## Werk

**Titel:** Journal für die reine und angewandte Mathematik
**Verlag:** de Gruyter
**Jahr:** 1847
**Kollektion:** Mathematica
**Digitalisiert:** Niedersächsische Staats- und Universitätsbibliothek Göttingen
**Werk Id:** PPN243919689_0035
**PURL:** http://resolver.sub.uni-goettingen.de/purl?PPN243919689_0035

**LOG Id:** LOG_0026
**LOG Titel:** Über die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfactoren.
**LOG Typ:** article

## Übergeordnetes Werk

**Werk Id:** PPN243919689
**PURL:** http://resolver.sub.uni-goettingen.de/purl?PPN243919689



## Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

# 16.

# Über die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfactoren.

(Von Herrn Dr. *E. E. Kummer*, Professor in Breslau.)

In dem vorstehenden Aufsatze, welchen ich als Einleitung zu dem hier folgenden anzusehen bitte, habe ich vor einiger Zeit die Resultate meiner Untersuchungen über die Zerlegung der complexen Zahlen niedergelegt. Die Entwickelung und Begründung derselben soll nun der Gegenstand der gegenwärtigen Abhandlung sein.

## §. 1.

Es sei $\lambda$ eine Primzahl und $\alpha$ eine imaginäre Wurzel der Gleichung $\alpha^\lambda = 1$, so ist die allgemeinste Form der complexen Zahlen, welche wir hier untersuchen:

$$\varphi(\alpha) = a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + \ldots + a_{\lambda-1}\alpha^{\lambda-1};$$

in welchem Ausdruck die Coëfficienten $a_1$, $a_2$, $a_3$, etc. ***ganze*** Zahlen sind. In besonderen Fällen können alle diejenigen Coëfficienten der complexen Zahl, welche mit den zu denselben Perioden gehörenden Wurzeln der Einheit multiplicirt sind, einander gleich werden; so dafs die complexe Zahl zu einer linearen Function der Perioden wird. Die Untersuchung dieser besondern Art complexer Zahlen, welche andrerseits, da die Perioden auch eingliedrig sein können, die allgemeine complexe Zahl als besondern Fall in sich schliefst, bildet die Grundlage für die Auffindung der Primfactoren aller aus den Wurzeln der Einheit geformten complexen Zahlen; weshalb wir zunächst nur von diesen zu handeln haben.

Besteht die Zahl $\lambda - 1$ aus den beiden Factoren $e$ und $f$, so dafs $\lambda - 1 = e \cdot f$, und bezeichnet $\gamma$ eine primitive Wurzel von $\lambda$, so kann man die imaginären Wurzeln der Gleichung $\alpha^\lambda = 1$ folgendermafsen in $e$ Perioden von je $f$ Gliedern zusammenordnen:

$$\begin{aligned}
\eta &= \alpha + \alpha^{\gamma^e} + \alpha^{\gamma^{2e}} + \ldots + \alpha^{\gamma^{(f-1)e}},\\
\eta_1 &= \alpha^\gamma + \alpha^{\gamma^{e+1}} + \alpha^{\gamma^{2e+1}} + \ldots + \alpha^{\gamma^{(f-1)e+1}},\\
\eta_2 &= \alpha^{\gamma^2} + \alpha^{\gamma^{e+2}} + \alpha^{\gamma^{2e+2}} + \ldots + \alpha^{\gamma^{(f-1)e+2}},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\eta_{e-1} &= \alpha^{\gamma^{e-1}} + \alpha^{\gamma^{2e-1}} + \alpha^{\gamma^{3e-1}} + \ldots + \alpha^{\gamma^{fe-1}}.
\end{aligned}$$

Das Product zweier Perioden läfst sich bekanntlich als lineare Function der ähnlichen Perioden mit ganzzahligen Coëfficienten darstellen; deshalb sei

$$(1.) \quad \eta.\eta_k = \overset{k}{\mu} f + \overset{k}{m}\eta + \overset{k}{m_1}\eta_1 + \overset{k}{m_2}\eta_2 + \ldots + \overset{k}{m_{e-1}}\eta_{e-1},$$

woraus auch die scheinbar allgemeinere Gleichung folgt:

$$(2.) \quad \eta_r\eta_{r+k} = \overset{k}{\mu} f + \overset{k}{m}\eta_r + \overset{k}{m_1}\eta_{r+1} + \overset{k}{m_2}\eta_{r+2} + \ldots + \overset{k}{m_{e-1}}\eta_{r+e-1}.$$

Der Coëfficient $\overset{k}{\mu}$ ist immer gleich Null, aufser wenn $f$ gerade und $k=0$, oder $f$ ungerade und zugleich $k=\frac{1}{2}e$ ist; in welchen beiden Fällen $\overset{k}{\mu}=1$ ist. Die übrigen Coëfficienten $\overset{k}{m_h}$ haben sehr einfache Beziehungen zu einander, welche wir kurz entwickeln wollen. Multiplicirt man zwei Perioden von $f$ Gliedern mit einander, so ist die Anzahl aller Glieder des entwickelten Products gleich $ff$; deshalb mufs, wenn in der Gleichung (1.) die Perioden als Summen von je $f$ Wurzeln aufgefafst werden, die Summe aller Coëfficienten gleich $ff$, also

$$ff = \overset{k}{\mu} f + \overset{k}{m} f + \overset{k}{m_1} f + \overset{k}{m_2} f + \ldots + \overset{k}{m_{e-1}} f,$$

mithin

$$(3.) \quad f = \overset{k}{\mu} + \overset{k}{m} + \overset{k}{m_1} + \overset{k}{m_2} + \ldots + \overset{k}{m_{e-1}}$$

sein. Setzt man ferner in der Gleichung (2.) nach einander $r=0, 1, 2, \ldots e-1$ und nimmt die Summe, so erhält man

$$\sum_0^{e-1} \eta_r\eta_{r+k} = ef\overset{k}{\mu} - \overset{k}{m} - \overset{k}{m_1} - \overset{k}{m_2} - \ldots - \overset{k}{m_{e-1}};$$

also, vermöge (3.), und weil $ef=\lambda-1$ ist:

$$(4.) \quad \sum_0^{e-1} \eta_r\eta_{r+k} = \overset{k}{\mu}\lambda - f.$$

Berücksichtigt man noch den oben angegebenen Werth von $\overset{k}{\mu}$, so zeigt sich, dafs diese Summe immer gleich $-f$ ist; mit Ausnahme der beiden Fälle: erstens, wo $f$ gerade und $k=0$, und zweitens, wo $f$ ungerade und $k=\frac{1}{2}e$ ist; in welchen Fällen diese Summe gleich $\lambda-f$ ist.

Verwandelt man ferner in der Gleichung (2.) $k$ in $e-k$, so wird

$$\eta_r\eta_{r-k} = \overset{e-k}{\mu} f + \overset{e-k}{m}\eta_r + \overset{e-k}{m_1}\eta_{r+1} + \overset{e-k}{m_2}\eta_{r+2} + \ldots + \overset{e-k}{m_{e-1}}\eta_{r+e-1}.$$

Setzt man aber in derselben Gleichung (2.) $r-k$ statt $r$, so ist

$$\eta_r\eta_{r-k} = \overset{k}{\mu} f + \overset{k}{m}\eta_{r-k} + \overset{k}{m_1}\eta_{r-k+1} + \overset{k}{m_2}\eta_{r-k+2} + \ldots + \overset{k}{m_{e-1}}\eta_{r-k+e-1}.$$

Durch Vergleichung dieser beiden Ausdrücke erhält man allgemein

$$(5.) \qquad \overset{k}{m}_h = \overset{e-k}{m}_{h-k}.$$

Multiplicirt man endlich die Gleichung (2.) mit $\eta_{h+r}$ und nimmt die Summe für $r = 0, 1, 2, \ldots . e-1$, so erhält man vermittels der Formel (4.):

$$\sum_0^{e-1} \eta_r \eta_{k+r} \eta_{h+r} = -ff + \lambda \overset{k}{m}_h, \text{ wenn } f \text{ gerade ist und}$$

$$\sum_0^{e-1} \eta_r \eta_{k+r} \eta_{h+r} = -ff + \lambda \overset{k}{m}_{h+\frac{1}{2}e}, \text{ wenn } f \text{ ungerade ist;}$$

und weil sich in den Summen zur Linken $h$ und $k$ vertauschen lassen, so folgt

$$(6.) \qquad \begin{cases} \overset{k}{m}_h = \overset{h}{m}_k, \text{ wenn } f \text{ gerade und} \\ \overset{k}{m}_{h+\frac{1}{2}e} = \overset{h}{m}_{k+\frac{1}{2}e}, \text{ wenn } f \text{ ungerade ist.} \end{cases}$$

Die Gleichung (1.), welche die Grundlage jeder Rechnung mit den Perioden ist, drückt eigentlich ein System von $e$ verschiedenen Gleichungen für $k = 0, 1, 2, \ldots . e-1$ aus. Diese zusammen reichen auch gerade hin, um aus ihnen die $e$ Perioden selbst zu finden. Eliminirt man nämlich alle Perioden, aufser der ersten $\eta$, so erhält man für $\eta$ eine Gleichung vom $e$ten Grade; und zwar genau jene bekannte Gleichung, deren Wurzeln alle $e$ Perioden sind. Läfst man ferner irgend eine der $e$ Gleichungen, welche in (1.) enthalten sind, weg, und betrachtet die erste Periode $\eta$ als bekannt, die übrigen $e-1$ Perioden als unbekannt, so erhält man ein System von $e-1$ Gleichungen mit $e-1$ Unbekannten; und zwar ein lineares System, aus welchem sich $\eta_1, \eta_2, \ldots . \eta_{e-1}$ alle rational durch $\eta$ ausdrücken lassen. Man erhält so die Ausdrücke der Perioden als rationale Functionen der ersten (d. h. einer beliebigen andern); welche Ausdrücke *Gaufs* auf andere Weise herleitet.

Wir fassen jetzt das System der in (1.) enthaltenen Gleichungen als ein System von Congruenzen auf, für den Modul $q$; wo $q$ eine Primzahl sein soll, welche der Bedingung $q^f \equiv 1$ mod. $\lambda$ genügt. Anstatt der Perioden $\eta, \eta_1, \eta_2, \ldots . \eta_{e-1}$ setzen wir die unbestimmten ganzen Zahlen $u, u_1, u_2, \ldots . u_{e-1}$. Dies giebt folgendes System von Congruenzen:

$$(7.) \qquad u u_k \equiv \overset{k}{\mu} f + \overset{k}{m} u + \overset{k}{m}_1 u_1 + \overset{k}{m}_2 u_2 + \ldots . + \overset{k}{m}_{e-1} u_{e-1}, \text{ mod. } q,$$

für $k = 0, 1, 2, \ldots . e-1$. Es giebt nun immer $e$ wirkliche ganze Zahlen $u, u_1, u_2, \ldots . u_{e-1}$, welche diesem Systeme von Congruenzen genugthun: denn eliminirt man auch hier alle Unbekannten, die erste $u$ ausgenommen,

so erhält man eine Congruenz vom $e$ten Grade für $u$, welche mit der Gleichung für $\eta$, welche alle Perioden zu Wurzeln hat, genau übereinstimmt.

Diese Gleichung sei

$$(8.) \quad y^e + A_1 y^{e-1} + A_2 y^{e-2} + \ldots + A_e = Y = 0:$$

so hat die Congruenz $Y \equiv 0$ mod. $q$ (wie ich in der Abhandlung über die Divisoren gewisser Formen der Zahlen, welche aus der Theorie der Kreistheilung entstehen, in diesem Journal Bd. 30. S. 107 bewiesen habe) immer $e$ reale Wurzeln; falls nämlich, wie vorausgesetzt worden, $q$ eine Primzahl von der Art ist, dafs $q^f \equiv 1$, mod. $\lambda$. Wenn nun $u$ aus der Congruenz $Y \equiv 0$, mod. $q$, bestimmt ist, so werden $u_1, u_2, u_3, \ldots u_{e-1}$ mittels der in (7.) enthaltenen Gleichungen nur noch linear bestimmt; eine Unmöglichkeit kann demnach nirgends eintreten, da überdies der Modul eine Primzahl ist. Man würde auch mit der einzigen Congruenz $Y \equiv 0$ mod. $q$ ausreichen, um alle Zahlen $u, u_1, u_2, \ldots u_{e-1}$ zu bestimmen, weil sie alle auf gleiche Weise Wurzeln dieser Congruenz sind; aber man würde so nicht finden können, in welcher Ordnung die Wurzeln dieser Congruenz zu nehmen sind, damit sie auch den in (7.) enthaltenen Congruenzen genügen.

Da man jede beliebige der $e$ Congruenzwurzeln von $Y \equiv 0$ mod. $q$ als erste ansehen kann (wonach sich dann nur die Reihenfolge der übrigen zu richten hat, welche cyklisch immer dieselbe bleibt), so folgt, dafs die den Congruenzen, welche in (7.) enthalten sind, genügenden Zahlen $u, u_1, u_2, \ldots u_{e-1}$, ebenso auch der scheinbar allgemeineren, der Gleichung (2.) entsprechenden Congruenz

$$(9.) \quad u_r u_{r+k} \equiv \overset{k}{\mu} f + \overset{k}{m} u_r + \overset{k+1}{m_1} u_{r+1} + \overset{k}{m_2} u_{r+2} + \ldots + \overset{k}{m_{e-1}} u_{r-1}, \text{ mod. } q,$$

genügen; für alle Werthe der Zahlen $r$ und $k$. Jeder der $e$ Perioden $\eta, \eta_1, \eta_2, \ldots \eta_{e-1}$ entspricht also eine der Congruenzwurzeln $u, u_1, u_2, \ldots u_{e-1}$, in der Art, dafs, wenn man statt der Perioden in den Gleichungen (2.) ihre analogen Congruenzwurzeln setzt, diese Gleichungen zu richtigen Congruenzen für den Modul $q$ werden.

## §. 2.

Die Congruenzwurzeln $u, u_1, u_2, \ldots u_{e-1}$ befolgen, wie wir im vorigen Paragraphen gezeigt haben, in ihrer Multiplication, genau dieselben Gesetze wie die Perioden; und da ohnedies die Addition und Subtraction für die Congruenzwurzeln dieselbe ist wie für die Perioden, so folgt der wichtige Satz: ***Dafs zu jeder Gleichung, unter den Perioden, welche nur Additio-***

*nen, Subtractionen und Multiplicationen derselben enthalten, stets eine entsprechende Congruenz sein mufs, welche man dadurch erhält, dafs man nur anstatt der Perioden ihre entsprechenden Congruenzwurzeln setzt.* Es gehören ferner zu einer einzigen solchen rationalen Gleichung immer noch $e-1$ conjugirte, welche aus ihr durch Vertauschung der Perioden, mit Beibehaltung der cyklischen Ordnung derselben, gebildet werden, oder, was dasselbe ist, durch gleiche Vergröfserung aller Indices der Perioden; wobei von den Indices, welche gröfser als $e-1$ werden, $e$, oder Vielfache von $e$, abzuziehen sind. Dafs nämlich eine solche Veränderung jeder rationalen Gleichung, unter den Perioden, die man auch nur als eine Änderung der Wurzel $\alpha$ der Gleichung $\frac{\alpha^\lambda-1}{\alpha-1}=0$ ansehen kann, stets gestattet ist, folgt sehr leicht aus der Irreductibilität dieser Gleichung. Ebenso gehören auch eigentlich zu einer solchen Gleichung unter den Perioden nicht nur eine, sondern stets $e$ Congruenzen, weil man die Congruenzwurzeln, mit Beibehaltung ihrer cyklischen Ordnung, auf $e$ verschiedene Arten den Perioden zuordnen kann.

Hiernach folgt z. B. aus der Gleichung $\eta+\eta_1+\eta_2+\ldots.+\eta_{e-1}=-1$ die Congruenz

$$(1.)\qquad u+u_1+u_2+\ldots.+u_{e-1}\equiv -1 \bmod. q;$$

ferner aus der Gleichung (4.) §. 1. die Congruenz

$$(2.)\qquad \sum_0^{e-1} u_r u_{r+k}\equiv -f \bmod. q;$$

mit Ausnahme der beiden Fälle: erstens, wo $f$ gerade und $k=0$, und zweitens, wo $f$ ungerade und $k=\frac{1}{2}e$ ist; in welchen Fällen diese Summe congruent $\lambda-f$ ist.

