, auxquelles correspondent deux nombres idéaux

déterminés, on pourra déduire la propriété C qui doit correspondre au produit de ces deux nombres idéaux*).

*) La légitimité ou plutôt la nécessité de telles exigences, qui devraient toujours s'imposer dans l'introduction ou la création de nouveaux éléments arithmétiques, deviendra encore plus évidente par la comparaison avec l'introduction des nombres réels irrationnels, objet dont je me suis occupé dans un écrit spécial (Stetigkeit und irrationale Zahlen; Brunswick, 1872). En admettant que l'arithmétique des nombres rationnels, dont nous désignerons l'ensemble par R, soit définitivement fondée, il s'agit de savoir de quelle manière on devra introduire les nombres irrationnels, et définir les opérations d'addition, de soustraction, de multiplication et de division à exécuter sur ces nombres. Comme première exigence, je reconnais que l'Arithmétique doit être maintenue exempte de tout mélange d'éléments étrangers, et pour cette raison je rejette la définition d'après laquelle le nombre serait le rapport de deux grandeurs de même espèce; au contraire, la définition ou la création du nombre irrationnel doit être fondée uniquement sur des phénomènes que l'on puisse déjà constater clairement dans le domaine R. En second lieu, on devra exiger que tous les nombres réels irrationnels puissent être engendrés à la fois par une commune définition, et non successivement comme racines des équations, comme logarithmes, etc. La définition devra, en troisième lieu, être de nature à permettre aussi une définition parfaitement claire des calculs (addition, etc.) que l'on aura à faire sur les nouveaux nombres. On parvient à tout cela de la manière suivante, que je ne ferai ici qu'indiquer:

1° J'appelle section du domaine R un partage quelconque de tous les nombres rationnels en deux catégories, tel que chaque nombre de la première catégorie soit algébriquement moindre que chaque nombre de la seconde catégorie.

2° Tout nombre rationnel déterminé a engendre une section déterminée (ou deux sections, non essentiellement différentes), par cela qu'un nombre rationnel quelconque sera classé dans la première ou dans la seconde catégorie, suivant qu'il sera algébriquement plus petit ou plus grand que a (tandis que a lui-même pourra être inscrit à volonté dans l'une ou dans l'autre des deux catégories).

3° Il y a une infinité de sections qui ne peuvent pas être engendrées par des nombres rationnels, de la manière indiquée: pour toute section de cette espèce, on crée et l'on introduit dans l'arithmétique un nombre irrationnel spécial, correspondant à cette section (ou l'engendrant).

4° Soient α, β deux nombres quelconques réels (rationnels ou irrationnels); il est facile, d'après les sections qu'ils engendrent, de définir si l'on a $\alpha > \beta$ ou $\alpha < \beta$; de plus, on peut aisément définir, au moyen de ces deux sections, les quatre sections auxquelles doivent correspondre la somme, la différence, le produit, le quotient des deux nombres α, β. Par là sont définies sans aucune obscurité les quatre opérations fondamentales de l'Arithmétique pour deux nombres réels quelconques, et l'on peut démontrer réellement des propositions telles, par exemple, que l'égalité $\sqrt{2}.\sqrt{3} = \sqrt{6}$, ce qui n'a pas encore été fait, que je sache, dans le sens rigoureux du mot.

5° Les nombres irrationnels ainsi définis forment, réunis aux nombres rationnels, un domaine $\mathfrak{R}$ sans lacunes et continu; toute section de ce domaine $\mathfrak{R}$ sera produite par un nombre déterminé du même domaine; il est impossible de classer encore de nouveaux nombres dans ce domaine $\mathfrak{R}$.

Ce problème est essentiellement simplifié par les réflexions suivantes. Comme une telle propriété caractéristique A sert à définir, non un nombre idéal lui-même, mais seulement la divisibilité des nombres contenus dans $\mathfrak{o}$ par un nombre idéal, on est conduit naturellement à considérer l'ensemble $\mathfrak{a}$ de tous ces nombres α du domaine $\mathfrak{o}$ qui sont divisibles par un nombre idéal déterminé; j'appellerai dès maintenant, pour abréger, un tel système $\mathfrak{a}$ un idéal, de sorte que, à tout nombre idéal déterminé, correspond un idéal déterminé $\mathfrak{a}$. Maintenant comme, réciproquement, la propriété A, c'est-à-dire la divisibilité d'un nombre α par le nombre idéal, consiste uniquement en ce que α appartient à l'idéal correspondant $\mathfrak{a}$, on pourra, au lieu des propriétés A, B, C, ..., par lesquelles a été définie l'introduction des nombres idéaux, considérer les idéaux correspondants $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, ..., pour établir leur caractère commun et exclusif. En ayant égard actuellement à ce que l'introduction des nombres idéaux n'a pas d'autre but que de ramener les lois de la divisibilité dans le domaine numérique $\mathfrak{o}$ à une complète conformité avec la théorie des nombres rationnels, il est évidemment nécessaire que les nombres réellement existants dans $\mathfrak{o}$, et qui toutefois se présentent en première ligne comme facteurs de nombres composés, ne soient considérés que comme un cas particulier des nombres idéaux; si donc μ est un nombre déterminé de $\mathfrak{o}$, le système $\mathfrak{a}$ de tous les nombres $\alpha = \mu\omega$ du domaine $\mathfrak{o}$ divisibles par μ aura également le caractère essentiel d'un idéal, et il sera appelé un idéal principal; ce système évidemment n'est pas altéré, quand on remplace μ par $\varepsilon\mu$, ε désignant une unité quelconque renfermée dans $\mathfrak{o}$. Maintenant, de la notion de nombre entier établie plus haut résultent immédiatement les deux théorèmes élémentaires suivants sur la divisibilité:

1° Si les deux nombres entiers $\alpha = \mu\omega$, $\alpha' = \mu\omega'$ sont divisibles par le nombre entier μ, leur somme $\alpha + \alpha' = \mu(\omega + \omega')$ et leur différence $\alpha - \alpha' = \mu(\omega - \omega')$ seront aussi divisibles par μ, puisque la somme $\omega + \omega'$ et la différence $\omega - \omega'$ de deux nombres entiers ω, ω' sont elles-mêmes aussi des nombres entiers.

2° Si $\alpha = \mu\omega$ est divisible par μ, tout nombre $\alpha\omega' = \mu(\omega\omega')$, divisible par α, sera aussi divisible par μ, puisque tout produit $\omega\omega'$ de deux nombres entiers ω, ω' est aussi lui-même un nombre entier.

Si l'on applique ces théorèmes, vrais pour tous les nombres entiers, aux nombres ω de notre domaine numérique $\mathfrak{o}$, en désignant

par μ un de ces nombres déterminés, et par $\mathfrak{a}$ l'idéal principal qui lui correspond, on obtiendra les deux propriétés fondamentales suivantes d'un tel système numérique $\mathfrak{a}$:

I. Les sommes et les différences de deux nombres quelconques du système $\mathfrak{a}$ sont toujours des nombres du même système $\mathfrak{a}$.

II. Tout produit d'un nombre du système $\mathfrak{a}$ par un nombre du système $\mathfrak{o}$ est un nombre du système $\mathfrak{a}$.

Maintenant, comme nous poursuivons le but de ramener généralement, par l'introduction des nombres idéaux et d'un mode de langage correspondant, les lois de la divisibilité dans le domaine numérique $\mathfrak{o}$ à une complète conformité avec celles qui règnent dans le domaine des nombres entiers rationnels, il s'ensuit que les définitions des nombres idéaux et de la divisibilité par ces nombres devront s'énoncer de telle manière que les deux théorèmes élémentaires ci-dessus, 1° et 2°, continuent à subsister lors même que μ ne serait pas un nombre existant, mais un nombre idéal, et par suite les deux propriétés I et II appartiendront non-seulement aux idéaux principaux, mais aussi à tous les idéaux. Nous avons donc trouvé par là un caractère commun à tous les idéaux; à tout nombre existant ou idéal correspond un idéal complétement déterminé $\mathfrak{a}$, jouissant toujours des deux propriétés I et II.

Mais un fait de la plus haute importance, et dont je n'ai pu démontrer rigoureusement la vérité qu'à la suite de nombreux et vains efforts et après avoir surmonté de grandes difficultés, c'est que, réciproquement, tout système $\mathfrak{a}$ qui jouit des propriétés I et II est aussi un idéal, c'est-à-dire que $\mathfrak{a}$ forme l'ensemble de tous les nombres α du domaine $\mathfrak{o}$ qui sont divisibles par un nombre existant déterminé, ou par un nombre idéal, indispensable pour compléter la théorie. Les deux propriétés I et II sont donc non-seulement les conditions nécessaires, mais encore les conditions suffisantes pour qu'un système numérique $\mathfrak{a}$ soit un idéal; toute autre condition à laquelle on voudrait assujettir les systèmes numériques $\mathfrak{a}$, si elle n'était pas une simple conséquence des propriétés I et II, rendrait impossible l'explication complète de tous les phénomènes de la divisibilité dans le domaine $\mathfrak{o}$.

Cette constatation m'a conduit naturellement à fonder toute la théorie des nombres du domaine $\mathfrak{o}$ sur cette définition simple, entiè-

rement délivrée de toute obscurité et de l'admission des nombres idéaux*):

Tout système $\mathfrak{a}$ de nombres entiers du corps Ω, qui possède les propriétés I et II, est dit *un idéal de ce corps.*

La divisibilité d'un nombre α par un nombre μ consiste en ce que α est un nombre $\mu\omega$ de l'idéal principal, qui correspond au nombre μ et peut être convenablement désigné par $\mathfrak{o}(\mu)$ ou $\mathfrak{o}\mu$; et de la propriété II ou du théorème 2°, il résulte qu'en même temps tous les nombres de l'idéal principal $\mathfrak{o}\alpha$ sont aussi des nombres de l'idéal principal $\mathfrak{o}\mu$. Réciproquement, il est évident que α est certainement divisible par μ, quand tous les nombres de l'idéal $\mathfrak{o}\alpha$, et par suite aussi α lui-même, sont contenus dans l'idéal $\mathfrak{o}\mu$. De là on est conduit à établir la notion suivante de la divisibilité, non-seulement pour les idéaux principaux, mais encore pour tous les idéaux:

Un idéal $\mathfrak{a}$ est dit divisible par un idéal $\mathfrak{b}$, ou un multiple de $\mathfrak{b}$, et $\mathfrak{b}$ un diviseur de $\mathfrak{a}$, lorsque tous les nombres de l'idéal $\mathfrak{a}$ sont en même temps contenus dans $\mathfrak{b}$. Un idéal $\mathfrak{p}$, différent de $\mathfrak{o}$, qui n'a aucun diviseur autre que $\mathfrak{o}$ et $\mathfrak{p}$, est dit un idéal premier**).

De cette divisibilité des idéaux, qui comprend évidemment celle des nombres, il faut d'abord bien séparer la notion suivante de la multiplication et des produits de deux idéaux:

Si α parcourt tous les nombres d'un idéal $\mathfrak{a}$, et β tous les nombres d'un idéal $\mathfrak{b}$, tous les produits de la forme $\alpha\beta$ et toutes les sommes de ces produits formeront un idéal qui s'appellera le produit des idéaux $\mathfrak{a}$, $\mathfrak{b}$, et que l'on désignera par $\mathfrak{a}\mathfrak{b}$***).

Or on voit immédiatement, il est vrai, que le produit $\mathfrak{a}\mathfrak{b}$ est divisible aussi bien par $\mathfrak{a}$ que par $\mathfrak{b}$; mais l'établissement complet de la liaison entre les deux notions de la divisibilité et de la multiplication des idéaux réussit seulement après que l'on a vaincu des difficultés caractéristiques, profondément attachées à la nature du sujet; cette liaison s'exprime essentiellement par les deux théorèmes suivants:

*) Il est naturellement permis, quoique ce ne soit aucunement nécessaire, de faire correspondre à tout idéal tel que $\mathfrak{a}$ un nombre idéal qui l'engendre, si ce n'est pas un idéal principal.

**) En même temps le nombre idéal correspondant à l'idéal $\mathfrak{a}$ s'appellerait divisible par le nombre idéal correspondant à l'idéal $\mathfrak{b}$; à un idéal premier correspondrait un nombre idéal premier.

***) Le nombre idéal correspondant à l'idéal $\mathfrak{a}\mathfrak{b}$ s'appellerait le produit des deux nombres idéaux correspondants à $\mathfrak{a}$ et $\mathfrak{b}$.

Si l'idéal $\mathfrak{c}$ est divisible par l'idéal $\mathfrak{a}$, il existera toujours un idéal $\mathfrak{b}$, et un seul, tel que le produit $\mathfrak{a}\mathfrak{b}$ soit identique avec $\mathfrak{c}$.

Tout idéal différent de $\mathfrak{o}$ ou est un idéal premier, ou peut être représenté, et cela d'une seule manière, sous forme d'un produit d'idéaux tous premiers.

Dans le présent Mémoire, je me borne à démontrer ces résultats avec une entière rigueur et par voie synthétique. En cela consiste le fondement propre de la théorie complète des idéaux et des formes décomposables, laquelle offre aux mathématiciens un champ inépuisable de recherches. De tous les développements ultérieurs, pour lesquels je dois renvoyer à l'exposition faite dans les Vorlesungen über Zahlentheorie de Dirichlet et à quelques Mémoires qui paraîtront plus tard, je n'ai inséré dans le Mémoire actuel que le partage des idéaux en classes, et la démonstration que le nombre de ces classes d'idéaux (ou des classes de formes correspondantes) est fini. La première Section contient seulement les propositions indispensables pour le but présent, extraites d'une théorie auxiliaire, importante aussi pour d'autres recherches, et dont je publierai ailleurs l'exposition complète. La seconde Section, qui a pour but d'éclaircir sur des exemples numériques complétement déterminés les notions générales qui devront être introduites plus tard, pourrait être entièrement supprimée; mais je l'ai conservée parce qu'elle peut être utile pour faciliter l'intelligence des Sections suivantes, où l'on trouvera la théorie des nombres entiers d'un corps fini quelconque développée jusqu'au point indiqué ci-dessus. Pour cela, il suffit d'emprunter seulement les premiers éléments à la théorie générale des corps, théorie dont le développement ultérieur conduirait aisément aux principes algébriques inventés par Galois, lesquels servent à leur tour de base aux recherches plus approfondies dans la théorie des idéaux.

I.

Théorèmes auxiliaires de la théorie des modules.

Ainsi qu'il ressort de l'Introduction, nous aurons dans la suite à considérer très-souvent des systèmes de nombres qui se repro-

duisent par addition et soustraction; le développement des propriétés générales de pareils systèmes forme l'objet d'une théorie assez étendue, qui peut aussi être utilisée pour d'autres recherches, tandis que, pour notre but, les premiers éléments de cette théorie sont suffisants. Pour ne pas interrompre plus tard le cours de notre exposition, et en même temps pour faire apercevoir plus clairement la portée des divers concepts sur lesquels s'appuie notre théorie suivante des nombres algébriques entiers, il nous semble à propos d'établir préalablement un petit nombre de théorèmes très-simples, bien qu'ils ne puissent offrir un véritable intérêt que par leurs applications. ...

... Les recherches dans cette première Section ont été exposées sous la forme spéciale qui répond à notre but; mais il est clair qu'elles ne cessent en rien d'être vraies, quand les lettres grecques désignent, non plus des nombres, mais des éléments quelconques, objets de l'étude que l'on poursuit, dont deux quelconques α, β, par une opération commutative et uniformément inversible (composition), tenant la place de l'addition, produiront un élément déterminé $\gamma = \alpha + \beta$ de la même espèce; les modules a se changent en groupes d'éléments, dont les résultats (les composés) appartiennent toujours au même groupe; les coefficients rationnels entiers indiquent combien de fois un élément contribue à la génération d'un autre.

II.

Le germe de la théorie des idéaux.

Dans cette Section, je me propose, comme je l'ai déjà indiqué dans l'Introduction, d'expliquer sur un exemple déterminé la nature du phénomène qui a conduit Kummer à la création des nombres idéaux, et j'utiliserai le même exemple pour éclaircir le concept d'idéal introduit par moi, et celui de la multiplication des idéaux.

§ 5. — Les nombres rationnels entiers.

La théorie des nombres s'occupe d'abord exclusivement du système des nombres rationnels entiers 0, ± 1, ± 2, ± 3, ..., et il sera bon de remémorer ici en peu de mots les lois importantes qui régissent ce domaine. Avant tout, il faut rappeler que ces nombres se reproduisent par addition, soustraction et multiplication, c'est-à-

dire que les sommes, les différences et les produits de deux nombres quelconques de ce domaine appartiennent au même domaine. La théorie de la divisibilité considère de préférence la combinaison des nombres par multiplication; le nombre a est dit divisible par le nombre b, lorsque $a = bc$, c étant également un nombre rationnel entier. Le nombre 0 est divisible par un nombre quelconque; les deux unités ± 1 divisent tous les nombres, et elles sont les seuls nombres qui jouissent de cette propriété. Si a est divisible par b, $\pm a$ sera aussi divisible par $\pm b$, et nous pourrons, par conséquent, nous restreindre à la considération des nombres positifs. Tout nombre positif, différent de l'unité, est ou un nombre premier, c'est-à-dire un nombre divisible seulement par lui-même et par l'unité, ou un nombre composé; dans ce dernier cas, on pourra toujours le mettre sous la forme d'un produit de nombres premiers, et, ce qui est le plus important, on ne le pourra que d'une seule manière, c'est-à-dire que le système de tous les nombres premiers qui entrent comme facteurs dans ce produit est complétement déterminé, ainsi que le nombre de fois qu'un nombre premier désigné entre comme facteur. Cette propriété repose essentiellement sur ce théorème, qu'un produit de deux facteurs n'est divisible par un nombre premier que lorsque celui-ci divise au moins un des deux facteurs.

La manière la plus simple de démontrer ces propositions fondamentales de la théorie des nombres est fondée sur la considération du procédé enseigné déjà par Euclide, et qui sert à trouver le plus grand commun diviseur de deux nombres*). Cette opération a, comme on sait, pour base l'application répétée de ce théorème, que, si m désigne un nombre positif, un nombre quelconque z pourra toujours être mis sous la forme $qm + r$, q et r désignant aussi des nombres entiers, dont le second est moindre que m; car il résulte de là que l'opération devra s'arrêter après un nombre fini de divisions.

La notion de la congruence des nombres a été introduite par Gauss**); deux nombres z, z' sont dits congrus par rapport au module m, ce qu'on exprime par la notation

$$z \equiv z' \pmod{m},$$

lorsque la différence $z - z'$ est divisible par m; dans le cas contraire, z et z' sont dits incongrus par rapport à m. Si l'on range

*) Voir, par exemple, les Vorlesungen über Zahlentheorie de Dirichlet.
**) Disquisitiones arithmeticæ, art. 1.

les nombres, pris deux à deux dans la même classe*) de nombres ou dans deux classes différentes suivant qu'ils sont congrus ou incongrus par rapport à m, on conclut aisément du théorème rappelé plus haut que le nombre de ces classes est fini, et qu'il est égal à la valeur absolue du module m. C'est ce qui résulte évidemment aussi des études de la Section précédente; car la définition de la congruence établie dans la Section I contient celle de Gauss comme cas particulier. Le système $\mathfrak{o}$ de tous les nombres entiers rationnels est identique avec le module fini [1], et de même le système $\mathfrak{m}$ de tous les nombres divisibles par m est identique avec $[m]$; la congruence de deux nombres par rapport au nombre m coïncide avec leur congruence par rapport au système $\mathfrak{m}$; donc (d'après § 3, 2°, ou § 4, 4°), le nombre des classes est $= (\mathfrak{o}, \mathfrak{m}) = \pm m$.

§ 6. — Les nombres complexes entiers de Gauss.

Le premier et le plus grand pas vers la généralisation de ces notions a été fait par Gauss, dans son second Mémoire sur les résidus biquadratiques, lorsqu'il les a transportées au domaine des nombres complexes entiers $x + yi$, x et y désignant des nombres rationnels entiers quelconques, et i étant $= \sqrt{-1}$, c'est-à-dire une racine de l'équation quadratique irréductible $i^2 + 1 = 0$. Les nombres de ce domaine se reproduisent encore par addition, soustraction et multiplication, et l'on peut par conséquent définir pour ces nombres la notion de divisibilité de la même manière que pour les nombres rationnels. On peut établir très-simplement, comme Dirichlet l'a montré d'une manière très-élégante**), que les propositions générales sur la composition des nombres au moyen de nombres premiers subsisteront encore dans ce nouveau domaine, en s'appuyant sur la remarque suivante. Si l'on entend par la norme $N(w)$ d'un nombre $w = u + vi$, u et v désignant des nombres rationnels quelconques, le produit $u^2 + v^2$ des deux nombres conjugués $u + vi$ et $u - vi$, la norme d'un produit sera égale au produit des normes des facteurs, et en outre il est clair que, w étant donné, on pourra toujours

*) Le mot classe semble avoir été employé par Gauss pour la première fois dans ce sens à propos des nombres complexes. (Theoria residuorum biquadraticorum, II, art. 42.)

**) Recherches sur les formes quadratiques à coefficients et à indéterminées complexes. (Journal de Crelle, t. 24.)

choisir un nombre complexe entier q, de telle sorte que l'on ait $N(w - q) \leqq \frac{1}{2}$; en désignant maintenant par z et m deux nombres complexes entiers quelconques, dont le second soit différent de zéro, il en résulte, si l'on prend $w = \frac{z}{m}$, que l'on pourra toujours poser $z = qm + r$, q et r étant des nombres complexes entiers, et cela de telle manière que l'on ait $N(r) < N(m)$. On pourra donc, absolument comme pour les nombres rationnels, trouver par un nombre fini de divisions le plus grand commun diviseur de deux nombres complexes entiers quelconques, et les démonstrations des lois générales de la divisibilité des nombres rationnels entiers pourront s'appliquer presque mot pour mot au domaine des nombres complexes entiers. Il y a quatre unités, ± 1, $\pm i$, c'est-à-dire quatre nombres qui divisent tous les nombres, et dont la norme est, par suite, $= 1$. Tout autre nombre différent de zéro est dit un nombre composé, lorsqu'il peut être représenté par le produit de deux facteurs dont aucun n'est une unité; dans le cas contraire, le nombre est dit un nombre premier, et un tel nombre ne peut diviser un produit s'il ne divise au moins l'un des facteurs. Tout nombre composé peut toujours, et d'une seule manière, être mis sous la forme d'un produit de nombres premiers, les quatre nombres premiers associés $\pm q$, $\pm qi$ ne comptant naturellement que comme les représentants d'un seul et même nombre premier q. L'ensemble de tous les nombres premiers q du domaine des nombres complexes entiers se compose:

1° De tous les nombres premiers rationnels qui (pris positivement) sont de la forme $4n + 3$;

2° Du nombre $1 + i$, qui divise le nombre premier rationnel $2 = (1 + i)(1 - i) = -i(1 + i)^2$;

3° Des couples de deux facteurs $a + bi$ et $a - bi$, contenus dans tout nombre premier rationnel p de la forme $4n + 1$, et dont la norme $a^2 + b^2 = p$.

L'existence des nombres premiers $a \pm bi$, cités en dernier lieu, laquelle résulte immédiatement du célèbre théorème de Fermat contenu dans l'équation $p = a^2 + b^2$, et entraîne réciproquement ce théorème comme conséquence, se déduit ici sans le secours de ce théorème, avec une merveilleuse facilité, et ce n'est là qu'un premier exemple de la puissance extraordinaire des principes auxquels nous

parviendrons par la plus grande généralisation de l'idée de nombre entier.

La congruence des nombres complexes entiers par rapport à un nombre donné de même nature m peut aussi se définir absolument de la même manière que dans la théorie de nombres rationnels; les nombres z, z' sont dits congrus par rapport à m, et l'on pose $z \equiv z' \pmod{m}$ lorsque la différence $z - z'$ est divisible par m. Si l'on range les nombres, pris deux à deux, dans la même classe ou dans deux classes différentes, suivant qu'ils sont congrus ou incongrus par rapport à m, le nombre total des classes différentes sera fini, et $= N(m)$. C'est ce qui résulte très-facilement des recherches de la première Section; car le système $\mathfrak{o}$ de tous les nombres complexes entiers $x + y\,i$ forme un module fini $[1, i]$, et pareillement le système $\mathfrak{m}$ de tous les nombres $m(x + y\,i)$ divisibles par m forme le module $[m, mi]$, dont la base est liée avec celle de $\mathfrak{o}$ par deux équations de la forme

$$m = a.1 + b.i, \quad mi = -b.1 + a.i;$$

par suite, on a (§ 4, 4°)

$$(\mathfrak{o}, \mathfrak{m}) = \begin{vmatrix} a & b \\ -b & a \end{vmatrix} = N(m).$$

§ 7. — Le domaine $\mathfrak{o}$ des nombres $x + y\sqrt{-5}$.

