ZUR THEORIE DER ELLIPTISCHEN FUNCTIONEN

VON

H. WEBER

in MARBURG.

Die vorliegende Abhandlung verfolgt in ihren ersten Teilen den Zweck, die Transformationstheorie der elliptischen Functionen im Zusammenhang darzustellen und zu den Anwendungen auf Zahlentheorie, so weit sie mit der Theorie der complexen Multiplication zusammenhängen, vorzubereiten, von welchen im letzten Abschnitt ein Teil durchgeführt ist. Ich hoffe diesen ersten Untersuchungen weitergehende folgen lassen zu können. Als der kürzeste und einfachste Weg, um zu den Grundlagen der doppelt periodischen Functionen zu gelangen ist der von JACOBI herrührende, welcher von den θ-Functionen ausgeht, gewählt, und zwar in der Weise, dass nur von den Reihenentwickelungen, nicht von den Productdarstellungen Gebrauch gemacht ist. Es ergeben sich zwar bekanntlich manche Sätze leichter aus den Darstellungen durch unendliche Producte; aber im Interesse einer einheitlichen Darstellung haben wir es vorgezogen nur von den Reihenentwickelungen Gebrauch zu machen, welche allein einer Verallgemeinerung für mehrere Variable fähig sind. Überdies hat es ein eigentümliches Interesse, auch die etwas tiefer liegenden Sätze bei den θ-Reihen direct aufzusuchen, worauf HERMITE an verschiedenen Stellen hingewiesen hat.

Was die Transformationstheorie betrifft, so ergiebt sich dieselbe als eine notwendige Consequenz aus der Teilungsaufgabe, wenn man letztere nach GALOIS'schen Principien auffasst; zugleich gelangt man so am natürlichsten und einfachsten zu den verschiedenen in der Transformationstheorie auftretenden algebraischen Gleichungen.

Acta mathematica. 6. Imprimé 29 Novembre 1884.

Bei den zahlentheoretischen Anwendungen, welche den Gegenstand des letzten Abschnitts bilden, haben wir es uns zum Grundsatz gemacht, nur solche Teile aus der Theorie der quadratischen Formen vorauszusetzen, welche zu den elementaren gerechnet werden können, und einige tiefer liegende Sätze, bis jetzt die Sätze über die Verhältnisse der Classenzahlen in den verschiedenen Ordnungen und über die Anzahl der zu einer Determinante gehörigen Geschlechter, freilich nur für negative Determinanten, als zahlentheoretischen Ausdruck für gewisse algebraische Eigenschaften der bei der complexen Multiplication auftretenden Gleichungen aufzufassen.

Marburg im September 1884.

I. Abschnitt.

§ 1. *Die Theta-Functionen m^{ter} Ordnung.*

Wir definiren als Theta-Function m^{ter} Ordnung der zwei Argumente u, ω eine Function $\theta(u, \omega)$ oder $\theta(u)$, welche folgende Bedingungen erfüllt:

I. $\theta(u)$ hat, als Function der Variablen u aufgefasst, für alle endlichen Werthe von u den Character einer ganzen rationalen Function.

II. Es ist

$$\theta(u + 1) = (-1)^g \theta(u)$$

$$\theta(u + \omega) = (-1)^h e^{-\pi i m(2u+\omega)} \theta(u).$$

Der Zahlencomplex (g, h), der aus den Elementen 0, 1 gebildet werden kann, heisst die *Charakteristik* der θ-Function, und wird als Index an das Zeichen θ angehängt: $[\theta_{g,h}(u)]$. Es giebt also nur vier wesentlich verschiedene Charakteristiken, (0, 0), (0, 1), (1, 0), (1, 1), von denen die drei ersten *gerade*, die letzte *ungerade* genannt wird. Wir betrachten hier, um uns kürzer ausdrücken zu können, u als veränderlich, ω als einen

constanten Parameter, von dem ein *positiver imaginärer* Teil vorausgesetzt wird.

Wir stellen nun die complexe Variable u in einer Ebene dar und begrenzen in derselben, von einem beliebigen Punkt u_0 ausgehend, ein Parallelogramm, dessen Ecken in den Punkten u_0, $u_0 + 1$, $u_0 + \omega$, $u_0 + \omega + 1$ liegen, welches wir das *Periodenparallelogramm* nennen. Die ganze u-Ebene lässt sich durch solche, an den Seiten angrenzende, congruente Parallelogramme ausfüllen, und einem Nullpunkte einer θ-Function entsprechen andere Nullpunkte an congruent liegenden Stellen in allen diesen Parallelogrammen.

Man erhält nun für diese Nullpunkte zwei fundamentale Sätze durch Betrachtung der beiden über die Begrenzung eines Periodenparallelogramms ausgedehnten Integrale

$$\frac{1}{2\pi i}\int d\log \theta_{g,h}(u), \qquad \frac{1}{2\pi i}\int u d\log \theta_{g,h}(u)$$

von welchen das erste bekanntlich die Anzahl, das zweite die Summe der u-Werte, für welche $\theta_{g,h}(u)$ im Innern des Parallelogramms verschwindet, darstellt. Die Anzahl dieser Nullwerte ergiebt sich darnach $= m$ und ihre Summe gleich

$$\frac{1}{2}m(\omega + 1) + \left(M + \frac{1}{2}g\right)\omega + \left(N + \frac{1}{2}h\right) \tag{1}$$

wenn M, N ganze Zahlen sind. Nullpunkte höherer Ordnung werden dabei nach Massgabe ihrer Vielfachheit, mehrfach gezählt.

III. *Eine θ-Function m^{ter} Ordnung hat also innerhalb eines Periodenparallelogramms m Nullpunkte, und von diesen ist einer durch die $m - 1$ übrigen bestimmt.*

Hat man mehrere θ-Functionen der gleichen Ordnung und Charakteristik, so ist jede lineare homogene Function derselben mit constanten Coefficienten wieder eine solche Function, und darnach folgt unmittelbar aus dem letzten Satz:

IV. *Jede θ-Function von der Ordnung m und gegebener Charakteristik ist eine lineare homogene Function mit constanten Coëfficienten von höchstens m solchen Functionen, welche linear unabhängig sind.*

Ferner ergiebt sich noch aus der Definition I, II der folgende Satz in welchem unter der Summe mehrerer Charakteristiken (g, h), (g', h'), ... die Charakteristik $(g + g' + \ldots, h + h' + \ldots)$ verstanden ist.

V. *Das Product mehrerer θ-Functionen von beliebiger Ordnung und Charakteristik ist eine θ-Function, deren Ordnung und Charakteristik die Summe der Ordnungen und Charakteristiken der einzelnen Factoren ist.*

§ 2. *Die Theta-Functionen der ersten Ordnung.*

Für die erste Ordnung existirt nach dem Vorstehenden nur je eine θ-Function, deren Nullpunkte durch die Formel (1) vollständig bestimmt sind. Hiernach kann man sofort zur Darstellung dieser Functionen durch unendliche Producte übergehen, oder man kann aus der Definition I, II durch die Methode der unbestimmten Coefficienten unendliche Reihen für dieselben finden, und dadurch die wirkliche Existenz der gesuchten Functionen nachweisen. Wir wählen den letzteren Weg und erhalten:

$$(1) \qquad \vartheta_{g,h}(u, \omega) = (-i)^{gh} \sum_{-\infty, \infty}^{n} (-1)^{hn} e^{\pi i\omega\left(n+\frac{g}{2}\right)^2 + 2\pi i u\left(n+\frac{g}{2}\right)}$$

indem über einen von ω allein abhängigen Factor, den die Definition I, II unbestimmt lässt, so verfügt ist, dass diese Functionen alle, nebst ihren nach u und ω genommenen Derivierten der partiellen Differentialgleichung

$$(2) \qquad \frac{\partial^2 \vartheta}{\partial u^2} = 4\pi i \frac{\partial \vartheta}{\partial \omega}$$

genügen, und dass für $q = 0$

$$(3) \quad \vartheta_{00}(u) = 1, \quad \vartheta_{01}(u) = 1, \quad \vartheta_{10}(u) = 2q^{\frac{1}{4}} \cos \pi u, \quad \vartheta_{11}(u) = 2q^{\frac{1}{4}} \sin \pi u$$

wird. Die Function $\vartheta_{11}(u)$ ist eine *ungerade Function*, während $\vartheta_{00}(u)$, $\vartheta_{01}(u)$, $\vartheta_{10}(u)$ *gerade Functionen* sind.

Jede dieser vier Functionen lässt sich durch jede andere ausdrücken vermittelst der Relationen

$$\vartheta_{g,h}\left(u+\frac{h'+g'\omega}{2}\right)=(-1)^{gh'}i^{g'(h+h')}e^{-\frac{\pi i\omega g'^2}{4}-\pi iug'}\vartheta_{g+g',h+h'}(u)$$

(4)

$$\vartheta_{g+2,h}(u)=\vartheta_{g,h}(u),\qquad \vartheta_{g,h+2}(u)=(-1)^g\vartheta_{g,h}(u).$$

Setzt man in diesen Formeln $u=0$, so erhält man, wenn man die ϑ-Functionen, in welche das Argument den Wert 0 hat, ohne Argument schreibt:

$$\begin{aligned}
\vartheta_{00}(0) &= \vartheta_{00}, & \vartheta_{10}(0) &= \vartheta_{10}\\
\vartheta_{00}\left(\tfrac{1}{2}\right) &= \vartheta_{01}, & \vartheta_{10}\left(\tfrac{1}{2}\right) &= 0\\
\vartheta_{00}\left(\tfrac{1}{2}\omega\right) &= e^{-\frac{\pi i\omega}{4}}\vartheta_{10}, & \vartheta_{10}\left(\tfrac{1}{2}\omega\right) &= e^{-\frac{\pi i\omega}{4}}\vartheta_{00}\\
\vartheta_{00}\left(\frac{1+\omega}{2}\right) &= 0, & \vartheta_{10}\left(\frac{1+\omega}{2}\right) &= -ie^{-\frac{\pi i\omega}{4}}\vartheta_{01}
\end{aligned}$$

