82

Ueber den Zusammenhang

zwischen

der Theorie der Ideale

und

der Theorie der höheren Congruenzen.

Von

R. Dedekind.

Aus dem dreiundzwanzigsten Bande der Abhandlungen der Königlichen Gesellschaft der Wissenschaften zu Göttingen.

Göttingen,
Dieterich'sche Verlags-Buchhandlung.
1878.

Die neuen Principien, 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 Gegenstande hatte ich mich schon vorher, durch die grosse Entdeckung Kummer's angeregt, eine lange Reihe von Jahren hindurch beschäftigt, wobei ich von einer ganz anderen Grundlage, nämlich von der Theorie der höheren Congruenzen 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 Congruenz aufgefasst wird, und dass die so erhaltenen Definitionen der idealen Zahlen (oder vielmehr der Theilbarkeit 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 eigenthümliche 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 Theilbarkeit 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 mitgetheilt, und namentlich habe ich daselbst den Grund aufgedeckt, auf welchem das Auftreten der erwähnten eigenthümlichen 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[1]) geht hervor, dass die Theorie von Zolotareff sich ebenfalls auf die Theorie der höheren Congruenzen 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* mitgetheilten Bemerkungen nachzuliefern. Hierbei muss ich sowohl meine Theorie der Ideale, als auch die Theorie der höheren

1) 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 Professor Wangerin geliehen erhalten, aber bei meiner Unkenntniss der russischen Sprache habe ich zu meinem grossen Bedauren nur das Wenige verfolgen können, was schon aus dem Anblick der Formeln verständlich ist.

Congruenzen, von welcher ich früher in Borchardt's *Journal* (Bd. 54, S. 1) eine gedrängte Darstellung gegeben habe, als bekannt voraussetzen; der Kürze halber werde ich diese Abhandlung über die Congruenzen mit *C.*, die zweite Auflage der *Zahlentheorie von Dirichlet* mit *D.*, und die oben angeführte Abhandlung im *Bulletin des sciences mathématiques* mit *B.* citiren.

§. 1.

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

$$\omega_1, \omega_2 \ldots \omega_n$$

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

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

aller Zahlen ω von der Form

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

wo

$$h_1, h_2 \ldots h_n$$

willkürliche ganze rationale Zahlen bedeuten; die Discriminante

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

welche von der Wahl der Basiszahlen $\omega_1, \omega_2 \ldots \omega_n$ unabhängig ist, heisst die Grundzahl oder die Discriminante des Körpers Ω (*D.* §§. 159, 160, 162; *B.* §§. 13—18).

Ist nun θ eine bestimmte ganze Zahl des Körpers, so kann man

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

setzen, wo die sämmtlichen n^2 Coefficienten oder Coordinaten c ganze rationale Zahlen bedeuten, und es ist

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

wo

$$k = \Sigma \pm c_1^0 c'_2 \ldots c_n^{(n-1)}$$

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

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

von einander unabhängig (*D.* §. 159; *B.* §§. 4, 15, 17) und θ ist die Wurzel einer irreductibelen Gleichung $n$ten Grades

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

deren Coefficienten $1, a_1, a_2 \ldots a_n$ ganze rationale Zahlen sind.

Bedeutet ferner $\varphi(t)$ jede beliebige *Function* der Variabelen t, — und ich bemerke ein für allemal, dass unter diesem Namen und unter einem Zeichen von der Form $\varphi(t), f(t) \ldots$ in der gegenwärtigen Abhandlung ausschliesslich eine ganze Function von t verstanden werden soll, deren Coefficienten 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 Ω und folglich auch in $\mathfrak{o}$ enthalten. Offenbar ist es gestattet, nur solche Functionen

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

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

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

dividirt, 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

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

setzen. Ausserdem ergiebt sich aus der Irreductibilität der Gleichung $F(\theta) = 0$, dass jede Zahl ω' 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 ω' beschränken, vielmehr auch Functionen von beliebig hohem Grade zulassen.

Die sämmtlichen *Primzahlen* p, — mit welchem Namen stets rationale, positive Primzahlen bezeichnet sein sollen —, zerfallen nun, nachdem einmal eine bestimmte Zahl θ gewählt und der Darstellung zu Grunde gelegt ist, in zwei verschiedene Arten; die *erste* Art besteht aus den unendlich vielen Primzahlen, welche in dem Index k der Zahl θ *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 giebt 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 $\mathfrak{o}p$[1]) in Producte aus lauter Primidealen sich vollständig zurückführen lässt auf die Zerlegung der Function $F(t)$ in ein Product aus lauter Primfunctionen 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 theilbar durch p. In diesem Fall ist eine in $\mathfrak{o}'$ enthaltene Zahl

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

nur dann durch p theilbar (also von der Form $p\omega$, wo ω eine ganze,

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

d. h. in $\mathfrak{o}$ enthaltene Zahl bedeutet), wenn alle Coefficienten x_0, x_1, x_2 $\ldots x_{n-1}$ durch p theilbar sind; denn setzt man

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

so ist

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

und wenn ω' durch p theilbar sein soll, so muss (zufolge der Bedeutung von ω_1, $\omega_2 \ldots \omega_n$) jede der Coordinaten h_1, $h_2 \ldots h_n$ durch p theilbar sein; hieraus ergiebt sich aber weiter, dass die Producte kx_0, kx_1, kx_2 $\ldots kx_{n-1}$, und folglich auch die Coefficienten x_0, x_1, $x_2 \ldots x_{n-1}$ sämmtlich durch p theilbar sein müssen, wie behauptet war. Denselben Satz kann man offenbar auch so aussprechen: ist eine Zahl ω' der Ordnung $\mathfrak{o}'$ theilbar durch eine Primzahl p der ersten Art, so ist auch der Quotient $\frac{\omega'}{p}$ eine Zahl derselben Ordnung $\mathfrak{o}'$. Umgekehrt, wenn alle Coefficienten x_0, x_1, $x_2 \ldots x_{n-1}$ durch p theilbar sind, so ist selbstverständlich auch ω' durch p theilbar. Es sind daher zwei Zahlen $\varphi_1(\theta)$ und $\varphi_2(\theta)$ der Ordnung $\mathfrak{o}'$ stets und nur dann einander congruent nach dem Modul p, d. h. ihre Differenz $\varphi_1(\theta) - \varphi_2(\theta)$ ist theilbar durch p, wenn je zwei entsprechende Coefficienten der beiden Functionen $\varphi_1(t)$ und $\varphi_2(t)$ einander nach p congruent sind, d. h. in der Bezeichnungsweise der Theorie der höheren Congruenzen, wenn

$$\varphi_1(t) \equiv \varphi_2(t) \,(\mathrm{mod.}\ p)$$

ist (*C.* 1.). Hierbei war aber vorausgesetzt, dass die Grade der Functionen $\varphi_1(t)$, $\varphi_2(t)$ 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 Congruenzen durch