Il y a encore d'autres domaines numériques qui peuvent se traiter absolument de la même manière. Désignons, par exemple, par θ une racine de l'une des cinq équations

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

et faisons prendre à x, y toutes les valeurs rationnelles et entières; les nombres $x + y\,\theta$ formeront un domaine numérique correspondant. Dans chacun de ces domaines, comme il est aisé de s'en assurer, on peut trouver le plus grand commun diviseur de deux nombres par un nombre fini de divisions, et il s'ensuit de là immédiatement que les lois générales de la divisibilité coïncident avec celles qui ont lieu pour les nombres rationnels, bien que, dans les deux derniers exemples, apparaisse cette circonstance, que le nombre des unités est infini.

Cette méthode, au contraire, n'est plus applicable au domaine $\mathfrak{o}$ des nombres entiers

$$\omega = x + y\,\theta,$$

où θ est une racine de l'équation

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

x, y prenant encore toutes les valeurs rationnelles et entières. Ici l'on rencontre déjà le phénomène qui a suggéré à Kummer la création des nombres idéaux, et que nous allons maintenant décrire en détail sur quelques exemples.

Les nombres ω du domaine $\mathfrak{o}$, dont il sera exclusivement question dans ce qui va suivre, se reproduisent encore par addition, soustraction et multiplication, et nous définirons, par suite, exactement comme dans ce qui précède, les notions de divisibilité et de congruence des nombres. Si l'on appelle, de plus, norme $N(\omega)$ d'un nombre $\omega = x + y\,\theta$ le produit $x^2 + 5\,y^2$ des deux nombres conjugués $x \pm y\,\theta$, la norme d'un produit sera égale au produit des normes de tous les facteurs; et si μ est un nombre déterminé, différent de zéro, on en conclut, absolument comme ci-dessus, que $N(\mu)$ exprime combien il y a de nombres non congrus par rapport à μ. Si μ est une unité, et partant divise tous les nombres, il faut que l'on ait $N(\mu) = 1$, d'où $\mu = \pm 1$.

Nous appellerons **décomposable** un nombre (différent de zéro et de ± 1), lorsqu'il sera le produit de deux facteurs dont aucun ne sera une unité; dans le cas contraire, le nombre sera dit **indécomposable**. Alors il résulte bien du théorème sur la norme d'un produit que tout nombre décomposable peut être mis sous la forme d'un nombre fini de facteurs indécomposables; mais dans une infinité de cas il se présente ici un phénomène tout nouveau, savoir, qu'un seul et même nombre est susceptible de plusieurs représentations de cette sorte, essentiellement différentes entre elles. Les exemples les plus simples de ces cas sont les suivants. Il est aisé de se convaincre que chacun des quinze nombres suivants:

$$a = 2, \quad b = 3, \quad c = 7;$$
$$b_1 = -2 + \theta, \quad b_2 = -2 - \theta; \quad c_1 = 2 + 3\theta, \quad c_2 = 2 - 3\theta;$$
$$d_1 = 1 + \theta, \quad d_2 = 1 - \theta; \quad e_1 = 3 + \theta, \quad e_2 = 3 - \theta;$$
$$f_1 = -1 + 2\theta, \quad f_2 = -1 - 2\theta; \quad g_1 = 4 + \theta, \quad g_2 = 4 - \theta$$

est indécomposable. En effet, pour qu'un nombre premier rationnel p soit décomposable et, par suite, de la forme $\omega\omega'$, il faut que $N(p) = p^2 = N(\omega)N(\omega')$, et comme ω, ω' ne sont pas des unités, on devra avoir $p = N(\omega) = N(\omega')$, c'est-à-dire que p devra pouvoir se représenter par la forme quadratique binaire $x^2 + 5y^2$. Or les trois nombres premiers 2, 3, 7, comme on le voit par la théorie de ces formes*), ou encore par un petit nombre d'essais directs, ne peuvent pas se représenter de cette manière; ils sont donc indécomposables. Il est aisé de démontrer la même chose, et d'une manière semblable, pour les douze autres nombres, dont les normes sont les produits de deux de ces trois nombres premiers. Mais, malgré l'indécomposabilité de ces quinze nombres, il existe entre leurs produits de nombreuses relations, qui toutes peuvent se déduire des suivantes:

$$(1) \qquad ab = d_1 d_2, \quad b^2 = b_1 b_2, \quad ab_1 = d_1^2,$$

$$(2) \qquad ac = e_1 e_2, \quad c^2 = c_1 c_2, \quad ac_1 = e_1^2,$$

$$(3) \qquad bc = f_1 f_2 = g_1 g_2, \quad af_1 = d_1 e_1, \quad ag_1 = d_1 e_2.$$

Dans chacune de ces dix relations, un même nombre est représenté de deux ou trois manières différentes sous la forme d'un produit de deux nombres indécomposables; on voit donc qu'un nombre indécomposable peut très-bien diviser un produit, sans toutefois diviser l'un ou l'autre des facteurs; un tel nombre indécomposable ne possède donc pas la propriété qui, dans la théorie des nombres rationnels, est tout à fait caractéristique pour un nombre premier.

Imaginons pour un instant que les quinze nombres précédents soient des nombres rationnels entiers; alors, d'après les lois générales de la divisibilité, on déduirait aisément des relations (1) une décomposition de la forme

$$a = \mu\alpha^2, \quad d_1 = \mu\alpha\beta_1, \quad d_2 = \mu\alpha\beta_2,$$
$$b = \mu\beta_1\beta_2, \quad b_1 = \mu\beta_1^2, \quad b_2 = \mu\beta_2^2,$$

et de même, des relations (2) une décomposition de la forme

$$a = \mu'\alpha'^2, \quad e_1 = \mu'\alpha'\gamma_1, \quad e_2 = \mu'\alpha'\gamma_2,$$
$$c = \mu'\gamma_1\gamma_2, \quad c_1 = \mu'\gamma_1^2, \quad c_2 = \mu'\gamma_2^2,$$

où toutes les lettres grecques désignent des nombres rationnels entiers, et il en résulterait immédiatement, en vertu de l'équation

*) Voir Dirichlet, Vorlesungen über Zahlentheorie, § 71.

$\mu\alpha^2 = \mu'\alpha'^2$, que les quatre nombres f_1, f_2, g_1, g_2, qui entrent dans les relations (3), seraient également des nombres entiers. Ces décompositions se simplifient si l'on introduit, en outre, l'hypothèse que a est un nombre premier avec b et avec c; car on tire de là $\mu = \mu' = 1$, $\alpha = \alpha'$, et l'on obtient les quinze nombres, exprimés comme il suit, au moyen des cinq nombres α, β_1, β_2, γ_1, γ_2,

$$(4) \qquad \begin{cases} a = \alpha^2, \quad b = \beta_1\beta_2, \quad c = \gamma_1\gamma_2; \\ b_1 = \beta_1^2, \quad b_2 = \beta_2^2; \quad c_1 = \gamma_1^2, \quad c_2 = \gamma_2^2; \\ d_1 = \alpha\beta_1, \quad d_2 = \alpha\beta_2; \quad e_1 = \alpha\gamma_1, \quad e_2 = \alpha\gamma_2; \\ f_1 = \beta_1\gamma_1, \quad f_2 = \beta_2\gamma_2; \quad g_1 = \beta_1\gamma_2, \quad g_2 = \beta_2\gamma_1. \end{cases}$$

Quoique maintenant nos quinze nombres soient en réalité indécomposables, ils se comportent cependant, chose remarquable, dans toutes les questions de divisibilité relatives au domaine o, absolument comme s'ils étaient composés, de la manière indiquée ci-dessus, au moyen de cinq nombres premiers α, β_1, β_2, γ_1, γ_2, différents les uns des autres. Je vais exposer tout à l'heure en détail ce qu'il faut entendre par cette relation des nombres.

§ 8. — Rôle du nombre 2 dans le domaine o.

Dans ce dessein, je remarque avant tout que, dans la théorie des nombres rationnels entiers, on peut reconnaître complétement la constitution essentielle d'un nombre, sans en effectuer la décomposition en facteurs premiers, en observant seulement la manière dont il se comporte comme diviseur. Si l'on sait, par exemple, qu'un nombre positif a ne divise un produit de deux carrés que si l'un au moins de ces carrés est divisible par a, on en conclut avec certitude que a est égal à 1, ou qu'il est un nombre premier ou le carré d'un nombre premier. Il est pareillement certain qu'un nombre a doit contenir au moins un facteur carré, outre l'unité, lorsqu'on peut démontrer l'existence d'un nombre non divisible par a, et dont le carré est divisible par a. Si l'on peut donc constater, pour un nombre a, l'un et l'autre de ces deux caractères, on en conclut d'une manière sûre que a est le carré d'un nombre premier.

Nous allons maintenant examiner, dans ce sens, comment se comporte le nombre 2 dans notre domaine o des nombres $\omega = x + y\theta$. Comme deux nombres conjugués quelconques sont congrus par rapport au module 2, on aura

$$\omega^2 \equiv N(\omega) \pmod 2,$$

et par suite aussi $\omega^2 \omega'^2 \equiv N(\omega) N(\omega')$ (mod 2); maintenant, pour que le nombre 2 divise le produit $\omega^2 \omega'^2$, et par suite aussi le produit des deux nombres rationnels $N(\omega)$, $N(\omega')$, il faut que l'une au moins de ces normes, et par suite aussi que l'un au moins des deux carrés ω^2, ω'^2 soient divisibles par 2. Si de plus on choisit pour x, y deux nombres impairs quelconques, on obtient un nombre $\omega = x + y\theta$ non divisible par 2, et dont le carré est divisible par 2. En ayant égard aux remarques précédentes sur les nombres rationnels, nous dirons donc que le nombre 2 se comporte dans notre domaine o comme s'il était le carré d'un nombre premier α.

Bien qu'un tel nombre premier α n'existe nullement dans le domaine o, nous n'en introduirons pas moins, comme l'a fait Kummer avec grand succès dans des circonstances semblables, un pareil nombre α sous le nom de nombre idéal, et nous nous laisserons d'abord conduire par l'analogie avec la théorie des nombres rationnels, pour définir avec précision la présence du nombre α dans les nombres existants quelconques ω du domaine o. Or, quand un nombre rationnel a est déjà reconnu comme étant le carré d'un nombre premier rationnel α, on peut aisément, sans même avoir à faire intervenir α, juger si α est contenu et combien de fois il est contenu comme facteur dans un nombre rationnel entier quelconque z; car il est clair que z est divisible par α^n toutes les fois, et alors seulement, que z^2 est divisible par a^n. Nous étendrons donc ce critérium au cas qui nous occupe, et nous dirons qu'un nombre ω du domaine o est divisible par la $n^{\text{ième}}$ puissance α^n du nombre premier idéal α, lorsque ω^2 sera divisible par 2^n. Le succès fera voir que cette définition est très-heureusement*) choisie, parce qu'elle conduit à un mode d'expression en harmonie parfaite avec les lois de la théorie des nombres rationnels.

Il s'ensuit d'abord, pour $n = 1$, qu'un nombre $\omega = x + y\theta$ est divisible par α dans le cas, et seulement dans ce cas, où $N(\omega)$ est un nombre pair, et où l'on a, par suite,

$$(\alpha) \qquad x \equiv y \pmod 2.$$

*) Heureusement, car, par exemple, la tentative de déterminer d'une manière analogue le rôle du nombre 2 dans le domaine des nombres $x + y\sqrt{-3}$ aurait complétement échoué; plus tard nous découvrirons clairement la raison de ce phénomène.

Le nombre ω n'est pas divisible par α, quand $N(\omega)$ est un nombre impair, et que l'on a par suite $x \equiv 1 + y$ (mod 2); et de là résulte évidemment le théorème dans lequel on reconnaîtra le caractère du nombre idéal α comme nombre premier: «Tout produit de deux nombres non divisibles par α est aussi non divisible par α».

Relativement aux puissances supérieures de α, on conclut d'abord de la définition qu'un nombre ω divisible par α^n l'est aussi par toutes les puissances inférieures de α, puisqu'un nombre ω^2 divisible par 2^n l'est aussi par toutes les puissances inférieures de 2. Nous allons maintenant, si ω est différent de zéro, chercher l'exposant m de la plus haute puissance de α qui divise ω, c'est-à-dire l'exposant de la plus haute puissance de 2 qui divise ω^2. Soit s l'exposant de la plus haute puissance de 2 qui divise ω lui-même; on aura

$$\omega = 2^s \omega_1 = 2^s (x_1 + y_1 \theta),$$

et l'un au moins des deux nombres rationnels entiers x_1, y_1 sera impair; si les deux sont impairs, ω_1 sera divisible par α, et l'on aura

$$\omega_1^2 = x_1^2 - 5 y_1^2 + 2 x_1 y_1 \theta = 2 \omega_2,$$

$\omega_2 = x_2 + y_2 \theta$ n'étant pas divisible par α, puisque x_2 est pair et y_2 impair; mais si l'un des deux nombres x_1, y_1 est pair, et partant l'autre impair, ω_1 et par suite aussi ω_1^2 ne seront pas divisibles par α. Donc, dans le premier cas, $m = 2s + 1$; dans le second cas, $m = 2s$; mais dans les deux cas $\omega^2 = 2^m \omega'$, ω' désignant un nombre non divisible par α. On voit en même temps que m est aussi l'exposant de la plus haute puissance de 2 qui divise la norme $N(\omega)$; on a donc ce théorème: «L'exposant de la plus haute puissance de α qui divise un produit est égal à la somme des exposants des plus hautes puissances de α qui divisent les facteurs.» Il est pareillement évident que tout nombre ω divisible par α^{2n} est aussi divisible par 2^n; car, si l'exposant désigné plus haut par s était $< n$, les nombres $2s$, $2s + 1$, et par suite aussi m seraient $< 2n$, ce qui est contre l'hypothèse. Il suit immédiatement de la définition que, réciproquement, tout nombre divisible par 2^n l'est aussi par α^{2n}.

Le nombre $1 + \theta$ étant divisible par α, mais ne l'étant pas par α^2, on reconnaît aisément, à l'aide du théorème précédent, que la congruence $\omega^2 \equiv 0$ (mod 2^n), qui a servi de définition pour la di-

visibilité du nombre ω par α^n, peut être complétement remplacée par la congruence

$$(\alpha^n) \qquad \omega(1+\theta)^n \equiv 0 \pmod{2^n},$$

qui a l'avantage de ne contenir le nombre ω qu'à la première puissance.

§ 9. — Rôle des nombres 3 et 7 dans le domaine o.

Quand toutes les quantités qui entrent dans les équations (4) du § 7 sont des nombres rationnels entiers, et qu'en même temps a est premier avec b et avec c, il est évident qu'un nombre rationnel entier quelconque z sera ou ne sera pas divisible par β_1, β_2, γ_1, γ_2, selon qu'il satisfera ou ne satisfera pas à la congruence correspondante

$$z d_2 \equiv 0, \quad z d_1 \equiv 0 \pmod{b},$$
$$z e_2 \equiv 0, \quad z e_1 \equiv 0 \pmod{c}.$$

Ces congruences ont maintenant ceci de particulier, que les nombres β_1, β_2, γ_1, γ_2 n'y entrent aucunement par eux-mêmes, et c'est précisément pour cela que, dans le cas que nous traitons effectivement, et où il s'agit de nombres du domaine o, elles sont appropriées pour servir à l'introduction de quatre nombres idéaux β_1, β_2, γ_1, γ_2. Nous dirons qu'un nombre quelconque $\omega = x + y\theta$ est divisible par l'un de ces quatre nombres, si ω est une racine de la congruence correspondante

$$(1-\theta)\omega \equiv 0, \quad (1+\theta)\omega \equiv 0 \pmod 3,$$
$$(3-\theta)\omega \equiv 0, \quad (3+\theta)\omega \equiv 0 \pmod 7.$$

En effectuant la multiplication, ces congruences se changent dans les suivantes:

$$(\beta_1) \qquad x \equiv y \pmod 3,$$
$$(\beta_2) \qquad x \equiv -y \pmod 3,$$
$$(\gamma_1) \qquad x \equiv 3y \pmod 7,$$
$$(\gamma_2) \qquad x \equiv -3y \pmod 7.$$

A cela nous rattacherons les remarques suivantes.

Chacune de ces conditions peut être satisfaite par l'un des nombres $\omega = 1+\theta$, $1-\theta$, $3+\theta$, $3-\theta$, ce nombre ne satisfaisant à aucune des trois autres, et il s'ensuit de là qu'il est légitime d'appeler ces quatre nombres idéaux différents entre eux. Comme, en outre, tout nombre ω divisible par β_1 et par β_2 est aussi divisible

par 3, puisque l'on doit avoir $x \equiv y \equiv -y \equiv 0 \pmod 3$, et que réciproquement tout nombre divisible par 3 est aussi divisible par chacun des nombres β_1, β_2, on devrait, par analogie avec la théorie des nombres rationnels, considérer le nombre 3 comme le plus petit commun multiple des deux nombres idéaux β_1, β_2. Mais chacun de ces deux nombres idéaux possède aussi le caractère d'un nombre premier, c'est-à-dire qu'il ne divise un produit $\omega\omega'$ que lorsqu'il divise un au moins des facteurs ω, ω'; si l'on pose, en effet,

$$\omega = x + y\theta, \quad \omega' = x' + y'\theta, \quad \omega'' = \omega\omega' = x'' + y''\theta,$$

on aura

$$x'' = xx' - 5yy', \quad y'' = xy' + yx',$$

et par suite

$$x'' \pm y'' \equiv (x \pm y)(x' \pm y') \pmod 3,$$

ce qui vérifie immédiatement notre assertion, en ayant égard aux congruences ci-dessus (β_1), (β_2). D'après cela, le nombre 3 devra être considéré, à un certain point de vue, comme le produit des deux nombres premiers idéaux différents β_1, β_2.

Comme, de plus, chacun de ces deux nombres premiers idéaux β_1, β_2 est différent (dans le sens indiqué ci-dessus) du nombre premier idéal α introduit plus haut, dès lors, en observant que 2 se comporte comme le carré de α, et que $1+\theta$ est divisible par α et par β_1, de même que $1-\theta$ est divisible par α et par β_2, on devra conclure, de l'équation $2.3 = (1+\theta)(1-\theta)$, que $1+\theta$ se comporte comme le produit de α et de β_1, et $1-\theta$ comme le produit de α et de β_2. Cette présomption se confirme en effet pleinement: tout nombre $\omega = x + y\theta$ divisible par $1+\theta$ est, en effet, divisible par α et par β_1, puisque

$$x + y\theta = (1+\theta)(x' + y'\theta),$$

d'où

$$x = x' - 5y', \quad y = x' + y',$$

et par suite

$$x \equiv y \pmod 2, \quad x \equiv y \pmod 3;$$

et réciproquement, tout nombre $\omega = x + y\theta$, divisible par α et par β_1, c'est-à-dire satisfaisant aux deux congruences précédentes, est aussi divisible par $1+\theta$, puisque l'on a $y = x + 6y'$, et par suite

$$x + y\theta = (1+\theta)(x + 5y' + y'\theta).$$

On peut maintenant introduire aussi les puissances des nombres premiers idéaux β_1, β_2, comme on l'a fait plus haut pour les puissances du nombre idéal α; par analogie avec la théorie des nombres

rationnels, nous définirons la divisibilité d'un nombre quelconque ω par β_1^n ou par β_2^n respectivement par les congruences

$$(\beta_1^n) \qquad \omega(1-\theta)^n \equiv 0 \pmod{3^n},$$

$$(\beta_2^n) \qquad \omega(1+\theta)^n \equiv 0 \pmod{3^n},$$

et il en résulterait une suite de théorèmes qui coïncideraient parfaitement avec ceux de la théorie des nombres rationnels. On traiterait de la même façon les nombres premiers idéaux γ_1, γ_2.

§ 10. — Lois de la divisibilité dans le domaine o.

En étudiant d'une manière semblable tout le domaine o des nombres $\omega = x + y\theta$, on trouve les résultats suivants:

1° Tous les nombres premiers rationnels positifs qui sont $\equiv 11$, 13, 17, 19 (mod 20) se comportent aussi, dans le cas actuel, comme des nombres premiers.

2° Le nombre θ, dont le carré $= -5$, possède le caractère d'un nombre premier; le nombre 2 se comporte comme le carré d'un nombre premier idéal α.

3° Tout nombre premier rationnel positif qui est $\equiv 1, 9 \pmod{20}$ peut se décomposer en deux facteurs différents, réellement existants, dont chacun a le caractère d'un nombre premier.

4° Tout nombre premier rationnel positif qui est $\equiv 3, 7 \pmod{20}$ se comporte comme un produit de deux nombres premiers idéaux différents entre eux.

5° Tout nombre existant ω, différent de zéro et de ± 1, est ou un des nombres désignés ci-dessus qui ont le caractère de nombres premiers, ou bien il se comporte, dans toutes les questions de divisibilité, comme s'il était un produit composé d'une manière complétement déterminée de facteurs premiers existants et idéaux.

Mais, pour parvenir à ce résultat et acquérir une certitude complète sur la question de savoir si, en réalité, toutes les lois générales de la divisibilité qui régissent le domaine des nombres rationnels peuvent s'étendre à notre domaine o à l'aide des nombres idéaux que nous avons introduits*), il faut encore, comme on s'en

*) Il semblera peut-être à quelques personnes évident a priori que le rétablissement de cette harmonie avec la théorie des nombres rationnels doit pouvoir s'imposer, quoi qu'il arrive, par l'introduction des nombres idéaux; mais l'exemple, déjà donné plus haut, du rôle irrégulier du nombre 2 dans le domaine des nombres $x + y\sqrt{-3}$, suffit bien pour dissiper cette illusion.

apercevra bientôt quand on essayera une déduction rigoureuse, se livrer à une étude très-approfondie, lors même qu'on voudrait supposer connue ici la théorie des résidus quadratiques et celle des formes quadratiques binaires (théorie qui, réciproquement, se tire avec la plus grande facilité de la théorie générale des nombres algébriques entiers). On peut bien atteindre en toute rigueur le but proposé, en suivant la voie indiquée; mais, comme nous l'avons remarqué dans l'Introduction, la plus grande circonspection est nécessaire pour ne pas se laisser entraîner à des conclusions prématurées, et, en particulier, la notion de produit de facteurs quelconques, existants ou idéaux, ne peut être exactement définie qu'à l'aide de détails assez minutieux. A cause de ces difficultés, il semblera toujours désirable de remplacer le nombre idéal de Kummer, qui n'est jamais défini en lui-même, mais seulement comme diviseur des nombres existants ω du domaine o, par un substantif réellement existant, et c'est ce qui peut se faire de plusieurs manières.

On pourrait, par exemple (et, si je ne me trompe, ce serait la voie que Kronecker aurait choisie dans ses recherches), introduire, au lieu des nombres idéaux, des nombres algébriques existants, mais non compris dans le domaine o, et les adjoindre à ce domaine dans le sens que Galois a donné à ce mot. En effet, si l'on pose

$$\beta_1 = \sqrt{-2+\theta}, \quad \beta_2 = \sqrt{-2-\theta},$$

et que l'on choisisse ces radicaux carrés de manière que l'on ait $\beta_1\beta_2 = 3$, on aura

$$\theta^2 = -5, \quad \beta_1^2 = -2+\theta, \quad \beta_2^2 = -2-\theta,$$

$$\beta_1\beta_2 = 3, \quad \theta\beta_1 = -2\beta_1 - 3\beta_2, \quad \theta\beta_2 = 3\beta_1 + 2\beta_2,$$

d'où il s'ensuit que les nombres quadrinômes

$$x + y\theta + z_1\beta_1 + z_2\beta_2,$$

où x, y, z_1, z_2 désignent des nombres rationnels entiers quelconques, se reproduiront par addition, soustraction et multiplication; le domaine o′ de ces nombres embrasse le domaine o, et tous les nombres idéaux qu'il fallait introduire dans ce dernier pourront être remplacés par des nombres existants du nouveau domaine o′. En posant, par exemple,

$$\alpha = \beta_1 + \beta_2, \quad \gamma_1 = 2\beta_1 + \beta_2, \quad \gamma_2 = \beta_1 + 2\beta_2,$$

toutes les équations (4) du § 7 seront satisfaites; pareillement, les deux facteurs premiers idéaux du nombre 23 dans le domaine $\mathfrak{o}$ seront remplacés par les deux nombres existants $2\beta_1 - \beta_2$ et $-\beta_1 + 2\beta_2$ du domaine $\mathfrak{o}'$, et il en sera de même de tous les nombres idéaux du domaine $\mathfrak{o}$.

