22.

Über einige allgemeine Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhangt, nebst Anwendungen derselben auf die Zahlentheorie.

(Als Fortsetzung der Abhandlung No. 19. im vorhergehenden Hefte.)

(Von Herrn Dr. G. *Eisenstein* zu Berlin.)

---

§. 4.

Aus dem im vorigen Paragraphen über die Form $y = \frac{x^{N(m)} + mP}{1 + mQ}$ der rationalen Function y von x bewiesenen Satze fliefsen durch Verallgemeinerung und wiederholte Anwendung desselben fruchtbare Principien, mittelst welcher sich die Lösung mannigfaltiger wichtiger Probleme über Lemniscatentheilung und deren Anwendung auf die Zahlentheorie bewerkstelligen läfst, während sich diesen Problemen auf anderen Wegen, so viel ich sehe, unüberwindliche Schwierigkeiten entgegenstellen.

Zunächst kann man den Satz selbst auf den Fall ausdehnen, wenn an die Stelle der complexen und primären Primzahl m eine beliebige Potenz von m gesetzt wird; denn da sich $\varphi(m^2t)$ in $\varphi(mt)$, $\varphi(m^3t)$ in $\varphi(m^2t)$ u. s. w. allgemein $\varphi(m^\mu t)$ in $\varphi(m^{\mu-1}t)$ eben so ausdrücken lassen, wie $\varphi(mt)$ in $\varphi(t)$, d. h. y in x, so ersieht man durch successive Substitution, dafs $\varphi(m^\mu t)$ von der Form $\frac{\varphi(t)^{p^\mu} + mP}{1 + mQ}$ sein wird, wo P und Q ganze ganzzahlige Functionen von $\varphi(t) = x$ sind; denn man sieht leicht, dafs wenn allgemein $f_1(x)$ und $f_2(x)$ irgend zwei ganze ganzzahlige Functionen von x sind, der Quotient $\frac{f_1(y)}{f_2(y)}$ die Form $\frac{f_1(x^p) + mP}{f_2(x^p) + mQ}$ annehmen wird.

Durch Multiplication mit dem Nenner ergiebt sich y in der Form $x^p + m(P - Qy)$, d. h. $\varphi(mt) = \varphi(t)^p + mT$, und allgemeiner $\varphi(m^\mu t) = \varphi(t)^{p^\mu} + mT$, wo T eine ganze ganzzahlige Function von den Gröfsen $\varphi(t)$, $\varphi(mt)$, $\varphi(m^2t)$ u. s. w. bis $\varphi(m^\mu t)$ ist.

Man wird leicht darauf geführt, bei Gelegenheit der Theilung der Lemniscate für den Divisor m den in Rede stehenden Satz auf einen von m *verschiedenen* Multiplicator n zu übertragen; denn wenn t von der Form $\frac{rC}{m}$ ist, so ist $\varphi(nt)$ zugleich mit $\varphi(t)$ Wurzel der Gleichung $W=0$ für jeden nicht durch m theilbaren Werth von n, und wenn n primäre Primzahl ist, so läfst sich dann $\varphi(nt)$ durch $\varphi(t)$ in der Form $\varphi(t)^q+nT$ ausdrücken, wo T eine ganze ganzzahlige Function der Wurzeln der Gleichung $W=0$ (hier von *zwei* Wurzeln) ist; es läfst sich diese Form auch benutzen, um umgekehrt $\varphi(t)^q$ durch $\varphi(nt)$ in der Form $\varphi(nt)+nT$ auszudrücken; q ist hier die Norm von n. Es ist dabei nicht zu vergessen, dafs man zwar T auch durch eine einzige Wurzel der Gleichung $W=0$ ausdrücken kann, dafs aber dann die Coëfficienten im Allgemeinen aufhören ganze Zahlen zu sein; für viele Untersuchungen ist es jedoch vortheilhafter, eine Function mehrerer Wurzeln mit ganzen Coëfficienten als eine solche von einer einzigen mit gebrochenen Coëfficienten zu betrachten.

Man bezeichne durch Ω_k den Inbegriff der $p-1$ Wurzeln der Gleichung $W=0$ in der schon oben angezogenen Form $\varphi\left(\frac{rkC}{m}\right)$, und es sei jetzt $F(k)$ eine beliebige ganze ganzzahlige Function aller oder einiger der $p-1$ Wurzeln Ω_k, welche recht gut als Function von k allein aufgefafst werden kann, also eine Summe von Termen von der Form

$$h.\varphi\left(\frac{r_1kC}{m}\right)^{\alpha_1}\varphi\left(\frac{r_2kC}{m}\right)^{\alpha_2}\ldots.\ \varphi\left(\frac{r_{p-1}kC}{m}\right)^{\alpha_{p-1}}=Z,$$

wo h eine ganze complexe Zahl ist und $\alpha_1, \alpha_2, \ldots. \alpha_{p-1}$ nicht negative ganze Exponenten vorstellen. Erhebt man ein solches Polynom $F(k)$ zur $q$ten Potenz, so kommen in der polynomischen Entwicklung desselben erstlich alle Glieder wie

$$h^q.\varphi\left(\frac{r_1kC}{m}\right)^{q\alpha_1}.\varphi\left(\frac{r_2kC}{m}\right)^{q\alpha_2}\ldots.\ \varphi\left(\frac{r_{p-1}kC}{m}\right)^{q\alpha_{p-1}}=Z^q$$

vor. Was die übrigen Glieder betrifft, so sind ihre Coëfficienten sämmtlich durch q, respective $\sqrt{q}$ theilbar, je nachdem q selbst Primzahl oder das Quadrat einer Primzahl, d. h. je nachdem n, deren Norm q ist, eine zweigliedrige oder eine eingliedrige complexe Primzahl vorstellt; in beiden Fällen sind die Coëfficienten der übrigen Glieder also durch n theilbar. Vernachlässigt man die durch n theilbaren Glieder, so bleiben nur diejenigen von der Form Z^q stehen. Man giebt der letzteren Potenz eine einfachere Form, wenn man be-

merkt, dafs mit Hinweglassung von Gliedern, welche den Factor n enthalten, h statt h^q und nach obigem Princip $\varphi\left(\frac{r_1 nkC}{m}\right)$ statt $\varphi\left(\frac{r_1 kC}{m}\right)^q$, $\varphi\left(\frac{r_2 nkC}{m}\right)$ statt $\varphi\left(\frac{r_2 kC}{m}\right)^q$ u. s. w. gesetzt werden darf; so erhält man

$$h.\varphi\left(\frac{r_1 nkC}{m}\right)^{\alpha_1}.\varphi\left(\frac{r_2 nkC}{m}\right)^{\alpha_2}.\ldots.\varphi\left(\frac{r_{p-1} nkC}{m}\right)^{\alpha_{p-1}} = Z_n.$$

Die Summe aller Glieder von dieser Form giebt aber genau Dasjenige, was aus $F(k)$ folgt, wenn überall nk an die Stelle von k gesetzt wird, also $F(nk)$.

„Wenn also $F(k)$ irgend eine ganze ganzzahlige Function der Wurzeln „Ω_k vorstellt, so ist immer $F(k)^q = F(nk) + nT$; wo T eine ähnliche „ganze Function, n eine beliebige von m verschiedene primäre complexe „Primzahl und q deren Norm bedeutet."

Dieser Satz ist von besonderer Wichtigkeit für Anwendungen auf die Zahlentheorie. Man bemerke noch, dafs die Coëfficienten in T von k unabhängig sind. Übrigens kann auch $n = m$, also $q = p$ sein; dann reducirt sich $F(nk) = F(mk) = F(0)$ auf eine ganze complexe Zahl und wird gleich dem Coëfficienten h desjenigen Gliedes, in welchem sämmtliche Exponenten $\alpha_1, \alpha_2, \ldots. \alpha_{p-1}$ der Null gleich sind: also selbst $= 0$, wenn ein solches Glied nicht vorkommt. Dies folgt daraus, dafs $\varphi(0) = 0$ ist.

Wenn man die gefundene Gleichung $F(k)^q = F(nk) + nT$ wiederholt auf beiden Seiten zur $q$ten Potenz erhebt und $F(n^2k)$ statt $F(nk)^q$, $F(n^3k)$ statt $F(n^2k)^q$ u. s. w. setzt, was nach derselben Gleichung erlaubt ist, so erhält man das allgemeinere Resultat

$$F(k)^{q^\mu} = F(n^\mu k) + nT;$$

wo T nicht dieselbe, aber eine ähnliche Function ist wie oben. Statt n^μ in $F(n^\mu k)$ kann man natürlich seinen Rest (mod. m) setzen; ist z. B. $n^\mu \equiv 1 \pmod{m}$, so hat man $F(k)^{q^\mu} = F(k) + nT$.

Der allgemeine Coëfficient h des Polynoms F, welcher bisher als ganze Zahl angenommen wurde, könnte selbst eine oder mehrere andere Gröfsen $z_1, z_2, \ldots.$ in ganzen Verbindungen enthalten. Schreibt man, um diese letzteren sichtbar zu machen, $F(k; z_1, z_2, \ldots.)$ statt $F(k)$, so hat man in diesem Falle:

$$F(k; z_1, z_2, \ldots.)^q = F(nk; z_1^q, z_2^q, \ldots.) + nT(z_1, z_2, \ldots.),$$

$$F(k; z_1, z_2, \ldots.)^{q^2} = F(n^2k; z_1^{q^2}, z_2^{q^2} \ldots.) + nT(z_1, z_2, \ldots.),$$

u. s. w. Fernere Reductionen bieten sich hier dar, wenn für die Gröfsen

z Wurzeln der Einheit genommen werden, oder auch lemniscatische Functionen aliquoter Theile des Umfanges C, welche sich auf andere Divisoren m', m'', u. s. w. beziehen. Namentlich findet sich, wenn z irgend eine $p-1$te Wurzel der Einheit, g eine primitive Congruenzwurzel mod. m, $n \equiv g^\nu \pmod{m}$, und $F(k;z)$ von der Form

$$F(k;z) = F(k) + zF(gk) + z^2F(g^2k) + \text{etc.} + z^{p-2}F(g^{p-2}k)$$

angenommen wird:

$$F(k;z)^q = F(nk;z^q) + nT(z) = \omega^{-q\nu}F(k;z^q) + nT(z).$$

Dies mag genügen, um die Verallgemeinerung desjenigen Princips zu zeigen, welches in seiner einfachsten Form durch die Gleichung $\varphi\left(\frac{kC}{m}\right)^{N(n)} = \varphi\left(\frac{nkC}{m}\right) + nT$ dargestellt wird. Unter den zahlreichen Anwendungen desselben will ich nur hervorheben, dafs sich mit Hülfe desselben die Divisoren (nämlich die complexen im gewöhnlichen *Gaufsischen* Sinne) derjenigen Gleichungen vollständig bestimmen lassen, welchen die Perioden aus den Wurzeln der Gleichung $W = 0$ oder aus ganzen Functionen dieser Wurzeln Genüge leisten. Man erhält auf diese Weise zahlentheoretische Sätze von grofser Allgemeinheit, welche denen von *Kummer* für die Kreistheilung aufgestellten vollkommen analog sind. Was z. B. die Function W selbst betrifft, so hat dieselbe aufser den Divisoren $1+i$ und m nur solche Primtheiler, welche $\equiv 1 \pmod{m}$ sind, und wenn umgekehrt n eine complexe Primzahl $\equiv 1 \pmod{m}$ ist, so hat die Congruenz $W \equiv 0 \pmod{n}$ $p-1$ Wurzeln, nämlich so viele als ihr Grad beträgt. Ist ferner μ für *irgend eine* primäre complexe Primzahl n der kleinste Exponent, der $n^\mu \equiv 1 \pmod{m}$ macht, so ist $W \equiv$ dem Producte aus $\frac{p-1}{\mu}$ ganzen ganzzahligen und *irreductibeln* Ausdrücken $\pmod{n}$ (im Sinne von *Schoenemann*) vom Grade μ. Der letztere Satz ist das Analogon zu einem von *Schoenemann* über den Ausdruck $\frac{x^p-1}{x-1}$ in seiner Abhandlung im 31ten Bande gegenwärtigen Journals bewiesenen Satzes *).

*) *Schoenemann* hat das Verdienst, zu einer allgemeineren und mehr erschöpfenden Auffassungsweise der Probleme über Congruenzen angeregt zu haben, indem er darauf aufmerksam machte, dafs neben der gewöhnlichen Frage nach den Wurzeln einer Congruenz, resp. Lösbarkeit oder Nichtlösbarkeit derselben, welche sich nur auf die Linearfactoren bezieht, auch die Factoren höherer Grade eines in Hinsicht auf einen vorgelegten Modul zu untersuchenden Ausdrucks berücksichtigt werden müssen. Nachdem der genannte Verfasser gezeigt, dafs sich jeder gegebene Ausdruck auf eine und nur eine Weise dem Producte irreductibler Factoren congruent setzen läfst, hat er ferner die

§. 5.

Die eben gemachten Auseinandersetzungen bezogen sich auf mod. n, eine von m verschiedene complexe Primzahl, und waren Folgerungen aus dem Satze, dafs, mit Vernachlässigung des $n$fachen einer ganzen Function von $\varphi(t)$ und $\varphi(nt)$, $\varphi(nt)$ sich auf $\varphi(t)^q$ und umgekehrt $\varphi(t)^q$ sich auf $\varphi(nt)$ zurückführen läfst. Ich kehre jetzt zum Modul m und zu denjenigen Schlüssen zurück, welche sich unmittelbar daran anknüpfen, dafs in der Gleichung $W = x^{p-1} + A_1 x^{p-5} + A_2 x^{p-9} + \text{etc.} = 0$ die Coëfficienten A_1, A_2, etc. durch m theilbare ganze Zahlen sind. Da jede symmetrische ganze ganzzahlige Function der Wurzeln sich als ganze ganzzahlige Function dieser Coëfficienten ausdrücken läfst, so ist jede solche symmetrische Function einer ganzen Zahl gleich, welche $\equiv 0 \pmod{m}$. Eine Ausnahme macht der Fall, wenn in der symmetrischen Function ein Glied vorkommt, welches die Wurzeln gar nicht enthält: dann ist die Function dem unabhängigen Gliede congruent (mod. m). Z. B., wenn w, w', w'', etc. die sämmtlichen $p-1$ Wurzeln der Gleichung $W = 0$ bezeichnen, so ist ein Product aus $p-1$ Factoren, wie

$$(a_0 + a_1 w + a_2 w^2 + \ldots.)(a_0 + a_1 w' + a_1 w'^2 + \text{etc.}) \ldots.,$$

wo a_0, a_1, etc. ganze Zahlen sind, $\equiv$ dem unabhängigen Gliede $a_0^{p-1} \pmod{m}$; ein solches Product ist also immer $\equiv 1 \pmod{m}$ und nie durch m theilbar, aufser wenn a_0 durch m theilbar ist. Unter den symmetrischen Functionen verdienen die Potenzsummen der Wurzeln eine besondere Beachtung. Bezeichnet man durch $\Sigma f(x)$ die Summe der $p-1$ Gröfsen $f(w) + f(w') + f(w'') + \text{etc.}$, so ist $\Sigma x^\mu \equiv 0 \pmod{m}$, aufser für $\mu = 0$; dann ist $\Sigma x^0 = p-1 \equiv -1 \pmod{m}$. Wenn demnach $f(x)$ irgend eine ganze ganzzahlige Function von x vorstellt, deren constantes Glied $= a$, so ist $\Sigma f(x) \equiv (p-1)a \equiv -a \pmod{m}$.

Existenz, die Anzahl und die wichtigsten allgemeinen Eigenschaften der irreductibeln Congruenzen aller Grade nachgewiesen. — Die von *Kummer* Seite 107 ff. im 30ten Bande des gegenwärtigen Journals gegebenen Sätze müssen der Betrachtungsweise von *Schoenemann* gemäfs ergänzt werden; was keine grofsen Schwierigkeiten darbietet. Setzt man $p-1 = ef$, und bedeutet μ den kleinsten Exponenten, welcher $q^\mu \equiv 1 \pmod{p}$ macht; ferner ϑ den gröfsten gemeinschaftlichen Theiler zwischen $\frac{p-1}{\mu}$ und $\frac{p-1}{f} = e$, so ist die Gleichung vom $e$ten Grade für die Perioden aus f Gliedern, wenn sie als Congruenz (mod. q) aufgefafst wird, genau in ϑ irreductible Ausdrücke vom Grade $\frac{e}{\vartheta}$ zerfällbar; einige specielle Werthe der Primzahl q geben Ausnahmefälle. Ganz Analoges gilt in Bezug auf die Wurzeln der Gleichung $W = 0$, wenn statt der reellen Primzahl q eine complexe n gesetzt wird und wenn μ den kleinsten Exponenten bedeutet, der $n^\mu \equiv 1 \pmod{m}$ macht; wie ich in einer besondern Abhandlung beweisen werde. n wird immer *primär* angenommen.

Die höheren Potenzsummen, von der $p-1$ten incl. aufwärts, kann man auch nach mod. m^2 bestimmen, von der $2(p-1)$ten an nach mod. m^3, u. s. w.; denn es ist $\Sigma W = 0$, also $\Sigma x^{p-1} = -A_1 \Sigma x^{p-5} - \ldots - m\Sigma x^0$, und da hier rechts jedes Glied aufser dem letzten durch m^2 theilbar ist, so erhält man $\Sigma x^{p-1} \equiv -m(p-1) \equiv m \pmod{m^2}$. Ferner ist auch $\Sigma x^\mu W = 0$, also $\Sigma x^{p-1+\mu} = -A_1 \Sigma x^{p-5+\mu} - \text{etc.} \equiv 0 \pmod{m^2}$, wenn $\mu > 0$. Nachdem erst einmal bewiesen, dafs alle Potenzsummen, deren Exponent zwischen $p-1$ und $2(p-1)$ liegt, durch m^2 theilbar sind, folgt wieder aus der Gleichung $\Sigma x^{p-1+\mu} = -A_1 \Sigma x^{p-5+\mu} - \text{etc.}$, dafs $\Sigma x^{2(p-1)} \equiv -m^2 \pmod{m^3}$ und $\Sigma x^{2(p-1)+\mu} \equiv 0 \pmod{m^3}$. So fortfahrend erhält man durch Induction zum Resultat, dafs allgemein

$$\Sigma x^{\nu(p-1)} \equiv (-1)^{\nu+1} m^\nu \pmod{m^{\nu+1}}, \quad \Sigma x^{\nu(p-1)+\mu} \equiv 0 \pmod{m^{\nu+1}}$$

für $\mu > 0$ ist. Aus der eben angewendeten Form

$$x^{p-1+\mu} = -A_1 x^{p-5+\mu} - A_5 x^{p-9+\mu} - \text{etc.}$$

der Gleichung $W = 0$, folgt auch, dafs jede Potenz einer Wurzel derselben, deren Exponent $\geqq p-1$ ist, sich als das $m$fache einer ganzen ganzzahligen Function dieser Wurzel darstellen läfst. Hieraus geht folgendes Princip hervor: „Wenn x Wurzel der Gleichung $W = 0$ ist und man darf in einer ganzen Function von x Vielfache von m weglassen, so ist es auch erlaubt, Potenzen von x wegzulassen, oder hinzuzufügen, deren Exponent $\geqq p-1$ ist, also z. B. nur diejenigen beizubehalten, deren Exponent $< p-1$ ist."

Es ist schon bemerkt worden, dafs, wenn w eine Wurzel der Gleichung $W = 0$ bezeichnet, jede andere Wurzel derselben, welche zunächst als gebrochene Function von w auftritt, auch als ganze Function von w dargestellt werden kann; wobei jedoch ein numerischer Nenner nicht zu vermeiden ist. ***Ein solcher numerischer Nenner kann nie durch m theilbar sein****). Es sei $\varphi(nt) = \frac{xf_1(x)}{f(x)}$, wenn $\varphi(t) = x$, so ist $\frac{wf_1(w)}{f(w)}$ irgend eine zweite Wurzel der Gleichung $W = 0$, wenn n eine ganze complexe Zahl, die weder $\equiv 0$ noch $\equiv 1 \pmod{m}$ ist. Man verwandelt die gebrochene Function auf die bekannte Weise in eine ganze, wenn man sie in der Form $\frac{wf_1(w)f(w')f(w'')\ldots.}{f(w)f(w')f(w'')\ldots.}$ schreibt; der Nenner ist dann eine symmetrische Function aller Wurzeln, also eine

*) Für eine spätere Gelegenheit behalte ich mir vor, zu beweisen, dafs bei der Reduction der ganzen Functionen mehrere Wurzeln der Gleichung $W = 0$ auf ganze Functionen einer Wurzel kein anderer Nenner auftreten kann, als eine Potenz von $1+i$.