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

oder noch kürzer (*C.* 7.) durch

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

Umgekehrt leuchtet ein, dass aus dieser letzten Functionen-Congruenz auch wieder die Zahlen-Congruenz

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

folgt; beide Congruenzen sind daher gleichbedeutend. Mithin giebt es in $\mathfrak{o}'$ genau ebenso viele nach p incongruente Zahlen $\varphi(\theta)$, als es incongruente Functionen $\varphi(t)$ in Bezug auf den Doppelmodul p, $F(t)$ giebt; 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 incongruenten Zahlen genau ebenso gross ist (*B.* §. 18; *D.* §. 162), so ergiebt sich das wichtige Resultat: *jede Zahl* ω *des Gebietes* $\mathfrak{o}$ *ist mit einer Zahl* $\omega' = \varphi(\theta)$ *der Ordnung* $\mathfrak{o}'$ *congruent nach dem Modul* p.

Zu derselben Folgerung gelangt man unmittelbar auch durch folgende einfache Betrachtung. Aus den n Relationen zwischen den Zahlen $1, \theta, \theta^2 \ldots \theta^{n-1}$ einerseits und den Zahlen $\omega_1, \omega_2 \ldots \omega_n$ andererseits geht hervor, dass die Producte $k\omega_1, k\omega_2 \ldots k\omega_n$ und folglich auch alle Producte von der Form $k\omega$, wo ω 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 theilbar ist, so kann man die ganze rationale Zahl l so wählen, dass $kl \equiv 1 \pmod{p}$ wird, und hieraus folgt $\omega \equiv lk\omega \equiv l\varphi(\theta) \pmod{p}$; also ist ω wirklich mit einer Zahl $l\varphi(\theta)$ der Ordnung $\mathfrak{o}'$ congruent 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 theilbar

ist, so kann man nach einem Satze, dessen sehr leichten Beweis ich hier wohl übergehen darf, n ganze rationale Zahlen x_0, $x_1 \ldots x_{n-1}$, die nicht alle durch p theilbar sind, so wählen, dass die oben mit h_1, $h_2 \ldots h_n$ bezeichneten Summen sämmtlich durch p theilbar werden; dann ist die entsprechende Zahl

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

der Ordnung $\mathfrak{o}'$ wirklich theilbar durch p, obgleich ihre Coefficienten x_0, $x_1 \ldots x_{n-1}$ nicht alle durch p theilbar sind. Hieraus folgt sofort, dass die Anzahl $(\mathfrak{o}', \mathfrak{o}p)$ der in $\mathfrak{o}'$ enthaltenen, nach p incongruenten Zahlen kleiner als p^n ist, und folglich giebt es in $\mathfrak{o}$ Zahlen ω, welche mit *keiner* in $\mathfrak{o}'$ enthaltenen Zahl $\varphi(\theta)$ nach p congruent sind, d. h. es giebt Zahlclassen (mod. p) in $\mathfrak{o}$, für welche in $\mathfrak{o}'$ kein Repraesentant 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 Congruenzen ein einfaches Mittel giebt, um das Hauptideal $\mathfrak{o}p$ in seine Primfactoren zu zerlegen. Dies geschieht dadurch, dass die Function $F(t)$, die wir kürzer auch durch F bezeichnen werden, nach dem Modul p als Product von lauter *Primfunctionen* $P(t)$ dargestellt wird (*C.* 6.); der bequemeren Ausdrucksweise halber wollen wir, was erlaubt ist, jede Primfunction P so wählen, dass ihr höchster Coefficient $= 1$ ist, woraus folgt, dass zwei incongruente Primfunctionen auch immer relative Primfunctionen sein werden (*C.* 5.). Durch Vereinigung aller einander congruenten Factoren in eine Potenz erhält man

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

wo P_1, $P_2 \ldots P_m$ die sämmtlichen incongruenten, in F aufgehenden Primfunctionen bedeuten.

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

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

völlig gleichbedeutend ist mit der Functionen-Congruenz

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

In der That, 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 α, β willkürliche Zahlen des Gebietes $\mathfrak{o}$ bedeuten, und da (nach § 1) jede Zahl α mit einer Zahl $\varphi(\theta)$ der Ordnung $\mathfrak{o}'$ congruent ist nach dem Modul p, so folgt aus (1) eine Congruenz von der Form

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

hieraus ergiebt sich aber (nach §. 1) die Functionen-Congruenz

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

also auch die Congruenz (2), weil F durch P theilbar 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 Hülfe dieses Resultates 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 $\mathfrak{p}$ incongruenten Zahlen bestimmen. Sind nämlich α_1, α_2 zwei beliebige Zahlen in $\mathfrak{o}$, so giebt es (nach §. 1) in $\mathfrak{o}'$ zwei Zahlen $\varphi_1(\theta)$, $\varphi_2(\theta)$, welche resp. den Zahlen α_1, α_2 nach p congruent sind, und da p durch $\mathfrak{p}$ theilbar ist, so ist auch

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

die beiden Zahlen α_1, α_2 sind daher stets und nur dann congruent in Bezug auf $\mathfrak{p}$, wenn

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

ist; diese Congruenz ist aber nach dem Obigen gleichbedeutend mit der Congruenz

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

es giebt daher in $\mathfrak{o}$ genau ebenso viele incongruente Zahlen α in Bezug auf $\mathfrak{p}$, als es incongruente Functionen $\varphi(t)$ in Bezug auf den Doppelmodul p, P giebt, und da die Anzahl der letzteren $= p^f$ ist, wo f den Grad der Function P bedeutet (*C.* 8.), so erhalten wir