Cependant cette voie, bien qu'elle puisse aussi conduire au but, ne me semble pas présenter toute la simplicité désirable, parce que l'on est forcé de passer du domaine donné $\mathfrak{o}$ à un domaine plus compliqué $\mathfrak{o}'$; et il est facile aussi de reconnaître que dans le choix de ce nouveau domaine $\mathfrak{o}'$ il règne un grand arbitraire. Dans l'Introduction, j'ai exposé avec tant de détails le courant d'idées qui m'a conduit à fonder cette théorie sur une tout autre base, savoir, sur la notion de l'idéal, qu'il serait superflu d'y revenir ici, et je me bornerai, en conséquence, à éclaircir cette notion par un exemple.

§ 11. — Idéaux dans le domaine $\mathfrak{o}$.

La condition pour qu'un nombre $\omega = x + y\theta$ soit divisible par le nombre premier idéal α consiste, d'après le § 8, dans la congruence $x \equiv y \pmod 2$; donc, pour obtenir le système $\mathfrak{a}$ de tous les nombres ω divisibles par α, on posera $x = y + 2z$, y et z désignant des nombres rationnels entiers quelconques; ce système $\mathfrak{a}$ se compose donc de tous les nombres de la forme $2z + (1+\theta)y$, c'est-à-dire que $\mathfrak{a}$ est un module fini, dont la base se compose des deux nombres indépendants 2 et $1+\theta$, et par suite

$$\mathfrak{a} = [2,\ 1+\theta].$$

En désignant de même par $\mathfrak{b}_1$, $\mathfrak{b}_2$, $\mathfrak{c}_1$, $\mathfrak{c}_2$ les systèmes de tous les nombres ω divisibles respectivement par les nombres premiers idéaux β_1, β_2, γ_1, γ_2, on tirera, des congruences correspondantes du § 9,

$$\mathfrak{b}_1 = [3,\ 1+\theta], \quad \mathfrak{b}_2 = [3,\ 1-\theta],$$
$$\mathfrak{c}_1 = [7,\ 3+\theta], \quad \mathfrak{c}_2 = [7,\ 3-\theta].$$

Si l'on désigne maintenant par $\mathfrak{m}$ un quelconque de ces cinq systèmes, $\mathfrak{m}$ jouira des propriétés suivantes:

I. Les sommes et les différences de deux nombres quelconques du système $\mathfrak{m}$ seront toujours des nombres de ce même système $\mathfrak{m}$.

II. Tout produit d'un nombre du système $\mathfrak{m}$ et d'un nombre du système $\mathfrak{o}$ est un nombre du système $\mathfrak{m}$.

La première propriété, caractéristique de chaque module, est évidente. Pour constater la seconde propriété relativement au système $\mathfrak{m}$, dont la base se compose des deux nombres μ, μ', il suffit évidemment de démontrer que les deux produits $\theta\mu$, $\theta\mu'$ appartiennent au même système; pour le système $\mathfrak{a}$, cela résulte des deux égalités

$$2\theta = -1.2 + 2(1+\theta), \quad (1+\theta)\theta = -3.2 + (1+\theta),$$

et il en est exactement de même pour les autres systèmes. Mais ces deux propriétés peuvent aussi s'établir sans ces vérifications, en s'appuyant sur ce que chacun des cinq systèmes $\mathfrak{m}$ est l'ensemble de tous les nombres ω du domaine $\mathfrak{o}$ qui satisfont à une congruence de la forme

$$\nu\omega \equiv 0 \pmod\mu,$$

μ, ν étant deux nombres donnés du domaine $\mathfrak{o}$.

Nous appellerons maintenant tout système $\mathfrak{m}$, composé de nombres du domaine $\mathfrak{o}$ et jouissant des deux propriétés I et II, un idéal, et nous nous poserons d'abord le problème de trouver la forme générale de tous les idéaux. En excluant le cas singulier où $\mathfrak{m}$ se compose du seul nombre zéro, et choisissant arbitrairement un nombre μ (différent de zéro), de l'idéal $\mathfrak{m}$, alors, si l'on désigne par μ' le nombre conjugué, la norme $N(\mu) = \mu\mu'$, ainsi que le produit $\theta N(\mu)$, appartiendra aussi, en vertu de II, à l'idéal $\mathfrak{m}$; donc tous les nombres du module $\mathfrak{o} = [1,\ \theta]$, en les multipliant par le nombre rationnel $N(\mu)$ différent de zéro, se changeront en nombres du module $\mathfrak{m}$, lequel est en même temps un multiple de $\mathfrak{o}$; or il s'ensuit de là (§ 3, 2°) que $\mathfrak{m}$ est un module fini, de la forme $[k,\ l+m\theta]$, k, l, m étant des nombres rationnels entiers, parmi lesquels k et m pourront être choisis positifs. Puisque $\mathfrak{m}$ possède déjà, comme module, la propriété I, il ne s'agit plus maintenant que de l'assujettir à la propriété II, qui consiste en ce que les deux produits $k\theta$ et $(l+m\theta)\theta$ appartiennent au même système $\mathfrak{m}$. Les conditions nécessaires et suffisantes pour cela consistent, comme on le voit sans peine, en ce que k et l soient divisibles par m et que les nombres rationnels entiers a, b, qui entrent dans l'expression

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

satisfassent, en outre, à la congruence

$$b^2 \equiv -5 \pmod a;$$

si l'on remplace b par un nombre quelconque qui soit $\equiv b \pmod a$, l'idéal $\mathfrak{m}$ ne sera pas changé. Les cinq idéaux ci-dessus $\mathfrak{a}$, $\mathfrak{b}_1$, $\mathfrak{b}_2$, $\mathfrak{c}_1$, $\mathfrak{c}_2$ sont évidemment contenus dans cette forme, puisque $(b+\theta)$ peut aussi être remplacé par $-(b+\theta)$.

L'ensemble de tous les nombres conjugués avec les nombres de l'idéal $\mathfrak{m}$ est évidemment aussi un idéal

$$\mathfrak{m}_1 = [m\,a,\ m(-b+\theta)];$$

deux idéaux de cette sorte $\mathfrak{m}$, $\mathfrak{m}_1$ peuvent être appelés des idéaux conjugués.

Soit μ un nombre quelconque du domaine $\mathfrak{o}$; le système $[\mu, \mu\theta]$ de tous les nombres divisibles par μ formera un idéal, que nous appellerons un idéal principal*), et que nous désignerons par $\mathfrak{o}(\mu)$ ou encore par $\mathfrak{o}\mu$; il est facile de lui donner la forme ci-dessus $[m\,a,\ m(b+\theta)]$; m est le plus grand nombre rationnel entier qui divise $\mu = m(u+v\theta)$, et l'on a, de plus

$$a = \frac{N(\mu)}{m^2}, \quad v\,b \equiv u \pmod a.$$

On trouve ainsi, par exemple,

$$\mathfrak{o}(\pm 1) = \mathfrak{o} = [1,\ \theta],$$

et

$$\mathfrak{o}(2) = [2,\ 2\theta], \quad \mathfrak{o}(3) = [3,\ 3\theta], \quad \mathfrak{o}(7) = [7,\ 7\theta],$$
$$\mathfrak{o}(1\pm\theta) = [6,\ \pm 1+\theta], \quad \mathfrak{o}(3\pm\theta) = [14,\ \pm 3+\theta],$$
$$\mathfrak{o}(-2\pm\theta) = [9,\ \mp 2+\theta], \quad \mathfrak{o}(2\pm 3\theta) = [49,\ \pm 17+\theta],$$
$$\mathfrak{o}(-1\pm 2\theta) = [21,\ \pm 10+\theta], \quad \mathfrak{o}(4\pm\theta) = [21,\ \pm 4+\theta].$$

Comme tous les idéaux sont en même temps des modules, nous dirons (d'après le § 2, 1°) que deux nombres ω, ω' sont congrus par rapport à l'idéal $\mathfrak{m}$, et nous poserons $\omega \equiv \omega' \pmod{\mathfrak{m}}$, lorsque la différence $\omega - \omega'$ sera un nombre contenu dans $\mathfrak{m}$; la norme $N(\mathfrak{m})$ de l'idéal $\mathfrak{m} = [m\,a,\ m(b+\theta)]$ sera le nombre

$$(\mathfrak{o}, \mathfrak{m}) = m^2 a$$

*) Si l'on étend la définition de l'idéal au domaine $\mathfrak{o}$ des nombres rationnels entiers, ou à celui des nombres complexes entiers de Gauss, ou à l'un des cinq domaines $\mathfrak{o}$ dont il a été question dans le § 7, on voit aisément que tout idéal est un idéal principal; il est évident aussi que, dans le domaine des nombres rationnels entiers, la propriété II est déjà contenue dans la propriété I.

des classes dans lesquelles se décompose le domaine $\mathfrak{o}$ par rapport au module $\mathfrak{m}$ (§ 4, 4°). Si $\mathfrak{m}$ est un idéal principal $\mathfrak{o}\mu$, la congruence précédente sera identique avec $\omega \equiv \omega' \pmod \mu$, et l'on aura

$$N(\mathfrak{m}) = N(\mu).$$

La norme d'un nombre quelconque $m\{a\,x+(b+\theta)\,y\}$ contenu dans l'idéal $\mathfrak{m} = [m\,a,\ m(b+\theta)]$ est égale au produit de $N(\mathfrak{m}) = m^2 a$ par la forme quadratique binaire $a\,x^2 + 2\,b\,x\,y + c\,y^2$, dont le déterminant, suivant la définition de Gauss, est $b^2 - a\,c = -5$ *).

§ 12. — Divisibilité et multiplication des idéaux dans le domaine $\mathfrak{o}$.

Je vais maintenant montrer de quelle manière la théorie des nombres $\omega = x + y\,\theta$ du domaine $\mathfrak{o}$ peut se fonder sur la notion de l'idéal; toutefois, je serai obligé, pour abréger, de laisser au lecteur le soin de développer quelques calculs faciles.

Nous dirons, absolument comme dans la théorie des modules (§ 1, 2°), qu'un idéal $\mathfrak{m}''$ est divisible par un idéal $\mathfrak{m}$, quand tous les nombres du premier seront contenus aussi dans le second. D'après cela, un idéal principal $\mathfrak{o}\mu''$ sera toujours divisible par un idéal principal $\mathfrak{o}\mu$ dans le cas, et seulement dans ce cas, où le nombre μ'' sera divisible par le nombre μ; de là résulte que la théorie de la divisibilité des nombres est contenue dans celle des idéaux. Les conditions nécessaires et suffisantes pour que l'idéal

$$\mathfrak{m}'' = [m''a'',\ m''(b''+\theta)]$$

soit divisible par l'idéal $\mathfrak{m} = [m\,a,\ m(b+\theta)]$ consiste, comme on l'aperçoit immédiatement, dans les trois congruences

$$m''a \equiv m''a'' \equiv m''(b''-b) \equiv 0 \pmod{m\,a}.$$

La définition de la multiplication des idéaux est celle-ci: Si μ parcourt tous les nombres de l'idéal $\mathfrak{m}$, et de même μ' tous les nombres de l'idéal $\mathfrak{m}'$, tous les produits $\mu\mu'$ et leurs sommes formeront un idéal $\mathfrak{m}''$, qui sera dit le produit**) des facteurs $\mathfrak{m}$, $\mathfrak{m}'$, et que l'on désignera par $\mathfrak{m}\mathfrak{m}'$. On aura évidemment $\mathfrak{o}\mathfrak{m} = \mathfrak{m}$, $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}'\mathfrak{m}$,

*) La théorie générale des formes se simplifie cependant un peu si l'on admet aussi les formes $A\,x^2 + B\,x\,y + C\,y^2$, où B est impair, et si l'on entend toujours par déterminant de la forme le nombre $B^2 - 4\,A\,C$.

**) La même définition s'applique aussi à la multiplication de deux modules quelconques.

$(\mathfrak{m}\mathfrak{m}')\mathfrak{n} = \mathfrak{m}(\mathfrak{m}'\mathfrak{n})$, et de là s'ensuivent, pour les produits d'un nombre quelconque d'idéaux, les mêmes théorèmes que pour les produits de nombres*); de plus, il est clair que le produit des deux idéaux principaux $\mathfrak{o}\mu$ et $\mathfrak{o}\mu'$ est l'idéal principal $\mathfrak{o}(\mu\mu')$.

Soient donnés maintenant deux idéaux,

$$\mathfrak{m} = [m a,\ m(b+\theta)], \quad \mathfrak{m}' = [m' a',\ m'(b'+\theta)];$$

on déduira de là leur produit

$$\mathfrak{m}'' = \mathfrak{m}\mathfrak{m}' = [m'' a'',\ m''(b''+\theta)],$$

à l'aide des méthodes indiquées dans la première Section (§ 4, 5° et 6°); car il est clair d'abord, en vertu de la définition, que le produit $\mathfrak{m}\mathfrak{m}'$ est un module fini, dont la base se compose des quatre produits

$$m m' a a', \quad m m' a(b'+\theta), \quad m m' a'(b+\theta),$$
$$m m'(b+\theta)(b'+\theta) = m m'[b b' - 5 + (b+b')\theta],$$

dont deux seulement sont indépendants entre eux. On trouve ainsi, par exemple, pour les idéaux considérés plus haut,

$$\mathfrak{b}_1 = [3,\ 1+\theta], \quad \mathfrak{c}_2 = [7,\ 3-\theta],$$

le produit

$$\mathfrak{b}_1\mathfrak{c}_2 = [21,\ 9-3\theta,\ \ 7+7\theta,\ \ 8+2\theta];$$

ce module se déduit de celui qui a été considéré à la fin de la première Section (§ 4, 6°), en y faisant $\omega_1 = 1$, $\omega_2 = \theta$, et l'on en tire

$$\mathfrak{b}_1\mathfrak{c}_2 = [21,\ -17+\theta] = [21,\ 4+\theta] = \mathfrak{o}(4+\theta);$$

on obtiendrait absolument de la même manière les résultats suivants, entièrement analogues aux équations hypothétiques (4) du § 7:

$$\begin{aligned}
\mathfrak{o}(2) &= \mathfrak{a}^2, \quad \mathfrak{o}(3) = \mathfrak{b}_1\mathfrak{b}_2, \quad \mathfrak{o}(7) = \mathfrak{c}_1\mathfrak{c}_2;\\
\mathfrak{o}(-2+\theta) &= \mathfrak{b}_1^2, \quad \mathfrak{o}(-2-\theta) = \mathfrak{b}_2^2;\\
\mathfrak{o}(2+3\theta) &= \mathfrak{c}_1^2, \quad \mathfrak{o}(2-3\theta) = \mathfrak{c}_2^2;\\
\mathfrak{o}(1+\theta) &= \mathfrak{a}\mathfrak{b}_1, \quad \mathfrak{o}(1-\theta) = \mathfrak{a}\mathfrak{b}_2;\\
\mathfrak{o}(3+\theta) &= \mathfrak{a}\mathfrak{c}_1, \quad \mathfrak{o}(3-\theta) = \mathfrak{a}\mathfrak{c}_2;\\
\mathfrak{o}(-1+2\theta) &= \mathfrak{b}_1\mathfrak{c}_1, \quad \mathfrak{o}(-1-2\theta) = \mathfrak{b}_2\mathfrak{c}_2;\\
\mathfrak{o}(4+\theta) &= \mathfrak{b}_1\mathfrak{c}_2, \quad \mathfrak{o}(4-\theta) = \mathfrak{b}_2\mathfrak{c}_1.
\end{aligned}$$

Pour effectuer en général la multiplication de deux idéaux quelconques $\mathfrak{m}$, $\mathfrak{m}'$, il faut transformer la base composée des quatre

*) Voir Dirichlet, Vorlesungen über Zahlentheorie, § 2.

nombres ci-dessus en une autre composée seulement des deux nombres $m'' a''$, $m''(b''+\theta)$. On y parvient (en vertu du § 4), au moyen de quatre équations de la forme

$$\begin{aligned}
m m' a a' &= p\ m'' a'' + q\ m''(b''+\theta),\\
m m' a(b'+\theta) &= p'\ m'' a'' + q'\ m''(b''+\theta),\\
m m' a'(b+\theta) &= p''\ m'' a'' + q''\ m''(b''+\theta),\\
m m'[b b' - 5 + (b+b')\theta] &= b'''m'' a'' + q'''m''(b''+\theta),
\end{aligned}$$

où p, p', ..., q''' désignent huit nombres rationnels entiers tellement choisis que les six déterminants, formés avec ces nombres,

$$\begin{aligned}
P &= p\ q' - q\ p', \quad Q = p\,q'' - q\,p'', \quad R = p\,q''' - q\,p''',\\
U &= p''q''' - q''p''', \quad T = p'q''' - q'p''', \quad S = p'q'' - q'p'',
\end{aligned}$$

n'admettent aucun diviseur commun. Des quatre équations précédentes, dont chacune se décompose en deux autres, on conclura maintenant sans peine que ces six déterminants sont respectivement proportionnels aux six nombres

$$\begin{aligned}
&a, \quad a', \quad b'+b,\\
&c, \quad c', \quad b'-b,
\end{aligned}$$

c et c' étant déterminés par les équations

$$b b - a c = b' b' - a' c' = -5;$$

or, comme ces six nombres n'admettent non plus aucun diviseur commun*), ils devront coïncider précisément avec ces six déterminants. Il s'ensuit de là, puisque l'on a $q = 0$, et que q', q'', q''' ne peuvent avoir aucun diviseur commun, que l'on déterminera comme il suit le produit $\mathfrak{m}'' = \mathfrak{m}\mathfrak{m}'$ des deux facteurs donnés $\mathfrak{m}$, $\mathfrak{m}'$. Soit p le plus grand commun diviseur (positif) des trois nombres donnés

$$a = pq', \quad a' = pq'', \quad b+b' = pq''';$$

on aura

$$m'' = p m m', \quad a'' = \frac{a a'}{p^2} = q'q'',$$

et b'' sera déterminé par les congruences

$$q' b'' \equiv q'\,b', \quad q''\,b'' \equiv q''\,b, \quad q'''\,b'' \equiv \frac{b\,b'-5}{p} \pmod{a''};$$

puis on aura en même temps $b''\,b'' \equiv -5 \pmod{a''}$, c'est-à-dire

$$b''\,b'' - a''\,c'' = -5,$$

*) Il n'en serait pas toujours ainsi dans le domaine des nombres $x + y\sqrt{-3}$.

c'' désignant un nombre rationnel entier, et, d'après la dénomination employée par Gauss*), la forme quadratique binaire (a'', b'', c'') sera composée des deux formes (a, b, c) et (a', b', c').

Des valeurs de m'', a'' on tire $m''^2 a'' = m^2 a . m'^2 a'$, d'où ce théorème

$$N(\mathfrak{m}\mathfrak{m}') = N(\mathfrak{m})\,N(\mathfrak{m}');$$

en outre, il faut remarquer le cas particulier où $\mathfrak{m}'$ est l'idéal $\mathfrak{m}_1$ conjugué avec $\mathfrak{m}$; des formules précédentes on déduit immédiatement ce résultat

$$\mathfrak{m}\,\mathfrak{m}_1 = \mathfrak{o}\,N(\mathfrak{m}).$$

Les deux notions de la divisibilité et de la multiplication des idéaux sont maintenant liées entre elles de la manière suivante. Le produit $\mathfrak{m}\mathfrak{m}'$ est divisible à la fois par $\mathfrak{m}$ et par $\mathfrak{m}'$, puisque, en vertu de la propriété II des idéaux, tous les produits $\mu\mu'$, dont les facteurs sont contenus respectivement dans $\mathfrak{m}$, $\mathfrak{m}'$, appartiennent également à ces idéaux; on tirerait la même conclusion de la forme de l'idéal-produit trouvée plus haut. Réciproquement, si l'idéal $\mathfrak{m}'' = [m''a'', m''(b''+\theta)]$ est divisible par l'idéal $\mathfrak{m} = [ma, m(b+\theta)]$, il existera un idéal $\mathfrak{m}'$, et un seul, tel que l'on aura $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}''$; si l'on désigne, en effet, par $\mathfrak{m}_1$ l'idéal conjugué de $\mathfrak{m}$, et que l'on forme, d'après les règles précédentes, le produit

$$\mathfrak{m}_1\mathfrak{m}'' = [m'''a', m'''(b'+\theta)],$$

il résulte, des trois congruences établies au commencement de ce paragraphe, que m''' est divisible par $N(\mathfrak{m}) = m^2 a$, et par suite que $m''' = m^2 a m'$, m' désignant un nombre entier; en joignant à cela le théorème précédent, que $\mathfrak{m}\mathfrak{m}_1 = \mathfrak{o}(m^2 a)$, on en conclut aisément que l'idéal $\mathfrak{m}' = [m'a', m'(b'+\theta)]$, et lui seul, remplit la condition $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}''$. Il en résulte en même temps que l'égalité $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}\mathfrak{m}'''$ entraîne toujours l'égalité $\mathfrak{m}' = \mathfrak{m}'''$.

Pour arriver maintenant à la conclusion de cette théorie, il ne nous reste plus qu'à introduire encore la notion suivante: un idéal $\mathfrak{p}$, différent de $\mathfrak{o}$ et n'ayant pour diviseur aucun autre idéal que $\mathfrak{o}$ et $\mathfrak{p}$, sera dit un idéal premier. η étant un nombre déterminé, le système $\mathfrak{r}$ de toutes les racines ϱ de la congruence $\eta\varrho \equiv 0 \pmod{\mathfrak{p}}$ formera un idéal, parce qu'il possède les propriétés I et II;

*) Disquisitiones arithmeticæ, art. 235, 242.

cet idéal $\mathfrak{r}$ est un diviseur de $\mathfrak{p}$, puisque tous les nombres contenus dans $\mathfrak{p}$ sont aussi des racines de cette congruence; donc, si $\mathfrak{p}$ est un idéal premier, $\mathfrak{r}$ devra être ou $= \mathfrak{o}$ ou $= \mathfrak{p}$. Si le nombre donné η n'est pas contenu dans $\mathfrak{p}$, le nombre 1, contenu dans $\mathfrak{o}$, ne sera pas une racine de la congruence, et partant dans ce cas $\mathfrak{r}$ ne sera pas $= \mathfrak{o}$, mais $= \mathfrak{p}$, c'est-à-dire que toutes les racines ϱ devront être contenues dans $\mathfrak{p}$. Ainsi se trouve évidemment établi le théorème suivant*): «Un produit $\eta\varrho$ de deux nombres η, ϱ n'est contenu dans un idéal premier $\mathfrak{p}$ que si l'un au moins des deux facteurs est contenu dans $\mathfrak{p}$.» Et de là résulte immédiatement cet autre théorème: «Si aucun des deux idéaux $\mathfrak{m}$, $\mathfrak{m}'$ n'est divisible par l'idéal premier $\mathfrak{p}$, leur produit $\mathfrak{m}\mathfrak{m}'$ ne sera pas non plus divisible par $\mathfrak{p}$»; car, puisqu'il y a dans $\mathfrak{m}$, $\mathfrak{m}'$ respectivement des nombres μ, μ' qui ne sont pas contenus dans $\mathfrak{p}$, il existera aussi dans $\mathfrak{m}\mathfrak{m}'$ un nombre $\mu\mu'$ qui ne sera pas non plus contenu dans $\mathfrak{p}$.