(5)

$$\begin{aligned}
\vartheta_{01}(0) &= \vartheta_{01}, & \vartheta_{11}(0) &= 0\\
\vartheta_{01}\left(\tfrac{1}{2}\right) &= \vartheta_{00}, & \vartheta_{11}\left(\tfrac{1}{2}\right) &= \vartheta_{10}\\
\vartheta_{01}\left(\tfrac{1}{2}\omega\right) &= 0, & \vartheta_{11}\left(\tfrac{1}{2}\omega\right) &= ie^{-\frac{\pi i\omega}{4}}\vartheta_{01}\\
\vartheta_{01}\left(\frac{1+\omega}{2}\right) &= e^{-\frac{\pi i\omega}{4}}\vartheta_{10}, & \vartheta_{11}\left(\frac{1+\omega}{2}\right) &= e^{-\frac{\pi i\omega}{4}}\vartheta_{00}.
\end{aligned}$$

Da die Quadrate der vier ϑ-Functionen von der zweiten Ordnung sind mit der Charakteristik (0, 0), so kann man zwei von ihnen linear durch die beiden andern ausdrücken und zwar wie folgt:

$$\begin{aligned}
\vartheta_{01}^2\vartheta_{10}^2(u) &= \vartheta_{10}^2\vartheta_{01}^2(u)-\vartheta_{00}^2\vartheta_{11}^2(u)\\
\vartheta_{01}^2\vartheta_{00}^2(u) &= \vartheta_{00}^2\vartheta_{01}^2(u)-\vartheta_{10}^2\vartheta_{11}^2(u)
\end{aligned}$$

(6)

woraus noch, durch $u=\frac{1}{2}$, die Relation sich ergiebt:

$$\vartheta_{00}^4=\vartheta_{01}^4+\vartheta_{10}^4. \tag{7}$$

Aus diesen Functionen kann man nun alle θ-Functionen von beliebiger Ordnung und Charakteristik zusammensetzen, wie man auf Grund der Sätze des vorigen § unmittelbar durch die Abzählung der Constanten findet, mit Rücksicht darauf, dass eine lineare Relation zwischen geraden und ungeraden Functionen nur dann bestehen kann, wenn der gerade Teil für sich und der ungerade Teil für sich verschwindet, und dass zwei der Functionen $\vartheta_{g,h}(u)$ nicht in constantem Verhältniss stehen.

Bezeichnen wir mit θ_0, θ_1 irgend zwei von den Functionen $\vartheta_{g,h}(u)^2$, oder auch zwei lineare Combinationen derselben, und mit $F^\nu(\theta_0, \theta_1)$ eine ganze rationale und homogene Function ν^{ter} Ordnung der beiden Argumente θ_0, θ_1, so erhalten wir auf dem angegebenen Weg folgende Darstellungen.

I. $m \equiv 0 \pmod 2$, *gerade Functionen*

$$\theta_{00}^{(m)}(u) = F^{\left(\frac{1}{2}m\right)}(\theta_0, \theta_1)$$

$$\theta_{01}^{(m)}(u) = \vartheta_{00}(u)\vartheta_{01}(u)F^{\left(\frac{1}{2}m-1\right)}(\theta_0, \theta_1)$$

$$\theta_{10}^{(m)}(u) = \vartheta_{00}(u)\vartheta_{10}(u)F^{\left(\frac{1}{2}m-1\right)}(\theta_0, \theta_1)$$

$$\theta_{11}^{(m)}(u) = \vartheta_{10}(u)\vartheta_{01}(u)F^{\left(\frac{1}{2}m-1\right)}(\theta_0, \theta_1)$$

ungerade Functionen

$$\theta_{00}^{(m)}(u) = \vartheta_{00}(u)\vartheta_{01}(u)\vartheta_{10}(u)\vartheta_{11}(u)F^{\left(\frac{1}{2}m-2\right)}(\theta_0, \theta_1)$$

$$\theta_{01}^{(m)}(u) = \vartheta_{10}(u)\vartheta_{11}(u)F^{\left(\frac{1}{2}m-1\right)}(\theta_0, \theta_1)$$

$$\theta_{10}^{(m)}(u) = \vartheta_{01}(u)\vartheta_{11}(u)F^{\left(\frac{1}{2}m-1\right)}(\theta_0, \theta_1)$$

$$\theta_{11}^{(m)}(u) = \vartheta_{00}(u)\vartheta_{11}(u)F^{\left(\frac{1}{2}m-1\right)}(\theta_0, \theta_1).$$

II. $m \equiv 1 \pmod 2$, *gerade Functionen*

$$\theta_{00}^{(m)}(u) = \vartheta_{00}(u) F^{\frac{1}{2}(m-1)}(\theta_0, \theta_1)$$

$$\theta_{01}^{(m)}(u) = \vartheta_{01}(u) F^{\frac{1}{2}(m-1)}(\theta_0, \theta_1)$$

$$\theta_{10}^{(m)}(u) = \vartheta_{10}(u) F^{\frac{1}{2}(m-1)}(\theta_0, \theta_1)$$

$$\theta_{11}^{(m)}(u) = \vartheta_{00}(u)\vartheta_{01}(u)\vartheta_{10}(u) F^{\frac{1}{2}(m-3)}(\theta_0, \theta_1).$$

ungerade Functionen

$$\theta_{00}^{(m)}(u) = \vartheta_{01}(u)\vartheta_{10}(u)\vartheta_{11}(u) F^{\frac{1}{2}(m-3)}(\theta_0, \theta_1)$$

$$\theta_{01}^{(m)}(u) = \vartheta_{00}(u)\vartheta_{10}(u)\vartheta_{11}(u) F^{\frac{1}{2}(m-3)}(\theta_0, \theta_1)$$

$$\theta_{10}^{(m)}(u) = \vartheta_{00}(u)\vartheta_{01}(u)\vartheta_{11}(u) F^{\frac{1}{2}(m-3)}(\theta_0, \theta_1)$$

$$\theta_{11}^{(m)}(u) = \vartheta_{11}(u) F^{\frac{1}{2}(m-1)}(\theta_0, \theta_1).$$

Hierdurch ist die in § 1 als Maximalzahl gefundene Anzahl der θ-Functionen als wirklich existirend nachgewiesen, oder, mit andern Worten, es ist gezeigt, dass man stets eine θ-Function m^{ter} Ordnung von gegebener Charakteristik so bestimmen kann, dass sie in $m - 1$ beliebig gegebenen Punkten eines Periodenparallelogramms verschwindet. Durch diese Nullpunkte ist dann aber auch, von einem constanten Factor abgesehen, die θ-Function ausnahmslos eindeutig bestimmt.

§ 3. *Die Theta-Functionen zweiter Ordnung.*

Zu den θ-Functionen der zweiten Ordnung gehören auch die vier Functionen $\vartheta_{g,h}(2u, 2\omega)$, und zwar ist ihre Charakteristik $(0, h)$; man kann sie daher, da man ihre Nullpunkte kennt, durch die Functionen

$\vartheta_{g,h}(u)$ ausdrücken und erhält, wenn man einen von u unabhängigen Coefficienten durch die Bedingungen (2), (3) bestimmt, die Formeln: (LANDEN'sche Transformation)

$$
\begin{aligned}
2\vartheta_{10}(0,\ 2\omega)\vartheta_{00}(2u,\ 2\omega) &= \vartheta_{10}(u)^2 + \vartheta_{11}(u)^2 \\
2\vartheta_{00}(0,\ 2\omega)\vartheta_{10}(2u,\ 2\omega) &= \vartheta_{10}(u)^2 - \vartheta_{11}(u)^2 \\
\vartheta_{01}(0,\ 2\omega)\vartheta_{01}(2u,\ 2\omega) &= \vartheta_{00}(u)\vartheta_{01}(u) \\
\vartheta_{01}(0,\ 2\omega)\vartheta_{11}(2u,\ 2\omega) &= \vartheta_{10}(u)\vartheta_{11}(u).
\end{aligned} \tag{1}
$$

(1)

Bezeichnet man die Differentiation nach der Variablen u durch einen Accent, so erhält man für $u = 0$ aus den vorstehenden Formeln:

$$
\begin{aligned}
2\vartheta_{10}(0,\ 2\omega)\vartheta_{00}(0,\ 2\omega) &= \vartheta_{10}^2 \\
\vartheta_{01}(0,\ 2\omega)^2 &= \vartheta_{00}\vartheta_{01} \\
2\vartheta_{01}(0,\ 2\omega)\vartheta'_{11}(0,\ 2\omega) &= \vartheta_{10}\vartheta'_{11}
\end{aligned} \tag{2}
$$

(2)

und hieraus:

$$
\frac{\vartheta'_{11}(0,\ 2\omega)}{\vartheta_{00}(0,\ 2\omega)\vartheta_{01}(0,\ 2\omega)\vartheta_{10}(0,\ 2\omega)} = \frac{\vartheta'_{11}}{\vartheta_{00}\vartheta_{01}\vartheta_{10}} \tag{3}
$$

(3)

woraus hervorgeht, dass die auf der rechten Seite stehende Function von ω ungeändert bleibt, wenn ω in 2ω verwandelt wird, so dass man den Wert derselben erhält, wenn man $\omega = \infty$, d. h. $q = 0$ setzt.

Man findet so aus (3) § 2 die bekannte und wichtige Formel

$$
\vartheta'_{11} = \pi\vartheta_{00}\vartheta_{01}\vartheta_{10}. \tag{4}
$$

(4)

---

(1) Am einfachsten leitet man zuerst mittelst (2), (3) die dritte und vierte der Formeln (1) her. Die beiden ersten folgen dann leicht aus (6) § 2.