ganze Zahl, die mit ϑ bezeichnet werden mag; das Product $f(w')f(w'')\ldots.$ wird einer ganzen ganzzahligen Function von w gleich und der Zähler erhält die Form $a_1w+a_5w^5+\ldots.$, also der ganze Ausdruck die Form $\frac{1}{\vartheta}(a_1w+a_5w^5+\ldots.)$; wo a_1, a_5 etc. ganze Zahlen sind; man kann immer annehmen, dafs die ganze Function von w in der Parenthese mit Hülfe der Gleichung $W=0$ auf einen Grad $<p-1$ gebracht ist. Das constante Glied in $f(x)$ ist $=1$, also ist $\vartheta=f(w)f(w')f(w'')\ldots.$ nach einer obigen Bemerkung $\equiv 1 \pmod{m}$ und daher gewifs nicht durch m theilbar. Man kann also $\frac{wf_1(w)}{f(w)}=w'=wF(w)$ setzen, wo $F(w)$ eine ganze Function von w vom Grade $p-5$ ist, deren Coëfficienten zwar gebrochene Zahlen sein können, welche aber sicher *nicht* m als Divisor in ihren Nennern enthalten. — Obgleich die Coëfficienten von $F(w)$ sich nicht *a priori* angeben lassen dürften, so können doch ihre Reste in Hinsicht auf $\mathrm{mod.}\, m$ auf eine elementare Weise bestimmt werden. Aus der Gleichung $\frac{f_1(w)}{f(w)}=F(w)$ oder $f_1(w)=f(w)F(w)$ folgt, dafs für einen unbestimmten Werth von x, $f_1(x)=f(x)F(x)+W.H$ ist; wo H eine ganze Function von x mit rationalen Coëfficienten bedeutet, deren Nenner ebenfalls nicht den Divisor m enthalten. Man entwickle den Quotienten $\frac{f_1(x)}{f(x)}$ in eine unendliche Reihe nach Potenzen von x und bringe diese Reihe auf die Form $R(x)+x^{p-1}S(x)$; $R(x)$ bedeutet den Anfang der Reihe bis zu der Potenz x^{p-5} incl., also eine ganze (geschlossene) Function von x vom Grade $p-5$, und $S(x)$ eine unendliche Reihe; man erhält dann

$$f_1(x)=f(x)R(x)+x^{p-1}S(x)f(x).$$

Das Product $S(x)f(x)$ mufs sich auf einen geschlossenen Ausdruck reduciren, da $f_1(x)-f(x)R(x)$ ein solcher ist. Es läfst sich auch das ganze Problem über die Entwicklung des Anfangs $R(x)$ der unendlichen Reihe so auffassen, als handelte es sich darum, eine ganze Function $R(x)$ zu bestimmen, von der Art, dafs die Differenz $f_1(x)-f(x)R(x)$ durch x^{p-1} algebraisch theilbar wird. Es sei also $f_1(x)=f(x)R(x)+x^{p-1}T(x)$. Setzt man diesen Werth von $f_1(x)$ in die obige Gleichung, so kommt

$$f(x)R(x)+x^{p-1}T(x)=f(x)F(x)+W.H.$$

Setzt man hier für x eine Wurzel w der Gleichung $W=0$, so ergiebt sich $f(w)(F(w)-R(w))=w^{p-1}T(w)$. $R(x)$ ist nichts anderes als der Anfang

der Entwicklung von $\frac{\varphi(nt)}{\varphi(t)}$ nach Potenzen von $\varphi(t)=x$, und da diese Entwicklung nur bis zu x^{p-5} fortgesetzt werden soll, so kann nach (§. 3.) in den Nennern der Coëfficienten von $R(x)$ kein Primtheiler vorkommen, dessen Norm $>p-4$, also namentlich nicht der Divisor m, dessen Norm p ist; dieser Divisor kann, der Bildung von $T(x)$ gemäfs, eben so wenig in den Nennern der Coëfficienten von $T(x)$ enthalten sein. Multiplicirt man nun die zuletzt gefundene Gleichung auf beiden Seiten mit $f(w')f(w'')\ldots.$, setzt wieder das Product $f(w)f(w')f(w'')\ldots.$ der ganzen, nicht durch m theilbaren Zahl ϑ gleich, verwandelt $f(w')f(w'')\ldots.$ in eine ganze Function von w und dividirt endlich durch ϑ, so erhält man $F(w)-R(w)$, als das Product aus w^{p-1} in eine ganze Function von w dargestellt, deren Coëfficienten rational sind und den Divisor m ***nicht*** in ihren Nennern enthalten. Da nun w^{p-1} dem $m$fachen einer ganzen Function von w gleich ist, nemlich $=-A_1w^{p-5}-\text{etc.}-m$, so wird $F(w)-R(w)$ ebenfalls dem $m$fachen einer solchen Function gleich. In Rücksicht auf die Irreductibilität der Gleichung $W=0$, und daraus, dafs $F(w)-R(w)$ von niedrigerem Grade als W ist, ergiebt sich, dafs in Hinsicht auf die Coëfficienten $F(x)\equiv R(x)\pmod m$ sein mufs. Bisher ist angenommen worden, dafs $F(x)$ zuvor mit Hülfe der Gleichung $W=0$ auf den niedrigsten Grad reducirt worden sei: aber selbst ohne diese Reduction würde noch immer derjenige Theil von $F(x)$, welcher niedrigere Potenzen als x^{p-1} enthält, $\equiv R(x)\pmod m$ sein, da ja bei jener Reduction w^{p-1} und höhere Potenzen von w, wie schon oben bemerkt, nur auf Glieder führen, die den Factor m enthalten. „Wenn man also auf irgend eine Art $\frac{\varphi(nt)}{\varphi(t)}$, für „den Fall, dafs $\varphi(t)=x$ eine Wurzel der Gleichung $W=0$ ist, als ganze „Function von $\varphi(t)$ ausdrückt, so sind die Coëfficienten derjenigen Potenzen „von x in dieser ganzen Function, welche vor x^{p-1} vorhergehen, $\equiv$ den „Coëfficienten der entsprechenden Potenzen in der unendlichen Reihen-Entwicklung von $\frac{\varphi(nt)}{\varphi(t)}$ nach Potenzen von x; oder auch, es ist $\varphi(nt)=$ dem „Anfange der Entwicklung von $\varphi(nt)$, wenn man die Reihe vor x^p abschneidet, „$+$ dem $m$fachen einer ganzen Function von x, welche den Factor x enthält." Die gebrochenen Zahlen hindern nicht die Anwendung der gewöhnlichen Sätze von Congruenzen, sobald man sich nur überzeugt, dafs keiner der vorkommenden Nenner den Modul als Divisor enthält. Statt des Anfangs der Entwicklung von $\varphi(nt)$ kann man auch irgend eine andere ganze Function

von x setzen, welche mit demselben in den vor x^p vorhergehenden Potenzen übereinstimmt: denn x^p und höhere Potenzen von x lassen sich sofort in das $m$fache einer ganzen durch x theilbaren Function verwandeln; nur müssen dabei stets Glieder vermieden werden, welche m im Nenner haben. Man kann also z. B. $\varphi(nt)$ nach Potenzen von t entwickeln, vor t^p abschneiden und für t überall den Anfang seiner Entwicklung bis x^p excl. setzen, statt dafs man eigentlich in jeder einzelnen Potenz von t bei der Entwicklung nach x vor x^p abschneiden müfste. Setzt man also, wie in (§. 3.),

$$t = x+\beta_5 x^5+\beta_9 x^9+\text{in inf.}, \quad x = t+\gamma_5 t^5+\gamma_9 t^9+\text{in inf.}$$

und ferner die ganze Function $x+\beta_5 x^5+\ldots.+\beta_{p-4}x^{p-4}=\xi$, so ist $\varphi(nt)$ $= n\xi+\gamma_5 n^5\xi^5+\gamma_9 n^9\xi^9+\ldots.+\gamma_{p-4}n^{p-4}\xi^{p-4}+$ dem $m$fachen einer durch x theilbaren ganzen Function von x, wenn für x eine Wurzel der Gleichung $W=0$ gesetzt wird. Bezeichnet man durch E irgend eine ganze Function von x, deren Coëfficienten rational sind und m nicht im Nenner enthalten, und setzt

$$t+\gamma_5 t^5+\ldots.+\gamma_{p-4}t^{p-4} = \chi(t),$$

so wird

$$\varphi(nt) = \chi(n\xi)+m.x.E.$$

Es seien jetzt r_1, r_2, r_3, ... beliebige, nicht durch m theilbare ganze complexe Zahlen, α_1, α_2, α_3, ... beliebige nicht negative ganze Exponenten, deren Summe $\alpha_1+\alpha_2+\alpha_3+\ldots.=\sigma$, und es sei der Ausdruck

$$\varphi(r_1 t)^{\alpha_1}\varphi(r_2 t)^{\alpha_2}\varphi(r_3 t)^{\alpha_3}\ldots. = Z;$$

so folgt leicht aus dem eben bewiesenen Resultate, dafs

$$Z = \chi(r_1\xi)^{\alpha_1}\chi(r_2\xi)^{\alpha_2}\chi(r_3\xi)^{\alpha_3}\ldots.+m.x^{\sigma}.E \text{ ist},$$

wenn für x irgend eine Wurzel der Gleichung $W=0$ gesetzt wird, oder auch dafs $Z=$ dem Anfange der Entwicklung von Z nach Potenzen von x ist, wenn man vor der Potenz $x^{p-1+\sigma}$ abschneidet, $+mx^{\sigma}.E$. Man hat auch $Z=Z'+mx^{\sigma}.E$, wenn man Z' so bestimmt, dafs Z nach Potenzen von t bis $t^{p-1+\sigma}$ excl. entwickelt wird, welcher Theil der Entwicklung die Potenzen t^{σ}, $t^{\sigma+4}$, etc. bis $t^{p-5+\sigma}$ enthält, und dann statt der Potenzen von t die ihnen gleichen Reihen nach x setzt, die man entweder sämmtlich, oder in denen man auch blofs die eine Reihe für t selbst vor $x^{p-1+\sigma}$ abbrechen kann.

Setzt man resp. kr_1, kr_2, etc. statt r_1, r_2, etc. und bezeichnet $\varphi(kr_1 t)^{\alpha_1}\varphi(kr_2 t)^{\alpha_2}\ldots.$ durch Z_k, so erhält man allgemein $Z_k=Z_k'+mx^{\sigma}.E_k$; wo die Coëfficienten von E_k, gleichviel auf welche Weise, von k abhangen,

und wo Z'_k gefunden wird, wenn man in der Entwicklung von Z nach t überall kt statt t schreibt und dann wie oben verfährt. Wir wollen jetzt k seine $p-1$ incongruenten Werthe (mod. m) durchlaufen lassen, und indem wir durch ΣZ_k die sich auf diese $p-1$ Werthe von k erstreckende Summe bezeichnen, die aus einer solchen Summation hervorgehende Zahl in Bezug auf eine möglichst hohe Potenz von m als Modul zu bestimmen suchen. Zunächst hat man $\Sigma Z_k = \Sigma Z'_k + m x^\sigma \Sigma E_k$; ΣE_k ist wieder von der Form E, da k nur in den Coëfficienten vorkommt, also kann man auch blofs schreiben:

$$\Sigma Z_k = \Sigma Z'_k + m x^\sigma . E.$$

Der Anfang der Entwicklung von Z_k ist von der Form

$$\delta_\sigma t^\sigma . k^\sigma + \delta_{\sigma+4} t^{\sigma+4} . k^{\sigma+4} + \ldots . + \delta_{\sigma+p-5} t^{\sigma+p-5} . k^{\sigma+p-5},$$

wo die Coëfficienten nicht von k abhangen. Es ist daher

$$\Sigma Z'_k = \delta_\sigma t^\sigma . \Sigma k^\sigma + \delta_{\sigma+4} t^{\sigma+4} \Sigma k^{\sigma+4} + \ldots . + \delta_{\sigma+p-5} . t^{\sigma+p-5} . \Sigma k^{\sigma+p-5},$$

wenn man die Potenzen von t durch den Anfang ihrer Entwicklungen nach x ersetzt, also durch ganze Functionen von x, die übrigens sämmtlich durch x^σ theilbar sind. Nun ist bekanntlich immer $\Sigma k^\mu \equiv 0$ (mod. m), aufser wenn der Exponent μ durch $p-1$ theilbar ist; in diesem letzteren Falle ist $\Sigma k^\mu \equiv 1+1+\ldots .+1 \equiv p-1$ (mod. m). Wendet man Dies auf die in obiger Reihe vorkommenden Summen dieser Art an, so erhält man ein Resultat von der Form

$$\Sigma Z'_k = -\delta_{\nu(p-1)} t^{\nu(p-1)} + m x^\sigma . E,$$

wenn $\nu(p-1)$ das einzige Vielfache von $p-1$ bezeichnet, welches sich unter den Exponenten σ, $\sigma+4$, $\sigma+8$, ... bis $\sigma+p-5$ befinden kann; ist $\sigma \equiv 0$ (mod. 4), so befindet sich immer ein Vielfaches von $p-1$ unter diesen Zahlen; im entgegengesetzten Falle verschwindet ΣZ_k, denn diese Summe mufs ungeändert bleiben, wenn man ik statt k setzt, indem ik, ebensowohl wie k, ein reducirtes Restensystem (mod. m) durchläuft. Nun ist, wie aus $\varphi(it) = i\varphi(t)$ folgt, $Z_{ik} = i^\sigma Z_k$, also $i^\sigma \Sigma Z_k = \Sigma Z_k$ und daher $\Sigma Z_k = 0$, aufser wenn $i^\sigma = 1$, nämlich $\sigma \equiv 0$ (mod. 4). Nehmen wir also σ als ein Vielfaches von 4 an und substituiren $\Sigma Z'_k = -\delta_{\nu(p-1)} t^{\nu(p-1)} + m x^\sigma E$ in $\Sigma Z_k = \Sigma Z'_k + m x^\sigma E$, so kommt $\Sigma Z_k = -\delta_{\nu(p-1)} t^{\nu(p-1)} + m x^\sigma E$, indem die beiden ganzen Functionen E in eine einzige zusammengezogen werden. Hier ist noch die Potenz $t^{\nu(p-1)}$ in Potenzen von x umzusetzen, deren niedrigste $x^{\nu(p-1)}$ und deren höchste $x^{\sigma+p-5}$ ist. Um nun ΣZ_k in Bezug auf eine möglichst hohe Potenz von m als Modul zu bestimmen, müssen die Gröfsen

zur rechten Seite $-\delta_{\nu(p-1)}t^{\nu(p-1)}$ und $mx^{\sigma}E$ untersucht werden, von denen die erste nur eine symbolische Bedeutung hat. Aus der Gleichung $x^{p-1+\mu} = -A_1x^{p-5+\mu} - \text{etc.} - mx^{\mu}$ folgt, wie schon oben bemerkt, dafs $x^{p-1+\mu}$ dem $m$fachen einer ganzen Function von x gleich ist. Man kann hinzufügen, dafs diese ganze Function mit x^{μ} aufgeht; es ist also $x^{p-1+\mu} = mx^{\mu}E$; für $\mu = 0$ ist $x^{p-1} = mxE - m$. Hieraus und aus der obigen Gleichung, wenn man in derselben $\mu \geqq p-1$ setzt, folgt wieder, dafs $x^{2(p-1)} = m^2xE + m^2$ und $x^{2(p-1)+\mu} = m^2x^{\mu}E$. Benutzt man dies und setzt in obiger Gleichung $x^{p-1+\mu} = -A_1x^{p-5+\mu}$ etc., $\mu \geqq 2(p-1)$, so kommt $x^{3(p-1)} = m^3xE - m^3$, $x^{3(p-1)+\mu} = m^3x^{\mu}E$. So fortfahrend erhält man allgemein $x^{\lambda(p-1)} = m^{\lambda}xE + (-1)^{\lambda}m^{\lambda}$ und $x^{\lambda(p-1)+\mu} = m^{\lambda}x^{\mu}E$. Jede Potenz von x also, deren Exponent $> \lambda(p-1)$ ist, ist $=$ dem Product aus m^{λ} in eine ganze Function von x, welche durch eine gewisse Potenz von x, mindestens durch x selbst theilbar ist; wenn der Exponent $= \lambda(p-1)$ ist, so mufs zu einem solchen Producte noch $(-m)^{\lambda}$ hinzugefügt werden. Da nun die ganze Zahl ν oben so bestimmt worden ist, dafs gewifs $\sigma > (\nu-1)(p-1)$ ist, so sind x^{σ} und alle höheren Potenzen von x als x^{σ} von der Form $m^{(\nu-1)}xE$; von derselben Form ist also auch $x^{\sigma}E$, und daher $mx^{\sigma}E$ von der Form $m^{\nu}xE$. Was die Bestandtheile von $t^{\nu(p-1)}$ betrifft, so ist das erste Glied $x^{\nu(p-1)} = m^{\nu}xE + (-m)^{\nu}$; die folgenden, welche höhere Potenzen von x enthalten, sind von den Formen resp. $m^{\nu}xE$, $m^{\nu}x^2E$, $m^{\nu}x^3E$, u. s. w., also, um zusammenzufassen, sämmtlich von der Form $m^{\nu}xE$. Im Ganzen hat man also für $t^{\nu(p-1)}$ einen Ausdruck von der Form $m^{\nu}xE + (-m)^{\nu}$ zu setzen, und da auch $mx^{\sigma}E = m^{\nu}xE$ gefunden worden ist, so erhält man

$$\Sigma Z_k = -\delta_{\nu(p-1)}t^{\nu(p-1)} + mx^{\sigma}E = m^{\nu}xE + (-1)^{\nu+1}\delta_{\nu(p-1)}.m^{\nu}.$$

Es läfst sich annehmen, dafs die ganze Function E in dem letzten Ausdrucke mit Hülfe der Gleichung $W = 0$ auf den $p-2$ten Grad erniedrigt ist; dann ist xE vom $p-1$ten Grade; das höchste Glied in xE, welches die Potenz x^{p-1} enthält, läfst sich wieder auf die Form mE' bringen, und die Gleichung wird so endlich zu

$$\Sigma Z_k = m^{\nu}xE + m^{\nu+1}E' + (-1)^{\nu+1}\delta_{\nu(p-1)}m^{\nu};$$

wo E vom $p-3$ten, also xE vom $p-2$ten und E' ebenfalls vom $p-2$ten Grade ist. ΣZ_k ist, wie leicht zu beweisen, eine ganze, mindestens eine rationale Zahl. Zur rechten Seite der Gleichung befindet sich eine ganze Function von niedrigerem Grade als W, und da die Gleichung für alle Wurzeln x der Gleichung $W = 0$ Statt findet, so mufs sie identisch erfüllt werden; es

mufs daher ΣZ_k dem constanten, von x freien Gliede rechts gleich sein. In dem Theile $m^\nu x E$ findet sich kein solches constantes Glied, also mufs $\Sigma Z_k =$ dem constanten Gliede in $m^{\nu+1}E' + (-1)^{\nu+1}\delta_{\nu(p-1)}m^\nu$ sein, mithin ist

$$\Sigma Z_k \equiv (-1)^{\nu+1}\delta_{\nu(p-1)}m^\nu \pmod{m^{\nu+1}}.$$

Die eben gefundenen merkwürdigen Resultate lassen sich auf eine etwas allgemeinere Weise folgendermafsen aussprechen:

„Wenn $F(k)$ eine *homogene* ganze ganzzahlige Function der Wurzeln „$\varphi\left(\frac{r_1 kC}{m}\right)$, $\varphi\left(\frac{r_2 kC}{m}\right)$, ... vom Grade σ bedeutet und man bezeichnet durch „$\nu(p-1)$ das kleinste Vielfache von $p-1$, welches der Bedingung $\sigma \leqq \nu(p-1)$ „genügt, so ist die Summe $\Sigma F(k)$, in der das Zeichen Σ sich auf die $p-1$ „incongruenten, nicht durch m theilbaren Werthe von k bezieht, einer durch m^ν „theilbaren ganzen Zahl gleich. Setzt man ferner t an die Stelle von $\frac{kC}{m}$ in $F(k)$ „und betrachtet t als eine unbestimmte Variable, nach deren Potenzen man „$F(k)$ in eine unendliche Reihe entwickelt, so ist der Quotient $\frac{(-1)^{\nu+1}}{m^\nu}\Sigma F(k)$ „$\equiv$ dem Coëfficienten von $t^{\nu(p-1)}$ in dieser Reihe, welche durch elementare „Methoden bestimmt werden kann. Endlich ist $F(k)$ selbst einer ganzen Func„tion von $x = \varphi(t) = \varphi\left(\frac{kC}{m}\right)$ gleich, welche, bis auf Vielfache von m, mit „demjenigen Theile jener Reihe übereinstimmt, welcher die Potenzen von x, „von x^σ an bis $x^{\sigma+p-5}$ incl. enthält."

Aus diesem Satze ergiebt sich leicht folgender.

„Wenn unter denselben Voraussetzungen $F(k)$ selbst einen rationalen „(ganzen) Werth hat, so ist dieser Werth durch m^ν theilbar und der Quo„tient $\frac{1}{m^\nu}F(k) \equiv (-1)^\nu \delta \pmod{m}$; wo δ den Coëfficienten von $t^{\nu(p-1)}$ in „der obigen Reihe bezeichnet."

Denn wenn $F(k)$ einen rationalen Werth hat, so mufs dieser (nach §. 2. am Schlusse) für alle $p-1$ Werthe von k derselbe bleiben; es ist also dann $\Sigma F(k) = (p-1)F(k)$ und $\frac{1}{m^\nu}\Sigma F(k) = (p-1).\ \frac{F(k)}{m^\nu}$, also da $p \equiv 0 \pmod{m}$, $\frac{1}{m^\nu}F(k) \equiv -\frac{1}{m^\nu}\Sigma F(k) \equiv (-1)^\nu \delta$.

§. 6.

Der grofse Nutzen dieser Sätze kann erst durch mannigfaltige Anwendungen auf specielle Probleme klar werden, welche ich in der Folge zu geben beabsichtige. Bei diesen Anwendungen wird man die bisherigen Principien gewöhnlich mit dem folgenden Hülfssatze in Verbindung zu bringen haben, dessen Nothwendigkeit sich schon im Vorhergehenden fühlbar gemacht hat: dafs nämlich: „wenn eine ganze ganzzahlige Function der Wurzeln der Gleichung $W=0$ „einer *rationalen* Zahl gleich ist, diese letztere nothwendig *ganz* sein mufs." Dieser leicht zu beweisende Hülfssatz, welcher für jede Gleichung richtig ist, deren höchster Term die Einheit zum Coëfficienten und sonst ganze Coëfficienten hat, scheint von *Abel* merkwürdiger Weise übersehen worden zu sein, da er mehrere solche Verbindungen der Wurzeln aufstellt, welche rationale Werthe haben, ohne zu bemerken, dafs sie deshalb allein schon nothwendig auch *ganze* Werthe haben müssen; Niemand wird aber bezweifeln, dafs man der vollständigen Erkenntnifs einer Gröfse bei weitem näher gerückt ist, wenn man weifs, sie sei eine *ganze* Zahl, als wenn man blofs weifs, sie sei eine *rationale* Zahl; wäre es auch, anderer Vortheile nicht zu gedenken, die sich später zeigen werden, blofs aus dem einfachen Grunde, weil eine ganze Zahl durch Einschliefsung zwischen Grenzen ermittelt werden kann, was bei einer blofs rationalen, deren es unendlich viele zwischen gegebenen Grenzen giebt, nicht der Fall ist. — Um den Hülfssatz zu beweisen, sei $x^\mu + a_1 x^{\mu-1} + a_2 x^{\mu-2} + \ldots + a_\mu = X = 0$ irgend eine Gleichung, in welcher $a_1, a_2, \ldots$ ganze (reelle oder complexe) Zahlen sind; $\alpha, \beta, \gamma, \ldots \omega$ seien ihre μ Wurzeln und $f(\alpha, \beta, \gamma, \ldots \omega) = z$ sei eine beliebig gegebene ganze Function dieser Wurzeln mit ganzen Coëfficienten, also eine Summe von Termen von der Form $h\alpha^n\beta^{n'}\gamma^{n''}\ldots$, wo h eine ganze Zahl ist und die Exponenten positive ganze Zahlen sind. Man permutire in der Function $f(\alpha, \beta, \gamma, \ldots \omega)$ die Wurzeln $\alpha, \beta, \gamma, \ldots \omega$ auf alle mögliche Arten und bezeichne die durch solche Permutation hervorgehenden Ausdrücke durch z', z'', z''', etc.; es wird hierbei keine Rücksicht darauf genommen, ob einige dieser Ausdrücke, incl. z selbst, einander gleich sind, sei es wegen ihrer Form, oder wegen ihres numerischen Werthes; man bilde rein typisch alle Permutationen, und es wird dann die Anzahl der Gröfsen z, z', z'', z''', etc. $1.2.3\ldots\mu$ betragen; welche letztere Zahl für einen Augenblick durch Π bezeichnet sei. Bildet man nun das Product $(x-z)(x-z')(x-z'')\ldots = x^\Pi + b_1 x^{\Pi-1} + b_2 x^{\Pi-2} + \text{etc.} = Y$, so ist z eine Wurzel der Gleichung $Y=0$ vom Grade Π. Ich behaupte,

dafs die Coëfficienten b_1, b_2, etc. ganze Zahlen sein werden; denn sie sind offenbar zunächst ganze ganzzahlige und symmetrische Functionen von z, z', z'', etc., also auch eben solche Functionen der Wurzeln α, β, γ, ... ω: folglich sind sie endlich ganze ganzzahlige Functionen der Coëfficienten a_1, a_2, ..., also ganze Zahlen. Man kann b_1, b_2, ... übrigens *) in die Potenzsummen der Gröfsen z, z', z'', ... ausdrücken, und diese Potenzsummen setzen sich aus Summen von der Form $hS\alpha^\nu\beta^{\nu'}\gamma^{\nu''}$ .... zusammen, wo das Zeichen S sich auf alle Permutationen der Wurzeln α, β, γ, ... bezieht. Nun ist bekanntlich jede rationale Wurzel einer Gleichung von der Form $Y=0$ einer ganzen Zahl gleich: denn wäre $z=\frac{c}{d}$, wo c und d ganze Zahlen sind, die keinen gemeinschaftlichen Theiler haben, so erhielte man aus $z^{II}+b_1z^{II-1}+b_2z^{II-2}+\ldots.=0$ die unmögliche Gleichung

$$\frac{c^{II}}{d} = -b_1c^{II-1}-b_2c^{II-2}.d-b_3c^{II-3}.d^2-\text{etc.},$$

in welcher links ein Bruch und rechts lauter ganze Zahlen stehen. Es kann also wirklich z keinen rationalen Werth haben, ohne einer ganzen Zahl gleich zu sein. Es ist möglich, dafs der eben bewiesene Satz schon von Anderen aufgestellt worden ist, ich lege auch keinen weiteren Werth auf denselben, als insofern er mir von mannigfaltigem Nutzen bei meinen Untersuchungen gewesen ist. Um die Art der Anwendung desselben zu zeigen, will ich mit Beibehaltung der obigen Bezeichnung noch einmal auf die Betrachtung der Summen von der Form $\Sigma F(k)$ zurückgehen. Aus der ursprünglichen Form von $\Sigma F(k)$ ersieht man *nicht*, dafs es eine symmetrische Function aller Wurzeln der Gleichung $W=0$ ist, man ersieht nur, dafs es eine solche Function ist, welche man eine *cyclische* nennen könnte, nemlich welche bei einer cyclischen Permutation der Wurzeln ungeändert bleibt. Hieraus folgt noch nicht, dafs sie die Eigenschaften symmetrischer Functionen der Wurzeln theilt, und es würde dieser Schlufs bei einer Gleichung im Allgemeinen gänzlich ungerechtfertigt sein; dafs dessenungeachtet $\Sigma F(k)$ in eine symmetrische Function der Wurzeln und somit in eine rationale Zahl verwandelt werden kann, liegt daran, dafs jede Wurzel als rationale Function *einer* Wurzel dargestellt werden kann, also an einer speciellen Eigenthümlichkeit der Gleichung $W=0$, und es ist dies gerade ein Punct bei diesen Untersuchungen, welcher von *Abel* mit grofser Klarheit hervorgehoben worden ist. Da man nämlich $\varphi\left(\frac{r_1kC}{m}\right)$,

*) Zur numerischen Berechnung und nicht zum Beweise des Satzes.