En combinant le théorème que nous venons de démontrer avec les théorèmes précédents relatifs à la dépendance entre les notions de divisibilité et de multiplication des idéaux, et ayant égard à ce que, en dehors de $\mathfrak{o}$, il n'existe aucun autre idéal dont la norme soit $= 1$, on arrive, par les mêmes raisonnements**) que dans la théorie des nombres rationnels, au théorème suivant: «Tout idéal différent de $\mathfrak{o}$ ou est un idéal premier, ou peut se mettre, et cela d'une seule manière, sous la forme d'un produit d'un nombre fini d'idéaux premiers.» De ce théorème il résulte immédiatement qu'un idéal $\mathfrak{m}''$ est toujours divisible par un idéal $\mathfrak{m}$ dans le cas, et seulement dans ce cas, où toutes les puissances d'idéaux premiers qui divisent $\mathfrak{m}$ divisent aussi $\mathfrak{m}''$. Si $\mathfrak{m} = \mathfrak{o}\mu$ et $\mathfrak{m}'' = \mathfrak{o}\mu''$ sont des idéaux principaux, le même critérium décide aussi de la divisibilité du nombre μ'' par le nombre μ. Et ainsi la théorie de la divisibilité des nombres dans le domaine $\mathfrak{o}$ se trouve ramenée à des lois fixes et simples.

Toute cette théorie peut s'appliquer presque mot pour mot à un domaine $\mathfrak{o}$ quelconque composé de tous les nombres entiers d'un corps quelconque Ω du second degré, quand la notion de nombre

*) Ce théorème conduit aisément à la détermination de tous les idéaux premiers contenus dans $\mathfrak{o}$, et ceux-ci correspondent exactement aux nombres premiers, existants et idéaux, énumérés dans le § 10.

**) Voir Dirichlet, Vorlesungen über Zahlentheorie, § 8.

entier est définie comme elle l'a été dans l'Introduction*). Mais cette base de la théorie, bien qu'elle ne laisse rien à désirer du côté de la rigueur, n'est nullement celle que je me propose d'établir. On peut remarquer, en effet, que les démonstrations des propositions les plus importantes se sont appuyées sur la représentation des idéaux par l'expression $[m\,a,\ m(b+\theta)]$ et sur la réalisation effective de la multiplication, c'est-à-dire sur un calcul qui coïncide avec la composition des formes quadratiques binaires, enseignée par Gauss. Si l'on voulait traiter de la même manière tous les corps Ω de degré quelconque, on se heurterait à de grandes difficultés, peut-être insurmontables. Mais, lors même qu'il n'en serait pas ainsi, une telle théorie, fondée sur le calcul, n'offrirait pas encore, ce me semble, le plus haut degré de perfection; il est préférable, comme dans la théorie moderne des fonctions, de chercher à tirer les démonstrations, non plus du calcul, mais immédiatement des concepts fondamentaux caractéristiques, et d'édifier la théorie de manière qu'elle soit, au contraire, en état de prédire les résultats du calcul (par exemple, la composition des formes décomposables de tous les degrés). Tel est le but que je vais poursuivre dans les Sections suivantes de ce Mémoire. ...

*) Le domaine, mentionné plus haut, des nombres $x+y\sqrt{-3}$, où x, y prennent toutes les valeurs rationnelles et entières, n'est pas un domaine de cette nature; mais il constitue seulement une partie du domaine $\mathfrak{o}$ de tous les nombres $x+y\varrho$, ϱ étant une racine de l'équation $\varrho^2+\varrho+1=0$.

[Erläuterungen gemeinsam mit denen zu XLVI, XLVII, XLIX am Schluß von XLIX.]

XLIX.

Über die Theorie der ganzen algebraischen Zahlen.

[Supplement XI von Dirichlets Vorlesungen über Zahlentheorie, 3. Aufl., S. 515—530 (1879).]

Inhalt.

§ 170.

Während unsere bisherigen Untersuchungen über Ideale wesentlich nur in einer Anwendung der Lehre von der Teilbarkeit der Moduln bestanden, gehen wir jetzt zu einer neuen Idealbildung, nämlich zur Multiplikation der Ideale über, welche den eigentlichen Kern der Idealtheorie bildet.

Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei beliebige Ideale, 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, welche als ein Produkt $\alpha\beta$ oder als Summe von mehreren solchen Produkten $\alpha\beta$ darstellbar sind. Alle diese Zahlen sind wieder in $\mathfrak{o}$ enthalten, und sie verschwinden nicht sämtlich; sie reproduzieren sich durch Addition und Subtraktion, sowie durch Multiplikation mit beliebigen Zahlen ω des Gebietes $\mathfrak{o}$, weil jedes Produkt $\beta\omega$ wieder in $\mathfrak{b}$ enthalten ist. Mithin ist das Produkt $\mathfrak{a}\mathfrak{b}$ wieder ein Ideal.

Es leuchtet ohne weiteres ein, daß $\mathfrak{a}\mathfrak{o}=\mathfrak{a}$, $\mathfrak{a}(\mathfrak{o}\eta)=\mathfrak{a}\eta$, $\mathfrak{a}\mathfrak{b}=\mathfrak{b}\mathfrak{a}$ und $(\mathfrak{a}\mathfrak{b})\mathfrak{c}=\mathfrak{a}(\mathfrak{b}\mathfrak{c})$ ist; wir bezeichnen dieses letztere Produkt kurz mit $\mathfrak{a}\mathfrak{b}\mathfrak{c}$, und aus der schon öfter angewendeten Schlußweise (§§ 2, 147) geht hervor, daß das mit $\mathfrak{a}\mathfrak{b}\mathfrak{c}\mathfrak{d}\ldots$ zu bezeichnende Produkt aus m beliebigen Idealen $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{d}\ldots$ eine vollständig bestimmte, von der Anordnung der sukzessiven Multiplikationen gänzlich

unabhängige Bedeutung hat*). Sind alle diese m Faktoren identisch mit dem Ideal $\mathfrak{a}$, so bezeichnen wir ihr Produkt mit $\mathfrak{a}^m$ und nennen es die m^{te} Potenz von $\mathfrak{a}$; m heißt der Exponent dieser Potenz, und wir dehnen diesen Begriff auch auf die beiden Fälle $m = 0$ und $m = 1$ aus, indem wir $\mathfrak{a}^0 = \mathfrak{o}$ und $\mathfrak{a}^1 = \mathfrak{a}$ setzen; dann gelten allgemein die Sätze $\mathfrak{a}^r \mathfrak{a}^s = \mathfrak{a}^{r+s}$ und $(\mathfrak{a}^r)^s = \mathfrak{a}^{rs}$.

Es wird nun unsere Hauptaufgabe sein, den Zusammenhang zwischen diesem Begriffe der Multiplikation und demjenigen der Teilbarkeit der Ideale vollständig zu ergründen; diese Untersuchung bietet erhebliche Schwierigkeiten dar, und wir begnügen uns für jetzt, die folgenden, äußerst einfachen Sätze zu beweisen.

1. Ist $\mathfrak{a}$ teilbar durch $\mathfrak{a}'$, und $\mathfrak{b}$ teilbar durch $\mathfrak{b}'$, so ist $\mathfrak{a}\mathfrak{b}$ teilbar durch $\mathfrak{a}'\mathfrak{b}'$.

Denn da jede Zahl α des Ideals $\mathfrak{a}$ auch in $\mathfrak{a}'$, und jede Zahl β des Ideals $\mathfrak{b}$ auch in $\mathfrak{b}'$ enthalten ist, so ist jedes Produkt $\alpha\beta$, und folglich auch jede Summe solcher Produkte $\alpha\beta$ in $\mathfrak{a}'\mathfrak{b}'$ enthalten.

2. Das Produkt $\mathfrak{a}\mathfrak{b}$ ist ein gemeinschaftliches Vielfaches der beiden Faktoren $\mathfrak{a}$ und $\mathfrak{b}$.

Denn $\mathfrak{a}$ ist durch $\mathfrak{a}$, und $\mathfrak{b}$ ist durch $\mathfrak{o}$ teilbar, woraus (nach 1.) folgt, daß $\mathfrak{a}\mathfrak{b}$ durch $\mathfrak{a}\mathfrak{o}$, d. h. durch $\mathfrak{a}$ teilbar ist.

3. Ist $\mathfrak{m}$ das kleinste gemeinschaftliche Vielfache, und $\mathfrak{d}$ der größte gemeinschaftliche Teiler von $\mathfrak{a}$ und $\mathfrak{b}$, so ist $\mathfrak{m}\mathfrak{d}$ durch $\mathfrak{a}\mathfrak{b}$ teilbar**).

Denn jede Zahl δ des Ideals $\mathfrak{d}$ ist von der Form $\alpha + \beta$, wo α in $\mathfrak{a}$, und β in $\mathfrak{b}$ enthalten ist, und jede Zahl μ des Ideals $\mathfrak{m}$ ist sowohl in $\mathfrak{b}$ als auch in $\mathfrak{a}$ enthalten, woraus folgt, daß die beiden Produkte $\alpha\mu$ und $\mu\beta$ dem Ideal $\mathfrak{a}\mathfrak{b}$ angehören; dasselbe gilt mithin auch von ihrer Summe $\mu\delta$, also auch von jeder Zahl des Ideals $\mathfrak{m}\mathfrak{d}$.

§ 171.

Zwei Ideale $\mathfrak{a}$, $\mathfrak{b}$ heißen relative Primideale, und jedes von ihnen heißt relatives Primideal zu dem anderen, wenn ihr größter gemeinschaftlicher Teiler $= \mathfrak{o}$ ist; da nun die Zahl 1 in $\mathfrak{o}$ enthalten

*) Es ist der Inbegriff aller Zahlen von der Form $\Sigma\alpha\beta\gamma\delta\ldots$, wo $\alpha, \beta, \gamma, \delta\ldots$ beliebige Zahlen bzw. der Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d}\ldots$ bedeuten; dies könnte auch von vornherein als Definition eines Produktes von beliebig vielen Idealen gelten.

**) Daß $\mathfrak{m}\mathfrak{d} = \mathfrak{a}\mathfrak{b}$ ist, werden wir erst später (§ 173, 9.) beweisen können.

ist, so gibt es eine Zahl α in $\mathfrak{a}$ und eine Zahl β in $\mathfrak{b}$, welche der Bedingung

$$\alpha + \beta = 1$$

genügen, und umgekehrt folgt aus der Existenz eines solchen Zahlenpaares α, β, daß $\mathfrak{a}, \mathfrak{b}$ relative Primideale sind, weil (nach § 168, 1.) $\mathfrak{o}$ das einzige Ideal ist, welches in 1 aufgeht. Dasselbe Kriterium kann man offenbar auch so ausdrücken, daß in $\mathfrak{b}$ eine Zahl β existiert, welche der Kongruenz

$$\beta \equiv 1 \pmod{\mathfrak{a}}$$

genügt. Wir bemerken ferner ein für allemal, daß, wenn wir mehr als zwei Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}\ldots$ relative Primideale nennen, hierunter immer zu verstehen ist, daß jedes dieser Ideale relatives Primideal zu jedem der übrigen ist. Aus dieser Definition ergeben sich zunächst die folgenden Sätze.

1. Ist $\mathfrak{a}$ relatives Primideal zu $\mathfrak{b}$ und zu $\mathfrak{c}$, so ist $\mathfrak{a}$ auch relatives Primideal zu dem Produkte $\mathfrak{b}\mathfrak{c}$.

Denn es gibt in $\mathfrak{b}, \mathfrak{c}$ Zahlen β, γ, welche den Bedingungen $\beta \equiv 1$, $\gamma \equiv 1 \pmod{\mathfrak{a}}$ genügen, und hieraus folgt, daß die in $\mathfrak{b}\mathfrak{c}$ enthaltene Zahl $\beta\gamma \equiv 1 \pmod{\mathfrak{a}}$ ist.

2. Ist jedes der Ideale $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3\ldots$ relatives Primideal zu jedem der Ideale $\mathfrak{b}_1, \mathfrak{b}_2\ldots$, so sind die Produkte $\mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3\ldots$ und $\mathfrak{b}_1\mathfrak{b}_2\ldots$ relative Primideale.

Der Beweis ergibt sich durch wiederholte Anwendung des vorhergehenden Satzes (vgl. § 5, 3.).

3. Sind $\mathfrak{a}, \mathfrak{b}$ relative Primideale, so ist $\mathfrak{a}\mathfrak{b}$ ihr kleinstes gemeinschaftliches Vielfaches, und $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$.

Denn bedeutet $\mathfrak{m}$ das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}, \mathfrak{b}$, so ist $\mathfrak{m}\mathfrak{o}$, also $\mathfrak{m}$ selbst teilbar durch $\mathfrak{a}\mathfrak{b}$ (nach § 170, 3.); da aber $\mathfrak{a}\mathfrak{b}$ (nach § 170, 2.) ein gemeinschaftliches Vielfaches von $\mathfrak{a}, \mathfrak{b}$, also durch $\mathfrak{m}$ teilbar ist, so ist $\mathfrak{m} = \mathfrak{a}\mathfrak{b}$; und hieraus folgt (nach § 169, 3.) der Satz über die Normen*).

4. Sind $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}\ldots$ relative Primideale, so ist ihr Produkt $\mathfrak{a}\mathfrak{b}\mathfrak{c}\ldots$ auch ihr kleinstes gemeinschaftliches Vielfaches, und zugleich ist $N(\mathfrak{a}\mathfrak{b}\mathfrak{c}\ldots) = N(\mathfrak{a})N(\mathfrak{b})N(\mathfrak{c})\ldots$.

*) Daß der letztere allgemein für je zwei beliebige Ideale $\mathfrak{a}, \mathfrak{b}$ gilt, kann erst später bewiesen werden (§ 173, 7.).

Der Beweis ergibt sich durch wiederholte Anwendung der vorhergehenden Sätze (vgl. § 7).

5. Sind $\mathfrak{a}, \mathfrak{b}$ relative Primideale, und ist $\mathfrak{bc}$ teilbar durch $\mathfrak{a}$, so geht $\mathfrak{a}$ in $\mathfrak{c}$ auf.

Denn es gibt in $\mathfrak{b}$ eine Zahl $\beta \equiv 1 \pmod{\mathfrak{a}}$; ist nun γ eine beliebige Zahl in $\mathfrak{c}$, so ist $\beta\gamma$ in $\mathfrak{bc}$, also auch in $\mathfrak{a}$ enthalten, woraus $\gamma \equiv \beta\gamma \equiv 0 \pmod{\mathfrak{a}}$ folgt, was zu beweisen war. —

Die bisher von uns entwickelten Sätze der Idealtheorie bieten eine augenscheinliche Analogie dar mit den Sätzen über die Teilbarkeit der ganzen rationalen Zahlen, und dies findet seinen natürlichen Grund darin, daß, wenn der Körper Ω vom Grade $n = 1$ ist, das Gebiet $\mathfrak{o} = [1]$ und jedes Ideal $\mathfrak{m}$ dieses Gebietes ein Modul $[m]$ ist, wo m irgendeine positive ganze rationale Zahl bedeutet (§ 165). Es liegt nun nahe, in die Theorie der Ideale auch einen Begriff einzuführen, welcher dem Begriffe der rationalen Primzahl entspricht. Das Ideal $\mathfrak{o}$ besitzt offenbar nur einen einzigen Teiler, nämlich $\mathfrak{o}$ selbst; jedes von $\mathfrak{o}$ verschiedene Ideal besitzt aber mindestens zwei verschiedene Teiler, da es außer durch $\mathfrak{o}$ auch noch durch sich selbst teilbar ist. Wir wollen nun ein Ideal $\mathfrak{p}$ ein Primideal nennen, wenn es von $\mathfrak{o}$ verschieden ist und keinen anderen Teiler als $\mathfrak{o}$ und $\mathfrak{p}$ besitzt; dagegen soll $\mathfrak{a}$ ein zusammengesetztes Ideal heißen, wenn es mindestens einen von $\mathfrak{a}$ und $\mathfrak{o}$ verschiedenen Teiler besitzt. Hieraus fließen die folgenden Sätze.

6. Ist $\mathfrak{a}$ von $\mathfrak{o}$ verschieden, so gibt es mindestens ein in $\mathfrak{a}$ aufgehendes Primideal.

Denn wählt man unter den von $\mathfrak{o}$ verschiedenen Teilern von $\mathfrak{a}$ ein solches Ideal $\mathfrak{p}$ aus, dessen Norm den möglich kleinsten Wert hat, so kann $\mathfrak{p}$ (nach § 169, 5.) keinen von $\mathfrak{o}$ und $\mathfrak{p}$ verschiedenen Teiler haben, und folglich ist $\mathfrak{p}$ ein in $\mathfrak{a}$ aufgehendes Primideal.

7. Zwei Ideale sind entweder relative Primideale, oder es gibt ein in beiden aufgehendes Primideal.

Denn ihr größter gemeinschaftlicher Teiler ist entweder $= \mathfrak{o}$, oder er ist (nach 6.) durch ein Primideal teilbar.

8. Ist $\mathfrak{p}$ ein Primideal, $\mathfrak{a}$ ein beliebiges Ideal, so findet einer und nur einer der folgenden beiden Fälle statt: entweder geht $\mathfrak{p}$ in $\mathfrak{a}$ auf, oder $\mathfrak{a}$ und $\mathfrak{p}$ sind relative Primideale.

Denn der größte gemeinschaftliche Teiler von $\mathfrak{a}, \mathfrak{p}$ ist ein Teiler von $\mathfrak{p}$, also entweder $= \mathfrak{p}$, oder $= \mathfrak{o}$.

9. Wenn ein Produkt von Idealen oder Zahlen durch das Primideal $\mathfrak{p}$ teilbar ist, so geht $\mathfrak{p}$ in mindestens einem der Faktoren auf.

Denn wenn $\mathfrak{p}$ in keinem der Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots$ aufgeht, so ist $\mathfrak{p}$ (nach 8.) relatives Primideal zu jedem derselben, also auch zu ihrem Produkte (nach 2.), welches folglich (nach 8.) nicht durch $\mathfrak{p}$ teilbar ist; und handelt es sich um ein Produkt aus Zahlen $\eta, \eta', \ldots$, so ergibt sich dasselbe, wenn man die entsprechenden Hauptideale $\mathfrak{o}\eta, \mathfrak{o}\eta', \ldots$ betrachtet.

10. Ist $\mathfrak{p}$ ein Primideal, so gibt es im Körper der rationalen Zahlen eine und nur eine positive Primzahl p, welche durch $\mathfrak{p}$ teilbar ist; zugleich ist $N(\mathfrak{p}) = p^f$, und der Exponent f soll der Grad des Primideals $\mathfrak{p}$ heißen.

Denn die durch $\mathfrak{p}$ teilbaren ganzen rationalen Zahlen, zu denen (nach § 169, 1.) auch $N(\mathfrak{p})$ gehört, bilden offenbar einen Modul, und wenn p die kleinste positive dieser Zahlen bedeutet, so ist dieser Modul $= [p]$ [nach § 165, (8)]; nun kann p nicht $= 1$ sein, weil sonst $\mathfrak{p} = \mathfrak{o}$ wäre (nach § 168, 1.), und p kann auch nicht ein Produkt aus zwei kleineren rationalen Zahlen sein, weil sonst eine von beiden (nach 9.) durch $\mathfrak{p}$ teilbar sein müßte, was gegen die Definition von p verstoßen würde; mithin ist p eine Primzahl im Körper der rationalen Zahlen, und es kann keine andere solche Primzahl durch $\mathfrak{p}$ teilbar sein, weil $[p]$ der Inbegriff aller durch $\mathfrak{p}$ teilbaren rationalen Zahlen ist. Da nun $\mathfrak{o}p$ durch $\mathfrak{p}$, und folglich $N(\mathfrak{o}p)$, d. h. p^n durch $N(\mathfrak{p})$ teilbar ist (§ 169, 5.), so folgt, daß $N(\mathfrak{p})$ selbst eine Potenz von p ist.

11. Ist $\mathfrak{a}$ ein zusammengesetztes Ideal, so gibt es zwei durch $\mathfrak{a}$ nicht teilbare Zahlen η, η', deren Produkt durch $\mathfrak{a}$ teilbar ist.

Denn $\mathfrak{a}$ besitzt einen von $\mathfrak{o}$ und $\mathfrak{a}$ verschiedenen Teiler $\mathfrak{e}$, und da derselbe nicht durch $\mathfrak{a}$ teilbar ist, so gibt es in $\mathfrak{e}$ eine durch $\mathfrak{a}$ nicht teilbare Zahl η; der größte gemeinschaftliche Teiler $\mathfrak{d}$ der beiden Ideale $\mathfrak{a}$ und $\mathfrak{o}\eta$ ist teilbar durch $\mathfrak{e}$, also von $\mathfrak{o}$ verschieden, und folglich ist $N(\mathfrak{d}) > 1$ (nach § 169, 2.). Nun sei $\mathfrak{a}'\eta$ das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$ und $\mathfrak{o}\eta$, so ist $\mathfrak{a}'$ ein Teiler von $\mathfrak{a}$, und zugleich ist (nach § 169, 4.) $N(\mathfrak{a}) = N(\mathfrak{a}')N(\mathfrak{d}) > N(\mathfrak{a}')$; mithin ist $\mathfrak{a}'$ ein echter Teiler von $\mathfrak{a}$, und es gibt folglich in $\mathfrak{a}'$ eine durch $\mathfrak{a}$ nicht teilbare Zahl η'; dann ist das Produkt $\eta\eta'$ in $\eta\mathfrak{a}'$ und folglich auch in $\mathfrak{a}$ enthalten, was zu beweisen war.

12. Ist $\mathfrak{a}$ teilbar durch das Primideal $\mathfrak{p}$, so kann man die Zahl ν so wählen, daß $\mathfrak{p}\nu$ das kleinste gemeinschaftliche Vielfache der beiden Ideale $\mathfrak{a}$ und $\mathfrak{o}\nu$ wird.

Der Beweis dieses einfachen, aber für unsere Theorie äußerst wichtigen Satzes*) ist mit einigen Schwierigkeiten verknüpft, die sich jedoch durch die folgende Kette von Schlüssen überwinden lassen. Zunächst leuchtet die Richtigkeit des Satzes ein, wenn $(\mathfrak{p}, \mathfrak{a}) = 1$, also $\mathfrak{a} = \mathfrak{p}$ ist, weil in diesem Falle die Zahl $\nu = 1$ die verlangte Eigenschaft besitzt. Es sei nun m irgendeine ganze rationale Zahl > 1, und wir wollen annehmen, der Satz sei schon für alle die Fälle bewiesen, in welchen $(\mathfrak{p}, \mathfrak{a}) < m$ ist, so brauchen wir offenbar nur noch zu zeigen, daß hieraus immer seine Richtigkeit auch für den Fall $(\mathfrak{p}, \mathfrak{a}) = m$ folgt. Zu diesem Zweck wollen wir wieder, wenn η eine von Null verschiedene Zahl ist, mit $\mathfrak{b}$ den größten gemeinschaftlichen Teiler, mit $\mathfrak{a}'\eta$ das kleinste gemeinschaftliche Vielfache der Ideale $\mathfrak{a}, \mathfrak{o}\eta$ bezeichnen; dann ist $\mathfrak{a}'$ ein Teiler von $\mathfrak{a}$, und zugleich ist $N(\mathfrak{a}) = N(\mathfrak{a}')N(\mathfrak{b})$. Ist nun $(\mathfrak{p}, \mathfrak{a}) = m > 1$, also $\mathfrak{p}$ ein echter Teiler von $\mathfrak{a}$, so wollen wir zunächst zeigen, daß man durch geeignete Wahl der Zahl η ein zugehöriges Ideal $\mathfrak{a}'$ erhalten kann, welches erstens durch $\mathfrak{p}$ teilbar und zweitens ein echter Teiler von $\mathfrak{a}$ ist; die letztere Forderung kommt offenbar darauf hinaus, daß $\mathfrak{b}$ von $\mathfrak{o}$ verschieden, also $N(\mathfrak{b}) > 1$, $N(\mathfrak{a}') < N(\mathfrak{a})$ werde. Um diesen Existenzbeweis zu führen, müssen wir zwei Fälle unterscheiden:

a) Wenn $\mathfrak{p}$ das einzige in $\mathfrak{a}$ aufgehende Primideal ist, so wähle man für η eine durch $\mathfrak{p}$, aber nicht durch $\mathfrak{a}$ teilbare Zahl, was stets möglich ist, weil $\mathfrak{p}$ ein echter Teiler von $\mathfrak{a}$, also nicht durch $\mathfrak{a}$ teilbar ist. Da nun $\mathfrak{o}\eta$, und folglich auch $\mathfrak{b}$ durch $\mathfrak{p}$ teilbar ist, so ist $N(\mathfrak{b}) > 1$, also $\mathfrak{a}'$ ein echter Teiler von $\mathfrak{a}$. Da ferner $\mathfrak{o}\eta$ nicht durch $\mathfrak{a}$ teilbar ist, so kann $\mathfrak{a}'$ nicht $= \mathfrak{o}$ sein, und folglich gibt es (nach 6.) ein in $\mathfrak{a}'$ aufgehendes Primideal $\mathfrak{q}$; da aber $\mathfrak{a}'$ ein Teiler von $\mathfrak{a}$ ist, so geht $\mathfrak{q}$ auch in $\mathfrak{a}$ auf und ist folglich $= \mathfrak{p}$; mithin ist $\mathfrak{a}'$ teilbar durch $\mathfrak{p}$, was zu zeigen war.