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

Ebenso leicht ergiebt 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 Product 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, 4^0). Ein solches zusammengesetztes Ideal $\mathfrak{m} = \mathfrak{a}_1\mathfrak{a}_2$ besitzt die charakteristische Eigenschaft, dass immer zwei durch $\mathfrak{m}$ nicht theilbare Zahlen α_1, α_2 existiren, deren Product $\alpha_1\alpha_2$ durch $\mathfrak{m}$ theilbar 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 Product $\mathfrak{m} = \mathfrak{a}_1\mathfrak{a}_2$ theilbar sein, und folglich giebt es eine durch $\mathfrak{a}_1$, aber nicht durch $\mathfrak{m}$ theilbare Zahl α_1, und ebenso eine durch $\mathfrak{a}_2$, aber nicht durch $\mathfrak{m}$ theilbare Zahl α_2, und offenbar ist $\alpha_1\alpha_2$ theilbar durch $\mathfrak{m}$. Es wird daher $\mathfrak{p}$ gewiss ein Primideal sein, wenn wir beweisen können, dass ein Product $\alpha_1\alpha_2$ nur dann durch $\mathfrak{p}$ theilbar ist, wenn wenigstens einer der Factoren α_1, α_2 durch $\mathfrak{p}$ theilbar ist. Zu diesem Zweck setzen wir, wie oben,

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

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 *Primfunction* ist, so muss wenigstens eine der beiden Congruenzen

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

Statt finden (*C.* 6.), also auch wenigstens eine der Congruenzen

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

d. h. wenigstens eine der beiden Zahlen α_1, α_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 That, wenn F nach dem Modul p durch P^e, aber nicht durch P^{e+1} theilbar ist, so kann man

$$F \equiv SP^e \pmod{p}$$

setzen, wo S nicht theilbar durch P ist, woraus nach dem Obigen folgt, dass die Zahl

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

nicht durch $\mathfrak{p}$ theilbar ist. Da ferner $\mathfrak{p}$ der grösste gemeinschaftliche Theiler 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 Zweck betrachten wir die Zahl

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

dieselbe kann nicht durch p theilbar sein, weil der Grad der Function SP^{e-1} kleiner als n, und weil ihr höchster Coefficient $= 1$ ist; aber η ist theilbar durch $\mathfrak{p}^{e-1}$, weil ϱ durch $\mathfrak{p}$ theilbar ist. Vermöge der Congruenz $F \equiv SP^e \pmod{p}$ ist nun das Product $\eta\varrho = \sigma\varrho^e$ theilbar durch

p, also ist auch das Ideal $\eta\mathfrak{p}\mathfrak{b}$ theilbar durch $\mathfrak{p}\mathfrak{a}$, mithin $\eta\mathfrak{b}$ theilbar durch $\mathfrak{a}$, folglich η theilbar 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 $\mathfrak{p}$ theilbar ist[1]), weil sonst η durch $\mathfrak{a}\mathfrak{p}$, also durch p theilbar wäre, was nicht der Fall ist. Da nun η durch $\mathfrak{p}^{e-1}$ theilbar ist, so muss auch $\mathfrak{a}$ durch $\mathfrak{p}^{e-1}$ theilbar sein. Wir haben jetzt nur noch zu zeigen, dass $\mathfrak{a}$ nicht durch $\mathfrak{p}^e$ theilbar ist. Da $e \geqq 1$ ist, so müsste wenn $\mathfrak{a}$ durch $\mathfrak{p}^e$ theilbar wäre, jedenfalls $\mathfrak{a}$ durch $\mathfrak{p}$ selbst theilbar sein; sobald aber $\mathfrak{a}$ durch $\mathfrak{p}$ theilbar ist, kann $\mathfrak{b}$ nicht durch $\mathfrak{p}$ theilbar sein, und folglich ist dann ϱ nicht theilbar durch $\mathfrak{p}^2$; da ferner σ nicht durch $\mathfrak{p}$ theilbar 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 η aufgehende Ideal $\mathfrak{a}$ nicht durch $\mathfrak{p}^e$ theilbar sein, w. z. b. w.

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

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

aufgehenden, incongruenten Primfunctionen

$$P_1, P_2 \ldots P_m$$

an, deren Grade wir resp. mit

$$f_1, f_2 \ldots f_m$$

bezeichnen; die diesen Functionen entsprechenden Primideale

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

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

---

1) Es ist daher $\mathfrak{a}$ der grösste gemeinschaftliche Theiler, 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 π der Congruenz $\eta\pi \equiv 0 \pmod{p}$. Dies hätte auch als Definition des Ideals $\mathfrak{p}$ benutzt werden können.

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

und

$$\mathfrak{p}_1^{e_1},\ \mathfrak{p}_2^{e_2} \ldots \mathfrak{p}_m^{e_m}$$

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

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

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

Aus allem Diesem folgt (*D.* §. 163; *B.* §. 25), dass

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

ist, und eine Bestätigung dieses Resultates ergiebt sich durch die Betrachtung der Normen, wenn man berücksichtigt, dass

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

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

I. *Ist der Index k der Zahl θ, welche der irreductibelen Gleichung $n$ten Grades $F(\theta) = 0$ genügt, nicht theilbar durch die Primzahl p, und ist*

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

wo $P_1, P_2 \ldots P_m$ incongruente Primfunctionen resp. vom Grade $f_1, f_2 \ldots f_m$ bedeuten, so ist

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

wo $\mathfrak{p}_1, \mathfrak{p}_2 \ldots \mathfrak{p}_m$ *von einander verschiedene Primideale resp. vom Grade* $f_1, f_2 \ldots f_m$ *sind, und zwar entspricht je einer Primfunction* P *ein bestimmtes Primideal* $\mathfrak{p}$ *in der Weise, dass* $\mathfrak{p}$ *der grösste gemeinschaftliche Theiler 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 θ des Körpers Ω, 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 θ aufgehen; es ist daher von grosser Wichtigkeit zu wissen, ob eine Primzahl p in dem Index k aufgeht oder nicht. Sobald freilich eine Basis $\omega_1, \omega_2 \ldots \omega_n$ des Gebietes $\mathfrak{o}$, oder auch nur die Grundzahl D des Körpers Ω bekannt ist, erledigt sich diese Frage sehr leicht, weil hieraus k direct gefunden werden kann; denn aus den Coefficienten der Gleichung $F(\theta) = 0$ lässt sich ihre Discriminante

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

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 Ω gegeben ist; es kommt darauf an zu entscheiden, ob eine bestimmte Primzahl p in dem noch unbekannten Index k der Zahl θ aufgeht oder nicht. Dies gelingt nun in der That, wie wir jetzt zeigen wollen, mit Hülfe der Theorie der höheren Congruenzen, und zwar hängt die Entscheidung, wenn wir die früheren Bezeichnungen beibehalten, wesentlich von der Beschaffenheit der Function M ab, welche in der Identität

$$F = P_1^{e_1}P_2^{e_2}\ldots P_m^{e_m} - pM$$

auftritt. Dies ergiebt sich aus den beiden folgenden Sätzen.

