

13.

Über eine besondere Art, aus complexen Einheiten gebildeter Ausdrücke.

(Von Herrn Dr. F. F. Kummer, Professor an der Universität zu Breslau.)

I.

In einer Abhandlung im (44ten Bande S. 106) dieses Journals, über die Ergänzungssätze des allgemeinen Reciprocitätsgesetzes für Potenzreste, habe ich eine Verallgemeinerung der Theorie der *Kreistheilung* gegeben, welche sich an die bekannten, von *Jacobi* durch $\psi(\alpha)$ bezeichneten complexen Zahlen der Kreistheilung anschließt, und welche zur Lösung des in der genannten Abhandlung behandelten Problems grade ausreicht. Eine wesentlich andere Verallgemeinerung der Theorie der Kreistheilung, welche ich vor längerer Zeit zu dem Zwecke ersann, sie als Mittel zu einem Beweise der allgemeinen Reciprocitätsgesetze zu benutzen, schließt sich an die bekannte *Lagrange'sche Resolvente der Kreistheilung* an; und wenn gleich sie den Erwartungen in Betreff der Reciprocitätsgesetze nicht vollständig entsprach, ist sie doch an sich bemerkenswerth, und verbreitet über manche schwierigen Punkte der allgemeinen Theorie der complexen Zahlen ein unerwartetes Licht; weshalb ich dieselbe in dem Folgenden kurz entwickeln will.

Die der *Lagrange'schen Resolvente der Kreistheilung* analogen, aus complexen Einheiten gebildeten Ausdrücke, welche hier behandelt werden sollen, sind in folgender Form enthalten:

$$1 + \varepsilon(x) + \varepsilon(x)\varepsilon(x^g) + \varepsilon(x)\varepsilon(x^g)\varepsilon(x^{g^2}) + \dots + \varepsilon(x)\varepsilon(x^g)\dots\varepsilon(x^{g^{p-3}}),$$

in welcher p eine *Primzahl*, x eine *imaginäre* Wurzel der Gleichung $x^p = 1$, g eine *primitive* Wurzel der Congruenz $g^{p-1} \equiv 1, \text{ Mod. } p$, und $\varepsilon(x)$ eine *complexe Einheit* bezeichnet, deren *Norm*, in Beziehung auf die verschiedenen Werthe von x genommen, gleich *Eins* sei. Damit die Untersuchung sogleich die nöthige Allgemeinheit bekomme, soll hier nicht vorausgesetzt werden, daß die in der complexen Einheit $\varepsilon(x)$ enthaltenen Coëfficienten *ganze* Zahlen sind; sie sollen vielmehr vorläufig ganz unbestimmt gelassen werden,

können also auch selbst wieder irrational sein, jedoch immer nur so, daß

$$N\varepsilon(x) = \varepsilon(x)\varepsilon(x^g)\varepsilon(x^{g^2}) \dots \varepsilon(x^{g^{p-2}}) = 1$$

und $\varepsilon(x)$ eine rationale Function in Beziehung auf x allein ist.

Da der oben aufgestellte Ausdruck durch die zu Grunde gelegte Einheit $\varepsilon(x)$ vollständig bestimmt ist, soll er als Function dieser Einheit angesehen und durch $P\varepsilon(x)$ bezeichnet werden, so daß

$$P\varepsilon(x) = 1 + \varepsilon(x) + \varepsilon(x)\varepsilon(x^g) + \dots + \varepsilon(x)\varepsilon(x^g) \dots \varepsilon(x^{g^{p-3}})$$

ist. Die $p-1$ Glieder, aus welchen dieser Ausdruck besteht, bilden eine vollständige Periode; denn wenn man sich dieselben nach dem herrschenden Gesetze weiter fortgesetzt vorstellt, so wird vermöge der Bedingung

$$N\varepsilon(x) = 1$$

das p^{te} Glied dem ersten gleich, das $p+1^{\text{te}}$ Glied dem zweiten u. s. f. Hieraus folgt, daß wenn man in diesem Ausdrucke x in x^g verwandelt und sodann mit $\varepsilon(x)$ multiplicirt, derselbe ganz ungeändert bleibt, da auf diese Weise nur das erste Glied in das zweite, das zweite in das dritte und so weiter, und das letzte in das erste übergeht. Man hat daher, als erste Grund-Eigenschaft dieser Ausdrücke:

$$(1.) \quad \varepsilon(x)P\varepsilon(x^g) = P\varepsilon(x);$$

was, verallgemeinert, sogleich die folgende giebt:

$$(2.) \quad \varepsilon(x)\varepsilon(x^g) \dots \varepsilon(x^{g^{h-1}})P\varepsilon(x^{g^h}) = P\varepsilon(x).$$

Bei der Verwandlung des x in x^{g^h} ändert sich also dieser Ausdruck nur in so weit, daß eine bestimmte complexe Einheit als Factor hinzutritt. Die Ausdrücke

$$P\varepsilon(x), P\varepsilon(x^g), P\varepsilon(x^{g^2}), \dots P\varepsilon(x^{g^{p-2}})$$

sind, wenn man von den dieselben begleitenden Einheiten absieht, alle als gleich zu erachten.

Setzt man in der Gleichung (2.) nach einander $h = 1, 2, 3 \dots p-1$, und multiplicirt die so entstehenden Gleichungen mit einander, so ergiebt sich:

$$(3.) \quad \varepsilon(x)^{p-1} \cdot \varepsilon(x^g)^{p-2} \cdot \varepsilon(x^{g^2})^{p-3} \dots \varepsilon(x^{g^{p-2}})^1 \cdot NP\varepsilon(x) = (P\varepsilon(x))^{p-1},$$

woraus sogleich

$$(4.) \quad NP\varepsilon(x) = \varepsilon(x^g)^1 \varepsilon(x^{g^2})^2 \dots \varepsilon(x^{g^{p-2}})^{p-2} (P\varepsilon(x))^{p-1}$$

folgt.

Es sei jetzt $e(x)$ eine zweite, ganz beliebige complexe Einheit, so hat man für dieselbe ebenfalls:

$$e(x)Pe(x^g) = Pe(x),$$

und wenn diese Gleichung mit der entsprechenden (1.) multiplicirt wird:

$$\varepsilon(x)e(x)P\varepsilon(x^g)Pe(x^g) = P\varepsilon(x)Pe(x).$$

Da ferner das Product der beiden Einheiten $\varepsilon(x)e(x)$ selbst wieder eine Einheit ist, so hat man für diese gleichfalls:

$$\varepsilon(x)e(x)P(\varepsilon(x^g)e(x^g)) = P(\varepsilon(x)e(x)),$$

und wenn die vorige Gleichung durch diese dividirt wird:

$$\frac{P\varepsilon(x^g)Pe(x^g)}{P(\varepsilon(x^g)e(x^g))} = \frac{P\varepsilon(x)Pe(x)}{P(\varepsilon(x)e(x))}.$$

Auf dieselbe Weise wird aus der Gleichung (2.) bewiesen, daß auch allgemein

$$\frac{P\varepsilon(x^{g^h})Pe(x^{g^h})}{P(\varepsilon(x^{g^h})e(x^{g^h}))} = \frac{P\varepsilon(x)Pe(x)}{P(\varepsilon(x)e(x))} \text{ ist.}$$

Der auf beiden Seiten dieser Gleichung vorkommende Ausdruck bleibt, wie hieraus zu sehen, vollständig ungeändert, wenn statt x irgend eine andere imaginäre Wurzel der Gleichung $x^p = 1$ gesetzt wird; woraus unmittelbar folgt, daß derselbe die Wurzel x in Wahrheit gar nicht enthält, sondern nur die in den Coëfficienten der Einheiten $\varepsilon(x)$ und $e(x)$ vorkommenden Gröfsen. Man hat daher

$$\frac{P\varepsilon(x)Pe(x)}{P(\varepsilon(x)e(x))} = A,$$

oder

$$(5.) \quad P\varepsilon(x)Pe(x) = AP(\varepsilon(x)e(x));$$

wo A eine Gröfse ist, welche die Wurzel x *nicht* enthält. Dies ist die *zweite* allgemeine Grund-Eigenschaft dieser Ausdrücke.

Besonders zu bemerken ist noch das specielle Resultat, welches sich findet, wenn man $e(x) = \frac{1}{\varepsilon(x)}$ annimmt, nämlich:

$$(6.) \quad P\varepsilon(x).P\left(\frac{1}{\varepsilon(x)}\right) = B,$$

wo B eine von x unabhängige Gröfse ist.