*) Derselbe läßt sich, ohne an Inhalt wesentlich zu gewinnen oder zu verlieren, in sehr verschiedenen Formen ausdrücken; so z. B. ergibt sich aus ihm ohne Zuziehung neuer Beweismittel der folgende Satz: Wenn $\mathfrak{a}$, $\mathfrak{b}$ nicht relative Primideale sind, so gibt es ein durch $\mathfrak{a}$ nicht teilbares Ideal $\mathfrak{c}$ von der Art, daß $\mathfrak{bc}$ durch $\mathfrak{a}$ teilbar wird (vgl. § 171, 5.). Umgekehrt folgt der obige Satz ebenso leicht aus diesem letzteren, der aber, trotz seiner scheinbaren Evidenz, schwerlich einen einfacheren direkten Beweis gestattet.

b) Wenn $\mathfrak{a}$ durch ein von $\mathfrak{p}$ verschiedenes Primideal $\mathfrak{q}$ teilbar ist, so wähle man für η eine durch $\mathfrak{q}$, aber nicht durch $\mathfrak{p}$ teilbare Zahl, was stets möglich ist, weil $\mathfrak{q}$ nicht durch $\mathfrak{p}$ teilbar ist. Da nun $\mathfrak{o}\eta$, und folglich auch $\mathfrak{b}$ durch $\mathfrak{q}$ teilbar ist, so ist $N(\mathfrak{b}) > 1$, also $\mathfrak{a}'$ ein echter Teiler von $\mathfrak{a}$. Da ferner $\mathfrak{a}'\eta$ durch $\mathfrak{a}$ und folglich auch durch $\mathfrak{p}$ teilbar ist, während $\mathfrak{p}$ in dem Faktor η nicht aufgeht, so ist (nach 9.) das Ideal $\mathfrak{a}'$ teilbar durch $\mathfrak{p}$, was zu zeigen war.

Hiermit ist die Existenz einer solchen Zahl η in allen Fällen nachgewiesen. Da nun das zugehörige Ideal $\mathfrak{a}'$ durch $\mathfrak{p}$ teilbar und zugleich ein echter Teiler von $\mathfrak{a}$ ist, so ist $m = (\mathfrak{p}, \mathfrak{a}) = (\mathfrak{p}, \mathfrak{a}')(\mathfrak{a}', \mathfrak{a})$, und $(\mathfrak{a}', \mathfrak{a}) > 1$, also $(\mathfrak{p}, \mathfrak{a}') < m$; mithin gibt es nach unserer obigen Annahme eine Zahl η' von der Art, daß $\mathfrak{p}\eta'$ das kleinste gemeinschaftliche Vielfache der Ideale $\mathfrak{a}', \mathfrak{o}\eta'$ ist, und da $\mathfrak{a}'\eta$ dasjenige der Ideale $\mathfrak{a}, \mathfrak{o}\eta$ ist, so folgt (nach § 168, 4.), daß $\mathfrak{p}\eta\eta'$ das kleinste gemeinschaftliche Vielfache der Ideale $\mathfrak{a}$ und $\mathfrak{o}\eta\eta'$ ist; mithin hat die Zahl $\nu = \eta\eta'$ die in unserem Satze verlangte Eigenschaft.

§ 172.

Man würde nun unsere bisherige Untersuchung auch ohne Zuziehung neuer Hilfsmittel noch einige Schritte weiterführen und z. B. den folgenden Satz beweisen können, in welchem unter einem einartigen Ideal ein solches verstanden wird, welches durch ein und nur durch ein einziges Primideal teilbar ist*):

13. Jedes von $\mathfrak{o}$ verschiedene Ideal $\mathfrak{a}$ ist entweder einartiges Ideal, oder es läßt sich, und zwar nur auf eine einzige Weise, als ein Produkt von lauter einartigen Idealen darstellen, die zugleich relative Primideale sind.

Es sei $\mathfrak{p}$ ein in $\mathfrak{a}$ aufgehendes Primideal, und $\mathfrak{p}'$ das kleinste gemeinschaftliche Vielfache aller in $\mathfrak{a}$ aufgehenden, durch $\mathfrak{p}$ teilbaren einartigen Ideale $\mathfrak{e}$, zu denen auch $\mathfrak{p}$ gehört, so ist $\mathfrak{p}'$ offenbar selbst eins der Ideale $\mathfrak{e}$; denn $\mathfrak{p}'$ geht in $\mathfrak{a}$ auf, weil $\mathfrak{a}$ ein gemeinschaftliches Vielfaches dieser Ideale $\mathfrak{e}$ ist, und $\mathfrak{p}'$ ist nur durch das einzige Primideal $\mathfrak{p}$ teilbar, weil selbst das durch $\mathfrak{p}'$ teilbare Produkt aller Ideale $\mathfrak{e}$ (nach 9.) durch kein von $\mathfrak{p}$ verschiedenes Primideal teilbar sein kann. Es sei ferner $\mathfrak{b}$ das kleinste gemeinschaftliche Vielfache aller der-

*) [Im Nachlaß fand sich das Manuskript der dritten Auflage, wobei die beiden Seiten mit dem Beweis dieses Satzes die Überschrift trugen: „Für die dritte Auflage kassiert, doch wichtig.“ Der Beweis soll hier eingeschaltet werden, als erstes explizites Beispiel eines Zerlegungssatzes der allgemeinen Idealtheorie. E. N.]

jenigen in $\mathfrak{a}$ aufgehenden Ideale $\mathfrak{q}$, welche, wie z. B. $\mathfrak{o}$, nicht durch $\mathfrak{p}$ teilbar sind, so ergibt sich auf dieselbe Weise, daß $\mathfrak{b}$ selbst eins dieser Ideale $\mathfrak{q}$ ist. Offenbar sind $\mathfrak{p}'$ und $\mathfrak{b}$ relative Primideale. Wir wollen uns nun begnügen, zu beweisen, daß $\mathfrak{a} = \mathfrak{p}'\mathfrak{b}$ ist, weil der Leser hieraus alles Übrige mit Hilfe der früheren Sätze leicht ableiten wird. Man wähle nach Belieben eine durch $\mathfrak{b}$, aber nicht durch $\mathfrak{p}$ teilbare Zahl η (was möglich ist, weil $\mathfrak{b}$ nicht durch $\mathfrak{p}$ teilbar ist), so wird $\mathfrak{b}$ immer der größte gemeinschaftliche Teiler von $\mathfrak{a}$ und $\mathfrak{o}\eta$ sein; denn jeder gemeinschaftliche Teiler dieser Ideale ist offenbar eins der Ideale $\mathfrak{q}$, mithin ein Teiler von $\mathfrak{b}$, und außerdem ist $\mathfrak{b}$ selbst ein solcher gemeinschaftlicher Teiler. Es sei nun $\mathfrak{r}\eta$ das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$ und $\mathfrak{o}\eta$, so ist $\mathfrak{r}$ ein Teiler von $\mathfrak{a}$ und (nach § 169, 4.)

$$N(\mathfrak{a}) = N(\mathfrak{r}) \cdot N(\mathfrak{b}).$$

Die Zahl η^2 ist ebenfalls, wie η, durch $\mathfrak{b}$, aber nicht durch $\mathfrak{p}$ teilbar, mithin haben die beiden Ideale $\mathfrak{a}$, $\mathfrak{o}\eta^2$ denselben größten gemeinschaftlichen Teiler $\mathfrak{b}$ wie die Ideale $\mathfrak{a}$, $\mathfrak{o}\eta$; hieraus folgt (nach § 168, 4.), daß $\mathfrak{r}\eta^2$ das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$, $\mathfrak{o}\eta^2$, mithin $\mathfrak{r}\eta$ dasjenige der Ideale $\mathfrak{r}$, $\mathfrak{o}\eta$ ist; bedeutet aber $\mathfrak{b}'$ den größten gemeinschaftlichen Teiler dieser beiden Ideale, so ist (nach § 169, 4.) $N(\mathfrak{r}) = N(\mathfrak{r})N(\mathfrak{b}')$, also $N(\mathfrak{b}') = 1$, $\mathfrak{b}' = \mathfrak{o}$. Es ist daher $\mathfrak{r}$ relatives Primideal zu dem Hauptideal $\mathfrak{o}\eta$ und folglich auch zu dessen Teiler $\mathfrak{b}$; mithin ist $\mathfrak{r}\mathfrak{b}$ (nach 3.) das kleinste gemeinschaftliche Vielfache von $\mathfrak{r}$ und $\mathfrak{b}$, und $N(\mathfrak{r}\mathfrak{b}) = N(\mathfrak{r}) \cdot N(\mathfrak{b})$, also $N(\mathfrak{r}\mathfrak{b}) = N(\mathfrak{a})$; da aber $\mathfrak{a}$ ein gemeinschaftliches Vielfaches von $\mathfrak{r}$ und $\mathfrak{b}$, mithin durch $\mathfrak{r}\mathfrak{b}$ teilbar ist, so folgt aus der Gleichheit der Normen (nach § 169, 5.), daß

$$\mathfrak{a} = \mathfrak{r}\mathfrak{b}$$

ist. Wir haben nun noch zu zeigen, daß $\mathfrak{r} = \mathfrak{p}'$ ist; zunächst leuchtet ein, daß das Ideal $\mathfrak{p}'$, weil es in $\mathfrak{r}\mathfrak{b}$ aufgeht, zugleich aber relatives Primideal zu $\mathfrak{b}$ ist, in $\mathfrak{r}$ aufgehen muß; wäre ferner $\mathfrak{r}$ durch ein von $\mathfrak{p}$ verschiedenes Primideal teilbar, so müßte letzteres auch in $\mathfrak{a}$ aufgehen, es wäre folglich eins der Ideale $\mathfrak{q}$ und ginge folglich in $\mathfrak{b}$ auf, was nicht möglich ist, weil $\mathfrak{r}$ und $\mathfrak{b}$ relative Primideale sind; hieraus folgt offenbar, daß $\mathfrak{r}$ eins der Ideale $\mathfrak{e}$ ist und daher in $\mathfrak{p}'$ aufgeht. Also ist $\mathfrak{r} = \mathfrak{p}'$, was wir zeigen wollten.

Indessen ist dieser Satz, den wir später (§ 173, 4.) doch durch einen noch schärferen zu ersetzen haben werden, für unsere Zwecke nicht erforderlich, und wir haben ihn nur erwähnt, um zu zeigen,

wie weit man mit den bisherigen Beweismitteln gelangen kann. Bei einer sorgfältigen Prüfung der letzteren und der durch sie gewonnenen Resultate ergibt sich nun folgendes.

So augenfällig auch die Analogie zwischen den vorhergehenden Sätzen und denjenigen über die Teilbarkeit der ganzen rationalen Zahlen ist, so kann dieselbe bis jetzt doch keineswegs eine vollständige genannt werden. Man darf nicht vergessen, daß die Teilbarkeit eines Ideals $\mathfrak{c}$ durch ein Ideal $\mathfrak{a}$ nach unserer Definition (§§ 165, 168) lediglich darin besteht, daß alle Zahlen des Ideals $\mathfrak{c}$ auch in $\mathfrak{a}$ enthalten sind; nun ergab sich zwar sehr leicht (§ 170, 2.), daß jedes Produkt aus $\mathfrak{a}$ und einem beliebigen Ideal $\mathfrak{b}$ stets durch $\mathfrak{a}$ teilbar ist, aber es ist keineswegs leicht zu beweisen, daß umgekehrt jedes durch $\mathfrak{a}$ teilbare Ideal $\mathfrak{c}$ auch ein Produkt aus $\mathfrak{a}$ und einem Ideal $\mathfrak{b}$ ist. Diese Schwierigkeit läßt sich auch mit den bisher von uns gebrauchten Beweismitteln allein durchaus nicht überwinden, und wir müssen den Grund dieser Tatsache hier etwas näher erörtern, weil dieselbe mit einer sehr wichtigen Verallgemeinerung der Theorie zusammenhängt. Bei einer genauen Prüfung der bisher entwickelten Theorie wird man sich leicht davon überzeugen, daß alle Definitionen einen bestimmten Sinn und die Beweise aller Sätze ihre volle Kraft behalten, auch wenn nicht vorausgesetzt wird, daß das mit $\mathfrak{o}$ bezeichnete Gebiet alle ganzen Zahlen des Körpers Ω umfaßt. Die wirklich benutzten Eigenschaften des Systems $\mathfrak{o}$ kommen vielmehr auf die folgenden zurück:

a) Das System $\mathfrak{o}$ ist ein endlicher Modul $[\omega_1, \omega_2, \ldots, \omega_n]$, dessen Basis zugleich eine Basis des Körpers Ω bildet (§ 162).

b) Jedes Produkt aus zwei Zahlen des Systems $\mathfrak{o}$ gehört demselben System $\mathfrak{o}$ an.

c) Die Zahl 1 ist in $\mathfrak{o}$ enthalten.

Ein Gebiet $\mathfrak{o}$, welches diese drei Eigenschaften besitzt, wollen wir eine Ordnung nennen. Aus der Verbindung von a) und b) folgt unmittelbar, daß eine Ordnung $\mathfrak{o}$ nur aus ganzen Zahlen des Körpers Ω besteht, und zufolge c) sind auch alle ganzen rationalen Zahlen in $\mathfrak{o}$ enthalten; aber hieraus folgt noch nicht (ausgenommen im Fall $n = 1$), daß $\mathfrak{o}$ alle ganzen Zahlen des Körpers Ω enthält. Nennt man nun eine Zahl α der Ordnung $\mathfrak{o}$ nur dann teilbar durch eine zweite solche Zahl μ, wenn $\alpha = \mu\nu$ ist, wo ν ebenfalls eine Zahl

in $\mathfrak{o}$ bedeutet (vgl. § 167), und modifiziert man in derselben Weise den Begriff der Kongruenz der Zahlen innerhalb des Gebietes $\mathfrak{o}$, so leuchtet unmittelbar ein, daß die Anzahl $(\mathfrak{o}, \mathfrak{o}\mu)$ der in bezug auf μ inkongruenten Zahlen der Ordnung $\mathfrak{o}$ auch jetzt $= \pm N(\mu)$ ist [§ 167, (9)], und ebenso leicht wird man erkennen, daß alle später entwickelten Begriffe und Sätze ihren Sinn und ihre Geltung behalten, wenn unter einer Zahl stets eine Zahl dieser Ordnung $\mathfrak{o}$ verstanden wird. In jeder Ordnung $\mathfrak{o}$ des Körpers Ω existiert daher eine besondere Theorie der Ideale, und diese Theorie ist für alle Ordnungen eine gemeinsame, soweit sie im vorhergehenden entwickelt ist. Aber während die Theorie der Ideale in derjenigen Ordnung $\mathfrak{o}$, welche aus allen ganzen Zahlen des Körpers Ω besteht, schließlich (§ 173) zu allgemeinen Gesetzen führen wird, welche keine Ausnahme erleiden und vollständig mit den Gesetzen der Teilbarkeit der rationalen Zahlen übereinstimmen, so ist die Theorie der Ideale jeder anderen Ordnung nicht von gleicher Einfachheit, insofern eine (immer endliche) Anzahl von Primidealen existiert, aus welchen sich die zugehörigen einartigen Ideale nicht alle durch Potenzierung bilden lassen. Diese allgemeinste Theorie der Ideale jeder Ordnung, deren Entwicklung für die Ziele der Zahlentheorie ebenfalls unerläßlich ist, und welche für den Fall $n = 2$ mit der Theorie der verschiedenen Ordnungen der binären quadratischen Formen zusammenfällt (§ 61), soll aber im folgenden von unserer Betrachtung gänzlich ausgeschlossen bleiben*), und wir wollen uns begnügen, an einem Beispiel auf den Charakter der oben erwähnten Ausnahmen aufmerksam zu machen.

Das Gebiet $\mathfrak{o}$ aller ganzen Zahlen desjenigen quadratischen Körpers, dessen Grundzahl $= -3$, ist $= [1, \theta]$, wo θ eine Wurzel der Gleichung $\theta^2 + \theta + 1 = 0$ bedeutet (§ 166). Das System $\mathfrak{o}' = [1, 2\theta] = [1, \sqrt{-3}]$ ist eine Ordnung, welche nicht alle ganzen Zahlen des Körpers enthält, weil $(\mathfrak{o}, \mathfrak{o}') = 2$ ist (§ 165); die durch $\mathfrak{o}'$ teilbaren Moduln $\mathfrak{p}' = [2, 2\theta] = \mathfrak{o}(2)$ und $\mathfrak{o}'(2) = [2, 4\theta]$ sind Ideale dieser Ordnung $\mathfrak{o}'$ (insofern sie die Eigenschaften I. und II. besitzen); aber obgleich $\mathfrak{o}'(2)$ durch $\mathfrak{p}'$ teilbar ist, so existiert in $\mathfrak{o}'$ doch kein Ideal $\mathfrak{q}'$ von der Art, daß $\mathfrak{p}'\mathfrak{q}' = \mathfrak{o}'(2)$ würde. —

*) In einem gewissen Umfange ist diese Theorie behandelt in des Herausgebers Abhandlung: Über die Anzahl der Ideal-Klassen in den verschiedenen Ordnungen eines endlichen Körpers (Braunschweig 1877).

Um nun die Theorie der Ideale in derjenigen Ordnung $\mathfrak{o}$, welche alle ganzen Zahlen des Körpers Ω umfaßt, zum vollständigen Abschlusse zu bringen, bedürfen wir der folgenden Hilfssätze:

1. Ist μ eine von Null verschiedene ganze, und φ eine gebrochene, d. h. nicht ganze Zahl des Körpers Ω*), so sind alle Glieder der geometrischen Reihe

$$\mu,\ \mu\varphi,\ \mu\varphi^2,\ \ldots,\ \mu\varphi^e,\ \mu\varphi^{e+1},\ \ldots$$

bis zu einem in endlicher Entfernung liegenden Gliede $\mu\varphi^e$ ganze Zahlen, und alle folgenden Glieder sind gebrochene Zahlen.

Zum Beweise bemerken wir zunächst, daß alle Glieder der Reihe in Ω enthalten sind, und daß das Anfangsglied eine ganze Zahl ist. Bedeutet nun m den absoluten Wert von $N(\mu)$, so können höchstens m Glieder ganze Zahlen, also in $\mathfrak{o}$ enthalten sein; wären nämlich mindestens $(m+1)$ Glieder ganze Zahlen, so müßten unter ihnen [nach § 167, (9)] mindestens zwei verschiedene einander kongruent sein nach dem Modul μ; bezeichnet man dieselben mit $\mu\varphi^s$ und $\mu\varphi^r$, wo $r > s$, so wäre $\mu\varphi^r \equiv \mu\varphi^s \pmod{\mu}$, und folglich würde die gebrochene Zahl φ einer Gleichung r^{ten} Grades von der Form

$$\varphi^r - \varphi^s - \omega = 0$$

genügen, wo ω eine ganze Zahl, was (nach § 160, 2.) unmöglich ist. Von einer bestimmten Stelle ab werden daher alle Glieder der Reihe gewiß gebrochene Zahlen sein; ist nun

$$\mu\varphi^e = \varkappa$$

die letzte in der Reihe auftretende ganze Zahl, so ist e ein endlicher Exponent $\geqq 0$; ist $e > 0$, so sind alle vorhergehenden Glieder ebenfalls ganze Zahlen; denn wenn $r < e$, so ist

$$(\mu\varphi^r)^e = \mu^{e-r}\varkappa^r$$

eine ganze Zahl, und hieraus folgt (nach § 160, 2.), daß auch $\mu\varphi^r$ eine ganze Zahl ist, was zu beweisen war.

2. Sind μ, ν zwei von Null verschiedene Zahlen in $\mathfrak{o}$, und ist ν nicht teilbar durch μ, so gibt es in $\mathfrak{o}$ immer zwei von Null verschiedene Zahlen $\varkappa, \lambda$ von der Art, daß $\varkappa\mu = \lambda\nu$, und daß $\varkappa^2$ nicht durch λ teilbar ist.

*) Da, wenn μ, φ irgendwelche algebraische Zahlen sind, sich immer leicht die Existenz eines endlichen Körpers Ω nachweisen läßt, welchem beide Zahlen angehören, so gilt der obige Satz allgemein, und ebenso der folgende Satz.

Dies folgt unmittelbar aus dem vorhergehenden Satze; denn wenn man $\nu = \mu\varphi$ setzt, so ist φ eine gebrochene Zahl des Körpers Ω, und von den Gliedern der Reihe

$$\mu,\ \mu\varphi,\ \mu\varphi^2,\ \ldots$$

sind die beiden ersten in $\mathfrak{o}$ enthalten; bezeichnet man nun (wie in 1.) die beiden letzten Glieder der Reihe, welche ganze Zahlen, also in $\mathfrak{o}$ enthalten sind, mit

$$\lambda = \mu\varphi^{e-1},\quad \varkappa = \mu\varphi^e,$$

so ist offenbar $\varkappa\mu = \lambda\nu$, und da das nächstfolgende Glied

$$\mu\varphi^{e+1} = \frac{\varkappa^2}{\lambda}$$

eine gebrochene Zahl ist, so kann $\varkappa^2$ nicht durch λ teilbar sein, was zu beweisen war.

§ 173.

Mit Hilfe dieser Sätze ist es leicht, die Theorie der Ideale unseres Gebietes $\mathfrak{o}$ zu dem gewünschten Abschluß zu bringen; dies geschieht durch die folgende Reihe von Sätzen.

1. Ist $\mathfrak{p}$ ein Primideal, so gibt es eine durch $\mathfrak{p}$ teilbare Zahl λ und eine durch $\mathfrak{p}$ nicht teilbare Zahl $\varkappa$ von der Art, daß $\mathfrak{p}\varkappa$ das kleinste gemeinschaftliche Vielfache der Ideale $\mathfrak{o}\lambda$ und $\mathfrak{o}\varkappa$ ist.

Denn es sei μ eine beliebige, aber von Null verschiedene Zahl in $\mathfrak{p}$, so gibt es, weil $\mathfrak{o}\mu$ durch $\mathfrak{p}$ teilbar ist, eine Zahl ν von der Art, daß $\mathfrak{p}\nu$ das kleinste gemeinschaftliche Vielfache der Ideale $\mathfrak{o}\mu$ und $\mathfrak{o}\nu$ wird (§ 171, 12.); diese Zahl ν kann nicht durch μ teilbar sein, weil sonst $\mathfrak{o}\nu$, und nicht $\mathfrak{p}\nu$ das kleinste gemeinschaftliche Vielfache von $\mathfrak{o}\mu$ und $\mathfrak{o}\nu$ wäre. Man kann daher (nach § 172, 2.) die beiden Zahlen $\varkappa, \lambda$ so wählen, daß $\varkappa\mu = \lambda\nu$, und $\varkappa^2$ nicht durch λ teilbar wird; dann ist (nach § 165) $\mathfrak{p}\nu\varkappa$ das kleinste gemeinschaftliche Vielfache von $\mathfrak{o}\mu\varkappa$ und $\mathfrak{o}\nu\varkappa$, und da das erste dieser beiden Ideale $= \mathfrak{o}\lambda\nu$ ist, so folgt durch Division mit ν (nach § 165), daß $\mathfrak{p}\varkappa$ das kleinste gemeinschaftliche Vielfache von $\mathfrak{o}\lambda$ und $\mathfrak{o}\varkappa$ ist; mithin ist $\mathfrak{p}$ ein Teiler von $\mathfrak{o}\lambda$ (nach § 168, 4.), d. h. λ ist teilbar durch $\mathfrak{p}$; aber $\varkappa$ ist nicht teilbar durch $\mathfrak{p}$, weil sonst $\varkappa^2$ durch $\mathfrak{p}\varkappa$, also auch durch λ teilbar wäre, was nicht der Fall ist.