Bezeichnet ferner $F(\eta)$ irgend eine ganze rationale Function der Perioden $\eta$, $\eta_1$, $\eta_2$, .... $\eta_{e-1}$ mit ganzzahligen Coëfficienten, welche irgend wie als Product von Factoren, oder als Summe solcher Producte erscheinen mag: so kann man dieselbe bekanntlich immer auf die Form

$$(3.)\qquad F(\eta)=a\eta+a_1\eta_1+a_2\eta_2+\ldots.+a_{e-1}\eta_{e-1}$$

bringen. Setzt man nun statt der Perioden die Congruenzwurzeln, und zwar so, dafs $u_r$ statt $\eta$, $u_{r+1}$ statt $\eta_1$, $u_{r+2}$ statt $\eta_2$, u. s. w. gesetzt wird, in welchem Falle wir die ganze Zahl, in welche $F(\eta)$ übergeht, durch $F(u_r)$ bezeichnen, so ist

$$(4.)\qquad F(u_r)\equiv au_r+a_1u_{r+1}+a_2u_{r+2}+\ldots.+a_{e-1}u_{r-1} \bmod. q,$$

für jeden beliebigen Werth von $r$. Enthält $F(\eta)$ den realen Factor $q$, so

müssen, nachdem diese complexe Zahl auf die einfache Grundform (3.) gebracht ist, alle Coëfficienten $a$, $a_1$, $a_2$, ..... $a_{e-1}$ einzeln durch $q$ theilbar sein; und in diesem Falle mufs deshalb auch $F(u_r) \equiv 0 \bmod. q$ sein, für jeden Werth von $r$. Stellt man sich ferner nicht nur die complexe Zahl $F(\eta)$, sondern auch alle ihre conjugirten, welche durch cyklische Veränderung der Perioden entstehen, auf die einfache Grundform gebracht vor, so erhält man

$$(5.)\quad \begin{cases} F(\eta) &= a\eta + a_1\eta_1 + a_2\eta_2 + \ldots + a_{e-1}\eta_{e-1}, \\ F(\eta_1) &= a\eta_1 + a_1\eta_2 + a_2\eta_3 + \ldots + a_{e-1}\eta, \\ F(\eta_2) &= a\eta_2 + a_1\eta_3 + a_2\eta_4 + \ldots + a_{e-1}\eta_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ F(\eta_{e-1}) &= a\eta_{e-1} + a_1\eta + a_2\eta_1 + \ldots + a_{e-1}\eta_{e-2}. \end{cases}$$

Multiplicirt man diese Gleichungen der Reihe nach mit $\eta_k$, $\eta_{k+1}$, $\eta_{k+2}$, .... u. s. w. und addirt, so erhält man, vermöge der Gleichung (4. §. 1.), wenn $f$ ***gerade*** ist:

$$(6.)\quad \eta_k F(\eta) + \eta_{k+1} F(\eta_1) + \eta_{k+2} F(\eta_2) + \ldots + \eta_{k-1} F(\eta_{e-1}) = a_k\lambda - (a + a_1 + \ldots + a_{e-1})f;$$

und da die Addition aller Gleichungen (5.)

$$(7.)\quad F(\eta) + F(\eta_1) + F(\eta_2) + \ldots + F(\eta_{e-1}) = -(a + a_1 + \ldots + a_{e-1})$$

giebt, so erhält man:

$$(8.)\quad (\eta_k - f)F(\eta) + (\eta_{k+1} - f)F(\eta_1) + \ldots + (\eta_{k-1} - f)F(\eta_{e-1}) = a_k.\lambda.$$

Wenn $f$ ***ungerade*** ist, modificirt sich dieses Resultat nur insofern, dafs anstatt $a_k.\lambda$ alsdann $a_{k+\frac{1}{2}e}.\lambda$ herauskommt. Setzt man nun statt der Perioden die Congruenzwurzeln, so ergiebt sich

$$(u_k - f)F(u) + (u_{k+1} - f)F(u_1) + \ldots + (u_{k-1} - f)F(u_{e-1}) \equiv a_k.\lambda, \bmod. q,$$

oder congruent $a_{k+\frac{1}{2}e}.\lambda$, wenn $f$ ***ungerade*** ist. Wenn nun $F(u_r) \equiv 0 \bmod. q$ ist, für jeden Werth von $r$, so folgt aus dieser Congruenz, dafs sämmtliche Coëfficienten $a$, $a_1$, $a_2$, .... $a_{e-1}$ durch $q$ theilbar sind, dafs also auch die complexe Zahl $F(\eta)$ den realen Factor $q$ hat. Es sind demnach folgende zwei Sätze bewiesen worden, von welchen einer der umgekehrte des andern ist:

***Wenn eine ganze rationale Function der Perioden mit ganzzahligen Coëfficienten durch den realen Factor q theilbar ist, so sind auch alle diejenigen ganzen Zahlen durch q theilbar, welche entstehen, wenn man statt der Perioden ihre entsprechenden Congruenzwurzeln für den Modul q setzt;***

und umgekehrt:

***Wenn alle die e ganzen Zahlen, welche aus einer ganzen rationalen Function der Perioden entstehen, indem statt der Perioden die Congruenzwurzeln für den Modul q gesetzt werden, durch q theilbar sind, so ist diese Function der Perioden selbst durch q theilbar.***

Ist $\varphi(\eta)$ irgend eine aus den Perioden gebildete complexe Zahl, so nennen wir das Product aller conjugirten complexen Zahlen, welches immer eine ganze Zahl ist, *die Norm* der complexen Zahl $\varphi(\eta)$ und bezeichnen dasselbe durch

$$N\varphi(\eta) = \varphi(\eta)\varphi(\eta_1)\varphi(\eta_2)\ldots\ldots\varphi(\eta_{e-1}).$$

Wendet man nun die sieben gefundenen Sätze auf diese Norm an, so ergiebt sich, ***dafs: Wenn die Norm $N\varphi(\eta)$ durch q theilbar ist, stets auch eine der ganzen Zahlen $\varphi(u)$, $\varphi(u_1)$, $\varphi(u_2)$, $\ldots\ldots\varphi(u_{e-1})$ durch q theilbar sein mufs; und umgekehrt, dafs, wenn eine dieser Zahlen durch q theilbar ist, auch die Norm durch q theilbar sein mufs.***

## §. 3.

Für die Untersuchung der Primfactoren jeder gegebenen complexen Zahl ist es noch sehr wichtig, zu beweisen, dafs es stets solche complexe, aus Perioden gebildete Zahlen giebt, deren Norm durch $q$ theilbar ist, aber nicht durch $q^2$; und zugleich zu zeigen, wie diese complexen Zahlen gefunden werden können. Im allgemeinen wird es schon unter den complexen Zahlen $u-\eta$, $u_1-\eta$, $u_2-\eta$, $\ldots\ldots u_{e-1}-\eta$, deren Normen alle durch $q$ theilbar sind, einige geben, welche die verlangte Eigenschaft haben; ja es ist leicht zu beweisen, dafs immer wenigstens eine dieser complexen Zahlen genügt, sobald es unter den Congruenzwurzeln $u$, $u_1$, $u_2$, $\ldots\ldots u_{e-1}$ nur noch eine giebt, welche keiner andern gleich ist. Da dies aber wirklich, namentlich für sehr kleine Werthe von $q$ und grofse Werthe von $e$, nicht immer der Fall ist, so wenden wir, um diese verlangten complexen Zahlen zu finden, folgende Methode an, welche stets sicher zum Ziele führt.

Wir suchen zunächst eine complexe Zahl $\varphi(\eta)$ von der Art, dafs das Product $\varphi(\eta_r)\varphi(\eta_s)$ durch $q$ theilbar sei, sobald $r$ und $s$ ***verschieden*** sind; aber nicht durch $q$ theilbar, sobald $r$ und $s$ einander ***gleich*** sind. Eine solche Zahl ist immer die folgende:

$$(1.)\qquad \varphi(\eta) = f + u\eta + u_1\eta_1 + u_2\eta_2 + \ldots\ldots + u_{e-1}\eta_{e-1}.$$

Es ist nämlich

$$\varphi(u_r) \equiv f + uu_r + u_1u_{r+1} + u_2u_{r+2} + \ldots + u_{e-1}u_{r-1}, \text{ mod. } q,$$

also, vermöge der Congruenz (2. §. 2.),

$$\varphi(u_r) \equiv 0, \text{ mod. } q,$$

mit Ausnahme der beiden Fälle: erstens, wo *f gerade* und $r = 0$, und zweitens, wo *f ungerade* und $r = \frac{1}{2}e$ ist; in welchen Fällen $\varphi(u_r) \equiv \lambda$ ist. Eben so ist $\varphi(u_s) \equiv 0$, oder $\equiv \lambda$, unter denselben Bedingungen. Demnach ist das Product

$$(2.) \qquad \varphi(u_r)\varphi(u_s) \equiv 0, \text{ mod. } q,$$

für jeden Werth von $r$ und $s$; mit Ausnahme der beiden Fälle: erstens, wo $r = s = 0$ und *f gerade*, und zweitens, wo $r = s = \frac{1}{2}e$ und *f ungerade* ist. Läfst man nun die Congruenzwurzeln alle möglichen Werthe durchlaufen, mit Beibehaltung der cyklischen Ordnung, so enthält diese eine Congruenz (2.) eigentlich $e$ Congruenzen, aus welchen mittels des zweiten Lehrsatzes im vorigen Paragraphen sogleich folgt, dafs

$$\varphi(\eta_r)\varphi(\eta_s) \equiv 0, \text{ mod. } q,$$

ist; mit alleiniger Ausnahme des Falles $r = s$; wie es verlangt wurde.

Ich untersuche nun weiter von der complexen Zahl $\lambda - \varphi(\eta) = \psi(\eta)$ die Norm

$$N\psi(\eta) = (\lambda - \varphi(\eta))(\lambda - \varphi(\eta_1))(\lambda - \varphi(\eta_2)) \ldots . (\lambda - \varphi(\eta_{e-1})).$$

Entwickelt man das Product rechts, und läfst dabei alle durch $q$ theilbaren Theile weg, so erhält man mittels der Congruenz $\varphi(\eta_r)\varphi(\eta_s) \equiv 0$, mod. $q$, folgende Congruenz:

$$N\psi(\eta) = \lambda^e - \lambda^{e-1}(\varphi(\eta) + \varphi(\eta_1) + \varphi(\eta_2) + \ldots . + \varphi(\eta_{e-1})), \text{ mod. } q,$$

und da

$$\varphi(\eta) + \varphi(\eta_1) + \varphi(\eta_2) + \ldots . + \varphi(\eta_{e-1}) \equiv \lambda, \text{ mod. } q,$$

ist, so ist

$$N\psi(\eta) \equiv 0, \text{ mod. } q.$$

Eben so soll jetzt die Theilbarkeit durch $q$ der complexen Zahl

$$\Psi(\eta) = \psi(\eta_1)\psi(\eta_2) \ldots . \psi(\eta_{e-1}) \text{ oder}$$
$$\Psi(\eta) = (\lambda - \varphi(\eta_1))(\lambda - \varphi(\eta_2)) \ldots . (\lambda - \varphi(\eta_{e-1}))$$

untersucht werden, welche, mit Ausnahme des ersten Factors, alle Factoren der Norm von $\psi(\eta)$ enthält. Durch Entwicklung und Vernachläfsigung aller durch $q$ theilbaren Theile erhält man hier:

$$\Psi(\eta) \equiv \lambda^{e-1} - \lambda^{e-2}(\varphi(\eta_1) + \varphi(\eta_2) + \ldots . + \varphi(\eta_{e-1})), \text{ mod. } q,$$

und da

$$\varphi(\eta_1)+\varphi(\eta_2)+\ldots.+\varphi(\eta_{e-1}) \equiv \lambda-\varphi(\eta)$$

ist, so ist

$$\Psi(\eta) \equiv \lambda^{e-1}-\lambda^{e-2}(\lambda-\varphi(\eta)) \equiv \lambda^{e-2}\varphi(\eta), \text{ mod. } q;$$

also ist $\Psi(\eta)$ nicht durch $q$ theilbar. Ich behaupte nun, dafs immer $\psi(\eta)$, oder doch $\psi(\eta)+q$, eine der verlangten complexen Zahlen ist, deren Norm den Factor $q$ einmal enthält, aber nicht mehrmals. Um dies zu beweisen, entwickle ich $N(\psi(\eta)+q)$ nach dem Modul $q^2$, was

$$N(\psi(\eta)+q) \equiv N\psi(\eta)+q(\Psi(\eta)+\Psi(\eta_1)+\ldots.+\Psi(\eta_{e-1})), \text{ mod. } q^2,$$

giebt. Wenn also wirklich $\psi(\eta)$ nicht eine der verlangten Zahlen, sondern, aufser durch $q$, auch durch $q^2$ theilbar ist, so ist

$$N(\psi(\eta)+q) \equiv q(\Psi(\eta)+\Psi(\eta_1)+\ldots.+\Psi(\eta_{e-1})), \text{ mod. } q^2.$$

Multiplicirt man mit $\Psi(\eta)$ und beachtet, dafs $\Psi(\eta)\Psi(\eta_r)$ immer den Factor $q$ enthält, aufser wenn $r=0$, so erhält man

$$\Psi(\eta)N(\psi(\eta)+q) \equiv q(\Psi(\eta))^2, \text{ mod. } q^2;$$

und da $(\Psi(\eta))^2$ nicht mit $q$ aufgeht, so folgt, dafs $N(\psi(\eta)+q)$ nicht durch $q^2$ theilbar ist. Es giebt also stets complexe Zahlen, deren Normen einen bestimmten realen Primfactor $q$ ***nur einmal*** enthalten.

## §. 4.

Wir wenden uns jetzt zu den allgemeineren complexen Zahlen, welche nicht aus den Perioden, sondern irgend wie aus den Wurzeln der Gleichung $\alpha^\lambda=1$ gebildet sind und welche also auf die Form

$$f(\alpha) = a_1\alpha+a_2\alpha^2+a_3\alpha^3+\ldots.+a_{\lambda-1}\alpha^{\lambda-1}$$

gebracht werden können. Jede complexe Zahl ist ein Factor irgend einer realen ganzen Zahl; namentlich ist sie stets ein Factor der Norm: deshalb ist auch jeder Primfactor einer complexen Zahl zugleich Primfactor einer realen ganzen Zahl; und zwar immer Primfactor der Norm. Aus diesem Grunde haben wir zunächst die Bedingungen zu suchen, unter welchen die Norm einer complexen Zahl einen gegebenen realen Primfactor $q$ enthält. Alle nicht durch $\lambda$ theilbaren Zahlen können nun bekanntlich nach den verschiedenen Exponenten eingetheilt werden, zu welchen sie gehören, für den Modul $\lambda$ (S. *Gaufs* Disquisitiones arithm. §. 52.); und diese Eintheilung begründet auch die wesentlich verschiedenen Charactere der Divisoren der Norm.

Es sei demnach $q$ eine Primzahl, welche zum Exponenten von $f$ (einem Divisor von $\lambda-1$) gehört, so dafs $q^f\equiv 1$, mod. $\lambda$, aber so, dafs keine niederere

Potenz von $q$ der Eins congruent sei: so ist (Vergl. die Abhandlung über die Divisoren etc. in diesem Journal Bd. XXX. S. 115)

$$(1.) \quad (f(\alpha))^q \equiv f(\alpha^q), \text{ mod. } q:$$

also, wenn man wiederholt zur $q$ten Potenz erhebt:

$$(2.) \quad (f(\alpha))^{q^h} \equiv f(\alpha^{q^h}), \text{ mod. } q,$$

und folglich, wenn $h = 0, 1, 2, \ldots f-1$ gesetzt und multiplicirt wird:

$$(3.) \quad (f(\alpha))^{1+q+q^2+\ldots+q^{f-1}} \equiv f(\alpha)f(\alpha^q)f(\alpha^{q^2})\ldots f(\alpha^{p^{f-1}}), \text{ mod. } q.$$

Setzt man nun $\alpha^{\gamma^m}$ statt $\alpha$, und für $q$, wo es als Exponent des $\alpha$ vorkommt, seinen congruenten Werth, als Potenz einer primitiven Wurzel $\gamma$, welche, da $q^f \equiv 1$, mod. $\lambda$ eine $e^{\text{te}}$ Potenz, also $q \equiv \gamma^{re}$, mod. $\lambda$, sein mufs: so erhält man

$$(4.) \quad (f(\alpha^{\gamma^m}))^{1+q+q^2+\ldots+q^{f-1}} \equiv f(\alpha^{\gamma^m})f(\alpha^{\gamma^{re+m}})f(\alpha^{\gamma^{2re+m}})\ldots f(\alpha^{\gamma^{(f-1)re+m}}), \text{ mod. } q.$$

Es hat $r$ keinen gemeinschaftlichen Factor mit $f$, weil $q$ nach der Voraussetzung so zum Exponenten $f$ gehört, dafs $q^f$, aber keine niedrigere Potenz von $q$, der Eins congruent wird für den Modul $\lambda$. Giebt man also dem $m$ nach einander $e$ Werthe, welche alle nach dem Modul $e$ incongruent sind, so erhält man durch Multiplication dieser Congruenzen rechts das Product aller conjugirten complexen Zahlen, d. h. die Norm der complexen Zahl $f(\alpha)$, folglich

$$(5.) \quad (\Pi f(\alpha^{\gamma^m}))^{1+q+q^2+\ldots+q^{f-1}} \equiv Nf(\alpha), \text{ mod. } q;$$

wo das Productzeichen $\Pi$ sich auf die $e$ verschiedenen Werthe des $m$ bezieht, welche nur der einen Bedingung unterworfen sind, dafs sie alle incongruent sein müssen, für den Modul $e$. Wenn nun die Norm $Nf(\alpha)$ durch $q$ theilbar ist, so ist auch

$$(\Pi f(\alpha^{g^m}))^{1+q+q^2+\ldots+q^{f-1}} \equiv 0, \text{ mod. } q;$$

woraus nothwendig folgt:

$$(6.) \quad \Pi f(\alpha^{g^m}) \equiv 0, \text{ mod. } q.$$

Wir haben also folgenden Satz:

***Wenn $Nf(\alpha)$ durch $q$ theilbar ist, wo $q$ eine zum Exponenten $f$ gehörende Primzahl bezeichnet, so müssen von den $\lambda-1$ conjugirten complexen Zahlen $f(\alpha)$, $f(\alpha^g)$, $f(\alpha^{g^2})$, etc. je $e$, deren Wurzeln nur verschiedenen von den $e$ Perioden, zu je $f$ Gliedern, angehören, immer ein Product geben, welches durch $q$ theilbar ist.***

Aufserdem folgt noch als Zusatz:

***Wenn die Norm $Nf(\alpha)$ durch den zum Exponenten $f$ gehörenden***

***Primfactor $q$ theilbar ist, so mufs sie immer $f$ mal den Factor $q$ enthalten, oder durch $q^f$ theilbar sein.***

Um nun weiter die Congruenzbedingungen zu finden, welchen die Coëfficienten der complexen Zahl $f(\alpha)$ genügen müssen, damit die Norm derselben durch $q$ theilbar sei, werden wir dieser complexen Zahl eine Form geben, in welcher statt der einfachen Wurzeln $\alpha$, $\alpha^2$, $\alpha^3$, etc., insoweit es möglich ist, die Perioden von je $f$ Gliedern auftreten. Nach *Gaufs* Disqu. arithm. §. 348, sind alle Wurzeln, welche in einer Periode von $f$ Gliedern vorkommen, zugleich Wurzeln einer Gleichung vom $f$ten Grade von der Form

$$\alpha^f + \boldsymbol{P}_1\alpha^{f-1} + \boldsymbol{P}_2\alpha^{f-2} + \ldots + \boldsymbol{P}_f = 0,$$

deren Coëfficienten ganze und ganzzahlige Functionen der Perioden von je $f$ Gliedern sind. Mittels dieser Gleichung kann man aus dem Ausdrucke

$$f(\alpha) = a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + \ldots + a_{\lambda-1}\alpha^{\lambda-1}$$

alle Potenzen des $\alpha$, von $\alpha^{\lambda-1}$ bis zu $\alpha^f$ hinab, eliminiren, und erhält dadurch einen Ausdruck von folgender Form:

$$(7.) \quad f(\alpha) = \varphi(\eta) + \alpha\varphi_1(\eta) + \alpha^2\varphi_2(\eta) + \ldots + \alpha^{f-1}\varphi_{f-1}(\eta),$$

wo $\varphi(\eta)$, $\varphi_1(\eta)$, $\varphi_2(\eta)$, etc. aus den Perioden von je $f$ Gliedern gebildete complexe ganze Zahlen sind. Es läfst sich auch eine bestimmte complexe Zahl $f(\alpha)$ nur auf eine einzige Weise auf diese Form bringen.