Es ist zu bemerken, daß für gewisse, zu Grunde gelegte Einheiten $\varepsilon(x)$ und $e(x)$ die Ausdrücke $P\varepsilon(x)$ und $Pe(x)$ gleich Null werden können,

und auch wirklich gleich Null werden; in welchen Fällen die aufgestellten Grund-Eigenschaften derselben zwar nicht unrichtig, aber nichtssagend werden. Diese ungünstigen Fälle lassen sich aber nunmehr durch geringe, an den Einheiten $\varepsilon(x)$ oder $e(x)$ anzubringende Änderungen leicht vermeiden.

An den gefundenen Grund-Eigenschaften der Ausdrücke $P\varepsilon(x)$ erkennt man sogleich ihre Analogie mit dem *Lagrangeschen* Ausdrücke der Kreistheilung

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

in welchem α irgend eine Wurzel der Gleichung $\alpha^{p-1} = 1$ bezeichnet. Die bekannten Eigenschaften desselben, nämlich

$$\alpha^h F(\alpha, x^{g^h}) = F(\alpha, x), \quad \frac{F(\alpha, x) F(\alpha^r, x)}{F(\alpha^{r+1}, x)} = \psi_r(\alpha),$$

$$F(\alpha, x) F(\alpha^{-1}, x) = \pm p$$

sind offenbar den durch die Gleichungen (2, 5 und 6.) ausgedrückten allgemeinen Eigenschaften der Ausdrücke $P\varepsilon(x)$ vollständig analog. Der Grund der Übereinstimmung in den Fundamental-Eigenschaften liegt einfach darin, daß die *Lagrangesche* Resolvente der Kreistheilungsgleichung $F(\alpha, x)$ in der That nur ein specieller Fall des allgemeineren Ausdrucks $Pe(x)$ ist. Setzt man nämlich die Einheit $\varepsilon(x) = \alpha x^{g-1}$, deren Norm, in Beziehung auf x genommen, gleich α^{p-1} , also gleich *Eins* ist, so hat man:

$$x P(\alpha x^{g-1}) = x + \alpha x^g + \alpha^2 x^{g^2} + \dots + \alpha^{p-2} x^{g^{p-2}} = F(\alpha, x).$$

II.

Für den Zweck des gegenwärtigen Aufsatzes sollen nun den zu Grunde gelegten Einheiten etwas speciellere Bestimmungen gegeben werden; indem festgesetzt wird, daß die Coëfficienten derselben *complex*e, aus den Wurzeln der Gleichung $\alpha^\lambda = 1$ gebildete *ganze* Zahlen sein sollen, wo λ eine *Primzahl* ist, und zwar ein Factor von $p-1$, so daß die Primzahl p von der Form $p = \nu\lambda + 1$ ist. Ich bezeichne demgemäß jetzt die zu Grunde zu legenden complexen Einheiten durch $\varepsilon(\alpha, x)$ und $e(\alpha, x)$ und wiederhole, um Mißverständnissen vorzubeugen, noch einmal, daß dieselben *ganze rationale* Functionen der beiden Wurzeln α und x mit ganzzahligen Coëfficienten sein sollen, und daß die in Beziehung auf x allein genommenen Normen dieser Einheiten gleich *Eins* sein müssen.

Der Ausdruck $P\varepsilon(\alpha, x)$, welcher als eine, die beiden verschiedenen Wurzeln der Einheit α und x enthaltende complexe ganze Zahl mit ganzzahligen Coëfficienten betrachtet werden kann, soll nun in seine idealen oder wirklichen Primfactoren zerlegt werden. Für diese allgemeinere Art der complexen Zahlen, und überhaupt für die aus den n^{ten} Wurzeln der Einheit (wo n eine zusammengesetzte Zahl ist) gebildeten complexen Zahlen existiren, eben so wie für die, für welche $n = \lambda$, gleich einer Primzahl ist (deren Theorie ich vollständig ausgearbeitet und veröffentlicht habe), bestimmte ideale Primfactoren, und für diese auch eben so die Hauptsätze: dafs jede gegebene complexe Zahl nur eine endliche Anzahl unveränderlich bestimmter idealer Primfactoren enthält: dafs zwei complexe Zahlen, welche genau dieselben idealen Primfactoren enthalten, sich nur durch eine Einheit unterscheiden, welche als Factor hinzutreten kann und: dafs eine bestimmte Potenz jeder idealen Zahl einer wirklichen complexen Zahl gleich ist. Aufser diesen allgemeinen Sätzen ist für die gegenwärtige Untersuchung nur noch die nähere Kenntnifs der idealen Primfactoren der Zahl p selbst, für die aus p^{ten} und λ^{ten} Wurzeln der Einheit zugleich gebildeten complexen Zahlen nöthig.

Wenn p , wie vorausgesetzt, eine Primzahl von der Form $p = r\lambda + 1$ ist, so ist bekanntlich für die complexen Zahlen, welche die Wurzel x allein enthalten, $1 - x$ der einzige Primfactor von p . Ferner giebt es für die complexen Zahlen, welche nur α allein, aber nicht x enthalten, $\lambda - 1$ verschiedene ideale Primfactoren von p , welche durch

$$f(\alpha), f(\alpha^\gamma), f(\alpha^{\gamma^2}), \dots f(\alpha^{\gamma^{\lambda-2}})$$

bezeichnet werden sollen; wo γ eine *primitive Wurzel* der Congruenz $\gamma^{\lambda-1} \equiv 1, \text{Mod. } \lambda$ ist. Wird nun ein idealer Primfactor von p für die complexen Zahlen, welche α und x zugleich enthalten, durch $f(\alpha, x)$ bezeichnet, so hat man:

$$f(\alpha, x)f(\alpha, x^g)f(\alpha, x^{g^2}) \dots f(\alpha, x^{g^{p-2}}) = E(\alpha)f(\alpha),$$

$$f(\alpha, x)f(\alpha^\gamma, x)f(\alpha^{\gamma^2}, x) \dots f(\alpha^{\gamma^{\lambda-2}}, x) = E(x)(1-x).$$

Die nur durch die verschiedenen Werthe des x sich unterscheidenden Primfactoren $f(\alpha, x), f(\alpha, x^g), f(\alpha, x^{g^2})$, u. s. w. sind alle als gleich zu erachten; eben so wie die Factoren $1 - x, 1 - x^g, 1 - x^{g^2}$, u. s. w., abgesehen von den Einheiten, einander gleich sind. Es sind daher in p nur $\lambda - 1$ wirklich von einander verschiedene ideale Primfactoren von der Form $f(\alpha^{\gamma^i}, x^{g^h})$

vorhanden, nämlich:

$$f(\alpha, x), \quad f(\alpha', x), \quad f(\alpha'^2, x), \quad \dots \quad f(\alpha'^{\lambda-2}, x).$$

Diesemnach ist auch

$$f(\alpha, x)^{p-1} = E(\alpha, x) f(\alpha),$$

wo $E(\alpha, x)$ eine Einheit bezeichnet.

Um zu finden, ob eine gegebene complexe Zahl $\varphi(\alpha, x)$ einen bestimmten der $\lambda - 1$ verschiedenen idealen Primfactoren von p , z. B. den idealen Primfactor $f(\alpha'^h, x)$ enthält, oder nicht, hat man nur zu untersuchen, ob dieselbe complexe Zahl, wenn in ihr *Ein*s statt x gesetzt wird, den Primfactor $f(\alpha'^h)$ enthält. Wenn nämlich $\varphi(\alpha, 1)$ den Primfactor $f(\alpha'^h)$ enthält, so enthält auch $\varphi(\alpha, x)$ den idealen Primfactor $f(\alpha'^h, x)$, und wenn $\varphi(\alpha, 1)$ den Primfactor $f(\alpha'^h)$ nicht enthält, so enthält auch $\varphi(\alpha, x)$ nicht den Primfactor $f(\alpha'^h, x)$.

Diese allgemeinen und besondern Sätze über die idealen Primfactoren der die beiden Wurzeln der Einheit α und x zugleich enthaltenden complexen Zahlen lassen sich nach denselben Principien beweisen, welche ich für die, nur die Wurzel α allein enthaltenden complexen Zahlen im (35ten Bande S. 327 sqq.) dieses Journals vollständig entwickelt habe. Aus diesem Grunde glaube ich die Ausführung der Beweise der hier angeführten Hülfsätze jetzt ersparen zu dürfen, und werde die Sätze sogleich auf die Zerlegung der complexen Zahl $P\varepsilon(\alpha, x)$ anwenden.