2. Jedes Primideal $\mathfrak{p}$ kann durch Multiplikation mit einem geeignet gewählten Ideal $\mathfrak{b}$ in ein Hauptideal $\mathfrak{o}\lambda = \mathfrak{p}\mathfrak{b}$ verwandelt werden.

Denn behalten $\varkappa$, λ dieselbe Bedeutung wie im vorhergehenden Satze, und bezeichnet man mit $\mathfrak{b}$ den größten gemeinschaftlichen Teiler von $\mathfrak{o}\lambda$, $\mathfrak{o}\varkappa$, so ist (nach § 170, 3.) das Produkt $\mathfrak{p}\varkappa\mathfrak{b}$ durch das Produkt $\mathfrak{o}\lambda\varkappa$, und folglich $\mathfrak{p}\mathfrak{b}$ durch $\mathfrak{o}\lambda$ teilbar (§ 165). Da aber $\varkappa$ nicht durch $\mathfrak{p}$ teilbar ist, so ist $\mathfrak{p}$ (nach § 171, 8.) relatives Primideal zu dem Ideal $\mathfrak{o}\varkappa$ und folglich auch zu dessen Teiler $\mathfrak{b}$, mithin ist (nach § 171, 3.) $\mathfrak{p}\mathfrak{b}$ das kleinste gemeinschaftliche Vielfache von $\mathfrak{p}$ und $\mathfrak{b}$, und da λ durch diese beiden Ideale teilbar ist, so muß $\mathfrak{o}\lambda$ auch durch $\mathfrak{p}\mathfrak{b}$ teilbar sein. Mithin ist $\mathfrak{p}\mathfrak{b} = \mathfrak{o}\lambda$, was zu beweisen war.

3. Ist das Ideal $\mathfrak{a}$ teilbar durch das Primideal $\mathfrak{p}$, so gibt es ein und nur ein Ideal $\mathfrak{q}$ von der Art, daß $\mathfrak{p}\mathfrak{q} = \mathfrak{a}$ wird; dieses Ideal $\mathfrak{q}$ ist ein echter Teiler von $\mathfrak{a}$, und folglich ist $N(\mathfrak{q}) < N(\mathfrak{a})$.

Denn wählt man (nach 2.) ein Ideal $\mathfrak{b}$ so, daß $\mathfrak{p}\mathfrak{b} = \mathfrak{o}\lambda$ wird, so muß $\mathfrak{a}\mathfrak{b}$ (nach § 170, 1.) durch $\mathfrak{p}\mathfrak{b}$, also durch λ teilbar sein, weil $\mathfrak{a}$ durch $\mathfrak{p}$ teilbar ist, und folglich ist $\mathfrak{a}\mathfrak{b} = \lambda\mathfrak{q}$, wo $\mathfrak{q}$ ein bestimmtes Ideal bedeutet (§ 168). Multipliziert man diese Gleichung mit $\mathfrak{p}$, so ergibt sich $\lambda\mathfrak{a} = \lambda\mathfrak{p}\mathfrak{q}$, also $\mathfrak{a} = \mathfrak{p}\mathfrak{q}$. Genügt nun das Ideal $\mathfrak{r}$ ebenfalls der Bedingung $\mathfrak{p}\mathfrak{r} = \mathfrak{a}$, so ist $\mathfrak{p}\mathfrak{r} = \mathfrak{p}\mathfrak{q}$; durch Multiplikation mit $\mathfrak{b}$ folgt hieraus $\lambda\mathfrak{r} = \lambda\mathfrak{q}$, also ist $\mathfrak{r} = \mathfrak{q}$ (§ 165). Man kann ferner (nach § 171, 12.) die Zahl ν so wählen, daß $\mathfrak{p}\nu$ das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$ und $\mathfrak{o}\nu$ wird; da nun $\mathfrak{p}\nu$ durch $\mathfrak{a}$, also durch $\mathfrak{p}\mathfrak{q}$ teilbar ist, so ergibt sich (nach § 170, 1.) durch Multiplikation mit $\mathfrak{b}$, daß $\lambda\nu$ durch $\lambda\mathfrak{q}$, also die Zahl ν durch $\mathfrak{q}$ teilbar ist; aber ν ist gewiß nicht teilbar durch $\mathfrak{a}$, weil sonst $\mathfrak{o}\nu$, und nicht $\mathfrak{p}\nu$, das kleinste gemeinschaftliche Vielfache von $\mathfrak{a}$ und $\mathfrak{o}\nu$ wäre. Da also ν teilbar durch $\mathfrak{q}$, aber nicht teilbar durch $\mathfrak{a}$ ist, so ist das Ideal $\mathfrak{q}$, welches offenbar in $\mathfrak{a}$ aufgeht, verschieden von $\mathfrak{a}$, also ein echter Teiler von $\mathfrak{a}$, was zu beweisen war.

4. Jedes von $\mathfrak{o}$ verschiedene Ideal $\mathfrak{a}$ ist entweder ein Primideal, oder es läßt sich, und zwar nur auf eine einzige Weise, als Produkt von lauter Primidealen darstellen.

Da $\mathfrak{a}$ von $\mathfrak{o}$ verschieden ist, so gibt es (nach § 171, 6.) ein in $\mathfrak{a}$ aufgehendes Primideal $\mathfrak{p}_1$, und folglich kann man (nach 3.) $\mathfrak{a} = \mathfrak{p}_1\mathfrak{a}_1$ setzen, wo $N(\mathfrak{a}_1) < N(\mathfrak{a})$ ist. Wenn $N(\mathfrak{a}_1) = 1$, also $\mathfrak{a}_1 = \mathfrak{o}$ ist, so ergibt sich $\mathfrak{a} = \mathfrak{p}_1$; ist aber $N(\mathfrak{a}_1) > 1$, also $\mathfrak{a}_1$ von $\mathfrak{o}$ verschieden, so kann man wieder $\mathfrak{a}_1 = \mathfrak{p}_2\mathfrak{a}_2$ setzen, wo $\mathfrak{p}_2$ ein Primideal und $N(\mathfrak{a}_2) < N(\mathfrak{a}_1)$ ist. Wenn $N(\mathfrak{a}_2) > 1$ ist, so kann man in derselben

Weise fortfahren, bis unter den Idealen $\mathfrak{a}_1, \mathfrak{a}_2, \ldots$ das Ideal $\mathfrak{o} = \mathfrak{a}_r$ auftritt, was nach einer endlichen Anzahl von Zerlegungen geschehen muß, weil die Normen dieser Ideale immer kleiner werden. Auf diese Weise erhält man

$$\mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_r,$$

wo $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ sämtlich Primideale sind. Ist nun zugleich

$$\mathfrak{a} = \mathfrak{q}_1 \mathfrak{q}_2 \ldots \mathfrak{q}_s,$$

wo $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_s$ ebenfalls Primideale bedeuten, so geht $\mathfrak{q}_1$ in $\mathfrak{a}$, also in dem Produkte der r Ideale $\mathfrak{p}$, und folglich (nach § 171, 9.) auch in einem der Faktoren $\mathfrak{p}$, z. B. in $\mathfrak{p}_1$ auf; da aber $\mathfrak{p}_1$ als Primideal keinen anderen Teiler als $\mathfrak{o}$ und $\mathfrak{p}_1$ besitzt, so muß $\mathfrak{q}_1 = \mathfrak{p}_1$ sein. Es ist daher

$$\mathfrak{p}_1 (\mathfrak{p}_2 \ldots \mathfrak{p}_r) = \mathfrak{p}_1 (\mathfrak{q}_2 \ldots \mathfrak{q}_s),$$

und hieraus folgt (nach 3.)

$$\mathfrak{p}_2 \ldots \mathfrak{p}_r = \mathfrak{q}_2 \ldots \mathfrak{q}_s.$$

Offenbar kann man in derselben Weise fortfahren (vgl. § 8), und man gelangt so zu dem Resultat, daß jedes Primideal, welches in dem einen Produkte einmal oder öfter als Faktor auftritt, genau ebenso oft in dem anderen Produkte als Faktor auftreten muß.

5. Jedes Ideal $\mathfrak{a}$ kann durch Multiplikation mit einem passend gewählten Ideal $\mathfrak{m}$ in ein Hauptideal $\mathfrak{a}\mathfrak{m} = \mathfrak{o}\mu$ verwandelt werden.

Denn man setze $\mathfrak{a}$ (nach 4.) in die Form $\mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_r$, so lassen sich die Primideale $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ (nach 2.) durch Multiplikation in Hauptideale $\mathfrak{p}_1 \mathfrak{b}_1 = \mathfrak{o}\lambda_1$, $\mathfrak{p}_2 \mathfrak{b}_2 = \mathfrak{o}\lambda_2 \ldots \mathfrak{p}_r \mathfrak{b}_r = \mathfrak{o}\lambda_r$ verwandeln; setzt man nun $\mathfrak{b}_1 \mathfrak{b}_2 \ldots \mathfrak{b}_r = \mathfrak{m}$, $\lambda_1 \lambda_2 \ldots \lambda_r = \mu$, so wird $\mathfrak{a}\mathfrak{m} = \mathfrak{o}\mu$, was zu beweisen war.

6. Ist das Ideal $\mathfrak{c}$ teilbar durch das Ideal $\mathfrak{a}$, so gibt es ein und nur ein Ideal $\mathfrak{b}$, welches der Bedingung $\mathfrak{a}\mathfrak{b} = \mathfrak{c}$ genügt. — Ist $\mathfrak{a}\mathfrak{b}$ teilbar durch $\mathfrak{a}\mathfrak{b}'$, so ist $\mathfrak{b}$ teilbar durch $\mathfrak{b}'$, und aus $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{b}'$ folgt $\mathfrak{b} = \mathfrak{b}'$.

Denn wenn $\mathfrak{c}$ durch $\mathfrak{a}$ teilbar, und $\mathfrak{m}$ ein beliebiges Ideal ist, so ist (nach § 170, 1.) $\mathfrak{c}\mathfrak{m}$ teilbar durch $\mathfrak{a}\mathfrak{m}$; wählt man daher (nach 5.) das Ideal $\mathfrak{m}$ so, daß $\mathfrak{a}\mathfrak{m}$ ein Hauptideal $\mathfrak{o}\mu$ wird, so ist (nach § 168) $\mathfrak{c}\mathfrak{m} = \mathfrak{b}\mu$, wo $\mathfrak{b}$ ein bestimmtes Ideal bedeutet; hieraus folgt, wenn man mit $\mathfrak{a}$ multipliziert, $\mathfrak{c}\mu = \mathfrak{a}\mathfrak{b}\mu$, also $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$. — Sind ferner $\mathfrak{a}, \mathfrak{b}, \mathfrak{b}'$ beliebige Ideale, und nehmen wir an, es sei $\mathfrak{a}\mathfrak{b}$ teilbar durch $\mathfrak{a}\mathfrak{b}'$, so folgt durch Multiplikation mit $\mathfrak{m}$, daß $\mathfrak{b}\mu$ durch $\mathfrak{b}'\mu$, also $\mathfrak{b}$ durch $\mathfrak{b}'$ teilbar ist. Und wenn $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{b}'$ ist, so muß jedes

der Ideale $\mathfrak{b}, \mathfrak{b}'$ durch das andere teilbar, folglich $\mathfrak{b} = \mathfrak{b}'$ sein, was zu beweisen war.

7. Sind $\mathfrak{a}, \mathfrak{b}$ beliebige Ideale, so ist $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$, und folglich $(\mathfrak{a}, \mathfrak{a}\mathfrak{b}) = N(\mathfrak{b})$.

Wir betrachten zunächst ein Produkt $\mathfrak{a} = \mathfrak{p}\mathfrak{q}$, dessen einer Faktor $\mathfrak{p}$ ein Primideal ist. Dann ist der andere Faktor $\mathfrak{q}$ ein echter Teiler von $\mathfrak{a}$, weil sonst $\mathfrak{q} = \mathfrak{a}$, und folglich (nach 6.) $\mathfrak{p} = \mathfrak{o}$ wäre, und es gibt daher in $\mathfrak{q}$ eine durch $\mathfrak{a}$ nicht teilbare Zahl η; bezeichnen wir nun (wie in § 169, 4.) mit $\mathfrak{a}'\eta$ das kleinste gemeinschaftliche Vielfache, mit $\mathfrak{d}$ den größten gemeinschaftlichen Teiler der beiden Ideale $\mathfrak{a}$ und $\mathfrak{o}\eta$, so ist $N(\mathfrak{a}) = N(\mathfrak{a}')N(\mathfrak{d})$, und hieraus folgt

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

weil, wie wir zugleich zeigen wollen, $\mathfrak{a}' = \mathfrak{p}$ und $\mathfrak{d} = \mathfrak{q}$ ist. In der Tat, da η durch $\mathfrak{q}$, also $\mathfrak{p}\eta$ (nach § 170, 1.) durch $\mathfrak{p}\mathfrak{q}$ teilbar ist, so ist $\mathfrak{p}\eta$ ein gemeinschaftliches Vielfaches von $\mathfrak{a}$ und $\mathfrak{o}\eta$, mithin teilbar durch $\mathfrak{a}'\eta$, woraus folgt, daß $\mathfrak{a}'$ in $\mathfrak{p}$ aufgehen, also $= \mathfrak{o}$ oder $= \mathfrak{p}$ sein muß; das erstere ist aber unmöglich, weil $\mathfrak{o}\eta$ nicht durch $\mathfrak{a}$ teilbar ist; also ist $\mathfrak{a}' = \mathfrak{p}$. Da ferner $\mathfrak{q}$ ein gemeinschaftlicher Teiler von $\mathfrak{a}$ und $\mathfrak{o}\eta$ ist und folglich in $\mathfrak{d}$ aufgeht, so kann man (nach 6.) $\mathfrak{d} = \mathfrak{e}\mathfrak{q}$ setzen, und da dieses Ideal $\mathfrak{d}$ in $\mathfrak{a} = \mathfrak{p}\mathfrak{q}$ aufgeht, so muß (nach 6.) das Ideal $\mathfrak{e}$ in $\mathfrak{p}$ aufgehen, also $= \mathfrak{o}$ oder $= \mathfrak{p}$ sein, woraus entsprechend $\mathfrak{d} = \mathfrak{q}$, oder $\mathfrak{d} = \mathfrak{p}\mathfrak{q} = \mathfrak{a}$ folgt; das letztere ist aber unmöglich, weil η nicht durch $\mathfrak{a}$ teilbar ist; also ist $\mathfrak{d} = \mathfrak{q}$, wie behauptet war. Nachdem hiermit unser Satz für den Fall bewiesen ist, daß einer der Faktoren ein Primideal ist, ergibt sich seine Allgemeingültigkeit leicht wie folgt. Da (nach 4.) jedes von $\mathfrak{o}$ verschiedene Ideal

$$\mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3 \ldots \mathfrak{p}_r$$

gesetzt werden darf, wo $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ Primideale bedeuten, so folgt aus dem eben Bewiesenen, daß

$$N(\mathfrak{a}) = N(\mathfrak{p}_1)N(\mathfrak{p}_2 \mathfrak{p}_3 \ldots \mathfrak{p}_r) = N(\mathfrak{p}_1)N(\mathfrak{p}_2)N(\mathfrak{p}_3 \ldots \mathfrak{p}_r),$$

also

$$N(\mathfrak{a}) = N(\mathfrak{p}_1)N(\mathfrak{p}_2)N(\mathfrak{p}_3) \ldots N(\mathfrak{p}_r)$$

ist. Setzt man nun, wenn $\mathfrak{b}$ ein zweites Ideal ist,

$$\mathfrak{b} = \mathfrak{q}_1 \mathfrak{q}_2 \ldots \mathfrak{q}_s,$$

so folgt ebenso

$$N(\mathfrak{b}) = N(\mathfrak{q}_1)N(\mathfrak{q}_2) \ldots N(\mathfrak{q}_s);$$

zugleich ist aber

$$\mathfrak{a}\mathfrak{b} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\dots\mathfrak{p}_r\mathfrak{q}_1\mathfrak{q}_2\dots\mathfrak{q}_s,$$

also

$$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{p}_1)N(\mathfrak{p}_2)\dots N(\mathfrak{p}_r)N(\mathfrak{q}_1)\dots N(\mathfrak{q}_s),$$

mithin wirklich $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$, was zu beweisen war.

8. Ein Ideal $\mathfrak{a}$ (oder eine Zahl α) ist stets und nur dann durch ein Ideal $\mathfrak{b}$ (oder eine Zahl δ) teilbar, wenn alle in $\mathfrak{b}$ (oder δ) aufgehenden Potenzen von Primidealen auch in $\mathfrak{a}$ (oder α) aufgehen.

Denn wenn $\mathfrak{p}$ ein Primideal ist, und $\mathfrak{p}^m$ in einem Ideale $\mathfrak{b}$ aufgeht, so ist (nach 6.) $\mathfrak{b} = \mathfrak{e}\mathfrak{p}^m$, und wenn man das Ideal $\mathfrak{e}$ (nach 4.) in seine Primfaktoren zerlegt, so ist auch $\mathfrak{b}$ als Produkt von lauter Primidealen dargestellt, unter denen folglich der Faktor $\mathfrak{p}$ mindestens $m$mal vorkommt; umgekehrt, wenn in der Zerlegung von $\mathfrak{b}$ in Primfaktoren das Primideal $\mathfrak{p}$ mindestens $m$mal als Faktor auftritt, so ist $\mathfrak{b}$ offenbar durch $\mathfrak{p}^m$ teilbar. Wenn daher gesagt wird, daß alle in $\mathfrak{b}$ aufgehenden Potenzen von Primidealen auch in einem Ideale $\mathfrak{a}$ aufgehen, so heißt dies nichts anderes, als daß alle in der Zerlegung von $\mathfrak{b}$ auftretenden Primfaktoren auch sämtlich mindestens ebensooft in der Zerlegung von $\mathfrak{a}$ als Faktoren auftreten; unter den Faktoren von $\mathfrak{a}$ finden sich daher zunächst alle Faktoren von $\mathfrak{b}$, und wenn man das Produkt der übrigen Faktoren von $\mathfrak{a}$ mit $\mathfrak{r}$ bezeichnet, so ist $\mathfrak{a} = \mathfrak{r}\mathfrak{b}$, und folglich ist $\mathfrak{a}$ teilbar durch $\mathfrak{b}$. Daß aber umgekehrt, wenn $\mathfrak{b}$ ein Teiler von $\mathfrak{a}$ ist, alle in $\mathfrak{b}$ aufgehenden Potenzen von Primidealen auch in $\mathfrak{a}$ aufgehen, versteht sich von selbst.

Nachdem unser Satz bewiesen ist, bemerken wir noch folgendes. Vereinigt man alle untereinander gleichen Primfaktoren eines Ideals $\mathfrak{a}$ zu einer Potenz, so erhält man

$$\mathfrak{a} = \mathfrak{p}^a\mathfrak{q}^b\mathfrak{r}^c\dots,$$

wo $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}\dots$ lauter voneinander verschiedene Primideale bedeuten, und nach dem eben bewiesenen Satze sind die sämtlichen Teiler von $\mathfrak{a}$ in der Form

$$\mathfrak{b} = \mathfrak{p}^{a'}\mathfrak{q}^{b'}\mathfrak{r}^{c'}\dots$$

enthalten, wo die Exponenten $a', b', c'\dots$ den Bedingungen

$$0 \leqq a' \leqq a,\ 0 \leqq b' \leqq b,\ 0 \leqq c' \leqq c\dots$$

genügen; da je zwei verschiedenen Kombinationen von Exponenten $a', b', c'\dots$ (nach 4.) zwei verschiedene Ideale $\mathfrak{b}$ entsprechen, so ist die Anzahl aller verschiedenen Teiler

$$= (a+1)(b+1)(c+1)\dots$$

9. Ist $\mathfrak{m}$ das kleinste gemeinschaftliche Vielfache und $\mathfrak{b}$ der größte gemeinschaftliche Teiler der beiden Ideale $\mathfrak{a}$, $\mathfrak{b}$, so ist

$$\mathfrak{a} = \mathfrak{b}\mathfrak{a}',\ \mathfrak{b} = \mathfrak{b}\mathfrak{b}',\ \mathfrak{m}\mathfrak{b} = \mathfrak{a}\mathfrak{b},$$
$$\mathfrak{m} = \mathfrak{b}\mathfrak{a}'\mathfrak{b}' = \mathfrak{a}\mathfrak{b}' = \mathfrak{b}\mathfrak{a}',$$

wo $\mathfrak{a}', \mathfrak{b}'$ relative Primideale bedeuten. Ist ferner $\mathfrak{b}\mathfrak{c}$ teilbar durch $\mathfrak{a}$, so ist $\mathfrak{c}$ teilbar durch $\mathfrak{a}'$.

Denn weil $\mathfrak{a}$ und $\mathfrak{b}$ durch $\mathfrak{b}$ teilbar sind, so kann man (nach 6.) $\mathfrak{a} = \mathfrak{b}\mathfrak{a}'$, $\mathfrak{b} = \mathfrak{b}\mathfrak{b}'$ setzen; bedeutet nun $\mathfrak{b}'$ den größten gemeinschaftlichen Teiler der Ideale $\mathfrak{a}'$, $\mathfrak{b}'$, so ist (nach § 170, 1.) das Produkt $\mathfrak{b}\mathfrak{b}'$ ein gemeinschaftlicher Teiler von $\mathfrak{a}$, $\mathfrak{b}$, also auch ein Teiler von $\mathfrak{b}$, woraus (nach 6.) $\mathfrak{b}' = \mathfrak{o}$ folgt; mithin sind $\mathfrak{a}'$, $\mathfrak{b}'$ relative Primideale. Ist nun $\mathfrak{b}\mathfrak{c}$ teilbar durch $\mathfrak{a}$, also $\mathfrak{b}\mathfrak{b}'\mathfrak{c}$ teilbar durch $\mathfrak{b}\mathfrak{a}'$, so muß (nach 6.) $\mathfrak{a}'$ in $\mathfrak{b}'\mathfrak{c}$, mithin (nach § 171, 5.) auch in $\mathfrak{c}$ aufgehen. Hieraus folgen sofort die Behauptungen über $\mathfrak{m}$; da nämlich $\mathfrak{m}$ teilbar durch $\mathfrak{b}$, also (nach 6.) von der Form $\mathfrak{b}\mathfrak{c}$, zugleich aber auch teilbar durch $\mathfrak{a}$ ist, so ist $\mathfrak{c}$ teilbar durch $\mathfrak{a}'$, also $\mathfrak{m}$ teilbar durch $\mathfrak{b}\mathfrak{a}'$ (nach § 170, 1.); da aber umgekehrt dieses letztere Ideal $\mathfrak{b}\mathfrak{a}' = \mathfrak{b}\mathfrak{a}'\mathfrak{b}' = \mathfrak{a}\mathfrak{b}'$ ein gemeinschaftliches Vielfaches von $\mathfrak{a}$, $\mathfrak{b}$ ist, so muß es durch $\mathfrak{m}$ teilbar und folglich $= \mathfrak{m}$ sein, was zu beweisen war.

Erläuterungen zu den vorstehenden Abhandlungen XLVI bis XLIX.

Im vorangehenden ist das „Elfte Supplement“ in den verschiedenen Fassungen gegeben, vollständig in der letzten, während von den früheren nur jeweils das dort nicht Übernommene gebracht wurde. Es zeigt sich, daß die Entwicklungen zur analytischen Zahlentheorie — Dedekindsche ζ-Funktion, transzendente Bestimmung der Klassenzahl — fast unverändert in alle Auflagen übernommen wurden, ebenso die Theorie der Einheiten. Dagegen hat das, was als Dedekinds ureigene Schöpfung zu bezeichnen ist, Körpertheorie und Idealtheorie, von Auflage zu Auflage neue Formen angenommen.

Die erste Begründung der Körpertheorie (in der 2. Auflage, XLVII) ruht vollständig auf hyperkomplexer Grundlage, einer Grundlage, die Dedekind später verlassen hat, weil sie für die hier vorliegenden Zwecke entbehrlich war, wohl auch um das Verständnis zu erleichtern; die hyperkomplexe Theorie war noch sehr kompliziert und formal. Die hyperkomplexe Auffassung, deren Wichtigkeit in neuester Zeit immer mehr hervortritt, steht aber auch hinter den späteren Fassungen; sie findet sich wieder ziemlich stark in Dedekind-Weber (vgl. die Erläuterungen zu XVIII). Die weiteren hyperkomplexen Arbeiten schließen direkt an die ursprüngliche Begründung der Körpertheorie an (vgl. die Erläuterungen zu XX).