$\varphi\left(\frac{r_2 kC}{m}\right)$, u. s. w. durch rationale und sogar ganze Functionen von $\varphi\left(\frac{kC}{m}\right)$ mit rationalen Coëfficienten ausdrücken kann, so wird auch $F(k) =$ einer solchen Function von $\varphi\left(\frac{kC}{m}\right)$ allein, nämlich

$$F(k) = \Psi\left(\varphi\left(\frac{kC}{m}\right)\right) = a_0 + a_1\varphi\left(\frac{kC}{m}\right) + a_2\varphi\left(\frac{kC}{m}\right)^2 + \text{etc.},$$

wo a_0, a_1, etc., rationale, ***nicht*** nothwendig ganze Zahlen sind, und es ist dann $\Sigma F(k) = a_0(p-1) + a_1\Sigma\varphi\left(\frac{kC}{m}\right) + a_2\Sigma\varphi\left(\frac{kC}{m}\right)^2 + \text{etc.} =$ einer symmetrischen Function aller Wurzeln mit rationalen Coëfficienten = einer ***rationalen*** Zahl. Wenn diese Transformation von $\Sigma F(k)$ nothwendig war, um zu zeigen, dafs es einen rationalen Werth hat, so mufs man doch bei der Anwendung des obigen Hülfssatzes gerade auf die ***ursprüngliche*** Form von $\Sigma F(k)$ zurückgehen. Da es in dieser Form eine ganze Function mit ***ganzen*** Coëfficienten der Wurzeln (nicht ***einer*** Wurzel) ist, so mufs es einer ganzen Zahl gleich sein, wenn es überhaupt einen rationalen Werth hat, und dies ist eben gezeigt worden. Die auf dem vorhin eingeschlagenen Wege der Transformation von $\Sigma F(k)$ in eine symmetrische Function gefundene rationale Zahl mufs sich also, gleichviel auf welche Weise, auf eine ganze reduciren. Im Allgemeinen: „Wenn eine ganze ganzzahlige Function der Wurzeln der Gleichung $W = 0$ „sich auf irgend eine Weise in eine symmetrische Function der Wurzeln, „wenn auch nur mit rationalen Coëfficienten, transformiren läfst, so ist sie einer „***ganzen*** Zahl gleich", denn sie ist dann als symmetrische Function einer rationalen, also deshalb nach dem Hülfsatze einer ganzen Zahl gleich. Diese Bemerkung gilt für jede Gleichung von der Form $x^\mu + a_1 x^{\mu-1} + a_2 x^{\mu-2} + \ldots$, in der a_1, a_2, ... ganze Zahlen sind. Nicht so ist es mit der folgenden Bemerkung, welche erfordert, dafs jede Wurzel sich als rationale ganzzahlige Function einer Wurzel ausdrücken läfst, nämlich: „Wenn $F(k)$, eine ganze ganzzahlige „Function der Wurzeln $\varphi\left(\frac{r_1 kC}{m}\right)$, $\varphi\left(\frac{r_2 kC}{m}\right)$, etc., für alle $p-1$ Werthe von k „denselben Werth behält, so ist $F(k)$, nämlich dieser gemeinschaftliche Werth, „selbst eine ganze Zahl"; denn es ist in diesem Falle $(p-1)F(k) = \Sigma F(k)$, welche letztere Summe sich wiederum, wie oben, in eine symmetrische Function der $p-1$ Wurzeln $\varphi\left(\frac{kC}{m}\right)$, also in eine rationale Zahl transformirt; es ist also $(p-1)F(k)$ und mithin auch $F(k)$ in diesem Falle einer rationalen Zahl gleich, und letztere mufs nach dem Hülfssatze ganz sein, da $F(k)$ mit ganzen

Coëfficienten vorausgesetzt wurde. Kürzer kann das eben Bewiesene so ausgesprochen werden:

„Jede *cyclische* ganze ganzzahlige Function der Wurzeln der Gleichung $W=0$ ist einer *ganzen* Zahl gleich." Der letztere Satz ist in dieser Form um so wichtiger, da die algebraische Auflösung der Gleichung $W=0$, wie schon *Abel* gezeigt hat, wesentlich von den Eigenschaften und der Auffindung der *cyclischen* Functionen der Wurzeln abhangt; d. h. derjenigen, welche bei einer *cyclischen* Permutation der Wurzeln ungeändert bleiben. Wenn die Coëfficienten der cyclischen Function, statt ganze Zahlen zu sein, ganze ganzzahlige Functionen einer neuen Gröfse z sind, so kann man behaupten, dafs die cyclische Function, welche in diesem Falle, um z sichtbar zu machen, durch $F(k;z)$ bezeichnet werden mag, sich auf eine ganze ganzzahlige Function von z reducirt; nur mufs vorausgesetzt werden können, dafs $F(k;z)$ für *mehr* Werthe von z die Eigenschaft einer cyclischen Verbindung hat, als ihr Grad in Bezug auf z beträgt. Denn setzt man, was erlaubt ist,

$$F(k;z) = F_0(k)+F_1(k)z+F_2(k)z^2+\ldots+F_\mu(k)z^\mu,$$

wo die Coëfficienten ganze ganzzahlige Functionen der Wurzeln der Gleichung $W=0$ sind, so hat man für jeden zweiten Werth k' von k:

$$F_0(k')+F_1(k')z+\ldots+F_\mu(k')z^\mu = F_0(k)+F_1(k)z+\ldots+F_\mu(k)z^\mu,$$

und wenn diese Gleichung für *mehr* als μ Werthe von z besteht, so mufs einzeln $F_0(k')=F_0(k)$, $F_1(k')=F_1(k)$ u. s. w. sein; es sind also dann die Coëfficienten der einzelnen Potenzen von z selbst cyclische Functionen, folglich nach dem Obigen ganze Zahlen, und $F(k;z)$ nimmt die Form

$$a_0+a_1z+a_2z^2+\ldots+a_\mu z^\mu$$

an, wo a_0, a_1, etc. ganze (complexe) Zahlen sind. Die Voraussetzung, dafs $F(k;z)$ für *mehr* Werthe von z *cyclisch* sein soll, als der Grad in Bezug auf z beträgt, wird z. B. erfüllt, wenn z Wurzel einer Gleichung mit ganzen Coëfficienten ist und die Eigenschaft der cyclischen Unveränderlichkeit von $F(k;z)$ für alle Wurzeln dieser Gleichung Statt findet, mag übrigens $F(k;z)$ dann von so hohem Grade gegeben sein, als man will; denn man kann diesen Grad mit Hülfe der Gleichung, welcher z genügt, unter den Grad der Gleichung selbst reduciren, und zwar ohne einen Nenner einzuführen *), so dafs $F(k;z)$ nach dieser Reduction immer noch ganzzahlig bleibt, aber zu einem Grade

*) Der Coëfficient des höchsten Gliedes der Gleichung, welcher z genügt, wird $=1$ angenommen, und es soll das Nämliche auch in der Folge bei allen Gleichungen mit ganzen Coëfficienten stillschweigend vorausgesetzt werden.

herabsinkt, der durch die Anzahl der Wurzeln der Gleichung, welcher z genügt, mindestens um eine Einheit übertroffen wird. So ist z. B. wenn man durch λ irgend einen Theiler von $p-1$, durch z irgend eine Wurzel der Gleichung $z^\lambda = 1$ und durch g eine primitive Congruenzwurzel (mod. m) bezeichnet, die λte Potenz jedes Ausdrucks wie

$$F(k)+zF(gk)+z^2F(g^2k)+\ldots.+z^{p-2}F(g^{p-2}k) = L$$

eine cyclische Function und deshalb von der Form

$$L^\lambda = a_0+a_1z+a_2z^2+\ldots.+a_{\lambda-1}z^{\lambda-1};$$

wo a_0, a_1, etc. *ganze*, nicht blofs rationale Zahlen (von der Form $a+bi$) sind, so oft für $F(k)$ irgend eine ganze ganzzahlige Function der Wurzeln $\varphi\left(\frac{rkC}{m}\right)$ gesetzt wird. Eben so verhält es sich mit einer Menge ähnlicher Verbindungen, in denen Wurzeln der Einheit neben Wurzeln der Gleichung $W=0$ vorkommen und die zum Theil von *Abel* betrachtet worden sind, bei denen man auch aus dem einmal erwiesenen cyclischen Verhalten schliefsen kann, dafs sie sich *ganzzahlig* in diejenigen Elemente *allein* ausdrücken lassen, welche sie in ihrer ursprünglichen Form neben den Wurzeln der Gleichung $W=0$ enthalten.

Wenn die cyclische Function homogen in Bezug auf die Wurzeln und vom Grade σ ist, so ist ihr Werth, nach dem weiter oben (§. 5.) Bewiesenen, durch m^ν theilbar, wo ν die kleinste der Bedingung $\sigma \leqq \nu(p-1)$ entsprechende ganze Zahl ist; und der Quotient, den sie durch m^ν dividirt giebt, ist $\equiv (-1)^\nu \delta$ (mod. m), wenn wieder δ wie oben den Coëfficienten von $t^{\nu(p-1)}$ in der Reihe bezeichnet, welche aus der cyclischen Function entspringt, nachdem man in derselben die unbestimmte Variable t an die Stelle von $\frac{kC}{m}$ gesetzt hat. Dies gilt auch, wenn die cyclische Function noch z enthält, also von der Form $F(k;z) = F_0(k)+F_1(k).z+$ etc. ist, und hierbei einzeln $F_0(k)$, $F_1(k)$, etc. cyclisch sind; diese letzteren Coëfficienten sind dann selbst durch m^ν theilbar, und δ wird eine Function von z. Man kann bei der Bestimmung von δ beliebig Vielfache von m vernachlässigen und dadurch den Werth von δ auf eine möglichst einfache Form reduciren, da δ doch nur in einer *Congruenz* (mod. m) vorkommt. Betrachten wir, um diese Art der Reduction deutlich zu machen, noch einmal die Potenz L^λ. Dieselbe ist homogen und vom Grade $\lambda\tau$, wenn $F(k)$, in $L = F(k)+zF(gk)+z^2F(g^2k)+$ etc., homogen und vom Grade τ ist. Bezeichnet $\nu(p-1)$ das kleinste die Zahl $\lambda\tau$

übertreffende oder auch das ihr gleiche Vielfache von $p-1$, so sind in $L^\lambda = a_0 + a_1 z + a_2 z^2 + \ldots + a_{\lambda-1} z^{\lambda-1}$ die ganzen Zahlen a_0, a_1, etc. durch m^ν theilbar und also $L^\lambda = m^\nu (b_0 + b_1 z + \text{etc.})$, wo b_0, b_1, etc. ebenfalls ganze Zahlen sind. Den Rest der letzteren (mod. m) kann man nun bestimmen, wenn man den Coëfficienten von $t^{\nu(p-1)}$ in der Entwicklung von L^λ aufsucht. Um diese Entwicklung zu erhalten, hat man zunächst statt $F(k)$ dieselbe ganze ganzzahlige Function von $\varphi(r_1 t)$, $\varphi(r_2 t)$, etc. zu setzen, welche $F(k)$ von $\varphi\left(\frac{r_1 kC}{m}\right)$, $\varphi\left(\frac{r_2 kC}{m}\right)$, etc. bedeutet, und die so erhaltene Function der unbestimmten Variabeln t nach Potenzen von t zu entwickeln. Es sei die hieraus hervorgehende Reihe $c_0 + c_1 t + c_2 t^2 + \text{etc.}$, oder besser:

$$c_\tau t^\tau + c_{\tau+1} t^{\tau+1} + \text{in inf.} = R(t).$$

Es ist nämlich $F(k)$ von der Dimension τ in Bezug auf die Wurzeln angenommen worden, und da jede der Gröfsen $\varphi(r_1 t)$, $\varphi(r_2 t)$, etc. in ihrer Entwicklung schon mit der ersten Potenz von t und nicht mit einem constanten Gliede beginnt, so fängt eine ganze Function derselben von der Ordnung τ mit der Potenz t^τ an. Für $F(gk)$, $F(g^2 k)$, etc. hat man dann die Entwicklungen $R(gt)$, $R(g^2 t)$, etc. zu setzen; diese sämmtlichen Entwicklungen brauchen nur bis $t^{\tau+p-1}$ excl. fortgeführt zu werden. An die Stelle von L tritt auf diese Weise

$$\begin{aligned} &c^\tau (1 + z g^\tau + z^2 g^{2\tau} + \ldots + z^{p-2} g^{(p-2)\tau}) t^\tau \\ &+ c_{\tau+1} (1 + z g^{\tau+1} + z^2 g^{2(\tau+1)} + \ldots + z^{p-2} g^{(p-2)(\tau+1)}) t^{\tau+1} + \text{etc.} \\ &= c_\tau t^\tau \Sigma z^\mu g^{\mu\tau} + c_{\tau+1} t^{\tau+1} \Sigma z^\mu g^{\mu(\tau+1)} + \text{etc.} = L(t), \end{aligned}$$

und in der λten Potenz dieser Reihe $L(t)$ hat man den Coëfficienten von $t^{\nu(p-1)}$ aufzusuchen. Bezeichnet man denselben durch $\delta = \delta_0 + \delta_1 z + \text{etc.} + \delta_{\lambda-1} z^{\lambda-1}$, so ist $b_0 \equiv \delta_0$, $b_1 \equiv \delta_1$ etc. (mod. m). Bei der Aufsuchung von δ findet nun, da man Vielfache von m vernachlässigen darf, folgende Vereinfachung Statt. Man kann, wenn $p-1 = \lambda e$ gesetzt wird, aus der Reihe $L(t)$ alle diejenigen Potenzen von t weglassen, deren Exponent nicht mit e aufgeht, denn ihre Coëfficienten sind durch m theilbar. Man hat nämlich allgemein, wegen $z^\lambda = 1$, für jede ganze Zahl ϱ:

$$1 + z g^\varrho + z^2 g^{2\varrho} + \ldots + z^{p-2} g^{(p-2)\varrho} = \text{dem Producte}$$

$$(1 + z g^\varrho + z^2 g^{2\varrho} + \ldots + z^{\lambda-1} g^{(\lambda-1)\varrho})(1 + g^{\lambda\varrho} + g^{2\lambda\varrho} + \ldots + g^{(e-1)\lambda\varrho}),$$

und hier ist der zweite Factor $= \frac{1-g^{e\lambda\varrho}}{1-g^{\lambda\varrho}} = \frac{1-g^{\varrho(p-1)}}{1-g^{\varrho\lambda}}$ durch m theilbar,

aufser wenn $\varrho \equiv 0 \pmod{e}$, dann ist derselbe $\equiv e \pmod{m}$; unter den Werthen $\varrho = \tau,\ \tau+1,\ \tau+2$, etc. brauchen also, da übrigens keiner der Coëfficienten c_τ, $c_{\tau+1}$, bis $c_{\tau+p-2}$ den Divisor m im Nenner enthalten kann, nur die durch e theilbaren beibehalten zu werden, und an die Stelle von $L(t)$ kann man schreiben:

$$e.\{c_{\nu e}(1+zg^{\nu e}+z^2g^{2\nu e}+\ldots.+z^{\lambda-1}g^{(\lambda-1)\nu e})t^{\nu e}+\text{etc.}\}.$$

In der λten Potenz dieser Reihe ist der Coëfficient der niedrigsten Potenz von t, deren Exponent mit $p-1$ aufgeht, nämlich der Coëfficient von $t^{\lambda\nu e} = t^{\nu(p-1)}$, offenbar

$$e^\lambda c_{\nu e}^\lambda(1+zg^{\nu e}+z^2g^{2\nu e}+\ldots.+z^{\lambda-1}g^{(\lambda-1)\nu e})^\lambda.$$

Diesem sehr einfachen Ausdrucke, mit $(-1)^\nu$ multiplicirt, ist also die ganze complexe Zahl aus λten Wurzeln der Einheit

$$\frac{L^\lambda}{m^\nu} = b_0+b_1z+b_2z^2+\ldots.+b_{\lambda-1}z^{\lambda-1} \text{ congruent } (\text{mod. } m).$$

Setzt man hier an die Stelle von z eine Wurzel der Congruenz $z^\lambda \equiv 1 \pmod{m}$, also eine Potenz von g^e, so verwandelt sich der Factor

$$1+zg^{\nu e}+\ldots.+z^{\lambda-1}g^{(\lambda-1)\nu e},$$

welcher $= \frac{1-g^{\nu(p-1)}}{1-zg^{\nu e}}$ ist, in eine durch m theilbare ganze Zahl; mit Ausnahme des einzigen Falles, wenn gerade die specielle Wurzel $g^{-\nu e}$ statt z gesetzt wird. In diesem Falle wird der eben betrachtete Factor $\equiv \lambda \pmod{m}$. Die mehrgliedrig complexe Zahl $b_0+b_1z+\ldots.$ geht also für jede Wurzel der Congruenz $z^\lambda \equiv 1 \pmod{m}$ in eine durch m theilbare ganze Zahl über; nur für die eine Wurzel $g^{-\nu e}$ geht sie in eine ganze Zahl über, welche $\equiv (-1)^\nu e^\lambda c_{\nu e}^\lambda . \lambda^\lambda \equiv (-1)^\nu(p-1)^\lambda c_{\nu e}^\lambda \equiv (-1)^{\nu+\lambda}c_{\nu e}^\lambda \pmod{m}$ ist, d. h. $\equiv (-1)^{\nu+\lambda}$mal der λten Potenz des Coëfficienten von $t^{\nu e}$ in der für $F(k)$ zu setzenden unendlichen Reihe. Im Vorbeigehen bemerkt, heifst dies, im Sinne der von ***Kummer*** eingeführten idealen Primfactoren: die complexe Zahl $b_0+b_1z+\ldots.$ enthält alle idealen Primfactoren von m aus λten Wurzeln der Einheit, mit Ausnahme desjenigen, welcher zur Congruenzwurzel $g^{-\nu e}$ gehört; der letztere kann nur dann in b_0+b_1z+ etc. enthalten sein, wenn der Coëfficient $c_{\nu e}$ durch m theilbar ist. Analoge Betrachtungen lassen sich, statt auf die Potenz L^λ, auf ein Product mehrerer Factoren von der Form $F(k)+z^\alpha F(gk)+z^{2\alpha}F(g^2k)+$ etc. anwenden, welches eine ***cyclische*** Function darstellt, sobald die Summe aller Exponenten α in den verschiedenen Factoren ein Vielfaches von λ ergiebt, mag übrigens die Function F als dieselbe, oder verschieden in den verschie-

denen Factoren angenommen werden. Ohne für den Augenblick in weiteres Detail einzugehen, will ich unter den Resultaten, welche sich in Folge einer ausführlichen Entwicklung der obigen Principien ergeben und auf welche ich später zurückkommen werde, nur eine characteristische Eigenschaft der in den Auflösungsformeln für die Wurzeln der Gleichung $W = 0$ vorkommenden ***Irrationalitäten*** als besonders bemerkenswerth hervorheben. Ehe die neuesten zahlentheoretischen Arbeiten von ***Kummer*** erschienen und mir bekannt geworden waren, hatte ich diese Eigenschaft in einer ziemlich complicirten Form gefunden; sie läfst sich mit gröfster Einfachheit und Kürze aufstellen, wenn man den schon oben berührten Begriff der *idealen* Zahlen zu Hülfe nimmt, und zwar müssen die Elemente der idealen Zahlen nicht als reell, wie bei ***Kummer***, sondern selbst als complex und von der Form: $a + bi$ angenommen werden. Man findet dann, dafs mit Hülfe dieser Gattung idealer Zahlen den Formeln für die Theilung der ganzen Lemniscate durch den Divisor m immer eine solche Form gegeben werden kann, ***dafs die vorkommenden Wurzelzeichen sich nur auf ideale Primfactoren des Divisors m beziehen und dafs die Potenzen und Producte jener Primfactoren von m unter den Wurzelzeichen ein demjenigen ganz analoges Gesetz befolgen,*** welches ***Kummer*** für die Kreistheilung und in Rücksicht auf die gewöhnlichen idealen Primfactoren der reellen Primzahl p nachgewiesen hat. Die so beschriebenen Irrationalitäten sind in der Lemniscatentheilung noch mit gewissen rationalen Factoren aufserhalb des Wurzelzeichens multiplicirt, welche durch die complicirte Natur der lemniscatischen Functionen bedingt werden. Diese zu den wesentlichen Wurzelgröfsen hinzutretenden rationalen Factoren entziehen sich den von mir angewandten Principien; sie kommen übrigens auch schon in der Kreistheilung vor, wenn man statt der Wurzeln der Einheit andere trigonometrische Functionen, z. B. die Tangenten aliquoter Theile des Kreis-Umfanges betrachtet. Glücklicher Weise ist aber die Bestimmung der genannten Factoren für eine ganze Reihe von zahlentheoretischen Anwendungen nicht erforderlich, sondern nur die genaue Untersuchung der wesentlichen Wurzelgröfsen selbst; welche letztere, wie bemerkt, mittels der obigen Principien vollständig durchgeführt werden kann.