II. *Ist der Index k der Zahl θ nicht theilbar durch p, so kann M nach dem Modul p durch keine Primfunction P theilbar 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 theilbar 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 theilbar durch $\mathfrak{p}^2$, folglich $\mathfrak{a}$ theilbar durch $\mathfrak{p}$, mithin $\mathfrak{b}$ nicht theilbar 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 $\mathfrak{p}^e$ theilbar ist, so kann $M(\theta)$ nicht durch $\mathfrak{p}$ theilbar sein, und folglich kann die Function M auch nicht $\equiv 0 \pmod{p, P}$ sein, w. z. b. w.

Auch ohne Benutzung der im vorigen Paragraphen gewonnenen Resultate lässt sich derselbe Satz leicht in der folgenden indirecten, aber vollständig aequivalenten Form beweisen:

Ist F nach dem Modul p theilbar durch das Quadrat einer Primfunction P, also

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

wo $e \geqq 2$, und ist M theilbar durch P, so muss der Index k der Zahl θ durch die Primzahl p theilbar sein.

Behalten die Buchstaben ϱ, σ, η dieselbe Bedeutung, wie im vorigen Paragraphen, setzen wir also

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

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 theilbar sein muss; denn die Function $S P^{e-1}$ ist von niedrigerem Grade als n und auch nicht $\equiv 0 \pmod{p}$. Die Zahl η wird ferner gewiss durch p theilbar sein, wenn bewiesen wird, dass alle in p aufge-

henden Potenzen von Primidealen auch in η 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 ϱ aufgehendes Primideal, so folgt aus $\eta\varrho = p\mu$ unmittelbar, dass η durch die höchste in p aufgehende Potenz von $\mathfrak{p}$ theilbar ist. Ist aber $\mathfrak{p}$ ein in p und gleichzeitig in ϱ aufgehendes Primideal, so ergiebt sich Folgendes. Da S und P relative Primfunctionen sind, so existiren zwei Functionen U, V, welche der Congruenz

$$SU + PV \equiv 1 \pmod{p}$$

genügen (*C.* 4.); hieraus ergeben sich die Zahlen-Congruenzen

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

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

$$er = h + m,$$

und dass der Exponent der höchsten in η aufgehenden Potenz von $\mathfrak{p}$ gleich

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

ist; um daher wieder zu beweisen, dass η durch $\mathfrak{p}^h$ theilbar ist, brauchen wir nur noch zu zeigen, dass

$$m \geqq r$$

ist. Hierbei unterscheiden wir zwei Fälle. Ist erstens $r \geqq h$, so verwerthen wir die erste Annahme unseres Satzes, derzufolge $e \geqq 2$ ist; hieraus folgt in der That $h + m = er \geqq 2r$, 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. $M \equiv PT$ (mod. p), also $\mu \equiv \varrho\, T(\theta)$ (mod. p) ist; da nun sowohl ϱ, als auch p durch

$\mathfrak{p}^r$ theilbar ist, so folgt aus dieser Congruenz, dass auch μ durch $\mathfrak{p}^r$ theilbar, 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 Primfunction P theilbar (mod. p), deren Quadrat zugleich in F aufgeht, so ist der Index k der Zahl θ nicht theilbar durch p.*

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

Ist der Index k der Zahl θ theilbar durch die Primzahl p, so giebt es eine in M aufgehende Primfunction P, deren Quadrat zugleich in F aufgeht (mod. p).

Dem Beweise legen wir die letztere Form zu Grunde, weil die Annahme, dass k durch p theilbar ist, eine leichtere Verwerthung gestattet, insofern aus ihr (nach §. 1) die Existenz einer durch p theilbaren Zahl

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

folgt, deren Coefficienten $x_0, x_1, x_2 \ldots x_{n-1}$ nicht alle durch p theilbar sind. Bezeichnet man nun mit A den grössten gemeinschaftlichen Theiler der beiden Functionen $\varphi(t)$ und F nach dem Modul p, so ist der Grad von A kleiner als n, weil φ von niedrigerem Grade als n und auch nicht $\equiv 0$ (mod. p) ist; setzt man daher

$$F = AB - pM,$$

so ist B keine Constante. Nun existiren zwei Functionen φ_1, φ_2, welche der Congruenz

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

genügen (*C.* 4.); hieraus ergiebt sich, dass die Zahl $A(\theta)$ ebenfalls durch $\mathfrak{p}$ theilbar ist[1]) und folglich einer Gleichung von der Form

1) In ähnlicher Weise kann man leicht zeigen, dass das Kriterium für die Theilbarkeit einer Zahl $\varphi(\theta)$ durch p in der Congruenz $\varphi(t) \equiv 0$ (modd. p, K) besteht, wo K einen völlig bestimmten Theiler der Function F nach dem Modul p bedeutet.

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

genügt, wo $h_1, h_2 \ldots h_s$ ganze rationale Zahlen bedeuten (*D.* §. 160; *B.* §. 13). Da die Gleichung $F(\theta) = 0$ irreductibel ist, so ergiebt sich hieraus eine in Bezug auf die Variabele t identische Gleichung von der Form

$$A^s + p h_1 A^{s-1} + p^2 h_2 A^{s-2} + \ldots + p^s h_s = FG,$$

also auch die Congruenz

$$A^s \equiv 0 \text{ (modd. } p, F);$$

mithin muss die Function A durch jede in F aufgehende Primfunction nach dem Modul p theilbar sein (*C.* 5. und 6.). Multiplicirt 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

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

und hieraus eine Identität von der Form

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

da nun $F \equiv 0$ (modd. p, B), so ergiebt sich

$$M^s \equiv 0 \text{ (modd. } p, B),$$

und folglich ist die Function M durch jede in B aufgehende Primfunction theilbar nach dem Modul p. Oben ist aber gezeigt, dass B keine Constante ist, mithin giebt es wenigstens eine in B aufgehende Primfunction P, und diese muss folglich auch in M aufgehen. Da ferner P in F aufgeht, weil F durch B theilbar ist, und da oben gezeigt ist, dass jede in F aufgehende Primfunction auch in A aufgeht, so geht P ebenfalls in A auf, und folglich ist F theilbar durch P^2, weil $F \equiv AB$ (mod. p) ist. Wir haben mithin wirklich gezeigt, dass es eine in M aufgehende Primfunction P giebt, deren Quadrat zugleich in F aufgeht, w. z. b. w.