Zufolge der ersten Grund-Eigenschaft der obigen Ausdrücke hat man:

$$\varepsilon(\alpha, x) P\varepsilon(\alpha, x^g) = P\varepsilon(\alpha, x).$$

Nimmt man auf beiden Seiten die *Norm* in Beziehung auf α allein, d. h. das Product für alle Werthe $\alpha, \alpha', \alpha'^2, \dots, \alpha'^{\lambda-2}$, so hat man, wenn diese partielle Norm durch N_α bezeichnet wird:

$$N_\alpha \varepsilon(\alpha, x) \cdot N_\alpha P\varepsilon(\alpha, x^g) = N_\alpha P\varepsilon(\alpha, x),$$

und wenn

$$N_\alpha \varepsilon(\alpha, x) = E(x), \quad N_\alpha P\varepsilon(\alpha, x) = F(x)$$

gesetzt wird, so ist

$$E(x) F(x^g) = F(x).$$

Einer solchen Gleichung für complexe Zahlen, welche nur x allein enthalten, und keine andere Irrationalität, kann aber nach der bekannten Theorie

dieser complexen Zahlen keine andere Zahl $F(x)$ genügen, als eine solche von der Form

$$F(x) = C.E(x)(1-x)^r,$$

in welcher C eine nicht complexe ganze Zahl, $E(x)$ eine complexe Einheit und r eine ganze Zahl ist. Es ergibt sich also hiernach:

$$N_\alpha P_\varepsilon(\alpha, x) = C.E(x)(1-x)^r.$$

Hieraus folgt, daß die complexe Zahl $P_\varepsilon(\alpha, x)$ selbst, nur Factoren von einer der folgenden drei Arten enthalten kann: nämlich *erstens* solche, deren Normen, in Beziehung auf α allein genommen, ganze, nicht complexe Zahlen sind, welche also kein x enthalten und nur von der Form $\varphi(\alpha)$ sein können; *zweitens* solche, deren Normen, in Beziehung auf α genommen, Einheiten sind, welche also selbst nur Einheiten von der Form $E(\alpha, x)$ sein können; endlich *drittens* solche, deren in Beziehung auf α genommene Normen gleich $1-x$ oder gleich einer Potenz von $1-x$ sind, also nur die idealen Primfactoren von $1-x$, oder, was Dasselbe ist, von p , nämlich:

$$f(\alpha, x), \quad f(\alpha^\gamma, x), \quad f(\alpha^{\gamma^2}, x), \quad \dots \quad f(\alpha^{\gamma^{\lambda-2}}, x).$$

Dem Ausdrücke $P_\varepsilon(\alpha, x)$ kann also immer folgende Form gegeben werden:

$$P_\varepsilon(\alpha, x) = \varphi(\alpha) E(\alpha, x) f(\alpha, x)^m \cdot f(\alpha^\gamma, x)^{m_1} \cdot f(\alpha^{\gamma^2}, x)^{m_2} \dots f(\alpha^{\gamma^{\lambda-2}}, x)^{m_{\lambda-2}}.$$

Für die Bestimmung der Exponenten $m, m_1, m_2, \dots, m_{\lambda-2}$, welche jetzt allgemein ausgeführt werden soll, ist wesentlich zu bemerken, daß alle Vielfachen von $p-1$, welche etwa in denselben enthalten sein sollten, gänzlich vernachlässigt werden können; weil nämlich, nach der Eigenschaft der idealen complexen Primfactoren von p ,

$$f(\alpha^{\gamma^h}, x)^{p-1} = f(\alpha^\gamma) E(\alpha^{\gamma^h}, x)$$

die $(p-1)^{\text{te}}$ Potenz eines solchen Primfactors einer nur α allein enthaltenden complexen Zahl, multiplicirt mit einer Einheit, gleich ist; so daß man diese immer mit dem Factor $\varphi(\alpha)$ und der Einheit $E(\alpha, x)$ verbunden annehmen kann. Mit Rücksicht hierauf werden die Exponenten $m, m_1, \dots, m_{\lambda-2}$ am leichtesten dadurch bestimmt, daß man den Ausdruck

$$P\left(\frac{1-x^r}{1-x} \varepsilon(\alpha, x)\right)$$

in Betracht zieht, und untersucht, unter welcher Bedingung derselbe einen der idealen Primfactoren von p , z. B. $f(\alpha^{\gamma^h}, x)$ nicht enthält. Die hierzu noth-

wendige und hinreichende Bedingung ist, nach Dem was oben bemerkt worden, die, daß dieser Ausdruck, für $x=1$, nämlich

$$1 + g^r \varepsilon(\alpha, 1) + g^{2r} \varepsilon(\alpha, 1)^2 + \dots + g^{(p-2)r} \varepsilon(\alpha, 1)^{p-2}$$

den Factor $f(\alpha^{\gamma^h})$ nicht enthalte. Jede, nur die eine Wurzel der Einheit α enthaltende complexe Zahl ist aber bekanntlich nach dem Modul $f(\alpha^{\gamma^h})$, welcher ein idealer Primfactor von p ist, einer nichtcomplexen ganzen Zahl congruent, welche sich wiederum als Potenz der primitiven Wurzel g darstellen läßt, wenn sie nicht congruent Null ist. Setzt man daher

$$\varepsilon(\alpha, 1) \equiv g^s, \quad \text{Mod. } f(\alpha^{\gamma^h}),$$

so geht die obige Bedingung in folgende über:

$$1 + g^{r+s} + g^{2r+2s} + \dots + g^{(p-2)(r+s)} \text{ nicht } \equiv 0,$$

für den Modul $f(\alpha^{\gamma^h})$, also auch für den Modul p ; aus welcher dann unmittelbar folgt, daß

$$r + s \equiv 0, \quad \text{Mod. } p-1,$$

sein muß. Nun hat man aber vermöge der Grund-Eigenschaft:

$$A \cdot P\left(\frac{1-x^{g^r}}{1-x} \varepsilon(\alpha, x)\right) = P\left(\frac{1-x^{g^r}}{1-x}\right) \cdot P\varepsilon(\alpha, x);$$

wo A von der Wurzel der Einheit x unabhängig ist. Ferner ist aus der Definition der mit $P\varepsilon(x)$ bezeichneten Ausdrücke selbst, leicht zu zeigen, daß

$$P\left(\frac{1-x^{g^r}}{1-x}\right) = \frac{C}{(1-x)(1-x^g) \dots (1-x^{g^{r-1}})} = \frac{CE(x)}{(1-x)^r}$$

ist, wo C eine ganze Zahl und $E(x)$ eine Einheit ist. Der ideale Primfactor $f(\alpha^{\gamma^h}, x)$ von p ist also in $P\left(\frac{1-x^{g^r}}{1-x}\right)$ genau $(p-1-r)$ mal enthalten, und da derselbe nach der oben angesetzten Form in $P\varepsilon(\alpha, x)$ genau m_h mal enthalten ist, so folgt, daß

$$P\left(\frac{1-x^{g^r}}{1-x} \varepsilon(\alpha, x)\right)$$

diesen idealen Primfactor $(p-1-r+m_h)$ mal enthält; wobei $p-1$, oder jedes beliebige Vielfache von $p-1$, hinzugefügt, oder auch weggelassen werden kann. Die Bedingung, daß dieser Ausdruck den idealen Primfactor $f(\alpha^{\gamma^h}, x)$ nicht enthalte, ist also:

$$m_h - r \equiv 0, \quad \text{Mod. } p-1,$$

und weil oben, für dieselbe Bedingung,

$$r + s \equiv 0, \text{ Mod. } p-1$$

gefunden wurde, so ergibt sich:

$$s \equiv -m_h, \text{ Mod. } p-1,$$

also auch:

$$\varepsilon(\alpha, 1) \equiv g^{-m_h}, \text{ Mod. } f(\alpha^{\gamma^h});$$

welche Congruenz die gesuchte Bestimmung der Exponenten $m, m_1, \dots, m_{\lambda-2}$ enthält.