Der gefundene Satz über die Theilbarkeit der Norm durch den Primfactor $q$ läfst sich nun folgendermafsen ausdrücken:

Wenn $Nf(\alpha)$ durch den zum Exponenten $f$ gehörenden Primfactor $q$ theilbar ist, so mufs das Product der $e$ Factoren

$$(8.) \quad \begin{cases} \left(cf(\alpha) + c_1 f(\alpha^{\gamma^e}) + c_2 f(\alpha^{\gamma^{2e}}) + \ldots + c_{f-1} f(\alpha^{\gamma^{(f-1)e}})\right), \\ \left(\overset{1}{c} f(\alpha^{\gamma}) + \overset{1}{c_1} f(\alpha^{\gamma^{e+1}}) + \overset{1}{c_2} f(\alpha^{\gamma^{2e+1}}) + \ldots + \overset{1}{c_{f-1}} f(\alpha^{\gamma^{(f-1)e+1}})\right), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \left(\overset{e-1}{c} f(\alpha^{\gamma^{e-1}}) + \overset{e-1}{c_1} f(\alpha^{\gamma^{2e-1}}) + \overset{e-1}{c_2} f(\alpha^{\gamma^{3e-1}}) + \ldots + \overset{e-1}{c_{f-1}} f(\alpha^{\gamma^{fe-1}})\right) \end{cases}$$

stets durch $q$ theilbar sein, für alle beliebigen Werthe der durch $c$ bezeichneten $\lambda-1$ Coëfficienten: denn alle einzelnen Theile dieses entwickelten Products sind dem obigen Satze zufolge durch $q$ theilbar; ganz abgesehen von den Coëfficienten. Setzen wir nun für $f(\alpha)$ den gefundenen Ausdruck:

$$f(\alpha) = \varphi(\eta) + \alpha\varphi_1(\eta) + \alpha^2\varphi_2(\eta) + \ldots + \alpha^{f-1}\varphi_{f-1}(\eta)$$

und der Kürze wegen

$$(9.)\quad \begin{cases} \overset{k}{c} + \overset{k}{c_1} + \overset{k}{c_2} + \ldots + \overset{k}{c_{f-1}} = \overset{k}{C}, \\ \alpha\overset{k}{c} + \alpha^{\gamma^e}\overset{k}{c_1} + \alpha^{\gamma^{2e}}\overset{k}{c_2} + \ldots + \alpha^{\gamma^{(f-1)e}}\overset{k}{c_{f-1}} = \overset{k}{C_1}, \\ \alpha^2\overset{k}{c} + \alpha^{2\gamma^e}\overset{k}{c_1} + \alpha^{2\gamma^{2e}}\overset{k}{c_2} + \ldots + \alpha^{2\gamma^{(f-1)e}}\overset{k}{c_{f-1}} = \overset{k}{C_2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \alpha^{f-1}\overset{k}{c} + \alpha^{(f-1)\gamma^e}\overset{k}{c_1} + \alpha^{(f-1)\gamma^{2e}}\overset{k}{c_2} + \ldots + \alpha^{(f-1)\gamma^{(f-1)e}}\overset{k}{c_{f-1}} = \overset{k}{C_{f-1}}, \end{cases}$$

so verwandelt sich dieses Product in folgendes:

$$(10.)\quad \begin{cases} \left(C\varphi(\eta) + C_1\varphi_1(\eta) + C_2\varphi_2(\eta) + \ldots + C_{f-1}\varphi_{f-1}(\eta)\right) \\ \times \left(\overset{1}{C}\varphi(\eta_1) + \overset{1}{C_1}\varphi_1(\eta_1) + \overset{1}{C_2}\varphi_2(\eta_1) + \ldots + \overset{1}{C_{f-1}}\varphi_{f-1}(\eta_1)\right) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \times\left(\overset{e-1}{C}\varphi(\eta_{e-1}) + \overset{e-1}{C_1}\varphi_1(\eta_{e-1}) + \overset{e-1}{C_1}\varphi_2(\eta_{e-1}) + \ldots + \overset{e-1}{C_{f-1}}\varphi_{f-1}\varphi_{f-1}(\eta_{e-1})\right); \end{cases}$$

welches also ebenfalls durch $q$ theilbar sein mufs, und zwar für alle beliebigen Werthe der $\lambda-1$ Gröfsen $C$: denn da die mit $c$ bezeichneten Gröfsen völlig beliebig waren, so folgt vermöge der Gleichungen (9.) das Gleiche für die Coëfficienten $C$. Nimmt man diese Coëfficienten unabhängig von $\alpha$ an, und setzt allgemein $\overset{k}{C_h} = C_h$, so geht das Product (10.) in die Norm der nur aus Perioden gebildeten complexen Zahl

$$C\varphi(\eta) + C_1\varphi_1(\eta) + C_2\varphi_2(\eta) + \ldots + C_{f-1}\varphi_{(f-1)}(\eta)$$

über; und damit dieselbe den Factor $q$ habe, mufs nach (§. 2.), wenn statt der Perioden die zugehörigen Congruenzwurzeln gesetzt werden,

$$(11.)\quad C\varphi(u_r) + C_1\varphi_1(u_r) + C_2\varphi_2(u_r) + \ldots + C_{f-1}\varphi_{f-1}(u_r) \equiv 0, \text{ mod. } q,$$

sein, für irgend einen Werth von $r$. Diese Congruenz aber kann, da die Coëfficienten noch völlig beliebig sind, nicht bestehen, ohne dafs die einzelnen Glieder der Null congruent sind, also nicht ohne dafs

$$\varphi(u_r) \equiv 0, \quad \varphi_1(u_r) \equiv 0, \quad \varphi_2(u_r) \equiv 0, \quad \ldots \quad \varphi_{f-1}(u_r) \equiv 0, \text{ mod. } q,$$

ist. Umgekehrt: wenn diese $f$ Congruenzen erfüllt werden, so ist auch

$$f(\alpha)f(\alpha^\gamma)f(\alpha^{\gamma^2})\ldots f(\alpha^{\gamma^{e-1}}) \equiv 0, \text{ mod. } q,$$

also $Nf(\alpha)$ durch $q^f$ theilbar. Diese Resultate lassen sich durch folgenden Satz aussprechen:

***Wenn $Nf(\alpha)$ durch die Primzahl $q$ theilbar ist, welche zum Exponenten $f$ gehört, für den Modul $\lambda$: so müssen die $f$ Congruenzbedingungen***

$$\varphi(u_r) \equiv 0, \quad \varphi_1(u_r) \equiv 0, \quad \varphi_2(u_r) \equiv 0, \quad \ldots \quad \varphi_{f-1}(u_r) \equiv 0, \text{ mod. } q,$$

***erfüllt werden, für irgend einen Werth von r; welche Congruenzen man dadurch erhält, dafs man*** $f(\alpha)$ ***auf die Form***

$$f(\alpha) = \varphi(\eta) + \alpha\varphi_1(\eta) + \alpha^2\varphi_2(\eta) + \ldots + \alpha^{f-1}\varphi_{f-1}(\eta)$$

***bringt und statt der Perioden in*** $\varphi(\eta)$, $\varphi(\eta_1)$, $\varphi(\eta_2)$, .... ***die entsprechenden Congruenzwurzeln setzt. Umgekehrt: wenn die f Congruenzbedingungen erfüllt werden, so ist auch*** $Nf(\alpha)$ ***durch q, (also auch durch*** $q^f$***) theilbar.***

Es giebt noch eine andere, aber weniger brauchbare Art, die Bedingung auszudrücken, dafs $Nf(\alpha)$ durch $q$ theilbar sein soll. Bildet man nämlich das Product

$$f(\alpha)f(\alpha^{\gamma^e})f(\alpha^{\gamma^{2e}}) \ldots . f(\alpha^{\gamma^{(f-1)e}}) = F(\eta),$$

welches, als symmetrische Function der in einer Periode enthaltenen Wurzeln, eine Function der Perioden von je $f$ Gliedern ist, so erhält man

$$Nf(\alpha) = F(\eta)F(\eta_1)F(\eta_2) \ldots . F(\eta_{e-1}).$$

Damit nun $Nf(\alpha)$ durch $q$ theilbar sei, ist es nothwendig und hinreichend, dafs $F(u_r) \equiv 0$, mod. $q$, sei, für irgend einen Werth von $r$. Es ist bemerkenswerth, dafs hier nur eine einzige Congruenzbedingung gefunden wurde, und zwar, in Beziehung auf die Coëfficienten von $f(\alpha)$, vom $f$ten Grade, während sich oben $f$ Congruenzbedingungen vom ersten Grade für die Theilbarkeit der Norm $Nf(\alpha)$ durch die Primzahl $q$ ergaben; und da beide in gleicher Weise hinreichend und nothwendig sind, so ist zu schliefsen, dafs die eine Congruenz vom $f$ten Grade $F(u_r) \equiv 0$, mod. $q$, genau Dasselbe ausdrückt, wie die $f$ linearen Congruenzen $\varphi(u_r) \equiv 0$, $\varphi_1(u_r) \equiv 0$, .... $\varphi_{f-1}(u_r) \equiv 0$, mod. $q$, oder dafs jene eine Congruenz nicht erfüllt werden kann, ohne dafs diese $f$ Congruenzen zugleich erfüllt werden.

## §. 5.

Wenn für eine complexe Zahl $f(\alpha)$, welche auf die Form

$$f(\alpha) = \varphi(\eta) + \alpha\varphi_1(\eta) + \alpha^2\varphi_2(\eta) + \ldots + \alpha^{f-1}\varphi_{f-1}(\eta)$$

gebracht ist, die $f$ Congruenzbedingungen

$$\varphi(u_r) \equiv 0, \quad \varphi_1(u_r) \equiv 0, \quad \varphi_2(u_r) \equiv 0, \quad \ldots \quad + \varphi_{f-1}(u_r) \equiv 0, \text{ mod. } q,$$

erfüllt werden, so wollen wir dies künftig kurz so ausdrücken: es sei $f(\alpha) \equiv 0$, mod. $q$, für $\eta = u_r$. Durch Festsetzung einer einzigen Congruenzwurzel, welche einer Periode entsprechen soll, ist, da die cyklische Ordnung bei beiden stets unverändert bleibt, zugleich für jede Periode die entsprechende Congruenz-

wurzel bestimmt; oder in der einen Bestimmung für $\eta = u_r$ liegen zugleich die folgenden: $\eta_1 = u_{r+1}$, $\eta_2 = u_{r+2}$, etc.; auch $\eta_{e-r} = u$.

Hiernach ist leicht einzusehen, dafs, wenn $f(\alpha)$ als ein Product von Factoren auftritt, und einer derselben hat die Eigenschaft, congruent Null zu werden für $\eta = u_r$: dafs dann auch das entwickelte Product dieselbe Eigenschaft haben mufs. Ist nämlich

$$(1.) \quad f(\alpha)g(\alpha) = h(\alpha)$$

und $f(\alpha) \equiv 0$, mod. $q$, für $\eta = u_r$ und man bringt $f(\alpha)$ auf die Form

$$f(\alpha) = \varphi(\eta) + \alpha\varphi_1(\eta) + \alpha^2\varphi_2(\eta) + \ldots + \alpha^{f-1}\varphi_{f-1}(\eta),$$

so sind alle Glieder des Products $f(\alpha)g(\alpha)$ mit einer der complexen Zahlen $\varphi(\eta)$, $\varphi_1(\eta)$, $\varphi_2(\eta)$, etc. multiplicirt; sie werden also alle durch $q$ theilbar, für $\eta = u_r$. Um aber den umgekehrten Satz zu beweisen, nämlich, dafs, wenn $h(\alpha) \equiv 0$, mod. $q$, für $\eta = u_r$, und $g(\alpha)$ nicht congruent Null ist, für $\eta = u_r$, nothwendig $f(\alpha) \equiv 0$, mod. $q$, für $\eta = u_r$ sein mufs, setze ich

$$f(\alpha)f(\alpha^{\gamma^e})f(\alpha^{\gamma^{2e}}) \ldots f(\alpha^{\gamma^{(f-1)e}}) = F(\eta),$$
$$g(\alpha)g(\alpha^{\gamma^e})g(\alpha^{\gamma^{2e}}) \ldots g(\alpha^{\gamma^{(f-1)e}}) = G(\eta),$$
$$h(\alpha)h(\alpha^{\gamma^e})h(\alpha^{\gamma^{2e}}) \ldots h(\alpha^{\gamma^{(f-1)e}}) = H(\eta).$$

Dann erhält man aus der Gleichung $f(\alpha)g(\alpha) = h(\alpha)$:

$$(2.) \quad F(\eta)G(\eta) = H(\eta).$$

Wenn nun $h(\alpha) \equiv 0$, mod. $q$, für $\eta = u_r$ ist, so ist auch $H(\eta) \equiv 0$, mod. $q$, für $\eta = u_r$, oder (wie wir dies bisher immer kurz bezeichneten) $H(u_r) \equiv 0$, mod. $q$: also mufs, wenn in (2.) $u_r$ statt $\eta$ gesetzt wird, auch eine der beiden ganzen Zahlen $F(u_r)$ oder $G(u_r)$ durch $q$ theilbar sein; und wenn nach der Voraussetzung $g(\alpha)$ nicht $\equiv 0$, mod. $q$, für $\eta = u_r$ ist, so ist auch $G(u_r)$ nicht congruent Null, also $F(u_r) \equiv 0$, mod. $q$. Die Bedingung $F(u_r) \equiv 0$, mod. $q$, ist aber, wie zu Ende des vorigen Paragraphen gezeigt wurde, identisch mit der Bedingung $\varphi(u_r) \equiv 0$, $\varphi_1(u_r) \equiv 0$, $\varphi_2(u_r) \equiv 0$, .... $\varphi_{f-1}(u_r) \equiv 0$, mod. $q$, also auch identisch mit der Bedingung $f(\alpha) \equiv 0$, mod. $q$, für $\eta = u_r$.

Da nun bewiesen ist, dafs die Bedingung $f(\alpha) \equiv 0$, mod. $q$, für $\eta = u_r$ stets dieselbe bleibt, es mag $f(\alpha)$ in entwickelter Form auftreten, oder in Form eines Products aus zweien, und folglich auch aus mehreren complexen Zahlen: so folgt von selbst der Satz:

***Wenn eine aus Factoren bestehende complexe Zahl durch q theilbar ist, so müssen für alle Werthe*** $\eta = u$, $\eta = u_1$, $\eta = u_2$, .... $\eta = u_{e-1}$ ***irgend einige ihrer Factoren congruent Null werden, mod. q.***

und umgekehrt:

***Wenn für jeden der Werthe*** $\eta = u$, $\eta = u_1$, $\eta = u_2$, .... $\eta = u_{e-1}$ ***irgend einer der Factoren einer complexen Zahl congruent Null wird, mod.*** $q$***: so enthält dieselbe den realen Factor*** $q$.

Die $f$ Congruenzbedingungen, welche wir in dem Ausdrucke $f(\alpha) \equiv 0$, mod. $q$, für $\eta = u_r$ zusammenfassen, lassen sich noch auf eine andere Weise sehr einfach ausdrücken. Ist nämlich $\psi(\eta)$ eine complexe Zahl von der Art, wie wir sie in (§. 3.) fanden, nemlich, dafs die Norm derselben oder das Product $\psi(\eta)\psi(\eta_1)\psi(\eta_2)\ldots\psi(\eta_{e-1})$ durch $q$ theilbar sei, nicht aber durch $q^2$: so mufs, wie oben gezeigt, $\psi(u_r) \equiv 0$, mod. $q$, sein, für irgend einen bestimmten Werth von $r$. Wird nun, wie in (§. 3.),

$$\Psi(\eta) = \psi(\eta_1)\psi(\eta_2)\ldots\psi(\eta_{e-1})$$

gesetzt, so behaupte ich, ***dafs die Bedingung*** $f(\alpha) \equiv 0$, mod. $q$, für $u = \eta_r$ ***identisch ist mit der Bedingung*** $f(\alpha)\Psi(\eta) \equiv 0$, mod. $q$. Es ist nämlich $\Psi(\eta)$, weil es die $e-1$ Factoren $\psi(\eta_1)$, $\psi(\eta_2)$, .... $\psi(\eta_{e-1})$ enthält, für alle Werthe $\eta = u$, $u_1$, $u_2$, .... $u_{e-1}$, mit Ausnahme des Werths $\eta = u_r$, durch $q$ theilbar: wenn also $f(\alpha) \equiv 0$, mod. $q$ ist, für $\eta = u_r$, so ist das Product $f(\alpha)\Psi(\eta)$ für alle Werthe $\eta = u$, $u_1$, $u_2$, .... $u_{e-1}$, ohne Ausnahme, congruent Null, mod. $q$, und enthält also den realen Factor $q$. Wenn ferner, umgekehrt, $f(\alpha)\Psi(\eta)$ durch $q$ theilbar ist, so müssen die beiden Factoren zusammen für alle Werthe $\eta = u$, $u_1$, $u_2$, .... $u_{e-1}$ durch $q$ theilbar sein, und da $\Psi(\eta)$ für $\eta = u_r$ nicht durch $q$ theilbar ist, so mufs nothwendig der andere Factor $f(\alpha) = 0$, mod. $q$, für $\eta = u_r$ es sein.

## §. 6.

Die Coëfficienten einer complexen Zahl von der Form

$$\varphi(\eta) = a\eta + a_1\eta_1 + a_2\eta_2 + \ldots + a_{e-1}\eta_{e-1}$$

lassen sich, wie in (§. 2.) gezeigt, auf unendlich viele verschiedene Arten so bestimmen, dafs die Norm $N\varphi(\eta)$ durch die zum Exponenten $f$ gehörende Primzahl $q$ theilbar, also ein Vielfaches von $q$ wird. In vielen Fällen, aber nicht immer, gelingt es sogar, complexe Zahlen zu finden, deren Norm die reale Primzahl $q$ selbst ist, so dafs $q = \varphi(\eta)\varphi(\eta_1)\varphi(\eta_2)\ldots\varphi(\eta_{e-1})$; die complexe Zahl $\varphi(\eta)$ mufs alsdann, wenn statt der Perioden die entsprechenden Congruenzwurzeln gesetzt werden, durch $q$ theilbar werden, so dafs $\varphi(u_r) \equiv 0$, mod. $q$, ist, für irgend einen bestimmten Werth von $r$. Wenn nun die Norm von $\varphi(\eta)$ gleich $q$ ist, so ist $\varphi(\eta)$ ein nicht weiter in Factoren zerlegbarer

Primfactor der realen Zahl $q$. Wäre nämlich $\varphi(\eta)$ in zwei complexe Factoren zerlegbar, so dafs $\varphi(\eta) = f(\alpha)$ wäre, so müfste zunächst, weil $\varphi(\eta) \equiv 0$, mod. $q$, für $\eta = u_r$ ist, auch einer der beiden Factoren, zu welchen ich $f(\alpha)$ nehme, congruent Null sein, mod. $q$, für $\eta = u_r$. Aus $\varphi(\eta) = f(\alpha)g(\alpha)$ folgt aber weiter, wenn man $\alpha$ in $\alpha^\gamma, \alpha^{\gamma^2}, \ldots \alpha^{\gamma^{e-1}}$ verwandelt und die Gleichungen multiplicirt:

$$\varphi(\eta)\varphi(\eta_1)\varphi(\eta_2)\ldots\varphi(\eta_{e-1})$$
$$= f(\alpha)f(\alpha^\gamma)f(\alpha^{\gamma^2})\ldots f(\alpha^{\gamma^{e-1}})g(\alpha)g(\alpha^\gamma)g(\alpha^{\gamma^2})\ldots g(\alpha^{\gamma^{e-1}}).$$

Da nun $f(\alpha) \equiv 0$, für $\eta = u_r$ ist, so ist das Product $f(\alpha)f(\alpha^\gamma)f(\alpha^{\gamma^2})\ldots f(\alpha^{\gamma^{e-1}})$ durch $q$ theilbar, also gleich $qF(\alpha)$; und da $\varphi(\eta)\varphi(\eta_1)\varphi(\eta_2)\ldots\varphi(\eta_{e-1}) = q$ ist, so erhält man, nach Weglassung des gemeinschaftlichen Factors $q$:

$$1 = F(\alpha)g(\alpha)g(\alpha^\gamma)g(\alpha^{\gamma^2})\ldots g(\alpha^{\gamma^{e-1}}):$$

es müssen also alle Factoren rechts nur complexe Einheiten und mithin mufs namentlich $g(\alpha)$ eine complexe Einheit sein. Wenn man demnach die Zahl $\varphi(\eta)$, deren Norm die Primzahl $q$ ist, auf irgend eine Weise in zwei Factoren zerlegt, so ist einer derselben stets nur eine complexe Einheit, und $\varphi(\eta)$ ist also wirklich eine complexe ***Primzahl.*** Wenn nun irgend eine complexe Zahl $f(\alpha)$ diesen Primfactor $\varphi(\eta)$ der realen Primzahl $q$ als Factor enthält, so dafs $f(\alpha) = \varphi(\eta)g(\alpha)$ ist, so mufs $f(\alpha) \equiv 0$, mod. $q$, für $\eta = u_r$ sein, weil $\varphi(u_r) \equiv 0$, mod. $q$, ist. Eine Umkehrung dieses Satzes läfst sich nicht ohne Weiteres aufstellen; denn in vielen Fällen existirt ein solcher Primfactor von $q$ nicht, während die Congruenzbedingung $f(\alpha) \equiv 0$, mod. $q$, für $\eta = u_r$ wirklich erfüllt wird. Diese Congruenzbedingung aber, als die bleibende und jener Zufälligkeit, ob $q$ sich als Product von $e$ conjugirten complexen Zahlen darstellen lasse, nicht unterworfene Eigenschaft einer complexen Zahl, soll nun als Definition der complexen Primfactoren benutzt werden, welche selbst sodann entweder als wirkliche complexe Zahlen für sich darstellbar sein können, oder auch nicht; in welchem letzteren Falle sie ***ideale*** Primfactoren genannt werden sollen. Anstatt der Congruenzbedingung selbst aber werden wir den Ausdruck derselben am Ende des vorigen Paragraphen wählen, weil dieser sich am leichtesten auch auf den Fall ausdehnen läfst, wo einer und derselbe Primfactor mehrmals in einer complexen Zahl enthalten ist.

