## XV.

# Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen.

[Abhandlungen der Königlichen Gesellschaft der Wissenschaften zu Göttingen, Bd. 23, S. 1—23 (1878).]

Die neuen Prinzipien, durch welche ich zu einer ausnahmelosen und strengen Theorie der Ideale gelangt bin, habe ich zuerst vor sieben Jahren in der zweiten Auflage der Vorlesungen über Zahlentheorie von Dirichlet (§§ 159—170) entwickelt und neuerdings in dem Bulletin des sciences mathématiques et astronomiques (t. XI, p. 278; t. I (2e série), p. 17, 69, 144, 207) ausführlicher und in etwas veränderter Form dargestellt. Mit demselben Gegenstand hatte ich mich schon vorher, durch die große Entdeckung Kummers angeregt, eine lange Reihe von Jahren hindurch beschäftigt, wobei ich von einer ganz anderen Grundlage, nämlich von der Theorie der höheren Kongruenzen ausging; allein obgleich diese Untersuchungen mich dem erstrebten Ziele sehr nahe brachten, so konnte ich mich zu ihrer Veröffentlichung doch nicht entschließen, weil die so entstandene Theorie hauptsächlich an zwei Unvollkommenheiten leidet. Die eine besteht darin, daß die Untersuchung eines Gebietes von ganzen algebraischen Zahlen sich zunächst auf die Betrachtung einer bestimmten Zahl und der ihr entsprechenden Gleichung gründet, welche als Kongruenz aufgefaßt wird, und daß die so erhaltenen Definitionen der idealen Zahlen (oder vielmehr der Teilbarkeit durch die idealen Zahlen) zufolge dieser bestimmt gewählten Darstellungsform nicht von vornherein den Charakter der Invarianz erkennen lassen, welcher in Wahrheit diesen Begriffen zukommt; die zweite Unvollkommenheit dieser Begründungsart besteht darin, daß bisweilen eigentümliche Ausnahmefälle auftreten, welche eine besondere Behandlung verlangen. Meine neuere Theorie dagegen gründet sich ausschließlich auf solche Begriffe, wie die des Körpers,

der ganzen Zahl, des Ideals, zu deren Definition es gar keiner bestimmten Darstellungsform der Zahlen bedarf, und wie hierdurch der erstgenannte Mangel von selbst wegfällt, so bewährt sich die Kraft dieser äußerst einfachen Begriffe auch darin, daß bei dem Beweise der allgemeinen Gesetze der Teilbarkeit eine Unterscheidung mehrerer Fälle gar niemals mehr auftritt. Über den Zusammenhang zwischen beiden Begründungsarten habe ich in den Göttingischen gelehrten Anzeigen vom 20. September 1871 (S. 1488—1492) einige Bemerkungen und Sätze ohne Beweis mitgeteilt, und namentlich habe ich daselbst den Grund aufgedeckt, auf welchem das Auftreten der erwähnten eigentümlichen Ausnahmefälle beruht. Seitdem ist im Jahre 1874 eine Theorie der idealen Zahlen von Zolotareff erschienen, welche in russischer Sprache abgefaßt und unter dem Titel Théorie des nombres entiers complexes, avec une application au calcul intégral im Jahrbuch über die Fortschritte der Mathematik (Bd. 6, S. 117) angezeigt und kurz besprochen ist. Aus dieser Anzeige*) geht hervor, daß die Theorie von Zolotareff sich ebenfalls auf die Theorie der höheren Kongruenzen gründet, daß aber gerade die Behandlung der erwähnten Ausnahmefälle vorläufig ausgeschlossen und einer späteren Darstellung vorbehalten ist. Ich weiß nicht, ob diese in Aussicht gestellte Vervollständigung seitdem veröffentlicht worden ist; da aber der Zusammenhang zwischen den beiden Begründungsarten der allgemeinen Idealtheorie an sich ein hinreichendes Interesse besitzt, so erlaube ich mir, im folgenden die Beweise zu den in den Göttingischen gelehrten Anzeigen mitgeteilten Bemerkungen nachzuliefern. Hierbei muß ich sowohl meine Theorie der Ideale, als auch die Theorie der höheren Kongruenzen, von welcher ich früher in Borchardts Journal (Bd. 54, S. 1) eine gedrängte Darstellung gegeben habe, als bekannt voraussetzen; der Kürze halber werde ich diese Abhandlung über die Kongruenzen mit C., die zweite Auflage der Zahlentheorie von Dirichlet mit D., und die oben angeführte Abhandlung im Bulletin des sciences mathématiques mit B. zitieren.

*) Nur auf diese kann ich mich hier berufen; zwar habe ich das Originalwerk nach mehreren vergeblichen Versuchen, es mir im Buchhandel zu verschaffen, kürzlich durch die Güte des Herrn Prof. Wangerin geliehen erhalten, aber bei meiner Unkenntnis der russischen Sprache habe ich zu meinem großen Bedauern nur das Wenige verfolgen können, was schon aus dem Anblick der Formeln verständlich ist.

§ 1.

Es sei $\Omega$ ein endlicher Körper vom Grade $n$, und $\mathfrak{o}$ das Gebiet aller in $\Omega$ enthaltenen ganzen Zahlen, so gibt es immer eine aus $n$ voneinander unabhängigen ganzen Zahlen

$$\omega_1, \omega_2 \cdots \omega_n$$

bestehende Basis des Gebietes $\mathfrak{o}$, d. h. das System $\mathfrak{o}$ ist identisch mit dem Inbegriffe

$$[\omega_1, \omega_2 \cdots \omega_n]$$

aller Zahlen $\omega$ von der Form

$$\omega = h_1 \omega_1 + h_2 \omega_2 + \cdots + h_n \omega_n,$$

wo

$$h_1, h_2 \cdots h_n$$

willkürliche ganze rationale Zahlen bedeuten; die Diskriminante

$$\Delta(\omega_1, \omega_2 \cdots \omega_n) = \Delta(\Omega) = D,$$

welche von der Wahl der Basiszahlen $\omega_1, \omega_2 \cdots \omega_n$ unabhängig ist, heißt die Grundzahl oder die Diskriminante des Körpers $\Omega$ (D. §§ 159, 160, 162; B. §§ 13—18).

Ist nun $\theta$ eine bestimmte ganze Zahl des Körpers, so kann man

$$\begin{aligned}
1 &= c_1^0 \omega_1 + c_2^0 \omega_2 + \cdots + c_n^0 \omega_n \\
\theta &= c_1' \omega_1 + c_2' \omega_2 + \cdots + c_n' \omega_n \\
\theta^2 &= c_1'' \omega_1 + c_2'' \omega_2 + \cdots + c_n'' \omega_n \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
\theta^{n-1} &= c_1^{(n-1)} \omega_1 + c_2^{(n-1)} \omega_2 + \cdots + c_n^{(n-1)} \omega_n
\end{aligned}$$

setzen, wo die sämtlichen $n^2$ Koeffizienten oder Koordinaten $c$ ganze rationale Zahlen bedeuten, und es ist

$$\Delta(1, \theta, \theta^2 \cdots \theta^{n-1}) = Dk^2,$$

wo

$$k = \sum \pm c_1^0 c_2' \cdots c_n^{(n-1)}$$

eine ganze rationale Zahl ist; diese Zahl $k$, deren absoluter Wert von der Wahl der Basiszahlen $\omega_1, \omega_2 \cdots \omega_n$ unabhängig ist, soll im folgenden der Kürze halber der Index der ganzen Zahl $\theta$ genannt werden. Ist $k$, wie wir immer voraussetzen werden, von 0 verschieden, so sind die $n$ Zahlen

$$1, \theta, \theta^2 \cdots \theta^{n-1}$$

voneinander unabhängig (D. § 159; B. §§ 4, 15, 17) und $\theta$ ist die Wurzel einer irreduktiblen Gleichung $n^{\text{ten}}$ Grades

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

deren Koeffizienten $1, a_1, a_2 \cdots a_n$ ganze rationale Zahlen sind.

Bedeutet ferner $\varphi(t)$ jede beliebige Funktion der Variabelen $t$, — und ich bemerke ein für allemal, daß unter diesem Namen und unter einem Zeichen von der Form $\varphi(t)$, $f(t)\cdots$ in der gegenwärtigen Abhandlung ausschließlich eine ganze Funktion von $t$ verstanden werden soll, deren Koeffizienten ganze rationale Zahlen sind —, so bildet der Inbegriff $\mathfrak{o}'$ aller Zahlen von der Form

$$\omega' = \varphi(\theta)$$

eine sogenannte Ordnung (D. §§ 165, 166; B. § 23); alle diese Zahlen sind ganze Zahlen des Körpers $\Omega$ und folglich auch in $\mathfrak{o}$ enthalten. Offenbar ist es gestattet, nur solche Funktionen

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

zu betrachten, deren Grad kleiner als $n$ ist; denn wenn der Grad einer Funktion $\varphi_1(t)$ gleich $n$ oder größer ist, so liefert sie, durch die Funktion

$$F(t) = t^n + a_1 t^{n-1} + a_2 t^{n-2} + \cdots + a_{n-1} t + a_n$$

dividiert, einen Rest $\varphi(t)$ von niedrigerem Grade als $n$, und gleichzeitig ist $\varphi_1(\theta) = \varphi(\theta)$; mit Benutzung einer schon oben gebrauchten Bezeichnungsweise (B. § 3) kann man daher

$$\mathfrak{o}' = [1, \theta, \theta^2 \cdots \theta^{n-1}]$$

setzen. Außerdem ergibt sich aus der Irreduktibilität der Gleichung $F(\theta) = 0$, daß jede Zahl $\omega'$ nur auf eine einzige Weise in dieser letzteren Form $\varphi(\theta)$ darstellbar ist; doch werden wir uns im folgenden durchaus nicht immer auf diese Darstellungsform der Zahlen $\omega'$ beschränken, vielmehr auch Funktionen von beliebig hohem Grade zulassen.

Die sämtlichen Primzahlen $p$ — mit welchem Namen stets rationale, positive Primzahlen bezeichnet sein sollen — zerfallen nun, nachdem einmal eine bestimmte Zahl $\theta$ gewählt und der Darstellung zugrunde gelegt ist, in zwei verschiedene Arten; die erste Art besteht aus den unendlich vielen Primzahlen, welche in dem Index $k$ der Zahl $\theta$ nicht aufgehen; falls $k = \pm 1$ ist, gehören alle Primzahlen dieser ersten Art an, und $\mathfrak{o}'$ ist identisch mit $\mathfrak{o}$. Wenn aber $k^2 > 1$ ist, so gibt es eine endliche Anzahl von Primzahlen der zweiten Art, nämlich solchen, welche in $k$ aufgehen. Es wird sich im folgenden Paragraphen zeigen, daß die Zerlegung der Primzahlen $p$ der ersten Art, oder vielmehr die Zerlegung der ihnen entsprechenden

Hauptideale $\mathfrak{o}\,p$*) in Produkte aus lauter Primidealen sich vollständig zurückführen läßt auf die Zerlegung der Funktion $F(t)$ in ein Produkt aus lauter Primfunktionen in bezug auf den Modul $p$ (C. 6), während dies für Primzahlen der zweiten Art nicht in gleich einfacher Weise möglich ist. Dieser Untersuchung sind folgende Bemerkungen vorauszuschicken.

Es sei $p$ eine bestimmte Primzahl der ersten Art, also $k$ nicht teilbar durch $p$. In diesem Falle ist eine in $\mathfrak{o}'$ enthaltene Zahl

$$\omega' = x_0 + x_1\theta + x_2\theta^2 + \cdots + x_{n-1}\theta^{n-1}$$

nur dann durch $p$ teilbar (also von der Form $p\,\omega$, wo $\omega$ eine ganze, d. h. in $\mathfrak{o}$ enthaltene Zahl bedeutet), wenn alle Koeffizienten $x_0$, $x_1$, $x_2 \cdots x_{n-1}$ durch $p$ teilbar sind; denn setzt man

$$\begin{aligned}
h_1 &= c_1^0 x_0 + c_1' x_1 + c_1'' x_2 + \cdots + c_1^{(n-1)} x_{n-1}\\
h_2 &= c_2^0 x_0 + c_2' x_1 + c_2'' x_2 + \cdots + c_2^{(n-1)} x_{n-1}\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
h_n &= c_n^0 x_0 + c_n' x_1 + c_n'' x_2 + \cdots + c_n^{(n-1)} x_{n-1},
\end{aligned}$$

so ist

$$\omega' = h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n,$$

und wenn $\omega'$ durch $p$ teilbar sein soll, so muß (zufolge der Bedeutung von $\omega_1$, $\omega_2 \cdots \omega_n$) jede der Koordinaten $h_1$, $h_2 \cdots h_n$ durch $p$ teilbar sein; hieraus ergibt sich aber weiter, daß die Produkte $k\,x_0$, $k\,x_1$, $k\,x_2 \cdots k\,x_{n-1}$, und folglich auch die Koeffizienten $x_0$, $x_1$, $x_2 \cdots x_{n-1}$ sämtlich durch $p$ teilbar sein müssen, wie behauptet war. Denselben Satz kann man offenbar auch so aussprechen: ist eine Zahl $\omega'$ der Ordnung $\mathfrak{o}'$ teilbar durch eine Primzahl $p$ der ersten Art, so ist auch der Quotient $\omega'/p$ eine Zahl derselben Ordnung $\mathfrak{o}'$. Umgekehrt, wenn alle Koeffizienten $x_0$, $x_1$, $x_2 \cdots x_{n-1}$ durch $p$ teilbar sind, so ist selbstverständlich auch $\omega'$ durch $p$ teilbar. Es sind daher zwei Zahlen $\varphi_1(\theta)$ und $\varphi_2(\theta)$ der Ordnung $\mathfrak{o}'$ stets und nur dann einander kongruent nach dem Modul $p$, d. h. ihre Differenz $\varphi_1(\theta) - \varphi_2(\theta)$ ist teilbar durch $p$, wenn je zwei entsprechende Koeffizienten der beiden Funktionen $\varphi_1(t)$ und $\varphi_2(t)$ einander nach $p$ kongruent sind, d. h. in der Bezeichnungsweise der Theorie der höheren Kongruenzen, wenn

$$\varphi_1(t) \equiv \varphi_2(t) \pmod{p}$$

*) Diese Bezeichnung der Hauptideale ist zweckmäßiger als diejenige $\mathfrak{i}(p)$, welche ich früher (D. § 163) gebraucht habe.