Noch weitere Folgerungen lassen sich aus (1), (2) ziehen, wenn man ω durch $\frac{1}{2}\omega$ und u durch 0 und $\frac{1}{4}$ ersetzt. Man erhält so

$$\sqrt{\vartheta_{00}\vartheta_{01}} = \vartheta_{01}(0,\ 2\omega) = \sum_{-\infty,\infty}^{n}(-1)^n q^{2n^2}$$

$$\sqrt{\vartheta_{00}\vartheta_{10}} = \frac{1}{\sqrt{2}}\vartheta_{10}\left(0,\ \frac{\omega}{2}\right) = \sqrt{2}\,q^{\frac{1}{8}}\sum_{0,\infty}^{n} q^{\frac{n.n+1}{2}}$$

$$\sqrt{\vartheta_{10}\vartheta_{01}} = \vartheta_{10}\left(\frac{1}{4},\ \frac{\omega}{2}\right) = \sqrt{2}\,q^{\frac{1}{8}}\sum_{0,\infty}^{n}(-q)^{\frac{n.n+1}{2}},$$

wodurch diese Quadratwurzeln als *eindeutige* Functionen von ω dargestellt sind. Man erhält daraus noch die nach HERMITE mit $\varphi(\omega)$ und $\psi(\omega)$ zu bezeichnenden Quotienten

(6)
$$\varphi(\omega) = \sqrt{\frac{\vartheta_{10}}{\vartheta_{00}}} = \sqrt{2}\,q^{\frac{1}{8}}\frac{\sum_{0,\infty}^{n}(-q)^{\frac{n.n+1}{2}}}{\sum_{-\infty,\infty}^{n}(-1)^n q^{2n^2}}$$

$$\psi(\omega) = \sqrt{\frac{\vartheta_{01}}{\vartheta_{00}}} = \frac{\sum_{0,\infty}^{n}(-q)^{\frac{n.n+1}{2}}}{\sum_{0,\infty}^{n} q^{\frac{n.n+1}{2}}}.$$ [1]

Auf dieselbe Weise wie das Formelsystem (1) lässt sich auch das folgende, der GAUSS'schen Transformation entsprechende System herleiten:

(7)
$$\vartheta_{01}\left(0,\ \frac{\omega}{2}\right)\vartheta_{00}\left(u,\ \frac{\omega}{2}\right) = \vartheta_{01}^2(u) - \vartheta_{11}^2(u)$$

$$\vartheta_{01}\left(0,\ \frac{\omega}{2}\right)\vartheta_{01}\left(u,\ \frac{\omega}{2}\right) = \vartheta_{00}^2(u) - \vartheta_{10}^2(u)$$

$$\vartheta_{10}\left(0,\ \frac{\omega}{2}\right)\vartheta_{10}\left(u,\ \frac{\omega}{2}\right) = 2\vartheta_{10}(u)\vartheta_{00}(u)$$

$$\vartheta_{10}\left(0,\ \frac{\omega}{2}\right)\vartheta_{11}\left(u,\ \frac{\omega}{2}\right) = 2\vartheta_{11}(u)\vartheta_{01}(u).$$

[1] HERMITE, Comptes rendus, tome LVII, 21 déc. 1863.

§ 4. *Die Functionen* $\vartheta_{g,h}(nu, n\omega)$ *und die Function* $\eta(\omega)$.

Die Functionen $\vartheta_{g,h}(nu, n\omega)$ sind θ-Functionen n^{ter} Ordnung, und zwar, wenn n ungerade vorausgesetzt wird, von der Charakteristik (g, h). Durch Berücksichtigung der Nullpunkte erhält man für dieselben folgende Ausdrücke:

$$\vartheta_{11}(nu, n\omega) = C\vartheta_{11}(u)\prod_{1,\frac{n-1}{2}}^{\nu}\vartheta_{11}\left(u+\frac{2\nu}{n}\right)\vartheta_{11}\left(u-\frac{2\nu}{n}\right)$$

$$\vartheta_{10}(nu, n\omega) = (-1)^{\frac{n-1}{2}} C\vartheta_{10}(u)\prod_{1,\frac{n-1}{2}}^{\nu}\vartheta_{10}\left(u+\frac{2\nu}{n}\right)\vartheta_{10}\left(u-\frac{2\nu}{n}\right)$$

(1)

$$\vartheta_{01}(nu, n\omega) = (-1)^{\frac{n-1}{2}} C\vartheta_{01}(u)\prod_{1,\frac{n-1}{2}}^{\nu}\vartheta_{01}\left(u+\frac{2\nu}{n}\right)\vartheta_{01}\left(u-\frac{2\nu}{n}\right)$$

$$\vartheta_{00}(nu, n\omega) = (-1)^{\frac{n-1}{2}} C\vartheta_{00}(u)\prod_{1,\frac{n-1}{2}}^{\nu}\vartheta_{00}\left(u+\frac{2\nu}{n}\right)\vartheta_{00}\left(u-\frac{2\nu}{n}\right),$$

und für die Constante C ergiebt sich mittelst der Formel (4) § 3

$$C = \frac{\pm 1}{\sqrt{n}}\prod_{1,\frac{n-1}{2}}^{\nu}\frac{\vartheta_{11}\left(\frac{2\nu}{n}\right)}{\vartheta_{00}\left(\frac{2\nu}{n}\right)\vartheta_{01}\left(\frac{2\nu}{n}\right)\vartheta_{10}\left(\frac{2\nu}{n}\right)}.$$

Nun lässt sich aber durch die Formel (1), (7) des vorigen § leicht zeigen, dass

$$\frac{\prod_{1,\frac{n-1}{2}}^{\nu}\vartheta_{00}\left(\frac{2\nu}{n}\right)\vartheta_{10}\left(\frac{2\nu}{n}\right)\vartheta_{01}\left(\frac{2\nu}{n}\right)}{\vartheta_{00}^{\frac{n-1}{2}}\vartheta_{10}^{\frac{n-1}{2}}\vartheta_{01}^{\frac{n-1}{2}}}$$

wenigstens vom Zeichen abgesehen, ungeändert bleibt, wenn ω durch 2ω

ersetzt wird. Man kann also den Wert dieses Quotienten dadurch ermitteln, dass man $q = 0$ setzt, und erhält so die Formel

$$(2) \qquad 2^{\frac{n-1}{2}} \prod_{1, \frac{n-1}{2}}^{\nu} \vartheta_{00}\left(\frac{2\nu}{n}\right) \vartheta_{10}\left(\frac{2\nu}{n}\right) \vartheta_{01}\left(\frac{2\nu}{n}\right) = (-1)^{\frac{n^2-1}{8}} \vartheta_{00}^{\frac{n-1}{2}} \vartheta_{10}^{\frac{n-1}{2}} \vartheta_{01}^{\frac{n-1}{2}}$$

Hieraus ergiebt sich, indem man in (1) das Vorzeichen wieder durch $q = 0$ bestimmt:

$$(3) \quad \sqrt{n}\, \vartheta_{11}(nu, n\omega) \vartheta_{00}^{\frac{n-1}{2}} \vartheta_{10}^{\frac{n-1}{2}} \vartheta_{01}^{\frac{n-1}{2}} = 2^{\frac{n-1}{2}} \vartheta_{11}(u) \prod_{1, \frac{n-1}{2}}^{\nu} \vartheta_{11}\left(\frac{2\nu}{n}\right) \vartheta_{11}\left(\frac{2\nu}{n} + u\right) \vartheta_{11}\left(\frac{2\nu}{n} - u\right)$$

aus welcher man die drei andern Formeln leicht ableitet.

Wir wenden die letzte Formel auf den Fall $n = 3$ an, für welchen wir erhalten, wenn wir u, ω durch 0, $\frac{1}{3}\omega$ ersetzen und (4) § 3 anwenden:

$$(4) \qquad 3\sqrt{3}\, \vartheta_{11}' = 2\pi \left[\vartheta_{11}\left(\frac{2}{3}, \frac{\omega}{3}\right)\right]^3,$$

wonach die dritte Wurzel aus ϑ_{11}' als eindeutige Function von ω dargestellt werden kann. Man setze

$$(5) \qquad \eta(\omega) = \frac{1}{\sqrt{3}} \vartheta_{11}\left(\frac{2}{3}, \frac{\omega}{3}\right) = q^{\frac{1}{12}} \sum_{-\infty, \infty}^{n} (-1)^n q^{3n^2+n}$$

und erhält:

$$(6) \qquad \sqrt[3]{\frac{1}{2} \vartheta_{00} \vartheta_{01} \vartheta_{10}} = \sqrt[3]{\frac{1}{2\pi} \vartheta_{11}'} = \eta(\omega).$$

Die Function $\eta(\omega)$, verschwindet, wie aus (6) hervorgeht, für keinen endlichen Wert von ω mit positiv imaginärem Teil, und ist für rein imaginäre Werte von ω reell und positiv. Die Gleichung (3) ergiebt:

$$(7) \qquad \sqrt{n}\, \eta(n\omega) \eta(\omega)^{\frac{n-3}{2}} = \prod_{1, \frac{n-1}{2}}^{\nu} \vartheta_{11}\left(\frac{2\nu}{n}\right).$$

Man schliesst ferner aus den Formeln (2) des vorigen §, wenn man beachtet dass

$$\vartheta_{00}(0,\ \omega+1)=\vartheta_{01},\qquad \eta(\omega+1)=e^{\frac{\pi i}{12}}\eta(\omega)$$

ist:

$$\vartheta_{10}\eta(\omega)=2\eta(2\omega)^2$$

$$\vartheta_{01}\eta(\omega)=\eta\left(\frac{\omega}{2}\right)^2 \tag{8}$$

$$e^{\frac{\pi i}{12}}\vartheta_{00}\eta(\omega)=\eta\left(\frac{1+\omega}{2}\right)^2.$$

Führt man noch die drei Functionen ein:

$$\eta(2\omega)=\eta_1(\omega),\qquad \eta\left(\frac{\omega}{2}\right)=\eta_2(\omega),\qquad \eta\left(\frac{1+\omega}{2}\right)=\eta_3(\omega), \tag{9}$$

so lassen sich durch diese die HERMITE'schen Functionen φ, ψ, χ folgendermassen darstellen:

$$\varphi(\omega)=e^{\frac{\pi i}{24}}\sqrt{2}\,\frac{\eta_1(\omega)}{\eta_3(\omega)}$$

$$\psi(\omega)=e^{\frac{\pi i}{24}}\frac{\eta_2(\omega)}{\eta_3(\omega)}$$

$$\chi(\omega)=\sqrt[3]{\varphi(\omega)\psi(\omega)}=e^{\frac{\pi i}{24}}\sqrt[6]{2}\,\frac{\eta(\omega)}{\eta_3(\omega)}.$$ [1]

§ 5. *Lineare Transformation.*

Bedeuten α, β, γ, δ vier ganze Zahlen, die der Bedingung

$$\alpha\delta-\beta\gamma=1 \tag{1}$$

genügen, so lassen sich die ϑ-Functionen mit dem Modul

$$\omega_1=\frac{\gamma+\delta\omega}{\alpha+\beta\omega} \tag{2}$$

[1] Vgl. DEDEKIND: *Ueber die elliptischen Modulfunctionen,* Journal f. Mathematik, Bd. 83.