Durch die Sätze II und III ist nun in der That die Entscheidung

der Frage, ob der Index k der Zahl θ durch die Primzahl p theilbar ist, vollständig zurückgeführt auf die Zerlegung

$$F = P_1^{e_1} P_2^{e_2} \ldots P_m^{e_m} - pM,$$

durch welche die Function F als Product von lauter Primfunctionen nach dem Modul p dargestellt wird. Zeigt es sich, dass F durch kein Quadrat einer Primfunction theilbar ist, dass also alle Exponenten $e_1, e_2 \ldots e_m = 1$ sind[1]), oder zeigt es sich, dass keine derjenigen Primfunctionen, deren Quadrate in F aufgehen, in M aufgeht, so ist k nicht durch p theilbar, und es gilt der Satz I des §. 2. Giebt es aber eine in M aufgehende Primfunction, deren Quadrat zugleich in F aufgeht, so ist k theilbar durch p, und aus dem zweiten Beweise des Satzes II geht leicht hervor, dass dann die Zerlegung des Ideals $\mathfrak{o}p$ in Primfactoren eine *andere* ist, als die im Satz I behauptete.

Diesem Resultate fügen wir noch folgende Bemerkung hinzu. Sind die Functionen $R_1, R_2 \ldots R_m$ resp. congruent den Functionen $P_1, P_2 \ldots P_m$, so sind sie ebenfalls Primfunctionen, und es wird

$$F = R_1^{e_1} R_2^{e_2} \ldots R_m^{e_m} - pN,$$

wo die Function N durchaus nicht $\equiv M \pmod{p}$ zu sein braucht. Da aber die Theilbarkeit des Index k der Zahl θ durch p von dieser Auswahl der Primfunctionen gänzlich unabhängig ist, so muss man schliessen, dass die Eigenschaft der Function M welche für diese Frage allein entscheidend ist, auch für jede Function N bestehen bleibt. Dies liesse sich leicht durch die Rechnung unmittelbar bestätigen; bezeichnet man mit Q das Product aller derjenigen in F aufgehenden Primfunctionen, deren Quadrate in F *nicht* aufgehen, so kann man durch geeignete Wahl der Functionen $R_1, R_2 \ldots R_m$ stets zu einer Function N gelangen, die relative Primfunction zu Q ist; aber sobald M durch eine Primfunction

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

P theilbar ist, deren Quadrat in F aufgeht, so zeigt die Rechnung, dass auch jede Function N durch P theilbar ist[1]).

§. 4.

In den zuerst von Kummer behandelten Zahlengebieten $\mathfrak{o}$, welche aus einer primitiven Wurzel θ der Gleichung $\theta^m = 1$ entspringen, tritt der glückliche Umstand auf, dass die Potenzen $1, \theta, \theta^2 \ldots \theta^{n-1}$, wo $n = \varphi(m)$, eine Basis des Gebietes $\mathfrak{o}$ bilden, und dass folglich der Index k der Zahl θ, welche der ganzen Untersuchung zu Grunde gelegt wird, stets $= 1$ ist. Bei der allgemeinen Untersuchung eines *beliebigen* endlichen Körpers Ω und des Gebietes $\mathfrak{o}$, welches aus allen in Ω 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 θ des Körpers Ω würde finden lassen, deren Index nicht durch p theilbar wäre, und mit deren Hülfe es folglich gelingen würde, die Bestimmung der Idealfactoren von p auf die Theorie der höheren

---

1) Hiernach beschränkt sich die Idealtheorie von Zolotareff auf den Fall, dass der Index k nicht durch p theilbar 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 Functionen $V, V_1, V_2 \ldots$ theilbar ist. Ist diese Bedingung nicht erfüllt, so kann man für einen gegebenen Modul p die Gleichung $F(x) = 0$ derart transformiren, dass jene Annahme erfüllt ist. Die Auseinandersetzung jener Transformation behält sich der Verfasser für eine andere Gelegenheit vor". — Da es nach meinen Untersuchungen (vergl. §. 5 dieser Abhandlung) Körper giebt, in welchen die Indices *aller* ganzen Zahlen θ durch dieselbe Primzahl p theilbar sind, und folglich auch *alle* Gleichungen $F(\theta) = 0$ diejenige störende Eigenschaft besitzen, welche sich der unmittelbaren Anwendung der Theorie von Zolotareff widersetzt, so vermuthe ich, dass in den eben citirten Worten der Anzeige ein Missverständniss 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 (Schlömilch's *Zeitschrift*, Bd. 10. S. 12 ff.)

Congruenzen zurückzuführen. Da aber alle meine Versuche, die Existenz einer solchen Zahl θ nachzuweisen, fruchtlos blieben, so entschloss ich mich endlich, wo möglich die Unrichtigkeit dieser Vermuthung darzuthun, und zu diesem Ziele gelangte ich, wie ich schon in den *Göttingischen gelehrten Anzeigen* vom 20. September 1871 angedeutet habe, durch die Betrachtungen, welche den Gegenstand dieses und des folgenden Paragraphen bilden.