ist (C. 1). Hierbei war aber vorausgesetzt, daß die Grade der Funktionen $\varphi_1(t)$, $\varphi_2(t)$ kleiner als $n$ waren; ist dies nicht der Fall, so erhält man durch Division mit $F(t)$ eine Identität von der Form

$$\varphi_1(t) - \varphi_2(t) = F(t)\psi(t) + \psi_1(t),$$

wo $\psi_1(t)$ von niedrigerem Grade als $n$ ist, und hieraus $\varphi_1(\theta) - \varphi_2(\theta) = \psi_1(\theta)$; soll nun

$$\varphi_1(\theta) \equiv \varphi_2(\theta) \pmod{p}$$

sein, so muß nach dem obigen $\psi_1(t) = p\,\psi_2(t)$, also

$$\varphi_1(t) - \varphi_2(t) = F(t)\psi(t) + p\,\psi_2(t)$$

sein; das Stattfinden einer solchen Identität bezeichnet man aber in der Theorie der höheren Kongruenzen durch

$$\varphi_1(t) - \varphi_2(t) \equiv F(t)\psi(t) \pmod{p}$$

oder noch kürzer (C. 7) durch

$$\varphi_1(t) \equiv \varphi_2(t) \pmod{p, F(t)}.$$

Umgekehrt leuchtet ein, daß aus dieser letzten Funktionenkongruenz auch wieder die Zahlenkongruenz

$$\varphi_1(\theta) \equiv \varphi_2(\theta) \pmod{p}$$

folgt; beide Kongruenzen sind daher gleichbedeutend. Mithin gibt es in $\mathfrak{o}'$ genau ebenso viele nach $p$ inkongruente Zahlen $\varphi(\theta)$, als es inkongruente Funktionen $\varphi(t)$ in bezug auf den Doppelmodul $p$, $F(t)$ gibt; da nun die Anzahl der letzteren $= p^n$ ist (C. 8), und da die Anzahl $(\mathfrak{o}, \mathfrak{o}\,p) = N(p)$ aller in $\mathfrak{o}$ enthaltenen, nach $p$ inkongruenten Zahlen genau ebenso groß ist (B. § 18; D. § 162), so ergibt sich das wichtige Resultat: jede Zahl $\omega$ des Gebietes $\mathfrak{o}$ ist mit einer Zahl $\omega' = \varphi(\theta)$ der Ordnung $\mathfrak{o}'$ kongruent nach dem Modul $p$.

Zu derselben Folgerung gelangt man unmittelbar auch durch folgende einfache Betrachtung. Aus den $n$ Relationen zwischen den Zahlen $1, \theta, \theta^2 \cdots \theta^{n-1}$ einerseits und den Zahlen $\omega_1, \omega_2 \cdots \omega_n$ andererseits geht hervor, daß die Produkte $k\,\omega_1, k\,\omega_2 \cdots k\,\omega_n$ und folglich auch alle Produkte von der Form $k\,\omega$, wo $\omega$ jede beliebige Zahl in $\mathfrak{o}$ bedeutet, in der Ordnung $\mathfrak{o}'$ enthalten sind; man kann daher $k\,\omega = \varphi(\theta)$ setzen. Da nun $k$ durch die Primzahl $p$ nicht teilbar ist, so kann man die ganze rationale Zahl $l$ so wählen, daß $k\,l \equiv 1 \pmod{p}$ wird, und hieraus folgt $\omega \equiv l\,k\,\omega \equiv l\,\varphi(\theta) \pmod{p}$; also ist $\omega$ wirklich mit einer Zahl $l\,\varphi(\theta)$ der Ordnung $\mathfrak{o}'$ kongruent nach dem Modul $p$.

Ganz anders verhält es sich dagegen, wenn $p$ eine Primzahl der zweiten Art ist; da in diesem Falle die Determinante $k$ durch $p$ teilbar ist, so kann man nach einem Satze, dessen sehr leichten Beweis ich hier wohl übergehen darf, $n$ ganze rationale Zahlen $x_0$, $x_1 \cdots x_{n-1}$, die nicht alle durch $p$ teilbar sind, so wählen, daß die oben mit $h_1$, $h_2 \cdots h_n$ bezeichneten Summen sämtlich durch $p$ teilbar werden; dann ist die entsprechende Zahl

$$\omega' = x_0 + x_1\theta + x_2\theta^2 + \cdots + x_{n-1}\theta^{n-1}$$

der Ordnung $\mathfrak{o}'$ wirklich teilbar durch $p$, obgleich ihre Koeffizienten $x_0$, $x_1 \cdots x_{n-1}$ nicht alle durch $p$ teilbar sind. Hieraus folgt sofort, daß die Anzahl $(\mathfrak{o}', \mathfrak{o}\,p)$ der in $\mathfrak{o}'$ enthaltenen, nach $p$ inkongruenten Zahlen kleiner als $p^n$ ist, und folglich gibt es in $\mathfrak{o}$ Zahlen $\omega$, welche mit keiner in $\mathfrak{o}'$ enthaltenen Zahl $\varphi(\theta)$ nach $p$ kongruent sind, d. h. es gibt Zahlklassen (mod. $p$) in $\mathfrak{o}$, für welche in $\mathfrak{o}'$ kein Repräsentant vorhanden ist. Die genaue Bestimmung der Anzahl $(\mathfrak{o}', \mathfrak{o}\,p)$ ist für unseren Hauptzweck nicht erforderlich [*)].

## § 2.

In diesem Paragraphen machen wir durchweg die Voraussetzung, daß $p$ eine Primzahl der ersten Art ist, und wir wollen beweisen, daß in diesem Falle die Theorie der höheren Kongruenzen ein einfaches Mittel gibt, um das Hauptideal $\mathfrak{o}\,p$ in seine Primfaktoren zu zerlegen. Dies geschieht dadurch, daß die Funktion $F(t)$, die wir kürzer auch durch $F$ bezeichnen werden, nach dem Modul $p$ als Produkt von lauter Primfunktionen $P(t)$ dargestellt wird (C. 6); der bequemeren Ausdrucksweise halber wollen wir, was erlaubt ist, jede Primfunktion $P$ so wählen, daß ihr höchster Koeffizient $= 1$ ist, woraus folgt, daß zwei inkongruente Primfunktionen auch immer relative Primfunktionen sein werden (C. 5). Durch Vereinigung aller einander kongruenten Faktoren in eine Potenz erhält man

$$F \equiv P_1^{e_1} P_2^{e_2} \cdots P_m^{e_m} \pmod{p},$$

wo $P_1$, $P_2 \cdots P_m$ die sämtlichen inkongruenten, in $F$ aufgehenden Primfunktionen bedeuten.

[*) Schon bei Zolotareff (Mélanges math. et astron. du Bulletin de l'academie, St. Petersburg, Bd. 5, 13./25. September 1877) findet man den Satz, daß die Ausnahmeprimzahlen eben diejenigen sind, wofür eine durch $p$ teilbare Zahl $\omega'$ in der Ordnung $\mathfrak{o}'$ vorkommt, worin nicht alle Koeffizienten durch $p$ teilbar sind. Zolotareff zeigt aber nicht, daß diese Primzahlen eben die Indexteiler sind.]

Ist nun $P$ eine beliebige dieser $m$ Primfunktionen, und $\varrho = P(\theta)$, so entspricht derselben ein bestimmtes Ideal $\mathfrak{p}$, welches wir als den größten gemeinschaftlichen Teiler der beiden Hauptideale $\mathfrak{o}\,p$ und $\mathfrak{o}\,\varrho$ definieren. Um die Eigenschaften dieses Ideals $\mathfrak{p}$ festzustellen, betrachten wir zunächst alle diejenigen in der Ordnung $\mathfrak{o}'$ enthaltenen Zahlen $\psi(\theta)$, welche durch $\mathfrak{p}$ teilbar (d. h. in $\mathfrak{p}$ enthalten) sind, und wir wollen beweisen, daß die Zahlenkongruenz

$$\psi(\theta) \equiv 0 \pmod{\mathfrak{p}} \tag{1}$$

völlig gleichbedeutend ist mit der Funktionenkongruenz

$$\psi(t) \equiv 0 \pmod{p, P}. \tag{2}$$

In der Tat, da das Ideal $\mathfrak{p}$ zufolge seiner Definition (D. § 163; B. § 19) der Inbegriff aller Zahlen von der Form

$$\varrho\,\alpha + p\,\beta$$

ist, wo $\alpha$, $\beta$ willkürliche Zahlen des Gebiets $\mathfrak{o}$ bedeuten, und da (nach § 1) jede Zahl $\alpha$ mit einer Zahl $\varphi(\theta)$ der Ordnung $\mathfrak{o}'$ kongruent ist nach dem Modul $p$, so folgt aus (1) eine Kongruenz von der Form

$$\psi(\theta) \equiv P(\theta)\,\varphi(\theta) \pmod{p};$$

hieraus ergibt sich aber (nach § 1) die Funktionenkongruenz

$$\psi(t) \equiv P(t)\,\varphi(t) \pmod{p, F},$$

also auch die Kongruenz (2), weil $F$ durch $P$ teilbar ist. Umgekehrt folgt aus (2) unmittelbar, daß $\psi(\theta)$ von der Form $\varrho\,\alpha + p\,\beta$, also $\equiv 0 \pmod{\mathfrak{p}}$ sein muß, womit die obige Behauptung bewiesen ist.

Mit Hilfe dieses Resultats kann man leicht die Norm des Ideals $\mathfrak{p}$, d. h. die Anzahl $(\mathfrak{o}, \mathfrak{p}) = N(\mathfrak{p})$ der in $\mathfrak{o}$ enthaltenen, nach $\mathfrak{p}$ inkongruenten Zahlen bestimmen. Sind nämlich $\alpha_1$, $\alpha_2$ zwei beliebige Zahlen in $\mathfrak{o}$, so gibt es (nach § 1) in $\mathfrak{o}'$ zwei Zahlen $\varphi_1(\theta)$, $\varphi_2(\theta)$, welche resp. den Zahlen $\alpha_1$, $\alpha_2$ nach $p$ kongruent sind, und da $p$ durch $\mathfrak{p}$ teilbar ist, so ist auch

$$\alpha_1 \equiv \varphi_1(\theta), \quad \alpha_2 \equiv \varphi_2(\theta) \pmod{\mathfrak{p}};$$

die beiden Zahlen $\alpha_1$, $\alpha_2$ sind daher stets und nur dann kongruent in bezug auf $\mathfrak{p}$, wenn

$$\varphi_1(\theta) \equiv \varphi_2(\theta) \pmod{\mathfrak{p}}$$

ist; diese Kongruenz ist aber nach dem obigen gleichbedeutend mit der Kongruenz

$$\varphi_1(t) \equiv \varphi_2(t) \pmod{p, P};$$

es gibt daher in $\mathfrak{o}$ genau ebenso viele inkongruente Zahlen $\alpha$ in bezug auf $\mathfrak{p}$, als es inkongruente Funktionen $\varphi(t)$ in bezug auf den Doppel-

modul $p$, $P$ gibt, und da die Anzahl der letzteren $= p^f$ ist, wo $f$ den Grad der Funktion $P$ bedeutet (C. 8), so erhalten wir