§. 7.

Nachdem in den vorhergehenden drei Paragraphen allgemeine Principien auseinandergesetzt worden sind, auf die ich mich in der Folge stützen

werde, soll hier die vollständige Durchführung eines speciellen Problems aus der Lemniscatentheilung versucht werden, welches wegen seiner Anwendung in der Theorie der 8ten Potenzreste ein besonderes Interesse hat. Neben den cyclischen Verbindungen der Wurzeln der Gleichung $W=0$ hat schon *Abel* diejenigen als besonders wichtig erkannt, welche, wie dies z. B. bei dem oben betrachteten Ausdrucke $F(k)+zF(gk)+z^2F(g^2k)+$ etc. der Fall ist, zu einer gewissen Potenz erhoben werden müssen, um eine cyclische Function zu ergeben. Ich beabsichtige hier ins Einzelne solche Functionen zu untersuchen, deren *achte* Potenz die eben genannte Eigenschaft hat und welche man als cyclische Verbindungen achter Ordnung bezeichnen kann, während dann die früher definirten gewöhnliche cyclische Functionen, oder cyclische Functionen erster Ordnung benannt werden müssen. Zuvor will ich noch einige Bemerkungen über die cyclischen Functionen 2ter und 4ter Ordnung vorausschicken, deren Untersuchung als Einleitung zu der viel schwierigeren Theorie der cyclischen Functionen 8ter Ordnung angesehen werden kann.

In einer früheren Abhandlung ist bereits ein sehr einfacher Ausdruck betrachtet worden, dessen *4te* Potenz einen rationalen Werth annimmt; ich will denselben hier in einer von der dortigen etwas verschiedenen Weise darstellen. Bezeichnet man der Kürze wegen die Wurzeln $\varphi\left(\frac{rC}{m}\right)$ durch $\psi(r)$ und, wie oben, durch g eine primitive Congruenzwurzel (mod. m), so sind

$$(1.)\qquad \psi(k),\quad \psi(gk),\quad \psi(g^2k),\quad \ldots.\ \psi(g^{p-1}k)$$

die sämmtlichen Wurzeln der Gleichung $W=0$. Ich wähle die Zahl g unter derjenigen Hälfte, welche der Bedingung $g^{\frac{1}{4}(p-1)}\equiv i$ (mod. m) und *nicht* der entgegengesetzten $g^{\frac{1}{4}(p-1)}\equiv i$ (mod. m) genügen. Bildet man den Ausdruck

$$\psi(k)\psi(gk)\psi(g^2k)\ \ldots.\ \psi(g^{p-2}k),$$

so ist derselbe, als Product aller Wurzeln, $=$ dem letzten Coëfficienten der Gleichung $W=0$, und zwar mit positivem Zeichen, weil der Grad $p-1$ dieser Gleichung eine gerade Zahl ist. Man hat folglich

$$(2.)\qquad \psi(k)\psi(gk)\psi(g^2k)\ldots.\psi(g^{p-2}k) = m.$$

Dieses Product, dessen Werth m ist, will ich in vier Partialproducte zerlegen, indem ich die ersten $\frac{1}{4}(p-1)$ Factoren und dann von den folgenden ebenfalls immer $\frac{1}{4}(p-1)$ vereinige. Diese vier Partialproducte lassen sich leicht auf einander reduciren. Bezeichnet man das erste derselben mit $P(k)$, setzt also

$$(3.)\qquad P(k) = \psi(k)\psi(gk)\ldots.\psi(g^{\frac{1}{4}(p-5)}k)$$

und bedenkt, dafs allgemein

$$\psi(g^{\frac{1}{4}(p-1)}r) = \psi(ir) = i\psi(r), \quad \psi(g^{\frac{1}{2}(p-1)}r) = \psi(-r) = -\psi(r);$$

und endlich $\psi(g^{\frac{3}{4}(p-1)}r) = \psi(-ir) = -i\psi(r)$ ist, so sieht man leicht, dafs die drei folgenden Producte durch resp. $i^{\frac{1}{4}(p-1)}.\boldsymbol{P}(k)$, $(-1)^{\frac{1}{4}(p-1)}\boldsymbol{P}(k)$, $(-i)^{\frac{1}{4}(p-1)}\boldsymbol{P}(k)$ ausgedrückt werden können und dafs demnach das ganze Product in (2.) durch $i^{\frac{1}{4}(p-1)}.(-1)^{\frac{1}{4}(p-1)}.(-i)^{\frac{1}{4}(p-1)}.\boldsymbol{P}(k)^4 = (-1)^{\frac{1}{4}(p-1)}.\boldsymbol{P}(k)^4$ ersetzt werden kann. Hieraus ergiebt sich

$$(4.) \qquad \boldsymbol{P}(k)^4 = (-1)^{\frac{1}{4}(p-1)}.m = \varepsilon m,$$

wo $\boldsymbol{P}(k)$ durch (3.) bestimmt ist. — Der Ausdruck $\boldsymbol{P}(k)$ ist eine cyclische Function 4ter Ordnung und $\boldsymbol{P}(k)^4$ eine gewöhnliche cyclische Function. Um im Allgemeinen von dem cyclischen Verhalten eines Ausdrucks sich zu überzeugen, genügt es offenbar, zu untersuchen, ob derselbe durch die Substitution von gk statt k unverändert bleibe. Man hat

$$\boldsymbol{P}(gk) = \psi(gk)\psi(g^2k) \ldots . \psi(g^{\frac{1}{4}(p-5)}k)\psi(g^{\frac{1}{4}(p-1)}k),$$

und da $\psi(g^{\frac{1}{4}(p-1)}k) = \psi(ik) = i\psi(k)$ ist, so genügt $\boldsymbol{P}(k)$ der Relation $\boldsymbol{P}(gk) = i\boldsymbol{P}(k)$, und es ist folglich $\boldsymbol{P}(gk)^4 = \boldsymbol{P}(k)^4$. Ich will auf eine bestimmtere Weise, als oben geschehen, durch die Benennung cyclische Functionen vierter Ordnung alle diejenigen ganzen ganzzahligen Functionen der Gröfsen (1.) definiren, welche der Relation $\boldsymbol{F}(gk) = i\boldsymbol{F}(k)$ oder auch der entgegengesetzten Relation $\boldsymbol{F}(gk) = i^3\boldsymbol{F}(k)$ Genüge leisten; für die cyclischen Functionen der zweiten Ordnung soll auf analoge Weise die Bedingung $\boldsymbol{F}(gk) = -\boldsymbol{F}(k)$ als Definition festgesetzt werden. Unter dieser Voraussetzung ist nicht allein die vierte Potenz jeder cyclischen Function vierter Ordnung, sondern auch das Product aus irgend vier, welche derselben Relation genügen, und aus zweien, die den beiden entgegengesetzten Relationen genügen, eine gewöhnliche cyclische Function; Dasselbe gilt von dem Producte aus irgend zwei Functionen zweiter Ordnung. Da demnach, mit Rücksicht auf (§. 6.), die eben bezeichneten Verbindungen *ganzen Zahlen* gleich sein müssen, so kann man diese Bemerkung dazu anwenden, um die Werthe aller cyclischen Functionen zweiter und vierter Ordnung auf den bereits durch (4.) ermittelten Werth von $\boldsymbol{P}(k)$ zurückzuführen. Gesetzt die drei Functionen $\boldsymbol{F}(k)$, $\boldsymbol{F}'(k)$, $\boldsymbol{F}''(k)$ genügen den Bedingungen resp. $\boldsymbol{F}(gk) = i\boldsymbol{F}(k)$, $\boldsymbol{F}'(gk) = -i\boldsymbol{F}'(k)$, $\boldsymbol{F}'''(gk) = -\boldsymbol{F}'''(k)$, so sind, da auch $\boldsymbol{P}(gk) = i\boldsymbol{P}(k)$ ist, die folgenden Combinationen $\boldsymbol{F}(k)\boldsymbol{P}(k)^3$, $\boldsymbol{F}'(k)\boldsymbol{P}(k)$ und $\boldsymbol{F}''(k)\boldsymbol{P}(k)^2$ ganzen Zahlen gleich. Bezeichnet man diese ganzen Zahlen durch h, h', h'' und erhebt zur vierten Potenz, so erhält man, mit

Rücksicht auf den Werth von $P(k)^4$, aus (4.):

$$F(k)^4.(\varepsilon m)^3 = h^4, \quad F'(k)^4.\varepsilon m = h'^4, \quad F''(k)^4.m^2 = h''^4.$$

Da nun auch $F(k)^4$, $F'(k)^4$ und $F''(k)^4$ ganzen Zahlen gleich sind, so müssen h^4, h'^4, h''^4 durch m theilbar sein, und da m eine Primzahl ist, so mufs Dasselbe von h, h', h'' gelten. Setzt man demnach

$$h = mh_1, \quad h' = mh_1', \quad h'' = mh_1'',$$

so erhält man, nach Weglassung gemeinschaftlicher Factoren, die Resultate

$$F(k) = h_1\sqrt[4]{(\varepsilon m)}, \quad F'(k) = h_1'\sqrt[4]{(\varepsilon m)^3}, \quad F''(k) = h_1''\sqrt[4]{(\varepsilon m)},$$

welche in folgenden Lehrsatz vereinigt werden können:

„Bezeichnet man durch Δ die Wurzelgröfse $\sqrt[4]{((-1)^{\frac{1}{4}(p-1)}.m)}$, so ist „der Werth jeder cyclischen Function vierter Ordnung, welche der Bedingung „$F(gk) = iF(k)$ genügt, von der Form $h\Delta$. Genügt dieselbe der Bedingung „$F(gk) = -iF(k)$, so ist ihr Werth von der Form $h\Delta^3$. Endlich: ist der „Werth jeder cyclischen Function zweiter Ordnung, welche der Bedingung „$F(gk) = -F(k)$ genügt, von der Form $h\Delta^2$; und es bedeutet dabei h „jedesmal eine von der Natur der Function abhängige *ganze Zahl*."

Als Beispiel betrachte man den Ausdruck

$$\psi(k)^\mu + i^\alpha\psi(gk)^\mu + i^{2\alpha}\psi(g^2k)^\mu + \ldots + i^{(p-2)\alpha}\psi(g^{p-2}k)^\mu,$$

welcher in die Categorie der bei *Abel* vorkommenden gehört. Die vierte Potenz dieses Ausdrucks ist von der Form $h^4(-1)^{\frac{1}{4}(p-1)}m$, oder von der Form $h^4(-1)^{\frac{1}{4}(p-1)}m^3$, je nachdem $\alpha \equiv 3$ oder $\equiv 1 \pmod 4$ ist. Wenn $\alpha \equiv 2 \pmod 4$, so ist schon das Quadrat desselben eine ganze Zahl von der Form $h^2(-1)^{\frac{1}{4}(p-1)}m$.

In gewissen Fällen kann die ganze Zahl h sich auf Null reduciren; in solchen Fällen ist die cyclische Function selbst $= 0$ und die Form des Resultats wird illusorisch, da es sich von selbst versteht, dafs Null die Eigenschaften der cyclischen Functionen theilt und unter den mannigfaltigsten Formen aufgefafst werden kann; dafs aber immer solche Verbindungen existiren, für welche *h von Null verschieden* ist, ergiebt sich aus dem Obigen, und wäre es auch nur die einzige Function $P(k)$ selbst, welche gewifs dieser Bedingung genügt, indem für sie $h = 1$ ist. Die besondere Wichtigkeit dieser letztern Bemerkung wird weiter unten noch klarer hervortreten.

Das biquadratische, von *Gaufs* aufgestellte Reciprocitätsgesetz ergiebt sich, wie ich hier kurz anführen will, mit der gröfsten Leichtigkeit aus der in obigem Lehrsatze ausgesprochenen Eigenthümlichkeit der cyclischen Func-

tionen vierter Ordnung, und zwar leistet jede Function dieser Art zu dem Ende gleiche Dienste, nur ist es nöthig, wenn man m mit einer anderen primären Primzahl n vergleichen will, $F(k)$ so auszuwählen, dafs h zu n relative Primzahl wird. Dieser Bedingung genügt $P(k)$ selbst unter allen Umständen. Hat man also $F(gk) = iF(k)$ und mithin dem Lehrsatze zufolge $F(k)^4 = \varepsilon m h^4$ gefunden, so ergiebt sich nach den Principien in (§. 4.) $(\varepsilon m)^{\frac{1}{4}(q+3)} h^{q+3} = F(k)^{q+3} = F(k)^3 (F(nk) + nT(k))$; wo $N(n) = q$ gesetzt ist. Nimmt man $n \equiv g^\nu \pmod{m}$ an, so wird $F(nk) = F(g^\nu k) = i^\nu F(k)$, und wenn man noch statt $F(k)^3 T(k)$ blofs $T(k)$ schreibt und $i^\nu F(k)^4$ durch $i^\nu . \varepsilon m h^4$ ersetzt, so gelangt man zu einer Gleichung, der sich die Form

$$(\varepsilon m)^{\frac{1}{4}(q+3)} h^{q+3} - i^\nu . \varepsilon m h^4 = n . T(k)$$

geben läfst. Hier steht links eine ganze Zahl. Dividirt man dieselbe durch n, so erhält man, wenn nicht eine ganze, so doch mindestens eine rationale Zahl. Es hat also $T(k)$, welches eine ganze ganzzahlige Function der Gröfsen (1.) bedeutet, einen rationalen Werth und ist demnach nach den Principien in (§. 6.) einer ganzen Zahl gleich. Die obige Gleichung verwandelt sich demnach in eine gewöhnliche Congruenz $(\mathrm{mod.}\, n)$; aus derselben kann man noch den Factor $\varepsilon m h^4$ weglassen, da m von n verschieden und h wie vorausgesetzt zu n relative Primzahl ist; dies giebt dann

$$(\varepsilon m)^{\frac{1}{4}(q-1)} h^{q-1} \equiv i^\nu \pmod{n}.$$

Aus dieser Congruenz, in welcher $\varepsilon = (-1)^{\frac{1}{4}(p-1)}$ ist, ergiebt sich unmittelbar das gesuchte Reciprocitätsgesetz, wenn man bedenkt, dafs h^{q-1}, welches $\equiv 1 \pmod{n}$ ist, ebenfalls weggelassen werden kann, und dafs ν den biquadratischen Character von n in Bezug auf m (nach der Definition von *Gaufs*) bedeutet. Es ist leicht zu sehen, dafs das ganze Verfahren illusorisch werden würde, sobald $h = 0$ wäre.

Hieran schliefsen sich auch, wenn man den Analogieen der Kreistheilung folgt, diejenigen Zerfällungen der ganzen Function W, welche der Eintheilung ihrer Wurzelwerthe (1.) in zwei oder vier Perioden entsprechen. Setzt man

$$W_1 = (x - \psi(k))(x - \psi(g^2 k))(x - \psi(g^4 k)) \ldots (x - \psi(g^{p-3} k)),$$
$$W_2 = (x - \psi(gk))(x - \psi(g^3 k))(x - \psi(g^5 k)) \ldots (x - \psi(g^{p-2} k)),$$

so geht, wenn gk statt k substituirt wird, W_1 in W_2 und zugleich W_2 in W_1 über; es bleibt daher $W_1 + W_2$ durch diese Substitution ungeändert und $W_1 - W_2$ wechselt sein Zeichen; und zwar gilt dies für jeden Werth von x, also auch in Rücksicht der Coëfficienten dieser ganzen Functionen. Diese Coëf-

ficienten sind demnach für die Summe W_1+W_2 gewöhnliche cyclische Functionen, also ganze Zahlen, und für die Differenz W_1-W_2 cyclische Functionen zweiter Ordnung, also von der Form $h\sqrt{m}$. Hiernach ist es erlaubt

$$W_1+W_2 = Y, \quad W_1-W_2 = Z\sqrt{m}$$

zu setzen, wo Y und Z ganze ganzzahlige Functionen von x bedeuten, die erste vom Grade $\frac{1}{2}(p-1)$, die zweite vom Grade $\frac{1}{2}(p-3)$. Aus diesen Gleichungen folgt, durch Addition und Subtraction:

$$2W_1 = Y+Z\sqrt{m}, \quad 2W_2 = Y-Z\sqrt{m},$$

und da $W =$ dem Producte $W_1 W_2$ ist, „so läfst sich immer $4W$ auf die Form

$$\text{„}4W = (Y+Z\sqrt{m})(Y-Z\sqrt{m}) = Y^2-mZ^2 = Y^2+m(Zi)^2$$

„bringen." Durch eine mehr detaillirte Untersuchung läfst sich sogar zeigen, „dafs W selbst auf diese Form Y^2-mZ^2 gebracht werden kann." Y und Z sind stets beide von Null verschieden, weil sonst W als ein vollständiges Quadrat dargestellt werden könnte, was offenbar der in (§. 2.) bewiesenen Irreductibilität der Gleichung $W=0$ widerstreitet. Um wenigstens *ein* Beispiel zu geben, sei $m=-3$, $p=9$; dann ist $\varphi(-3t) = \frac{-3x+6x^5+x^9}{1+6x^4-3x^8}$, also $W = x^8+6x^4-3 = (x^4+3)^2-3.4$, $Y = x^4+3$, $Z = 2i$. Hier kann man nämlich $g = 1+i$ setzen, und die geraden Potenzen von g werden $\equiv 1$, $-i$, -1, i (mod. -3), die ungeraden Potenzen von $g \equiv$ denselben Zahlen noch mit $1+i$ multiplicirt; es nehmen daher W_1 und W_2 die Formen resp. x^4-w^4 und $x^4-w'^4$ an, wo w^4 und w'^4 die beiden Wurzeln der quadratischen Gleichung $\xi^2+6\xi-3=0$ sind. — Diese Art der Zerfällung steht im genauesten Zusammenhange mit der von *Dirichlet* im 24ten Bande gegenwärtigen Journals untersuchten Anzahl der binären quadratischen Formen in der complexen Zahlentheorie; doch will ich dem hochgeehrten Verfasser in der näheren Auseinandersetzung jenes Zusammenhanges nicht störend vorgreifen, da der zweite Theil seiner betreffenden Abhandlung (a. a. O. Seite 291) noch zu erwarten ist und *Dirichlet's eigene* weitere Durchführung dieses Gegenstandes gewifs ein Wunsch aller Freunde der Zahlentheorie sein wird.

Eine der obigen analoge Betrachtung der vier Factoren von W, welche der Zerlegung der Totalität der $p-1$ Wurzeln in 4 Perioden entsprechen, zeigt, mit Rücksicht auf die Eigenthümlichkeit der cyclischen Functionen vierter Ordnung, dafs diese vier Factoren in der Form

$$\tfrac{1}{4}(Y+Y'\Delta+Y''\Delta^2+Y'''\Delta^3)$$

enthalten sind, aus welcher sie hervorgehen, wenn man der Wurzelgröfse $\Delta = \sqrt[4]{((-1)^{\frac{1}{4}(p-1)}m)}$ ihre vier verschiedenen Werthe giebt. Y, Y', Y'', Y''' sind vier ganze Functionen von x mit ganzen Coëfficienten; die erste Y ist vom Grade $\frac{1}{4}(p-1)$, die übrigen drei sind wenigstens um einen Grad niedriger. Bezeichnet man nämlich die vier Factoren durch W_0, W_1, W_2, W_3, so ist nur zu bemerken, dafs die ganzen Functionen von x:

$$W_0+W_1+W_2+W_3, \quad W_0+iW_1-W_2-iW_3, \quad W_0-W_1+W_2-W_3$$
$$\text{und} \quad W_0-iW_1-W_2+iW_3,$$

so wie ihre Coëfficienten, cyclische Verbindungen resp. von der ersten, vierten, zweiten und vierten Ordnung sind, und dafs aufser der ersten in den drei anderen das höchste Glied $x^{\frac{1}{4}(p-1)}$ sich aufhebt. Das Übrige ergiebt sich leicht.

Cyclische Verbindungen *achter* Ordnung, zu denen ich jetzt übergehe, finden nur dann Statt, wenn $p \equiv 1 \pmod 8$, also $\frac{1}{4}(p-1)$ eine gerade Zahl ist. Unter dieser Voraussetzung, welche im Folgenden stets gelten soll, ist $(-1)^{\frac{1}{4}(p-1)} = +1$, $P(k)^4 = m$, und die Wurzelgröfse Δ geht in $\sqrt[4]{m}$ über.

Um die einfachste cyclische Function achter Ordnung, oder wenigstens eine solche, welche die leichteste Behandlung zuläfst, zu finden, zerlege ich das Product $P(k)$ abermals in zwei Factoren

$$(5.) \quad \begin{cases} \psi(k)\psi(g^2k)\psi(g^4k)\ldots\psi(g^{2\lambda-2}k) = Q(k), \\ \psi(gk)\psi(g^3k)\psi(g^5k)\ldots\psi(g^{2\lambda-1}k) = R(k), \end{cases}$$

wo der Kürze wegen $p-1 = 8\lambda$ gesetzt ist. Aus Q und R bilde ich die Verbindung

$$(6.) \quad Q(k) - \omega i R(k) = S(k) = S(k;\omega),$$

in welcher ω *irgend eine* der beiden Wurzeln der Gleichung $\omega^2 = i$ bezeichnet. Zwischen den Functionen Q und R finden folgende Relationen, bei denen nicht zu vergessen, dafs $\psi(g^{2\lambda}k) = \psi(ik) = i\psi(k)$ ist, Statt: $Q(gk) = R(k)$, $R(gk) = Q(g^2k) = iQ(k)$, $R(g^2k) = iQ(gk) = iR(k)$, u. s. w.; ferner $QR = P$, $Q^4R^4 = P^4 = m$. Für die Function S ergiebt sich hieraus $S(gk) = Q(gk) - \omega i R(gk) = R(k) + \omega Q(k) = \omega(Q(k) - \omega i R(k)) = \omega S(k)$; also ist S in der That eine cyclische Verbindung 8ter Ordnung: denn aus $S(gk) = \omega S(k)$ folgt $S(gk)^8 = S(k)^8$, da $\omega^8 = 1$ ist; und zwar gilt dies für beide Werthe von ω, die der Gleichung $\omega^2 = i$ genügen und deren einer dem andern entgegengesetzt und zugleich die 5te Potenz desselben ist. Statt indessen gleich von vorn herein bis zur 8ten Potenz von S aufzusteigen, be-

trachte ich zunächst S^2 und andere eben so einfache Verbindungen, welche sich bequem mit den bereits untersuchten cyclischen Functionen 4ter Ordnung vergleichen lassen. Beachtet man die für alles Folgende sehr wesentlichen Relationen

$$(7.) \quad P(gk) = iP(k) = \omega^2 P(k), \quad S(gk;\omega) = \omega S(k;\omega),$$
$$S(gk;\omega^5) = \omega^5 S(k;\omega^5),$$

so zeigt sich leicht, dafs die Verbindungen

$$S(k;\omega)^2 P(k)^3, \quad S(k;\omega^5)^2 P(k)^3, \quad S(k;\omega) S(k;\omega^5) P(k)$$

durch die Substitution von gk statt k unverändert bleiben; denn die in Folge der Relationen (7.) als Factoren hinzutretenden Potenzen von ω vereinigen sich jedesmal zu $\omega^8 = 1$. Da diese Unveränderlichkeit für beide Werthe von ω Statt findet, so sind alle jene Verbindungen nach (§. 6.) ganzen complexen Zahlen von der Form $A + B\omega$ gleich, so dafs A und B gewöhnliche ganze complexe Zahlen aus vierten Wurzeln der Einheit bedeuten. Um jene Verbindungen übersichtlicher darzustellen, kann man $S(k;\omega^5) = S'(k)$ setzen und die Zahl k überall weglassen, so dafs $S = Q - \omega iR$, $S' = Q + \omega iR$ geschrieben wird. Dann sind also

(8.) S^2P^3, S'^2P^3, $SS'P$, = ganzen Zahlen von der Form $A + B\omega$.