und dem Argument

$$u_1 = \frac{u}{\alpha + \beta\omega} \tag{3}$$

durch solche mit dem Modul ω und dem Argument u ausdrücken. Man findet in der That leicht, wenn A einen constanten Factor bedeutet:

$$\begin{aligned}
e^{-\pi i\beta u u_1}\vartheta_{11}(u_1,\ \omega_1) &= A\vartheta_{11}(u,\ \omega)\\
e^{-\pi i\beta u u_1}\vartheta_{10}(u_1,\ \omega_1) &= i^{\beta}e^{-\frac{\pi i}{4}\alpha\beta}A\vartheta_{1+\beta,\ 1-\alpha}(u,\ \omega)\\
e^{-\pi i\beta u u_1}\vartheta_{01}(u_1,\ \omega_1) &= i^{\delta-1}e^{-\frac{\pi i}{4}\gamma\delta}A\vartheta_{1+\delta,\ 1-\gamma}(u,\ \omega)\\
e^{-\pi i\beta u u_1}\vartheta_{00}(u_1,\ \omega_1) &= i^{\delta+\beta-\alpha\delta}e^{-\frac{\pi i}{4}(\alpha\beta+\gamma\delta)}A\vartheta_{1+\beta+\delta,\ 1-\alpha-\gamma}(u,\ \omega),
\end{aligned} \tag{4}$$

und durch Anwendung der Formel (4) § 3 erhält man eine Bestimmung von A^2. Es soll hier nur

$$A^4 = (-1)^{\beta\gamma+\alpha\beta+\gamma\delta}(\alpha + \beta\omega)^2 \tag{5}$$

angeführt werden. Aus der ersten der Formeln (4) folgt dann die Transformation der η-Function:

$$\eta\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right) = e^{\frac{\pi i}{12}\lambda}\sqrt{-i(\alpha + \beta\omega)}\,\eta(\omega), \tag{6}$$

worin λ eine nach dem Modul 24 bestimmte Zahl ist, wenn wir festsetzen, dass β positiv sei, und die Quadratwurzel mit positiv reellem Teil zu nehmen ist. Für den besonderen Fall $\beta = 0$ ergiebt sich direct:

$$\eta(\omega + 1) = e^{\frac{\pi i}{12}}\eta(\omega); \qquad \eta(\omega + \gamma) = e^{\frac{\pi i}{12}\gamma}\,\eta(\omega), \tag{7}$$

und ausserdem hat man, wie man aus der Annahme eines rein imaginären ω schliesst:

$$\eta\left(-\frac{1}{\omega}\right) = \sqrt{-i\omega}\,\eta(\omega). \tag{8}$$

Durch wiederholte Anwendung der beiden letzten Formeln lässt sich die allgemeine Formel (6) ableiten. Ist λ bestimmt, so ist auch A bekannt nach der Formel

$$A = -ie^{\frac{\pi i\lambda}{4}}\sqrt{-i(\alpha+\beta\omega)}, \tag{9}$$

und den besonderen Fällen (7), (8) entsprechend ergiebt sich:

I.
$$\vartheta_{11}(u,\ \omega+1) = e^{\frac{\pi i}{4}}\vartheta_{11}(u,\ \omega)$$
$$\vartheta_{10}(u,\ \omega+1) = e^{\frac{\pi i}{4}}\vartheta_{10}(u,\ \omega)$$
$$\vartheta_{01}(u,\ \omega+1) = \vartheta_{00}(u,\ \omega)$$
$$\vartheta_{00}(u,\ \omega+1) = \vartheta_{01}(u,\ \omega).$$

II.
$$e^{-\frac{\pi i u^2}{\omega}}\vartheta_{11}\left(\frac{u}{\omega},\ \frac{-1}{\omega}\right) = -i\sqrt{-i\omega}\,\vartheta_{11}(u,\ \omega)$$
$$e^{-\frac{\pi i u^2}{\omega}}\vartheta_{10}\left(\frac{u}{\omega},\ \frac{-1}{\omega}\right) = \sqrt{-i\omega}\,\vartheta_{01}(u,\ \omega)$$
$$e^{-\frac{\pi i u^2}{\omega}}\vartheta_{01}\left(\frac{u}{\omega},\ \frac{-1}{\omega}\right) = \sqrt{-i\omega}\,\vartheta_{10}(u,\ \omega)$$
$$e^{-\frac{\pi i u^2}{\omega}}\vartheta_{00}\left(\frac{u}{\omega},\ \frac{-1}{\omega}\right) = \sqrt{-i\omega}\,\vartheta_{00}(u,\ \omega).$$

Vergleicht man (9) mit (5), so folgt:

$$\lambda \equiv \beta\gamma + \alpha\beta + \gamma\delta + 1 \pmod 2$$

oder:

$$\beta\lambda \equiv \alpha + \delta \pmod 2. \tag{10}$$

Die Zahl λ, die von den vier der Bedingung (1) genügenden ganzen Zahlen abhängig ist, wird nun mittelst der speciellen Transformationen (7), (8) durch ein recurrentes Verfahren bestimmt. Zunächst erkennt man

leicht aus (7), dass die beiden Verbindungen $\alpha\lambda - \gamma$, $\beta\lambda - \delta$ nur von den beiden *relativen Primzahlen* α, β abhängig sind, und demnach setzen wir mit Rücksicht auf (10)

$$\beta\lambda - \delta - \alpha = -2(\alpha, \beta), \tag{11}$$

worin (α, β) eine von α und β abhängige nach dem Modul 12 bestimmte Zahl ist. Da die gleichzeitige Änderung der Vorzeichen von α, β, γ, δ den Wert von λ nicht ändert, so folgt aus (11)

$$(-\alpha, -\beta) = -(\alpha, \beta); \qquad (1, 0) = 1. \tag{12}$$

Da die beiden Functionen

$$\eta\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right), \qquad \eta\left(\frac{\gamma - \delta\omega}{-\alpha + \beta\omega}\right)$$

für rein imaginäre ω conjugirt imaginär sind, so schliesst man aus (6) und (11), (12):

$$(\alpha, \beta) \equiv -(-\alpha, \beta) \equiv (\alpha, -\beta) \pmod{12}. \tag{13}$$

Vertauscht man in (6) α, β, γ, δ mit $-\beta$, α, $-\delta$, γ und bezeichnet den diesem Zahlencomplex entsprechenden Wert von λ mit λ' so ergiebt die Anwendung von (8)

$$\lambda' \equiv \lambda \mp 3 \pmod{24}, \tag{14}$$

wenn das obere Zeichen für ein positives, das untere für ein negatives α genommen und β positiv vorausgesetzt wird.

Macht man in der Gleichung (11) dieselbe Vertauschung, so ergiebt sich nach (14), wenn mit $|\alpha|$ der absolute Wert von α bezeichnet wird:

$$\alpha\lambda - \gamma + \beta - 3|\alpha| \equiv 2(\beta, \alpha) \pmod{24}, \tag{15}$$

und aus (11) und (15)

$$\lambda \equiv \delta\{2(\beta, \alpha) - \beta + 3|\alpha|\} + \gamma\{2(\alpha, \beta) - \alpha\} \pmod{24}, \tag{16}$$

wodurch die Bestimmung von λ vollständig auf die des Symbols (α, β)

zurückgeführt ist. Für die Berechnung dieses Symbols ergiebt sich aber, wenn man in (6) ω durch $\omega + 1$ ersetzt und (7), (8) und (11) anwendet:

$$(17)\qquad \begin{aligned} &(\alpha', \beta) \equiv (\alpha, \beta) \pmod{12}, \quad \text{wenn} \quad \alpha' \equiv \alpha \pmod{\beta} \\ &(\alpha, 1) \equiv (0, 1) \equiv 0 \pmod{12}, \end{aligned}$$

und wenn man λ aus (11) und (15) eliminirt:

$$(18)\qquad 2\alpha(\alpha, \beta) + 2\beta(\beta, \alpha) \equiv 1 + \alpha^2 + \beta^2 - 3|\alpha|\beta \pmod{24},$$

wodurch dasselbe völlig bestimmt ist.

Nimmt man in (18) α und β ungerade und positiv an, und vergleicht diese Formel mit der aus dem Reciprocitätsgesetz der quadratischen Reste folgenden

$$(19)\qquad 2\alpha\left(\frac{\alpha}{\beta}\right) + 2\beta\left(\frac{\beta}{\alpha}\right) \equiv (\alpha + 1)(\beta + 1) \pmod 8,$$

so leitet man daraus her

$$(20)\qquad \alpha\left|(\alpha, \beta) + \left(\frac{\alpha}{\beta}\right) - \frac{\beta + 1}{2}\right| + \beta\left|(\beta, \alpha) + \left(\frac{\beta}{\alpha}\right) - \frac{\alpha + 1}{2}\right| \equiv 0 \pmod 4$$

und hieraus schliesst man durch Anwendung des Algorithmus vom grössten gemeinschaftlicher Teiler

$$(21)\qquad (\alpha, \beta) \equiv \frac{\beta + 1}{2} - \left(\frac{\alpha}{\beta}\right) \pmod 4$$

eine Formel, die wegen (13) und (17) auch für negative und gerade α gültig bleibt.

Hiernach ergiebt sich ohne Schwierigkeiten das Verhalten von (α, β) zu dem Modul 4 auch für ein gerades β aus der Formel (18) und desgleichen für den Modul 3, wodurch das Symbol (α, β) nach dem Modul

12, worauf es allein ankommt, für alle Fälle bestimmt ist. Wir stellen hier das vollständige Formelsystem übersichtlich zusammen.

$$(0,\ 1)\equiv 0, \qquad (1,\ 0)\equiv 1 \pmod{12}$$

$$(-\alpha,\ \beta)\equiv -(\alpha,\ \beta) \pmod{12}$$

$$(\alpha,\ -\beta)\equiv (\alpha,\ \beta). \pmod{12}$$

$$(-\alpha,\ -\beta)\equiv -(\alpha,\ \beta) \pmod{12}$$

(22)

$$(\alpha,\ \beta)\equiv \alpha \pmod 3, \qquad \beta\equiv 0 \pmod 3$$

$$(\alpha,\ \beta)\equiv 0 \pmod 3, \qquad \beta\equiv \pm 1 \pmod 3$$

$$(\alpha,\ \beta)\equiv \frac{\beta+1}{2}-\left(\frac{\alpha}{\beta}\right) \pmod 4, \qquad \beta\equiv 1 \pmod 2,\ \beta>0$$

$$(\alpha,\ \beta)\equiv \alpha \pmod 4, \qquad \beta\equiv 0 \pmod 8$$

$$(\alpha,\ \beta)\equiv -\alpha \pmod 4, \qquad \beta\equiv 4 \pmod 8$$

$$(\alpha,\ \beta)\equiv 0 \pmod 4, \qquad \beta\equiv 2 \pmod 8,\ \beta>0$$

$$(\alpha,\ \beta)\equiv 2 \pmod 4, \qquad \beta\equiv 6 \pmod 8,\ \beta>0$$

$$\lambda\equiv\delta\{2(\beta,\ \alpha)-\beta+3|\alpha|\}+\gamma\{2(\alpha,\ \beta)-\alpha\} \pmod{24}.$$