Um dieselbe in ihrer einfachsten Form darzustellen, verwandle ich α in $\alpha^{\gamma^{-h}}$. Dies giebt

$$\varepsilon(\alpha^{\gamma^{-h}}, 1) \equiv g^{-m_h}, \text{ Mod. } f(\alpha).$$

Ferner bezeichne ich allgemein durch $\text{Ind. } \varphi(\alpha)$ den Index der complexen Zahl $\varphi(\alpha)$, für den Modul $f(\alpha)$ und für die primitive Wurzel g ; dann ist

$$(7.) \quad m_h \equiv -\text{Ind. } \varepsilon(\alpha^{\gamma^{-h}}, 1), \text{ Mod. } p-1,$$

die gesuchte Bestimmung der Exponenten in dem Ausdrücke

$$(8.) \quad P\varepsilon(\alpha, x) = \varphi(\alpha) E(\alpha, x) \cdot f(\alpha, x)^m \cdot f(\alpha^{\gamma}, x)^{m_1} \cdot f(\alpha^{\gamma^2}, x)^{m_2} \dots f(\alpha^{\gamma^{\lambda-2}}, x)^{m_{\lambda-2}}.$$

In dieser allgemeinen Formel ist unter andern auch die Zerlegung der *Lagrangeschen* Resolvente der Kreistheilung, welche oben mit $F(\alpha, x)$ bezeichnet wurde, in ihre idealen Primfactoren enthalten, und es werden für dieselbe, wenn man die Gleichung $F(\alpha, x)F(\alpha^{-1}, x) = p$ zu Hülfe nimmt, die Exponenten $m, m_1, \dots, m_{\lambda-2}$ nicht nur durch Congruenzen für den Modul $p-1$, sondern vollständig bestimmt. Man erhält nämlich, wenn man $\varepsilon(\alpha, x) = \alpha^{-1} x^{g-1}$ annimmt:

$$F(\alpha^{-1}, x) = E(\alpha, x) f(\alpha, x)^{\nu} \cdot f(\alpha^{\gamma}, x)^{\nu\gamma-1} f(\alpha^{\gamma^2}, x)^{\nu\gamma-2} \dots f(\alpha^{\gamma^{\lambda-2}}, x)^{\nu\gamma-(\lambda-2)},$$

wo $E(\alpha, x)$ eine Einheit und γ^{-h} die kleinste positive Zahl bezeichnet, welche der Potenz γ^{-h} congruent ist, für den Modul λ , $\nu = \frac{p-1}{\lambda}$; und dieser Ausdruck stimmt vollständig mit demjenigen überein, welchen ich früher für die λ^{te} Potenz dieser *Lagrangeschen* Resolvente gegeben habe.

Für die Anwendung, welche hier von der Zerlegung des Ausdrucks $P\varepsilon(\alpha, x)$ in seine idealen Primfactoren gemacht werden soll, nehme man noch eine besondere Einheit für $\varepsilon(\alpha, x)$ an, welche nicht sowohl die Wurzeln x, x^g , u. s. w. selbst, sondern nur die λ Perioden derselben, von je ν Glied-

dern, enthält. Wird eine beliebige von diesen Perioden durch η_r bezeichnet, so dafs

$$\eta_r = x^{g^r} + x^{g^{\lambda+r}} + x^{g^{2\lambda+r}} + \dots + x^{g^{(\nu-1)\lambda+r}}$$

ist, so ist

$$(1 - \alpha x)(1 - \alpha x^{g^\lambda})(1 - \alpha x^{g^{2\lambda}}) \dots (1 - \alpha x^{g^{(\nu-1)\lambda}}) = e(\alpha, \eta)$$

eine Einheit, welche nur die Perioden $\eta, \eta_1, \dots, \eta_{\lambda-1}$ enthält, und deren in Beziehung auf diese Perioden allein genommene Norm gleich *Eins* ist. Aus dieser setze man nun die folgende zusammen:

$$E_n(\alpha, \eta) = e(\alpha, \eta) e(\alpha^\gamma, \eta)^{\gamma^{-2n}} e(\alpha^{\gamma^2}, \eta)^{\gamma^{-4n}} \dots e(\alpha^{\gamma^{\lambda-2}}, \eta)^{\gamma^{-2(\lambda-2)n}},$$

und bilde den Ausdruck

$$PE_n(\alpha, \eta) = \varphi(\alpha) E(\alpha, x) f(\alpha, x)^m f(\alpha^\gamma, x)^{m_1} \dots f(\alpha^{\gamma^{\lambda-2}}, x)^{m_{\lambda-2}}.$$

Um allgemein den Exponenten m_h zu bestimmen, mufs man in der Einheit $E_n(\alpha^{\gamma^{-h}}, \eta)$ dem x den Werth *Eins* geben, wodurch dieselbe in

$$(1 - \alpha^{\gamma^{-h}})^\nu (1 - \alpha^{\gamma^{1-h}})^{\nu\gamma^{-2n}} (1 - \alpha^{\gamma^{2-h}})^{\nu\gamma^{-4n}} \dots (1 - \alpha^{\gamma^{\lambda-2-h}})^{\nu\gamma^{-2(\lambda-2)n}}$$

übergeht. Hieraus folgt sogleich, nach der Congruenz (7.):

$$m_h \equiv -\nu \sum_0^{\lambda-2} \gamma^{-2ni} \text{Ind.}(1 - \alpha^{\gamma^{i-h}}), \quad \text{Mod. } p-1,$$

und wenn in dieser Summe i in $i+h$ verwandelt wird:

$$m_h \equiv -\nu\gamma^{-2nh} \sum_0^{\lambda-2} \gamma^{-2ni} \text{Ind.}(1 - \alpha^{\gamma^i}), \quad \text{Mod. } p-1.$$

Wird nun der Kürze wegen

$$\sum_0^{\lambda-2} \gamma^{-2ni} \text{Ind.}(1 - \alpha^{\gamma^i}) \equiv -s, \quad \text{Mod. } \lambda,$$

gesetzt, so ist

$$m_h \equiv \nu s \gamma^{-2nh},$$

und diesemnach:

$$PE_n(\alpha, \eta) = \varphi(\alpha) E(\alpha, x) \{f(\alpha, x) f(\alpha^\gamma, x)^{\gamma^{-2n}} \dots f(\alpha^{\gamma^{\lambda-2}}, x)^{\gamma^{-2(\lambda-2)n}}\}^{\nu s}.$$

Die Seite rechts in dieser Gleichung läfst sich ebenfalls leicht als Function der λ Perioden $\eta, \eta_1, \dots, \eta_{\lambda-1}$ darstellen. Setzt man nämlich

$$f(\alpha, x) f(\alpha, x^{g^\lambda}) f(\alpha, x^{g^{2\lambda}}) \dots f(\alpha, x^{g^{(\nu-1)\lambda}}) = f(\alpha, \eta),$$

so ist, weil, abgesehen von den Einheiten, $f(\alpha, x), f(\alpha, x^{g^\lambda})$ u. s. w. einander gleich sind, eben so auch

$$f(\alpha, \eta)^\lambda = f(\alpha) \quad \text{und} \quad f(\alpha, \eta) = f(\alpha, x)^\nu,$$

und wenn man von diesen Ausdrücken Gebrauch macht, so erhält man

$$(9.) \quad PE_n(\alpha, \eta) = \varphi(\alpha) E(\alpha, \eta) \{f(\alpha, \eta) f(\alpha^\gamma, \eta)^{\gamma^{-2n}} \dots f(\alpha^{\gamma^{\lambda-2}}, \eta)^{\gamma^{-2(\lambda-2)n}}\}^s.$$

Nimmt man auf beiden Seiten die *Norm* in Beziehung auf die λ Perioden, und erwägt, daß $Nf(\alpha, \eta) = f(\alpha)$ ist, so hat man:

$$(10.) \quad NPE_n(\alpha, \eta) = \varphi(\alpha)^\lambda E(\alpha) \{f(\alpha) f(\alpha^\gamma)^{\gamma^{-2n}} \dots f(\alpha^{\gamma^{\lambda-2}})^{\gamma^{-2(\lambda-2)n}}\}^s.$$

Damit dieser Ausdruck für die in dem Folgenden davon zu machende Anwendung noch besser zubereitet werde, wende man eine, nur die Perioden $\eta, \eta_1, \dots, \eta_{\lambda-1}$ enthaltende, von α ganz unabhängige Einheit an, nämlich:

$$\frac{(1-x^g)(1-x^{g^{\lambda+1}})(1-x^{g^{2\lambda+1}}) \dots (1-x^{g^{(\nu-1)\lambda+1}})}{(1-x)(1-x^{g^\lambda})(1-x^{g^{2\lambda}}) \dots (1-x^{g^{(\nu-1)\lambda+1}})} = e(\eta),$$