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

Ebenso leicht ergibt sich, daß $\mathfrak{p}$ ein Primideal ist. Da nämlich $f \geqq 1$, also $N(\mathfrak{p}) > 1$ ist, so ist $\mathfrak{p}$ jedenfalls von $\mathfrak{o}$ verschieden, und es braucht daher nur noch gezeigt zu werden, daß $\mathfrak{p}$ kein zusammengesetztes Ideal, d. h. kein Produkt von der Form $\mathfrak{a}_1 \mathfrak{a}_2$ ist, wo die Ideale $\mathfrak{a}_1$, $\mathfrak{a}_2$ beide von $\mathfrak{o}$ verschieden sind (D. § 163; B. § 25, 4°). Ein solches zusammengesetztes Ideal $\mathfrak{m} = \mathfrak{a}_1 \mathfrak{a}_2$ besitzt die charakteristische Eigenschaft, daß immer zwei durch $\mathfrak{m}$ nicht teilbare Zahlen $\alpha_1$, $\alpha_2$ existieren, deren Produkt $\alpha_1 \alpha_2$ durch $\mathfrak{m}$ teilbar ist; denn weil die Ideale $\mathfrak{a}_1$, $\mathfrak{a}_2$ beide von $\mathfrak{o}$ verschieden sind, so kann auch keines von ihnen durch ihr Produkt $\mathfrak{m} = \mathfrak{a}_1 \mathfrak{a}_2$ teilbar sein, und folglich gibt es eine durch $\mathfrak{a}_1$, aber nicht durch $\mathfrak{m}$ teilbare Zahl $\alpha_1$, und ebenso eine durch $\mathfrak{a}_2$, aber nicht durch $\mathfrak{m}$ teilbare Zahl $\alpha_2$, und offenbar ist $\alpha_1 \alpha_2$ teilbar durch $\mathfrak{m}$. Es wird daher $\mathfrak{p}$ gewiß ein Primideal sein, wenn wir beweisen können, daß ein Produkt $\alpha_1 \alpha_2$ nur dann durch $\mathfrak{p}$ teilbar ist, wenn wenigstens einer der Faktoren $\alpha_1$, $\alpha_2$ durch $\mathfrak{p}$ teilbar ist. Zu diesem Zweck setzen wir, wie oben,

$$\alpha_1 \equiv \varphi_1(\theta), \quad \alpha_2 \equiv \varphi_2(\theta) \pmod{\mathfrak{p}},$$

so ist

$$\alpha_1 \alpha_2 \equiv \varphi_1(\theta)\, \varphi_2(\theta) \pmod{\mathfrak{p}};$$

soll nun $\alpha_1 \alpha_2 \equiv 0 \pmod{\mathfrak{p}}$ sein, so muß auch

$$\varphi_1(\theta)\, \varphi_2(\theta) \equiv 0 \pmod{\mathfrak{p}},$$

mithin

$$\varphi_1(t)\, \varphi_2(t) \equiv 0 \pmod{p, P}$$

sein; da aber $P$ eine Primfunktion ist, so muß wenigstens eine der beiden Kongruenzen

$$\varphi_1(t) \equiv 0, \quad \varphi_2(t) \equiv 0 \pmod{p, P}$$

stattfinden (C. 6), also auch wenigstens eine der Kongruenzen

$$\varphi_1(\theta) \equiv 0, \quad \varphi_2(\theta) \equiv 0 \pmod{\mathfrak{p}},$$

d. h. wenigstens eine der beiden Zahlen $\alpha_1$, $\alpha_2$ muß $\equiv 0 \pmod{\mathfrak{p}}$ sein. Also ist $\mathfrak{p}$ ein Primideal; und zwar sagen wir (B. § 21), daß $\mathfrak{p}$ ein Primideal vom Grade $f$ ist, weil $N(\mathfrak{p}) = p^f$ ist.

Jetzt wollen wir beweisen, daß der Exponent $e$ der höchsten in $F$ aufgehenden Potenz von $P$ zugleich der Exponent der höchsten in $p$ aufgehenden Potenz des Primideals $\mathfrak{p}$ ist. In der Tat, wenn $F$ nach dem Modul $p$ durch $P^e$, aber nicht durch $P^{e+1}$ teilbar ist, so kann man

$$F \equiv S P^e \pmod{p}$$

setzen, wo $S$ nicht teilbar durch $P$ ist, woraus nach dem Obigen folgt, daß die Zahl

$$\sigma = S(\theta)$$

nicht durch $\mathfrak{p}$ teilbar ist. Da ferner $\mathfrak{p}$ der größte gemeinschaftliche Teiler der beiden Ideale $\mathfrak{o}\,p$ und $\mathfrak{o}\,\varrho$ ist, so können wir

$$\mathfrak{o}\,p = \mathfrak{p}\,\mathfrak{a}, \quad \mathfrak{o}\,\varrho = \mathfrak{p}\,\mathfrak{b}$$

setzen, wo $\mathfrak{a}$, $\mathfrak{b}$ relative Primideale bedeuten, und wir haben zu beweisen, daß $\mathfrak{p}^{e-1}$ die höchste in $\mathfrak{a}$ aufgehende Potenz von $\mathfrak{p}$ ist. Zu diesem Zwecke betrachten wir die Zahl

$$\eta = \sigma\,\varrho^{e-1} = S(\theta)\,P(\theta)^{e-1};$$

dieselbe kann nicht durch $p$ teilbar sein, weil der Grad der Funktion $S\,P^{e-1}$ kleiner als $n$, und weil ihr höchster Koeffizient $= 1$ ist; aber $\eta$ ist teilbar durch $\mathfrak{p}^{e-1}$, weil $\varrho$ durch $\mathfrak{p}$ teilbar ist. Vermöge der Kongruenz $F \equiv S\,P^e \pmod{p}$ ist nun das Produkt $\eta\,\varrho = \sigma\,\varrho^e$ teilbar durch $p$, also ist auch das Ideal $\eta\,\mathfrak{p}\,\mathfrak{b}$ teilbar durch $\mathfrak{p}\,\mathfrak{a}$, mithin $\eta\,\mathfrak{b}$ teilbar durch $\mathfrak{a}$, folglich $\eta$ teilbar durch $\mathfrak{a}$, weil $\mathfrak{a}$ und $\mathfrak{b}$ relative Primideale sind. Man kann daher

$$\mathfrak{o}\,\eta = \mathfrak{a}\,\mathfrak{c}$$

setzen, wo $\mathfrak{c}$ ein Ideal bedeutet, welches nicht durch $\mathfrak{p}$ teilbar ist*), weil sonst $\eta$ durch $\mathfrak{a}\,\mathfrak{p}$, also durch $p$ teilbar wäre, was nicht der Fall ist. Da nun $\eta$ durch $\mathfrak{p}^{e-1}$ teilbar ist, so muß auch $\mathfrak{a}$ durch $\mathfrak{p}^{e-1}$ teilbar sein. Wir haben jetzt nur noch zu zeigen, daß $\mathfrak{a}$ nicht durch $\mathfrak{p}^e$ teilbar ist. Da $e \geqq 1$ ist, so müßte, wenn $\mathfrak{a}$ durch $\mathfrak{p}^e$ teilbar wäre, jedenfalls $\mathfrak{a}$ durch $\mathfrak{p}$ selbst teilbar sein; sobald aber $\mathfrak{a}$ durch $\mathfrak{p}$ teilbar ist, kann $\mathfrak{b}$ nicht durch $\mathfrak{p}$ teilbar sein, und folglich ist dann $\varrho$ nicht teilbar durch $\mathfrak{p}^2$; da ferner $\sigma$ nicht durch $\mathfrak{p}$ teilbar ist, so ist in diesem Falle $\mathfrak{p}^{e-1}$ die höchste in der Zahl $\eta = \sigma\,\varrho^{e-1}$ aufgehende Potenz von $\mathfrak{p}$, und folglich kann das in $\eta$ aufgehende Ideal $\mathfrak{a}$ nicht durch $\mathfrak{p}^e$ teilbar sein, w. z. b. w.

Nachdem die Untersuchung für eine bestimmte in $F$ aufgehende Primfunktion $P$ und für das ihr entsprechende Primideal $\mathfrak{p}$ so weit geführt ist, wenden wir dieselbe auf alle in der Funktion

$$F \equiv P_1^{e_1}\,P_2^{e_2} \cdots P_m^{e_m} \pmod{p}$$

*) Es ist daher $\mathfrak{a}$ der größte gemeinschaftliche Teiler, und folglich $\eta\,\mathfrak{p}$ das kleinste gemeinschaftliche Vielfache der beiden Ideale $\mathfrak{o}\,p$ und $\mathfrak{o}\,\eta$, d. h. $\mathfrak{p}$ ist der Inbegriff aller Wurzeln $\pi$ der Kongruenz $\eta\,\pi \equiv 0 \pmod{p}$. Dies hätte auch als Definition des Ideals $\mathfrak{p}$ benutzt werden können.

aufgehenden, inkongruenten Primfunktionen

$$P_1,\ P_2 \cdots P_m$$

an, deren Grade wir resp. mit

$$f_1,\ f_2 \cdots f_m$$

bezeichnen; die diesen Funktionen entsprechenden Primideale

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

haben resp. dieselben Grade, d. h. es ist

$$N(\mathfrak{p}_1) = p^{f_1},\quad N(\mathfrak{p}_2) = p^{f_2} \cdots N(\mathfrak{p}_m) = p^{f_m},$$

und

$$\mathfrak{p}^{e_1},\ \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_m^{e_m}$$

sind die höchsten in $p$ aufgehenden Potenzen dieser Ideale. Diese $m$ Primideale sind verschieden voneinander; denn da z. B. $P_2$ nicht durch $P_1$ teilbar ist (mod. $p$), so ist die durch $\mathfrak{p}_2$ teilbare Zahl $P_2(\theta)$ nicht durch $\mathfrak{p}_1$ teilbar, und folglich sind $\mathfrak{p}_1$, $\mathfrak{p}_2$ verschiedene Primideale. Endlich bemerken wir, daß $p$ durch kein anderes Primideal teilbar sein kann; da nämlich

$$P_1(\theta)^{e_1} P_2(\theta)^{e_2} \cdots P_m(\theta)^{e_m} \equiv 0 \pmod{p}$$

ist, so muß ein in $p$ aufgehendes Primideal auch in einer der $m$ Zahlen $\varrho = P(\theta)$ aufgehen und folglich mit dem Primideal $\mathfrak{p}$ identisch sein, welches der größte gemeinschaftliche Teiler der beiden Ideale $\mathfrak{o}\,p$ und $\mathfrak{o}\,\varrho$ ist.

Aus allen diesem folgt (D. § 163; B. § 25), daß

$$\mathfrak{o}\,p = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_m^{e_m}$$

ist, und eine Bestätigung dieses Resultats ergibt sich durch die Betrachtung der Normen, wenn man berücksichtigt, daß

$$n = e_1 f_1 + e_2 f_2 + \cdots + e_m f_m$$

ist. Es ist somit folgender Satz bewiesen, den ich zuerst in den Göttingischen gelehrten Anzeigen vom 20. September 1871 ohne Beweis mitgeteilt habe:

I. Ist der Index $k$ der Zahl $\theta$, welche der irreduktiblen Gleichung $n^{\text{ten}}$ Grades $F(\theta) = 0$ genügt, nicht teilbar durch die Primzahl $p$, und ist

$$F \equiv P_1^{e_1} P_2^{e_2} \cdots P_m^{e_m} \pmod{p},$$

wo $P_1,\ P_2 \cdots P_m$ inkongruente Primfunktionen resp. vom Grade $f_1,\ f_2 \cdots f_m$ bedeuten, so ist

$$\mathfrak{o}\,p = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_m^{e_m},$$

wo $\mathfrak{p}_1, \mathfrak{p}_2 \cdots \mathfrak{p}_m$ voneinander verschiedene Primideale resp. vom Grade $f_1, f_2 \cdots f_m$ sind, und zwar entspricht je einer Primfunktion $P$ ein bestimmtes Primideal $\mathfrak{p}$ in der Weise, daß $\mathfrak{p}$ der größte gemeinschaftliche Teiler der beiden Ideale $\mathfrak{o}p$ und $\mathfrak{o}P(\theta)$ ist.

§ 3.

Aus diesem Satze geht hervor, daß man bei Zugrundelegung einer bestimmten ganzen Zahl $\theta$ des Körpers $\Omega$, welche zur Darstellung von unendlich vielen ganzen Zahlen $\varphi(\theta)$ dient, mit voller Sicherheit die Zerlegung aller derjenigen Primzahlen $p$ findet, welche nicht in dem Index $k$ dieser Zahl $\theta$ aufgehen; es ist daher von großer Wichtigkeit zu wissen, ob eine Primzahl $p$ in dem Index $k$ aufgeht oder nicht. Sobald freilich eine Basis $\omega_1, \omega_2 \cdots \omega_n$ des Gebiets $\mathfrak{o}$, oder auch nur die Grundzahl $D$ des Körpers $\Omega$ bekannt ist, erledigt sich diese Frage sehr leicht, weil hieraus $k$ direkt gefunden werden kann; denn aus den Koeffizienten der Gleichung $F(\theta) = 0$ läßt sich ihre Diskriminante

$$\Delta(1, \theta, \theta^2 \cdots \theta^{n-1}) = (-1)^{\frac{1}{2}n(n-1)} N(F'(\theta)) = Dk^2,$$

und hieraus durch Division mit $D$ das Quadrat des Index $k$ bestimmen. Bei den meisten Untersuchungen liegt aber die Sache ganz anders, nämlich so, daß nur die Gleichung $F(\theta) = 0$, nicht aber die Grundzahl $D$ des ihr entsprechenden Körpers $\Omega$ gegeben ist; es kommt darauf an zu entscheiden, ob eine bestimmte Primzahl $p$ in dem noch unbekannten Index $k$ der Zahl $\theta$ aufgeht oder nicht. Dies gelingt nun in der Tat, wie wir jetzt zeigen wollen, mit Hilfe der Theorie der höheren Kongruenzen, und zwar hängt die Entscheidung, wenn wir die früheren Bezeichnungen beibehalten, wesentlich von der Beschaffenheit der Funktion $M$ ab, welche in der Identität

$$F = P_1^{e_1} P_2^{e_1} \cdots P_m^{e_m} - pM$$

auftritt. Dies ergibt sich aus den beiden folgenden Sätzen.