Ich entwickle jetzt die Ausdrücke in (8.), indem ich statt S und S' wieder die Verbindungen $Q - i\omega R$ und $Q + i\omega R$ setze und die Gleichungen $QR = P$, $P^4 = m$ zu Hülfe nehme. Dies giebt

$$S^2P^3 = (Q^2 - iR^2 - 2\omega iQR)P^3 = (Q^2 - iR^2)P^3 - 2\omega iP^4.$$

Der Coëfficient von ω wird also $= -2im$ und ist *a priori* angebbar; der übrige Theil $(Q^2 - iR^2)P^3$, welcher ω nicht enthält, mufs für sich ebenfalls einer ganzen Zahl gleich sein. Dies kann *a posteriori* nachgewiesen werden; denn setzt man gk statt k, so geht Q^2 in R^2, R^2 in $-Q^2$, also $Q^2 - iR^2$ in $R^2 + iQ^2 = i(Q^2 - iR^2)$, ferner P^3 in i^3P^3 über, also bleibt $(Q^2 - iR^2)P^3$ durch diese Substitution unverändert und ist deshalb nach (§. 6.) einer ganzen Zahl gleich. Diese ganze Zahl ist überdies nach (§. 5.) durch m theilbar, da der Ausdruck in Bezug auf die Wurzeln (1.) homogen und vom Grade $2\lambda + 6\lambda = 8\lambda = p - 1 > 0$ ist. Die für S^2P^3 zu setzende complexe Zahl $A + B\omega$ hat also die beiden Eigenschaften $B = -2im$ und $A \equiv 0 \pmod{m}$. Der Werth von S'^2P^3 geht entweder aus dem von S^2P^3 durch Vertauschung von ω mit $\omega^5 = -\omega$ hervor, oder kann auf dieselbe Weise ermittelt werden,

und man erhält

$$(9.) \qquad S^2P^3 = m(u-2i\omega), \quad S'^2P^3 = m(u+2i\omega).$$

Die Multiplication dieser beiden Gleichungen giebt

$$S^2S'^2P^6 = m^2(u+2i\omega)(u-2i\omega).$$

Läfst man links P^4, rechts statt dessen den Factor m weg, so kommt $(SS'P)^2 = m(u+2i\omega)(u-2i\omega)$, und da $SS'P$ ebenfalls eine ganze Zahl und zwar eine gewöhnliche complexe Zahl ist, indem $SS'P = (Q^2+iR^2)P$ die Wurzel ω nicht enthält, so mufs $m(u+2i\omega)(u-2i\omega)$ ein vollständiges Quadrat sein; woraus hervorgeht, dafs $(u+2i\omega)(u-2i\omega)$ (welches sich übrigens auf die gewöhnliche complexe Zahl u^2+4i reducirt) mit m aufgeht und dafs der Quotient der Division ebenfalls ein vollständiges Quadrat sein mufs. Setzt man $(u+2i\omega)(u-2i\omega) = mv^2$, so ist v eine gewöhnliche ganze complexe Zahl und man findet

$$(10.) \qquad SS'P = mv, \quad (u+2i\omega)(u-2i\omega) = mv^2.$$

Aus dem Werthe $\pm 2im$ des Coëfficienten von ω in S^2P^3 und S'^2P^3 (9.) ergiebt sich sogleich, dafs diese Gröfsen, und folglich auch S und S' selbst, ***von Null verschieden sind und dafs es demnach immer cyclische Verbindungen achter Ordnung giebt, die einen von Null verschiedenen Werth haben.*** — Die ganze Zahl u bleibt unbekannt; es läfst sich indessen ihr Rest (mod. m) angeben. Zu dem Ende ist es nach den Principien von (§. 5.) nur nöthig, den Ausdruck $(Q^2-iR^2)P^3 = mu$ in eine unendliche Reihe nach Potenzen von t zu entwickeln, nachdem man zuvor t statt $\frac{kC}{m}$ in den Wurzelgröfsen $\psi(k) = \varphi\left(\frac{kC}{m}\right)$, $\varphi(gk) = \psi\left(\frac{gkC}{m}\right)$ u. s. w. gesetzt hat, und in diese Reihe den Coëfficienten der niedrigsten Potenz von t aufzusuchen, deren Exponent durch $p-1$ theilbar ist. Für das vorliegende Beispiel wird die Auffindung jenes Coëfficienten dadurch ungemein erleichtert, dafs der zu entwickelnde Ausdruck vom Grade $p-1$ ist und also nur das erste Glied der Entwicklung, welches die Potenz t^{p-1} enthält, beibehalten zu werden braucht; auch bei der Entwicklung der einzelnen Theile ist jedesmal nur das erste Glied beizubehalten nöthig. Da wir es hierbei nur mit Producten von der Form $\varphi(rt)\varphi(r't)\varphi(r''t)$ zu thun haben, so bemerke man, dafs allgemein die Entwicklung der lemniscatischen Function $\varphi(rt)$ mit rt als erstem Gliede beginnt, und dafs demnach für ein Product wie $\varphi(rt)\varphi(r't)\varphi(r''t)\ldots$ der erste Coëfficient der Entwicklung zu dem Product der Zahlen $rr'r''\ldots$ wird,

wobei übrigens die Zahlen r, r', r'', ... ungleich, oder auch zum Theil gleich sein können. Hiernach fängt, wenn man die Entwicklung ausführt, Q^2 mit $(g^2g^4g^6 \ldots . g^{2\lambda-2})^2 t^{2\lambda} = g^{2\lambda(\lambda-1)} t^{2\lambda}$, R^2 mit $(gg^3g^5 \ldots . g^{2\lambda-1})^2 t^{2\lambda} = g^{2\lambda^2} t^{2\lambda}$ an, also $Q^2 - iR^2$ mit $g^{2\lambda(\lambda-1)}(1-ig^{2\lambda})t^{2\lambda}$; ferner fängt P^3 mit $(gg^2g^3g^4 \ldots . g^{2\lambda-1})^3 t^{6\lambda} = g^{3\lambda(2\lambda-1)} t^{6\lambda}$, also endlich der zu untersuchende Ausdruck $(Q^2 - iR^2)P^3$ mit $g^{2\lambda(\lambda-1)+3\lambda(2\lambda-1)}(1-ig^{2\lambda})t^{2\lambda} = g^{8\lambda^2-5\lambda}(1-ig^{2\lambda})t^{p-1}$ an. Da es sich nur um den Rest (mod. m) des gefundenen Coëfficienten $g^{8\lambda^2-5\lambda}(1-ig^{2\lambda})$ handelt, so kann man denselben vereinfachen, indem man die Congruenz $g^{2\lambda} \equiv i$ (mod. m) hinzuzieht; $1-ig^{2\lambda}$ geht dann in $1-i.i=2$ über, $g^{8\lambda^2}$ wird $\equiv 1$, $g^{-5\lambda} \equiv g^{3\lambda} \equiv ig^{\lambda}$, also kann blofs $2ig^{\lambda}$ statt des Coëfficienten von t^{p-1} geschrieben werden. Vergleicht man dies mit dem allgemeinen Satze $\frac{1}{m^{\nu}} F(k) \equiv (-1)^{\nu}\delta$ (mod. m) in (§. 5.), so ist hier $\nu = 1$, $\delta \equiv 2ig^{\lambda}$ (mod. m), mithin $u = \frac{1}{m}(Q^2 - iR^2)P^3 \equiv -2ig^{\lambda}$ (mod. m). Man bemerke die hieraus sich ergebenden Congruenzen

$$(11.) \qquad u - 2i\omega \equiv -2i(g^{\lambda} + \omega), \quad u + 2i\omega \equiv -2i(g^{\lambda} - \omega) \text{ (mod. } m),$$

durch deren Multiplication sich das schon oben gefundene Resultat bestätigen läfst, dafs nämlich das Product $(u-2i\omega)(u+2i\omega)$ durch m theilbar ist; denn dieses Product wird $\equiv -4(g^{\lambda}+\omega)(g^{\lambda}-\omega) \equiv -4(g^{2\lambda}-i)$ (mod. m) und $g^{2\lambda}-i$ ist wirklich durch m theilbar. Um indessen einzusehen, wie sich der Divisor m auf die beiden Factoren vertheilt, sind einige Sätze aus der elementaren Theorie der aus achten Wurzeln der Einheit zusammengesetzten Zahlen nothwendig, mit welchen ich mich im folgenden Paragraphen beschäftigen werde. Inzwischen folgt über die Form von S und S', soweit das Bisherige reicht, dafs

$$(12). \qquad \begin{cases} S = \sqrt{(u-2i\omega)}\sqrt[8]{m}, & S' = \sqrt{(u+2i\omega)}\sqrt[8]{m}, \\ S^8 = m(u-2i\omega)^4, & S'^8 = m(u+2i\omega)^4 \end{cases}$$

ist, wie sich aus (9.) ergiebt, wenn man statt P seinen Werth $\sqrt[4]{m}$ setzt; das Product beider Wurzelverbindungen in (12.) enthält nur noch die eine Irrationalität $\sqrt[4]{m}$, wie aus (10.) hervorgeht, und die ganze Zahl u ist $\equiv -2ig^{\lambda}$ (mod. m). Zu einer gründlichen Erforschung der in (12.) vorkommenden Irrationalitäten ist es jedoch ebenfalls erforderlich, die wichtigsten elementaren Sätze über die aus achten Wurzeln der Einheit zusammengesetzten Zahlen vorauszuschicken.

§. 8.

Die aus 8ten Wurzeln der Einheit zusammengesetzten complexen Zahlen betrachte ich immer unter der Form $A+B\omega$, in welcher $A=a+bi$, $B=c+di$ gewöhnliche complexe Zahlen sind und $\omega^2=i$ ist. Vollständig ausgeschrieben wird eine solche Zahl

$$a+bi+(c+di)\omega = a+c\omega+b\omega^2+d\omega^3,$$

und wenn man $a+cx+bx^2+dx^3=a+bx^2+(c+dx^2)x=f(x)$ setzt, so wird sie $=f(\omega)$. A und B bleiben unverändert, wenn $\omega^5=-\omega$ an die Stelle von ω tritt; dann geht $A+B\omega=f(\omega)$ in $A-B\omega=f(\omega^5)$ über. Anders verhält es sich, wenn ω^3 oder ω^7 statt ω gesetzt wird, wodurch i in $-i$ und A und B gleichzeitig in ihre conjugirten Werthe $a-bi$ resp. $c-di$ übergehen. Da das Product der beiden Werthe $A+B\omega$ und $A-B\omega$, welche ich *zugeordnete* nennen will, eine wichtige Rolle spielt, und da das Wort *Norm* schon eine anderweitige, ganz bestimmte Bedeutung als Quadrat des analytischen Moduls für die imaginären Ausdrücke erhalten hat, so entsteht in der That eine Verlegenheit, wie ein solches Product zu bezeichnen sei. Ich will, in Ermangelung eines besseren Ausdrucks, das Product $(A+B\omega)(A-B\omega)=f(\omega)f(\omega^5)$, welches die gewöhnliche complexe Zahl A^2-iB^2 vorstellt, einstweilen das *Normalproduct* von $A+B\omega$ oder $A-B\omega$ nennen und durch $\mathfrak{N}(A+B\omega)=\mathfrak{N}(A-B\omega)$ bezeichnen. Die Norm von $f(\omega)$ ist dagegen das immer positive Product $f(\omega)f(\omega^7)=Nf(\omega)=Nf(\omega^7)$, die Norm von $f(\omega^3)$ das ebenfalls positive Product $f(\omega^3)f(\omega^5)=Nf(\omega^3)=Nf(\omega^5)$. Das Product aller vier Werthe $f(\omega)f(\omega^3)f(\omega^5)f(\omega^7)$ ist die Norm des Normalproducts $=N\mathfrak{N}(A+B\omega)=N(A^2-iB^2)$ und hat immer einen reellen positiven und zwar *ganzen* Werth, wenn A und B ganze Zahlen sind. Da die vorliegenden complexen Zahlen vom Standpuncte der gewöhnlichen complexen Zahlentheorie und nicht von dem der reellen angesehen werden und ω nicht sowohl als achte Wurzel der Einheit, sondern als Wurzel der Gleichung $\omega^2=i$ zu betrachten ist, so soll im Allgemeinen eine Trennung von A und B in ihre weiteren Bestandtheile nicht unnöthigerweise vorgenommen werden, und ich unterscheide nur die beiden Fälle der complexen Zahl $A+B\omega$, wenn $B=0$, und wenn B von Null verschieden ist. Im ersten Falle ist dieselbe monom und man hat $f(\omega)=f(\omega^5)$, $\mathfrak{N}f(\omega)=f(\omega)^2=A^2$, im zweiten ist sie binom und $f(\omega^5)$ ist von $f(\omega)$ verschieden. Für gewisse Betrachtungen könnte es von Interesse sein, die Fälle, in welchen die complexe Zahl auf die Form $a+b\sqrt{2}$ oder $a+b\sqrt{-2}$ gebracht werden kann und in welchen

entweder $f(\omega)$ mit $f(\omega^7)$ und $f(\omega^3)$ mit $f(\omega^5)$, oder $f(\omega)$ mit $f(\omega^3)$ und $f(\omega^5)$ mit $f(\omega^7)$ übereinstimmt, speciell hervorzuheben und von den übrigen abzusondern: für den gegenwärtigen Zweck scheint indessen eine solche Unterscheidung überflüssig und würde nur unnöthige Complicationen verursachen.

Obwohl die elementaren Sätze über diese complexen Zahlen aus der von *Dirichlet* gegebenen Theorie der binären quadratischen Formen für die gewöhnlichen complexen Zahlen abgeleitet werden können, wenn man der Determinante den speciellen Werth i giebt*), so scheint es mir doch einfacher und angemessener, einem demjenigen ähnlichen Wege zu folgen, welchen auch *Dirichlet* am Anfange seiner oben erwähnten Abhandlung (a. a. O. §. 2.) eingeschlagen hat und welcher schon von *Gaufs* in seinen „Disq. Arithm." für reelle Zahlen, ja selbst schon von *Euclid* vorgezeichnet worden ist. Man geht hierbei von folgender Grundbetrachtung aus. Ist $\alpha+\beta\omega$ eine beliebige gegebene complexe Zahl, in welcher α und β nicht nothwendig ganze Zahlen sind, sondern beliebig rationale oder irrationale Werthe haben können, $k+l\omega$ eine unbestimmte *ganze* complexe Zahl, und setzt man die Differenz

$$\alpha+\beta\omega-(k+l\omega) = (\alpha-k)+(\beta-l)\omega = f(\omega),$$

so läfst sich über die unbestimmten ganzen Zahlen k und l immer so verfügen, dafs das Product $f(\omega)f(\omega^3)f(\omega^5)f(\omega^7)<1$ wird, wobei das Zeichen $<$ in allen Fällen die Gleichheit ausschliefst. Setzt man $f(\omega)f(\omega^3)f(\omega^5)f(\omega^7)=\Pi$ und bezeichnet durch ein vorgesetztes M den analytischen Modul irgend einer Gröfse, so erhält man

$$\Pi = N[(\alpha-k)^2-i(\beta-l)^2], \qquad \sqrt{\Pi} = M[(\alpha-k)^2-i(\beta-l)^2].$$

Betrachtet man den Ausdruck $(\alpha-k)^2-i(\beta-l)^2$ als die Summe aus $(\alpha-k)^2$ und $-i(\beta-l)^2$, und bemerkt, dafs $M(\alpha-k)^2=N(\alpha-k)$ und $M(-i(\beta-l)^2)$ $=M(\beta-l)^2=N(\beta-l)$ ist, so folgt aus einem bekannten Satze:

$$\sqrt{\Pi} \leqq N(\alpha-k)+N(\beta-l).$$

In den beiden Normen $N(\alpha-k)$ und $N(\beta-l)$ kann man die ganzen Zahlen k und l immer so bestimmen, dafs jene entweder beide $<\frac{1}{2}$ werden, oder wenigstens die eine $<\frac{1}{2}$, die andere $=\frac{1}{2}$ wird. Eine Ausnahme macht nur der Fall, wenn α und β gleichzeitig von der Form $\pm\frac{1}{2}\pm\frac{1}{2}i$ sind; d. h. man kann immer $N(\alpha-k)\leqq\frac{1}{2}$ und $N(\beta-l)\leqq\frac{1}{2}$ machen und beide untere Zeichen zugleich braucht man nur in dem einzigen eben erwähnten Falle gelten zu lassen. Mit Ausnahme dieses einen Falles hat man also stets, wenn k und l

*) Vergl. *Jacobi's* Bemerkung hierüber im 19ten Bande dieses Journals S. 316.

demgemäfs bestimmt werden, $\sqrt{\Pi} \leqq N(\alpha - k) + N(\beta - l) < \frac{1}{2} + \frac{1}{2} < 1$, also auch $\Pi < 1$ (nicht $\leqq 1$); wie behauptet. Was den ausgenommenen Fall betrifft, in welchem $\alpha = \pm\frac{1}{2} \pm \frac{1}{2}i$ und zugleich $\beta = \frac{1}{2} \pm \frac{1}{2}i$, so kann man für diesen der Zahl $f(\omega)$ die Form $(\frac{1}{2} + \frac{1}{2}i) + \omega(\frac{1}{2} + \frac{1}{2}i) = \frac{1}{2}(1+i).(1+\omega)$ geben und es wird $\Pi = \frac{1}{2}$, also auch in diesem Falle $\Pi < 1$.

Aus diesem Princip geht hervor, dafs zu dem Quotienten je zweier gegebenen ganzen complexen Zahlen von der hier betrachteten Art $\frac{A + B\omega}{A' + B'\omega}$ immer eine *ganze* complexe Zahl $k + l\omega$ dergestalt bestimmt werden kann, dafs für die Differenz $\frac{A + B\omega}{A' + B'\omega} - (k + l\omega)$ die Norm des Normalproducts unter der Einheit liegt und dafs also

$$N\mathfrak{R}(A + B\omega - (k + l\omega)(A' + B'\omega)) < N\mathfrak{R}(A' + B'\omega)$$

wird. Hierdurch wird die Möglichkeit gegeben, die bekannte Operation der Aufsuchung des gröfsten gemeinschaftlichen Theilers zweier Zahlen auch für die hier vorliegenden complexen Zahlen so durchzuführen, dafs die Reihe der zu bildenden Quotienten und Reste endlich abbricht; und im Gefolge dieser Operation ergeben sich alle diejenigen elementaren Sätze über die Theilbarkeit der Zahlen durch einander und ihre Darstellbarkeit durch Producte von Primzahlen, welche das Fundament der reellen und der gewöhnlichen, von *Gaufs* eingeführten complexen Zahlentheorie ausmachen. Da sich demnach in der neuen Theorie mit wenigen Ausnahmen Alles vollkommen analog gestaltet, so wird es der Kürze wegen genügen, wiederholt auf die ersten Paragraphen der schon oft citirten Abhandlung von *Dirichlet* im 24ten Bande gegenwärtigen Journals zu verweisen und nur die eigenthümlichen Puncte der Theorie hervorzuheben, unter welchen die Betrachtung der complexen Einheiten obenan steht.