Für diese Einheit findet sich nach den oben gegebenen allgemeinen Regeln sehr leicht:

$$P(e(\eta)^s) = C.E(\eta) \{f(\alpha, \eta) f(\alpha^\gamma, \eta) f(\alpha^{\gamma^2}, \eta) \dots f(\alpha^{\gamma^{\lambda-2}}, \eta)\}^{-s},$$

und wenn man diesen Ausdruck mit dem obigen (9.) multiplicirt, so erhält man, unter Anwendung der Grund-Eigenschaft (5.), folgendes Resultat:

$$(11.) \quad P(e(\eta)^s E_n(\alpha, \eta)) \\ = \varphi(\alpha) E(\alpha, \eta) \{f(\alpha^\gamma, \eta)^{\gamma^{-2n-1}} f(\alpha^{\gamma^2}, \eta)^{\gamma^{-4n-1}} \dots f(\alpha^{\gamma^{\lambda-2}}, \eta)^{\gamma^{-2(\lambda-2)n-1}}\}^s.$$

Nimmt man endlich noch die Norm in Beziehung auf die Perioden $\eta, \eta_1, \dots, \eta_{\lambda-1}$, so ergibt sich auch

$$(12.) \quad NP(e(\eta)^s E_n(\alpha, \eta)) \\ = \varphi(\alpha)^\lambda E(\alpha) \{f(\alpha^\gamma)^{\gamma^{-2n-1}} f(\alpha^{\gamma^2})^{\gamma^{-4n-1}} \dots f(\alpha^{\gamma^{\lambda-2}})^{\gamma^{-2(\lambda-2)n-1}}\}^s,$$

wo

$$s \equiv -\sum_0^{\lambda-2} \gamma^{-2ni} \text{Ind}(1 - \alpha^{\gamma^i}), \quad \text{Mod. } \lambda \text{ ist.}$$

Die Gröfse s ist aus meiner Abhandlung über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen (Band 44. dieses Journals) näher bekannt. Sie läßt sich, wie daselbst (S. 99) gezeigt, in folgende Form schreiben:

$$(13.) \quad s \equiv \frac{-2 \text{Ind } E_n(\alpha)}{\gamma^{2n} - 1},$$

wo $E_n(\alpha)$ die zusammengesetzte Kreistheilungs-Einheit bezeichnet, deren Index in der genannten Abhandlung gefunden wird, nämlich die Einheit

$$E_n(\alpha) = e(\alpha) e(\alpha^\gamma)^{\gamma^{-2n}} e(\alpha^{\gamma^2})^{\gamma^{-4n}} \dots e(\alpha^{\gamma^{\mu-1}})^{-2(\mu-1)n},$$

für

$$\mu = \frac{1}{2}(\lambda - 1) \quad \text{und} \quad e(\alpha) = \sqrt{\frac{(1-\alpha^\gamma)(1-\alpha^{-\gamma})}{(1-\alpha)(1-\alpha^{-1})}}.$$

III.

Es sollen jetzt die gefundenen Resultate auf denjenigen Fall der allgemeinen Reciprocitätsgesetze angewendet werden, wo zwei conjugirte complexe Primzahlen mit einander zu vergleichen sind.

Zu diesem Zwecke müssen zunächst die in der Formel (12.) vorkommenden idealen oder wirklichen complexen Primfactoren von p , nämlich $f(\alpha)$, $f(\alpha^\gamma)$, $f(\alpha^{\gamma^2})$, u. s. w., in Betreff der Einheiten mit welchen sie multiplicirt sein können, näher bestimmt werden. Wenn sie ideal sind, so werden sie zunächst zu einer Potenz des Exponenten H erhoben; was sie zu wirklichen complexen Zahlen macht. Diese wirklichen complexen Zahlen werden sodann durch Multiplication mit passenden Einheiten in die Form gebracht, welche ich als die *primäre* bezeichne, in welcher nämlich die complexe Zahl den beiden Bedingungen genügen muß: *erstens*: dafs sie für den Modul $(1-\alpha)^2$ einer nicht complexen ganzen Zahl congruent ist; *zweitens*: dafs sie, mit ihrer reciproken multiplicirt, ein Product giebt, welches, für den Modul λ , einer nicht complexen ganzen Zahl congruent ist. Auf diese primäre Form läßt sich auch, wie ich früher bewiesen habe, jede aus λ^{ten} Wurzeln der Einheit gebildete complexe Zahl bringen, aufser wenn λ eine von denjenigen Ausnahmезahlen ist, die in einer der ersten $\frac{1}{2}(\lambda - 3)$ *Bernoullischen* Zahlen als Factoren des Zählers vorkommen (M. s. dieses Journal Bd. 44. S. 138 u. S. 141). Diese Ausnahmезahlen, für welche auch der niedrigste Exponent H derjenigen Potenz von $f(\alpha)$, welche *wirklich* wird, durch λ theilbar sein kann, sollen aus diesem Grunde von der gegenwärtigen Untersuchung ausgeschlossen bleiben.

Unter der Voraussetzung, dafs die Primfactoren $f(\alpha)$, $f(\alpha^\gamma)$, u. s. w. von p in der primären Form genommen werden, ist nun, wie leicht zu sehen, die H^{te} Potenz des Products

$$f(\alpha^\gamma)^{\gamma^{-2n}-1} \cdot f(\alpha^{\gamma^2})^{\gamma^{-4n}-1} \dots f(\alpha^{\gamma^{\lambda-2}})^{\gamma^{-2(\lambda-2)n}-1}$$

einer nicht complexen ganzen Zahl c für den Modul λ congruent. Wenn man daher beide Seiten der Gleichung (12.) zur H^{ten} Potenz erhebt, und daraus eine Congruenz für den Modul λ bildet, so erhält man:

$$[NP(e(\eta)^H E_n(\alpha, \eta))]^H \equiv cE(\alpha)^H, \quad \text{Mod. } \lambda.$$

29 *

Nach den oben in (§. I.) bewiesenen Grund-Eigenschaften der Ausdrücke $P\epsilon(x)$ wird nun die Norm eines solchen Ausdrucks folgendermaßen durch eine Potenz desselben ausgedrückt:

$$NP(e(\eta)^s E_n(\alpha, \eta)) = \sum_0^{\lambda-1} e(\eta_i)^{si} E_n(\alpha, \eta_i)^i \cdot (Pe(\eta)^s E_n(\alpha, \eta))^\lambda.$$

Beachtet man, daß in Beziehung auf den Modul λ jede λ^{te} Potenz einer complexen Zahl, welche α enthält, einer von α unabhängigen Zahl congruent ist, so findet sich

$$NP(e(\eta)^s E_n(\alpha, \eta)) \equiv C \sum_0^{\lambda-1} E_n(\alpha, \eta_i)^i, \quad \text{Mod. } \lambda,$$

wo C eine complexe Zahl ist, welche zwar die Perioden $\eta, \eta_1, \text{etc.}$, nicht aber die Wurzel der Einheit α enthält. Aus dieser Congruenz, verglichen mit der vorhergehenden, folgt

$$cE(\alpha)^H \equiv C^H \sum_0^{\lambda-1} E_n(\alpha, \eta_i)^{iH}, \quad \text{Mod. } \lambda.$$

Hieraus soll nun die bisher unbestimmte Einheit $E(\alpha)$ näher bestimmt werden. Zu diesem Zwecke nehme ich auf beiden Seiten der Congruenz die *Logarithmen*; und zwar in dem Sinne, in welchem ich die Theorie der logarithmischen Ausdrücke für complexe Zahlen in der mehrmals erwähnten Abhandlung (dieses Journals Bd. 44. S. 130 etc.) entwickelt habe. Dies giebt, wenn man noch durch H , welches nach der Annahme nicht durch λ theilbar ist, dividirt:

$$l\left(\frac{E(\alpha)}{E(1)}\right) \equiv \sum_0^{\lambda-1} i l\left(\frac{E_n(\alpha, \eta_i)}{E_n(1, \eta_i)}\right), \quad \text{Mod. } \lambda,$$

und da

$$E_n(\alpha, \eta) = e(\alpha, \eta) e(\alpha^\gamma, \eta)^{\gamma^{-2n}} \dots e(\alpha^{\gamma^{\lambda-2}}, \eta)^{\gamma^{-2(\lambda-2)n}},$$

$$e(\alpha, \eta) = (1 - \alpha x)(1 - \alpha x^{\gamma^\lambda}) \dots (1 - \alpha x^{\gamma^{(\lambda-1)\lambda}})$$

ist, so verwandelt sich dieser Ausdruck leicht in den folgenden:

$$l\left(\frac{E(\alpha)}{E(1)}\right) \equiv \sum_0^{p-2} \sum_0^{\lambda-2} i \gamma^{-2nh} l\left(\frac{1 - \alpha^{\gamma^h} x^{\gamma^i}}{1 - x^{\gamma^i}}\right), \quad \text{Mod. } \lambda.$$