Es sei p eine bestimmte Primzahl, und $\mathfrak{p}_1, \mathfrak{p}_2 \ldots \mathfrak{p}_m$ seien die sämmtlichen von einander verschiedenen Primideale, welche in p aufgehen; ihre Grade wollen wir mit $f_1, f_2 \ldots f_m$ bezeichnen, so dass z. B. $N(\mathfrak{p}_1) = p^{f_1}$ ist. Existirt nun eine ganze Zahl θ in Ω, deren Index k nicht durch p theilbar ist, so folgt aus dem Satze I in §. 2, dass es in Bezug auf den Modul p auch m *incongruente* Primfunctionen $P_1, P_2 \ldots P_m$ *giebt*, deren Grade resp. gleich $f_1, f_2 \ldots f_m$ sind. Es ist nun von der grössten Wichtigkeit für unsere Untersuchung, dass diese Folgerung sich umkehren lässt, dass also folgender Satz besteht:

IV *Sind $f_1, f_2 \ldots f_m$ die Grade der sämmtlichen verschiedenen, in der Primzahl p aufgehenden Primideale $\mathfrak{p}_1, \mathfrak{p}_2 \ldots \mathfrak{p}_m$, und giebt es m nach dem Modul p incongruente Primfunctionen $P_1, P_2 \ldots P_m$ resp. vom Grade $f_1, f_2 \ldots f_m$, so existirt in Ω eine ganze Zahl θ, deren Index k nicht durch p theilbar ist.*

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

Es sei $\mathfrak{p}$ irgend ein in p aufgehendes Primideal vom Grade f, so genügen (*D.* §. 163; *B.* §. 26, 3⁰) *alle* ganzen Zahlen ω des Körpers Ω der Congruenz

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

bedeutet nun t wieder eine Variabele, so ist die Function

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

nach dem Modul p congruent dem Producte aus allen incongruenten Primfunctionen, deren Grade Divisoren der Zahl f sind (*C.* 19.); unter

diesen wähle man *nach Belieben* eine solche Primfunction P, deren Grad $= f$ ist; dies ist stets möglich, da es immer mindestens eine solche Function giebt (*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 $\mathfrak{p}$ theilbar ist, so folgt, dass *jede* in $\mathfrak{o}$ enthaltene Zahl ω der Congruenz

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

genügt; mithin ist die Anzahl ihrer nach $\mathfrak{p}$ incongruenten 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 $\mathfrak{o}$ eine Congruenz $r$ten Grades, deren Modul ein Primideal dieses Gebietes ist, niemals mehr als r incongruente Wurzeln haben kann, und hieraus folgt für unseren Fall, dass die Congruenz $H(\omega) \equiv 0 \pmod{\mathfrak{p}}$ höchstens $(p^f - f)$ incongruente Wurzeln besitzt, und dass folglich die Repraesentanten ω der f übrigen Zahlclassen nothwendig der Congruenz $P(\omega) \equiv 0 \pmod{\mathfrak{p}}$ genügen müssen. Für unseren Zweck reicht aber schon die Gewissheit aus, dass diese Congruenz wenigstens eine Wurzel hat. Es sei α 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 Congruenz

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

mit der Functionen-Congruenz

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

gleichbedeutend ist. In der That, wenn die letztere Statt findet, 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 $\mathfrak{p}$ theilbar sind, so ist auch $\varphi(\alpha) \equiv 0 \pmod{p}$; ist aber zweitens $\varphi(t)$ *nicht* theilbar durch die Primfunction $P(t)$, so sind $\varphi(t)$ und $P(t)$ relative Primfunctionen, und folglich existiren zwei Functionen $\varphi_1(t)$, $\varphi_2(t)$, welche der Congruenz

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

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 $\mathfrak{p}$ theilbar 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 $\mathfrak{p}^2$ theilbar ist, wollen wir ferner die Wurzel α der Congruenz $P(\alpha) \equiv 0 \pmod{\mathfrak{p}}$ so wählen, dass die Zahl $P(\alpha)$ *nicht* durch $\mathfrak{p}^2$ theilbar wird. Dies ist stets möglich; ist nämlich α eine Wurzel der Congruenz $P(\alpha) \equiv 0 \pmod{\mathfrak{p}^2}$, so wähle man nach Belieben eine durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ theilbare Zahl λ, und setze $\alpha' = \alpha + \lambda$, so ist

$$\begin{aligned} P(\alpha') &= P(\alpha) + \lambda P'(\alpha) + \lambda^2 P''(\alpha) + \ldots \\ &\equiv \lambda P'(\alpha) \pmod{\mathfrak{p}^2}; \end{aligned}$$

da nun die derivirte Function $P'(t)$ 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 theilbar durch $\mathfrak{p}$; mithin ist das Product $\lambda P'(\alpha)$, und folglich auch die Zahl $P(\alpha')$ wohl theilbar durch $\mathfrak{p}$, aber nicht theilbar durch $\mathfrak{p}^2$. Nachdem so die Existenz einer solchen Zahl α' bewiesen ist, lassen wir den Accent wieder weg, und nehmen also an, dass $P(\alpha)$ durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ theilbar ist.

Ist nun $\mathfrak{p}^e$ die höchste in p aufgehende Potenz des Primideals $\mathfrak{p}$, so wollen wir beweisen, dass die Zahlen-Congruenz

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

mit der Functionen-Congruenz

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

gleichbedeutend ist. In der That, wenn die letztere Statt findet, 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 $\mathfrak{p}^e$ theilbar sind, so folgt $\varphi(\alpha) \equiv 0 \pmod{\mathfrak{p}^e}$; wenn dagegen die Functionen-Congruenz *nicht* Statt findet, so ist der grösste gemeinschaftliche Theiler, welchen die Functionen $\varphi(t)$ und $P(t)^e$ nach dem Modul p haben, von der Form $P(t)^s$, wo $s < e$; bestimmt man die Functionen $\varphi_1(t)$, $\varphi_2(t)$ 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 $\mathfrak{p}^e$ theilbar sind, so ergiebt sich

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

da nun $s < e$, und $P(\alpha)$ nicht durch $\mathfrak{p}^2$ theilbar ist, so ist $P(\alpha)^s$ nicht theilbar 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 $\mathfrak{p}_1, \mathfrak{p}_2 \ldots \mathfrak{p}_m$ so, wie es im Vorhergehenden beschrieben ist, d. h. man wähle *nach Belieben* m Primfunctionen $P_1, P_2 \ldots P_m$, welche resp. dieselben Grade $f_1, f_2 \ldots f_m$ haben, wie jene Primideale, und bestimme ebenso viele Zahlen $\alpha_1, \alpha_2 \ldots \alpha_m$ der Art, dass $P_1(\alpha_1), P_2(\alpha_2) \ldots P_m(\alpha_m)$ resp. durch $\mathfrak{p}_1, \mathfrak{p}_2 \ldots \mathfrak{p}_m$ theilbar werden, mit der eventuellen Beschränkung, dass eine solche Zahl $P_r(\alpha_r)$ nicht durch $\mathfrak{p}_r^2$ theilbar sein darf, falls p durch $\mathfrak{p}_r^2$ theilbar ist. Da nun die Primideale $\mathfrak{p}_1, \mathfrak{p}_2$