II. Ist der Index $k$ der Zahl $\theta$ nicht teilbar durch $p$, so kann $M$ nach dem Modul $p$ durch keine Primfunktion $P$ teilbar sein, deren Quadrat in $F$ aufgeht.

Zum Beweise dürfen wir alle Folgerungen benutzen, welche im vorigen Paragraphen aus der Annahme gezogen sind, daß $k$ nicht

durch $p$ teilbar ist. Indem wir alle dort gebrauchten Bezeichnungen beibehalten, setzen wir $F \equiv S P^e \pmod{p}$, also

$$F = S P^e - p M,$$

und nehmen an, es sei $e \geqq 2$; dann ist $p$ teilbar durch $\mathfrak{p}^2$, folglich $\mathfrak{a}$ teilbar durch $\mathfrak{p}$, mithin $\mathfrak{b}$ nicht teilbar durch $\mathfrak{p}$. Es ist daher $\mathfrak{p}^e$ die höchste in der Zahl

$$S(\theta)\, P(\theta)^e = p M(\theta)$$

aufgehende Potenz von $\mathfrak{p}$, und da $p$ durch $\mathfrak{p}^e$ teilbar ist, so kann $M(\theta)$ nicht durch $\mathfrak{p}$ teilbar sein, und folglich kann die Funktion $M$ auch nicht $\equiv 0$ (modd. $p$, $P$) sein, w. z. b. w.

Auch ohne Benutzung der im vorigen Paragraphen gewonnenen Resultate läßt sich derselbe Satz leicht in der folgenden indirekten, aber vollständig äquivalenten Form beweisen:

Ist $F$ nach dem Modul $p$ teilbar durch das Quadrat einer Primfunktion $P$, also

$$F = S P^e - p M,$$

wo $e \geqq 2$, und ist $M$ teilbar durch $P$, so muß der Index $k$ der Zahl $\theta$ durch die Primzahl $p$ teilbar sein.

Behalten die Buchstaben $\varrho$, $\sigma$, $\eta$ dieselbe Bedeutung, wie im vorigen Paragraphen, setzen wir also

$$\varrho = P(\theta), \quad \sigma = S(\theta), \quad \eta = \sigma \varrho^{e-1},$$

so wird (nach § 1) der Beweis unseres Satzes geführt sein, wenn wir zeigen, daß unter den jetzigen Annahmen die Zahl $\eta = S(\theta)\, P(\theta)^{e-1}$ durch $p$ teilbar sein muß; denn die Funktion $S P^{e-1}$ ist von niedrigerem Grade als $n$ und auch nicht $\equiv 0 \pmod{p}$. Die Zahl $\eta$ wird ferner gewiß durch $p$ teilbar sein, wenn bewiesen wird, daß alle in $p$ aufgehenden Potenzen von Primidealen auch in $\eta$ aufgehen (D. § 163, B. § 25). Zu diesem Zweck setzen wir

$$\mu = M(\theta)$$

und betrachten die Gleichung

$$\sigma \varrho^e = \eta \varrho = p \mu.$$

Ist nun $\mathfrak{p}$ ein in $p$, aber nicht in $\varrho$ aufgehendes Primideal, so folgt aus $\eta \varrho = p \mu$ unmittelbar, daß $\eta$ durch die höchste in $p$ aufgehende Potenz von $\mathfrak{p}$ teilbar ist. Ist aber $\mathfrak{p}$ ein in $p$ und gleichzeitig in $\varrho$ aufgehendes Primideal, so ergibt sich folgendes. Da $S$ und $P$ relative

Primfunktionen sind, so existieren zwei Funktionen $U$, $V$, welche der Kongruenz

$$S\,U + P\,V \equiv 1 \pmod{p}$$

genügen (C. 4); hieraus ergeben sich die Zahlenkongruenzen

$$\sigma\,U(\theta) + \varrho\,V(\theta) \equiv 1 \pmod{p}$$
$$\sigma\,U(\theta) \equiv 1 \pmod{\mathfrak{p}},$$

und folglich ist $\sigma$ nicht teilbar durch $\mathfrak{p}$. Sind daher $\mathfrak{p}^h$, $\mathfrak{p}^r$, $\mathfrak{p}^m$ die höchsten resp. in $p$, $\varrho$, $\mu$ aufgehenden Potenzen von $\mathfrak{p}$, so folgt aus $\sigma\,\varrho^e = p\,\mu$ und $\eta = \sigma\,\varrho^{e-1}$, daß

$$e\,r = h + m,$$

und daß der Exponent der höchsten in $\eta$ aufgehenden Potenz von $\mathfrak{p}$ gleich

$$(e-1)\,r = h + m - r$$

ist; um daher wieder zu beweisen, daß $\eta$ durch $\mathfrak{p}^h$ teilbar ist, brauchen wir nur noch zu zeigen, daß

$$m \geqq r$$

ist. Hierbei unterscheiden wir zwei Fälle. Ist erstens $r \geqq h$, so verwerten wir die erste Annahme unseres Satzes, derzufolge $e \geqq 2$ ist; hieraus folgt in der Tat $h + m = e\,r \geqq 2\,r$, mithin $m - r \geqq r - h \geqq 0$, wie behauptet war. Ist aber zweitens $r \leqq h$, so benutzen wir die zweite Annahme unseres Satzes, derzufolge $M \equiv 0$ (modd. $p, P$), d. h. $M \equiv P\,T \pmod{p}$, also $\mu \equiv \varrho\,T(\theta) \pmod{p}$ ist; da nun sowohl $\varrho$, als auch $p$ durch $\mathfrak{p}^r$ teilbar ist, so folgt aus dieser Kongruenz, daß auch $\mu$ durch $\mathfrak{p}^r$ teilbar, d. h. daß $m \geqq r$ ist, w. z. b. w.

Nachdem der Satz II auf zwei verschiedene Arten bewiesen ist, behaupten wir auch die Richtigkeit des umgekehrten Satzes:

III. Ist $M$ durch keine solche Primfunktion $P$ teilbar (mod. $p$), deren Quadrat zugleich in $F$ aufgeht, so ist der Index $k$ der Zahl $\theta$ nicht teilbar durch $p$.

Derselbe Satz kann offenbar auch in der folgenden Form ausgesprochen werden:

Ist der Index $k$ der Zahl $\theta$ teilbar durch die Primzahl $p$, so gibt es eine in $M$ aufgehende Primfunktion $P$, deren Quadrat zugleich in $F$ aufgeht (mod. $p$).

Dem Beweise legen wir die letztere Form zugrunde, weil die Annahme, daß $k$ durch $p$ teilbar ist, eine leichtere Verwertung gestattet, insofern aus ihr (nach § 1) die Existenz einer durch $p$ teilbaren Zahl

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

folgt, deren Koeffizienten $x_0, x_1, x_2 \cdots x_{n-1}$ nicht alle durch $p$ teilbar sind. Bezeichnet man nun mit $A$ den größten gemeinschaftlichen Teiler der beiden Funktionen $\varphi(t)$ und $F$ nach dem Modul $p$, so ist der Grad von $A$ kleiner als $n$, weil $\varphi$ von niedrigerem Grade als $n$ und auch nicht $\equiv 0 \pmod{p}$ ist; setzt man daher

$$F = AB - pM,$$

so ist $B$ keine Konstante. Nun existieren zwei Funktionen $\varphi_1$, $\varphi_2$, welche der Kongruenz

$$\varphi(t)\,\varphi_1(t) + F(t)\,\varphi_2(t) \equiv A(t) \pmod{p}$$

genügen (C. 4); hieraus ergibt sich, daß die Zahl $A(\theta)$ ebenfalls durch $p$ teilbar ist*) und folglich einer Gleichung von der Form

$$A(\theta)^s + p h_1 A(\theta)^{s-1} + p^2 h_2 A(\theta)^{s-2} + \cdots + p^s h_s = 0$$

genügt, wo $h_1, h_2 \cdots h_s$ ganze rationale Zahlen bedeuten (D. § 160; B. § 13). Da die Gleichung $F(\theta) = 0$ irreduktibel ist, so ergibt sich hieraus eine in bezug auf die Variable $t$ identische Gleichung von der Form

$$A^s + p h_1 A^{s-1} + p^2 h_2 A^{s-2} + \cdots + p^s h_s = F G,$$

also auch die Kongruenz

$$A^s \equiv 0 \pmod{p, F};$$

mithin muß die Funktion $A$ durch jede in $F$ aufgehende Primfunktion nach dem Modul $p$ teilbar sein (C. 5 und 6). Multipliziert man ferner die obige Gleichung, welcher die Zahl $A(\theta)$ genügt, mit $B(\theta)^s$, und bedenkt, daß $A(\theta)\,B(\theta) = pM(\theta)$ ist, so erhält man

$$M(\theta)^s + h_1 M(\theta)^{s-1} B(\theta) + h_2 M(\theta)^{s-2} B(\theta)^2 + \cdots + h_s B(\theta)^s = 0,$$

und hieraus eine Identität von der Form

$$M^s + h_1 M^{s-1} B + h_2 M^{s-2} B^2 + \cdots + h_s B^s = FH;$$

da nun $F \equiv 0 \pmod{p, B}$, so ergibt sich

$$M^s \equiv 0 \pmod{p, B},$$

und folglich ist die Funktion $M$ durch jede in $B$ aufgehende Primfunktion teilbar nach dem Modul $p$. Oben ist aber gezeigt, daß $B$ keine Konstante ist, mithin gibt es wenigstens eine in $B$ aufgehende

*) In ähnlicher Weise kann man leicht zeigen, daß das Kriterium für die Teilbarkeit einer Zahl $\varphi(\theta)$ durch $p$ in der Kongruenz $\varphi(t) \equiv 0 \pmod{p, K}$ besteht, wo $K$ einen völlig bestimmten Teiler der Funktion $F$ nach dem Modul $p$ bedeutet.

Primfunktion $P$, und diese muß folglich auch in $M$ aufgehen. Da ferner $P$ in $F$ aufgeht, weil $F$ durch $B$ teilbar ist, und da oben gezeigt ist, daß jede in $F$ aufgehende Primfunktion auch in $A$ aufgeht, so geht $P$ ebenfalls in $A$ auf, und folglich ist $F$ teilbar durch $P^2$, weil $F \equiv A\,B \pmod{p}$ ist. Wir haben mithin wirklich gezeigt, daß es eine in $M$ aufgehende Primfunktion $P$ gibt, deren Quadrat zugleich in $F$ aufgeht, w. z. b. w.

Durch die Sätze II und III ist nun in der Tat die Entscheidung der Frage, ob der Index $k$ der Zahl $\theta$ durch die Primzahl $p$ teilbar ist, vollständig zurückgeführt auf die Zerlegung

$$F = P_1^{e_1} P_2^{e_2} \cdots P_m^{e_m} - p\,M,$$

durch welche die Funktion $F$ als Produkt von lauter Primfunktionen nach dem Modul $p$ dargestellt wird. Zeigt es sich, daß $F$ durch kein Quadrat einer Primfunktion teilbar ist, daß also alle Exponenten $e_1, e_2 \cdots e_m = 1$ sind*), oder zeigt es sich, daß keine derjenigen Primfunktionen, deren Quadrate in $F$ aufgehen, in $M$ aufgeht, so ist $k$ nicht durch $p$ teilbar, und es gilt der Satz I des § 2. Gibt es aber eine in $M$ aufgehende Primfunktion, deren Quadrat zugleich in $F$ aufgeht, so ist $k$ teilbar durch $p$, und aus dem zweiten Beweise des Satzes II geht leicht hervor, daß dann die Zerlegung des Ideals $\mathfrak{o}\,p$ in Primfaktoren eine andere ist, als die im Satz I behauptete.

Diesem Resultat fügen wir noch folgende Bemerkung hinzu. Sind die Funktionen $R_1, R_2 \cdots R_m$ resp. kongruent den Funktionen $P_1, P_2 \cdots P_m$, so sind sie ebenfalls Primfunktionen, und es wird

$$F = R_1^{e_1} R_2^{e_2} \cdots R_m^{e_m} - p\,N,$$

wo die Funktion $N$ durchaus nicht $\equiv M \pmod{p}$ zu sein braucht. Da aber die Teilbarkeit des Index $k$ der Zahl $\theta$ durch $p$ von dieser Auswahl der Primfunktionen gänzlich unabhängig ist, so muß man schließen, daß die Eigenschaft der Funktion $M$, welche für diese Frage allein entscheidend ist, auch für jede Funktion $N$ bestehen bleibt. Dies ließe sich leicht durch die Rechnung unmittelbar bestätigen; bezeichnet man mit $Q$ das Produkt aller derjenigen in $F$ aufgehenden Primfunktionen, deren Quadrate in $F$ nicht aufgehen, so kann man durch geeignete Wahl der Funktionen $R_1, R_2 \cdots R_m$ stets zu einer Funktion $N$ gelangen, die relative Primfunktion zu $Q$

*) Dies wird stets und nur dann der Fall sein, wenn die Diskriminante $\Delta(1, \theta, \theta^2 \cdots \theta^{n-1})$ der Gleichung $F(\theta) = 0$ nicht durch $p$ teilbar ist.

ist; aber sobald $M$ durch eine Primfunktion $P$ teilbar ist, deren Quadrat in $F$ aufgeht, so zeigt die Rechnung, daß auch jede Funktion $N$ durch $P$ teilbar ist*).

§ 4.