Das Symbol $(\alpha,\ \beta)$ ist von DEDEKIND in die Theorie eingeführt (RIEMANN's gesammelte Werke, Erläuterungen zu No. XXVII und Journal für Mathematik, Bd. 83, S. 265). Das vollständige Formelsystem (22) welches ich mit seiner Zustimmung hier aufnehme, verdanke ich einer brieflichen Mitteilung. Das Symbol ist in der Transformationstheorie der elliptischen Functionen kaum zu entbehren und umfasst alle verwandten specielleren Untersuchungen. So ergeben sich sehr leicht aus den Formeln (10) § 4 die HERMITE'schen Transformationsformeln für die Functionen $\varphi(\omega)$, $\psi(\omega)$, $\chi(\omega)$, von denen hier nur die folgenden den speciellen Trans-

formationen (7), (8) entsprechenden angeführt sein mögen, aus welchen die übrigen durch wiederholte Anwendung folgen.

$$\eta_1(\omega+1)=e^{\frac{\pi i}{6}}\eta_1(\omega),\qquad \eta_1\left(-\frac{1}{\omega}\right)=\sqrt{\frac{-i\omega}{2}}\eta_2(\omega)$$

$$\eta_2(\omega+1)=\quad\eta_3(\omega),\qquad \eta_2\left(-\frac{1}{\omega}\right)=\sqrt{-2i\omega}\,\eta_1(\omega) \tag{23}$$

$$\eta_3(\omega+1)=e^{\frac{\pi i}{12}}\eta_2(\omega),\qquad \eta_3\left(-\frac{1}{\omega}\right)=\sqrt{-i\omega}\,\eta_3(\omega).$$

$$\varphi(\omega+1)=e^{\frac{i\pi}{8}}\frac{\varphi(\omega)}{\psi(\omega)},\qquad \varphi\left(-\frac{1}{\omega}\right)=\psi(\omega)$$

$$\psi(\omega+1)=\quad\frac{1}{\psi(\omega)},\qquad \psi\left(-\frac{1}{\omega}\right)=\varphi(\omega) \tag{24}$$

$$\chi(\omega+1)=e^{\frac{i\pi}{24}}\frac{\chi(\omega)}{\psi(\omega)},\qquad \chi\left(-\frac{1}{\omega}\right)=\chi(\omega).$$

Wenn man die Formeln (4) für die lineare Transformation auf (2) § 4 anwendet, so ergiebt sich die allgemeinere Formel, in welcher α, β irgend zwei relative Primzahlen sind:

$$2^{\frac{n-1}{2}}\prod_{1,\frac{n-1}{2}}^{\nu}\vartheta_{00}\left(\frac{2\nu(\alpha+\beta\omega)}{n}\right)\vartheta_{10}\left(\frac{2\nu(\alpha+\beta\omega)}{n}\right)\vartheta_{01}\left(\frac{2\nu(\alpha+\beta\omega)}{n}\right) \tag{25}$$

$$=(-1)^{\frac{n^2-1}{8}}e^{\frac{\pi i}{6}\beta(\alpha+\beta\omega)\frac{n^2-1}{n}}\vartheta_{00}^{\frac{n-1}{2}}\vartheta_{10}^{\frac{n-1}{2}}\vartheta_{01}^{\frac{n-1}{2}}.$$

Ebenso kann man durch Verbindung mit der linearen Transformation aus (7) § 4 die allgemeine Transformationsformel für

$$\eta\left(\frac{c+d\omega}{a+b\omega}\right)$$

herleiten, wenn a, b, c, d ganze Zahlen ohne gemeinsamen Teiler sind, die der Bedingung $ad-bc=n$ genügen. Wählt man nämlich die ganzen Zahlen x, y so dass

$$\alpha=xa+yc$$
$$\beta=xb+yd \tag{26}$$

ohne gemeinsamen Teiler sind,(1) und γ, δ so dass

$$\alpha\delta - \beta\gamma = 1$$

ist, so lässt sich die Transformation

$$\begin{pmatrix} a, & b \\ c, & d \end{pmatrix}$$

in folgender Weise zusammensetzen

$$\begin{pmatrix} a, & b \\ c, & d \end{pmatrix} = \begin{pmatrix} a\delta - b\gamma, & -y \\ c\delta - d\gamma, & x \end{pmatrix} \begin{pmatrix} 1, & 0 \\ 0, & n \end{pmatrix} \begin{pmatrix} a, & \beta \\ \gamma, & \delta \end{pmatrix}. \tag{27}$$

Wenn nun λ, λ' die oben festgesetzte Bedeutung haben für die beiden linearen Transformationen

$$\begin{pmatrix} a, & \beta \\ \gamma, & \delta \end{pmatrix}, \qquad \begin{pmatrix} a\delta - b\gamma, & -y \\ c\delta - d\gamma, & x \end{pmatrix}$$

so folgt unter der Voraussetzung eines positiven β und y

$$\eta\left(\frac{c + d\omega}{a + b\omega}\right) \eta(\omega)^{\frac{n-3}{2}}$$

$$= (-i)^{\frac{n-1}{2}} e^{\frac{\pi i}{12}(n\lambda + \lambda')} e^{\pi i\beta(a+\beta\omega)\frac{n^2-1}{6n}} \sqrt{\frac{a + b\omega}{n}} \prod_{1, \frac{n-1}{2}}^{\nu} \vartheta_{11}\left(\frac{2\nu(a + \beta\omega)}{n}\right) \tag{28}$$

wo die Quadratwurzel mit positivem reellem Teil zu nehmen ist.

---

(1) Dass ein solches Zahlensystem x, y immer existirt, ist leicht einzusehen; denn ist p irgend eine in n aufgehende Primzahl, so kann man zunächst die beiden Zahlen x_p, y_p so wählen, dass $ax_p + cy_p$, $bx_p + dy_p$ nicht beide durch p teilbar sind, und wenn man dann $x \equiv x_p$, $y \equiv y_p \pmod{p}$; $x \equiv x_{p'}$, $y \equiv y_{p'} \pmod{p'}$, ... setzt, für alle in n aufgehenden Primzahlen p, p', ... so genügen diese Werte der gestellten Forderung (Vgl. KÖNIGSBERGER, *Ellipt. Functionen*, II, S. 93).

II. Abschnitt.

§ 6. *Die elliptischen Functionen.*

Die Quotienten zweier θ-Functionen gleicher Ordnung sind doppelt periodische Functionen, und es ergiebt sich sehr leicht aus den Sätzen des § 1, dass sich *alle* eindeutigen doppelt periodischen Functionen, welche im Innern eines Periodenparallelogramms in einer endlichen Anzahl von Punkten unendlich in endlicher Ordnung werden, als solche Quotienten darstellen lassen; und da die Differentialquotienten von doppelt periodischen Functionen wieder ebensolche Functionen sind, so kann man auf Grund der oben nachgewiesenen algebraischen Beziehungen zwischen den θ-Functionen algebraische Differentialgleichungen für die doppelt periodischen Functionen erhalten. Wir betrachten als die einfachsten von diesen Functionen die folgenden:

$$x = \frac{\vartheta_{00}}{\vartheta_{10}} \frac{\vartheta_{11}(u)}{\vartheta_{01}(u)}$$

$$y = \frac{\vartheta_{01}}{\vartheta_{10}} \frac{\vartheta_{10}(u)}{\vartheta_{01}(u)} \tag{1}$$

$$z = \frac{\vartheta_{01}}{\vartheta_{00}} \frac{\vartheta_{00}(u)}{\vartheta_{01}(u)}.$$

Die Ableitungen dieser Functionen nach u sind doppelt periodische Functionen, deren Zähler und Nenner θ-Functionen zweiter Ordnung sind, die sich daher nach § 2 darstellen lassen. Man findet so durch Nullsetzen der Argumente für die Zähler dieser Ableitungen die Ausdrücke

$$\vartheta'_{11}(u)\vartheta_{01}(u) - \vartheta'_{01}(u)\vartheta_{11}(u) = \pi\vartheta_{01}^2\vartheta_{00}(u)\vartheta_{10}(u)$$

$$\vartheta'_{10}(u)\vartheta_{01}(u) - \vartheta'_{01}(u)\vartheta_{10}(u) = -\pi\vartheta_{00}^2\vartheta_{11}(u)\vartheta_{00}(u) \tag{2}$$

$$\vartheta'_{00}(u)\vartheta_{01}(u) - \vartheta'_{01}(u)\vartheta_{00}(u) = -\pi\vartheta_{10}^2\vartheta_{11}(u)\vartheta_{10}(u).$$

Setzt man daher

$$k = \frac{\vartheta_{10}^2}{\vartheta_{00}^2}, \qquad k' = \frac{\vartheta_{01}^2}{\vartheta_{00}^2}, \qquad k^2 + k'^2 = 1$$

(3)
$$\sqrt[4]{k} = \varphi(\omega), \quad \sqrt[4]{k'} = \psi(\omega), \qquad \sqrt[12]{kk'} = \chi(\omega),$$

so dass

(4)
$$x^2 + y^2 = 1, \qquad z^2 + k^2x^2 = 1$$

wird, und ferner

(5)
$$\pi\vartheta_{00}^2 = 2K, \qquad \omega K = iK', \qquad v = 2Ku,$$

so erhält man für die Functionen x, y, z das System von Differentialgleichungen

(6)
$$\frac{dx}{dv} = yz$$
$$\frac{dy}{dv} = -zx$$
$$\frac{dz}{dv} = -k^2xy$$

mit den Nebenbedingungen, dass

(7)
$$\text{für} \quad v = 0 \; : \; x = 0, \; y = 1, \; z = 1$$

sei; und dies System ist also durch die Ausdrücke (1) vollständig integrirt. x, y, z heissen die *elliptischen Grundfunctionen* und k der *Modul*. Als Functionen von v und k werden sie mit