Die allgemeine Definition der realen oder idealen Primfactoren einer gegebenen complexen Zahl ist also folgende:

***Es sei $\psi(\eta)$ eine aus den $e$ Perioden von je $f$ Gliedern gebildete complexe Zahl, von der Art, dafs die Norm $\psi(\eta)\psi(\eta_1)\psi(\eta_2)\ldots\psi(\eta_{e-1})$***

*durch die zum Exponenten f gehörende reale Primzahl q theilbar ist, nicht aber durch $q^2$, so wie, dafs $\psi(u) \equiv 0$, mod. q: dann setze man*

$$\Psi(\eta) = \psi(\eta_1)\psi(\eta_2)\ldots\psi(\eta_{e-1}).$$

*Wenn nun irgend eine complexe Zahl $f(\alpha)$ die Eigenschaft hat, dafs das Product $f(\alpha)\Psi(\eta_r)$ durch q theilbar ist, so soll dies so ausgedrückt werden: es enthalte $f(\alpha)$ den zu $\eta_r = u$ gehörenden Primfactor von q. Wenn ferner $f(\alpha)$ die Eigenschaft hat, dafs $f(\alpha)(\Psi(\eta_r))^\mu$ durch $q^\mu$ theilbar ist, aber $f(\alpha)(\Psi(\eta_r))^{\mu+1}$ nicht theilbar durch $q^{\mu+1}$, so soll dies heifsen: es enthalte $f(\alpha)$ den zu $\eta_r = u$ gehörenden Primfactor von q genau $\mu$ mal.*

Die Zweckmäfsigkeit dieser Definition kann sich erst aus der auf dieselbe gegründeten Theorie ergeben; in welcher wir zeigen werden, dafs man mit den Eigenschaften der complexen Zahlen, welche wir so eben als Primfactoren derselben definirten, und welche in vielen Fällen auch *wirkliche* Primfactoren derselben geben, genau eben so rechnen kann, wie mit den ganzzahligen Primfactoren der zusammengesetzten ganzen Zahlen. Zunächst aber ist hier noch nachzuweisen, dafs diese Primfactoren von den *besondern* Eigenschaften der zu ihrer Auffindung zu benutzenden complexen Zahl $\Psi(\eta)$ ganz unabhängig sind, oder dafs man immer genau dieselben Primfactoren erhält, auch wenn man statt der complexen Zahl $\Psi(\eta)$ eine andere Zahl von denselben oben angegebenen *allgemeinen* Eigenschaften anwendet.

Es sei also $\Psi'(\eta)$ eine andere complexe Zahl, von der Art, dafs $\Psi'(\eta)\Psi'(\eta_1)\Psi'(\eta_2)\ldots\Psi'(\eta_{e-1})$ durch $q$, aber nicht durch $q^2$ theilbar ist, und $\Psi'(u) \equiv 0$, mod. $q$; auch sei $\Psi'(\eta) = \psi(\eta_1)\psi(\eta_2)\ldots\psi(\eta_{e-1})$: so wird behauptet, dafs, wenn $f(\alpha)(\Psi(\eta_r))^\mu$ durch $q^\mu$ theilbar ist, nicht aber $f(\alpha)(\Psi(\eta_r))^{\mu+1}$ durch $q^{\mu+1}$, auch $f(\alpha)(\Psi'(\eta_r))^\mu$ durch $q^\mu$ theilbar sein mufs, aber $f(\alpha)(\Psi'(\eta_r))^{\mu+1}$ nicht theilbar durch $q^{\mu+1}$. Der Voraussetzung zufolge hat man

$$f(\alpha)(\Psi(\eta_r))^\mu = q^\mu Q(\alpha),$$

und $Q(\alpha)\Psi(\eta_r)$ ist nicht theilbar durch $q$, oder, was Dasselbe ist: $Q(\alpha)$ ist nicht congruent Null, mod. $q$, für $\eta_r = u$. Multiplicirt man nun mit $(\psi(\eta_r))^\mu(\Psi'(\eta_r))^\mu$, so ergiebt sich

$$f(\alpha)(\psi(\eta_r))^\mu(\Psi(\eta_r))^\mu(\Psi'(\eta_r))^\mu = q^\mu Q(\alpha)(\psi(\eta_r))^\mu(\Psi'(\eta_r))^\mu.$$

Nun ist $\psi(\eta_r)\Psi(\eta_r)$, die Norm von $\psi(\eta)$, gleich $qP$; wo $P$ eine nicht durch $q$ theilbare ganze Zahl ist; ferner ist $\psi(\eta_r)\Psi'(\eta_r) = qR(\eta_r)$, d. h. eine durch $q$ theilbare complexe Zahl. Setzt man diese Ausdrücke in die Gleichung, und

läfst den gemeinschaftlichen Factor $q^\mu$ weg, so erhält man

$$f(\alpha)\,\Psi'(\eta_r))^\mu P^\mu = q^\mu Q(\alpha)(R(\eta_r))^\mu;$$

und da $P$ nicht durch $q$ theilbar ist, so folgt, dafs $f(\alpha)(\Psi'(\eta_r))^\mu$ durch $q^\mu$ theilbar sein mufs. Multiplicirt man nun noch einmal mit $\Psi'(\eta_r)$, so erhält man

$$f(\alpha)(\Psi'(\eta_r))^{\mu+1} P^\mu = q^\mu Q(\alpha)(R(\eta_r))^\mu \Psi'(\eta_r).$$

Es ist aber $Q(\alpha)(R(\eta_r))^\mu \Psi'(\eta_r)$ nicht theilbar durch $q$, weil keiner der drei Factoren für $\eta_r = u$ mit $q$ aufgeht: also ist auch $f(\alpha)(\Psi'(\eta_r))^{\mu+1}$ nicht theilbar durch $q^{\mu+1}$. Es ist daher in der That Dasselbe, ob man die complexe Zahl $\Psi'(\eta)$, oder $\Psi'(\eta)$, zur Untersuchung des in $f(\alpha)$ enthaltenen Primfactors anwendet.

Da wir die Bedingung, dafs $f(\alpha)$ den zu $\eta_r = u$ gehörenden Primfactor von $q$ einmal enthalte, durch $f$ Congruenzen ausgedrückt haben, welchen die Coëfficienten der complexen Zahl $f(\alpha)$ genügen müssen, so wollen wir hier auch zeigen, wie die Bedingung, dafs $f(\alpha)$ einen solchen Primfactor mehreremale enthalte, durch Congruenzen auszudrücken sei. Bringt man $f(\alpha)$ wieder auf die Form

$$f(\alpha) = \varphi(\eta) + \alpha\varphi_1(\eta) + \alpha^2\varphi_2(\eta) + \ldots + \alpha^{f-1}\varphi_{f-1}(\eta),$$

so ergiebt sich

$$f(\alpha)\,\Psi(\eta_r) = \varphi(\eta)\,\Psi(\eta_r) + \alpha\varphi_1(\eta)\,\Psi(\eta_r) + \ldots + \alpha^{f-1}\varphi_{f-1}(\eta)\,\Psi(\eta_r).$$

Wenn nun $f(\alpha)$ den zu $\eta_r = u$ gehörenden Primfactor der zum Exponenten $f$ gehörenden realen Primzahl $q$ einmal enthält, so dafs $f(\alpha)\,\Psi(\eta_r)$ durch $q$ theilbar ist, so müssen, wie (§. 4.) zeigt, $\varphi(\eta)$, $\varphi_1(\eta)$, .... $\varphi_{f-1}(\eta)$ alle denselben idealen Primfactor enthalten: also müssen auch $\varphi(\eta)\,\Psi(\eta_r)$, $\varphi_1(\eta)\,\Psi(\eta_r)$, .... $\varphi_{f-1}(\eta)\,\Psi(\eta_r)$ alle durch $q$ theilbar sein. Setzt man demnach

$$\varphi(\eta)\,\Psi(\eta_r) = q\varphi'(\eta),\quad \varphi_1(\eta)\,\Psi(\eta_r) = q\varphi_1'(\eta),\quad \ldots\quad \varphi_{f-1}(\eta)\,\Psi(\eta_r) = q\varphi_{f-1}'(\eta),$$

so erhält man

$$f(\alpha)\,\Psi(\eta_r) = q[\varphi'(\eta) + \alpha\varphi_1'(\eta) + \alpha^2\varphi_2'(\eta) + \ldots + \alpha^{f-1}\varphi_{f-1}'(\eta)].$$

Wenn nun $f(\alpha)$ den zu $\eta_r = u$ gehörenden Primfactor von $q$ zweimal enthält, so ist $f(\alpha)(\Psi(\eta_r))^2$ durch $q^2$ theilbar; multiplicirt man daher noch einmal mit $\Psi(\eta_r)$, so müssen wieder $\varphi'(\eta)\Psi(\eta_r)$, $\varphi_1'(\eta)\Psi(\eta_r)$, .... $\varphi_{f-1}'(\eta)\Psi(\eta_r)$ alle einzeln durch $q$ theilbar sein, folglich $\varphi(\eta)(\Psi(\eta_r))^2$, $\varphi_1(\eta)(\Psi(\eta_r))^2$, .... $\varphi_{f-1}(\eta)(\Psi(\eta_r))^2$ alle theilbar durch $q^2$. So fortfahrend, zeigt sich, dafs, wenn $f(\alpha)(\Psi(\eta_r))^\mu$ durch $q^\mu$ theilbar ist, allemal auch $\varphi(\eta)(\Psi(\eta_r))^\mu$, $\varphi_1(\eta)(\Psi(\eta_r))^\mu$, .... $\varphi_{f-1}(\eta)(\Psi(\eta_r))^\mu$ einzeln durch $q^\mu$ theilbar sein müssen; oder, was Dasselbe ist: wenn $f(\alpha)$ den

zu $\eta_r = u$ gehörenden Primfactor von $q$ $\mu$mal enthält, so müssen die complexen, aus den Perioden gebildeten Zahlen $\varphi(\eta)$, $\varphi_1(\eta)$, $\varphi_2(\eta)$, .... $\varphi_{f-1}(\eta)$ den nämlichen Primfactor jede $\mu$mal enthalten. Entwickelt man nun das Product $\varphi_k(\eta)(\Psi(\eta_r))^\mu$ in linearer Form, so dafs

$$\varphi_k(\eta)(\Psi(\eta_r))^\mu = C\eta + C_1\eta_1 + C_2\eta_2 + .... + C_{e-1}\eta_{e-1},$$

so folgt sehr leicht, dafs

$$\varphi_k(\eta)(\Psi(\eta_r))^\mu + \varphi_k(\eta_1)(\Psi(\eta_{r+1}))^\mu + .... + \varphi_k(\eta_{e-1})(\Psi(\eta_{r+e-1}))^\mu = -(C + C_1 + C_2 + .... + C_{e-1})$$

ist. Multiplicirt man noch einmal mit $(\Psi(\eta_r))^\mu$ und erwägt, dafs $\Psi(\eta_r)\Psi(\eta_s)$ immer durch $q$ theilbar ist, den einen Fall $r = s$ ausgenommen, so erhält man

$$\varphi_k(\eta)(\Psi(\eta_r))^{2\mu} \equiv -(C + C_1 + C_2 + .... + C_{e-1})(\Psi(\eta_r))^\mu, \text{ mod. } q^\mu.$$

Hieraus folgt, dafs die Bedingung: $\varphi(\eta_r)(\Psi(\eta_r))^\mu$ sei durch $q^\mu$ theilbar, identisch ist mit der Bedingung $C + C_1 + C_2 + .... + C_{e-1} \equiv 0$, mod. $q^\mu$. Also die Bedingung, dafs $f(\alpha)$ den zu $\eta_r = u$ gehörenden (idealen) Primfactor von $q$ $\mu$mal enthalte, wird durch $f$ Congruenzen für den Modul $q^n$ ausgedrückt, welche unter den Coëfficienten der complexen Zahl $f(\alpha)$ Statt finden müssen. Wir bemerken noch ausdrücklich, dafs diese Congruenzen in Beziehung auf die Coëfficienten von $f(\alpha)$ nur vom ersten Grade sind; denn $\varphi_k(\eta)$ enthält dieselben nur linear, und $(\Psi(\eta_r))^\mu$ enthält sie gar nicht; also enthalten auch $C$, $C_1$, $C_2$, .... $C_{e-1}$ die Coëfficienten nur in linearer Weise.

## §. 7.

Wir haben nun dieselben einfachen Sätze, welche für die Rechnung mit den realen ganzen Primfactoren der ganzen Zahlen gelten, für die in dem vorigen Paragraphen definirten idealen oder wirklichen Primfactoren der complexen Zahlen aufzustellen und zu beweisen. Es werde zunächst folgender Satz bewiesen:

***Das entwickelte Product zweier oder mehrerer complexen Zahlen hat genau dieselben Primfactoren wie die Factoren des Products zusammengenommen.***

Es seien $f(\alpha)$ und $g(\alpha)$ zwei complexe Factoren, $h(\alpha)$ das entwickelte Product derselben, so dafs $f(\alpha)g(\alpha) = h(\alpha)$. Es enthalte $f(\alpha)$ den zu $\eta_r = u$ gehörenden Primfactor von $q$ genau $\mu$mal, $g(\alpha)$ denselben Factor genau $\nu$mal: so wird behauptet, dafs $h(\alpha)$ denselben genau $\mu + \nu$mal enthält. Nach der Voraussetzung ist $f(\alpha)(\Psi(\eta_r))^\mu = q^\mu Q(\alpha)$ und $g(\alpha)(\Psi(\eta_r))^\nu = q^\nu R(\alpha)$, und

weder $Q(\alpha)\Psi(\eta_r)$ noch $R(\alpha)\Psi(\eta_r)$ ist durch $q$ theilbar, weil sonst $f(\alpha)$ oder $g(\alpha)$ den zu $\eta_r = u$ gehörenden Primfactor von $q$, $\mu+1$ mal oder $\nu+1$ mal enthalten würden; gegen die Voraussetzung. Hieraus folgt $f(\alpha)g(\alpha)(\Psi(\eta_r))^{\mu+\nu} = q^{\mu+\nu}Q(\alpha)R(\alpha)$, also auch $h(\alpha)(\Psi(\eta_r))^{\mu+\nu} = q^{\mu+\nu}Q(\alpha)R(\alpha)$. Multiplicirt man noch einmal mit $\Psi(\eta_r)$, so ist $h(\alpha)(\Psi(\eta_r)^{\mu+\nu+1}$ auch durch keine höhere Potenz als durch $q^{\mu+\nu}$ theilbar; denn $Q(\alpha)R(\alpha)\Psi(\eta_r)$ ist nicht durch $q$ theilbar, weil für $\eta_r = u$ keiner der drei Factoren dieses Products der Null congruent wird. Was nun hier von einem beliebigen idealen Primfactor bewiesen ist, gilt offenbar für alle; und da man ferner auch jeden der Factoren des Products wieder in Factoren zerfället sich vorstellen kann, so ist klar, dafs der aufgestellte Satz auch eben so für jedes Product beliebig vieler Factoren gilt.

Dafs eine complexe Zahl, welche als Product mehrerer Factoren auftritt, durch $q$ theilbar ist, wenn sie alle $e$ ideale Primfactoren von $q$ enthält, und nicht durch $q$ theilbar, wenn sie irgend einen dieser Primfactoren nicht enthält, ist schon oben in (§. 5.) gezeigt worden; nur ist daselbst noch nicht der Ausdruck *idealer Primfactor*, sondern statt dessen die ihm gleichbedeutende Congruenzbedingung gebraucht worden. Wir erweitern hier den Satz wie folgt:

***Wenn eine complexe Zahl $f(\alpha)$ alle idealen Primfactoren von $q$ enthält, und zwar denjenigen, welcher am wenigsten oft darin vorkommt, $\mu$ mal, so ist die Zahl durch $q^\mu$ theilbar.***

Nach der Voraussetzung hat man folgende Congruenzen:

$$f(\alpha)(\Psi(\eta))^\mu \equiv 0,\ f(\alpha)(\Psi(\eta_1))^\mu \equiv 0,\ \ldots.\ f(\alpha)(\Psi(\eta_{e-1}))^\mu \equiv 0,\ \text{mod. } q^\mu:$$

also ist auch die Summe.

$$f(\alpha)[(\Psi(\eta))^\mu + (\Psi(\eta_1))^\mu + \ldots. + (\Psi(\eta_{e-1}))^\mu] \equiv 0,\ \text{mod. } q^\mu.$$

Der Ausdruck in den Klammern ist aber eine reale ganze Zahl, welche nicht durch $q$ theilbar ist, weil sie sogar, wie leicht zu zeigen, keinen einzigen idealen Primfactor von $q$ enthält: also mufs $f(\alpha)$ durch $q^\mu$ theilbar sein; wie es behauptet wurde.

***Wenn die complexe Zahl $f(\alpha)$ genau $m$ ideale Primfactoren der realen, zum Exponenten $f$ gehörenden Primzahl $q$ enthält, sie mögen verschieden, oder zum Theil, oder alle dieselben sein: so enthält die Norm $Nf(\alpha)$ den Factor $q^{mf}$; aber keine höhere Potenz von $q$.***

Die conjugirten complexen Zahlen $f(\alpha)$, $f(\alpha^\gamma)$, $f(\alpha^{\gamma^2})$, $\ldots$ $f(\alpha^{\gamma^{\lambda-2}})$ enthalten alle gleich viele, und zwar jede genau $m$ ideale Primfactoren von $q$.