In den zuerst von Kummer behandelten Zahlengebieten $\mathfrak{o}$, welche aus einer primitiven Wurzel $\theta$ der Gleichung $\theta^m = 1$ entspringen, tritt der glückliche Umstand auf, daß die Potenzen $1, \theta, \theta^2 \cdots \theta^{n-1}$, wo $n = \varphi(m)$, eine Basis des Gebietes $\mathfrak{o}$ bilden, und daß folglich der Index $k$ der Zahl $\theta$, welche der ganzen Untersuchung zugrunde gelegt wird, stets $= 1$ ist. Bei der allgemeinen Untersuchung eines beliebigen endlichen Körpers $\Omega$ und des Gebietes $\mathfrak{o}$, welches aus allen in $\Omega$ enthaltenen ganzen Zahlen besteht, erkannte ich zwar sehr bald, daß derselbe einfache Fall nur ausnahmeweise auftritt, aber ich hielt es doch lange Zeit für sehr wahrscheinlich, daß für jede gegebene Primzahl $p$ sich eine ganze Zahl $\theta$ des Körpers $\Omega$ würde finden lassen, deren Index nicht durch $p$ teilbar wäre, und mit deren Hilfe es folglich gelingen würde, die Bestimmung der Idealfaktoren von $p$ auf die Theorie der höheren Kongruenzen zurückzuführen. Da aber alle meine Versuche, die Existenz einer solchen Zahl $\theta$ nachzuweisen, fruchtlos blieben, so entschloß ich mich endlich, wo möglich die Unrichtigkeit dieser Vermutung darzutun, und zu diesem Ziele gelangte ich, wie ich schon in den Göttingischen gelehrten Anzeigen vom 20. September 1871 angedeutet

*) Hiernach beschränkt sich die Idealtheorie von Zolotareff auf den Fall, daß der Index $k$ nicht durch $p$ teilbar ist. Dies scheint wenigstens aus folgenden Worten hervorzugehen, welche sich in der oben erwähnten Anzeige finden (Jahrbuch über die Fortschritte der Mathematik, Bd. 6): „Um die Theorie in ihrer einfachsten Gestalt darzustellen, nimmt der Verfasser an, daß $F_1(x)$ durch keine der Funktionen $V$, $V_1$, $V_2 \cdots$ teilbar ist. Ist diese Bedingung nicht erfüllt, so kann man für einen gegebenen Modul $p$ die Gleichung $F(x) = 0$ derart transformieren, daß jene Annahme erfüllt ist. Die Auseinandersetzung jener Transformation behält sich der Verfasser für eine andere Gelegenheit vor.“ — Da es nach meinen Untersuchungen (vgl. § 5 dieser Abhandlung) Körper gibt, in welchen die Indizes aller ganzen Zahlen $\theta$ durch dieselbe Primzahl $p$ teilbar sind, und folglich auch alle Gleichungen $F(\theta) = 0$ diejenige störende Eigenschaft besitzen, welche sich der unmittelbaren Anwendung der Theorie von Zolotareff widersetzt, so vermute ich, daß in den eben zitierten Worten der Anzeige ein Mißverständnis obwaltet. Wahrscheinlich wird die von dem Verfasser beabsichtigte Vervollständigung seiner Theorie sich auf ähnliche Betrachtungen stützen, wie diejenigen, welche in der Theorie der idealen Zahlen von Selling entwickelt sind (Schlömilchs Zeitschrift, Bd. 10, S. 12ff.).

habe, durch die Betrachtungen, welche den Gegenstand dieses und des folgenden Paragraphen bilden.

Es sei $p$ eine bestimmte Primzahl, und $\mathfrak{p}_1, \mathfrak{p}_2 \cdots \mathfrak{p}_m$ seien die sämtlichen voneinander verschiedenen Primideale, welche in $p$ aufgehen; ihre Grade wollen wir mit $f_1, f_2 \cdots f_m$ bezeichnen, so daß z. B. $N(\mathfrak{p}_1) = p^{f_1}$ ist. Existiert nun eine ganze Zahl $\theta$ in $\Omega$, deren Index $k$ nicht durch $p$ teilbar ist, so folgt aus dem Satze I in § 2, daß es in bezug auf den Modul $p$ auch $m$ inkongruente Primfunktionen $P_1, P_2 \cdots P_m$ gibt, deren Grade resp. gleich $f_1, f_2 \cdots f_m$ sind. Es ist nun von der größten Wichtigkeit für unsere Untersuchung, daß diese Folgerung sich umkehren läßt, daß also folgender Satz besteht:

IV. Sind $f_1, f_2 \cdots f_m$ die Grade der sämtlichen verschiedenen, in der Primzahl $p$ aufgehenden Primideale $\mathfrak{p}_1$, $\mathfrak{p}_2 \cdots \mathfrak{p}_m$, und gibt es $m$ nach dem Modul $p$ inkongruente Primfunktionen $P_1, P_2 \cdots P_m$ resp. vom Grade $f_1, f_2 \cdots f_m$, so existiert in $\Omega$ eine ganze Zahl $\theta$, deren Index $k$ nicht durch $p$ teilbar ist.

Dem Beweise dieses Satzes schicken wir aber zunächst einige Betrachtungen voraus, welche zum Teil von den Voraussetzungen desselben unabhängig sind.

Es sei $\mathfrak{p}$ irgend ein in $p$ aufgehendes Primideal vom Grade $f$, so genügen (D. § 163; B. § 28, 3°) alle ganzen Zahlen $\omega$ des Körpers $\Omega$ der Kongruenz

$$\omega^{p^f} - \omega \equiv 0 \pmod{\mathfrak{p}};$$

bedeutet nun $t$ wieder eine Variable, so ist die Funktion

$$t^{p^f} - t$$

nach dem Modul $p$ kongruent dem Produkte aus allen inkongruenten Primfunktionen, deren Grade Divisoren der Zahl $f$ sind (C. 19); unter diesen wähle man nach Belieben eine solche Primfunktion $P$, deren Grad $= f$ ist; dies ist stets möglich, da es immer mindestens eine solche Funktion gibt (C. 20). Da nun

$$t^{p^f} - t \equiv P(t)\, H(t) \pmod{p},$$

also auch

$$\omega^{p^f} - \omega \equiv P(\omega)\, H(\omega) \pmod{p},$$

und da $p$ durch $\mathfrak{p}$ teilbar ist, so folgt, daß jede in $\mathfrak{o}$ enthaltene Zahl $\omega$ der Kongruenz

$$P(\omega)\, H(\omega) \equiv 0 \pmod{\mathfrak{p}}$$

genügt; mithin ist die Anzahl ihrer nach $\mathfrak{p}$ inkongruenten Wurzeln $= (\mathfrak{o}, \mathfrak{p}) = N(\mathfrak{p}) = p^f$, also genau so groß, wie ihr Grad. Durch

dieselben einfachen Schlüsse, welche in der rationalen Zahlentheorie zu einem ähnlichen Zwecke angewendet werden (D. § 26), kann man nun leicht beweisen, was ich der Kürze halber hier übergehe, daß in dem Zahlengebiete $o$ eine Kongruenz $r^{\text{ten}}$ Grades, deren Modul ein Primideal dieses Gebietes ist, niemals mehr als $r$ inkongruente Wurzeln haben kann, und hieraus folgt für unseren Fall, daß die Kongruenz $H(\omega) \equiv 0 \pmod{\mathfrak{p}}$ höchstens $(p^f - f)$ inkongruente Wurzeln besitzt, und daß folglich die Repräsentanten $\omega$ der $f$ übrigen Zahlklassen notwendig der Kongruenz $P(\omega) \equiv 0 \pmod{\mathfrak{p}}$ genügen müssen. Für unseren Zweck reicht aber schon die Gewißheit aus, daß diese Kongruenz wenigstens eine Wurzel hat. Es sei $\alpha$ eine bestimmte solche Wurzel, also

$$P(\alpha) \equiv 0 \pmod{\mathfrak{p}};$$

wir betrachten nun alle Zahlen von der Form $\varphi(\alpha)$ und wollen beweisen, daß die Kongruenz

$$\varphi(\alpha) \equiv 0 \pmod{\mathfrak{p}}$$

mit der Funktionenkongruenz

$$\varphi(t) \equiv 0 \pmod{p, P}$$

gleichbedeutend ist. In der Tat, wenn die letztere stattfindet, wenn also

$$\varphi(t) \equiv P(t)\,\psi(t) \pmod{p}$$

ist, so folgt auch

$$\varphi(\alpha) \equiv P(\alpha)\,\psi(\alpha) \pmod{p},$$

und da die beiden Zahlen $p$ und $P(\alpha)$ durch $\mathfrak{p}$ teilbar sind, so ist auch $\varphi(\alpha) \equiv 0 \pmod{\mathfrak{p}}$; ist aber zweitens $\varphi(t)$ nicht teilbar durch die Primfunktion $P(t)$, so sind $\varphi(t)$ und $P(t)$ relative Primfunktionen, und folglich existieren zwei Funktionen $\varphi_1(t)$, $\varphi_2(t)$, welche der Kongruenz

$$\varphi(t)\,\varphi_1(t) + P(t)\,\varphi_2(t) \equiv 1 \pmod{p}$$

genügen (C. 5); dann ist auch

$$\varphi(\alpha)\,\varphi_1(\alpha) + P(\alpha)\,\varphi_2(\alpha) \equiv 1 \pmod{p},$$

und da $p$ und $P(\alpha)$ durch $\mathfrak{p}$ teilbar sind, so ist

$$\varphi(\alpha)\,\varphi_1(\alpha) \equiv 1 \pmod{\mathfrak{p}},$$

und folglich ist in diesem Falle $\varphi(\alpha)$ nicht $\equiv 0 \pmod{\mathfrak{p}}$. Hiermit ist unsere obige Behauptung vollständig bewiesen.

Für den Fall, daß $p$ durch $\mathfrak{p}^2$ teilbar ist, wollen wir ferner die Wurzel $\alpha$ der Kongruenz $P(\alpha) \equiv 0 \pmod{\mathfrak{p}}$ so wählen, daß die Zahl $P(\alpha)$ nicht durch $\mathfrak{p}^2$ teilbar wird. Dies ist stets möglich; ist

nämlich $\alpha$ eine Wurzel der Kongruenz $P(\alpha) \equiv 0 \pmod{\mathfrak{p}^2}$, so wähle man nach Belieben eine durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbare Zahl $\lambda$, und setze $\alpha' = \alpha + \lambda$, so ist

$P(\alpha') = P(\alpha) + \lambda P'(\alpha) + \lambda^2 P''(\alpha) + \cdots \equiv \lambda P'(\alpha) \pmod{\mathfrak{p}^2}$ [*)]; da nun die derivierte Funktion $P'(t)$ den Grad $(f-1)$ hat und nicht $\equiv 0 \pmod{p}$ ist, so kann sie auch nicht $\equiv 0 \pmod{p, P}$ sein, und folglich ist nach dem obigen die Zahl $P'(\alpha)$ nicht teilbar durch $\mathfrak{p}$; mithin ist das Produkt $\lambda P'(\alpha)$, und folglich auch die Zahl $P(\alpha')$ wohl teilbar durch $\mathfrak{p}$, aber nicht teilbar durch $\mathfrak{p}^2$. Nachdem so die Existenz einer solchen Zahl $\alpha'$ bewiesen ist, lassen wir den Akzent wieder weg, und nehmen also an, daß $P(\alpha)$ durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbar ist.

Ist nun $\mathfrak{p}^e$ die höchste in $p$ aufgehende Potenz des Primideals $\mathfrak{p}$, so wollen wir beweisen, daß die Zahlenkongruenz

$$\varphi(\alpha) \equiv 0 \pmod{\mathfrak{p}^e}$$

mit der Funktionenkongruenz

$$\varphi(t) \equiv 0 \pmod{p, P^e}$$

gleichbedeutend ist. In der Tat, wenn die letztere stattfindet, so ist

$$\varphi(t) \equiv P(t)^e \psi(t) \pmod{p},$$

also auch

$$\varphi(\alpha) \equiv P(\alpha)^e \psi(\alpha) \pmod{p},$$

und da beide Zahlen $p$ und $P(\alpha)^e$ durch $\mathfrak{p}^e$ teilbar sind, so folgt $\varphi(\alpha) \equiv 0 \pmod{\mathfrak{p}^e}$; wenn dagegen die Funktionenkongruenz nicht stattfindet, so ist der größte gemeinschaftliche Teiler, welchen die Funktionen $\varphi(t)$ und $P(t)^e$ nach dem Modul $p$ haben, von der Form $P(t)^s$, wo $s < e$; bestimmt man die Funktionen $\varphi_1(t)$, $\varphi_2(t)$ so, daß

$$\varphi(t)\varphi_1(t) + P(t)^e \varphi_2(t) \equiv P(t)^s \pmod{p}$$

wird (C. 4), und bedenkt, daß $p$ und $P(\alpha)^e$ durch $\mathfrak{p}^e$ teilbar sind, so ergibt sich

$$\varphi(\alpha)\varphi_1(\alpha) \equiv P(\alpha)^s \pmod{\mathfrak{p}^e};$$

da nun $s < e$, und $P(\alpha)$ nicht durch $\mathfrak{p}^2$ teilbar ist, so ist $P(\alpha)^s$ nicht teilbar durch $\mathfrak{p}^e$, und folglich ist auch $\varphi(\alpha)$ nicht $\equiv 0 \pmod{\mathfrak{p}^e}$. Unsere Behauptung ist daher erwiesen.