Die ausführliche Entwicklung der Galoisschen Theorie in der heutigen Form findet sich erst in der 4. Auflage (XLVI), Andeutungen davon schon in der ersten Begründung der Körpertheorie (vgl. Anm. *) S. 228), weiter ausgeführte in den folgenden Darstellungen. Dedekind geht aus von der Betrachtung der Iso-

morphismen beliebiger Körper und ihrer Zusammensetzung, Betrachtungen, die erst in neuester Zeit wieder aufgenommen wurden; durch Spezialisierung auf Galoissche Körper kommt er zur Automorphismengruppe. Diese Auffassung der Galoisschen Gruppe als Automorphismengruppe ist einer der Ausgangspunkte in der neueren Entwicklung der Algebra geworden; Dedekind hat sie schon in seinen Göttinger Vorlesungen 1857/58 entwickelt (vgl. Anm. *) S. 52). Dabei arbeitet Dedekind bei dem Fortsetzungssatz der Isomorphismen ohne Benutzung eines primitiven Elements, ein Umstand, der ihm die Übertragung auf unendliche Körper ermöglichte (XXXI); auch das ist erst in neuester Zeit allgemein in die Algebra eingedrungen.

Die Entwicklung der Idealtheorie läuft ganz ähnlich wie die der Körpertheorie; die ersten Fassungen sind allgemeiner, aber noch sehr kompliziert. Die erste Begründung der 2. Auflage (XLVII) spaltet den Zerlegungssatz in zwei Teile: das Ideal wird als kl. gem. Vielf. (Durchschnitt) von symbolischen Primidealpotenzen dargestellt; erst dann wird der Produktbegriff eingeführt und zu der üblichen Zerlegungsform übergegangen. Dabei wird aber schon bei der Durchschnittsdarstellung benutzt, daß es sich um die Hauptordnung handelt; die ganze Abgeschlossenheit wird wesentlich herangezogen.

Die 3. Auflage enthält ein Stück allgemeine Idealtheorie, die eindeutige Zerlegung der Ideale einer Ordnung in Primärideale (einartige Ideale). Der ausgeführte Beweis fand sich im Nachlaß mit dem Vermerk „für die dritte Auflage kassiert, doch wichtig“ und ist jetzt an der betreffenden Stelle wieder eingefügt (XLIX). Daß nur in der Hauptordnung die ausnahmslose Darstellung der Primärideale als Potenzen von Primidealen gilt, ist dort (XLIX, § 172) klar ausgesprochen, ebenso, daß nur in der Hauptordnung ausnahmslos aus Teilbarkeit Produktdarstellung folgt; auch auf die Bedeutung der allgemeineren Idealtheorie ist hingewiesen. Bis auf diese Zufügungen ist der Aufbau aus der französischen Darstellung (XLVIII) übernommen, die im übrigen stärker als die übrigen Fassungen durch zahlreich eingefügte Beispiele den Charakter einer elementaren Einführung trägt.

Die 4. Auflage (XLVI) steht auf neuer Grundlage: sie stellt die Gruppeneigenschaft der ganzen und gebrochenen Ideale in den Vordergrund, indem auf Grund der ganzen Abgeschlossenheit — formal eingekleidet in einen allgemeinen Modulsatz — gezeigt wird, daß jedes Ideal ein eigentlicher (umkehrbarer) Modul ist. Diese Auffassung wollte Dedekind in einer nicht mehr zur Ausführung gekommenen 5. Auflage noch unterstreichen, dadurch, daß er von vornherein ganze und gebrochene Ideale seinen Definitionen zugrunde legte. Im übrigen plante er nach den vorgefundenen Notizen keine wesentliche Änderung des 11. Supplements, nur ein noch etwas stärkeres Hervorheben der formalen Modulidentitäten, im Anschluß an XXX.

Über die axiomatische Begründung der Idealtheorie, die überall durch Dedekindsche Gedankengänge beeinflußt ist, ist in den Erläuterungen zu XXV berichtet; die Begriffsbildungen des 11. Supplements durchziehen heute die ganze abstrakte Algebra.

Noether.

L.

Stetigkeit und irrationale Zahlen.

[Erste Auflage 1872. Fünfte Auflage 1927.]

Seinem geliebten Vater,
dem
Geh. Hofrat, Professor, Dr. jur. **Julius Levin Ulrich Dedekind**
in Braunschweig bei Gelegenheit seines funfzigjährigen Amts-Jubiläums
am 26. April 1872 gewidmet.

Inhalt.

Die Betrachtungen, welche den Gegenstand dieser kleinen Schrift bilden, stammen aus dem Herbst des Jahres 1858. Ich befand mich damals als Professor am eidgenössischen Polytechnikum zu Zürich zum ersten Male in der Lage, die Elemente der Differentialrechnung vortragen zu müssen, und fühlte dabei empfindlicher als jemals früher den Mangel einer wirklich wissenschaftlichen Begründung der Arithmetik. Bei dem Begriffe der Annäherung einer veränderlichen Größe

an einen festen Grenzwert und namentlich bei dem Beweise des Satzes, daß jede Größe, welche beständig, aber nicht über alle Grenzen wächst, sich gewiß einem Grenzwert nähern muß, nahm ich meine Zuflucht zu geometrischen Evidenzen. Auch jetzt halte ich ein solches Heranziehen geometrischer Anschauung bei dem ersten Unterrichte in der Differentialrechnung vom didaktischen Standpunkte aus für außerordentlich nützlich, ja unentbehrlich, wenn man nicht gar zu viel Zeit verlieren will. Aber daß diese Art der Einführung in die Differentialrechnung keinen Anspruch auf Wissenschaftlichkeit machen kann, wird wohl niemand leugnen. Für mich war damals dies Gefühl der Unbefriedigung ein so überwältigendes, daß ich den festen Entschluß faßte, so lange nachzudenken, bis ich eine rein arithmetische und völlig strenge Begründung der Prinzipien der Infinitesimalanalysis gefunden haben würde. Man sagt so häufig, die Differentialrechnung beschäftige sich mit den stetigen Größen, und doch wird nirgends eine Erklärung von dieser Stetigkeit gegeben, und auch die strengsten Darstellungen der Differentialrechnung gründen ihre Beweise nicht auf die Stetigkeit, sondern sie appellieren entweder mit mehr oder weniger Bewußtsein an geometrische, oder durch die Geometrie veranlaßte Vorstellungen, oder aber sie stützen sich auf solche Sätze, welche selbst nie rein arithmetisch bewiesen sind. Zu diesen gehört z. B. der oben erwähnte Satz, und eine genauere Untersuchung überzeugte mich, daß dieser oder auch jeder mit ihm äquivalente Satz gewissermaßen als ein hinreichendes Fundament für die Infinitesimalanalysis angesehen werden kann. Es kam nur noch darauf an, seinen eigentlichen Ursprung in den Elementen der Arithmetik zu entdecken und hiermit zugleich eine wirkliche Definition von dem Wesen der Stetigkeit zu gewinnen. Dies gelang mir am 24. November 1858, und wenige Tage darauf teilte ich das Ergebnis meines Nachdenkens meinem teuren Freunde Durège mit, was zu einer langen und lebhaften Unterhaltung führte. Später habe ich wohl dem einen oder anderen meiner Schüler diese Gedanken über eine wissenschaftliche Begründung der Arithmetik auseinandergesetzt, auch hier in Braunschweig in dem wissenschaftlichen Verein der Professoren einen Vortrag über diesen Gegenstand gehalten, aber zu einer eigentlichen Publikation konnte ich mich nicht recht entschließen, weil erstens die Darstellung nicht ganz leicht, und weil außerdem die Sache so wenig fruchtbar ist. Indessen hatte ich doch schon halb und halb

daran gedacht, dieses Thema zum Gegenstande dieser Gelegenheitsschrift zu wählen, als vor wenigen Tagen, am 14. März, die Abhandlung: „Die Elemente der Funktionenlehre“, von E. Heine (Crelles Journal, Bd. 74) durch die Güte ihres hochverehrten Verfassers in meine Hände gelangte und mich in meinem Entschlusse bestärkte. Dem Wesen nach stimme ich zwar vollständig mit dem Inhalte dieser Schrift überein, wie es ja nicht anders sein kann, aber ich will freimütig gestehen, daß meine Darstellung mir der Form nach einfacher zu sein und den eigentlichen Kernpunkt präziser hervorzuheben scheint. Und während ich an diesem Vorwort schreibe (20. März 1872), erhalte ich die interessante Abhandlung: „Über die Ausdehnung eines Satzes aus der Theorie der trigonometrischen Reihen“, von G. Cantor (Math. Annalen von Clebsch und Neumann, Bd. 5), für welche ich dem scharfsinnigen Verfasser meinen besten Dank sage. Wie ich bei raschem Durchlesen finde, so stimmt das Axiom in § 2 derselben, abgesehen von der äußeren Form der Einkleidung, vollständig mit dem überein, was ich unten in § 3 als das Wesen der Stetigkeit bezeichne. Welchen Nutzen aber die wenn auch nur begriffliche Unterscheidung von reellen Zahlgrößen noch höherer Art gewähren wird, vermag ich gerade nach meiner Auffassung des in sich vollkommenen reellen Zahlgebietes noch nicht zu erkennen.

§ 1.

Eigenschaften der rationalen Zahlen.

Die Entwicklung der Arithmetik der rationalen Zahlen wird hier zwar vorausgesetzt, doch halte ich es für gut, einige Hauptmomente ohne Diskussion hervorzuheben, nur um den Standpunkt von vornherein zu bezeichnen, den ich im folgenden einnehme. Ich sehe die ganze Arithmetik als eine notwendige oder wenigstens natürliche Folge des einfachsten arithmetischen Aktes, des Zählens, an, und das Zählen selbst ist nichts anderes als die sukzessive Schöpfung der unendlichen Reihe der positiven ganzen Zahlen, in welcher jedes Individuum durch das unmittelbar vorhergehende definiert wird; der einfachste Akt ist der Übergang von einem schon erschaffenen Individuum zu dem darauffolgenden neu zu erschaffenden. Die Kette dieser Zahlen bildet an sich schon ein überaus nützliches Hilfsmittel für den menschlichen Geist, und sie bietet einen unerschöpflichen Reichtum an merkwürdigen

Gesetzen dar, zu welchen man durch die Einführung der vier arithmetischen Grundoperationen gelangt. Die Addition ist die Zusammenfassung einer beliebigen Wiederholung des obigen einfachsten Aktes zu einem einzigen Akte, und aus ihr entspringt auf dieselbe Weise die Multiplikation. Während diese beiden Operationen stets ausführbar sind, zeigen die umgekehrten Operationen, die Subtraktion und Division, nur eine beschränkte Zulässigkeit. Welches nun auch die nächste Veranlassung gewesen sein mag, welche Vergleichungen oder Analogieen mit Erfahrungen, Anschauungen dazu geführt haben mögen, bleibe dahingestellt; genug, gerade diese Beschränktheit in der Ausführbarkeit der indirekten Operationen ist jedesmal die eigentliche Ursache eines neuen Schöpfungsaktes geworden; so sind die negativen und gebrochenen Zahlen durch den menschlichen Geist erschaffen, und es ist in dem System aller rationalen Zahlen ein Instrument von unendlich viel größerer Vollkommenheit gewonnen. Dieses System, welches ich mit R bezeichnen will, besitzt vor allen Dingen eine Vollständigkeit und Abgeschlossenheit, welche ich an einem anderen Orte*) als Merkmal eines Zahlkörpers bezeichnet habe, und welche darin besteht, daß die vier Grundoperationen mit je zwei Individuen in R stets ausführbar sind, d. h. daß das Resultat derselben stets wieder ein bestimmtes Individuum in R ist, wenn man den einzigen Fall der Division durch die Zahl Null ausnimmt.

Für unseren nächsten Zweck ist aber noch wichtiger eine andere Eigenschaft des Systems R, welche man dahin aussprechen kann, daß das System R ein wohlgeordnetes, nach zwei entgegengesetzten Seiten hin unendliches Gebiet von einer Dimension bildet. Was damit gemeint sein soll, ist durch die Wahl der Ausdrücke, welche geometrischen Vorstellungen entlehnt sind, hinreichend angedeutet; um so notwendiger ist es, die entsprechenden rein arithmetischen Eigentümlichkeiten hervorzuheben, damit es auch nicht einmal den Anschein behält, als bedürfte die Arithmetik solcher ihr fremden Vorstellungen.

Soll ausgedrückt werden, daß die Zeichen a und b eine und dieselbe rationale Zahl bedeuten, so setzt man sowohl $a = b$ wie $b = a$. Die Verschiedenheit zweier rationaler Zahlen a, b zeigt sich darin, daß die Differenz $a - b$ entweder einen positiven oder einen

*) Vorlesungen über Zahlentheorie von P. G. Lejeune Dirichlet. Zweite Auflage. § 159.

negativen Wert hat. Im ersten Falle heißt a größer als b, b kleiner als a, was auch durch die Zeichen $a > b$, $b < a$ angedeutet wird*). Da im zweiten Falle $b - a$ einen positiven Wert hat, so ist $b > a$, $a < b$. Hinsichtlich dieser doppelten Möglichkeit in der Art der Verschiedenheit gelten nun folgende Gesetze.

I. Ist $a > b$, und $b > c$, so ist $a > c$. Wir wollen jedesmal, wenn a, c zwei verschiedene (oder ungleiche) Zahlen sind, und wenn b größer als die eine, kleiner als die andere ist, ohne Scheu vor dem Anklang an geometrische Vorstellungen dies kurz so ausdrücken: b liegt zwischen den beiden Zahlen a, c.

II. Sind a, c zwei verschiedene Zahlen, so gibt es immer unendlich viele verschiedene Zahlen b, welche zwischen a, c liegen.

III. Ist a eine bestimmte Zahl, so zerfallen alle Zahlen des Systems R in zwei Klassen, A_1 und A_2, deren jede unendlich viele Individuen enthält; die erste Klasse A_1 umfaßt alle Zahlen a_1, welche $< a$ sind, die zweite Klasse A_2 umfaßt alle Zahlen a_2, welche $> a$ sind; die Zahl a selbst kann nach Belieben der ersten oder der zweiten Klasse zugeteilt werden, und sie ist dann entsprechend die größte Zahl der ersten oder die kleinste Zahl der zweiten Klasse. In jedem Falle ist die Zerlegung des Systems R in die beiden Klassen A_1, A_2 von der Art, daß jede Zahl der ersten Klasse A_1 kleiner als jede Zahl der zweiten Klasse A_2 ist.

§ 2.

Vergleichung der rationalen Zahlen mit den Punkten einer geraden Linie.

Die soeben hervorgehobenen Eigenschaften der rationalen Zahlen erinnern an die gegenseitigen Lagenbeziehungen zwischen den Punkten einer geraden Linie L. Werden die beiden in ihr existierenden entgegengesetzten Richtungen durch „rechts“ und „links“ unterschieden, und sind p, q zwei verschiedene Punkte, so liegt entweder p rechts von q, und gleichzeitig q links von p, oder umgekehrt, es liegt q rechts von p, und gleichzeitig p links von q. Ein dritter Fall ist unmöglich, wenn p, q wirklich verschiedene Punkte sind. Hinsichtlich dieser Lagenverschiedenheit bestehen folgende Gesetze.

*) Es ist also im folgenden immer das sogenannte „algebraische“ größer und kleiner Sein gemeint, wenn nicht das Wort „absolut“ hinzugefügt wird.

I. Liegt p rechts von q, und q wieder rechts von r, so liegt auch p rechts von r; und man sagt, daß q zwischen den Punkten p und r liegt.

II. Sind p, r zwei verschiedene Punkte, so gibt es immer unendlich viele Punkte q, welche zwischen p und r liegen.

III. Ist p ein bestimmter Punkt in L, so zerfallen alle Punkte in L in zwei Klassen, P_1, P_2, deren jede unendlich viele Individuen enthält; die erste Klasse P_1 umfaßt alle die Punkte p_1, welche links von p liegen, und die zweite Klasse P_2 umfaßt alle die Punkte p_2, welche rechts von p liegen; der Punkt p selbst kann nach Belieben der ersten oder der zweiten Klasse zugeteilt werden. In jedem Falle ist die Zerlegung der Geraden L in die beiden Klassen oder Stücke P_1, P_2 von der Art, daß jeder Punkt der ersten Klasse P_1 links von jedem Punkte der zweiten Klasse P_2 liegt.

Diese Analogie zwischen den rationalen Zahlen und den Punkten einer Geraden wird bekanntlich zu einem wirklichen Zusammenhange, wenn in der Geraden ein bestimmter Anfangspunkt oder Nullpunkt o und eine bestimmte Längeneinheit zur Ausmessung der Strecken gewählt wird. Mit Hilfe der letzteren kann für jede rationale Zahl a eine entsprechende Länge konstruiert werden, und trägt man dieselbe von dem Punkte o aus nach rechts oder links auf der Geraden ab, je nachdem a positiv oder negativ ist, so gewinnt man einen bestimmten Endpunkt p, welcher als der der Zahl a entsprechende Punkt bezeichnet werden kann; der rationalen Zahl Null entspricht der Punkt o. Auf diese Weise entspricht jeder rationalen Zahl a, d. h. jedem Individuum in R, ein und nur ein Punkt p, d. h. ein Individuum in L. Entsprechen den beiden Zahlen a, b bzw. die beiden Punkte p, q, und ist $a > b$, so liegt p rechts von q. Den Gesetzen I, II, III des vorigen Paragraphen entsprechen vollständig die Gesetze I, II, III des jetzigen.

§ 3.

Stetigkeit der geraden Linie.

Von der größten Wichtigkeit ist nun aber die Tatsache, daß es in der Geraden L unendlich viele Punkte gibt, welche keiner rationalen Zahl entsprechen. Entspricht nämlich der Punkt p der rationalen Zahl a, so ist bekanntlich die Länge op kommensurabel mit der bei der Konstruktion benutzten unabänderlichen Längeneinheit, d. h. es gibt eine dritte Länge, ein sogenanntes gemeinschaftliches Maß, von welcher diese beiden Längen ganze Vielfache sind. Aber schon die alten Griechen haben gewußt und bewiesen, daß es Längen gibt, welche mit einer gegebenen Längeneinheit inkommensurabel sind, z. B. die Diagonale des Quadrates, dessen Seite die Längeneinheit ist. Trägt man eine solche Länge von dem Punkt o aus auf der Geraden ab, so erhält man einen Endpunkt, welcher keiner rationalen Zahl entspricht. Da sich ferner leicht beweisen läßt, daß es unendlich viele Längen gibt, welche mit der Längeneinheit inkommensurabel sind, so können wir behaupten: Die Gerade L ist unendlich viel reicher an Punktindividuen, als das Gebiet R der rationalen Zahlen an Zahlindividuen.

Will man nun, was doch der Wunsch ist, alle Erscheinungen in der Geraden auch arithmetisch verfolgen, so reichen dazu die rationalen Zahlen nicht aus, und es wird daher unumgänglich notwendig, das Instrument R, welches durch die Schöpfung der rationalen Zahlen konstruiert war, wesentlich zu verfeinern durch eine Schöpfung von neuen Zahlen der Art, daß das Gebiet der Zahlen dieselbe Vollständigkeit oder, wie wir gleich sagen wollen, dieselbe Stetigkeit gewinnt, wie die gerade Linie.

Die bisherigen Betrachtungen sind allen so bekannt und geläufig, daß viele ihre Wiederholung für sehr überflüssig erachten werden. Dennoch hielt ich diese Rekapitulation für notwendig, um die Hauptfrage gehörig vorzubereiten. Die bisher übliche Einführung der irrationalen Zahlen knüpft nämlich geradezu an den Begriff der extensiven Größen an — welcher aber selbst nirgends streng definiert wird — und erklärt die Zahl als das Resultat der Messung einer solchen Größe durch eine zweite gleichartige*). Statt dessen fordere ich, daß die Arithmetik sich aus sich selbst heraus entwickeln soll. Daß solche Anknüpfungen an nicht arithmetische Vorstellungen die nächste Veranlassung zur Erweiterung des Zahlbegriffes gegeben haben, mag im allgemeinen zugegeben werden (doch ist dies bei der Einführung der komplexen Zahlen entschieden nicht der Fall gewesen);

*) Der scheinbare Vorzug der Allgemeinheit dieser Definition der Zahl schwindet sofort dahin, wenn man an die komplexen Zahlen denkt. Nach meiner Auffassung kann umgekehrt der Begriff des Verhältnisses zwischen zwei gleichartigen Größen erst dann klar entwickelt werden, wenn die irrationalen Zahlen schon eingeführt sind.

aber hierin liegt ganz gewiß kein Grund, diese fremdartigen Betrachtungen selbst in die Arithmetik, in die Wissenschaft von den Zahlen aufzunehmen. So wie die negativen und gebrochenen rationalen Zahlen durch eine freie Schöpfung hergestellt, und wie die Gesetze der Rechnungen mit diesen Zahlen auf die Gesetze der Rechnungen mit ganzen positiven Zahlen zurückgeführt werden müssen und können, ebenso hat man dahin zu streben, daß auch die irrationalen Zahlen durch die rationalen Zahlen allein vollständig definiert werden. Nur das Wie? bleibt die Frage.

Die obige Vergleichung des Gebietes R der rationalen Zahlen mit einer Geraden hat zu der Erkenntnis der Lückenhaftigkeit, Unvollständigkeit oder Unstetigkeit des ersteren geführt, während wir der Geraden Vollständigkeit, Lückenlosigkeit oder Stetigkeit zuschreiben. Worin besteht denn nun eigentlich diese Stetigkeit? In der Beantwortung dieser Frage muß alles enthalten sein, und nur durch sie wird man eine wissenschaftliche Grundlage für die Untersuchung aller stetigen Gebiete gewinnen. Mit vagen Reden über den ununterbrochenen Zusammenhang in den kleinsten Teilen ist natürlich nichts erreicht; es kommt darauf an, ein präzises Merkmal der Stetigkeit anzugeben, welches als Basis für wirkliche Deduktionen gebraucht werden kann. Lange Zeit habe ich vergeblich darüber nachgedacht, aber endlich fand ich, was ich suchte. Dieser Fund wird von verschiedenen Personen vielleicht verschieden beurteilt werden, doch glaube ich, daß die meisten seinen Inhalt sehr trivial finden werden. Er besteht im folgenden. Im vorigen Paragraphen ist darauf aufmerksam gemacht, daß jeder Punkt p der Geraden eine Zerlegung derselben in zwei Stücke von der Art hervorbringt, daß jeder Punkt des einen Stückes links von jedem Punkte des anderen liegt. Ich finde nun das Wesen der Stetigkeit in der Umkehrung, also in dem folgenden Prinzip:

„Zerfallen alle Punkte der Geraden in zwei Klassen von der Art, daß jeder Punkt der ersten Klasse links von jedem Punkte der zweiten Klasse liegt, so existiert ein und nur ein Punkt, welcher diese Einteilung aller Punkte in zwei Klassen, diese Zerschneidung der Geraden in zwei Stücke hervorbringt.“

Wie schon gesagt, glaube ich nicht zu irren, wenn ich annehme, daß jedermann die Wahrheit dieser Behauptung sofort zugeben wird; die meisten meiner Leser werden sehr enttäuscht sein, zu vernehmen, daß

durch diese Trivialität das Geheimnis der Stetigkeit enthüllt sein soll. Dazu bemerke ich folgendes. Es ist mir sehr lieb, wenn jedermann das obige Prinzip so einleuchtend findet und so übereinstimmend mit seinen Vorstellungen von einer Linie; denn ich bin außerstande, irgendeinen Beweis für seine Richtigkeit beizubringen, und niemand ist dazu imstande. Die Annahme dieser Eigenschaft der Linie ist nichts als ein Axiom, durch welches wir erst der Linie ihre Stetigkeit zuerkennen, durch welches wir die Stetigkeit in die Linie hineindenken. Hat überhaupt der Raum eine reale Existenz, so braucht er doch nicht notwendig stetig zu sein; unzählige seiner Eigenschaften würden dieselben bleiben, wenn er auch unstetig wäre. Und wüßten wir gewiß, daß der Raum unstetig wäre, so könnte uns doch wieder nichts hindern, falls es uns beliebte, ihn durch Ausfüllung seiner Lücken in Gedanken zu einem stetigen zu machen; diese Ausfüllung würde aber in einer Schöpfung von neuen Punktindividuen bestehen und dem obigen Prinzip gemäß auszuführen sein.