$\ldots \mathfrak{p}_m$ von einander verschieden, und ihre Quadrate folglich relative Primideale sind, so kann man stets eine Zahl θ 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 ergiebt sich, dass die Zahlen $P_1(\theta)$, $P_2(\theta) \ldots P_m(\theta)$ resp. durch $\mathfrak{p}_1, \mathfrak{p}_2 \ldots \mathfrak{p}_m$ theilbar sind, dass aber, falls p durch $\mathfrak{p}_r^2$ theilbar ist, die Zahl $P_r(\theta)$ *nicht* durch $\mathfrak{p}_r^2$ theilbar ist. Die Zahl θ vereinigt daher in sich alle diejenigen Eigenschaften in Bezug auf die sämmtlichen m Primideale, welche einer jeden Zahl α_r in Bezug auf das ihr correspondirende Primideal $\mathfrak{p}_r$ zukommen. Ist daher

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

also, wie aus der Bildung der Norm hervorgeht,

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

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

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

Statt findet; da ferner eine ganze Zahl des Körpers stets und nur dann

durch p theilbar ist, wenn sie durch *jede* der m Potenzen $\mathfrak{p}_1^{e_1}, \mathfrak{p}_2^{e_2} \ldots \mathfrak{p}_m^{e_m}$ theilbar ist, so leuchtet ein, dass die eine Zahlen-Congruenz

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

gleichbedeutend ist mit dem *System* der m vorstehenden Functionen-Congruenzen.

Bis hierher haben wir absichtlich über die *Wahl* der Primfunctionen $P_1, P_2 \ldots P_m$ nichts Anderes festgesetzt, als dass ihre Grade resp. mit denen der Primideale $\mathfrak{p}_1, \mathfrak{p}_2 \ldots \mathfrak{p}_m$ 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 unter einander *incongruente* Primfunctionen von den vorgeschriebenen Graden *giebt*, und wir wollen unter $P_1, P_2 \ldots P_m$ solche incongruente Primfunctionen verstehen. Dann sind die Potenzen $P_1^{e_1}, P_2^{e_2} \ldots P_m^{e_m}$ relative Primfunctionen, und wenn man ihr Product

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

setzt, so ist (*C.* 5.) das System der m obigen Functionen-Congruenzen, und folglich auch die eine Zahlen-Congruenz

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

gleichbedeutend mit der einzigen Functionen-Congruenz

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

Da ferner der Grad des Productes R gleich

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

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

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

nur dann durch p theilbar sein, wenn

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

d. h. wenn alle n Coefficienten $x_0, x_1, x_2 \ldots x_{n-1}$ durch p theilbar sind. Der Index k der Zahl θ ist folglich (nach §. 1) *nicht* theilbar durch p.

Hiermit ist unser obiger Satz bewiesen, und wir fügen nur noch die folgende Bemerkung hinzu.

Da k nicht theilbar durch p ist, so ist k auch von 0 verschieden, und folglich ist die gefundene Zahl θ die Wurzel einer irreductibelen Gleichung $F(\theta) = 0$ vom $n$ten Grade; da nun $F(\theta) \equiv 0 \pmod{p}$, so muss die Function F durch R theilbar sein nach dem Modul p; da ferner beide Functionen denselben Grad n und denselben höchsten Coefficienten 1 haben, so muss $F \equiv R \pmod{p}$, d. h.

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

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

§. 5.

Die letzte Untersuchung hat uns ein Kriterium geliefert, durch welches die Frage entschieden wird, ob es wirklich in Ω eine ganze Zahl θ giebt, deren Index durch eine gegebene Primzahl p *nicht* theilbar ist. Wenn

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

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

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

ihre Anzahl ist $= p$; der obige singuläre Fall wird daher gewiss in einem Körper Ω eintreten, in welchem die Primzahl p durch mindestens $(p+1)$ verschiedene Primideale ersten Grades theilbar ist; da aber, wie

aus der Betrachtung der Normen hervorgeht, das Ideal $\mathfrak{o}p$ ein Product 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 *cubische* Körper Ω giebt, in welchen die Zahl 2 durch *drei* verschiedene Primideale ersten Grades theilbar ist; in einem solchen Körper würden die Indices *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 mitzutheilen.

Es sei α eine Wurzel der irreductibelen Gleichung dritten Grades

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

um ihre Discriminante zu finden, betrachten wir die Zahl

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

und bilden successive, unter Zuziehung von $F(\alpha) = 0$, die Producte

$$\begin{aligned} \delta\alpha &= 24 + 4\alpha + \alpha^2 \\ \delta\alpha^2 &= 8 + 26\alpha + 5\alpha^2; \end{aligned}$$

durch lineare Elimination von 1, α, α^2 aus diesen drei Gleichungen erhält man

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

d. h.

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

und folglich ist die Discriminante

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

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

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

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

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

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 theilbar, 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 That, man erhält mit Rücksicht auf $F(\alpha) = 0$ die Gleichungen

$$\begin{aligned} \alpha^2 &= 2 + \alpha + 2\beta \\ \beta^2 &= -2 + 2\alpha - \beta \\ \alpha\beta &= 4 \end{aligned}$$

und hieraus

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

Da ferner

$$\begin{aligned} 1 &= 1.1 + 0.\alpha + 0.\beta \\ \alpha &= 0.1 + 1.\alpha + 0.\beta \\ \alpha^2 &= 2.1 + 1.\alpha + 2.\beta, \end{aligned}$$

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) theilbar ist, so ist sie die Grundzahl D unseres cubischen Körpers Ω, und die Zahlen $1, \alpha, \beta$ bilden eine Basis des aus allen ganzen Zahlen ω dieses Körpers Ω bestehenden Gebietes $\mathfrak{o}$, 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 ω 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 Resultates die Idealfactoren der Zahl 2 bestimmen. Da

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

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 ω des Gebietes $\mathfrak{o}$ genügt der Congruenz

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

Hieraus folgt zunächst, dass die Zahl 2 durch kein Quadrat eines Primideals theilbar 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 $\mathfrak{o}(2)$ theilbar ist, eine Zahl ω existiren, welche durch $\mathfrak{p}\mathfrak{q}$, aber nicht durch 2 theilbar wäre; dann wäre aber ω^2 theilbar durch $\mathfrak{p}^2\mathfrak{q}^2$, also auch durch 2, und dies widerspricht der vorstehenden Congruenz $\omega^2 \equiv \omega \pmod 2$. Mithin ist $\mathfrak{o}(2)$ entweder ein Primideal oder ein Product aus lauter verschiedenen Primidealen. Es sei $\mathfrak{p}$ irgend ein in 2 aufgehendes Primideal, so genügt *jede* in $\mathfrak{o}$ enthaltene Zahl ω der Congruenz