Man verfahre nun mit jedem der in $p$ aufgehenden verschiedenen Primideale $\mathfrak{p}_1, \mathfrak{p}_2 \cdots \mathfrak{p}_m$ so, wie es im vorhergehenden beschrieben

---

[*) Durch ein Versehen schreibt Dedekind $P''(\alpha)$ statt $\frac{P''(\alpha)}{2!}$; die Zahlen $\frac{P''(\alpha)}{2!}$, $\frac{P'''(\alpha)}{3!}$, $\cdots$ sind aber auch alle ganz.]

ist, d. h. man wähle nach Belieben $m$ Primfunktionen $P_1$, $P_2 \cdots P_m$, welche resp. dieselben Grade $f_1$, $f_2 \cdots f_m$ haben, wie jene Primideale, und bestimme ebenso viele Zahlen $\alpha_1$, $\alpha_2 \cdots \alpha_m$ der Art, daß $P_1(\alpha_1)$, $P_2(\alpha_2) \cdots P_m(\alpha_m)$ resp. durch $\mathfrak{p}_1$, $\mathfrak{p}_2 \cdots \mathfrak{p}_m$ teilbar werden, mit der eventuellen Beschränkung, daß eine solche Zahl $P_r(\alpha_r)$ nicht durch $\mathfrak{p}_r^2$ teilbar sein darf, falls $p$ durch $\mathfrak{p}_r^2$ teilbar ist. Da nun die Primideale $\mathfrak{p}_1$, $\mathfrak{p}_2 \cdots \mathfrak{p}_m$ voneinander verschieden, und ihre Quadrate folglich relative Primideale sind, so kann man stets eine Zahl $\theta$ so bestimmen, daß

$$\begin{aligned} \theta &\equiv \alpha_1 \pmod{\mathfrak{p}_1^2} \\ \theta &\equiv \alpha_2 \pmod{\mathfrak{p}_2^2} \\ &\cdots\cdots\cdots \\ \theta &\equiv \alpha_m \pmod{\mathfrak{p}_m^2} \end{aligned}$$

wird (D. § 163; B. § 26); da hieraus

$$\begin{aligned} P_1(\theta) &\equiv P_1(\alpha_1) \pmod{\mathfrak{p}_1^2} \\ P_2(\theta) &\equiv P_2(\alpha_2) \pmod{\mathfrak{p}_2^2} \\ &\cdots\cdots\cdots\cdots \\ P_m(\theta) &\equiv P_m(\alpha_m) \pmod{\mathfrak{p}_m^2} \end{aligned}$$

folgt, so ergibt sich, daß die Zahlen $P_1(\theta)$, $P_2(\theta) \cdots P_m(\theta)$ resp. durch $\mathfrak{p}_1$, $\mathfrak{p}_2 \cdots \mathfrak{p}_m$ teilbar sind, daß aber, falls $p$ durch $\mathfrak{p}_r^2$ teilbar ist, die Zahl $P_r(\theta)$ nicht durch $\mathfrak{p}_r^2$ teilbar ist. Die Zahl $\theta$ vereinigt daher in sich alle diejenigen Eigenschaften in bezug auf die sämtlichen $m$ Primideale, welche einer jeden Zahl $\alpha_r$ in bezug auf das ihr korrespondierende Primideal $\mathfrak{p}_r$ zukommen. Ist daher

$$\mathfrak{o}\,p = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_m^{e_m},$$

also, wie aus der Bildung der Norm hervorgeht,

$$n = e_1 f_1 + e_2 f_2 + \cdots + e_m f_m,$$

so ist eine Zahl von der Form $\varphi(\theta)$ stets und nur dann durch eine der Potenzen $\mathfrak{p}_1^{e_1}$, $\mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_m^{e_m}$ teilbar, wenn die ihr entsprechende Funktionenkongruenz

$$\begin{aligned} \varphi(t) &\equiv 0 \pmod{p,\ P_1^{e_1}} \\ \varphi(t) &\equiv 0 \pmod{p,\ P_2^{e_2}} \\ &\cdots\cdots\cdots\cdots \\ \varphi(t) &\equiv 0 \pmod{p,\ P_m^{e_m}} \end{aligned}$$

stattfindet; da ferner eine ganze Zahl des Körpers stets und nur dann durch $p$ teilbar ist, wenn sie durch jede der $m$ Potenzen $\mathfrak{p}_1^{e_1}$, $\mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_m^{e_m}$ teilbar ist, so leuchtet ein, daß die eine Zahlenkongruenz

$$\varphi(\theta) \equiv 0 \pmod{p}$$

gleichbedeutend ist mit dem System der $m$ vorstehenden Funktionenkongruenzen.

Bis hierher haben wir absichtlich über die Wahl der Primfunktionen $P_1, P_2 \cdots P_m$ nichts anderes festgesetzt, als daß ihre Grade resp. mit denen der Primideale $\mathfrak{p}_1, \mathfrak{p}_2 \cdots \mathfrak{p}_m$ übereinstimmen sollen, und es war z. B., falls $f_1 = f_2$, nicht ausgeschlossen, $P_1 = P_2$ zu wählen. Wir wollen jetzt die besondere Annahme unseres Satzes hinzufügen, welche darin besteht, daß es $m$ untereinander inkongruente Primfunktionen von den vorgeschriebenen Graden gibt, und wir wollen unter $P_1, P_2 \cdots P_m$ solche inkongruente Primfunktionen verstehen. Dann sind die Potenzen $P_1^{e_1}, P_2^{e_2} \cdots P_m^{e_m}$ relative Primfunktionen, und wenn man ihr Produkt

$$P_1^{e_1} P_2^{e_2} \cdots P_m^{e_m} = R$$

setzt, so ist (C. 5) das System der $m$ obigen Funktionenkongruenzen, und folglich auch die eine Zahlenkongruenz

$$\varphi(\theta) \equiv 0 \pmod{p}$$

gleichbedeutend mit der einzigen Funktionenkongruenz

$$\varphi(t) \equiv 0 \pmod{p, R}.$$

Da ferner der Grad des Produktes $R$ gleich

$$e_1 f_1 + e_2 f_2 + \cdots + e_m f_m$$

und folglich $= n$ ist, so kann eine Zahl

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

nur dann durch $p$ teilbar sein, wenn

$$\varphi(t) \equiv 0 \pmod{p},$$

d. h. wenn alle $n$ Koeffizienten $x_0, x_1, x_2 \cdots x_{n-1}$ durch $p$ teilbar sind. Der Index $k$ der Zahl $\theta$ ist folglich (nach § 1) nicht teilbar durch $p$. Hiermit ist unser obiger Satz bewiesen, und wir fügen nur noch die folgende Bemerkung hinzu.

Da $k$ nicht teilbar durch $p$ ist, so ist $k$ auch von 0 verschieden, und folglich ist die gefundene Zahl $\theta$ die Wurzel einer irreduktiblen Gleichung $F(\theta) = 0$ vom $n^{\text{ten}}$ Grade; da nun $F(\theta) \equiv 0 \pmod{p}$, so muß die Funktion $F$ durch $R$ teilbar sein nach dem Modul $p$; da ferner beide Funktionen denselben Grad $n$ und denselben höchsten Koeffizienten 1 haben, so muß $F \equiv R \pmod{p}$, d. h.

$$F \equiv P_1^{e_1} P_2^{e_2} \cdots P_m^{e_m} \pmod{p}$$

sein, und hiermit sind wir zum Ausgangspunkt unserer Untersuchung in § 2 zurückgekehrt.

§ 5.

Die letzte Untersuchung hat uns ein Kriterium geliefert, durch welches die Frage entschieden wird, ob es wirklich in $\Omega$ eine ganze Zahl $\theta$ gibt, deren Index durch eine gegebene Primzahl $p$ nicht teilbar ist. Wenn

$$\mathfrak{o}\,p = \mathfrak{p}_1^{e_1}\,\mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_m^{e_m}$$

ist, wo $\mathfrak{p}_1, \mathfrak{p}_2 \cdots \mathfrak{p}_m$ verschiedene Primideale resp. von den Graden $f_1, f_2 \cdots f_m$ bedeuten, so wird der singuläre Fall, daß die Indizes aller in $\Omega$ enthaltenen ganzen Zahlen durch $p$ teilbar sind, jedesmal und nur dann eintreten, wenn es unmöglich ist, $m$ nach dem Modul $p$ inkongruente Primfunktionen von den Graden $f_1, f_2 \cdots f_m$ aufzustellen. Es fragt sich daher nur noch, ob diese Erscheinung, daß nicht genug Primfunktionen existieren, wirklich jemals auftreten kann. Um hierüber zu entscheiden, wollen wir den denkbar einfachsten Versuch anstellen. Die inkongruenten Primfunktionen ersten Grades sind die folgenden

$$t,\ t+1,\ t+2 \cdots t+(p-1),$$

ihre Anzahl ist $= p$; der obige singuläre Fall wird daher gewiß in einem Körper $\Omega$ eintreten, in welchem die Primzahl $p$ durch mindestens $(p+1)$ verschiedene Primideale ersten Grades teilbar ist; da aber, wie aus der Betrachtung der Normen hervorgeht, das Ideal $\mathfrak{o}\,p$ ein Produkt von höchstens $n$ Primidealen ist, so muß der Grad $n$ eines solchen Körpers mindestens $= p+1$ sein. Nimmt man, um den einfachsten Fall zu erhalten, die kleinste Primzahl $p = 2$, so entsteht also die Frage, ob es kubische Körper $\Omega$ gibt, in welchen die Zahl 2 durch drei verschiedene Primideale ersten Grades teilbar ist; in einem solchen Körper würden die Indizes aller ganzen Zahlen gerade sein. Diese Untersuchung ist in den Göttingischen gelehrten Anzeigen vom 20. September 1871 in voller Allgemeinheit angestellt, und sie hat zu einer bejahenden Antwort geführt; hier will ich mich begnügen, ein einziges, auch dort schon angeführtes Beispiel mitzuteilen [*)].

[*) Die eben erwähnte Anzeige enthält auch eine Ausführung über die Methode, wodurch Dedekind auf das hier behandelte Beispiel gekommen ist. Weiter wird ein anderes Beispiel eines Körpers mit gemeinsamen Indexteilern gegeben, nämlich ein Körper vierten Grades, worin die Primzahl 2 in zwei Primideale zweiten Grades zerfällt.]

Es sei $\alpha$ eine Wurzel der irreduktiblen Gleichung dritten Grades

$$F(\alpha) = \alpha^3 - \alpha^2 - 2\alpha - 8 = 0;$$

um ihre Diskriminante zu finden, betrachten wir die Zahl

$$F'(\alpha) = \delta = -2 - 2\alpha + 3\alpha^2$$

und bilden sukzessive, unter Zuziehung von $F(\alpha) = 0$, die Produkte

$$\delta\alpha = 24 + 4\alpha + \alpha^2$$
$$\delta\alpha^2 = 8 + 26\alpha + 5\alpha^2;$$

durch lineare Elimination von $1, \alpha, \alpha^2$ aus diesen drei Gleichungen erhält man

$$\begin{vmatrix} -2-\delta, & -2 & , & 3 \\ 24 & , & 4-\delta, & 1 \\ 8 & , & 26 & , & 5-\delta \end{vmatrix} = 0,$$

d. h.

$$\delta^3 - 7\delta^2 - 2012 = 0,$$

und folglich ist die Diskriminante

$$\Delta(1, \alpha, \alpha^2) = -N(\delta) = -2012 = -2^2 \cdot 503.$$

Da 503 eine Primzahl ist, so gehen in dieser Diskriminante nur die beiden Quadrate 1 und 4 auf, und folglich ist der Index $k$ der Zahl $\alpha$ entweder $= 1$, oder $= 2$; es ist daher die Funktion

$$F(t) = t^3 - t^2 - 2t - 8$$

nur in bezug auf den Modul $p = 2$ zu untersuchen. Offenbar ist

$$F = P_1^2 P_2 - 2M \equiv P_1^2 P_2 \pmod 2,$$

wo

$$P_1 = t, \quad P_2 = t - 1, \quad M = t + 4;$$

da nun gleichzeitig $P_1$ in $M$, und $P_1^2$ in $F$ aufgeht nach dem Modul 2, so muß (nach dem zweiten Beweise des Satzes II in § 3) die Zahl

$$P_1(\alpha)\, P_2(\alpha) = \alpha(\alpha - 1)$$

durch 2 teilbar, und folglich $k = 2$ sein. Dies wird sich sofort dadurch bestätigen, daß die Zahl

$$\beta = \tfrac{1}{2}\alpha(\alpha - 1) - 1$$

sich ebenfalls als eine ganze Zahl erweist; in der Tat, man erhält mit Rücksicht auf $F(\alpha) = 0$ die Gleichungen

$$\alpha^2 = 2 + \alpha + 2\beta$$
$$\beta^2 = -2 + 2\alpha - \beta$$
$$\alpha\beta = 4$$

und hieraus

$$\beta^3 + \beta^2 + 2\beta - 8 = 0.$$

Da ferner

$$1 = 1 \cdot 1 + 0 \cdot \alpha + 0 \cdot \beta$$
$$\alpha = 0 \cdot 1 + 1 \cdot \alpha + 0 \cdot \beta$$
$$\alpha^2 = 2 \cdot 1 + 1 \cdot \alpha + 2 \cdot \beta,$$

so ist

$$\Delta(1, \alpha, \alpha^2) = \begin{vmatrix} 1, & 0, & 0 \\ 0, & 1, & 0 \\ 2, & 1, & 2 \end{vmatrix}^2 \Delta(1, \alpha, \beta) = 2^2 \Delta(1, \alpha, \beta),$$

also

$$\Delta(1, \alpha, \beta) = -503,$$

und da diese Zahl durch kein Quadrat (außer 1) teilbar ist, so ist sie die Grundzahl $D$ unseres kubischen Körpers $\Omega$, und die Zahlen 1, $\alpha$, $\beta$ bilden eine Basis des aus allen ganzen Zahlen $\omega$ dieses Körpers $\Omega$ bestehenden Gebiets $\mathfrak{o}$, d. h. nach der schon mehrfach gebrauchten Bezeichnung, es ist

$$\mathfrak{o} = [1, \alpha, \beta];$$

jede solche ganze Zahl, d. h. jede in $\mathfrak{o}$ enthaltene Zahl $\omega$ ist von der Form

$$\omega = z + x\alpha + y\beta,$$

wo $z$, $x$, $y$ willkürliche ganze rationale Zahlen bedeuten.