Ändert man nämlich nur die Benennungen der Primfactoren in $f(\alpha^{\gamma^h})$, jeden um eine Stufe, so erhält man die in $f(\alpha^{\gamma^{h+1}})$ enthaltenen Primfactoren. Das Product aller dieser $\lambda-1$ conjugirten Factoren, welches gleich $Nf(\alpha)$ ist, mufs also genau $(\lambda-1)m$, das heifst $e.f.m$ ideale Primfactoren von $q$ enthalten. Ferner ist leicht zu sehen, dafs in diesem Producte alle $e$ verschiedenen Primfactoren von $q$ gleichvielmal vorkommen, weil sonst $Nf(\alpha)$ gar nicht einmal eine ganze Zahl sein könnte. Es mufs also jeder dieser Primfactoren genau $mf$ mal vorkommen, und folglich mufs $Nf(\alpha)$ genau durch $q^{fm}$ theilbar sein.

Hieraus folgt von selbst der wichtige Satz:

*Jede gegebene complexe Zahl enthält nur eine endliche bestimmte Anzahl (idealer) Primfactoren.*

Umgekehrt aber ist, wenn die idealen Primfactoren einer complexen Zahl bekannt sind, zu untersuchen, ob dieselben nur einer einzigen bestimmten, oder auch verschiedenen complexen Zahlen angehören können. Sind $f(\alpha)$ und $\varphi(\alpha)$ zwei complexe Zahlen, welche genau dieselben (idealen) Primfactoren enthalten, so ist zunächst aus dem so eben bewiesenen Satze klar, dafs die Normen derselben gleich sein müssen, also dafs $Nf(\alpha) = N\varphi(\alpha)$ sein mufs. Es mag nun $f(\alpha)$ sowohl, als $\varphi(\alpha)$, $m$ Primfactoren der zum Exponenten $f$ gehörenden Primzahl $q$ enthalten, $m'$ Primfactoren der zum Exponenten $f'$ gehörenden Primzahl $q$, $m''$ Primfactoren der zum Exponenten $f''$ gehörenden Primzahl $q''$, etc., so ist:

$$Nf(\alpha) = N\varphi(\alpha) = q^{mf}.q'^{m'f'}.q''^{m''f''}\ldots.$$

Da $f(\alpha)$ dieselben (idealen) Primfactoren enthält wie $\varphi(\alpha)$, so mufs auch $f(\alpha)\varphi(\alpha^g)\varphi(\alpha^{g^2})\ldots.\varphi(\alpha^{g^{\lambda-2}})$ genau dieselben enthalten wie $N\varphi(\alpha)$: also mufs es alle (idealen) Primfactoren von $q$ enthalten, jeden $mf$ mal, alle Primfactoren von $q'$, jeden $m'f'$ mal, alle Primfactoren von $q''$, jeden $m''f''$ mal u. s. w.; mithin mufs, nach einem oben bewiesenen Satze, $f(\alpha)\varphi(\alpha^g)\varphi(\alpha^{g^2})\ldots.\varphi(\alpha^{g^{\lambda-2}})$ durch $q^{mf}$ und eben so durch $q'^{m'f'}$, durch $q''^{m''f''}$ u. s. w. theilbar sein, folglich auch durch das Product davon, das heifst durch $N\varphi(\alpha)$. Es ist demnach

$$\frac{f(\alpha)\varphi(\alpha^g)\varphi(\alpha^{g^2})\ldots.\varphi(\alpha^{g^{\lambda-2}})}{N\varphi(\alpha)} = \frac{f(\alpha)}{\varphi(\alpha)} = E(\alpha);$$

wo $E(\alpha)$ eine ganze complexe Zahl bedeutet. Hieraus folgt weiter

$$f(\alpha) = \varphi(\alpha)E(\alpha) \quad \text{und} \quad Nf(\alpha) = N\varphi(\alpha).NE(\alpha),$$

und da $N\varphi(\alpha) = Nf(\alpha)$ ist, so folgt

$$NE(\alpha) = 1;$$

also ist $E(\alpha)$ eine complexe Einheit und wir haben folgenden Satz:

***Zwei complexe Zahlen, welche genau dieselben (idealen) Primfactoren haben, unterscheiden sich nur durch eine complexe Einheit, welche als Factor hinzutreten kann.***

Es möge jetzt ein Divisor $\varphi(\alpha)$ genau dieselben (idealen) Primfactoren haben, welche wir so eben für diese complexe Zahl annahmen; ein Dividendus $f(\alpha)$ aber möge nicht nur dieselben Factoren haben, sondern aufser diesen noch andere, oder auch die nemlichen mehrmals: dann läfst sich leicht zeigen, dafs $f(\alpha)$ durch $\varphi(\alpha)$ theilbar, d. h. dafs der Quotient eine complexe *ganze* Zahl ist. Bringt man nämlich den Quotienten wieder auf die Form

$$\frac{f(\alpha)}{\varphi(\alpha)} = \frac{f(\alpha)\varphi(\alpha^g)\varphi(\alpha^{g^2})\ldots\ldots\varphi(\alpha^{g^{\lambda-2}})}{N\varphi(\alpha)},$$

so hat der Zähler $f(\alpha)\varphi(\alpha^g)\varphi(\alpha^{g^2})\ldots\ldots\varphi(\alpha^{g^{\lambda-2}})$ alle (idealen) Primfactoren, welche der Nenner $N\varphi(\alpha)$ enthält; denn $f(\alpha)$ enthält der Voraussetzung nach alle Primfactoren von $\varphi(\alpha)$. Dieser Zähler enthält also alle Primfactoren von $q$, und zwar jeden $m$ mal; weshalb er denn durch $q^{mf}$ theilbar sein mufs. Ferner enthält er alle Primfactoren von $q'$, und zwar jeden $m'$ mal, weshalb er durch $q'^{m'f'}$ theilbar sein mufs, u. s. w. Der Zähler enthält also die ganze Zahl $q^{mf}q'^{m'f'}q''^{m''f''}\ldots\ldots$ als Factor, welche gleich $N\varphi(\alpha)$ ist: folglich ist

$$\frac{f(\alpha)}{\varphi(\alpha)} = Q(\alpha),$$

und $Q(\alpha)$ ist eine complexe ganze Zahl. Hieraus folgt weiter $f(\alpha) = \varphi(\alpha)Q(\alpha)$; und da das Product die idealen Primfactoren der beiden Factoren zusammen enthält, so folgt, dafs $Q(\alpha)$ genau alle diejenigen Primfactoren enthalten mufs, welche den Überschufs der Primfactoren des Dividendus $f(\alpha)$ über die des Divisors $\varphi(\alpha)$ ausmachen. Wir erhalten also folgenden Satz:

***Eine complexe Zahl ist durch eine andere theilbar, wenn alle (idealen) Primfactoren des Divisors auch im Dividendus enthalten sind, und der Quotient enthält genau den Überschufs der (idealen) Primfactoren des Dividendus über die des Divisors.***

Aufser den hier behandelten Primfactoren derjenigen Primzahlen, welche zu Divisoren von $\lambda-1$ für den Modul $\lambda$ gehören, müssen noch die Primfactoren von $\lambda$ selbst, besonders erwähnt werden. Da

$$(x-\alpha)(x-\alpha^2)\ldots\ldots(x-\alpha^{\lambda-1}) = x^{\lambda-1}+x^{\lambda-2}+\ldots\ldots+x+1$$

ist, so erhält man, wenn man $x=1$ setzt:

$$(1-\alpha)(1-\alpha^2)(1-\alpha^3)\ldots\ldots(1-\alpha^{\lambda-1}) = \lambda.$$

Es sind demnach $1-\alpha$, $1-\alpha^2$, etc. Factoren von $\lambda$, und zwar Primfactoren, weil, wenn $1-\alpha = f(\alpha)\varphi(\alpha)$ gesetzt wird, auch $Nf(\alpha)\cdot N\varphi(\alpha) = \lambda$ sein mufs; woraus folgt, dafs einer der beiden ganzzahligen Factoren $Nf(\alpha)$ oder $N\varphi(\alpha)$ gleich Eins, also dafs eine der beiden complexen Zahlen $f(\alpha)$ oder $\varphi(\alpha)$ eine complexe Einheit sein mufs. Diese Primfactoren von $\lambda$ haben das Eigenthümliche, dafs sie, wenn man die Einheiten abrechnet, mit welchen sie multiplicirt vorkommen, einander gleich sind; denn es ist $1-\alpha^n = (1-\alpha)(1+\alpha+\alpha^2+\ldots+\alpha^{n-1})$, und $1+\alpha+\alpha^2+\ldots+\alpha^{n-1}$ ist eine complexe Einheit. Es ist also hier niemals die Frage, welche Primfactoren von $\lambda$ in einer complexen Zahl enthalten sind, sondern nur, wie viele derselben es sind. Ist $f(\alpha)$ irgend eine complexe Zahl, so hat man offenbar

$$(f(\alpha))^\lambda = f(1), \text{ mod. } \lambda.$$

Wenn nun $f(\alpha)$ einen Primfactor von $\lambda$ enthält, so ist $(f(\alpha))^\lambda$, weil es deren $\lambda$ hat, durch $\lambda$ theilbar; mithin mufs auch $f(1)$, d. h. die Summe aller Coëfficienten von $f(\alpha)$, durch $\lambda$ theilbar sein. Wenn aber diese Bedingung erfüllt ist, so kann man durch mehrmalige Addition oder Subtraction der Gleichung $1+\alpha+\alpha^2+\ldots+\alpha^{\lambda-1} = 0$ diese Summe der Coëfficienten gleich Null machen; und alsdann ist die complexe Zahl offenbar durch $1-\alpha$ theilbar; sogar wenn $\alpha$ eine belibige veränderliche Gröfse bezeichnet. Will man daher wissen, wie viele Primfactoren von $\lambda$ eine complexe Zahl enthalte, so hat man nur zu untersuchen, wie viele mal nach einander sie sich durch $1-\alpha$ dividiren lasse.

## §. 8.

Nachdem in dem vohergehenden Paragraphen die einfachen Rechnungsregeln für die Primfactoren der complexen Zahlen gefunden worden, (welche stets dieselben sind, es mögen die Primfactoren für sich als complexe Zahlen darstellbar sein, oder nur ideale) wollen wir jetzt noch über die Wirklichkeit oder Idealität der durch ihre Primfactoren gegebenen complexen Zahlen einige Untersuchungen anstellen, bei welchen alles hauptsächlich nur auf die eine Hauptfrage ankommen wird: ***Welche ideale Primfactoren setzen sich zu wirklichen complexen Zahlen zusammen; und welche nicht?***

Das Product aller conjugirten idealen Primfactoren einer gegebenen realen Primzahl $q$ ist stets eine wirkliche complexe Zahl, und zwar die Zahl $q$ selbst, welche auch noch eine complexe Einheit zum Factor haben kann. Die Zahl $q$ enthält nämlich wirklich nach unserer Definition alle conjugirten Primfactoren von $q$, deren Anzahl gleich $e$ ist, wenn $q$ zum Exponenten $f$ gehört, mod. $\lambda$, und $ef = \lambda - 1$ ist.

Ist ferner $\mathfrak{I}(\alpha)$ irgend eine (ideale) complexe Zahl, welche beliebige gegebene Primfactoren enthält, so ist immer die Norm

$$N\mathfrak{I}(\alpha) = \mathfrak{I}(\alpha).\mathfrak{I}(\alpha^{\gamma}).\mathfrak{I}(\alpha^{\gamma^2}).\ldots.\mathfrak{I}(\alpha^{\gamma^{\lambda-1}})$$

eine ***wirkliche*** Zahl, und zwar: Wenn $\mathfrak{I}(\alpha)$ den zu $u = \eta_r$ gehörenden Primfactor von $q$, welcher zum Exponenten $f$ gehört, $\mu$mal enthält, ferner den zu $u' = \eta'_{r'}$ gehörenden Primfactor von $q'$, welcher zum Exponenten $f'$ gehört $\mu'$mal, u. s. w., so ist

$$N\mathfrak{I}(\alpha) = q^{\mu f} q'^{\mu' f'} \ldots;$$

denn in der That enthält $q^{\mu f} q'^{\mu' f'} \ldots$ alle in $\mathfrak{I}(\alpha)\mathfrak{I}(\alpha^{\gamma})\mathfrak{I}(\alpha^{\gamma^2}).\ldots.\mathfrak{I}(\alpha^{\gamma^{\lambda-1}})$ vorkommenden Primfactoren, jeden genau eben so oft, als er in diesem Producte vorkommt; und aufser diesen keinen. Dies ist aber auch die einzige allgemeine Art der Zusammensetzung idealer complexer Zahlen zu wirklichen, welche sich von selbst darbietet.

Wenn irgend eine ideale complexe Zahl $\mathfrak{I}(\alpha)$ gegeben ist, so läfst sich die Aufgabe, andere ideale Zahlen zu finden, welche, mit $\mathfrak{I}(\alpha)$ multiplicirt, ***wirkliche*** complexe Zahlen geben, stets auf unendlich viele verschiedene Arten lösen. Diese Aufgabe kann nämlich auch so ausgedrückt werden: Wirkliche complexe Zahlen zu finden, welche gegebene (ideale) Primfactoren haben, und welche aufser diesen gegebenen noch irgend andere enthalten dürfen. Die Lösung beruht aber nur darauf, einer gewissen Anzahl Congruenzen vom ersten Grade genugzuthun, welche für die Coëfficienten einer wirklichen complexen Zahl Statt haben müssen, und welche sich niemals widersprechen, sondern stets eine unendliche Anzahl verschiedener Lösungen zulassen. Es giebt deshalb auch immer eine unendliche Menge idealer Zahlen, welche, mit einer gegebenen idealen Zahl multiplicirt, eine wirkliche complexe Zahl erzeugen. Wählt man nun unter allen diesen immer nur diejenigen, deren Normen möglichst klein sind, so findet man das sehr bemerkenswerthe Resultat: ***Dafs stets eine endliche bestimmte Zahl idealer Multiplicatoren hinreicht, um alle idealen complexen Zahlen zu wirklichen zu machen.*** Wir wollen jetzt den Beweis dieses ersten Hauptsatzes geben.

Die ideale complexe Zahl $\mathfrak{I}(\alpha)$ enthalte wieder, wie oben, den zu $u = \eta_r$ gehörenden Primfactor der zum Exponenten $f$ gehörenden Primzahl $q$, und zwar $\mu$mal; ferner den zu $u' = \eta'_{r'}$ gehörenden Primfactor der zum Exponenten $f'$ gehörenden Primzahl $q'$, $\mu'$mal u. s. w. und es sei

$$F(\alpha) = a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + \ldots + a_{\lambda-1}\alpha^{\lambda-1}$$

eine wirkliche complexe Zahl, welche alle Primfactoren von $I(\alpha)$, also auch den idealen Factor $I(\alpha)$ selbst enthalten soll. Es sind nun, damit $F(\alpha)$ den zu $u = \eta_r$ gehörenden Primfactor von $q$ $\mu$mal enthalte, $f$ Congruenzen für den Modul $q^\mu$ zu erfüllen. Dieselben seien

$$\Phi = 0, \quad \Phi_1 = 0, \quad \Phi_2 = 0, \quad \ldots\ldots \quad \Phi_{f-1} = 0, \text{ mod. } q^\mu.$$

Ferner sind, damit $F(\alpha)$ den zu $u' = \eta'_{r'}$ gehörenden Primfactor von $q'$, $\mu'$mal enthalte, weiter $f'$ Congruenzen für den Modul $q'^{\mu'}$ zu erfüllen; sie seien

$$\Phi' = 0, \quad \Phi'_1 = 0, \quad \Phi'_2 = 0, \quad \ldots\ldots \quad \Phi'_{f-1} = 0, \text{ mod. } q'^{\mu'};$$

und so fort. Alle diese Congruenzen sind auch, wie gezeigt, in Beziehung auf die zu bestimmenden Coëfficienten $a_1$, $a_2$, $a_3$, $\ldots\ldots$ $a_{\lambda-1}$ nur linear.

Wir geben nun allen den $\lambda-1$ Coëfficienten der complexen Zahl $F(\alpha)$ alle die Werthe 0, 1, 2, 3, $\ldots\ldots$ $k-1$, so dafs im Ganzen $k^{\lambda-1}$ Werthcombinationen Statt finden, welche eben so viele verschiedene complexe Zahlen geben. Für diese verschiedenen Werthcombinationen kann jede der Gröfsen $\Phi$, $\Phi_1$, $\Phi_2$, $\ldots\ldots$ $\Phi_{f-1}$ nur $q^\mu$ verschiedene Reste lassen, für den Modul $q^\mu$; eben so jede der $f'$ Gröfsen $\Phi'$, $\Phi'_1$, $\Phi'_2$, $\ldots\ldots$ $\Phi'_{f'-1}$, nur $q'^{\mu'}$ verschiedene Reste, für den Modul $q'^{\mu'}$ etc. Die Anzahl aller verschiedenen Restcombinationen, welche überhaupt Statt haben können, ist also $q^{\mu f} q'^{\mu' f'} \ldots\ldots$ Nimmt man nun $k$ so grofs an, dafs $k^{\lambda-1} > q^{\mu f} q'^{\mu' f'} \ldots\ldots$, also die Anzahl der Werthcombinationen der Coëfficienten gröfser ist als die Anzahl aller Restcombinationen der durch $\Phi$ bezeichneten Gröfsen, so müssen immer gewisse Restcombinationen sich wiederholen. Es mögen für die bestimmten Werthe $a_1 = m_1$, $a_2 = m_2$, $a_3 = m_3$, $\ldots\ldots$ $a_{\lambda-1} = m_{\lambda-1}$ die Gröfsen $\Phi$, $\Phi_1$, $\ldots\ldots$ $\Phi_{f-1}$, modulo $q^\mu$, $\Phi'$, $\Phi_1$, $\ldots\ldots$ $\Phi'_{f'-1}$, modulo $q'^{\mu'}$, etc. alle einzeln dieselben Reste geben, wie für die Werthe $a_1 = n_1$, $a_2 = n_2$, $a_3 = n_3$, $\ldots\ldots$ $a_{\lambda-1} = n_{\lambda-1}$: so folgt, dafs die Gröfsen $a_1$, $a_2$, $a_3$, $\ldots\ldots$ $a_{\lambda-1}$, weil sie in allen diesen Ausdrücken nur linear vorkommen, alle congruent Null werden müssen, für $a_1 = m_1 - n_1$, $a_2 = m_2 - n_2$, $a_3 = m_3 - n_3$, $\ldots\ldots$ $a_{\lambda-1} = m_{\lambda-1} - n_{\lambda-1}$. Alle Congruenzen also, welche nöthig und hinreichend sind, damit $F(\alpha)$ die verlangten idealen Primfactoren habe, lassen sich immer befriedigen, wenn man den Coëfficienten nur positive oder negative Werthe giebt, welche, abgesehen vom Vorzeichen, nicht gröfser sind als $k-1$; wo $k$ nur durch die Bedingung $k^{\lambda-1} > q^{\mu f} q'^{\mu' f'} \ldots\ldots$ bestimmt wird.