Ich mache jetzt von der allgemeinen Formel meiner Abhandlung (Bd. 44. S. 134) Gebrauch, nämlich von der Formel

$$\sum_0^{\lambda-2} \gamma^{-kh} l\left(\frac{\varphi(\alpha^{\gamma^h})}{\varphi(1)}\right) \equiv \frac{d_0^k l\varphi(e^v)}{dv^k} X_k(\alpha), \quad \text{Mod. } \lambda,$$

in welcher

$$X_k(\alpha) = \alpha + \gamma^{-k} \alpha^\gamma + \gamma^{-2k} \alpha^{\gamma^2} + \dots + \gamma^{-(\lambda-2)k} \alpha^{\gamma^{\lambda-2}}$$

ist, und vermöge deren, wenn $\varphi(\alpha)$ hier gleich $1 - \alpha x^{g^i}$ angenommen wird, der gefundene Ausdruck sich in folgenden verwandelt:

$$l\left(\frac{E(\alpha)}{E(1)}\right) \equiv \sum_0^{p-2} \frac{i d_0^{2n} l(1 - e^v x^{g^i})}{d v^{2n}} X_{2n}(\alpha), \quad \text{Mod. } \lambda,$$

oder, wenn der Kürze wegen

$$(14.) \quad \sum_0^{p-2} \frac{i d_0^{2n} l(1 - e^v x^{g^i})}{d v^{2n}} \equiv D_n, \quad \text{Mod. } \lambda,$$

gesetzt wird, in

$$l\left(\frac{E(\alpha)}{E(1)}\right) \equiv D_n X_{2n}(\alpha), \quad \text{Mod. } \lambda.$$

Für die zusammengesetzte Kreistheilungs-Einheit $E_n(\alpha)$, dieselbe, welche oben in (§. II.) vollständig definit wurde, hat man aber nach (S. 139.) der erwähnten Abhandlung:

$$l\left(\frac{E_n(\alpha)}{E_n(1)}\right) \equiv \frac{(-1)^{n+1}(\gamma^{2n}-1)B_n}{4n} X_{2n}(\alpha), \quad \text{Mod. } \lambda,$$

wo B_n die n^{te} Bernoullische Zahl bezeichnet. Also wenn M_n durch die Congruenz

$$(15.) \quad \frac{(-1)^{n+1}(\gamma^{2n}-1)B_n}{4n} \cdot M_n \equiv D_n, \quad \text{Mod. } \lambda,$$

bestimmt wird, so ist

$$l\left(\frac{E(\alpha)}{E(1)}\right) \equiv M_n \cdot l\left(\frac{E_n(\alpha)}{E_n(1)}\right);$$

woraus nach der bekannten Theorie dieser logarithmischen Ausdrücke und der Einheiten, ohne Schwierigkeit

$$(16.) \quad E(\alpha) = E_n(\alpha)^{M_n},$$

folgt, und wo die gesuchte Bestimmung der Einheit $E(\alpha)$ in der Gleichung (12.) liegt.

Das besondere Reciprocitätsgesetz, welches hier entwickelt werden soll, liegt nur in der Congruenz (15.), welche M_n und D_n verbindet. Diese Größen lassen sich nämlich beide durch die Indices der complexen Primzahlen $f(\alpha^\gamma)$, $f(\alpha^{\gamma^2})$, ..., $f(\alpha^{\gamma^{\lambda-2}})$, in Beziehung auf den Modul $f(\alpha)$ genommen, ausdrücken, so daß diese Congruenz für die verschiedenen Werthe 1, 2, 3, ... $\frac{1}{2}(\lambda-3)$ von n , ebenso viele Reciprocitätsgleichungen giebt, aus welchen

das einfache Gesetz, wie ich es längst durch Induction gefunden hatte, sich leicht entwickeln läßt. Ich beginne mit der Entwicklung der Gröfse

$$D_n \equiv \sum_0^{p-2} i d_0^{2n} l(1 - e^v x^{g^i}), \text{ Mod. } \lambda.$$

Zunächst hat man

$$\frac{dl(1 - e^v x)}{dv} = \frac{-e^v x}{1 - e^v x};$$

was auf folgende Form gebracht werden kann:

$$\frac{-e^v x}{1 - e^v x} = \frac{x + (1 + e^v)x^2 + (1 + e^v + e^{2v})x^3 + \dots + (1 + e^v + \dots + e^{(p-1)v})x^p}{1 + e^v + e^{2v} + \dots + e^{(p-1)v}},$$

deren Richtigkeit sogleich durch Multiplication mit dem Nenner $1 - e^v x$ ersichtlich wird. Bildet man nun den $(2n-1)^{\text{ten}}$ Differentialquotienten dieses Bruchs, und setzt darin $v=0$, so werden alle Differentialquotienten des Nenners $1 + e^v + \dots + e^{(p-1)v}$, vom ersten bis zum $(2n-1)^{\text{ten}}$, congruent *Null*, für den Modul λ ; dieser Nenner selbst aber wird congruent *Eins*. Die Differentialquotienten dieses Bruchs sind daher für $v=0$ nur den Differentialquotienten seines Zählers für $v=0$ congruent. Man erhält also:

$$\frac{d_0^{2n} l(1 - e^v x)}{dv^{2n}} \equiv 1^{2n-1} x^2 + (1^{2n-1} + 2^{2n-1}) x^3 + \dots + (1^{2n-1} + 2^{2n-1} + \dots + (p-1)^{2n-1}) x^p,$$

oder, wenn der Kürze wegen

$$1^{2n-1} + 2^{2n-1} + 3^{2n-1} + \dots + (k-1)^{2n-1} = S_{2n-1}(k)$$

gesetzt wird, und wenn man beachtet, dafs $S_{2n-1}(p) \equiv 0$ für den Modul λ ist, so hat man

$$\frac{d_0^{2n} l(1 - e^v x)}{dv^{2n}} \equiv \sum_2^{p-1} S_{2n-1}(k) x^k, \text{ Mod. } \lambda,$$

und demgemäfs:

$$D_n \equiv \sum_0^{p-2} \sum_2^{p-1} i S_{2n-1}(k) x^{kg^i}, \text{ Mod. } \lambda.$$

Setzt man in dem Exponenten von x , $g^{\text{Ind. } k}$ statt k und verwandelt i in $i - \text{Ind. } k$, wobei man dem veränderten i wieder genau dieselben Werthe $i=0, 1, 2, \dots, p-2$ lassen kann, so wird

$$D_n \equiv \sum_0^{p-2} \sum_2^{p-1} (i - \text{Ind. } k) S_{2n-1}(k) x^{g^i},$$

und da $\sum_2^{p-1} S_{2n-1}(k) \equiv 0, \text{ Mod. } \lambda$, $\sum_0^{p-2} x^{g^i} = -1$ ist, so fällt x aus dieser Con-

gruenz gänzlich weg, und es wird

$$D_n \equiv \sum_k^{p-1} S_{2n-1}(k) \text{Ind. } k, \quad \text{Mod. } \lambda.$$

Dieser Ausdruck wird zu dem vorliegenden Zwecke weiter auf folgende Weise eingerichtet. Zunächst wird die einfache Summe, indem man $k + h\lambda$ statt k setzt, in folgende Doppelsumme verwandelt:

$$D_n \equiv \sum_k^{\lambda-1} \sum_h^{\nu-1} S_{2n-1}(k) \text{Ind. } (k + h\lambda).$$

Sodann ist

$$\text{Ind. } (k + h\lambda) \equiv \text{Ind. } (k\nu + h\lambda\nu) - \text{Ind. } \nu,$$

und da $\lambda\nu = p-1$ ist, und da die Vielfachen von p innerhalb der Indices weggelassen werden können,

$$\text{Ind. } (k + h\lambda) \equiv \text{Ind. } (k\nu - h) - \text{Ind. } \nu,$$

also

$$\sum_h^{\nu-1} \text{Ind. } (k + h\lambda) \equiv \text{Ind. } \left(\frac{\Pi k\nu}{\Pi(k-1)\nu} \right) - \nu \text{Ind. } \nu,$$

wenn $\Pi(r) = 1.2.3 \dots r$ oder

$$\sum_h^{\nu-1} \text{Ind. } (k + h\lambda) \equiv \text{Ind. } \left(\frac{\Pi k\nu}{\Pi(k-1)\nu \Pi\nu} \right) - \nu \text{Ind. } \nu + \text{Ind. } \Pi\nu \text{ ist.}$$