(8)
$$x = \sin\operatorname{am}(v, k)$$
$$y = \cos\operatorname{am}(v, k)$$
$$z = \Delta\operatorname{am}(v, k)$$

bezeichnet. Da durch die Nebenbedingungen (7) die Lösungen der Differentialgleichungen (6) völlig und eindeutig bestimmt sind, so folgt, dass, wenn zwei verschiedene Werte von ω, ω und ω_1, zu demselben Werte von k^2 führen, die Functionen

$$\vartheta_{g,h}(u, \omega) \quad \text{und} \quad \vartheta_{g,h}(u_1, \omega_1)$$

wenn

$$\vartheta_{00}^2(0,\ \omega)u = \vartheta_{00}^2(0,\ \omega_1)u_1$$

ist, für dieselben Werte von u verschwinden, und dass in Folge dessen ω und ω_1 in der Verbindung stehen

$$\omega_1 = \frac{2\gamma + \delta\omega}{\alpha + 2\beta\omega}, \qquad \alpha\delta - 4\beta\gamma = 1, \tag{9}$$

wenn α, β, γ, δ ganze Zahlen sind, oder, mit andern Worten, dass die Gleichung

$$\varphi(\omega)^8 = \varphi(\omega_1)^8$$

die Gleichung (9) zur notwendigen Folge hat.(1) Es folgt aber auch umgekehrt aus der linearen Transformation der ϑ-Functionen (§ 5 (4)) dass k^2 immer denselben Wert erhält, sobald ω durch ω_1 ersetzt wird. Allgemeiner ergiebt sich aus den erwähnten Formeln, dass, wenn ω durch irgend einen Ausdruck

$$\frac{\gamma + \delta\omega}{\alpha + \beta\omega}, \qquad \alpha\delta - \beta\gamma = 1 \tag{10}$$

ersetzt wird, k^2 immer in einen der 6 Werte

$$k^2, \quad k'^2, \quad \frac{1}{k^2}, \quad \frac{1}{k'^2}, \quad -\frac{k^2}{k'^2}, \quad -\frac{k'^2}{k^2} \tag{11}$$

übergeht, und dass auch umgekehrt, sobald $\varphi(\omega_1)^8$ einem dieser 6 Werte gleich wird, ω_1 ein Ausdruck von der Form (10) sein muss. Eine symmetrische Function der 6 Grössen (11) hat also die Eigenschaft, ungeändert zu bleiben, wenn für ω eine der Substitutionen (10), die wir in üblicher Weise durch

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$$

bezeichnen, darin ausgeführt wird. Jede solche symmetrische Function

(1) Vgl. DEDEKIND, Journal f. Mathematik, Bd. 83, S. 266.

ist aber rational ausdrückbar durch die Coëfficienten der rationalen Function 6^{ten} Grades:

$$(\xi - k^2)(\xi - k'^2)\left(\xi - \frac{1}{k^2}\right)\left(\xi - \frac{1}{k'^2}\right)\left(\xi + \frac{k^2}{k'^2}\right)\left(\xi + \frac{k'^2}{k^2}\right)$$

$$= \xi^6 - 3\xi^5 + A\xi^4 - B\xi^3 + A\xi^2 - 3\xi + 1$$

zwischen denen die Relation besteht (aus $\xi = 1$)

$$2A - B = 5$$

$$A = 6 - \frac{(1 - k^2k'^2)^3}{k^4k'^4}.$$

Hiernach können wir alle diese symmetrischen Functionen rational ausdrücken durch die eine

$$j(\omega) = 2^8 \frac{(1 - k^2k'^2)^3}{k^4k'^4} \tag{12}$$

welche die *absolute Invariante* des Systems doppelt periodischer Functionen genannt wird.

Nennen wir zwei Zahlen ω, ω_1 *äquivalent* wenn

$$\omega_1 = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}, \qquad \alpha\delta - \beta\gamma = 1$$

ist für ganzzahlige α, β, γ, δ, so hat die Function $j(\omega)$ nach dem obigen die fundamentale Eigenschaft, *dass sie für äquivalente Werte von ω und nur für solche denselben Wert erhält.* (1)

Ausser dieser absoluten Invariante führen wir (nach WEIERSTRASS, vgl. die von H. A. SCHWARZ herausgegebenen *Formeln und Lehrsätze zum Gebrauch der elliptischen Functionen*) noch zwei andere einwertige Func-

(1) Die von DEDEKIND l. c. eingeführte Valenz, $\mathrm{val}(\omega)$ ist nach dieser Bezeichnung $\frac{1}{27.64} j$; dieselbe Bedeutung hat das von KLEIN in seinen Untersuchungen benutzte Zeichen J (Mathematische Annalen, Bd. XIV, S. 112).

tionen g_2, g_3 ein, die wir die Invarianten schlechtweg nennen, und die als eindeutige Functionen von ω folgendermassen definirt sind:

$$(13)\qquad g_2 = \frac{4}{3}\frac{1-k^2k'^2}{\sqrt[3]{k^4k'^4}} = \frac{1}{3}\sqrt[3]{\frac{1}{4}j}$$

$$g_3 = \frac{4}{27}\frac{(2+k^2k'^2)(k'^2-k^2)}{k^2k'^2} = \frac{\sqrt{j-27.64}}{2.27},$$

und daher der Bedingung genügen

$$(14)\qquad g_2^3 - 27g_3^2 = 16.$$

Die Grundformeln für die lineare Transformation dieser Functionen ergeben sich mittelst der Formeln (24) § 5:

$$(15)\qquad g_2(\omega+1) = e^{-\frac{2\pi i}{3}} g_2(\omega),$$

$$g_3(\omega+1) = -g_3(\omega)$$

$$(16)\qquad g_2\left(-\frac{1}{\omega}\right) = g_2(\omega)$$

$$g_3\left(-\frac{1}{\omega}\right) = -g_3(\omega).$$

§ 7. *Der Modul und die Invariante als unabhängige Variable.*

Während in den bisherigen Betrachtungen der Modul k^2 und die Invariante $j(\omega)$ als Functionen von ω betrachtet wurden, wollen wir jetzt umgekehrt das Periodenverhältniss ω als Function der ersteren untersuchen. Am vollständigsten geschieht dies vermittelst der Darstellung durch hypergeometrische Reihen. Da diese Darstellungen aber für unsern Zweck nicht unbedingt erforderlich sind, so wollen wir hier nicht auf dieselben eingehen. Dagegen ist es notwendig, die Differentialgleichungen zwischen ω und j aufzustellen, die man sehr leicht aus der partiellen Differentialgleichung (§ 2 (2))

$$(1)\qquad \frac{\partial^2\vartheta}{\partial u^2} = 4\pi i\frac{\partial\vartheta}{\partial\omega}$$

ableiten kann. Wenn man die letzte Gleichung (2) § 6 nach u differentiirt und dann $u = 0$ setzt, so folgt nach (1):

$$dk^2 = -dk'^2 = \pi i \vartheta_{00}^4 k^2 k'^2 d\omega, \tag{2}$$

woraus durch einfache Rechnung folgt:

$$\begin{aligned} dj &= 3^4 \cdot 2^2 g_2^2 dg_2 = 3^6 \cdot 2^3 g_3 dg_3, \\ \frac{dj}{g_2^2 g_3} &= -\pi i 2^3 \cdot 3^5 \cdot \sqrt[3]{2}\, \eta(\omega)^4 d\omega. \end{aligned} \tag{3}$$

Stellen wir also die complexe Variable k^2 in einer Ebene dar, so findet für die Function ω eine Verzweigung nur statt in den drei Punkten

$$k^2 = 0, \qquad k^2 = 1, \qquad k^2 = \infty,$$

und die verschiedenen Werte, welche ω für einen und denselben Wert von k^2 erhält, sind alle in der Form enthalten

$$\frac{2\gamma + \delta\omega}{\alpha + 2\beta\omega}, \qquad \alpha\delta - 4\beta\gamma = 1. \tag{4}$$

Desgleichen folgt aus (3), dass ω als Function von j betrachtet nur in den Punkten

$$j = \infty, \qquad j = 0, \qquad j = 27.64$$

verzweigt ist, und dass alle Werte, deren ω für dasselbe j fähig ist, in der Form

$$\frac{\gamma + \delta\omega}{\alpha + \beta\omega}, \qquad \alpha\delta - \beta\gamma = 1 \tag{5}$$

enthalten sind.

Nun folgt aus (6) § 6

$$v = \int_0^x \frac{dx}{\sqrt{(1 - x^2)(1 - k^2 x^2)}} \tag{6}$$

wodurch v als Function von x, wenn auch nicht eindeutig, dargestellt

ist. Für $v = K$, $u = \frac{1}{2}$ hat x den Wert 1 und für $v = K + iK'$, $u = \frac{1}{2}(1 + \omega)$ den Wert $1 : k$, und darnach ergiebt sich aus (6)

$$(7) \qquad K = \int_0^1 \frac{dx}{\sqrt{(1 - x^2)(1 - k^2x^2)}}$$

$$iK' = \int_1^{\frac{1}{k}} \frac{dx}{\sqrt{(1 - x^2)(1 - k^2x^2)}}.$$

In (7) sind die Integrationswege und die Vorzeichen der Wurzeln dadurch völlig bestimmt, dass man in der u-Ebene, etwa den Seiten des Periodenparallelogramms parallel von 0 bis $\frac{1}{2}$ und von $\frac{1}{2}$ bis $\frac{1}{2}(1 + \omega)$ geht, und die zugehörigen Werte x, $y = \sqrt{1 - x^2}$, $z = \sqrt{1 - k^2x^2}$ immer aus den Gleichungen (1) § 6 bestimmt.

Nimmt man ω rein imaginär an, so sind $\varphi(\omega)$, $\psi(\omega)$ reell und mithin $\sqrt{k}$, $\sqrt{k'}$ positive echte Brüche; und wenn u auf reellem Wege von 0 bis $\frac{1}{2}$ geht, so bleiben die vier Functionen $\vartheta_{00}(u)$, $\vartheta_{10}(u)$, $\vartheta_{01}(u)$, $\vartheta_{11}(u)$ reell und positiv; denn keine derselben geht auf diesem Wege durch Null, und ϑ_{00}, ϑ_{10}, ϑ_{01}, $\vartheta_{11}\left(\frac{1}{2}\right) = \vartheta_{10}$ sind positiv. (Bezüglich ϑ_{00} zeigt dies die Reihe unmittelbar, und für die andern Functionen folgt das Gleiche aus den positiven Werten von $\sqrt{k}$, $\sqrt{k'}$.) Es bleiben also nach § 6 (1), (6) auch die Variablen x, y, z reell und positiv, und keine derselben hat auf dem Wege ein Maximum oder Minimum.