Wir wollen nun auf Grund dieses Resultats die Idealfaktoren der Zahl 2 bestimmen. Da

$$\left.\begin{aligned} \alpha^2 &= \quad 2 + \alpha + 2\beta \equiv \alpha \\ \beta^2 &= -2 + 2\alpha - \beta \equiv \beta \end{aligned}\right\} \pmod 2,$$

so folgt allgemein

$$(z + x\alpha + y\beta)^2 \equiv z^2 + x^2\alpha^2 + y^2\beta^2 \equiv z + x\alpha + y\beta \pmod 2,$$

d. h. jede Zahl $\omega$ des Gebietes $\mathfrak{o}$ genügt der Kongruenz

$$\omega^2 - \omega \equiv 0 \pmod 2.$$

Hieraus folgt zunächst, daß die Zahl 2 durch kein Quadrat eines Primideals teilbar sein kann; wäre nämlich $\mathfrak{o}(2) = \mathfrak{p}^2\mathfrak{q}$, wo $\mathfrak{p}$ ein Primideal oder wenigstens ein von $\mathfrak{o}$ verschiedenes Ideal bedeutet, so würde, da $\mathfrak{p}\mathfrak{q}$ nicht durch $\mathfrak{o}(2)$ teilbar ist, eine Zahl $\omega$ existieren, welche durch $\mathfrak{p}\mathfrak{q}$, aber nicht durch 2 teilbar wäre; dann wäre aber $\omega^2$ teilbar durch $\mathfrak{p}^2\mathfrak{q}^2$, also auch durch 2, und dies widerspricht der vorstehenden Kongruenz $\omega^2 \equiv \omega \pmod 2$. Mithin ist $\mathfrak{o}(2)$ entweder ein Primideal oder ein Produkt aus lauter verschiedenen Primidealen. Es sei $\mathfrak{p}$ irgend ein in 2 aufgehendes Primideal, so genügt jede in $\mathfrak{o}$ enthaltene Zahl $\omega$ der Kongruenz

$$\omega^2 - \omega \equiv 0 \pmod{\mathfrak{p}},$$

und folglich ist die Anzahl ihrer inkongruenten Wurzeln $= (\mathfrak{o}, \mathfrak{p}) = N(\mathfrak{p})$; da diese Anzahl aber niemals größer als der Grad der Kongruenz sein kann, so ergibt sich $N(\mathfrak{p}) \leqq 2$, und folglich $N(\mathfrak{p}) = 2$, weil $\mathfrak{p}$ ein Primideal, also von $\mathfrak{o}$ verschieden, mithin $N(\mathfrak{p}) > 1$ ist. Jedes in 2 aufgehende Primideal ist daher vom ersten Grade, und folglich muß, da $N(2) = 2^3 = 8$ ist,

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

sein, wo $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ drei voneinander verschiedene Primideale ersten Grades bedeuten. Hiermit ist das Auftreten der erwähnten singulären Erscheinung erwiesen, und es muß sich bestätigen, daß die Indizes aller Zahlen $\omega$ durch 2 teilbar sind. In der Tat, setzt man

$$z' = z^2 + 2x^2 - 2y^2 + 8xy$$
$$x' = x^2 + 2y^2 + 2xz$$
$$y' = 2x^2 - y^2 + 2yz,$$

so ist

$$\omega^2 = z' + x'\alpha + y'\beta,$$

und der Index der Zahl $\omega$ ist gleich der Determinante

$$\begin{vmatrix} 1, & 0, & 0 \\ z, & x, & y \\ z', & x', & y' \end{vmatrix} = xy' - yx' = 2x^3 - x^2y - xy^2 - 2y^3,$$

welche offenbar stets eine gerade Zahl ist.

Um unser Beispiel ganz zu vollenden, und um die aus der allgemeinen Theorie geschöpften Voraussagungen auch durch die Rechnung zu bestätigen, wollen wir endlich zur Darstellung der hier auftretenden Ideale in Form von endlichen, dreigliedrigen Moduln (D. § 161; B. § 3), d. h. zur Bestimmung dieser Ideale durch ihre Basiszahlen schreiten. Diese Darstellungen sind die folgenden

$$\mathfrak{a} = [2,\ \alpha,\ 1+\beta]$$
$$\mathfrak{b} = [2,\ 1+\alpha,\ \beta]$$
$$\mathfrak{c} = [2,\ \alpha,\ \beta].$$

Das System $\mathfrak{a}$ aller Zahlen von der Form

$$\alpha' = 2z + \alpha x + (1+\beta)y,$$

wo $z$, $x$, $y$ willkürliche ganze rationale Zahlen bedeuten, besitzt in der Tat die beiden fundamentalen Eigenschaften eines Ideals, nämlich:

I. Die Summen und Differenzen von je zwei Zahlen $\alpha'$ des Systems $\mathfrak{a}$ gehören demselben System $\mathfrak{a}$ an.

II. Jedes Produkt aus einer Zahl $\alpha'$ des Systems $\mathfrak{a}$ und aus einer Zahl $\omega$ des Gebiets $\mathfrak{o}$ ist wieder eine Zahl des Systems $\mathfrak{a}$.

Die erste Eigenschaft ist evident, und um die zweite nachzuweisen, genügt es, darzutun, daß die Produkte aus je einer der Basiszahlen 2, $\alpha$, $(1+\beta)$ von $\mathfrak{a}$ und je einer der Basiszahlen 1, $\alpha$, $\beta$ von $\mathfrak{o}$ sämtlich in $\mathfrak{a}$ enthalten sind; dies ist unmittelbar evident für die fünf Produkte

$$2\cdot 1,\ \alpha\cdot 1,\ (1+\beta)\cdot 1,\ 2\cdot\alpha,\ 2\cdot\beta = -2+2(1+\beta),$$

und für die übrigen vier ergibt sich dasselbe aus den Gleichungen

$$\alpha\cdot\alpha = \alpha+2(1+\beta), \qquad \alpha\cdot\beta = 2\cdot 2,$$
$$(1+\beta)\alpha = 2\cdot 2+\alpha, \qquad (1+\beta)\beta = -2+2\alpha.$$

Ebenso wird bewiesen, daß die Systeme $\mathfrak{b}$ und $\mathfrak{c}$ Ideale sind.

Die Norm $N(\mathfrak{m})$ eines Ideals $\mathfrak{m}$ ist die Anzahl $(\mathfrak{o}, \mathfrak{m})$ der in $\mathfrak{o}$ enthaltenen, nach $\mathfrak{m}$ inkongruenten Zahlen (D. § 163; B. § 20), und diese Anzahl ist gleich der Determinante der Ausdrücke, welche in bezug auf die Basiszahlen von $\mathfrak{o}$ linear sind und die Basiszahlen von $\mathfrak{m}$ darstellen (D. § 161; B. § 4, 4°). Es ist daher z. B.

$$N(\mathfrak{a}) = \begin{vmatrix} 2, & 0, & 0 \\ 0, & 1, & 0 \\ 1, & 0, & 1 \end{vmatrix} = 2,$$

und ebenso ergibt sich

$$N(\mathfrak{b}) = N(\mathfrak{c}) = 2.$$

Wenn aber die Norm eines Ideals eine Primzahl ist, so muß das Ideal notwendig ein Primideal sein, weil allgemein $N(\mathfrak{a}_1\mathfrak{a}_2) = N(\mathfrak{a}_1)N(\mathfrak{a}_2)$ ist; mithin sind $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ Primideale. Sie sind ferner verschieden voneinander, weil die in $\mathfrak{b}$ und in $\mathfrak{c}$ enthaltene Zahl $\beta$ nicht in $\mathfrak{a}$ enthalten, und weil die in $\mathfrak{c}$ enthaltene Zahl $\alpha$ nicht in $\mathfrak{b}$ enthalten ist. Es muß folglich die in allen drei Idealen enthaltene Zahl 2 auch in dem Produkte $\mathfrak{a}\mathfrak{b}\mathfrak{c}$ enthalten sein; mithin ist $\mathfrak{o}(2) = \mathfrak{m}\mathfrak{a}\mathfrak{b}\mathfrak{c}$, wo $\mathfrak{m}$ ein Ideal bedeutet; nimmt man aber die Norm, so ergibt sich

$$N(2) = 8 = N(\mathfrak{m})\,N(\mathfrak{a})\,N(\mathfrak{b})\,N(\mathfrak{c}) = 8\,N(\mathfrak{m});$$

mithin ist $N(\mathfrak{m}) = 1$, also $\mathfrak{m} = \mathfrak{o}$, und $\mathfrak{o}(2) = \mathfrak{a}\mathfrak{b}\mathfrak{c}$. Aber auch dieses, aus allgemeinen Sätzen geschlossene Resultat wollen wir durch die eigentliche Rechnung, d. h. durch die wirkliche Ausführung der Multiplikation der Ideale bestätigen (D. § 165; B. § 12).

Unter dem Produkte $\mathfrak{a}\mathfrak{b}$ zweier Ideale wird das System aller Produkte $\alpha'\beta'$ und aller Summen von solchen Produkten $\alpha'\beta'$ verstanden, wo $\alpha'$, $\beta'$ beliebige Zahlen resp. der Ideale $\mathfrak{a}$, $\mathfrak{b}$ bedeuten

(D. § 163; B. § 22). Ein solches Produkt erscheint daher zunächst als ein endlicher Modul, dessen Basiszahlen die sämtlichen Produkte aus je einer Basiszahl von $\mathfrak{a}$ und je einer Basiszahl von $\mathfrak{b}$ sind. In unserem Falle ist daher $\mathfrak{a}\,\mathfrak{b}$ der endliche Modul, dessen Basiszahlen die neun Produkte

$$2\cdot 2 = 4, \quad 2(1+\alpha) = 2+2\alpha, \quad 2\cdot\beta = 2\beta,$$
$$\alpha\cdot 2 = 2\alpha, \quad \alpha(1+\alpha) = 2+2\alpha+2\beta, \quad \alpha\beta = 4,$$
$$(1+\beta)\cdot 2 = 2+2\beta, \quad (1+\beta)(1+\alpha) = 5+\alpha+\beta,$$
$$(1+\beta)\beta = -2+2\alpha$$

sind; da aber von diesen neun Zahlen nur drei voneinander unabhängig sind (D. § 159; B. § 4), so ist die von mir ausführlich beschriebene Methode (B. § 4, 6°) anzuwenden, um diesen neungliedrigen Modul auf einen dreigliedrigen zurückzuführen; durch die Ausführung dieser sehr einfachen und leichten Rechnung erhält man die eine der sechs folgenden Gleichungen:

$$\mathfrak{a}^2 = [4, \quad \alpha, \quad 3+\beta]; \quad \mathfrak{b}\,\mathfrak{c} = [2, \quad 2\alpha, \quad \beta]$$
$$\mathfrak{b}^2 = [4, \quad 1+\alpha, \quad \beta]; \quad \mathfrak{c}\,\mathfrak{a} = [2, \quad \alpha, \quad 2\beta]$$
$$\mathfrak{c}^2 = [4, \quad 2+\alpha, \quad 2+\beta]; \quad \mathfrak{a}\,\mathfrak{b} = [2, \quad 2\alpha, \quad 1+\alpha+\beta].$$

Die übrigen ergeben sich auf dieselbe Weise; und wenn man abermals nach derselben Methode mit $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ multipliziert, so erhält man folgende zehn Hauptideale:

$$\mathfrak{a}\,\mathfrak{b}\,\mathfrak{c} = [2, \quad 2\alpha, \quad 2\beta \quad] = \mathfrak{o}(2)$$
$$\mathfrak{a}^2\mathfrak{c} = [4, \quad \alpha, \quad 2+2\beta] = \mathfrak{o}\,\alpha$$
$$\mathfrak{b}^2\mathfrak{c} = [4, \quad 2+2\alpha, \quad \beta \quad] = \mathfrak{o}\,\beta$$
$$\mathfrak{a}\,\mathfrak{c}^2 = [4, \quad 2+\alpha, \quad 2\beta \quad] = \mathfrak{o}(\alpha-2)$$
$$\mathfrak{b}\,\mathfrak{c}^2 = [4, \quad 2\alpha, \quad 2+\beta \quad] = \mathfrak{o}(2-\beta)$$
$$\mathfrak{a}^2\mathfrak{b} = [4, \quad 2\alpha, \quad 3+\alpha+\beta] = \mathfrak{o}(3+\alpha+\beta)$$
$$\mathfrak{a}\,\mathfrak{b}^2 = [4, \quad 2+2\alpha, \quad 1+\alpha+\beta] = \mathfrak{o}(1+\alpha+\beta)$$
$$\mathfrak{a}^3 = [8, \quad 4+\alpha, \quad 3+\beta \quad] = \mathfrak{o}(3+2\alpha+\beta)$$
$$\mathfrak{b}^3 = [8, \quad 1+\alpha, \quad 4+\beta \quad] = \mathfrak{o}(1+\alpha)$$
$$\mathfrak{c}^3 = [8, \quad 2+\alpha, \quad 2+\beta \quad] = \mathfrak{o}(\alpha+\beta-4)$$