Unter den complexen Einheiten will ich alle diejenigen ganzen Zahlen zusammenfassen, deren Normalproduct eine gewöhnliche Einheit ± 1, oder $\pm i$ ist. Aufser den Potenzen von ω sind also noch die übrigen Lösungen der Gleichungen $A^2 - iB^2 = \pm 1$ und $A^2 - iB^2 = \pm i$ aufzusuchen. Ich bemerke, dafs aus den Lösungen der Gleichung $A^2 - iB^2 = +1$ sofort die der drei übrigen in der Form $A^2 - iB^2 = i^\mu$ enthaltenen Gleichungen durch Multiplication mit einer Potenz von ω hervorgehen. Denn genügt $f(\omega)$ der ersteren, so dafs $f(\omega)f(\omega^5) = 1$ ist, so hat man, $f'(\omega) = \omega^{-\mu} f(\omega)$ setzend:

$$f'(\omega)f'(\omega^5) = \omega^{-\mu}\omega^{-5\mu} f(\omega)f(\omega^5) = \omega^{-6\mu} = \omega^{2\mu} = i^\mu;$$

also genügt dann $\omega^\mu f(\omega)$ der Gleichung $A^2 - iB^2 = i^\mu$; und umgekehrt: jedesmal, wenn $f'(\omega)$ der letzteren Gleichung genügt, ist $\omega^\mu f'(\omega) = f(\omega)$ eine Lösung von $A^2 - iB^2 = 1$; so dafs demnach, wenn $f(\omega)$ *alle* Lösungen dieser Gleichung enthält, $\omega^{-\mu} f(\omega)$ *alle* Lösungen von $A^2 - iB^2 = i^\mu$ ergeben wird. *Dirichlet* hat die allgemeine Theorie der Gleichung $A^2 - DB^2 = 1$ für eine beliebige gewöhnliche complexe Zahl D aufgestellt und dabei den Fall besonders hervor gehoben, wenn D einen reellen Werth hat, oder, wie dies hier der Fall ist, das $i$fache einer reellen Zahl bedeutet. Seinen Andeutungen folgend, setze man $A = \alpha + \beta i$, $B = \gamma + \delta i$, wodurch die Gleichung

$$(\alpha + \beta i)^2 - i(\gamma + \delta i)^2 = 1$$

in die beiden

$$\text{(a.)}\quad \alpha^2 - \beta^2 + 2\gamma\delta = 1 \quad \text{und} \quad \text{(b.)}\quad 2\alpha\beta - \gamma^2 + \delta^2 = 0$$

zerfällt. Die zweite läfst sich so schreiben:

$$\text{(c.)}\quad 2\alpha\beta = (\gamma + \delta)(\gamma - \delta);$$

woraus hervorgeht, dafs einer der beiden Factoren $\gamma + \delta$ und $\gamma - \delta$ gerade ist, also, da Summe und Differenz zweier Zahlen immer zugleich entweder gerade oder ungerade sind, dafs auch der andere Factor gerade sein mufs. Setzt man demnach $\gamma + \delta = 2k$, $\gamma - \delta = 2h$, so wird $\gamma = k + h$, $\delta = k - h$, $2\gamma\delta = 2(k^2 - h^2)$ und aus (c.) wird

$$\text{(b.)}\quad \alpha\beta = 2kh.$$

Erster Fall: β gerade $= 2\beta'$; $\alpha\beta' = kh = abcd$, $\alpha = ab$, $\beta' = cd$, $k = ac$, $h = bd$; aus (a.) wird $a^2b^2 - 4c^2d^2 + 2a^2c^2 - 2b^2d^2 = (a^2 - 2d^2)(b^2 + 2c^2) = 1$; da also $b^2 + 2c^2$ in 1 aufgeht und gewifs positiv ist, so kann nur $b^2 + 2c^2 = +1$ sein, also $c = 0$ und $b = \pm 1 = \varepsilon$; ferner ist dann zugleich $a^2 - 2d^2 = 1$. Hiernach ist $\beta' = cd = 0$, also auch $\beta = 0$, $k = ac = 0$, $h = \varepsilon d$, $\alpha = \varepsilon a$, $\gamma = \varepsilon d$, $\delta = -\varepsilon d$, folglich in diesem Falle $f(\omega) = \varepsilon(a + \omega(1-i)d) = \varepsilon(a + d\sqrt{2})$, während $a^2 - 2d^2 = 1$. ***Zweiter Fall:*** α gerade $= 2\alpha'$; $\alpha'\beta = kh = abcd$, $\alpha' = ab$, $\beta = cd$, $k = ac$, $h = bd$; aus (a.) wird $(2a^2 - d^2)(2b^2 + c^2) = 1$, woraus, wie vorhin, $b = 0$, $c = \pm 1 = \varepsilon$, $d^2 - 2a^2 = -1$, $\alpha = h = 0$, $\beta = \varepsilon d$, $\gamma = \delta = k = \varepsilon a$, $f(\omega) = \varepsilon(di + \omega(1+i)a) = \varepsilon i(d + a\sqrt{2})$, während $d^2 - 2a^2 = -1$. Die einfachste Lösung der Gleichung $x^2 - 2y^2 = -1$ ist $x = 1$, $y = 1$, also sind alle Lösungen von $x^2 - 2y^2 = -1$ in $\pm(1+\sqrt{2})^{2\nu+1}$, ν von $-\infty$ bis ∞, und alle Lösungen von $x^2 - 2y^2 = +1$ in $\pm(1+\sqrt{2})^{2\nu}$ enthalten. Daher sind alle Werthe von $f(\omega)$ in den beiden Formen

$$\pm(1+\sqrt{2})^{2\nu} \quad \text{und} \quad \pm i(1+\sqrt{2})^{2\nu+1}$$

enthalten, die sich in $\pm[i(1+\sqrt{2})]^\nu$ vereinigen lassen, weil $i^\nu = \pm 1$ oder $= \pm i$, je nachdem ν gerade oder ungerade ist. Da $i\sqrt{2} = \omega.\omega\sqrt{2} = \omega(1+i)$ ist, so hat man, in der gewöhnlichen Form ausgedrückt, $f(\omega) = \pm(i+\omega(1+i))^\nu = \pm e^\nu$, wenn die einfachste complexe Einheit $i+\omega(1+i)$ hier und im Folgenden durch e bezeichnet wird. Alle complexen Einheiten sind demnach in der Formel

$$(13.)\quad \mathfrak{E}(\omega) = \omega^\mu e^\nu \begin{Bmatrix} \mu \text{ von } 0 \text{ bis } 7 \\ \nu \text{ von } -\infty \text{ bis } \infty \end{Bmatrix},\quad e = i+\omega(1+i) = (1+\omega)^2:(1-i)$$

enthalten. Die Zahl e fällt, abgesehen von dem Factor i, mit dem positiven und von 1 verschiedenen Werthe $1+\sqrt{2}$ zusammen, und es sind daher alle ihre Potenzen sowohl unter sich als auch von den Potenzen von ω verschieden. Die Potenzen der zugeordneten Zahl $e' = i-\omega(1+i)$ liefern keine neuen complexen Einheiten; denn aus $ee' = 1$ folgt $e' = e^{-1}$, also fallen die positiven Potenzen von e' mit den negativen von e und umgekehrt zusammen.

Nach den complexen Einheiten sind die einfachsten complexen Zahlen $1+\omega$ und die Potenzen dieser Zahl. Von ihnen ist zu bemerken: 1) das Normalproduct von $1+\omega$ ist $(1+\omega)(1-\omega) = 1-i$, hiervon 2 ist die Norm; 2) $1+\omega$ geht für jeden ganzen Werth von μ in $1+\omega^\mu$ auf; wenn μ ungerade, so ist der Quotient eine complexe Einheit; jede Potenz von ω ist $\equiv 1 \pmod{1+\omega}$. 3) Die Potenzen von $1+\omega$ können, so oft sie als Moduln vorkommen, durch einfachere Zahlen ersetzt werden: die geraden Potenzen $(1+\omega)^2$, $(1+\omega)^4$, $(1+\omega)^6$, $(1+\omega)^8$ u. s. w. durch resp. $1\pm i$, 2, $2\pm 2i$, 4 u. s. w., die ungeraden Potenzen durch die Producte dieser Zahlen in $1+\omega$, so dafs z. B. $(1+\omega)^{17}$ mit $8+8\omega$ gleichgeltend ist. 4) Alle complexen ganzen Zahlen zerfallen in ***ungerade*** und in solche, die durch $1+\omega$ oder eine höhere Potenz von $1+\omega$ theilbar sind; jede ungerade Zahl $A+B\omega$ ist $\equiv 1 \pmod{1+\omega}$ und für sie ist eine der beiden Zahlen A, B ungerade, die andere gerade, d. h. durch $1+i$ theilbar. Wenn $A+B\omega$ durch $1+\omega$, aber nicht durch $1+i$ theilbar ist, so sind A und B beide ungerade; in jedem anderen Falle sind A und B beide durch $1+i$ theilbar. 5) Die ungeraden Zahlen kann man durch Multiplication mit Potenzen von ω und mit der einfachsten Einheit e immer so einrichten, dafs sie in Bezug auf die hier in Rede stehenden Moduln gewissen Bedingungen genügen, die in der Folge von Wichtigkeit sein werden. In $f(\omega) = A+B\omega$ ist entweder A ungerade und B gerade, oder es verhält sich umgekehrt, und in letzterm Falle wird $\omega(A+B\omega) = iB+\omega A$ eine solche Zahl, für welche der erste Bestandtheil ungerade, der

Coëfficient von ω gerade ist; unter den beiden Zahlen $f(\omega)$ und $\omega f(\omega)$ befindet sich also eine und nur eine, die dieser Bedingung genügt. Durch Multiplication mit i kann man ferner erreichen, dafs $A \equiv 1 \pmod 2$ wird, d. h. dafs in $A = a + bi$, a ungerade, b gerade wird und dafs nicht das Umgekehrte Statt findet; genügt A schon von selbst dieser Bedingung, so unterläfst man die Multiplication. Auf diese Weise ermittelt man unter den vier Zahlen $f(\omega)$, $\omega f(\omega)$, $if(\omega)$, $i\omega f(\omega)$ eine und nur eine, $A + B\omega$, für welche gleichzeitig $A \equiv 1 \pmod 2$ und $B \equiv 0 \pmod{1+i}$ ist. Nachdem dies geschehen, kann man mittels der Factoren ± 1 und e über neue Bedingungen verfügen. Je nachdem B durch 2 oder blofs durch $1+i$ theilbar ist, wird die dem Vorhergehenden gemäfs eingerichtete Zahl $\equiv 1$ oder $\equiv 1 + \omega(1-i) \pmod 2$; im letzteren Falle wird $if(\omega) \equiv e \pmod 2$. Man findet demnach unter je vier Zahlen, wie $f(\omega)$, $\omega f(\omega)$, $if(\omega)$, $i\omega f(\omega)$, stets eine und nur eine, die entweder $\equiv 1 \pmod 2$, oder $\equiv e \pmod 2$ ist; und zwar hangt das Letztere vom Reste des Quotienten $\frac{B}{1+i} \pmod{1+i}$ ab. Das Product zweier Zahlen, welche beide $\equiv e \pmod 2$ sind, ist $\equiv 1 \pmod 2$; denn dasselbe ist $\equiv e^2 \pmod 2$ und man hat $e^2 = -1 + 2\omega(1+i)i + 2i.\omega^2 \equiv -1 \equiv 1 \pmod 2$; wenn also $f(\omega)$ nicht schon $\equiv 1 \pmod 2$ ist, sondern $\equiv e \pmod 2$, so ist sicher $ef(\omega) \equiv 1 \pmod 2$. Vereinigt man dies mit dem Früheren, so folgt, dafs es, wenn $f(\omega)$ irgend eine ungerade Zahl bezeichnet, unter den acht Zahlen

$$f(\omega),\ \omega f(\omega),\ \omega^2 f(\omega),\ \omega^3 f(\omega),\ ef(\omega),\ e\omega f(\omega),\ e\omega^2 f(\omega),\ e\omega^3 f(\omega)$$

eine und nur eine giebt, welche $\equiv 1 \pmod 2$, d. h. für welche $A \equiv 1 \pmod 2$ und $B \equiv 0 \pmod 2$, für welche also, wenn $A = a + bi$, $B = c + di$ gesetzt wird, a ungerade, b, c und d gerade sind. Benutzt man endlich den Factor ± 1 dazu, um, wie es für die Anwendung auf die Theorie der achten Potenzreste am zweckmäfsigsten scheint,

$$(14.)\quad \begin{cases} A \equiv 1 \pmod{2+2i} \text{ zu machen, wenn } B \equiv 0 \pmod{2+2i} \text{ (I.) und} \\ A \equiv -1 \pmod{2+2i} \text{ zu machen, wenn } B \equiv 2 \pmod{2+2i} \text{ (II.),} \end{cases}$$

und nennt eine so bestimmte complexe Zahl eine *primäre* Zahl (der ersten oder zweiten Art, je nachdem I. oder II. Statt findet), so findet sich unter den 16, in den beiden Formeln $\omega^\mu f(\omega)$ und $\omega^\mu ef(\omega)$ enthaltenen Zahlen ebenfalls eine und nur eine primäre Zahl. Ob dieselbe zur ersten oder zweiten Art, d. h. in die Categorie (I.) oder (II.) gehört, hangt davon ab, ob B durch $2+2i$, oder blofs durch 2 und nicht mehr durch $(1+i)^3$ theilbar ist, und es kann

hierüber nicht mehr nach Willkür verfügt werden. Die in (I.) enthaltenen primären Zahlen sind $\equiv 1 \pmod{2+2i}$, die in (II.) enthaltenen $\equiv -1+2\omega \equiv 3+2\omega \pmod{2+2i}$, beide Arten sind $\equiv 1 \pmod{2+2\omega}$. Zwei Zahlen, welche entweder beide zur ersten oder beide zur zweiten Art gehören, geben mit einander multiplicirt ein Product, welches zur ersten Art gehört, denn es ist $(3+2\omega)^2 \equiv 9 \equiv 1 \pmod 4$, also gewifs $\equiv 1 \pmod{2+2i}$. Zwei zu verschiedenen Arten gehörige primäre Zahlen geben ein in (II.) gehöriges Product; eine *monome* Zahl A, für welche also $B=0$, ist offenbar nach der hier gegebenen Definition primär und zur ersten Art gehörig, wenn sie im Sinne von *Gauſs* primär, nämlich $\equiv 1 \pmod{2+2i}$ ist. Es ist von Wichtigkeit, unter den einer ungeraden Zahl $f(\omega)$ associirten und in der Form $\omega^\mu e^\nu f(\omega)$ enthaltenen Zahlen diejenigen hervorzuheben, welche gleichzeitig primär sind, wenn $f(\omega)$ als primär vorausgesetzt wird. Diese Zahlen sind in der Form $e^{2\nu} f(\omega)$ begriffen, und alle übrigen sind nicht primär; der zweite Theil dieser Behauptung wird durch das Vorhergehende evident. Um sich von der Richtigkeit des ersten Theils zu überzeugen, genügt es offenbar, zu untersuchen, ob e^2 und demnach jede Potenz von e^2 eine primäre Zahl sei. Dies ist in der That der Fall; denn $e^2 = -3+(2+2i)i\omega$ ist nicht blofs primär, sondern überdies zur Categorie (I.) gehörig, so dafs die Zahlen $e^{2\nu} f(\omega)$ primär sind und mit $f(\omega)$ zu derselben Art gehören. Eine primäre Zahl bleibt demnach primär, wenn man sie mit solchen complexen Einheiten multiplicirt, welche geraden Potenzen von $e = i+(1+i)\omega$ gleich sind. Dies ist nicht der Fall in Bezug auf andere complexe Einheiten; ferner ist es unmöglich, durch eine solche Multiplication die primäre Zahl aus einer Art in die andere zu versetzen. 6) Läfst man für einen Augenblick $f(\omega)$ die Totalität aller primären Zahlen bedeuten, so ist nach dem Vorhergehenden jede ungerade Zahl in einer der beiden Formen $\omega^\mu f(\omega)$, $\omega^\mu e f(\omega)$ enthalten, welche in der That 16 verschiedene Formen ausmachen. Es lassen sich hieraus verschiedene Folgerungen ziehn. Bildet man das Normalproduct dieser Formen, so erhält man, da $ee' = 1$ und $\omega^\mu \omega^{5\mu} = (-i)^\mu$ ist: $(-i)^\mu f(\omega) f(\omega^5) = (-i)^\mu (A^2 - iB^2)$. Da nun $f(\omega)$ primär, also jedenfalls $A \equiv 1 \pmod 2$, $B \equiv 0 \pmod 2$ vorausgesetzt wird, so hat man $A^2 - iB^2 \equiv 1 \pmod 4$, und der obige Ausdruck wird $\equiv (-i)^\mu \pmod 4$. Es wird hierdurch ersichtlich, dafs verschiedenen Formen der Zahl verschiedene Formen des Normalproducts und umgekehrt entsprechen, dafs die Zahl nur dann primär sein kann, wenn auch das Normalproduct im gewöhnlichen Sinne primär ist, dafs es keine Zahl giebt, deren Normalproduct

$\equiv 3+2i \pmod 4$ wäre, dafs eine Zahl, deren Normalproduct primär und folglich (da der andere Fall eben ausgeschlossen worden ist) $\equiv 1 \pmod 4$ ist, nur in den Formen $\pm f(\omega)$ oder $\pm ef(\omega)$ enthalten sein kann u. s. w. Das Quadrat jeder ungeraden Zahl ist in den Formen $i^\mu+4L$ oder $i^\mu e^2+4L$ enthalten, die sich wegen $e^2 \equiv 1 \pmod{2+2i}$ in $i^\mu+(2+2i)L$ vereinigen lassen; das Biquadrat ist in $(-1)^\mu+8L$ oder $(-1)^\mu e^4+8L$ zusammen in $(-1)^\mu+(4+4i)L$ enthalten, die achte Potenz immer in der Form $1+(8+8i)L$ u. s. w.

Bei der Untersuchung der ungeraden complexen ***Primzahlen***, welche nun ihren Platz findet, gehe ich dem oben festgesetzten Standpuncte gemäfs nicht von der Zerfällung der reellen, sondern, was die Betrachtung ungemein vereinfacht, von der Zerfällung der gewöhnlichen complexen Primzahlen aus. Es sei m eine solche Primzahl und wenn es möglich ist $m=(A+B\omega)(C+D\omega)$, wo beide Factoren von complexen Einheiten verschieden sind. Man kann m als primär voraussetzen, da ja die Zerfällung von Einheiten wiederum nur auf die bereits vollständig erledigten Einheiten zurückführt. $A+B\omega$ und $C+D\omega$ dürfen dann ebenfalls beide primär angenommen werden. A und B können keinen gemeinschaftlichen Factor haben, denn ein solcher könnte, da m Primzahl ist, nur m selbst sein, und $C+D\omega$ würde sich dann auf eine complexe Einheit reduciren; eben so wenig können C und D einen gemeinschaftlichen Factor haben. Die vorgelegte Gleichung zerfällt in $AC+BDi=m$ und $AD+BC=0$; schreibt man die letztere so: $AD=-BC$, so folgt, da A zu B und D zu C relative Primzahl ist, dafs nur entweder $C=\pm A$ und dann $D=\mp B$, oder $C=\pm iA$ und dann $D=\mp iB$ angenommen werden kann. Die zweite Annahme ist deshalb unstatthaft, weil bei derselben nicht gleichzeitig A und $C \equiv 1 \pmod 2$ sein könnten, und in Bezug auf die erste können nur die obern Zeichen gelten, weil sonst ebenfalls $A+B\omega$ und $C+D\omega$ nicht beide primär sein könnten. Es wird also der zweite Factor $C+D\omega = A-B\omega$ die dem ersten $A+B\omega$ zugeordnete Zahl und $m=A^2-iB^2$, so dafs nur noch zu untersuchen bleibt, welche Primzahlen m in diese Form gebracht und demnach als Normalproducte anderer Zahlen $A+B\omega$ angesehen werden können. Alle primären Primzahlen m zerfallen in dieser Hinsicht in zwei Classen, je nachdem sie $\equiv 1$ oder $\equiv 3+2i \pmod 4$ sind, und es ist dies dieselbe Eintheilung, welche auch bei den biquadratischen Resten eine Rolle spielt und zuerst von ***Gaufs*** aufgestellt worden ist. Dafs die zur zweiten Classe gehörigen Zahlen nicht als Normalproducte dienen können, ist schon

oben gezeigt worden; es bleibt nur zu beweisen, dafs die der ersten Classe wirklich diese Eigenschaft besitzen. Wenn $m \equiv 1 \pmod 4$, so ist $N(m) = p \equiv 1 \pmod 8$. Setzt man, wie im vorigen Paragraphen, $p-1 = 8\lambda$ und bedeutet wieder g eine primitive Congruenzwurzel (mod. m), die der Bedingung $g^{2\lambda} \equiv i \pmod m$ genügt, so ist $g^{2\lambda} - i = (g^\lambda + \omega)(g^\lambda - \omega)$ durch m theilbar, und da die beiden Factoren $g^\lambda + \omega$ und $g^\lambda - \omega$ keinen anderen gemeinschaftlichen Theiler haben können, aufser einen solchen, der in ihrer Differenz 2ω aufgeht, also eine Potenz von $1+\omega$ ist, übrigens m in keinem der beiden Factoren enthalten sein kann, da diese Zahl sonst in ± 1, dem Coëfficienten von ω aufgehen müfste: so bleibt nichts anderes übrig, als dafs m in das Product zweier complexen Factoren zerfällt, deren einer in $g^\lambda + \omega$, der andere in $g^\lambda - \omega$ enthalten ist und welche beide von complexen Einheiten verschieden sind. Nach dem Obigen ist es immer möglich, diese Zerfällung in der Form $m = (A + B\omega)(A - B\omega) = m_1 m_5$ und zwar nur in dieser Form zu bewerkstelligen, wenn $A + B\omega$ primär angenommen wird. Man kann hierbei ferner annehmen, dafs m_1 in $g^\lambda - \omega$ und m_5 in $g^\lambda + \omega$ aufgeht, dafs also $g^\lambda \equiv \omega \pmod{m_1}$ und $g^\lambda \equiv \omega^5 \pmod{m_5}$ ist. Wenn die Zerfällung $m = m_1 m_5$ in irgend einer Weise ausgeführt ist, so gehen alle Primzahlen, welche das Normalproduct m haben, und überhaupt alle in m aufgehenden Primzahlen aus m_1 oder aus m_5 durch Multiplication mit Einheiten hervor. Setzt man $f(\omega) = \varepsilon m_1$, wo ε eine Einheit ist, und soll $\mathfrak{N} f(\omega) = f(\omega) f(\omega^5) = m$ werden, so mufs, da auch schon $\mathfrak{N}(m_1) = m_1 m_5 = m$ ist, $\mathfrak{N}(\varepsilon) = 1$ werden; und dieser Bedingung genügen, wie oben gefunden, nur Einheiten von der Form $\varepsilon = \pm e^\nu$, wo $e = i + (1+i)\omega$; es ist also z. B. im_1 kein Werth von $f(\omega)$, noch weniger ωm_1. Es sind demnach alle Zahlen, deren Normalproduct $= m$ ist und die zu m_1 associirt sind, in der Form $\pm e^\nu m_1$ enthalten; eben so sind alle zu m_5 associirten Werthe, die der Bedingung $\mathfrak{N} f(\omega) = m$ genügen, in der Form $f(\omega) = \pm e^\nu m_5$ enthalten; unter allen diesen sind die *primären:* einerseits $f(\omega) = e^{2\nu} m_1$, andrerseits $f(\omega) = e^{2\nu} m_5$, wenn m_1 und m_5 selbst als primär vorausgesetzt werden.

Hierin ist bereits die elementare Theorie der Primzahlen vollständig enthalten; denn fügt man hinzu, dafs eine zusammengesetzte Zahl auch ein zusammengesetztes Normalproduct ergiebt und dafs jede im gewöhnlichen Sinne zusammengesetzte Zahl auch in dieser Theorie als zusammengesetzt angesehen werden mufs, ferner keine zusammengesetzte Zahl als Normalproduct einer binomen Primzahl dienen kann, so leuchtet ein, dafs, abgesehen von complexen Einheiten, welche als Factoren hinzutreten können und den Character

der Primzahl nicht verändern, von Primzahlen keine anderen existiren aufser den beiden folgenden Arten:

1) Die gewöhnlichen Primzahlen $m \equiv 3+2i \pmod 4$, deren Norm $p \equiv 5 \pmod 8$ ist, wie z. B. $-1 \pm 2i$ mit der Norm 5, $3 \pm 2i$ mit der Norm 13, u. s. w., welche in dieser Theorie ebenfalls als Primzahlen angesehen werden müssen. Es sind zugleich die einzigen gewöhnlichen Zahlen, welche hier als (monome) Primzahlen gelten, namentlich sind die gewöhnlichen *reellen* Primzahlen ohne Ausnahme als zusammengesetzt zu betrachten.

2) Die aus der Zerfällung der gewöhnlichen Primzahlen $m \equiv 1 \pmod 4$, deren Norm $p \equiv 1 \pmod 8$ ist, entspringenden. Diese sind die binomen Primzahlen, und jedes $m = m_1 m_5$ giebt zwei derselben m_1 und m_5, welche einander zugeordnet sind. Hierunter sind auch diejenigen begriffen, welche aus den Zerfällungen $a^2+2b^2 = (a+b(1+i)\omega)(a-b(1+i)\omega)$ und $a^2-2b^2 = (a+b(1-i)\omega)(a-b(1-i)\omega)$ reeller Primzahlen hervorgehen, welche abgesehen vom Zeichen $\pm$, resp. $\equiv 3$ und $\equiv 7 \pmod 8$ sind und deren Norm mit ihrem Quadrate zusammenfällt, also gewifs $\equiv 1 \pmod 8$ ist. Es würde indessen überflüssig sein, die Primzahlen dieser Art zu einer besonderen Gattung zu rechnen, im Gegentheil liegt es, wie schon weiter oben bemerkt, im Interesse der Einfachheit und Übersichtlichkeit für alle spätern Untersuchungen, sie gemeinschaftlich mit den übrigen hier unter 2) enthaltenen Primzahlen zu betrachten, und nur die monomen von den binomen Primzahlen zu unterscheiden.