Hierdurch ist der Integrationsweg für K (längs der reellen Axe mit positivem Werte der Quadratwurzel) bestimmt. Beachtet man ferner dass nach § 2 (4) für ein rein imaginäres u die Functionen $\vartheta_{00}\left(u + \frac{1}{2}\right)$, $\vartheta_{01}\left(u + \frac{1}{2}\right)$, $\vartheta_{11}\left(u + \frac{1}{2}\right)$ reell, $\vartheta_{10}\left(u + \frac{1}{2}\right)$ rein imaginär bleiben, so erkennt man, dass, während u von $\frac{1}{2}$ bis $\frac{1}{2}(1 + \omega)$ geht, (parallel der imaginären

Axe), x, z reell, y rein imaginär bleiben; und auch auf diesem Wege findet für keine dieser Functionen ein Maximum oder Minimum statt. Man hat also auch in dem Integral iK' den Integrationsweg von 1 bis $1:k$ längs der reellen Axe zu nehmen und zwar mit solchem Zeichen der Quadratwurzel, dass K' positiv wird. ($\sqrt{1-x^2} = -i\sqrt{x^2-1}$ und $\sqrt{x^2-1}$, $\sqrt{1-k^2x^2}$ positiv.)

Wenn nun die Variable k^2 in ihrer Ebene den Punkt 1 (mit Ausschluss des Punktes 0) in positivem Sinne umkreist, so umkreisen in der x-Ebene die Punkte $\pm 1:k$ resp. die Punkte ± 1 in negativem Sinne; und daraus erkennt man, indem man die Integrationswege stetig ändert, dass bei diesem Vorgang

$$K, \qquad iK' \quad \text{in} \quad K + 2iK', \qquad iK'$$

übergehen. Wenn der Punkt k^2 den Punkt 0 (mit Ausschluss des Punktes 1) in positivem Sinne umkreist, so geht in der x-Ebene der Punkt $1:k$ in negativem Sinne nach $-1:k$ und umgekehrt. Hieraus ergiebt sich ebenso, dass hierbei

$$K, \qquad iK' \quad \text{in} \quad K, \qquad 2K + iK'$$

übergehen. Wenn wir also ω als Function von k^2 auffassen, so wird beim Umkreisen des Punktes 1 und 0

$$\omega \quad \text{in} \quad \frac{\omega}{1 + 2\omega} \quad \text{und in} \quad \omega + 2$$

übergehen. Da nun alle Substitutionen

$$\begin{pmatrix} \alpha, & 2\beta \\ 2\gamma, & \delta \end{pmatrix}$$

sich aus den beiden

$$\begin{pmatrix} 1, & 2 \\ 0, & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1, & 0 \\ 2, & 1 \end{pmatrix}$$

zusammensetzen lassen, so zeigt sich also, dass ω, als Function von k^2 aufgefasst, durch stetige Änderung für einen und denselben Wert von k^2 in der That alle Werte von der Form (4) anzunehmen fähig ist.

Lassen wir ferner k^2 auf reellem Wege nach $1-k^2$ gehen, so erhält j den Ausgangswert wieder, während K und iK' übergehen in

$$\int_0^1 \frac{dx}{\sqrt{(1-x^2)(1-k'^2x^2)}}, \qquad \int_1^{\frac{1}{k'}} \frac{dx}{\sqrt{(1-x^2)(1-k'^2x^2)}}$$

d. h. in K', iK, wie man aus der Substitution $1-k^2x^2 = k'^2x_1^2$ erkennt; demnach geht ω in $-1:\omega$ über. Führt man endlich durch einen halben positiven Umlauf um den Punkt 1 k^2 in $1:k^2$ über, so geht $1:k$ durch einen halben negativen Umlauf nach dem Punkt k, j erhält seinen ursprünglichen Wert wieder, und es geht K, iK' über in

$$\int_0^k \frac{dx}{\sqrt{(1-x^2)\left(1-\frac{x^2}{k^2}\right)}} + i\int_k^1 \frac{dx}{\sqrt{(1-x^2)\left(\frac{x^2}{k^2}-1\right)}},$$

$$i\int_k^1 \frac{dx}{\sqrt{(1-x^2)\left(\frac{x^2}{k^2}-1\right)}},$$

mit positivem Wert der Quadratwurzel. Die Substitution $x = kx_1$ zeigt aber, dass diese beiden Werte gleich

$$k(K+iK'), \qquad kiK'$$

sind, und dass also ω in $\omega:(1+\omega)$ übergegangen ist. Hieraus schliesst man nun, dass es in der j-Ebene Kreiswege giebt, durch welche

$$\omega \quad \text{in} \quad \frac{-1}{\omega} \quad \text{und in} \quad \frac{\omega}{1+\omega}$$

übergeführt wird, und da alle Substitutionen

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$$

aus den beiden

$$\begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}, \qquad \begin{pmatrix} 1, & 1 \\ 0, & 1 \end{pmatrix}$$

zusammengesetzt werden können, so folgt wie oben, dass für einen und denselben Wert j die Function ω wirklich aller Werte (5) fähig ist.

Hieraus ergeben sich nun auf Grund des Satzes der Functionentheorie, dass eine einwertige Function *einer* Veränderlichen, welche überall den Charakter einer algebraischen Function hat, notwendig eine rationale Function sein muss, die folgenden speciellen Theoreme:

Wenn eine Function von ω, als Function von k^2 aufgefasst, überall einen algebraischen Charakter besitzt und

1° durch die beiden Substitutionen

$$\frac{\omega}{1+2\omega}, \qquad \omega+2$$

ungeändert bleibt, so ist sie eine rationale Function von k^2;

2° durch die Substitutionen

$$-\frac{1}{\omega}, \qquad \omega+1$$

ungeändert bleibt, so ist sie eine rationale Function von j;

3° durch die beiden Substitutionen

$$\frac{-1}{\omega}, \qquad \omega+1$$

ihr Zeichen ändert, so ist sie das Product von g_3 mit einer rationalen Function von j;

4° durch $-1:\omega$ ungeändert bleibt, durch $\omega+1$ den Factor

$$e^{-\frac{2\pi i}{3}} \quad \text{oder} \quad e^{\frac{2\pi i}{3}}$$

annimmt, so ist sie das Product von g_2 oder g_2^2 mit einer rationalen Function von j;

5° durch die Substitutionen $-1:\omega$, $\omega+1$ beziehlich die Factoren

$$-1, \quad -e^{-\frac{2\pi i}{3}} \quad \text{oder} \quad -1, \quad -e^{\frac{2\pi i}{3}}$$

annimmt, so ist sie das Product von g_2g_3 oder von $g_2^2g_3$ mit einer rationalen Function von j.

III. Abschnitt.

§ 8. *Das Additionstheorem.*

Ein Product mehrerer θ-Functionen von der Form

$$(1) \qquad \theta_{g,h}(u+v)\theta_{g',h'}(u+v')\theta_{g'',h''}(u+v'')\ldots$$

ist eine θ-Function von u unter der Voraussetzung

$$v + v' + v'' + \ldots \equiv 0 \pmod{1, \omega},$$

und zwar ist Ordnung und Charakteristik derselben gleich der Summe der Ordnungen und Charakteristiken der einzelnen Factoren. Man kann daher das Product (1) als ganze rationale Function der $\vartheta_{g,h}(u)$ ausdrücken, so zwar, dass diese Ausdrücke noch von den Variablen $v, v', v'', \ldots$ abhängen. Diese Ausdrücke erhält man aus den Nullpunkten des Productes (1). Dies ist die allgemeinste Form des *Additionstheorems* der θ-Functionen, aus welchem das Additionstheorem für die elliptischen Functionen folgt. Die einfachsten und wichtigsten unter diesen Formeln sind die folgenden

$$(2) \quad \begin{aligned}
\vartheta_{01}^2\vartheta_{01}(u+v)\vartheta_{01}(u-v) &= \vartheta_{01}^2(v)\vartheta_{01}^2(u) - \vartheta_{11}^2(v)\vartheta_{11}^2(u)\\
\vartheta_{00}\vartheta_{01}\vartheta_{00}(u+v)\vartheta_{01}(u-v) &= \vartheta_{00}(u)\vartheta_{00}(v)\vartheta_{01}(u)\vartheta_{01}(v) - \vartheta_{11}(u)\vartheta_{11}(v)\vartheta_{10}(u)\vartheta_{10}(v)\\
\vartheta_{10}\vartheta_{01}\vartheta_{10}(u+v)\vartheta_{01}(u-v) &= \vartheta_{10}(u)\vartheta_{10}(v)\vartheta_{01}(u)\vartheta_{01}(v) - \vartheta_{11}(u)\vartheta_{11}(v)\vartheta_{00}(u)\vartheta_{00}(v)\\
\vartheta_{00}\vartheta_{10}\vartheta_{11}(u+v)\vartheta_{01}(u-v) &= \vartheta_{01}(u)\vartheta_{11}(u)\vartheta_{00}(v)\vartheta_{10}(v) + \vartheta_{01}(v)\vartheta_{11}(v)\vartheta_{00}(u)\vartheta_{10}(u),
\end{aligned}$$

aus welchen man durch Division die drei Grundformeln des Additionstheorems der elliptischen Functionen erhält:

$$(3) \quad \begin{aligned}
\operatorname{sin\,am}(u \pm v) &= \frac{\operatorname{sin\,am} u \operatorname{cos\,am} v \,\Delta\operatorname{am} v \pm \operatorname{cos\,am} u \,\Delta\operatorname{am} u \operatorname{sin\,am} v}{1 - k^2 \operatorname{sin\,am} u^2 \operatorname{sin\,am} v^2}\\
\operatorname{cos\,am}(u \pm v) &= \frac{\operatorname{cos\,am} u \operatorname{cos\,am} v \mp \operatorname{sin\,am} u \,\Delta\operatorname{am} u \operatorname{sin\,am} v \,\Delta\operatorname{am} v}{1 - k^2 \operatorname{sin\,am} u^2 \operatorname{sin\,am} v^2}\\
\Delta\operatorname{am}(v \pm v) &= \frac{\Delta\operatorname{am} u \,\Delta\operatorname{am} v \mp k^2 \operatorname{sin\,am} u \operatorname{cos\,am} u \operatorname{sin\,am} v \operatorname{cos\,am} v}{1 - k^2 \operatorname{sin\,am} u^2 \operatorname{sin\,am} v^2}
\end{aligned}$$