Erwägt man nun, daß $\sum_k^{\lambda-1} S_{2n-1}(k) \equiv 0$ ist, so folgt hieraus:

$$D_n \equiv \sum_k^{\lambda-1} S_{2n-1}(k) \text{Ind. } \left(\frac{\Pi k\nu}{\Pi(k-1)\nu \Pi\nu} \right), \quad \text{Mod. } \lambda.$$

Der in diesem Ausdrucke vorkommende Binomialcoefficient kann durch eine der von *Jacobi* mit $\Psi_k(\alpha)$ bezeichneten complexen Kreistheilungszahlen ersetzt werden. Aus der Theorie der Kreistheilung (M. s. eine Notiz von *Jacobi* über die Kreistheilung und ihre Anwendung auf Zahlentheorie in den Monatsberichten der Berliner Akademie vom Jahre 1837, abgedruckt in diesem Journal Bd. 30. S. 166 etc.) hat man nämlich:

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

$$\frac{F(\alpha^{-1}, x) F(\alpha^{-k}, x)}{F(\alpha^{-(k+1)}, x)} = \Psi_k(\alpha^{-1}),$$

und wenn g^r statt α gesetzt wird:

$$\Psi_{k-1}(g^{-r}) \equiv - \frac{\Pi k\nu}{\Pi(k-1)\nu \Pi\nu}, \quad \text{Mod. } p.$$

Wird nun $f(\alpha)$ als derjenige ideale Primfactor von p betrachtet, welcher in $g^v - \alpha$ enthalten ist, so dafs

$$g^v \equiv \alpha, \text{ Mod. } f(\alpha)$$

ist, so ist

$$\Psi_{k-1}(\alpha^{-1}) \equiv -\frac{\Pi k v}{\Pi(k-1)v \Pi v}, \text{ Mod. } f(\alpha).$$

Also, wenn das Zeichen Ind. nicht mehr auf den Modul p , sondern nur auf den Modul $f(\alpha)$, Factor von p , bezogen wird, kann D_n folgendermassen dargestellt werden:

$$D_n = \sum_k^{\lambda-1} S_{2n-1}(k) \text{ Ind. } \Psi_{k-1}(\alpha^{-1}), \text{ Mod. } \lambda.$$

Es ist noch die complexe Zahl $\Psi_{k-1}(\alpha^{-1})$ in ihre Primfactoren, welche zugleich Primfactoren von p sind, zu zerlegen. Aus der von mir angegebenen Zerlegung der λ^{ten} Potenz des *Lagrangeschen* Ausdrucks $F(\alpha, x)$ der Kreistheilung, welche, wenn allgemein $\left| \frac{b}{a} \right|$ die kleinste positive Zahl bezeichnet, die der Congruenz $ax \equiv b, \text{ Mod. } \lambda$, genügt, folgendermassen dargestellt werden kann:

$$F(\alpha^{-1}, x)^\lambda = \pm \alpha^5 f(\alpha)^{\left| \frac{1}{h} \right|} \cdot f(\alpha^2)^{\left| \frac{2}{h} \right|} \cdot f(\alpha^3)^{\left| \frac{3}{h} \right|} \dots f(\alpha^{\lambda-2})^{\left| \frac{\lambda-2}{h} \right|},$$

erhält man sehr leicht:

$$\Psi_{k-1}(\alpha^{-1}) = \pm \Pi_h^{\lambda-1} f(\alpha^h)^{\left(\left| \frac{1}{h} \right| + \left| \frac{k-1}{h} \right| - \left| \frac{k}{h} \right| \right)}$$

und demnach

$$D_n \equiv \sum_k^{\lambda-1} \sum_h^{\lambda-1} S_{2n-1}(k) \left(\frac{\left| \frac{1}{h} \right| + \left| \frac{k-1}{h} \right| - \left| \frac{k}{h} \right|}{\lambda} \right) \text{ Ind. } f(\alpha^h), \text{ Mod. } \lambda,$$

wo, wenn $f(\alpha^h)$ ideal und H der kleinste Exponent ist, für welchen $f(\alpha^h)^H$ wirklich wird, die Bedeutung des Ind. $f(\alpha^h)$ als gleich $\frac{1}{H} \text{ Ind. } f(\alpha^h)^H$ anzusehen ist.

Man setze nun statt $S_{2n-1}(k)$ die in Beziehung auf den Modul λ congruente Reihe $S_{(2n-1)\lambda}(k)$ und multiplicire mit λ , so erhält man

$$\lambda D_n \equiv \sum_k^{\lambda-1} \sum_h^{\lambda-1} S_{(2n-1)\lambda}(k) \left(\left| \frac{1}{h} \right| + \left| \frac{k-1}{h} \right| - \left| \frac{k}{h} \right| \right) \text{ Ind. } f(\alpha^h), \text{ Mod. } \lambda^2.$$

Nun ist aus den bekannten Formeln für die Potenzsummen der natürlichen Zahlen leicht zu zeigen, dafs

$$\sum_k^{\lambda-1} S_{(2n-1)\lambda}(k) \equiv -\sum_h^{\lambda-1} k^{(2n-1)\lambda+1} \text{ und}$$

$$\sum_2^{\lambda-1} S_{(2n-1)\lambda}(k) \left(\left| \frac{k-1}{h} \right| - \left| \frac{k}{h} \right| \right) \equiv \sum_1^{\lambda-1} k^{(2n-1)\lambda} \left| \frac{k}{h} \right| \equiv h^{(2n-1)\lambda} \cdot \sum_1^{\lambda-1} k^{(2n-1)\lambda+1},$$

$$\sum_1^{\lambda-1} k^{(2n-1)\lambda+1} \equiv \frac{(-1)^{n+1} B_n \lambda}{2n}$$

für den Modul λ^2 ist. Setzt man diese Werthe hinein, so wird sich der gemeinschaftliche Factor λ hinwegheben, und man erhält so wieder eine Congruenz für den einfachen Modul λ . Setzt man alsdann noch für $h^{(2n-1)\lambda}$ das einfachere h^{2n-1} zurück, so ergibt sich endlich:

$$(17.) \quad D_n \equiv \frac{(-1)^{n+1} B_n}{2n} \sum_2^{\lambda-1} \frac{h^{2n}-1}{h} \text{Ind. } f(\alpha^h), \quad \text{Mod. } \lambda.$$

Nachdem so der schwierigste Theil der gegenwärtigen Untersuchung vollendet ist, wende ich mich zur Bestimmung der Gröfse M_n , die aus der oben gefundenen Gleichung (12.)

$$NP(e(\eta)^s E_n(\alpha, \eta))$$

$$= \varphi(\alpha)^\lambda E(\alpha) \left\{ f(\alpha^\gamma)^{\gamma^{2n}-1} f(\alpha^{\gamma^2})^{\gamma^{4n}-1} \dots f(\alpha^{\gamma^{\lambda-2}})^{\gamma^{2(\lambda-2)n}-1} \right\}^s$$

entwickelt werden mufs, in welcher

$$E(\alpha) = E_n(\alpha)^{M_n} \quad \text{und} \quad s \equiv \frac{-2 \text{Ind. } E_n(\alpha)}{\gamma^{2n}-1}, \quad \text{Mod. } \lambda \text{ ist.}$$

Man erhebe beide Seiten dieser Gleichung zur Potenz p , und mache daraus eine Congruenz für den Modul p . Für diesen Modul wird, wie bekannt, die p^{te} Potenz jeder complexen Zahl, welche α und x , oder auch die Perioden $\eta, \eta_1, \dots, \eta_{\lambda-1}$ enthält, einer complexen Zahl congruent, welche nur α enthält; also wird die p^{te} Potenz von $P(e(\eta)^s E_n(\alpha, \eta))$ einer complexen Zahl $F(\alpha)$ congruent und mithin wird

$$N(Pe(\eta)^s E_n(\alpha, \eta))^p \equiv F(\alpha)^\lambda, \quad \text{Mod. } p.$$