§ 4.

Schöpfung der irrationalen Zahlen.

Durch die letzten Worte ist schon hinreichend angedeutet, auf welche Art das unstetige Gebiet R der rationalen Zahlen zu einem stetigen vervollständigt werden muß. In § 1 ist hervorgehoben (III), daß jede rationale Zahl a eine Zerlegung des Systems R in zwei Klassen A_1, A_2 von der Art hervorbringt, daß jede Zahl a_1 der ersten Klasse A_1 kleiner ist als jede Zahl a_2 der zweiten Klasse A_2; die Zahl a ist entweder die größte Zahl der Klasse A_1, oder die kleinste Zahl der Klasse A_2. Ist nun irgendeine Einteilung des Systems R in zwei Klassen A_1, A_2 gegeben, welche nur die charakteristische Eigenschaft besitzt, daß jede Zahl a_1 in A_1 kleiner ist als jede Zahl a_2 in A_2, so wollen wir der Kürze halber eine solche Einteilung einen Schnitt nennen und mit (A_1, A_2) bezeichnen. Wir können dann sagen, daß jede rationale Zahl a einen Schnitt oder eigentlich zwei Schnitte hervorbringt, welche wir aber nicht als wesentlich verschieden ansehen wollen; dieser Schnitt hat außerdem die Eigenschaft, daß entweder unter den Zahlen der ersten Klasse eine größte, oder unter den Zahlen der zweiten Klasse eine kleinste existiert. Und umgekehrt,

besitzt ein Schnitt auch diese Eigenschaft, so wird er durch diese größte oder kleinste rationale Zahl hervorgebracht.

Aber man überzeugt sich leicht, daß auch unendlich viele Schnitte existieren, welche nicht durch rationale Zahlen hervorgebracht werden. Das nächstliegende Beispiel ist folgendes.

Es sei D eine positive ganze Zahl, aber nicht das Quadrat einer ganzen Zahl, so gibt es eine positive ganze Zahl λ von der Art, daß

$$\lambda^2 < D < (\lambda + 1)^2$$

wird.

Nimmt man in die zweite Klasse A_2 jede positive rationale Zahl a_2 auf, deren Quadrat $> D$ ist, in die erste Klasse A_1 aber alle anderen rationalen Zahlen a_1, so bildet diese Einteilung einen Schnitt (A_1, A_2), d. h. jede Zahl a_1 ist kleiner als jede Zahl a_2. Ist nämlich $a_1 = 0$ oder negativ, so ist a_1 schon aus diesem Grunde kleiner als jede Zahl a_2, weil diese zufolge der Definition positiv ist; ist aber a_1 positiv, so ist ihr Quadrat $\leqq D$, und folglich ist a_1 kleiner als jede positive Zahl a_2, deren Quadrat $> D$ ist.

Dieser Schnitt wird aber durch keine rationale Zahl hervorgebracht. Um dies zu beweisen, muß vor allem gezeigt werden, daß es keine rationale Zahl gibt, deren Quadrat $= D$ ist. Obgleich dies aus den ersten Elementen der Zahlentheorie bekannt ist, so mag doch hier der folgende indirekte Beweis Platz finden. Gibt es eine rationale Zahl, deren Quadrat $= D$ ist, so gibt es auch zwei positive ganze Zahlen t, u, welche der Gleichung

$$t^2 - D u^2 = 0$$

genügen, und man darf annehmen, daß u die kleinste positive ganze Zahl ist, welche die Eigenschaft besitzt, daß ihr Quadrat durch Multiplikation mit D in das Quadrat einer ganzen Zahl t verwandelt wird. Da nun offenbar

$$\lambda u < t < (\lambda + 1) u$$

ist, so wird die Zahl

$$u' = t - \lambda u$$

eine positive ganze Zahl, und zwar kleiner als u. Setzt man ferner

$$t' = D u - \lambda t,$$

so wird t' ebenfalls eine positive ganze Zahl, und es ergibt sich

$$t'^2 - D u'^2 = (\lambda^2 - D)(t^2 - D u^2) = 0,$$

was mit der Annahme über u im Widerspruch steht.

Mithin ist das Quadrat einer jeden rationalen Zahl x entweder $< D$ oder $> D$. Hieraus folgt nun leicht, daß es weder in der Klasse A_1 eine größte, noch in der Klasse A_2 eine kleinste Zahl gibt. Setzt man nämlich

$$y = \frac{x(x^2 + 3D)}{3x^2 + D},$$

so ist

$$y - x = \frac{2x(D - x^2)}{3x^2 + D}$$

und

$$y^2 - D = \frac{(x^2 - D)^3}{(3x^2 + D)^2}.$$

Nimmt man hierin für x eine positive Zahl aus der Klasse A_1, so ist $x^2 < D$, und folglich wird $y > x$, und $y^2 < D$, also gehört y ebenfalls der Klasse A_1 an. Setzt man aber für x eine Zahl aus der Klasse A_2, so ist $x^2 > D$, und folglich wird $y < x$, $y > 0$ und $y^2 > D$, also gehört y ebenfalls der Klasse A_2 an. Dieser Schnitt wird daher durch keine rationale Zahl hervorgebracht.

In dieser Eigenschaft, daß nicht alle Schnitte durch rationale Zahlen hervorgebracht werden, besteht die Unvollständigkeit oder Unstetigkeit des Gebietes R aller rationalen Zahlen.

Jedesmal nun, wenn ein Schnitt (A_1, A_2) vorliegt, welcher durch keine rationale Zahl hervorgebracht wird, so erschaffen wir eine neue, eine irrationale Zahl α, welche wir als durch diesen Schnitt (A_1, A_2) vollständig definiert ansehen; wir werden sagen, daß die Zahl α diesem Schnitt entspricht, oder daß sie diesen Schnitt hervorbringt. Es entspricht also von jetzt ab jedem bestimmten Schnitt eine und nur eine bestimmte rationale oder irrationale Zahl und wir sehen zwei Zahlen stets und nur dann als verschieden oder ungleich an, wenn sie wesentlich verschiedenen Schnitten entsprechen.

Um nun eine Grundlage für die Anordnung aller reellen, d. h. aller rationalen und irrationalen Zahlen zu gewinnen, müssen wir

zunächst die Beziehungen zwischen irgend zwei Schnitten (A_1, A_2) und (B_1, B_2) untersuchen, welche durch irgend zwei Zahlen α und β hervorgebracht werden. Offenbar ist ein Schnitt (A_1, A_2) schon vollständig gegeben, wenn eine der beiden Klassen, z. B. die erste A_1, bekannt ist, weil die zweite A_2 aus allen nicht in A_1 enthaltenen rationalen Zahlen besteht, und die charakteristische Eigenschaft einer solchen ersten Klasse A_1 liegt darin, daß sie, wenn die Zahl a_1 in ihr enthalten ist, auch alle kleineren Zahlen als a_1 enthält. Vergleicht man nun zwei solche erste Klassen A_1, B_1 miteinander, so kann es 1. sein, daß sie vollständig identisch sind, d. h. daß jede in A_1 enthaltene Zahl a_1 auch in B_1, und daß jede in B_1 enthaltene Zahl b_1 auch in A_1 enthalten ist. In diesem Falle ist dann notwendig auch A_2 identisch mit B_2, die beiden Schnitte sind vollständig identisch, was wir in Zeichen durch $\alpha = \beta$ oder $\beta = \alpha$ andeuten.

Sind aber die beiden Klassen A_1, B_1 nicht identisch, so gibt es in der einen, z. B. in A_1, eine Zahl $a_1' = b_2'$, welche nicht in der anderen B_1 enthalten ist, und welche sich folglich in B_2 vorfindet; mithin sind gewiß alle in B_1 enthaltenen Zahlen b_1 kleiner als diese Zahl $a_1' = b_2'$, und folglich sind alle Zahlen b_1 auch in A_1 enthalten.

Ist nun 2. diese Zahl a_1' die einzige in A_1, welche nicht in B_1 enthalten ist, so ist jede andere in A_1 enthaltene Zahl a_1 in B_1 enthalten, und folglich kleiner als a_1', d. h. a_1' ist die größte unter allen Zahlen a_1, mithin wird der Schnitt (A_1, A_2) durch die rationale Zahl $\alpha = a_1' = b_2'$ hervorgebracht. Von dem anderen Schnitte (B_1, B_2) wissen wir schon, daß alle Zahlen b_1 in B_1 auch in A_1 enthalten und kleiner als die Zahl $a_1' = b_2'$ sind, welche in B_2 enthalten ist; jede andere in B_2 enthaltene Zahl b_2 muß aber größer als b_2' sein, weil sie sonst auch kleiner als a_1', also in A_1 und folglich auch in B_1 enthalten wäre; mithin ist b_2' die kleinste unter allen in B_2 enthaltenen Zahlen, und folglich wird auch der Schnitt (B_1, B_2) durch dieselbe rationale Zahl $\beta = b_2' = a_1' = \alpha$ hervorgebracht. Die beiden Schnitte sind daher nur unwesentlich verschieden.

Gibt es aber 3. in A_1 wenigstens zwei verschiedene Zahlen $a_1' = b_2'$ und $a_1'' = b_2''$, welche nicht in B_1 enthalten sind, so gibt es deren auch unendlich viele, weil alle die unendlich vielen zwischen

a_1' und a_1'' liegenden Zahlen (§ 1. II) offenbar in A_1, aber nicht in B_1 enthalten sind. In diesem Falle nennen wir die diesen beiden wesentlich verschiedenen Schnitten (A_1, A_2) und (B_1, B_2) entsprechenden Zahlen α und β ebenfalls verschieden voneinander, und zwar sagen wir, daß α größer als β, daß β kleiner als α ist, was wir in Zeichen sowohl durch $\alpha > \beta$, als durch $\beta < \alpha$ ausdrücken. Hierbei ist hervorzuheben, daß diese Definition vollständig mit der früheren zusammenfällt, wenn beide Zahlen α, β rational sind.

Die nun noch übrigen möglichen Fälle sind diese. Gibt es 4. in B_1 eine und nur eine Zahl $b_1' = a_2'$, welche nicht in A_1 enthalten ist, so sind die beiden Schnitte (A_1, A_2) und (B_1, B_2) nur unwesentlich verschieden und sie werden durch eine und dieselbe rationale Zahl $\alpha = a_2' = b_1' = \beta$ hervorgebracht. Gibt es aber 5. in B_1 mindestens zwei verschiedene Zahlen, welche nicht in A_1 enthalten sind, so ist $\beta > \alpha$, $\alpha < \beta$.

Da hiermit alle Fälle erschöpft sind, so ergibt sich, daß von zwei verschiedenen Zahlen notwendig die eine die größere, die andere die kleinere sein muß, was zwei Möglichkeiten enthält. Ein dritter Fall ist unmöglich. Dies lag zwar schon in der Wahl des Komparativs (größer, kleiner) zur Bezeichnung der Beziehung zwischen α, β; aber diese Wahl ist erst jetzt nachträglich gerechtfertigt. Gerade bei solchen Untersuchungen hat man sich auf das sorgfältigste zu hüten, daß man selbst bei dem besten Willen, ehrlich zu sein, durch eine voreilige Wahl von Ausdrücken, welche anderen schon entwickelten Vorstellungen entlehnt sind, sich nicht verleiten lasse, unerlaubte Übertragungen aus dem einen Gebiete in das andere vorzunehmen.

Betrachtet man nun noch einmal genau den Fall $\alpha > \beta$, so ergibt sich, daß die kleinere Zahl β, wenn sie rational ist, gewiß der Klasse A_1 angehört; da es nämlich in A_1 eine Zahl $a_1' = b_2'$ gibt, welche der Klasse B_2 angehört, so ist die Zahl β, mag sie die größte Zahl in B_1 oder die kleinste Zahl in B_2 sein, gewiß $\leqq a_1$ und folglich in A_1 enthalten. Ebenso ergibt sich aus $\alpha > \beta$, daß die größere Zahl α, wenn sie rational ist, gewiß der Klasse B_2 angehört, weil $\alpha \geqq a_1'$ ist. Vereinigt man beide Betrachtungen, so erhält man folgendes Resultat: Wird ein Schnitt (A_1, A_2) durch die Zahl α hervorgebracht, so gehört irgendeine rationale Zahl zu der

Klasse A_1 oder zu der Klasse A_2, je nachdem sie kleiner oder größer ist als α; ist die Zahl α selbst rational, so kann sie der einen oder der anderen Klasse angehören.

Hieraus ergibt sich endlich noch folgendes. Ist $\alpha > \beta$, gibt es also unendlich viele Zahlen in A_1, welche nicht in B_1 enthalten sind, so gibt es auch unendlich viele solche Zahlen, welche zugleich von α und von β verschieden sind; jede solche rationale Zahl c ist $< \alpha$, weil sie in A_1 enthalten ist, und sie ist zugleich $> \beta$, weil sie in B_2 enthalten ist.

§ 5.

Stetigkeit des Gebietes der reellen Zahlen.

Zufolge der eben festgesetzten Unterscheidungen bildet nun das System $\mathfrak{R}$ aller reellen Zahlen ein wohlgeordnetes Gebiet von einer Dimension; hiermit soll weiter nichts gesagt sein, als daß folgende Gesetze herrschen.

I. Ist $\alpha > \beta$, und $\beta > \gamma$, so ist auch $\alpha > \gamma$. Wir wollen sagen, daß die Zahl β zwischen den Zahlen α, γ liegt.

II. Sind α, γ zwei verschiedene Zahlen, so gibt es immer unendlich viele verschiedene Zahlen β, welche zwischen α, γ liegen.

III. Ist α eine bestimmte Zahl, so zerfallen alle Zahlen des Systems $\mathfrak{R}$ in zwei Klassen $\mathfrak{A}_1$ und $\mathfrak{A}_2$, deren jede unendlich viele Individuen enthält; die erste Klasse $\mathfrak{A}_1$ umfaßt alle die Zahlen α_1, welche $< \alpha$ sind, die zweite Klasse $\mathfrak{A}_2$ umfaßt alle die Zahlen α_2, welche $> \alpha$ sind; die Zahl α selbst kann nach Belieben der ersten oder der zweiten Klasse zugeteilt werden, und sie ist dann entsprechend die größte Zahl der ersten oder die kleinste Zahl der zweiten Klasse. In jedem Falle ist die Zerlegung des Systems $\mathfrak{R}$ in die beiden Klassen $\mathfrak{A}_1$, $\mathfrak{A}_2$ von der Art, daß jede Zahl der ersten Klasse $\mathfrak{A}_1$ kleiner als jede Zahl der zweiten Klasse $\mathfrak{A}_2$ ist, und wir sagen, daß diese Zerlegung durch die Zahl α hervorgebracht wird.

Der Kürze halber, und um den Leser nicht zu ermüden, unterdrücke ich die Beweise dieser Sätze, welche unmittelbar aus den Definitionen des vorhergehenden Paragraphen folgen.

Außer diesen Eigenschaften besitzt aber das Gebiet $\mathfrak{R}$ auch Stetigkeit, d. h. es gilt folgender Satz:

IV. Zerfällt das System $\mathfrak{R}$ aller reellen Zahlen in zwei Klassen $\mathfrak{A}_1$, $\mathfrak{A}_2$ von der Art, daß jede Zahl α_1 der Klasse $\mathfrak{A}_1$ kleiner ist als jede Zahl α_2 der Klasse $\mathfrak{A}_2$, so existiert eine und nur eine Zahl α, durch welche diese Zerlegung hervorgebracht wird.

Beweis. Durch die Zerlegung oder den Schnitt von $\mathfrak{R}$ in $\mathfrak{A}_1$ und $\mathfrak{A}_2$ ist zugleich ein Schnitt (A_1, A_2) des Systems R aller rationalen Zahlen gegeben, welcher dadurch definiert wird, daß A_1 alle rationalen Zahlen der Klasse $\mathfrak{A}_1$ und A_2 alle übrigen rationalen Zahlen, d. h. alle rationalen Zahlen der Klasse $\mathfrak{A}_2$ enthält. Es sei α die völlig bestimmte Zahl, welche diesen Schnitt (A_1, A_2) hervorbringt. Ist nun β irgendeine von α verschiedene Zahl, so gibt es immer unendlich viele rationale Zahlen c, welche zwischen α und β liegen. Ist $\beta < \alpha$, so ist $c < \alpha$; mithin gehört c der Klasse A_1 und folglich auch der Klasse $\mathfrak{A}_1$ an, und da zugleich $\beta < c$ ist, so gehört auch β derselben Klasse $\mathfrak{A}_1$ an, weil jede Zahl in $\mathfrak{A}_2$ größer ist als jede Zahl c in $\mathfrak{A}_1$. Ist aber $\beta > \alpha$, so ist $c > \alpha$; mithin gehört c der Klasse A_2 und folglich auch der Klasse $\mathfrak{A}_2$ an, und da zugleich $\beta > c$ ist, so gehört auch β derselben Klasse $\mathfrak{A}_2$ an, weil jede Zahl in $\mathfrak{A}_1$ kleiner ist als jede Zahl c in $\mathfrak{A}_2$. Mithin gehört jede von α verschiedene Zahl β der Klasse $\mathfrak{A}_1$ oder der Klasse $\mathfrak{A}_2$ an, je nachdem $\beta < \alpha$ oder $\beta > \alpha$ ist; folglich ist α selbst entweder die größte Zahl in $\mathfrak{A}_1$ oder die kleinste Zahl in $\mathfrak{A}_2$, d. h. α ist eine und offenbar die einzige Zahl, durch welche die Zerlegung von $\mathfrak{R}$ in die Klassen $\mathfrak{A}_1$, $\mathfrak{A}_2$ hervorgebracht wird, was zu beweisen war.

§ 6.

Rechnungen mit reellen Zahlen.

Um irgendeine Rechnung mit zwei reellen Zahlen α, β auf die Rechnungen mit rationalen Zahlen zurückzuführen, kommt es nur darauf an, aus den Schnitten (A_1, A_2) und (B_1, B_2), welche durch die Zahlen α und β im Systeme R hervorgebracht werden, den Schnitt (C_1, C_2) zu definieren, welcher dem Rechnungsresultate γ entsprechen soll. Ich beschränke mich hier auf die Durchführung des einfachsten Beispieles, der Addition.

Ist c irgendeine rationale Zahl, so nehme man sie in die Klasse C_1 auf, wenn es eine Zahl a_1 in A_1 und eine Zahl b_1 in B_1 von der Art gibt, daß ihre Summe $a_1 + b_1 \geqq c$ wird; alle anderen

rationalen Zahlen c nehme man in die Klasse C_2 auf. Diese Einteilung aller rationalen Zahlen in die beiden Klassen C_1, C_2 bildet offenbar einen Schnitt, weil jede Zahl c_1 in C_1 kleiner ist als jede Zahl c_2 in C_2. Sind nun beide Zahlen α, β rational, so ist jede in C_1 enthaltene Zahl $c_1 \leqq \alpha + \beta$, weil $a_1 \leqq \alpha$, $b_1 \leqq \beta$, also auch $a_1 + b_1 \leqq \alpha + \beta$ ist; wäre ferner eine in C_2 enthaltene Zahl $c_2 < \alpha + \beta$, also $\alpha + \beta = c_2 + p$, wo p eine positive rationale Zahl bedeutet, so wäre

$$c_2 = (\alpha - {}^1/_2 p) + (\beta - {}^1/_2 p),$$

was im Widerspruch mit der Definition der Zahl c_2 steht, weil $\alpha - {}^1/_2 p$ eine Zahl in A_1, und $\beta - {}^1/_2 p$ eine Zahl in B_1 ist; folglich ist jede in C_2 enthaltene Zahl $c_2 \geqq \alpha + \beta$. Mithin wird in diesem Falle der Schnitt (C_1, C_2) durch die Summe $\alpha + \beta$ hervorgebracht. Man verstößt daher nicht gegen die in der Arithmetik der rationalen Zahlen geltende Definition, wenn man in allen Fällen unter der Summe $\alpha + \beta$ von zwei beliebigen reellen Zahlen α, β diejenige Zahl γ versteht, durch welche der Schnitt (C_1, C_2) hervorgebracht wird. Ist ferner nur eine der beiden Zahlen α, β, z. B. α, rational, so überzeugt man sich leicht, daß es keinen Einfluß auf die Summe $\gamma = \alpha + \beta$ hat, ob man die Zahl α in die Klasse A_1 oder in die Klasse A_2 aufnimmt.

Ebenso wie die Addition lassen sich auch die übrigen Operationen der sogenannten Elementar-Arithmetik definieren, nämlich die Bildung der Differenzen, Produkte, Quotienten, Potenzen, Wurzeln, Logarithmen, und man gelangt auf diese Weise zu wirklichen Beweisen von Sätzen (wie z. B. $\sqrt{2} . \sqrt{3} = \sqrt{6}$), welche meines Wissens bisher nie bewiesen sind. Die Weitläufigkeiten, welche bei den Definitionen der komplizierteren Operationen zu befürchten sind, liegen teils in der Natur der Sache, zum größten Teil aber lassen sie sich vermeiden. Sehr nützlich ist in dieser Beziehung der Begriff eines Intervalls, d. h. eines Systems A von rationalen Zahlen, welches folgende charakteristische Eigenschaft besitzt: sind a und a' Zahlen des Systems A, so sind auch alle zwischen a und a' liegenden rationalen Zahlen in A enthalten. Das System R aller rationalen Zahlen, ebenso die beiden Klassen eines jeden Schnittes sind Intervalle. Gibt es aber eine rationale Zahl a_1, welche kleiner, und eine rationale Zahl a_2, welche größer ist, als jede Zahl des Intervalls A,

so heiße A ein endliches Intervall; es gibt dann offenbar unendlich viele Zahlen von derselben Beschaffenheit wie a_1, und unendlich viele Zahlen von derselben Beschaffenheit wie a_2; das ganze Gebiet R zerfällt in drei Stücke, A_1, A, A_2, und es treten zwei vollständig bestimmte rationale oder irrationale Zahlen α_1, α_2 auf, welche bzw. die untere und obere (oder die kleinere und größere) Grenze des Intervalls A genannt werden können; die untere Grenze α_1 ist durch den Schnitt bestimmt, bei welchem die erste Klasse durch das System A_1 gebildet wird, und die obere Grenze α_2 durch den Schnitt, bei welchem A_2 die zweite Klasse bildet. Von jeder rationalen oder irrationalen Zahl α, welche zwischen α_1 und α_2 liegt, mag gesagt werden, sie liege innerhalb des Intervalls A. Sind alle Zahlen eines Intervalls A auch Zahlen eines Intervalls B, so heiße A ein Stück von B.

Noch viel größere Weitläufigkeiten scheinen in Aussicht zu stehen, wenn man dazu übergehen will, die unzähligen Sätze der Arithmetik der rationalen Zahlen (wie z. B. den Satz $(a + b)c = ac + bc$) auf beliebige reelle Zahlen zu übertragen. Dem ist jedoch nicht so; man überzeugt sich bald, daß hier alles darauf ankommt, nachzuweisen, daß die arithmetischen Operationen selbst eine gewisse Stetigkeit besitzen. Was ich hiermit meine, will ich in die Form eines allgemeinen Satzes einkleiden:

„Ist die Zahl λ das Resultat einer mit den Zahlen α, β, γ ... angestellten Rechnung, und liegt λ innerhalb des Intervalls L, so lassen sich Intervalle A, B, C ... angeben, innerhalb deren die Zahlen α, β, γ ... liegen, und von der Art, daß das Resultat derselben Rechnung, in welcher die Zahlen α, β, γ ... durch beliebige Zahlen der Intervalle A, B, C ... ersetzt werden, jedesmal eine innerhalb des Intervalls L liegende Zahl wird.“ Die abschreckende Schwerfälligkeit aber, welche dem Ausspruche eines solchen Satzes anklebt, überzeugt uns, daß hier etwas geschehen muß, um der Sprache zu Hilfe zu kommen; dies wird in der Tat auf die vollkommenste Weise erreicht, wenn man die Begriffe der veränderlichen Größen, der Funktionen, der Grenzwerte einführt, und zwar wird es das Zweckmäßigste sein, schon die Definitionen der einfachsten arithmetischen Operationen auf diese Begriffe zu gründen, was hier jedoch nicht weiter ausgeführt werden kann.