Die zehn Zahlen $\mu$, welchen diese Hauptideale $\mathfrak{o}\,\mu = [\mu, \alpha\mu, \beta\mu]$ entsprechen, sind durch die folgenden, leicht zu verifizierenden Relationen miteinander verbunden:

$$\alpha(\alpha-2)(1+\alpha) = 2^3; \quad \alpha\beta = (\alpha-2)(1+\alpha+\beta) = 2^2$$
$$(\alpha-2)(3+\alpha+\beta) = 2\alpha; \quad \alpha(2-\beta) = 2(\alpha-2)$$
$$(\alpha-2)(3+2\alpha+\beta) = \alpha^2; \quad \alpha(\alpha+\beta-4) = (\alpha-2)^2.$$

Durch dieses Beispiel, welchem man viele andere an die Seite stellen könnte, ist außer Zweifel gesetzt, daß es Körper $\Omega$ gibt, in welchen die Indizes aller ganzen Zahlen durch eine und dieselbe Primzahl $p$ teilbar sind. Dies Resultat ist in mancher Beziehung kein willkommenes. Es gibt in der Tat sehr wichtige Sätze der Idealtheorie, welche sich durch die Theorie der höheren Kongruenzen sehr leicht würden beweisen lassen, wenn der Satz I in § 2 nicht an die Voraussetzung gebunden wäre, daß der Index $k$ der Zahl $\theta$ nicht durch $p$ teilbar sein darf; wir haben aber jetzt gesehen, daß in manchen Fällen diese Voraussetzung auf keine Weise zu erfüllen ist, wie man auch die Zahl $\theta$ wählen mag, und hieraus geht hervor, daß solche Beweise, die sich auf den genannten Satz stützen, häufig die erforderliche Allgemeinheit nicht besitzen. Als Beispiel führe ich den folgenden, besonders wichtigen Satz an, den ich ebenfalls in den Göttingischen gelehrten Anzeigen vom 20. September 1871 zuerst ausgesprochen habe:

Die Grundzahl $D$ eines Körpers $\Omega$ ist aus allen und nur aus denjenigen rationalen Primzahlen $p$ zusammengesetzt, welche in diesem Körper durch das Quadrat eines Primideals teilbar sind.

Gibt es in $\Omega$ eine ganze Zahl, deren Index durch die Primzahl $p$ nicht teilbar ist, so folgt für diese Primzahl $p$ die Richtigkeit des Satzes augenscheinlich sehr leicht aus § 2. Aber auf diese Weise gelangt man offenbar nicht zu dem Beweise der allgemeinen Gültigkeit des Satzes, und es ist mir erst nach manchen vergeblichen Versuchen gelungen, den allgemeinen Beweis in aller Strenge zu führen. Die ausführliche Darstellung dieses Gegenstandes, bei welcher der Satz selbst noch eine wesentliche Erweiterung erfahren wird, muß ich aber für eine andere Gelegenheit mir vorbehalten.

---

## Erläuterungen zur vorstehenden Abhandlung.

Das Problem der Verallgemeinerung der Kummerschen Theorie der Ideale in Kreisteilungskörpern auf beliebige Körper führt natürlich zu einer Definition der Ideale mittels höheren Kongruenzen. Schon Selling (Zeitschr. f. Math. u. Phys., Bd. 10, S. 17—47 (1865)) schlägt diesen Weg ein, und es gelingt ihm, zwar unter Anwendung von Galoisschen Imaginären und weiteren Hilfskörpern, eine ausnahmslose Theorie der Ideale in Galoisschen Körpern zu gewinnen. Die Primidealzerlegung einer Primzahl $p$ wird aus der Zerlegung der definierenden Gleichung (mod. $p^a$) in diesen Hilfskörpern abgeleitet. Ein Nach-

weis der Invarianz dieser Ideale, d. h. ihre Unabhängigkeit von der gewählten Gleichung wird aber nicht gebracht.

Wie aus der Einleitung hervorgeht, hat auch Dedekind zuerst diese Methode versucht, aber wieder aufgegeben, um die Theorie der Ideale in der abstrakten Form zu schaffen, wie er sie in der zweiten Auflage von Dirichlets Zahlentheorie dargestellt hat. In dieser Form entsteht aber sofort die Frage, wie die Primidealzerlegung einer gegebenen Zahl im Körper bestimmt werden kann, und speziell wie Primideale bei gegebener, definierender Gleichung abgeleitet werden können. Diese Frage wird für Primzahlen, welche den Index nicht teilen, durch den Satz I, § 2 erledigt, aber die vollständige Lösung scheitert an dem Vorkommen der gemeinsamen Indexteiler (gemeinsame außerwesentliche Diskriminantenteiler).

In der mehrmals von Dedekind erwähnten Arbeit von Zolotareff (1874) wird umgekehrt die Primidealzerlegung durch die Zerlegung des Satzes I definiert. Wenn aber $p$ ein Teiler des Index ist, genügt diese Definition nicht der Forderung der Invarianz. Eine ausnahmslose Theorie der Ideale gibt aber Zolotareff in der Arbeit: „Sur la théorie des nombres complexes“ (Journ. de Math., Bd. 6, S. 51—84, 129—166, 3e série (1880); man vgl. auch: Mélanges math. et astron., Bulletin de l'academie des sciences, St. Petersburg, Bd. 5, 13./25. September 1877), worin er auch eine Übersicht über seine erste Theorie gibt. Bei seiner allgemeinen Theorie der Ideale muß aber Zolotareff so wie Dedekind eine Definition der Ideale mittels der definierenden Gleichung aufgeben.

Man kann die Zolotareffsche Theorie kurz folgendermaßen beschreiben: Zuerst wird eine Methode angegeben, wodurch man in endlich vielen Schritten ein vollständiges Restsystem

$$(1) \qquad \alpha_1, \alpha_2, \ldots, \alpha_{p^n-1} \pmod{p} \text{ (die Null ausgenommen)}$$

aufstellen kann. Eine Zahl $\alpha$ in (1) heißt relativ prim zu $p$, wenn es keine Zahl $\gamma$ in (1) gibt, wofür $\alpha\gamma$ durch $p$ teilbar ist. Zwei Zahlen $\alpha$ und $\beta$ heißen relativ prim in bezug auf $p$, wenn es keine Zahl $\gamma$ in (1) gibt, wofür gleichzeitig $\alpha\gamma$ und $\beta\gamma$ durch $p$ teilbar sind. Es können dann zwei Zahlen $\gamma$ und $\delta$ so bestimmt werden, daß

$$\alpha\gamma + \beta\delta \equiv 1 \pmod{p},$$

und hieraus erhält man leicht eine Definition des größten gemeinsamen Teilers in bezug auf $p$. Die Primideale werden dann folgendermaßen eingeführt: Eine Zahl $\alpha$ enthält nur ein Primideal $\beta$ von $p$, wenn jede Zahl in (1), welche nicht zu $\alpha$ relativ prim ist, die Zahl $\alpha$ als Teiler in bezug auf $p$ enthält. Aus (1) können dann in endlich vielen Schritten die Anzahl der vorkommenden verschiedenen Primideale bestimmt werden.

Es würde hier zu weit führen, auf alle späteren Begründungen der Idealtheorie einzugehen. Es sollen hier nur ganz kurz die wichtigsten Methoden zur Bestimmung der Primideale erwähnt werden.

Die Kroneckersche Theorie der Formen (Journ. f. Math., Bd. 92, S. 1—122 (1882)) gibt eine theoretisch besonders einfache Bestimmung der Primidealzerlegung der rationalen Primzahlen. Wie zuerst in voller Allgemeinheit von Hensel (Journ. f. Math., Bd. 113, S. 61—83 (1894)) gezeigt worden ist, besteht in dieser Theorie für alle Primzahlen ein vollständiges Analogon zum Dedekindschen Satze.

Die Schwierigkeiten der gemeinsamen Indexteiler werden hier dadurch überwunden, daß man statt einer speziellen Gleichung eine Fundamentalgleichung

$F(x_1 \dots x_n) = 0$ des Körpers studiert. Wenn die Zahlen $\omega_i$ eine Minimalbasis bilden, ist $F(x_1 \dots x_n) = 0$ die Gleichung, welcher die Fundamentalform

$$\omega = \omega_1 x_1 + \cdots + \omega_n x_n \tag{2}$$

genügt. Die entsprechende Indexform ist dann eine Einheitsform, d. h. ihre Koeffizienten haben keinen gemeinsamen Teiler, und man erhält für die Fundamentalgleichung Resultate, welche dem Dedekindschen Satze I genau entsprechen.

Diese Lösung des Problems gibt aber keine Auskunft über den Zusammenhang zwischen den Eigenschaften der Gleichungen des Körpers und der Primidealzerlegung, wie es beim Dedekindschen Satze der Fall ist. In der von Hensel begründeten $p$-adischen Theorie der algebraischen Zahlen wird diese Lücke zum Teil ausgefüllt, indem man zeigt, daß die Zerlegung der definierenden Gleichung in irreduzible $p$-adische Faktoren der Zerlegung von $p$ in Primidealpotenzen entspricht. Für die vollständige Bestimmung der Primidealzerlegung muß man aber auch hier auf die Kroneckersche Theorie zurückgreifen. (Man sehe K. Hensel: Theorie der algebraischen Zahlen I, Leipzig 1908.)

Man kann aber zeigen, daß die Schwierigkeiten der Dedekindschen Theorie dadurch vollständig beseitigt werden können, daß man statt Kongruenzen (mod. $p$) immer Kongruenzen (mod. $p^\alpha$) betrachtet, wo $\alpha$ eine feste Zahl ist, und $\alpha > \delta$, wenn die Diskriminante der entsprechenden Gleichung genau durch $p^\delta$ teilbar ist. Die entsprechenden irreduziblen Faktoren sind dann zwar nicht (mod. $p^\alpha$), aber doch (mod. $p^{\alpha-\delta}$) eindeutig bestimmt. Die gemeinsamen Indexteiler verlieren dadurch gänzlich ihre Ausnahmestellung und man erhält eine eindeutige Korrespondenz zwischen Primidealzerlegung und Faktoren der Gleichung (O. Ore, Math. Ann., Bd. 96, S. 315—352 (1926) und Bd. 97, S. 569—598 (1927)). Weiter kann die Dedekindsche Darstellung der Primideale in der Form $\beta = (p, \varphi(\vartheta))$ durch eine Methode bestimmt werden, welche mit der Bestimmung der Reihenentwicklung algebraischer Funktionen große Ähnlichkeit zeigt (O. Ore, Math. Ann., Bd. 99, S. 84—117 (1928)).

Die Resultate in § 4 der vorliegenden Abhandlung geben ein einfaches Kriterium für gemeinsame Indexteiler. Hensel (Journ. f. Math., Bd. 113, S. 128—160 (1894)) leitet ein weiteres Kriterium ab, indem er die Bedingung dafür aufstellt, daß die Indexform $k(x_1, \dots, x_n)$ zu (1) für alle ganzzahligen Werte der $x_i$ einen gemeinsamen Teiler hat. Durch diese Untersuchung gelang es auch Hensel, die Kroneckersche Vermutung zu beweisen, daß für Körper mit gemeinsamen Indexteilern immer Erweiterungskörper $K$ derart existieren, daß, wenn die Variablen $x_i$ in (1) alle ganze Zahlen in $K$ durchlaufen, keine gemeinsame Idealteiler der entsprechenden Werte der Indexform vorkommen können.

Das Henselsche Kriterium zeigt, daß für einen gemeinsamen Indexteiler $p$ gleich $p < \frac{n(n-1)}{2}$ ist. E. v. Zylinsky (Math. Ann., Bd. 73, S. 273—274 (1913)) beweist unter Anwendung des Dedekindschen Kriteriums, daß sogar $p < n$ ist. M. Bauer (Math. Ann., Bd. 64, S. 573—576 (1907)) zeigt umgekehrt, daß, wenn diese Bedingung erfüllt ist, auch immer Körper $n$-ten Grades existieren, worin $p$ gemeinsamer Indexteiler ist. Weiter wird die Existenz von Indexteilern mit speziellen Eigenschaften nachgewiesen. Diese Resultate folgen auch sofort aus dem allgemeinen Existenzsatz für Körper mit vorgeschriebenen Primidealzerlegungen gegebener Primzahlen (H. Hasse, Math. Ann., Bd. 95, S. 229—238 (1925); O. Ore, Math. Zeitschr., Bd. 20, S. 267—279 (1924)).

**Ore.**