Die p^{te} Potenz einer nur α allein enthaltenden complexen Zahl aber ist dieser complexen Zahl selbst congruent, wenn nämlich, wie hier, $p = \nu\lambda + 1$ ist. Die obige Gleichung giebt daher folgende Congruenz:

$$F(\alpha)^\lambda \equiv \varphi(\alpha)^\lambda E_n(\alpha)^{M_n} \left\{ f(\alpha^\gamma)^{\gamma^{2n}-1} f(\alpha^{\gamma^2})^{\gamma^{4n}-1} \dots f(\alpha^{\gamma^{\lambda-2}})^{\gamma^{2(\lambda-2)n}-1} \right\}^s$$

für den Modul p , und darum auch für den Modul $f(\alpha)$, welcher ein Primfactor von p ist. Nimmt man nun auf beiden Seiten dieser Congruenz die Indices in Beziehung auf den Modul $f(\alpha)$, und setzt für s seinen oben gefundenen Werth, so erhält man:

$$0 \equiv M_n \text{Ind. } E_n(\alpha) - \frac{2 \text{Ind. } E_n(\alpha)}{\gamma^{2n}-1} \cdot \sum_1^{\lambda-2} (\gamma^{-2ni} - 1) \text{Ind. } f(\alpha^{\gamma^i}), \quad \text{Mod. } \lambda.$$

Unter der Voraussetzung, daß $\text{Ind. } E_n(\alpha)$ nicht congruent Null ist, für den Modul λ , kann man $\text{Ind. } E_n(\alpha)$ aufheben, und man findet dann folgenden Ausdruck von M_n :

$$(18.) \quad M_n \equiv \frac{2}{\gamma^{2n}-1} \sum_1^{\lambda-2} (\gamma^{-2ni} - 1) \text{Ind. } f(\alpha^{\gamma^i}), \quad \text{Mod. } \lambda.$$

Die gefundenen Ausdrücke von D_n und M_n sind nun in die Congruenz

$$\frac{(-1)^{n+1}(\gamma^{2n}-1)B_n}{4n} \cdot M_n \equiv D_n, \quad \text{Mod. } \lambda,$$

zu setzen, wodurch dieselbe, nach Aufhebung der gemeinschaftlichen Factoren, folgende Gestalt annimmt:

$$\sum_1^{\lambda-2} (\gamma^{-2ni} - 1) \text{Ind. } f(\alpha^{\gamma^i}) \equiv \sum_2^{\lambda-1} \frac{h^{2n}-1}{1} \text{Ind. } f(\alpha^h).$$

Setzt man $h \equiv \gamma^{-i}$, so wird

$$\sum_1^{\lambda-2} (\gamma^{-2ni} - 1) (\text{Ind. } f(\alpha^{\gamma^i}) - \gamma^i \text{Ind. } f(\alpha^{\gamma^{-i}})) \equiv 0.$$

Multiplicirt man mit γ^{2nk} , wo k jede beliebige der Zahlen $1, 2, 3, \dots, \lambda-1$ bedeuten kann, jedoch mit Ausschluß von $k = \frac{1}{2}(\lambda-1)$, und nimmt die Summe in Beziehung auf $n = 0, 1, 2, \dots, \frac{1}{2}(\lambda-3)$, so wird dieselbe stets congruent Null; mit alleiniger Ausnahme des Falles $i = k$, für welchen sich

$$(19.) \quad \text{Ind. } f(\alpha^{\gamma^k}) \equiv \gamma^k \text{Ind. } f(\alpha^{\gamma^{-k}}), \quad \text{Mod. } \lambda$$

ergiebt.

Diese Congruenz stellt das gesuchte einfache Reciprocitätsgesetz unter je zwei complexen Primfactoren einer und derselben Primzahl p dar. Dasselbe kann in den Zeichen, welche für λ^{te} Potenzreste den *Legendreschen* für quadratische nachgebildet sind, folgendermaßen dargestellt werden:

$$(20.) \quad \left(\frac{f(\alpha^{\gamma^k})}{f(\alpha)} \right) = \left(\frac{f(\alpha)}{f(\alpha^{\gamma^k})} \right).$$

Nach der Definition des *Legendreschen* Zeichens hat man nämlich:

$$\left(\frac{f(\alpha^{\gamma^k})}{f(\alpha)} \right) = \alpha^{\text{Ind. } f(\alpha^{\gamma^k})},$$

also auch

$$\left(\frac{f(\alpha^{\gamma^{-k}})}{f(\alpha)} \right) = \alpha^{\text{Ind. } f(\alpha^{\gamma^{-k}})},$$

und wenn α in α^{γ^k} verwandelt wird:

$$\left(\frac{f(\alpha)}{f(\alpha^{\gamma^k})}\right) = \alpha^{\gamma^k \text{Ind.} f(\alpha^{\gamma^{-k}})};$$

woraus die Übereinstimmung beider Darstellungen dieses Reciprocitätsgesetzes erhellet.

Da der Fall $k = \frac{1}{2}(\lambda - 1)$ oben ausgeschlossen werden mußte, so sagt dieses Reciprocitätsgesetz über den Index des einen complexen Primfactors $f(\alpha^{-1})$ nichts aus. Dieser Mangel läßt sich durch diejenige Reciprocitätsgleichung, welche die von mir gefundene Formel der Kreistheilung giebt, leicht ergänzen. Aus dem Ausdrücke

$$F(\alpha^{-1}, x)^\lambda = \pm \alpha^s f(\alpha)^1 f(\alpha^\gamma)^{\gamma-1} f(\alpha^{\gamma^2})^{\gamma^2-2} \dots f(\alpha^{\gamma^{\lambda-2}})^{\gamma^{-(\lambda-2)}},$$

in welchem für primäre Werthe von $f(\alpha)$ die Einheit α^s gleich Eins wird, erhält man nämlich, wenn man auf beiden Seiten durch $p = f(\alpha) \cdot f(\alpha^\gamma) \dots f(\alpha^{\gamma^{\lambda-2}})$ dividirt und die Indices in Beziehung auf den Modul $f(\alpha)$ nimmt:

$$0 \equiv \sum_h^{\lambda-2} (\gamma^{-h} - 1) \text{Ind.} f(\alpha^{\gamma^h}), \quad \text{Mod. } \lambda.$$

Fasset man in dieser Summe je zwei vom Anfange und Ende gleich weit entfernte Glieder zusammen, so wird, vermöge des oben bewiesenen Reciprocitätsgesetzes, die Summe derselben congruent Null, und es bleibt nur das mittelste Glied, nämlich $-2 \text{Ind.} f(\alpha^{-1})$ übrig. Man erhält also

$$(21.) \quad \text{Ind.} f(\alpha^{-1}) \equiv 0, \quad \text{Mod. } \lambda,$$

oder, nach der *Legendreschen* Bezeichnung:

$$(22.) \quad \left(\frac{f(\alpha^{-1})}{f(\alpha)}\right) = 1.$$

Nach ähnlichen Methoden, jedoch nicht ohne Anwendung einiger andern Hilfsmittel, welche ziemlich bedeutende Vorarbeiten erfordern, habe ich auch den Beweis des allgemeinen Reciprocitätsgesetzes für zwei verschiedene nicht congruente complexe Primzahlen gesucht. Dieser allgemeinere Beweis aber leidet, eben so wie der hier gegebene, an dem Mangel, dafs er, auch für Potenzreste von einem bestimmten Exponenten λ , *nicht alle* complexen Primzahlen umfasset, weil die obige Voraussetzung, dafs $\text{Ind.} E_n(\alpha)$ für den Modul λ nicht congruent Null sein darf, und zwar für keinen der Werthe $n = 1, 2, 3, \dots, \frac{1}{2}(\lambda - 3)$, nicht für alle Primzahlen $f(\alpha)$ erfüllt wird. Für $\lambda = 5$, also für die *fünften* Potenzreste, giebt es folgende acht Primzahlen

unter Tausend, für deren complexe Primfactoren $\text{Ind. } E_n(\alpha) \equiv 0, \text{ Mod. } 5$ ist nämlich: $p = 211, 281, 421, 461, 521, 691, 881$ und 991 , auf welche also auch der vorstehende Beweis des Reciprocitätsgesetzes unter conjugirten Primzahlen sich nicht erstreckt, obgleich, wie die wirkliche Ausrechnung mit Hülfe der Tafeln des Canon arithmeticus von *Jacobi* leicht ergibt, dasselbe auch für diese vollständig richtig ist. Sollte es mir nicht gelingen, diese Unvollständigkeit der auf die Ausdrücke $P_\varepsilon(\alpha, x)$ gegründeten Beweise der Reciprocitätsgesetze zu entfernen, so würde ich genöthigt sein, den Weg, welchen ich seit mehreren Jahren ausdauernd verfolgt habe, gänzlich zu verlassen und einen andern zu suchen.

Breslau, den 31. August 1854.