Da wir nun eine gewisse Grenze der Gröfse gefunden haben, welche die Coëfficienten der complexen Zahl $F(\alpha)$ nicht zu überschreiten brauchen,

um den Bedingungen der Aufgabe zu genügen, so wollen wir jetzt sehen, wie grofs höchstens die Norm einer solchen complexen Zahl werden könne.

Multiplicirt man die beiden reciproken complexen Zahlen $F(\alpha)$ und $F(\alpha^{-1})$ mit einander, verwandelt sodann $\alpha$ in $\alpha^2$, $\alpha^3$, .... $\alpha^{\frac{1}{2}(\lambda-1)}$ und addirt, so erhält man sehr leicht folgende Gleichung:

$$F(\alpha)F(\alpha^{-1})+F(\alpha^2)F(\alpha^{-2})+F(\alpha^3)F(\alpha^{-3})+\ldots+F(\alpha^{\frac{1}{2}(\lambda-1)})F(\alpha^{\frac{1}{2}(\lambda+1)})$$
$$=\tfrac{1}{2}\lambda(a_1^2+a_2^2+a_3^2+\ldots+a_{\lambda-1}^2)-\tfrac{1}{2}(a_1+a_2+a_3+\ldots+a_{\lambda-1})^2.$$

Sind nun die Coëfficienten $a_1$, $a_2$, .... $a_{\lambda-1}$ alle, absolut genommen, nicht gröfser als $k-1$, so folgt hieraus:

$$F(\alpha)F(\alpha^{-1})+F(\alpha^2)F(\alpha^{-2})+\ldots+F(\alpha^{\frac{1}{2}(\lambda-1)})F(\alpha^{\frac{1}{2}(\lambda+1)})\leqq\tfrac{1}{2}\lambda(\lambda-1)(k-1)^2.$$

Aus dem möglich-gröfsten Werthe, welchen die Summe aller dieser stets positiven Gröfsen haben kann, läfst sich aber sehr leicht auf den möglich-gröfsten Werth des Products derselben, welches die Norm $NF(\alpha)$ ist, schliefsen. Ein solches Product positiver Gröfsen, deren Summe gegeben ist, erhält nämlich seinen möglich-gröfsten Werth, wenn die einzelnen Factoren desselben alle einander gleich angenommen werden: im gegenwärtigen Falle also, wenn jeder der Factoren gleich dem $\frac{1}{2}(\lambda-1)$ten Theile der möglich-gröfsten Summe aller gleichen genommen wird; also gleich $\lambda(k-1)^2$. Hierdurch wird das möglich-gröfste Product aller gleich $\lambda^{\frac{1}{2}(\lambda-1)}(k-1)^{\lambda-1}$. Man erhält also

$$NF(\alpha)\leqq\lambda^{\frac{1}{2}(\lambda-1)}(k-1)^{\lambda-1}.$$

Nehmen wir nun die Zahl $k$ so an, dafs, wie es oben verlangt wurde, $k^{\lambda-1}>q^{\mu f}\cdot q'^{\mu' f'}\ldots\ldots$, aber $(k-1)^{\lambda-1}<q^{\mu f}\cdot q'^{\mu' f'}\ldots.$ ist, so ergiebt sich

$$NF(\alpha)<\lambda^{\frac{1}{2}(\lambda-1)}\cdot q^{\mu f}\cdot q'^{\mu' f'}\ldots.$$

Die wirkliche complexe Zahl $F(\alpha)$ enthält nach der Voraussetzung den idealen Factor $I(\alpha)$. Setzt man daher $F(\alpha)=M(\alpha)\cdot I(\alpha)$, so ist $NF(\alpha)=NM(\alpha)\cdot NI(\alpha)$, und da $NI(\alpha)=q^{\mu f}\cdot q'^{\mu' f'}\ldots.$, so ist

$$NM(\alpha)<\lambda^{\frac{1}{2}(\lambda-1)}.$$

Die Multiplicatoren also, welche beliebige ideale complexe Zahlen zu wirklichen machen, lassen sich immer so annehmen, dafs die Normen derselben kleiner sind als die bestimmte Zahl $\lambda^{\frac{1}{2}(\lambda-1)}$; und da die Anzahl solcher idealer Zahlen nur endlich und begrenzt sein kann, so erhalten wir den Beweis folgenden Satzes:

***Es giebt immer eine endliche bestimmte Anzahl idealer complexer Multiplicatoren, welche nöthig und hinreichend sind, um alle idealen complexen Zahlen zu wirklichen zu machen.***

§. 9.

Auf den im vorigen Paragraph bewiesenen Hauptsatz gründen wir nun eine Classification der idealen complexen Zahlen, indem wir festsetzen:

***Alle diejenigen (idealen) complexen Zahlen, welche durch Multiplication mit einer und derselben (idealen) Zahl zu wirklichen complexen Zahlen werden, sollen äquivalent heifsen und zusammen eine Classe ausmachen.***

Eine *wirkliche* complexe Zahl, mit einer *idealen* multiplicirt, kann immer nur ein *ideales,* aber niemals ein wirkliches Product geben. Dies ist eine unmittelbare Folge des in (§. 7.) bewiesenen Satzes, welchem zufolge eine wirkliche complexe Zahl durch eine andere wirkliche theilbar ist, wenn alle idealen Primfactoren des Divisors auch im Dividendus enthalten sind und der Quotient alsdann wieder eine wirkliche complexe Zahl ist. Wenn nämlich eine wirkliche Zahl, mit einer idealen multiplicirt, eine wirkliche Zahl zum Product gäbe, so müfste auch eine wirkliche Zahl, durch eine andere wirkliche dividirt, welche keine andern idealen Primfactoren hat als diese, eine ideale Zahl zum Quotienten geben; was dem angeführten Satze widerspricht.

Es seien nun $f(\alpha)$ und $\varphi(\alpha)$ zwei *äquivalente* ideale Zahlen; und zwar sollen beide, mit derselben idealen Zahl $M(\alpha)$ multiplicirt, zu wirklichen werden. Es werde ferner auch $f(\alpha)$, mit $\psi(\alpha)$ multiplicirt, zu einer wirklichen Zahl: so behaupte ich, dafs auch $\varphi(\alpha)$, mit $\psi(\alpha)$ multiplicirt, eine wirkliche Zahl geben mufs. Da nämlich $I(\alpha)\cdot M(\alpha)$ wirklich ist, so folgt, dafs auch $f(\alpha^2)f(\alpha^3)\ldots.f(\alpha^{\lambda-1})\cdot M(\alpha^2)\cdot M(\alpha^3)\ldots. M(\alpha^{\lambda-1})$ wirklich sein mufs. Wird dies mit der wirklichen Zahl $\varphi(\alpha)M(\alpha)$ multiplicirt, so folgt ferner, dafs $\varphi(\alpha)f(\alpha^2)f(\alpha^3)\ldots.f(\alpha^{\lambda-1})\cdot NM(\alpha)$ eine wirkliche Zahl sein mufs; und da der Factor $NM(\alpha)$ wirklich ist, so mufs auch der andere Factor $\varphi(\alpha)f(\alpha^2)f(\alpha^3)\ldots.f(\alpha^{\lambda-1})$ wirklich sein. Multiplicirt man endlich noch mit der wirklichen Zahl $f(\alpha)\psi(\alpha)$ und erwägt, dafs $Nf(\alpha)$ wirklich ist, so folgt, dafs $\varphi(\alpha)\psi(\alpha)$ ebenfalls wirklich sein mufs; wie behauptet; also:

***Wenn zwei ideale complexe Zahlen äquivalent sind, so macht jeder Multiplicator, durch welchen die eine zu einer wirklichen Zahl wird, auch die andere zu einer wirklichen Zahl.***

Aus diesem Satze folgt unmittelbar auch der folgende:

***Wenn zwei ideale Zahlen einer und derselben dritten Zahl äquivalent sind, so sind sie auch unter einander äquivalent.***

Es müssen nämlich nach dem vorigen Satze diese Zahlen alle drei einen und denselben Multiplicator haben, welcher sie zu wirklichen complexen Zahlen macht.

Durch diese Sätze erlangt der Begriff der ***Äquivalenz*** idealer complexer Zahlen erst seine wahre Vollkommenheit; indem sich zeigt, dafs die Äquivalenz eine von der zufälligen Wahl der Multiplicatoren unabhängige Beziehung der idealen Zahlen zu einander ist, und dafs auch die Classification nach der Äquivalenz und die endliche Anzahl der verschiedenen Classen nur eine einzige bestimmte ist, für jeden Werth von $\lambda$.

In die Classification der idealen complexen Zahlen begreifen wir auch die wirklichen mit ein. Der Ausdruck *ideale complexe Zahl* hat nämlich zwei verschiedene Bedeutungen: eine weitere und eine engere; in der weiteren Bedeutung des Idealen ist das Wirkliche nur ein besonderer Fall desselben; in der engeren ist das Wirkliche der Gegensatz des Idealen: es verhält sich hier das Ideale und Wirkliche, wie das Imaginäre und Reale. Die wirklichen complexen Zahlen müssen unter einander alle als äquivalent betrachtet werden; sie machen also eine Classe für sich aus, welche wir als die erste Classe ansehen und ***Hauptclasse*** nennen. Für die Anordnung der übrigen Classen lassen sich nicht eher bestimmte Regeln geben, als bis von der Zusammensetzung der verschiedenen Classen äquivalenter Zahlen gehandelt worden ist; über welche wir Folgendes erwähnen:

***Äquivalente Zahlen, mit äquivalenten multiplicirt, geben stets äquivalente Producte.***

Es seien nämlich $f(\alpha)$ und $f_1(\alpha)$ zwei äquivalente Zahlen; ein Multiplicator, welcher beide zu wirklichen macht, sei $m(\alpha)$; es seien ferner $\varphi(\alpha)$ und $\varphi_1(\alpha)$ zwei andere äquivalente Zahlen, und $M(\alpha)$ der Multiplicator, welcher beide zu wirklichen macht: so ist offenbar $m(\alpha)M(\alpha)$ ein Multiplicator, der sowohl das Product $f(\alpha)\cdot\varphi(\alpha)$, als auch das Product $f_1(\alpha)\cdot\varphi_1(\alpha)$ zu einer wirklichen complexen Zahl macht; mithin sind $f(\alpha)\cdot\varphi(\alpha)$ und $f_1(\alpha)\cdot\varphi_1(\alpha)$ äquivalent. Dieser Satz läfst sich auch folgendermaafsen ausdrücken:

***Wenn man irgend zwei ideale Zahlen mit einander multiplicirt, so ist die Classe, welcher das Product angehört, durch die Classen, welchen die Factoren angehören, vollständig bestimmt.***

Multiplicirt man irgend eine ideale Zahl mit einer Zahl aus jeder Classe, so erhält man so viele Producte, als Classen vorhanden sind, und es kann keines derselben irgend einem andern äquivalent sein; oder jedes dieser Producte gehört einer andern Classe an. Unter diesen mufs es also auch immer

ein Product geben, und zwar ***nur*** eins, welches wirklich ist oder der Hauptclasse angehört; also:

***Zu jeder Classe idealer Zahlen gehört eine bestimmte Zahl, welche, mit ihr zusammengesetzt, die Hauptclasse giebt.***

Es giebt hier auch noch solche Classen, welche, mit sich selbst zusammengesetzt, die Hauptclasse geben (classes ancipites); namentlich ist die Hauptclasse selbst stets eine solche. Aufser dieser existiren aber für besondere Werthe von $\lambda$ auch noch andere mit dieser Eigenschaft.

Erhebt man irgend eine ideale Zahl $f(\alpha)$ zu Potenzen, so ist klar, dafs die Reihe idealer Zahlen

$$f(\alpha),\ f(\alpha)^2,\ f(\alpha)^3,\ f(\alpha)^4,\ \text{etc.}$$

äquivalente Zahlen enthalten mufs; denn die Anzahl nicht äquivalenter Zahlen ist eine endliche. Es seien nun $f(\alpha)^r$ und $f(\alpha)^s$ äquivalent, und $m(\alpha)$ sei ein Multiplicator, welcher beide zu wirklichen Zahlen macht, so ist $f(\alpha)^r \cdot m(\alpha)$ wirklich, und auch $f(\alpha)^s \cdot m(\alpha)$ ist wirklich. Ist nun $s > r$, so kann man demselben die Form $f(\alpha)^{s-r} \cdot f(\alpha)^r \cdot m(\alpha)$ geben, und da $f(\alpha)^r m(\alpha)$ wirklich ist, so mufs auch der andere Factor $f(\alpha)^{s-r}$ wirklich sein. Wir erhalten hieraus folgenden wichtigen Satz:

***Jede ideale complexe Zahl hat die Eigenschaft, dafs gewisse ganze Potenzen derselben wirkliche complexe Zahlen sind. Alle idealen complexen Zahlen lassen sich daher als Wurzeln aus wirklichen complexen Zahlen darstellen***

Es sei nun die $h$te Potenz der idealen Zahl $f(\alpha)$ die niedrigste, für welche $f(\alpha)^h$ zu einer wirklichen complexen Zahl wird, so müssen alle die Zahlen

$$1,\ f(\alpha),\ f(\alpha)^2,\ f(\alpha)^3,\ \ldots\ f(\alpha)^{h-1}$$

verschiedenen Classen angehören; denn wäre $f(\alpha)^r$ äquivalent $f(\alpha)^s$, wo $s > r$ ist, und $s$ und $r$ beide kleiner sind als $h$, so würde wie oben folgen, dafs $f(\alpha)^{s-r}$ eine wirkliche Zahl sei; gegen die Voraussetzung, da $s - r < h$ ist. Diese $h$ complexen Zahlen können nun entweder alle vorhandenen Classen grade erschöpfen, in welchem Fall die Anzahl aller Classen gleich $h$ ist, oder es können noch andere, nicht äquivalente ideale Zahlen vorhanden sein. Es sei $\varphi(\alpha)$ eine solche ideale Zahl, welche mit keiner der obigen äquivalent ist, so behaupte ich, dafs auch die idealen Zahlen

$$\varphi(\alpha),\ \varphi(\alpha)f(\alpha),\ \varphi(\alpha)f(\alpha)^2,\ \ldots\ \varphi(\alpha)f(\alpha)^{h-1}$$

alle, sowohl unter sich, als auch mit den obigen, nicht äquivalent sind. Wäre nämlich $\varphi(\alpha)f(\alpha)^r$ äquivalent $\varphi(\alpha)f(\alpha)^s$, wo $r$ und $s$ beide kleiner als $h$ sind, so würde auch $f(\alpha)^r$ äquivalent $f(\alpha)^s$ sein; was unmöglich ist; und wäre $\varphi(\alpha)f(\alpha)^r$ äquivalent $f(\alpha)^s$, so würde durch Multiplication mit $f(\alpha)^{h-r}$ folgen, dafs $\varphi(\alpha)$ äquivalent $f(\alpha)^{s+h-r}$ oder äquivalent $f(\alpha)^{s-r}$ sei; welches ebenfalls der über $\varphi(\alpha)$ gemachten Voraussetzung zuwider ist. Es kann nun geschehen, dafs diese idealen Zahlen, zusammen mit den vorigen, alle nicht äquivalenten Zahlen erschöpfen; in welchem Falle die Anzahl aller Classen gleich $2h$ sein würde: es kann aber auch sein, dafs es aufser diesen noch andere nicht äquivalente Zahlen giebt. In diesem letztern Falle beweiset man eben so, dafs eine mit den obigen nicht äquivalente Zahl $\psi(\alpha)$ stets die ganze Gruppe

$$\psi(\alpha),\ \psi(\alpha)f(\alpha),\ \psi(\alpha)f(\alpha)^2,\ \ldots.\ \psi(\alpha)f(\alpha)^{h-1}$$

nach sich zieht; welche Zahlen sowohl unter sich, als mit den obigen, nicht äquivalent sind. Sämmtliche nicht äquivalente ideale Zahlen ordnen sich so immer in Gruppen von je $h$ Zahlen; woraus folgt, dafs die vollständige Anzahl derselben immer ein Vielfaches von $h$ sein mufs. Wir sprechen dies Resultat folgendermaafsen aus:

***Die vollständige Anzahl aller Classen ist immer ein Vielfaches des niedrigsten Exponenten derjenigen Potenz, zu welcher eine ideale Zahl erhoben werden mufs, um zu einer wirklichen zu werden.***

Wenn es nun wirklich eine *ideale* Zahl $f(\alpha)$ giebt, von der Art, dafs $f(\alpha)^h$, aber keine niedrigere Potenz von $f(\alpha)$, eine *wirkliche* complexe Zahl ist, und dafs $1, f(\alpha), f(\alpha)^2, f(\alpha)^3, \ldots. f(\alpha)^{h-1}$ alle nicht äquivalenten idealen Zahlen erschöpfen, so erhält man eine passende Anordnung aller Classen, wenn man die wirklichen zur ersten Classe, die Classe, welche $f(\alpha)$ enthält, zur zweiten, die $f(\alpha)^2$ enthaltende zur dritten nimmt u. s. w. Es kann alsdann die Classe, welcher das Product zweier oder mehrerer Factoren angehört, aus den Classen, welchen die Factoren angehören, unmittelbar bestimmt werden, weil alsdann offenbar die Summe der um Eins verminderten Classenzahlen aller Factoren der um Eins verminderten Classenzahl des Products, für den Modul $h$, congruent ist. Wenn aber eine solche ideale Zahl $f(\alpha)$ nicht existirt, deren Potenzen alle Classen nicht äquivalenter Zahlen erschöpfen, so kann man nach diesem Principe die Classen nur in Gruppen theilen und die den einzelnen Gruppen angehörenden Classen ordnen; für die Ordnung der Gruppen unter einander ist aber dann ein anderes Princip nöthig.