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

und folglich ist die Anzahl ihrer incongruenten Wurzeln $= (\mathfrak{o}, \mathfrak{p}) = N(\mathfrak{p})$; da diese Anzahl aber niemals grösser als der Grad der Congruenz sein

kann, so ergiebt 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* von einander verschiedene Primideale ersten Grades bedeuten. Hiermit ist das Auftreten der erwähnten singulären Erscheinung erwiesen, und es muss sich bestätigen, dass die Indices *aller* Zahlen ω durch 2 theilbar sind. In der That, setzt man

$$\begin{aligned} z' &= z^2 + 2x^2 - 2y^2 + 8xy \\ x' &= x^2 + 2y^2 + 2xz \\ y' &= 2x^2 - y^2 + 2yz, \end{aligned}$$

so ist

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

und der Index der Zahl ω 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:

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

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 That die beiden fundamentalen Eigenschaften eines Ideals, nämlich:

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

II. Jedes Product aus einer Zahl α' des Systems $\mathfrak{a}$ und aus einer Zahl ω des Gebietes $\mathfrak{o}$ ist wieder eine Zahl des Systems $\mathfrak{a}$.

Die erste Eigenschaft ist evident, und um die zweite nachzuweisen, genügt es darzuthun, dass die Producte aus je einer der Basiszahlen 2, α, $(1+\beta)$ von $\mathfrak{a}$ und je einer der Basiszahlen 1, α, β von $\mathfrak{o}$ sämmtlich in $\mathfrak{a}$ enthalten sind; dies ist unmittelbar evident für die fünf Producte

$$2.1,\ \alpha.1,\ (1+\beta).1,\ 2.\alpha,\ 2.\beta = -2+2(1+\beta),$$

und für die übrigen vier ergiebt sich dasselbe aus den Gleichungen

$$\alpha.\alpha = \alpha+2(1+\beta),\ \alpha.\beta = 2.2,$$
$$(1+\beta)\alpha = 2.2+\alpha,\ (1+\beta)\beta = -2+2\alpha.$$

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 $\mathfrak{m}$ incongruenten 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, 4^0). Es ist daher z. B.

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

und ebenso ergiebt sich

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

Wenn aber die Norm eines Ideals eine Primzahl ist, so muss das Ideal nothwendig 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 von einander, weil die in $\mathfrak{b}$ und in $\mathfrak{c}$ enthaltene Zahl β nicht in $\mathfrak{a}$ enthalten, und weil die in $\mathfrak{c}$ enthaltene Zahl α nicht in $\mathfrak{b}$ enthalten ist. Es muss folglich die in allen drei Idealen enthaltene Zahl 2 auch in dem Pro-

ducte $\mathfrak{abc}$ enthalten sein; mithin ist $\mathfrak{o}(2) = \mathfrak{mabc}$, wo $\mathfrak{m}$ ein Ideal bedeutet; nimmt man aber die Norm, so ergiebt sich

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

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

Unter dem *Producte* $\mathfrak{ab}$ zweier Ideale wird das System aller Producte $\alpha'\beta'$ und aller Summen von solchen Producten $\alpha'\beta'$ verstanden, wo α', β' beliebige Zahlen resp. der Ideale $\mathfrak{a}$, $\mathfrak{b}$ bedeuten (*D.* §. 163; *B.* §. 22). Ein solches Product erscheint daher zunächst als ein endlicher Modul, dessen Basiszahlen die sämmtlichen Producte aus je einer Basiszahl von $\mathfrak{a}$ und je einer Basiszahl von $\mathfrak{b}$ sind. In unserem Falle ist daher $\mathfrak{ab}$ der endliche Modul, dessen Basiszahlen die neun Producte

$$2.2 = 4, \quad 2(1+\alpha) = 2+2\alpha, \qquad 2.\beta = 2\beta,$$
$$\alpha.2 = 2\alpha, \quad \alpha(1+\alpha) = 2+2\alpha+2\beta, \quad \alpha\beta = 4,$$
$$(1+\beta).2 = 2+2\beta, \quad (1+\beta)(1+\alpha) = 5+\alpha+\beta, \quad (1+\beta)\beta = -2+2\alpha$$

sind; da aber von diesen neun Zahlen nur drei von einander *unabhängig* sind (*D.* §. 159; *B.* §. 4), so ist die von mir ausführlich beschriebene Methode (*B.* §. 4, 6^0) 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:

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

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

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

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

$$\begin{aligned}
\alpha(\alpha-2)(1+\alpha) &= 2^3\ ; & \alpha\beta &= (\alpha-2)(1+\alpha+\beta) = 2^2\\
(\alpha-2)(3+\alpha+\beta) &= 2\alpha; & \alpha(2-\beta) &= 2(\alpha-2)\\
(\alpha-2)(3+2\alpha+\beta) &= \alpha^2\ ; & \alpha(\alpha+\beta-4) &= (\alpha-2)^2.
\end{aligned}$$

Durch dieses Beispiel, welchem man viele andere an die Seite stellen könnte, ist ausser Zweifel gesetzt, dass es Körper Ω giebt, in welchen die Indices *aller* ganzen Zahlen durch eine und dieselbe Primzahl p theilbar sind. Dies Resultat ist in mancher Beziehung kein willkommenes. Es giebt in der That sehr wichtige Sätze der Idealtheorie, welche sich durch die Theorie der höheren Congruenzen sehr leicht würden beweisen lassen, wenn der Satz I in §. 2 nicht an die Voraussetzung gebunden wäre, dass der Index k der Zahl θ nicht durch p theilbar sein darf; wir haben aber jetzt gesehen, dass in manchen Fällen diese Voraussetzung auf keine Weise zu erfüllen ist, wie man auch die Zahl θ 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 Ω ist aus allen und nur aus denjenigen rationalen Primzahlen p zusammengesetzt, welche in diesem Körper durch das Quadrat eines Primideals theilbar sind.

Giebt es in Ω eine ganze Zahl, deren Index durch die Primzahl p nicht theilbar 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.