Die Theorie der Potenzreste für die aus achten Wurzeln der Einheit zusammengesetzten Zahlen ist vollkommen analog derselben Theorie für die früheren complexen Zahlen. Man hat auch hier, wenn $f(\omega)$ eine ungerade Primzahl und p die Norm ihres Normalproductes bedeutet, analog dem *Fermat*schen Satze $F(\omega)^{p-1} \equiv 1 \pmod{f(\omega)}$, für jede nicht durch $f(\omega)$ theilbare ganze Zahl $F(\omega)$. Der Exponent $p-1$ ist in allen Fällen durch 8 theilbar, und deshalb zerfällt die Differenz $F(\omega)^{p-1}-1 = F(\omega)^{8\lambda}-1$ in 8 Factoren, deren jeder die Form $F(\omega)^\lambda - \omega^\mu$ hat, wo μ die Werthe 0, 1, 2 .... 7 erhält. Einer und nur einer dieser Factoren ist jedesmal durch $f(\omega)$ theilbar, und nach dem Werthe von μ, welcher die Congruenz $F(\omega)^\lambda \equiv \omega^\mu \pmod{f(\omega)}$ erfüllt, zerfallen für eine gegebene ungerade Primzahl $f(\omega)$ alle Werthe von $F(\omega)$ und für ein gegebenes $F(\omega)$ alle nicht in $F(\omega)$ aufgehenden ungeraden Primzahlen $f(\omega)$ in acht Classen, deren erste, für welche $F(\omega)^\lambda \equiv 1 \pmod{f(\omega)}$ ist, einerseits die achten Potenzreste $\pmod{f(\omega)}$, andrerseits alle ungeraden

Primzahlen $f(\omega)$ enthält, zu denen als Moduln eine gegebene Zahl $F(\omega)$ achter Potenzrest ist. Die vollkommen bestimmte Potenz von ω, welche in der Congruenz $F(\omega)^\lambda \equiv \omega^\mu \pmod{f(\omega)}$ für ein gegebenes $F(\omega)$ und $f(\omega)$ vorkommt, kann durch $\left(\frac{F(\omega)}{f(\omega)}\right)_8$, oder wenn keine Zweideutigkeit zu befürchten ist, blofs durch $\left(\frac{F(\omega)}{f(\omega)}\right)$ bezeichnet werden, und es kann die Bedeutung dieses Symbols nach Analogie der zuerst von *Jacobi**) für die *Legendre*schen Zeichen eingeführten fruchtbaren Verallgemeinerung auf den Fall eines zusammengesetzten Nenners ausgedehnt werden, indem man unter $\left(\frac{F(\omega)}{f(\omega)f'(\omega)\ldots.}\right)_8$ das Product $\left(\frac{F(\omega)}{f(\omega)}\right)_8\left(\frac{F(\omega)}{f'(\omega)}\right)_8 \ldots.$ versteht.

Dies ist ungefähr Alles, was aus der elementaren Theorie der hier betrachteten complexen Zahlen im Folgenden vorausgesetzt werden wird, und es scheint daher ein ausführlicheres Eingehen in dieselbe überflüssig. Es versteht sich von selbst, dafs beim jetzigen Standpuncte der Wissenschaft, und namentlich in Rücksicht auf *Dirichlet's* und *Kummer's* neueste zahlentheoretische Arbeiten, die bisherigen Entwicklungen dieses Paragraphen nicht als etwas Neues beansprucht werden können, sondern nur des Zusammenhanges wegen vorgetragen worden sind. Übrigens habe ich Grund zu vermuthen, dafs auch *Kummer*, von demselben Principe des Algorithmus der Aufsuchung des gröfsten gemeinschaftlichen Theilers ausgehend, nicht blofs die elementare Theorie der aus 8ten, sondern auch der aus 5ten Wurzeln der Einheit zusammengesetzten complexen Zahlen abgeleitet hat. Viel weiter möchte sich indessen das hier zum Grunde liegende Princip nicht erstrecken, da es wesentlich darauf beruht, dafs man das Product aller Werthe der complexen Zahl < 1 machen kann, während die Elemente derselben arithmetische Reihen mit der Differenz 1 durchlaufen, und es ist demgemäfs eine in den Pariser „Comptes rendus" vorkommende Notiz eines andern Verfassers zu berichtigen, in welcher diesem Princip die unbeschränkte und ausgedehnteste Anwendbarkeit auf complexe Zahlen aller möglichen Gattungen zugeschrieben wird.

§. 9.

Zurückkehrend zu der am Schlusse von (§. 7.) abgebrochenen Untersuchung, beschäftige ich mich jetzt mit einer näheren Erforschung der dort

*) Monatsberichte der Berl. Akademie vom Oct. 1837.

vorkommenden complexen ganzen Zahlen $u-2i\omega$ und $u+2i\omega$. Man zerlege, was für eine gewöhnliche complexe Primzahl $m \equiv 1 \pmod{2+2i}$, deren Norm $p \equiv 1 \pmod 8$, nach dem Obigen (§. 8.) immer möglich ist, m in seine beiden zugeordneten Primfactoren $m = m_1 m_5$ und setze fest, dafs diese beiden einander zugeordneten Factoren in solcher Reihenfolge genommen seien, dafs die Congruenzen

$$(15.) \qquad g^\lambda \equiv \omega \pmod{m_1} \quad \text{und} \quad g^\lambda \equiv \omega^5 \equiv -\omega \pmod{m_5}$$

erfüllt werden. Durch diese Congruenzen sind, nach Annahme einer gewissen primitiven Congruenzwurzel g, die beiden Factoren m_1 und m_5, bis auf hinzutretende Einheiten von der Form $\pm e^\nu$, vollkommen bestimmt, und eine Vertauschung von m_1 mit m_5 würde die Annahme eines neuen Werthes von g bedingen. Ferner werden m_1 und m_5 als primär vorausgesetzt und dürfen dann, wenn man nicht aus dieser Bedingung heraustreten will, nur noch mit $e^{2\nu}$ resp. $e^{-2\nu}$ multiplicirt werden. Verbindet man jetzt die Congruenzen (11.) in (§. 7.) mit denen in (15.), so erhellet, dafs $u-2i\omega$ durch m_5, aber nicht durch m_1, und $u+2i\omega$ durch m_1, aber nicht durch m_5 theilbar ist. Man kann demnach $u-2i\omega = hm_5^\alpha$ und $u+2i\omega = h'm_1^\alpha$ setzen, wo h und h' zugeordnete Zahlen sind, die mit m keinen Theiler weiter gemein haben. Das Product $(u-2i\omega)(u+2i\omega)$ nimmt demnach die Form $hh'm_5^\alpha m_1^\alpha = hh'm^\alpha$ an, und da dasselbe Product nach (§. 7.) Gleichung (10.) auf die Form mv^2 gebracht werden kann *), so mufs $hh'm^{\alpha-1} = v^2$ ein vollständiges Quadrat und $\alpha-1$ mufs daher eine gerade Zahl sein, weil nach der Voraussetzung hh' zu m relative Primzahl ist. Hieraus ergiebt sich, dafs $u-2i\omega$ und $u+2i\omega$ den Primtheiler m_5, resp. m_1, in einer ungeraden Potenz enthalten, so dafs die zu untersuchenden complexen ganzen Zahlen in folgender Form erscheinen: $u-2i\omega = hm_5^{2\beta+1}$, $u+2i\omega = h'm_1^{2\beta+1}$; wo h und h', wie bemerkt, keinen Factor, weder m_1 noch m_5, mit m gemein haben.

Um jetzt zu untersuchen, in welcher Weise dieselben Zahlen die in ihnen vorkommenden, von m_1 und m_5 *verschiedenen* ungeraden Primtheiler enthalten (wenigstens so weit es hier erforderlich ist), bediene ich mich der folgenden Reductionsmethode, welche sich auf die Sätze in (§. 4.) stützt und für die ganze Theorie der Lemniscatentheilung bemerkenswerth scheint. Es sei $F(k;\omega)$ irgend eine ganze ganzzahlige Function der Gröfsen (1.) und

*) So dafs beiläufig u und v eine Lösung der unbestimmten Gleichung $u^2 - mv^2 = -4i$ ausmachen.

von ω, welche der Bedingung $F(gk) = \omega F(k)$, und zwar für beide Werthe von ω aus $\omega^2 = i$ genügt. Jede solche Function ist eine cyclische Verbindung 8ter Ordnung und ihre 8te Potenz $F(k)^8 =$ einer ganzen Zahl aus 8ten Wurzeln der Einheit. Nach (§. 4.) ist, wenn n irgend eine von m verschiedene gewöhnliche primäre Primzahl und $N(n) = q$ ihre Norm bedeutet:

$$(16.) \quad \begin{cases} F(k;\omega)^q &= F(nk;\omega^q) + nT(k;\omega), \\ F(k;\omega)^{q^2} &= F(n^2k;\omega^{q^2}) + nT(k;\omega). \end{cases}$$

Wenn $q \equiv 1 \pmod 8$, so geht ω^q in ω, also $F(nk;\omega^q)$ in $F(nk;\omega) = F(nk)$ über: wenn dagegen $q \equiv 5 \pmod 8$, also erst $q^2 \equiv 1 \pmod 8$ ist, so kann man wenigstens in der zweiten Gleichung $F(n^2k)$ statt $F(n^2k;\omega^{q^2})$ schreiben; und da überdies $F(n^2k)$ und $F(nk)$ nach der Voraussetzung sich von $F(k)$ nur durch eine Potenz von ω unterscheiden, so läfst sich in beiden Fällen eine Gleichung finden, deren erster Term rechts genau dieselbe Gröfse $F(k)$ enthält, welche links zur Potenz q resp. q^2 erhoben ist. Um die für beide Fälle $n \equiv 1$ und $n \equiv 3 + 2i \pmod 4$ sich ergebenden Formeln bequem vereinigen zu können, lasse man die bisherige Bedeutung von n fallen und bezeichne vielmehr durch n das Normalproduct einer primären Primzahl h aus 8ten Wurzeln der Einheit; n ist dann, nach der Untersuchung über die complexen Primzahlen im vorigen Paragraphen, entweder selbst eine gewöhnliche Primzahl, welche $\equiv 1 \pmod 4$, oder das Quadrat einer solchen, welche $\equiv 3 + 2i \pmod 4$ ist, je nachdem h binom oder monom angenommen wird. Im ersten Falle ist h als Theiler in n enthalten und $n = hh'$; im zweiten fällt h selbst mit der früheren Bedeutung von n zusammen. Hiernach sieht man, dafs, h' mag binom oder monom angenommen werden, stets eine Gleichung von der Form

$$(17.) \quad F(k;\omega)^{N(n)} = \omega^\nu F(k;\omega) + hT(k;\omega) \text{ oder kürzer } F^q = \omega^\nu F + hT$$

Statt findet, in welcher $n = \mathfrak{N}(h)$, $q = N(n)$ ist; ω^ν entspringt aus $F(nk) = \omega^\nu F(k)$, und es bedeutet also ν den der Congruenz $n \equiv g^\nu \pmod m$ oder auch $n \equiv g^\nu \pmod{m_1}$ genügenden Exponenten, und da hieraus mit Zuziehung von (15.) $n^\lambda \equiv g^{\lambda\nu} \equiv \omega^\nu \pmod{m_1}$ folgt, so kann ω^ν durch $\left(\frac{n}{m_1}\right)_8$ ersetzt werden. Die Gleichung (17.) geht für einen binomen Werth von h aus der ersten in (16.) hervor, wenn dort hh' statt n und darauf $T(k)$ statt $h'T(k)$ geschrieben wird, und fällt für einen monomen Werth von h mit der zweiten in (16.) zusammen; im letzteren Falle wird aus der ersten in (16.), weil dann $N(h) \equiv 5 \pmod 8$ ist:

$$(18.)\qquad F(k;\omega)^{N(h)} = \omega^{5\varrho}F(k;\omega^5)+hT(k;\omega) = \omega^{5\varrho}F'+hT,$$

welches nur für eine monome primäre Primzahl h gilt; ϱ genügt der Congruenz $h\equiv g^\varrho \pmod{m}$, also auch der Congruenz $h\equiv g^\varrho \pmod{m_1}$, und da hieraus $h^\lambda \equiv g^{\lambda\varrho}\equiv\omega^\varrho \pmod{m_1}$ folgt, so kann $\omega^{5\varrho}$ durch $\left(\frac{h}{m_1}\right)_8^5$ ersetzt werden. Die Gleichung (17.), welche später bei den arithmetischen Anwendungen in der Form

$$(17'.)\qquad F^q = \left(\frac{n}{m_1}\right).F+hT$$

zugleich mit (18.) in der Form

$$(18'.)\qquad F^{N(h)} = \left(\frac{h}{m_1}\right)^5.F'+hT$$

eine Rolle spielen wird, benutze ich für den vorliegenden Zweck, um umgekehrt nicht die $q$te Potenz F^q durch die erste F, sondern die erste Potenz F durch die übrigen Theile der Gleichung auszudrücken. Ich gebe ihr deshalb die nachstehende Form:

$$(19.)\qquad F(k) = \omega^{-\nu}F(k)^q - h.\omega^{-\nu}T(k);$$

auch wende ich sie im Augenblick nur auf den Fall an, wenn h Primtheiler der ganzen Zahl $F(k)^8$ ist. Schreibt man die Potenz $F(k)^q$ so: $F(k)^8.F(k)^{q-8}$, so wird in diesem Falle, da $q>8$, also $q-8$ ein positiver Exponent ist, die ganze Seite rechts das *hfache* einer ganzzahligen Function der Wurzeln der Gleichungen $W=0$ und $\omega^2=i$; nämlich wenn $F(k)^8=hl$ ist: $F=h.\{\omega^{-\nu}lF^{q-8}-\omega^{-\nu}T\}$. Dies gilt für alle $p-1$ Werthe von k und für beide Werthe von ω. Wird demnach $F(k)=hF_1(k)$ gesetzt, wo $F_1(k)$ die in der Parenthese $\{\ \}$ stehende Function bedeutet, so hat man ebenfalls $F(gk)=hF_1(gk)$, indem h zugleich mit $F(k)^8$ von k unabhängig ist; und aus der Voraussetzung $F(gk)=\omega F(k)$ ergiebt sich dann, dafs auch $F_1(k)$ der analogen Relation $F_1(gk)=\omega F_1(k)$ genügt, also, wie $F(k)$, eine cyclische Function 8ter Ordnung vorstellt. Wird ω mit ω^5 vertauscht, so geht h in die ihr zugeordnete Zahl h' über, die übrigens, wenn h monom ist, mit ihr zusammenfällt, und man erhält

$$F(k;\omega^5) = h'F_1(k;\omega^5),\quad F_1(gk;\omega^5) = \omega^5F_1(k;\omega^5).$$

„Wenn also $F(k)$ irgend eine *ganze ganzzahlige* Function der Wur„zeln der Gleichungen $W=0$ und $\omega^2=i$ bezeichnet, die der Relation $F(gk)$ „$=\omega F(k)$ genügt, und h bedeutet einen der von m_1, m_5 und $1+\omega$ ver„schiedenen Primtheiler der ganzen Zahl $F(k)^8$, so läfst sich die erste Potenz „$F(k)$ auf die Form $hF_1(k)$ bringen, wo $F_1(k)$ alle von $F(k)$ vorausgesetzten

„Eigenschaften ebenfalls besitzt. Es ist demnach $F_1(k)^8$ wieder einer ganzen „Zahl gleich und $F(k)^8$ nicht blofs durch h, sondern durch h^8 theilbar."

Statt (19.) hätte man bei dieser Reduction von $F(k)$ auch eine allgemeinere Gleichung zum Grunde legen können, in der q durch eine beliebige Potenz von q ersetzt ist und die sich eben so leicht aus den Principien von (§. 4.) ergiebt. Eine wiederholte Anwendung desselben Verfahrens, durch welches der Primfactor h herausgezogen und $F(k)$ auf die neue cyclische Function $F_1(k)$ reducirt worden ist, dient zur successiven Absonderung sämmtlicher in $F(k)^8$ aufgehenden ungeraden Primfactoren, aufser m_1 und m_5, und man kann auf diese Weise zuletzt $F(k)$ auf eine neue cyclische Function reduciren, in deren achter Potenz nur noch $1+\omega$, m_1 und m_5, und keine anderen Primfactoren mehr aufgehen. Denn ist h_1 irgend ein Primfactor der ganzen Zahl $F_1(k)^8$ (aufser m_1, m_5 und $1+\omega$, wie immer stillschweigend vorausgesetzt wird), von dem es übrigens gleichgültig ist, ob er mit h übereinstimmt oder nicht, so läfst sich nach dem Obigen wiederum $F_1(k)$ auf die Form $h_1F_2(k)$ bringen, wo auf's Neue $F_2(k)$ allen Bedingungen einer (ganzen ganzzahligen) cyclischen Function 8ter Ordnung genügt, und man hat nun schon $F(k)=hh_1F_2(k)$. Ist ferner h_2 ein Primfactor der ganzen Zahl $F_2(k)^8$, so erhält man durch das wiederholte Verfahren $F_2(k)=h_2F_3(k)$; woraus $F(k)=hh_1h_2F_3(k)$ folgt, u. s. w. Da jede ganze Zahl, also auch der Werth von $F(k)^8$, wenn man von den complexen Einheiten absieht, nur eine *endliche* Anzahl von gleichen oder ungleichen Primfactoren enthalten kann, so kommt man in der Reihe der cyclischen Functionen

$$F(k),\ F_1(k),\ F_2(k),\ F_3(k),\ \ldots.$$

nothwendig zuletzt auf eine solche, deren 8te Potenz keine von m_1 und m_5 verschiedenen ungeraden Primtheiler mehr enthält. Mit dieser letzten cyclischen Function, welche ich durch $G(k)$ bezeichnen will, findet das Verfahren sein Ende. Man hat dann $F(k)=hh_1h_2\ldots.\ G(k)=f(\omega).G(k)$, $F(k)^8=f(\omega)^8G(k)^8$. $G(k)$ ist eine der Bedingung $G(gk)=\omega G(k)$ genügende ganze ganzzahlige Function der oft erwähnten Gröfsen, und zwar, was das Wichtigste ist, von der Art, dafs $G(k)^8$ eine durch *keinen* ungeraden Primfactor aufser m_1 und m_5 theilbare ganze Zahl wird, die also nur Potenzen von $1+\omega$, m_1 und m_5 und aufserdem nur noch complexe Einheiten enthalten kann. Eine Ausnahme macht nur der einzige Fall, wenn $F(k)^8=0$, also auch $F(k)=0$ sein sollte; denn da Null durch jede beliebige ganze Zahl, also, wenn man sich so ausdrücken will, durch *unendlich viele* Primzahlen theilbar ist, so würde man

in diesem Falle bei dem Reductions-Verfahren, welches dann ohnedies ganz illusorisch wäre, nie zum Schlusse kommen, und jede folgende cyclische Function hätte, wie die erste, den Werth Null. Man sieht hieraus, wie wichtig es ist, sich nicht allein jedesmal, ehe man das Verfahren beginnt, vom Nichtstattfinden dieses Ausnahmefalles zu überzeugen, sondern auch, wie schon früher bemerkt, sich überhaupt der Existenz zunächst nur einer von Null verschiedenen cyclischen Verbindung achter Ordnung zu versichern, um sich derselben als Ausgangspunct für und zur Vergleichung mit allen andern Functionen derselben Art zu bedienen. Wenn *eine* solche von Null verschiedene Verbindung existirt (und wir haben uns davon durch die Function $S(k)$ (6.) überzeugt), so existirt auch stets eine, deren achte Potenz einen solchen ganzen Werth erhält, welcher zu einer, nicht durch m_1 oder m_5 theilbaren, sonst beliebig gegebenen ungeraden Zahl relative Primzahl wird.

Als Corollar zu dieser fortgesetzten Reductions-Methode ergiebt sich, dafs die 8te Potenz jeder cyclischen Function 8ter Ordnung (und ich verstehe darunter immer eine der Bedingung $F(gk) = \omega F(k)$ genügende ganze ganzzahlige Function) jede von m_1 und m_5 wesentlich, d. h. nicht blofs durch complexe Einheiten verschiedene ungerade Primzahl nur in einer solchen Potenz enthalten kann, deren Exponent durch 8 theilbar ist, und dafs demnach, wenn $F(k)$ in der Form $F(k) = \sqrt[8]{(F(k)^8)}$ geschrieben wird, alle diese Primzahlen aus dem Wurzelzeichen herausgezogen werden können. Wir werden bald sehen, dafs das Gleiche auch von der Primzahl $1+\omega$ und von den complexen Einheiten gilt und dafs demnach unter dem im Werthe der cyclischen Function vorkommenden nothwendigen Wurzelzeichen nur Potenzen von m_1 und m_5 enthalten sind.

Wendet man diese Reduction im einzelnen auf unsere Functionen $S(k)$, mit ihrer zugeordneten $S'(k)$ an, aus denen die Zahlen $u \mp 2i\omega$ entsprungen sind, so ergiebt sich, in Verbindung mit dem Früheren, Folgendes:

1) $S(k)$ läfst sich auf die Form $S(k) = f(\omega) G(k)$ und zugleich $S'(k)$ auf die Form $S'(k) = f(\omega^5) G'(k)$ bringen, wo $f(\omega)$, $f(\omega^5)$ zwei zugeordnete *ganze* complexe Zahlen sind und $G(k)$ eine neue cyclische Function 8ter Ordnung von gröfserer Einfachheit als $S(k)$ ist, insofern ihre 8te Potenz nur die drei Primfactoren $1+\omega$, m_1 und m_5 enthält; $G'(k)$ geht aus $G(k)$, so wie $S'(k)$ aus $S(k)$ durch Vertauschung von ω^5 mit ω hervor.

2) Die Verbindungen $S^2P^3 = m(u - 2i\omega)$, $S'^2P^3 = m(u + 2i\omega)$ und $SS'P = mv$ werden resp. zu $f(\omega)^2G^2P^3$, $f(\omega^5)^2G'^2P^3$, $f(\omega)f(\omega^5)GG'P$; und

zwar sind die neuen Verbindungen G^2P^3, G'^2P^3, $GG'P$ ebenfalls ganze Zahlen, welche keine andern als die drei obigen Primfactoren enthalten. Letzteres ergiebt sich zunächst für die achten Potenzen dieser Zahlen aus der über G^8 und G'^8 in dieser Hinsicht gemachten Voraussetzung und aus der Gleichung $P^4 = m$; sodann für die Zahlen selbst, welche keine anderen Primfactoren haben können, als solche, die auch in ihren achten Potenzen aufgehen.