## §. 10.

Wir haben schon oben bemerkt, dafs die idealen Primfactoren stets Primfactoren ganzer realer Primzahlen sind, und dafs die Natur derselben vorzüglich von den Exponenten (Divisoren von $\lambda-1$) abhangt, zu welchen diese realen Primzahlen für den Modul $\lambda$ gehören. Unter allen diesen sind die idealen Primfactoren der zum Exponenten ***Eins*** gehörenden realen Primzahlen, d. h. der Primzahlen von der Form $2m\lambda+1$, als die einfachsten zu betrachten, welche vor den übrigen sich auszeichnen und darum besondere Beachtung verdienen. Von den nur aus solchen idealen Primfactoren zusammengesetzten idealen Zahlen wollen wir nun zeigen, dafs sie auch allein alle oben angegebenen Classen idealer Zahlen erschöpfen, und dafs die übrigen idealen Zahlen, welche noch andere, zu höhern Exponenten gehörige Primfactoren enthalten, für sich keine neuen Classen geben, sondern nur jenen sich einordnen *). Wir beweisen zu diesem Zwecke zunächst folgenden Satz:

***Jeder ideale Primfactor, der zu einem Exponenten gehört, welcher gröfser als Eins ist, ist einer idealen Zahl äquivalent, deren ideale Primfactoren alle zu niedrigeren Exponenten gehören.***

Um diesen Satz zu beweisen, gehen wir von der Gleichung aus, deren Wurzeln alle die in einer und derselben Periode von $f$ Gliedern enthaltenen Wurzeln der Gleichung $\alpha^\lambda=1$ sind, und von welcher schon oben (§. 4.) Gebrauch gemacht wurde, nemlich von der Gleichung

$$(1.)\qquad \alpha^f+\boldsymbol{P}_1(\eta)\alpha^{f-1}+\boldsymbol{P}_2(\eta)\alpha^{f-2}+\ldots.+\boldsymbol{P}_f(\eta)=0,$$

in welcher die Coëfficienten $\boldsymbol{P}_1(\eta)$, $\boldsymbol{P}_2(\eta)$, etc. aus den Perioden von je $f$ Gliedern gebildete ganze complexe Zahlen sind. Es seien ferner $\boldsymbol{P}_1(\boldsymbol{u})$, $\boldsymbol{P}_2(\boldsymbol{u})$, $\boldsymbol{P}_3(\boldsymbol{u})$, etc. diejenigen ganzen Zahlen, welche man erhält, wenn man in jenen statt der Perioden $\eta$, $\eta_1$, $\eta_2$, etc. die entsprechenden Congruenzwurzeln $\boldsymbol{u}$, $\boldsymbol{u}_1$, $\boldsymbol{u}_2$, etc. für den Modul $q$ setzt, der zum Exponenten $f$ gehört. Setzt man jetzt

$$(2.)\quad \boldsymbol{F}(\alpha)=\alpha^f+\boldsymbol{P}_1(\boldsymbol{u})\alpha^{f-1}+\boldsymbol{P}_2(\boldsymbol{u})\alpha^{f-2}+\ldots.+\boldsymbol{P}_{f-1}(\boldsymbol{u})\alpha+\boldsymbol{P}_f(\boldsymbol{u})+q,$$

so erhält man, wenn die Gleichung (1.) subtrahirt wird, und wenn man erwägt, dafs $\boldsymbol{P}_f(\eta)=\pm1$, also $\boldsymbol{P}_f(\boldsymbol{u})=\boldsymbol{P}_f(\eta)$ ist:

$$(3.)\quad \boldsymbol{F}(\alpha)=(\boldsymbol{P}_1(\boldsymbol{u})-\boldsymbol{P}_1(\eta))\alpha^{f-1}+(\boldsymbol{P}_2(\boldsymbol{u})-\boldsymbol{P}_2(\eta))\alpha^{f-2}+\ldots. \\ \ldots.+(\boldsymbol{P}_{f-1}(\boldsymbol{u})-\boldsymbol{P}_{f-1}(\eta))\alpha+q.$$

*) Statt: Idealer Primfactor einer realen, zum Exponenten $f$ gehörigen Primzahl, werden wir hier und im Folgenden kürzer: ***Zum Exponenten f gehöriger idealer Primfactor*** schreiben.

Diese complexe Zahl $F(\alpha)$ hat nun, *Erstens*, keinen idealen Primfactor, welcher zu einem höhern Exponenten gehörte, als zum Exponenten $f$. Wenn nämlich $f'$ ein gröfserer Divisor von $\lambda-1$ ist, als $f$, so mufs man nach (§. 4.), um zu sehen ob eine wirkliche complexe Zahl einen zum Exponenten $f'$ gehörenden idealen Primfactor haben könne, oder, was Dasselbe ist, ob die Norm derselben durch eine zum Exponenten $f'$ gehörende reale Primzahl theilbar sein könne, aus der zu untersuchenden Zahl mit Hülfe der Gleichung, deren Wurzeln die sämmtlichen, eine Periode von $f$ Gliedern bildenden Wurzeln sind, alle Potenzen von $\alpha$, welche höher sind als $\alpha^{f'-1}$, eliminiren; worauf dann alle Glieder einzeln diesen idealen Factor haben müssen. Im gegenwärtigen Falle enthält $F(\alpha)$ an sich schon keine höhern Potenzen von $\alpha$: es hat also bereits die verlangte Form, welche im Allgemeinen durch Elimination der höhern Potenzen von $\alpha$ hervorzubringen ist. Es müfsten demnach in dem Ausdrucke von $F(\alpha)$, welchen die Gleichung (2.) giebt, wenn $F(\alpha)$ einen zum Exponenten $f'$ gehörenden idealen Primfactor haben sollte, alle Coëfficienten der einzelnen Glieder, also auch der erste Coëfficient *Eins*, denselben enthalten; was nicht möglich ist.

*Zweitens* hat $F(\alpha)$ auch keinen idealen Primfactor einer andern, zum Exponenten $f$ gehörenden Primzahl, als der Primzahl $q$; denn es müfste nach (§. 4.) jeder solcher Primfactor auch ein gemeinschaftlicher Factor aller Glieder der complexen Zahl $F(\alpha)$ in der Form (3.) sein, also namentlich auch ein idealer Primfactor des letzten Gliedes $q$.

*Drittens* enthält $F(\alpha)$ auch nur einen einzigen idealen Primfactor von $q$, nämlich den zu $u=\eta$ gehörenden Factor, und diesen nur einmal. Dafs es den genannten idealen Primfactor wirklich enthält, ist klar, weil $F(\alpha)\equiv 0$, mod. $q$, ist, für $u=\eta$; und wenn es den Factor mehrmals enthielte, so müfsten in der Form (3.) alle einzelnen Glieder, also auch das letzte Glied $q$, denselben mehrmals enthalten; welches nicht der Fall ist. Bildet man ferner folgende complexe Zahlen:

$$\begin{aligned}
F(\alpha) &= \alpha^f + P_1(u)\alpha^{f-1} + P_2(u)\alpha^{f-2} + \ldots + P_f(u) + q,\\
F_1(\alpha) &= \alpha^f + P_1(u_1)\alpha^{f-1} + P_2(u_1)\alpha^{f-2} + \ldots + P_f(u_1) + q,\\
F_2(u) &= \alpha^f + P_1(u_2)\alpha^{f-1} + P_2(u_2)\alpha^{f-2} + \ldots + P_f(u_2) + q,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
F_{e-1}(\alpha) &= \alpha^f + P_1(u_{e-1})\alpha^{f-1} + P_2(u_{e-1})\alpha^{f-2} + \ldots + P_f(u_{e-1}) + q,
\end{aligned}$$

so enthält $F(\alpha)$ den zu $u_1=\eta$ gehörenden idealen Primfactor von $q$, $F_1(\alpha)$ den zu $u_1=\eta$ gehörenden, $F_2(\alpha)$ den zu $u_2=\eta$ gehörenden Factor u. s. w.;

das Product aller dieser complexen Zahlen ist also, weil es alle idealen Primfactoren von $q$ enthält, durch $q$ theilbar. Enthielte nun aber $F(\alpha)$ aufser dem zu $u = \eta$ gehörenden Primfactor noch einen andern, welcher zu $u_r = \eta$ gehören möge, so müfste das Product dieser complexen Zahlen, auch mit Ausschlufs der Zahl $F_r(\alpha)$, durch $q$ theilbar sein, weil es auch schon ohne $F_r(\alpha)$ alle idealen Primfactoren von $q$ enthielte. Dieses Product würde folgende Form haben:

$$\alpha^{(e-1)f} + C_1\alpha^{(e-1)f-1} + C_2\alpha^{(e-1)f-2} + \ldots + C_{(e-1)f};$$

wo $C_1$, $C_2$, etc. ganze Zahlen sind. Es müfsten also wieder alle einzelnen Glieder, folglich auch das erste, dessen Coëfficient Eins ist, durch $q$ theilbar sein; was nicht der Fall ist.

Wir schliefsen hieraus, dafs es immer wirkliche complexe Zahlen giebt, die nur einen einzigen, zum Exponenten $f$ gehörenden idealen Primfactor enthalten, deren übrige Primfactoren aber alle zu niedrigeren Exponenten gehören. Dafs der Fall $f = 1$ eine Ausnahme macht, ist klar. Bezeichnet man nun den einen, zum Exponenten $f$ gehörenden idealen Primfactor, welcher in $F(\alpha)$ enthalten ist, durch $f(\alpha)$, und das Product aller übrigen, welche nur zu niedrigeren Exponenten gehören, durch $\varphi(\alpha)$, so dafs $F(\alpha) = f(\alpha)\cdot\varphi(\alpha)$ eine wirkliche complexe Zahl ist: so folgt, dafs $f(\alpha)$ äquivalent ist mit $\varphi(\alpha^2)\varphi(\alpha^3)\ldots\varphi(\alpha^{\lambda-1})$; denn beide, mit $\varphi(\alpha)$ multiplicirt, geben *wirkliche* Zahlen. Hiermit ist auch der obige Satz vollständig bewiesen.

Aus dem so eben bewiesenen Satze folgt von selbst der allgemeine Satz:

***Jede beliebige ideale Zahl ist einer andern äquivalent, deren ideale Primfactoren alle nur zum Exponenten Eins gehören.***

Wenn nämlich in $\varphi(\alpha)$, und folglich auch in $\varphi(\alpha^2)\varphi(\alpha^3)\ldots\varphi(\alpha^{\lambda-1})$, noch Primfactoren vorhanden sind, die nicht zum Exponenten Eins gehören, so kann man sie immer durch äquivalente ideale Zahlen ersetzen, deren Primfactoren zu immer niedrigeren Exponenten gehören; und so fortfahrend gelangt man nothwendig dahin, dafs alle Primfactoren der äquivalenten Zahl nur zum Exponenten *Eins* gehören. Wenn ferner alle beliebigen Primfactoren solchen idealen Zahlen äquivalent sind, so folgt das Nemliche für alle beliebigen zusammengesetzten idealen Zahlen von selbst.

Anmerkung. Ich kann nicht umhin, hier, wo ich die allgemeine Theorie der Zerlegung der complexen Zahlen, wenn auch unvollendet, verlasse, um in den folgenden Paragraphen noch einige Anwendungen zu geben, auf die grofse Analogie aufmerksam zu machen, welche diese Theorie mit der *Chemie*

hat. Der chemischen Verbindung entspricht für die complexen Zahlen die Multiplication; den Elementen, oder eigentlich den Atomgewichten derselben, entsprechen die Primfactoren; und die chemischen Formeln für die Zerlegung der Körper sind genau dieselben, wie die Formeln für die Zerlegung der Zahlen. Auch selbst die idealen Zahlen unserer Theorie finden sich in der Chemie, vielleicht nur allzuoft, als hypothetische Radicale, welche bisher noch nicht dargestellt worden sind, die aber, so wie die idealen Zahlen, in den Zusammensetzungen ihre Wirklichkeit haben. Das Fluor, für sich bisher nicht darstellbar und noch den Elementen zugezählt, kann als Analogon eines idealen Primfactors gelten. Die Idealität in der Chemie verhält sich aber darin wesentlich anders, als die der complexen Zahlen, dafs chemische ideale Stoffe, mit wirklichen verbunden, auch wirkliche Stoffe produciren; was bei den idealen Zahlen nicht der Fall ist. In der Chemie hat man ferner zur Prüfung der in einem unbekannten aufgelöseten Körper enthaltenen Stoffe die Reagentien, welche Niederschläge geben, aus denen die Anwesenheit der verschiedenen Stoffe sich erkennen läfst. Ganz Dasselbe findet für die complexen Zahlen Statt; denn es sind die oben mit $\Psi$ bezeichneten complexen Zahlen ebenso die Reagentien für die idealen Primfactoren, und die reale Primzahl $q$, welche nach der Multiplication mit einer solchen als Factor aus dem Producte heraustritt, ist genau Dasselbe, wie der unlösliche Niederschlag, der nach Anwendung des Reagens zu Boden fällt. Auch der Begriff der Äquivalenz ist in der Chemie fast derselbe, wie in der Theorie der complexen Zahlen. So wie nämlich dort zwei Gewichtsmengen verschiedener Stoffe äquivalent heifsen, wenn sie sich gegenseitig vertreten können, entweder zum Zwecke des Neutralisirens, oder um Isomorphie hervorzubringen: so sind zwei ideale Zahlen äquivalent, wenn sie für den Zweck, eine andere ideale Zahl zu einer wirklichen zu machen, sich gegenseitig vertreten können. — Diese hier angedeuteten Analogieen sind nicht etwa als blofse Spiele des Witzes zu betrachten, sondern haben ihren guten Grund darin, dafs die Chemie, so wie der hier behandelte Theil der Zahlentheorie, beide denselben Grundbegriff, nämlich den der *Zusammensetzung*, wenn gleich innerhalb verschiedener Sphären des Seins, zu ihrem Principe haben; woraus folgt, dafs auch die diesem verwandten, mit ihm nothwendig gegebenen Begriffe sich in beiden auf ähnliche Weise finden müssen. Die Chemie der natürlichen Stoffe und die hier behandelte Chemie der complexen Zahlen sind beide als Verwirklichungen des Begriffs der Zusammensetzung und der davon abhängigen Begriffs-Sphäre anzusehen: jene

als eine physische, mit den Zufälligkeiten der äufsern Existenz verbundene und deshalb reichere, diese als eine mathematische, in ihrer innern Nothwendigkeit vollkommen reine, aber dafür auch ärmere, als jene.

## §. 11.

Die hauptsächlichsten Schwierigkeiten der Lehre von der Kreistheilung liegen bekanntlich in gewissen complexen, in derselben auftretenden Zahlen. Es bleibt von der rein theoretischen Seite eine genauere Einsicht in die Natur dieser complexen Zahlen, von der practischen Seite eine leichtere Methode für die Bildung derselben noch zu wünschen. Diese beiden Mängel dürften nun mittels der hier gegebenen Theorie der complexen Zahlen vollständig gehoben werden können.

Ist $p$ eine Primzahl von der Form $p = \mu\lambda + 1$, $g$ eine primitive Wurzel von $p$, $\alpha$ eine imaginäre Wurzel der Gleichung $\alpha^\lambda = 1$, und $x$ eine imaginäre Wurzel der Gleichung $x^p = 1$, so beruht die hauptsächlichste Aufgabe der Kreistheilung in der Bildung der $\lambda$ten Potenz des Ausdrucks

$$(\alpha, x) = x + \alpha x^g + \alpha^2 x^{g^2} + \ldots + \alpha^{p-2} x^{g^{p-2}},$$

welche Potenz, von $x$ unabhängig, eine aus den Wurzeln $\alpha$, $\alpha^2$, $\alpha^3$, etc. gebildete complexe Zahl ist. Diese complexe Zahl setzt ***Jacobi*** (S. Monatsberichte der Berliner Akademie vom Jahre 1837, wieder abgedruckt in diesem Journal Bd. XXX. S. 166) als Product aus complexen, ebenfalls von $x$ unabhängigen Zahlen zusammen, welche durch die Gleichung

$$\psi_k(\alpha) = \frac{(\alpha, x)(\alpha^k, x)}{(\alpha^{k+1}, x)}$$

bestimmt sind. Es ist nämlich

$$(\alpha, x)^\lambda = p\psi_1(\alpha)\psi_2(\alpha)\psi_3(\alpha)\ldots\psi_{\lambda-2}(\alpha).$$

Nun weiset auch ***Jacobi*** a. a. O. nach, dafs, wenn $r$ eine primitive Wurzel der Gleichung $r^{p-1} = 1$, und $g$ dieselbe primitive Wurzel der Congruenz $g^{p-1} \equiv 1$ ist, welche auch schon in $(\alpha, x)$ vorkommt, und wenn in dem von $x$ unabhängigen Ausdrucke

$$\psi(r) = \frac{(r^{-m}, x)(r^{-n}, x)}{(r^{-m-n}, x)}$$

anstatt der primitiven Wurzel $r$, die primitive Congruenzwurzel $g$ gesetzt wird, dafs dann

$$\psi(g) \equiv 0, \text{ mod. } p,$$

ist, sobald $m + n > p - 1$, aber $m$ und $n$ für sich kleiner als $p - 1$ und positiv

sind. Setzt man nun

$$r^{-m} = \alpha, \quad g^{p-1-m} \equiv u, \text{ mod. } p,$$
$$n \equiv km, \text{ mod. } p-1, \qquad m \equiv h\mu, \text{ mod. } p-1,$$

so ergiebt sich

$$\psi(r) = \psi_k(\alpha^h), \quad \text{also auch} \quad \psi(\alpha) \equiv \psi_k(u^h).$$

Es ist demnach $\psi_k(u^h) \equiv 0$, mod. $p$, für $m+n > p-1$; welche Bedingung sich nach den festgesetzten Werthen von $m$ und $n$ darauf vereinfacht, dafs die positiven Reste von $hk$ und von $h$, für den Modul $\lambda$, zusammen gröfser sein müssen als $\lambda$.

Dieses *Jacobi*sche Resultat giebt unmittelbar die idealen Primfactoren der complexen Zahl $\psi_k(\alpha)$. In unsere Ausdrucksweise übersetzt, heifst es: ***Es enthält*** $\psi_k(\alpha)$ ***den zu*** $\alpha = u^h$ ***gehörenden idealen Primfactor von*** $p$, ***wenn*** $h$ ***und der positive Rest von*** $hk$, ***mod.*** $\lambda$, ***zusammen gröfser sind als*** $\lambda$. Die Anzahl der Werthe von $h$, welche dieser Bedingung genügen, ist offenbar gleich $\frac{1}{2}(\lambda-1)$; denn von je zwei Werthen von $h$, deren Summe gleich $\lambda$ ist, genügt immer einer, und zwar ***nur*** einer von beiden. Es sind also dadurch $\frac{1}{2}(\lambda-1)$ Primfactoren der complexen Zahl $\psi_k(\alpha)$ gegeben, und aufser diesen können keine andern vorhanden sein; denn $\psi_k(\alpha^{-1})$ mufs genau eben so viele Primfactoren enthalten als $\psi_k(\alpha)$, und da $\psi_k(\alpha)\psi_k(\alpha^{-1}) = p$, $p$ aber nur $\lambda-1$ (ideale) Primfactoren enthält, so mufs $\psi_k(\alpha)$ genau $\frac{1}{2}(\lambda-1)$ Primfactoren enthalten, welche die oben gefundenen sind. Bezeichnet $f(\alpha)$ einen idealen Primfactor von $p$, und zwar den zu $\alpha = u$ gehörenden; bedeutet ferner $m_h^{h'}$ diejenige positive Zahl, welche kleiner als $\lambda$ ist und der Congruenz $hm_h \equiv 1$, mod. $\lambda$, genügt, so ist

$$\psi_k(\alpha) = \pm\alpha^r \Pi f(\alpha^{m_h});$$

wo das Productzeichen $\Pi$ sich auf alle diejenigen $\frac{1}{2}(\lambda-1)$ Werthe von $h$ bezieht, für welche $h$ und der positive Rest von $hk$, mod. $\lambda$, zusammen gröfser sind als $\lambda$. Nach dem vorletzten Satze in (§. 7.) mufs diesem Producte, welches nur durch seinen idealen Primfactor bestimmt ist, irgend eine complexe Einheit $E(\alpha)$ als Factor beigegeben werden; diese mufs aber vermöge der Gleichung $\psi_k(\alpha)\psi_k(\alpha^{-1}) = p$ so beschaffen sein, dafs $E(\alpha)E(\alpha^{-1}) = 1$ ist; und dieser Gleichung genügt keine andere Einheit, und überhaupt keine andere complexe Zahl als $\pm\alpha^r$, weshalb wir diese Einheit als Factor des Products hinzugefügt haben.

Mit den gefundenen Primfactoren von $\psi_k(\alpha)$ sind nun diejenigen der Potenz $(\alpha, x)^\lambda$ zugleich mit gegeben. Der bestimmte, zu $\alpha = u^h$ gehörige ideale

Primfactor von $p$ kommt nämlich in dem Producte $\psi_1(\alpha)\psi_2(\alpha)\psi_3(\alpha)\ldots\psi_{\lambda-2}(\alpha)$ gerade so viele mal vor, als es Zahlen $k$ giebt, für welche der positive Rest von $kh$, wenn $h$ hinzu addirt wird, gröfser wird als $\lambda$, also für welche der positive Rest von $kh$, mod. $\lambda$, gröfser ist als $\lambda-h$. Nun hat für $k=1,2,3,\ldots.\lambda-2$ das Product $hk$ alle Reste $1,2,3,\ldots.\lambda-1$, mit Ausnahme von $\lambda-h$; die Anzahl derer, die gröfser sind als $\lambda-h$, ist also $h-1$; folglich kommt der zu $\alpha=u^h$ gehörende ideale Primfactor von $p$, welcher nach der obigen Bezeichnung $f(\alpha^{m_h})$ ist, in diesem Producte $h-1$ mal vor. Man erhält folglich

$$\psi_1(\alpha)\psi_2(\alpha)\ldots.\psi_{\lambda-2}(\alpha) = \pm\alpha^s f(\alpha^{m_2})^1\cdot f(\alpha^{m_3})^2\cdot f(\alpha^{m_4})^3\ldots.f(\alpha^{m_{\lambda-1}})^{\lambda-2},$$

und wenn mit $p=f(\alpha)\cdot f(\alpha^2)\cdot f(\alpha^3)\ldots.f(\alpha^{\lambda-1})$, oder, was Dasselbe ist, mit $p=f(\alpha^{m_1})\cdot f(\alpha^{m_2})\cdot f(\alpha^{m_3})\ldots.f(\alpha^{m_{\lambda-1}})$ multiplicirt wird:

$$(\alpha,x)^\lambda = \pm\alpha^s f(\alpha^{m_1})^1\cdot f(\alpha^{m_2})^2\cdot f(\alpha^{m_3})^3\ldots.f(\alpha^{m_{\lambda-1}})^{\lambda-1};$$

welches nach einer andern Anordnung der Factoren auch so dargestellt werden kann:

$$(\alpha,x)^\lambda = \pm\alpha^s f(\alpha)^{m_1}\cdot f(\alpha^2)^{m_2}\cdot f(\alpha^{\lambda-1})^{m_{\lambda-1}}.$$

(Man vergleiche das Breslauer Programm zur Jubelfeier der Universität Königsberg, in welchem ich diese Darstellung des $(\alpha,x)^\lambda$ zuerst aufgestellt und nach einer andern einfachen Methode bewiesen habe; für den Fall, dafs $f(\alpha)$ ein wirklicher (nicht idealer) complexer Primfactor von $p$ ist.)

Zur Bestimmung des allein noch unbestimmt gebliebenen Factors $\pm\alpha^s$ erwäge man, dafs $(\alpha,x)^\lambda\equiv(1,x^\lambda)\equiv-1$, mod. $\lambda$, ist; es mufs also dieser Factor so genommen werden, dafs auch die andere Seite dieser Gleichung congruent $-1$ werde, für den Modul $\lambda$ *).

Für die Erkenntnifs der innern Natur dieser complexen Zahlen der Kreistheilung lassen die gegebenen Zerlegungen in die Primfactoren nichts zu wünschen übrig. Was ferner die wirkliche Berechnung derselben für bestimmte Werthe des $p$ und $\lambda$ betrifft, so reduciren sie die ganze Aufgabe auf den einen Punct: einen complexen Primfactor von $p$ zu finden, welcher immer, entweder als wirkliche complexe Zahl, oder doch als Wurzel aus einer solchen dargestellt werden kann. Im ersten Fall läfst sich ein solcher Primfactor durch indirecte Methoden, welche ich in dem erwähnten Programm ent-

*) Ich verdanke diese Bemerkung einer Privat-Mittheilung des Hrn. Dr. *Eisenstein*. Anm. d. Verf.

wickelt habe, stets sehr leicht finden; ist er ideal, so mufs man zunächst ermitteln, zu welcher Potenz er erhoben werden mufs, um zu einem wirklichen Factor zu werden. Diese Potenz läfst sich alsdann durch dieselben Methoden finden, und die entsprechende Wurzel daraus giebt den gesuchten idealen Factor. In diesem letzten Falle giebt es übrigens noch andere Mittel zur wirklichen Berechnung von $(\alpha, x)^\lambda$; welche ich jedoch hier übergehe. Hätte man eine vollständige Tafel aller complexen Primfactoren der realen Primzahlen (z. B. bis $p = 997$, als so weit der „Canon arithmeticus" von *Jacobi* reicht), nicht blofs für den Fall, dafs $\lambda$ eine Primzahl ist, sondern auch wenn es eine Potenz einer Primzahl ist: so hätte man für den ganzen Bereich dieser Tafel auch die Lösung aller Kreistheilungen, ohne alle weitere Rechnung. Einen Anfang für eine solche Tafel der complexen Primfactoren habe ich in dem erwähnten Programme gegeben.

## §. 12.

Das Product idealer Primfactoren, durch welches wir die in der Kreistheilung vorkommenden, mit $\psi_k(\alpha)$ bezeichneten complexen Zahlen ausgedrückt haben, nämlich

$$\pm\alpha^r \Pi f(\alpha^{m_h}) = \psi_k(\alpha),$$

wo $h$ diejenigen $\frac{1}{2}(\lambda-1)$ Werthe hat, welche der Bedingung genügen, dafs der kleinste positive Rest von $kh$, mod. $\lambda$, um $h$ vermehrt, gröfser als $\lambda$ ist, und wo $m_h$ eine der Congruenz $hm_h$, mod. $\lambda$, genügende Zahl bedeutet, hat die merkwürdige Eigenschaft, immer eine *wirkliche* complexe Zahl zu geben; nicht blofs, wenn, wie im vorigen Paragraph, $f(\alpha)$ ein idealer Primfactor der Primzahl $p$ von der Form $\mu\lambda+1$ ist, sondern auch wenn $f(\alpha)$ irgend eine beliebige ideale complexe Zahl ist. Ist nämlich $f(\alpha)$ irgend eine beliebige ideale Zahl, so ist sie nach (§. 10.) stets solchen idealen Zahlen äquivalent, deren ideale Primfactoren nur zum Exponenten *Eins* gehören. Was also in Beziehung auf die Wirklichkeit des obigen Products von einer solchen idealen Zahl gilt, das gilt auch von jeder beliebigen. Ist aber $f(\alpha)$ ein Product aus idealen Primfactoren, welche alle zum Exponenten *Eins* gehören, d. h. welche nur ideale Primfactoren realer Primzahlen von der Form $\mu\lambda+1$ sind, so zerfällt das obige Product in ein Product ähnlicher Producte, welche alle einzeln, dem vorigen Paragraphen zufolge, wirkliche complexe Zahlen sind. Es ist demnach in der That $\Pi f(\alpha^{m_h})$ stets eine wirkliche complexe Zahl, wenn $f(\alpha)$ irgend eine beliebige ideale Zahl bedeutet. Dasselbe gilt nun auch

von dem Producte

$$f(\alpha^{m_1})^1 \cdot f(\alpha^{m_2})^2 \cdot f(\alpha^{m_3})^3 \ldots . f(\alpha^{m_{\lambda-1}})^{\lambda-1} = \boldsymbol{P}(\alpha);$$

denn dieses ist, wie im vorigen Paragraph gezeigt, nur aus den obigen Producten zusammengesetzt.

Es soll nun für $f(\alpha)$ eine aus Perioden von je $f$ Gliedern gebildete ideale Zahl genommen werden, d. h. eine solche, welche, durch $\varphi(\eta)$ bezeichnet, der Bedingung genügt, dafs

$$\varphi(\eta)\varphi(\eta_1)\varphi(\eta_2) \ldots . \varphi(\eta_{e-1}) = N\varphi(\eta) = \boldsymbol{M}$$

gleich einer realen ganzen Zahl sei. Nach (§. 7.) gestattet auch jede Zahl $\boldsymbol{M}$, welche die Eigenschaft hat, dafs alle ihre Divisoren, zur $f^{\text{ten}}$ Potenz erhoben, congruent ***Eins*** sind, für den Modul $\lambda$, eine solche ideale Zerlegung in complexe Factoren. Es sei ferner $\gamma$ eine primitive Wurzel der Congruenz $\gamma^{\lambda-1} \equiv 1$, mod. $\lambda$, ferner allgemein $\gamma_r$ der kleinste positive Rest, welchen $\gamma^r$ läfst, für den Modul $\lambda$, und dann

$$\begin{aligned}
1 + \gamma_e + \gamma_{2e} + \ldots . + \gamma_{(f-1)e} &= \lambda s_0, \\
\gamma_1 + \gamma_{e+1} + \gamma_{2e+1} + \ldots . + \gamma_{(f-1)e+1} &= \lambda s_1, \\
\gamma_2 + \gamma_{e+2} + \gamma_{2e+2} + \ldots . + \gamma_{(f-1)e+2} &= \lambda s_2, \\
\ldots & \ldots \\
\gamma_{e-1} + \gamma_{2e-1} + \gamma_{3e-1} + \ldots . + \gamma_{fe-1} &= \lambda s_{e-1}:
\end{aligned}$$

so sind $s_0, s_1, s_2, \ldots . s_{e-1}$ ganze Zahlen, weil diese Summen bekanntlich alle durch $\lambda$ theilbar sind. Schreibt man nun das Product $\boldsymbol{P}(\alpha)$ in der Form

$$\boldsymbol{P}(\alpha) = f(\alpha)^1 \cdot f(\alpha^{\gamma^{-1}})^{\gamma_1} \cdot f(\alpha^{\gamma^{-2}})^{\gamma_2} \ldots . f(\alpha^{\gamma^{2-\lambda}})^{\gamma_{\lambda-2}},$$

so erhält man, wenn $\varphi(\eta)$ statt $f(\alpha)$ gesetzt wird,

$$(1.) \qquad \boldsymbol{P}(\alpha) = \varphi(\eta)^{\lambda s_0} \cdot \varphi(\eta_{-1})^{\lambda s_1} \cdot \varphi(\eta_{-2})^{\lambda s_2} \ldots . \varphi(\eta_1)^{\lambda s_{e-1}}.$$

Es ist aber, wie sich leicht zeigen läfst, im gegenwärtigen Fall nicht nur $\boldsymbol{P}(\alpha)$ eine wirkliche complexe Zahl, sondern auch die $\lambda^{\text{te}}$ Wurzel daraus; denn es ist allgemein

$$\frac{\boldsymbol{P}(\alpha)\boldsymbol{P}(\alpha^k)}{\boldsymbol{P}(\alpha^{k+1})} = (\psi_k(\alpha))^\lambda;$$

und wenn $k+1$ einer der Zahlen $\gamma_e, \gamma_{2e}, \ldots . \gamma_{(f-1)e}$ gleich angenommen wird, so ist $\boldsymbol{P}(\alpha) = \boldsymbol{P}(\alpha^{k+1})$ für $f(\alpha) = \varphi(\eta)$, also auch

$$\boldsymbol{P}(\alpha^k) = (\psi_k(\alpha))^\lambda,$$

d. h. $\boldsymbol{P}(\alpha^k)$, und folglich auch $\boldsymbol{P}(\alpha)$ selbst die $\lambda^{\text{te}}$ Potenz einer ***wirklichen***

complexen Zahl. Deshalb ist denn auch

$$\varphi(\eta)^{s_0}\cdot\varphi(\eta_{-1})^{s_1}\cdot\varphi(\eta_{-2})^{s_2}\cdot\ldots\cdot\varphi(\eta_1)^{s_{e-1}}$$

eine ***wirkliche*** complexe Zahl. Es sei nun $s_r$ die kleinste der Zahlen $s_0$, $s_1$, $s_2$, .... $s_{e-1}$, so ist diese wirkliche complexe Zahl noch durch die wirkliche Zahl $[\varphi(\eta)\varphi(\eta_{-1})\varphi(\eta_{-2})\ldots\cdot\varphi(\eta_1)]^{s_r}$ theilbar, und es ist

$$(2.)\qquad \varphi(\eta)^{s_0-s_r}\cdot\varphi(\eta_{-1})^{s_1-s_r}\cdot\varphi(\eta_{-2})^{s_2-s_r}\ldots\cdot\varphi(\eta_1)^{s_{e-1}-s_r} = \Phi(\eta)$$

gleich einer ***wirklichen*** complexen Zahl. Dieses Resultat ist in dem Fall, wo $f$ (die Anzahl der in einer Periode enthaltenen Wurzeln) eine ***gerade*** Zahl ist, nichtssagend: denn alsdann sind die Zahlen $s_0$, $s_1$, $s_2$, .... $s_{e-1}$ alle einander gleich, und man erhält nichts weiter, als dafs ***Eins*** eine wirkliche Zahl ist. Wenn aber $f$ ungerade ist, so sind die Zahlen $s_0$, $s_1$, $s_2$, .... $s_{e-1}$ nicht alle gleich, sondern es ist nur $s_0+s_{\frac{1}{2}e}=s_1+s_{\frac{1}{2}e+1}=s_2+s_{\frac{1}{2}e+2}=\ldots=f$. Multiplicirt man also $\Phi(\eta)$ mit der reciproken complexen Zahl, welche $\Phi(\eta_{\frac{1}{2}e})$ ist, so erhält man

$$(3.)\qquad \Phi(\eta)\cdot\Phi(\eta_{\frac{1}{2}e}) = M^{f-2s_r}.$$

Dies ist das analoge Resultat zu dem von ***Jacobi*** gefundenen $\psi_k(\alpha)\cdot\psi_k(\alpha^{-1})=p$. Der merkwürdigste specielle Fall ist unstreitig der, wenn $e=2$, $f=\frac{1}{2}(\lambda-1)$ und, da $f$ ungerade sein mufs, $\lambda$ von der Form $4n+3$ ist. Hier kommen nur die beiden Perioden $\eta$ und $\eta_1$ vor, deren Werthe bekanntlich $\frac{1}{2}(-1\pm\sqrt{-\lambda})$ sind; ferner ist $\Phi(\eta)=x+y\eta$, $\Phi(\eta_{\frac{1}{2}e})=x+y\eta_1$ und $(x+y\eta)(x+y\eta_1)=x^2-xy+\frac{1}{4}(\lambda+1)y^2$; auch ist hier $\lambda s_0$ gleich der Summe der quadratischen Reste, und $\lambda s_1$ gleich der Summe der quadratischen Nichtreste. Bezeichnet man diese Summen durch $\Sigma a$ und $\Sigma b$, so erhält man

$$(4.)\qquad M^{\frac{1}{\lambda}(\Sigma b-\Sigma a)} = x^2-xy+\tfrac{1}{4}(\lambda+1)y^2;$$

das heifst: die Potenz mit dem Exponenten $\frac{1}{\lambda}(\Sigma b-\Sigma a)$ von einer jeden Zahl, welche überhaupt durch quadratische Formen der Determinante $-\lambda$ dargestellt werden kann, ist stets durch die Hauptform $x^2-xy+\frac{1}{4}(\lambda+1)y^2$ darstellbar. Dasselbe kann auch so ausgedrückt werden: Jede Classe quadratischer Formen der Determinante $-\lambda$, wenn sie $\frac{1}{\lambda}(\Sigma b-\Sigma a)$ mal mit sich selbst zusammengesetzt wird, giebt die Hauptclasse. Es ist dies dasselbe Resultat, aus welchem, zusammengehalten mit dem Satze §. 305. der Disqu. arithm. von Gaufs, ***Jacobi*** zuerst vermuthet hat, dafs die Zahl $\frac{1}{\lambda}(\Sigma b-\Sigma a)$ gleich der Anzahl der nicht äquivalenten Classen der quadratischen Formen der Determinante $-\lambda$ sein dürfte.

(S. dieses Journal Bd. IX. S. 189.) Die allgemeinere Formel (3.) giebt zu ähnlichen Vermuthungen über einen Zusammenhang der Zahlen $s_0, s_1, s_2, \ldots s_{e-1}$, namentlich der Zahl $f-2s_r$ mit der Anzahl der nicht äquivalenten complexen Zahlen für jeden Werth von $\lambda$ Anlafs.

Die Wirklichkeit des Products $\boldsymbol{P}(\alpha)$ für alle beliebigen idealen Zahlen $f(\alpha)$ gewährt noch ein Mittel, zu finden, welche Potenz einer idealen Zahl zu einer wirklichen wird. Giebt man nämlich in dem Ausdrucke von $\boldsymbol{P}(\alpha)$ dem $\alpha$ die Werthe $\alpha, \alpha^2, \alpha^3, \ldots \alpha^{\lambda-1}$, so erhält man $\lambda-1$ Gleichungen, in welchen man $f(\alpha)$, $f(\alpha^2)$, etc. als Unbekannte betrachten kann; und aus diesen Gleichungen, welche für die Logarithmen dieser unbekannten Factoren nur linear sind, kann man, weil sie nicht ganz unabhängig von einander sind, zwar nicht $f(\alpha)$ selbst finden, aber man kann stets den Quotienten $\frac{f(\alpha)}{f(\alpha^{-1})}$, oder vielmehr eine bestimmte Potenz desselben finden, welche, durch $\boldsymbol{P}(\alpha)$, $\boldsymbol{P}(\alpha^2)$, etc. ausgedrückt, eine wirkliche complexe Zahl ist. Ist nun $\varphi(\alpha)$ eine ideale complexe Zahl, von der Art, dafs sie der Bedingung: $\varphi(\alpha)$ äquivalent $f(\alpha^{-1})\varphi(\alpha)$, genügt, für irgend eine Bestimmung der idealen Zahl $f(\alpha)$: so kann man durch Auflösung eines Systems linearer Gleichungen, oder vielmehr nur durch Ausrechnung der Determinante dieses Systems, stets eine Zahl $n$ finden, welche der Bedingung genügt, dafs $(\varphi(\alpha))^n$ eine wirkliche complexe Zahl sei. Die wirkliche Ausrechnung hat folgende bestimmte Werthe des $n$ gegeben: $n=1$ für $\lambda=5, 7, 11, 13, 17$ und $19$, $n=3$ für $\lambda=23$, $n=2$ für $\lambda=29$, $n=9$ für $\lambda=31$, $n=37$ für $\lambda=37$, $n=11$ für $\lambda=41$, $n=211$ für $\lambda=43$, $n=5.139$ für $\lambda=47$.

Die vollständige Bestimmung derjenigen Potenzen idealer Zahlen, welche zu wirklichen werden, so wie auch die Bestimmung der Anzahl nicht äquivalenter idealer Zahlen, erfordert aber noch wesentlich andere Principien, als in der gegenwärtigen Abhandlung enthalten sind. Wir verfolgen diese wichtige Frage auch schon deshalb jetzt nicht weiter, weil, wie bereits erwähnt, die Veröffentlichung einer Arbeit von *Dirichlet* nahe bevorsteht, in welcher er dieselbe Frage für einen sehr nahe verwandten Gegenstand vollständig gelöset hat.

Breslau, im September 1846.