3) Die ganzen Zahlen $u \mp 2i\omega$ lassen sich in solcher Weise durch ein vollständiges Quadrat dividiren, dafs der Quotient nur durch $1+\omega$, m_1 oder m_5 theilbar bleibt; und da sich am Anfange dieses Paragraphen bereits zeigte, dafs $u-2i\omega$ nur m_5 und nicht m_1, $u+2i\omega$ nur m_1 und nicht m_5, und zwar beide den in ihnen vorkommenden Primfactor in einer ***ungeraden*** Potenz enthalten, so kann vor der Hand

(20.) $$u-2i\omega = h^2.\varepsilon.(1+\omega)^\alpha.m_5, \qquad u+2i\omega = h'^2.\varepsilon'.(1-\omega)^\alpha.m_1$$

gesetzt werden. Die etwa noch hinzutretende Potenz von m_5, resp. m_1, mit geradem Exponenten, ist als bereits in den Quadraten h^2 resp. h'^2 enthalten anzunehmen. Da diese zugeordneten quadratischen Factoren h und h'^2 keiner Beschränkung unterworfen sind, so kann ferner α der Exponent von $1+\omega$ (resp. $1-\omega$) auf einen der beiden Werthe 0 oder 1 reducirt werden; denn setzt man $\alpha = 2\beta+\alpha'$, wo $0 \leqq \alpha' < 2$, so kann man die gerade Potenz $(1+\omega)^{2\beta}$ mit h^2 zu einem einzigen quadratischen Factor vereinigen. Weiter unten wird sich zeigen, dafs $\alpha = 2$ ist, also auf 0 reducirt werden kann. Aus ähnlichem Grunde ist es erlaubt, die complexe Einheit ε nur unter den folgenden vier Einheiten

$$1, \quad \omega, \quad e, \quad \omega e,$$

und ε' dann unter den entsprechenden zugeordneten

$$1, \quad \omega^5, \quad e^{-1}, \quad \omega^5 e^{-1}$$

anzunehmen, da jede andere Einheit sich von diesen nur durch einen quadratischen Factor unterscheidet, welcher ebenfalls mit h^2 resp. h'^2 zusammengezogen werden kann. Der Werth von v wird jetzt durch die Gleichung $v^2 = (hh')^2\varepsilon\varepsilon'(1-i)^\alpha$ bestimmt.

4) Nach Annahme der obigen Formen in (20.), und wenn man m_1m_5 statt m schreibt, wird also

(21.) $$S^2P^3 = h^2.\varepsilon.(1+\omega)^\alpha.m_1m_5^2, \qquad S'^2P^3 = h'^2.\varepsilon'.(1-\omega)^\alpha.m_1^2m_5.$$

Wenn man zur vierten Potenz erhebt und mit $P^{12} = m^3 = m_1^3m_5^3$ dividirt, so erhält man

(22.) $$S^8 = h^8.\varepsilon^4.(1+\omega)^{4\alpha}.m_1m_5^5, \qquad S'^8 = h'^8.\varepsilon'^4.(1-\omega)^{4\alpha}.m_1^5m_5.$$

§. 10.

Die wichtigste Untersuchung besteht jetzt noch darin, den Exponenten α von $1+\omega$ und die complexen Einheiten ε, ε' zu ermitteln, welche wir wenigstens schon solchen Beschränkungen unterworfen haben, dafs nur noch zwischen einer geringen Anzahl Fälle die Wahl sein kann. Ferner sind noch einige andere hier vorkommende Unbestimmtheiten zu heben; z. B. es ist der zweifelhafte Werth von v in der Gröfse $SS'P = mv$ zu bestimmen, von der nur das Quadrat und nicht die erste Potenz aus den etwa bekannten Werthen von S^2P^3 und S'^2P^3 ohne Zweideutigkeit abgeleitet werden kann.

Zur Bestimmung einer complexen Einheit und eines zweifelhaften Vorzeichens ergiebt sich hier kein anderer Weg, als der durch eine Congruenz in Bezug auf eine Potenz von $1+\omega$, als Modul. Es wird also, um die noch obschwebenden Fragen zu erledigen, zu untersuchen sein: 1) Welches die höchste Potenz von $1+\omega$ sei, die in den für S^2P^3, S'^2P^3, $SS'P$ sich ergebenden ganzen Zahlen aufgeht. 2) Nachdem man die letzteren durch jene höchste Potenz von $1+\omega$ dividirt hat, welches der Rest sei, den die Quotienten der Division in Bezug auf eine neue Potenz von $1+\omega$ ergeben.

Um die so eben kurz bezeichnete Untersuchung durchzuführen, leite man aus dem Additionstheorem für die lemniscatischen Functionen, indem man das zweite Argument dem ersten oder dem $i$fachen des ersten gleich setzt, folgende Multiplicationsformeln ab:

$$\varphi(2t) = \frac{2x\sqrt{(1-x^4)}}{1+x^4}, \qquad \varphi((1+i)t) = \frac{(1+i)x}{\sqrt{(1-x^4)}},$$

welche sich auf die Multiplicatoren 2 und $1+i$ beziehen und in denen wie immer $x = \varphi(t)$ gesetzt ist. Multiplicirt man beide Formeln mit einander, schafft die Nenner weg und setzt der Kürze wegen $1+i = \eta$, $\varphi(2t) = x_2$, $\varphi(\eta t) = x_\eta$, so erhält man

$$(23.) \qquad x_2 x_\eta (1+x^4) = (2+2i).x^2; \qquad \eta = 1+i.$$

Bedeutet jetzt x eine Wurzel der Gleichung $W = 0$, so sind x_2 und x_η ebenfalls Wurzeln dieser Gleichung; multiplicirt man links und rechts mit dem Producte der aufser x_2 und x_η noch fehlenden $p-3$ Wurzeln, so erhält man links $1+x^4$ multiplicirt mit dem Producte aller Wurzeln, also $m(1+x^4)$, und rechts das $(2+2i)$fache eines Products aus theils gleichen, theils ungleichen Wurzeln, jedenfalls also das $(2+2i)$fache einer ganzen ganzzahligen Function der Wurzeln. Schreibt man die Zahl m, welche $\equiv 1 \pmod{2+2i}$ ist, in der

Form $1+(2+2i)m'$, und bringt den Theil $(2+2i)m'(1+x^4)$ auf die rechte Seite hinüber, „so erhält man $1+x^4$ selbst in der Form $(2+2i)T$ dargestellt." Es wird also, wenn man statt x seinen Werth $\varphi\left(\frac{rC}{m}\right)$ oder $\psi(r)$ setzt, „$\psi(r)^4+1 \equiv$ dem $(2+2i)$fachen einer ganzen ganzzahligen Function der „Gröfsen $\psi(k)$, $\psi(gk)$, ..., während r irgend einen der Werthe k, gk, ... „vorstellen kann." — Für die nachfolgenden Untersuchungen scheint es zweckmäfsig (und es hätte vielleicht schon früher geschehen können), das Zeichen $\equiv$ in einer solchen Bedeutung zu nehmen, dafs der Modul statt mit einer ganzen Zahl, auch mit einer ganzen ganzzahligen Function der Wurzeln der Gleichung $W=0$ multiplicirt sein kann, und $L \equiv L' \pmod{\vartheta}$ zu schreiben, wenn die Differenz $L-L'$ zweier *ganzen ganzzahligen* Functionen L und L' dieser Wurzeln dem ϑfachen einer andern ebenfalls *ganzen ganzzahligen* Function derselben gleich wird. Hiernach wird das oben gefundene Resultat so ausgedrückt:

$$\psi(r)^4 \equiv -1 \pmod{2+2i}. \tag{24.}$$

Eine Congruenz dieser Art ist nicht mit einer gewöhnlichen zu verwechseln, indem das Zeichen $\equiv$ dabei nur der Kürze wegen und in Ermangelung einer eigenthümlichen Bezeichnung des Begriffs angewandt wird. Nur in dem einzigen Falle, wenn sich nachweisen läfst, dafs L und L' *ganzen* Zahlen gleich sind, ist man nach (§. 6.) berechtigt, eine solche Congruenz wie eine gewöhnliche anzusehen und zu behandeln; was wir denn auch in der Folge thun werden. Übrigens versteht es sich, dafs man in Hinsicht auf Addition, Subtraction, Multiplication (aber *nicht* Division) mit dieser Art von Congruenzen eben wie mit gewöhnlichen operiren kann.

Auf diese Betrachtungen, namentlich auf die Congruenz (24.) gestützt, läfst sich die Untersuchung in folgende Puncte zusammenfassen.

1) Aus $S \equiv Q - iR\omega$ folgt, wenn man beim Quadriren das doppelte Product vernachlässigt, $S^2 \equiv Q^2 - iR^2 \pmod 2$ und hieraus $S^4 \equiv (Q^2-iR^2)^2 \pmod 4$, d. h. $S^4 \equiv Q^4 - R^4 - 2iQ^2R^2 \pmod 4$, also auch $\pmod{2+2i}$. Nun ist $Q^4 - R^4 \equiv 0 \pmod{2+2i}$; denn Q^4 und R^4 sind Producte aus lauter Gröfsen von der Form $\psi(r)^4$, deren Anzahl jedesmal λ beträgt. Wendet man also (24.) auf jede der in Q und R enthaltenen Wurzeln an, so ergiebt sich, *multiplicando*, $Q^4 \equiv R^4 \equiv (-1)^\lambda \pmod{2+2i}$. Die Congruenz für $S^4 \pmod{2+2i}$ wird, da man hiernach aus derselben $Q^4 - R^4$ weglassen kann und ferner auch,

da für diesen Modul $+2$ statt $-2i$ geschrieben werden darf, $S^4 \equiv 2Q^2R^2 = 2P^2 \pmod{2+2i}$. Hieraus folgt endlich durch abermaliges Quadriren $S^8 \equiv 4P^4 = 4m \pmod{4+4i}$. Die letztere Congruenz $S^8 \equiv 4m \pmod{4+4i}$ enthält nur ganze Zahlen und gilt daher auch im gewöhnlichen Sinne. Als erstes Resultat ergiebt sich aus derselben, wenn man sie vorläufig nur in Bezug auf den Modul 4 betrachtet, der durch $(1+\omega)^8$ ersetzt werden kann, „dafs „S^8 durch $(1+\omega)^8$, oder 4 theilbar ist." Dafs S^8 auch durch keine höhere Potenz von $1+\omega$, als $(1+\omega)^8$, theilbar sein kann, sieht man aus derselben Congruenz, wenn man sie (was hiernach erlaubt ist) folgendermafsen schreibt: $\frac{1}{4}S^8 \equiv m \pmod{1+i}$; denn da m eine ungerade Zahl ist, so ist $\frac{1}{4}S^8$ ebenfalls ungerade und durch keine weitere Potenz von $1+\omega$ theilbar. Dieselben Betrachtungen lassen sich auf S'^8 anwenden.

2) Die vierte Potenz von S^2P^3 ist $S^8P^{12} = m^3S^8$, und da m^3 ungerade ist, so ist diese Gröfse, so wie S^8, ebenfalls durch $(1+\omega)^8$ und durch keine höhere Potenz von $1+\omega$ theilbar; S^2P^3 selbst, oder $m(u-2i\omega)$, ist demnach genau durch $(1+\omega)^2$ oder $1+i$ theilbar, und aus ähnlichem Grunde ist $S'^2P^3 = m(u+2i\omega)$ genau durch $(1+\omega)^2$ oder $1+i$ theilbar.

3) Die beiden ganzen Zahlen $u \mp 2i\omega$ sind demnach durch $1+i$ oder $(1+\omega)^2$ theilbar und der Quotient der Division ist eine ungerade Zahl. Da der Coëfficient von ω in diesen beiden Zahlen durch 2, also durch $(1+i)^2$ theilbar ist, so gilt Obiges auch von u, und es ist $u \equiv 1+i \pmod{2}$, $u \mp 2i\omega \equiv 1+i \pmod{2}$. Aus $u^2+4i = mv^2$ ergiebt sich dann, dafs v^2 durch 2, also v durch $1+i$ und durch keine höhere Potenz von $1+i$ theilbar ist. Setzt man $u = (1+i)u'$, $v = (1+i)v'$, so wird $u^2 = 2iu'^2$, $v^2 = 2iv'^2$, $u'^2 - mv'^2 = -2$; wo u' und v' ungerade Zahlen sind. Das letztere ergiebt sich auch aus der Gleichung $u'^2 - mv'^2 = -2$ selbst und ohne die früheren Betrachtungen: denn wäre u' gerade, so wäre es auch v', und umgekehrt. Gesetzt also, es wäre $u' = (1+i)u''$ und $v' = (1+i)v''$, so erhielte man, nach Division mit $(1+i)^2 = 2i$, $u''^2 - mv''^2 = i$; da aber das Quadrat jeder ungeraden (gewöhnlichen) Zahl $\equiv 1 \pmod{2}$ und das jeder durch $1+i$ theilbaren $\equiv 0 \pmod{2}$ ist, so könnte die linke Seite der Gleichung nur entweder $\equiv 0$, oder $\equiv 1-m$, oder $\equiv 1$, oder endlich $\equiv -m \pmod{2}$ werden, und keiner dieser Fälle giebt ein Resultat, welches $\equiv i \pmod{2}$ wäre.

4) Setzt man $u \mp 2i\omega = (1-i)(\alpha \mp \beta\omega)$, so ist $(1-i)\beta = 2i$, $\beta = i(1+i)$, also auch $\beta \equiv 1+i \pmod{2}$, oder allgemeiner $\beta \equiv i^\mu(1+i) \pmod{2}$; α ist ungerade und daher entweder $\equiv \pm 1$, oder $\equiv \pm i \pmod{2}$;

demnach ist $\alpha \mp \beta\omega$ entweder $\equiv i + (1+i)\omega$ (mod. 2), wenn $\alpha \equiv i$ (mod. 2), oder $\alpha \mp \beta\omega \equiv i(i+(1+i)\omega)$, wenn $\alpha \equiv 1$ (mod. 2), d. h. $\alpha \mp \beta\omega \equiv e$, oder $\equiv ie$ (mod. 2). Hätte man, statt $u \mp 2\omega$ durch $1-i$ zu dividiren und den Quotienten $= \alpha \mp \beta\omega$ zu setzen, dieselben Zahlen vielmehr durch $(1+\omega)^2$ dividirt und $u \mp 2\omega = (1+\omega)^2(\gamma \mp \delta\omega)$ gesetzt, so müfste sich $\gamma \mp \delta\omega \equiv 1$ oder $\equiv i$ (mod. 2) ergeben; denn unter dieser Voraussetzung ist $\alpha \mp \beta\omega = e(\gamma \mp \delta\omega)$, weil e selbst sich, wie schon in der Gleichung (13.) angemerkt ist, $= \frac{(1+\omega)^2}{1-i}$ findet. Schreibt man die Gleichung $\alpha \mp \beta\omega = e(\gamma \mp \delta\omega)$ als Congruenz (mod. 2), so liefert sie das Behauptete, da die linke Seite nach dem Obigen nur $\equiv e$ oder $\equiv ie$ (mod. 2) sein kann. Da $i = \omega^2$ ein vollständiges Quadrat ist, so läfst sich sagen, dafs $u \mp 2i\omega$ sich mit Hülfe einer quadratischen Factors, nämlich entweder $(1+\omega)^2$, oder $[\omega(1+\omega)]^2 = (i+\omega)^2$, auf eine Zahl reduciren läfst, die $\equiv 1$ (mod. 2) ist; und da ± 1 ebenfalls ein vollständiges Quadrat ist, so können sich $u \mp 2i\omega$ von *primären* Zahlen (vergl. §. 8.) nur durch einen quadratischen Factoren unterscheiden. ***Hierin ist die Bestimmung der am Schlusse von (§. 9.) mit ε bezeichneten complexen Einheit enthalten:*** denn da m_5 selbst als primär vorausgesetzt ist und für den Werth von ε nur unter den vier Einheiten 1, ω, e, ωe die Wahl bleibt, so mufs nothwendig $\varepsilon = 1$ sein; dasselbe gilt von ε'. Es bleibt nun kein Zweifel mehr, dafs $u \mp 2i\omega$ die Form

$$(20'.) \qquad u - 2i\omega = h^2(1+\omega)^2 m_5, \quad u + 2i\omega = h'^2(1-\omega)^2 m_1$$

annehmen müssen; wo h, h' zwei einander zugeordnete ***ungerade*** Zahlen bedeuten.

5) Setzt man diese Werthe und verfährt wie am Schlusse des vorigen Paragraphen, so ergiebt sich, als Ergänzung der dortigen Formeln:

$$(21'.) \qquad S^2P^3 = h^2(1+\omega)^2 m_1 m_5^2, \qquad S'^2P^3 = h'^2(1-\omega)^2 m_1^2 m^5,$$

$$(22'.) \qquad S^8 = h^8(1+\omega)^8 m_1 m_5^5, \qquad S'^8 = h'^8(1-\omega)^8 m_1^5 m_5,$$

$$S = h(1+\omega)\sqrt[8]{(m_1 m_5^5)}, \qquad S' = h'(1-\omega)\sqrt[8]{(m_1^5 m_5)},$$

wobei ins Gedächtnifs zurückzurufen ist, dafs m_1, m_5 zwei primäre (14.), einander zugeordnete und den Bedingungen (15.) genügende Primzahlen bedeuten, deren Normalproduct $m_1 m_5 = m$ ist, und dafs, wenn unter den, allen diesen Bedingungen zugleich genügenden, immer noch unendlich vielen Systemen m_1, m_5 zwei verschiedene genommen werden, dies nichts anderes, als eine Veränderung des Werths von h und h' in den obigen Formeln zur Folge hahen

kann; wodurch die wesentlichen Irrationalitäten $\sqrt[8]{(m_1 m_5^5)}$, $\sqrt[8]{(m_1^5 m_5)}$ nicht betroffen werden. Sollte man aber m_1 und m_5 nicht primär angenommen haben, so müfste zu den Formeln in (21′.) rechts im Allgemeinen noch eine der complexen Einheiten ω, e oder ωe hinzutreten, und nur unter der gemachten Voraussetzung haben die Formeln die obige (gröfste) Einfachheit; wenigstens besteht die einzige Freiheit, die man sich, ohne diese Einfachheit zu stören, noch erlauben könnte, darin, m_1, m_5 mit ± 1 oder $\pm i$ zu multipliciren, da sich diese Factoren als Quadrate schreiben und mit h^2, h'^2 vereinigen liefsen. Dafs auch diese Unbestimmtheit in der Definition der primären Zahlen bereits aufgehoben ist (was für (21′.) allein nicht unbedingt nothwendig wäre): davon wird sich der Vortheil in der folgenden Nr. zeigen.

(Der Schlufs folgt im nächsten Hefte.)

Crelle Journal d. Math. Bd. 39. Heft 3.

Fac-simile einer Handschrift von J. A. Euler

à St: Petersbourg le 6 Juillet 1789 = VI nst.
reçu le 1 Aout

Monsieur mon très chèr et très honoré Oncle.

En remettant d'un jour de poste à l'autre le plaisir de Vous écrire, je n'ai pas cru devoir debuter enfin par un evenement des plus affligeans qui me soit arrivés dans ma vie. C'est la mort subite de mon cher gendre Bernoulli, que nous pleurons, et que nous pleurerons encore long temps. Ce fut mardi 3 de ce mois entre 5 et 6 heures du soir qu'il finit sa courte mais honorable et vertueuse carriere dans les ondes de la petite Nevka en se baignant, et après avoir fait très gaiement quelques tours de nâge à la vue de M. Fuss qui s'étoit baigné aussi et qui alloit deja remettre ses habits. Fuss l'entendit à peine râler, et voyant qu'il couloit à fond, il se jetta dans l'eau et risqua sa propre vie pour le retirer de l'eau: car comme il ne sait pas nager, il ne pouvoit l'approcher que par le moyen des quelques branches qu'il étoit obligé d'aller chercher au rivage; car il n'y avoit personne aux environs, qu'il auroit pu appeller au Secours. Cependant, le corps ne sauroit avoir été sous l'eau au delà de 5 minutes, et M. Fuss ne le tenoit gueres au rivage qu'il employoit tous les secours pour le rappeller à la vie qui etoient à sa portée. Enfin voyant approcher de loin quelques hommes, il les appella et fut tout droit annoncer le triste evenement à ma femme et à toute notre famille qui se trouvoient rassemblée en partie chez Mad. Amay, et en partie dans la maison de campagne de mes enfans, pour y passer une agréable Soirée et y souper. Pour lui il couroit tout de suite sans consulter ses forces en ville pour appeller des Chirurgiens et en moins d'un heure en arriverent deux des nos plus habiles, mais qui declarerent aussi tout de suite, qu'il n'y avoit aucune esperance de le faire revenir à la vie, le defunt

étant mort d'un coup d'appoplexie qui lui est monté tout de suite à la tête. Toutefois on continua, comme on l'avoit fait jusques là à employer tous les remedes connus et approuvés dans des pareils cas. On avoit transporté le corps dans la maison de M. Amay qui est la plus voisine, on l'avoit couché entre deux draps chauds, on le frottoit, on employoit des eaux fortes, on appliquoit des lavemens de tabac, on saigna &c &c le corps resta mort et manifesta dès le lendemain déja des marques de la putrefaction: en sorte qu'on n'a pas pu le garder plus long temps que 30 heures, et qu'il a fallu l'enterrer sans aucune ceremonie la nuit du 4 au 5. Notre ami Krafft, moi et mes deux fils ainés accompagnerent le cercueil qui fut posé à la cimetiere de notre isle, où il fut enterré près des personnes de notre famille. Jugés mon très-honoré Oncle de l'affliction de ma pauvre fille, qui l'aimoit le plus tendrement possible et qui en étoit bien payé du plus parfait retour. Ce soir il y aura dans notre église une oraison funebre, que je compte de faire imprimer pour la distribuer à toute la famille et en envoyer des exemplaires à Bâle et à Berlin. Nous lui ferons aussi poser un pierre avec un épitaphe —— Que diront ses bons vieux parens à Bâle, que dira son frère à Berlin! Le defunt s'étoit proposé de faire l'année prochaine un tour en Suisse avec sa jeune femme pour la présenter à ses parens, et peut-être pour s'y domicilier entirement; car on lui avoit fait esperer une bonne place à Neufchatel qu'il auroit acceptée avec plaisir. —— Apresent mon très-honoré Oncle, je voudrois bien que Vous priez en mon nom un de Messieurs Vos gendres d'aller chez Votre Bernoulli pour lui annoncer cette triste mort d'une bonne façon, et de lui remettre ensuite la condoleance ci-jointe du bon Comte Anhalt, qui a versé des larmes en apprenant ce coup fâtal, et qui l'a véritablement chéri et estimé. J'y joins encore un billet du defunt qu'il m'avoit remis peu de jours avant sa mort pour l'inserer dans le premier pacquet que je Vous adresserois. Je ne suis pas en état de lui écrire aujourd'hui: qu'il me le pardonne. Je suis encore trop emu, et il regne tout autour de moi une emotion continuelle ——.

\- - - - - - - - - - - - - -

Monsieur et très-honoré Oncle

Votre

Très-humble et très-obéissant
Serviteur et Neveu J. A. Euler