§ 9. *Multiplication der elliptischen Functionen.*

Die Function

$$\vartheta_{g,h}(nu)$$

ist, wenn n eine ganze Zahl ist, eine θ-Function der Variablen u von der Ordnung n^2, und ihre Charakteristik ist bei ungeradem n (g, h) bei geradem n $(0, 0)$. Es lassen sich daher alle diese Functionen nach § 2 I, II rational durch die Functionen $\vartheta_{g,h}(u)$ ausdrücken, und wir wollen diesen Ausdrücken im Hinblick auf die elliptischen Functionen die folgende Gestalt geben:

I. $n \equiv 0 \pmod 2$

$$\vartheta_{00}\vartheta_{10}\vartheta_{01}^{n^2-3}\vartheta_{11}(nu)$$

$$= \vartheta_{00}(u)\vartheta_{01}(u)\vartheta_{10}(u)\vartheta_{11}(u)\sum_{0,\frac{1}{2}n^2-2}^{\nu} a_\nu \vartheta_{11}(u)^{2\nu}\vartheta_{01}(u)^{n^2-4-2\nu}\frac{\vartheta_{00}^{2\nu}}{\vartheta_{10}^{2\nu}}$$

$$\vartheta_{01}^{n^2}\vartheta_{10}(nu) = \vartheta_{10}\sum_{0,\frac{1}{2}n^2}^{\nu} b_\nu \vartheta_{11}(u)^{2\nu}\vartheta_{01}(u)^{n^2-2\nu}\frac{\vartheta_{00}^{2\nu}}{\vartheta_{10}^{2\nu}}$$

$$\vartheta_{01}^{n^2}\vartheta_{00}(nu) = \vartheta_{00}\sum_{0,\frac{1}{2}n^2}^{\nu} c_\nu \vartheta_{11}(u)^{2\nu}\vartheta_{01}(u)^{n^2-2\nu}\frac{\vartheta_{00}^{2\nu}}{\vartheta_{10}^{2\nu}}$$

$$\vartheta_{01}^{n^2}\vartheta_{01}(nu) = \vartheta_{01}\sum_{0,\frac{1}{2}n^2}^{\nu} d_\nu \vartheta_{11}(u)^{2\nu}\vartheta_{01}(u)^{n^2-2\nu}\frac{\vartheta_{00}^{2\nu}}{\vartheta_{10}^{2\nu}}.$$

II $n \equiv 1 \pmod 2$

$$\vartheta_{01}^{n^2-1}\vartheta_{11}(nu) = \vartheta_{11}(u)\sum_{0,\frac{n^2-1}{2}}^{\nu} a_\nu \vartheta_{11}(u)^{2\nu}\vartheta_{01}(u)^{n^2-1-2\nu}\frac{\vartheta_{00}^{2\nu}}{\vartheta_{10}^{2\nu}}$$

$$\vartheta_{01}^{n^2-1}\vartheta_{10}(nu) = \vartheta_{10}(u)\sum_{0,\frac{n^2-1}{2}}^{\nu} b_\nu \vartheta_{11}(u)^{2\nu}\vartheta_{01}(u)^{n^2-1-2\nu}\frac{\vartheta_{00}^{2\nu}}{\vartheta_{10}^{2\nu}}$$

$$\vartheta_{01}^{n^2-1}\vartheta_{00}(nu) = \vartheta_{00}(u)\sum_{0,\frac{n^2-1}{2}}^{\nu} c_\nu \vartheta_{11}(u)^{2\nu}\vartheta_{01}(u)^{n^2-1-2\nu}\frac{\vartheta_{00}^{2\nu}}{\vartheta_{10}^{2\nu}}$$

$$\vartheta_{01}^{n^2-1}\vartheta_{01}(nu) = \vartheta_{01}(u)\sum_{0,\frac{n^2-1}{2}}^{\nu} d_\nu \vartheta_{11}(u)^{2\nu}\vartheta_{01}(u)^{n^2-1-2\nu}\frac{\vartheta_{00}^{2\nu}}{\vartheta_{10}^{2\nu}}$$

oder indem man die elliptischen Functionen x, y, z (§ 6) einführt:

III. $n \equiv 0 \pmod 2$

$$\frac{\vartheta_{00}\vartheta_{01}^{n^2-1}}{\vartheta_{10}} \frac{\vartheta_{11}(nu)}{\vartheta_{01}(u)^{n^2}} = xyz\sum^{\nu} a_\nu x^{2\nu} = xyzA(x^2, k^2), \qquad a_0 = n$$

$$\frac{\vartheta_{01}^{n^2}}{\vartheta_{10}} \frac{\vartheta_{10}(nu)}{\vartheta_{01}(u)^{n^2}} = \sum^{\nu} b_\nu x^{2\nu} = B(x^2, k^2), \qquad b_0 = 1$$

$$\frac{\vartheta_{01}^{n^2}}{\vartheta_{00}} \frac{\vartheta_{00}(nu)}{\vartheta_{01}(u)^{n^2}} = \sum^{\nu} c_\nu x^{2\nu} = C(x^2, k^2), \qquad c_0 = 1$$

$$\vartheta_{01}^{n^2-1} \frac{\vartheta_{01}(nu)}{\vartheta_{01}(u)^{n^2}} = \sum^{\nu} d_\nu x^{2\nu} = D(x^2, k^2), \qquad d_0 = 1.$$

IV. $n \equiv 1 \pmod 2$

$$\frac{\vartheta_{00}\vartheta_{01}^{n^2-1}}{\vartheta_{10}} \frac{\vartheta_{11}(nu)}{\vartheta_{01}(u)^{n^2}} = x\sum^{\nu} a_\nu x^{2\nu} = xA(x^2, k^2), \qquad a_0 = n$$

$$\frac{\vartheta_{01}^{n^2}}{\vartheta_{10}} \frac{\vartheta_{10}(nu)}{\vartheta_{01}(u)^{n^2}} = y\sum^{\nu} b_\nu x^{2\nu} = yB(x^2, k^2), \qquad b_0 = 1$$

$$\frac{\vartheta_{01}^{n^2}}{\vartheta_{00}} \frac{\vartheta_{00}(nu)}{\vartheta_{01}(u)^{n^2}} = z\sum^{\nu} c_\nu x^{2\nu} = zC(x^2, k^2), \qquad c_0 = 1$$

$$\vartheta_{01}^{n^2-1} \frac{\vartheta_{01}(nu)}{\vartheta_{01}(u)^{n^2}} = \sum^{\nu} d_\nu x^{2\nu} = D(x^2, k^2), \qquad d_0 = 1.$$

Da von den vier Functionen $\vartheta_{11}(nu)$, $\vartheta_{10}(nu)$, $\vartheta_{00}(nu)$, $\vartheta_{01}(nu)$ nicht zwei für denselben Wert von u verschwinden, so sind die vier Functionen A, B, C, D ohne gemeinschaftlichen Teiler. Für die elliptischen Functionen ergeben sich daraus die folgenden Multiplicationsformeln.

$n \equiv 0 \pmod 2$

$$\sin\operatorname{am}(nv) = \frac{xyzA(x^2)}{D(x^2)},$$

$$(1) \qquad \cos\operatorname{am}(nv) = \frac{B(x^2)}{D(x^2)},$$

$$\Delta\operatorname{am}(nv) = \frac{C(x^2)}{D(x^2)},$$

$n \equiv 1 \pmod 2$

$$\sin\operatorname{am}(nv) = \frac{xA(x^2)}{D(x^2)}$$

$$(2) \qquad \cos\operatorname{am}(nv) = \frac{yB(x^2)}{D(x^2)}$$

$$\Delta\operatorname{am}(nv) = \frac{zC(x^2)}{D(x^2)}.$$

Das Additionstheorem liefert zur Berechnung der Functionen A, B, C, D Recursionsformeln, die sich mit Rücksicht auf die in I bis IV angegebenen Werte $A(0)$, $B(0)$, $C(0)$, $D(0)$ leicht ergeben

$$(3)\quad \begin{cases} A_{2n} = 2A_nB_nC_nD_n \\ B_{2n} = B_n^2D_n^2 - x^2y^2z^2A_n^2C_n^2, & n \equiv 0 \pmod 2 \\ \quad = y^2B_n^2D_n^2 - x^2z^2A_n^2C_n^2, & n \equiv 1 \pmod 2 \\ C_{2n} = C_n^2D_n^2 - k^2x^2y^2z^2A_n^2B_n^2, & n \equiv 0 \pmod 2 \\ \quad = z^2C_n^2D_n^2 - k^2x^2y^2A_n^2B_n^2, & n \equiv 1 \pmod 2 \\ D_{2n} = D_n^4 - k^2x^4y^4z^4A_n^4, & n \equiv 0 \pmod 2 \\ \quad = D_n^4 - k^2x^4A_n^4, & n \equiv 1 \pmod 2 \end{cases}$$

$$(4)\quad \begin{cases} A_{2n+1} = y^2z^2A_nD_nB_{n+1}C_{n+1} + A_{n+1}D_{n+1}C_nB_n, & n \equiv 0 \pmod 2 \\ \quad = A_nD_nB_{n+1}C_{n+1} + y^2z^2A_{n+1}D_{n+1}C_nB_n, & n \equiv 1 \pmod 2 \\ B_{2n+1} = D_nD_{n+1}B_nB_{n+1} - x^2z^2A_nA_{n+1}C_nC_{n+1}, \\ C_{2n+1} = C_nC_{n+1}D_nD_{n+1} - k^2x^2y^2A_nA_{n+1}B_nB_{n+1}, \\ D_{2n+1} = D_n^2D_{n+1}^2 - k^2x^4y^2z^2A_n^2A_{n+1}^2. \end{cases}$$

Aus diesen Formeln schliesst man, dass die Coëfficienten a_ν, b_ν, c_ν, d_ν ganze rationale Functionen von k^2 sind mit ganzzahligen Coëfficienten, und zwar höchstens vom Grade ν; denn in den ersten Fällen $n = 1$, $n = 2$ haben diese Eigenschaften statt, und aus (3) und (4) folgen dieselben unter der Voraussetzung dass sie für n und $n + 1$ richtig sind, für $2n$ und $2n + 1$.

Zwischen den Functionen A, B, C, D bestehen die Relationen

$$(5)\quad \begin{aligned} D^2 &= B^2 + x^2y^2z^2A^2 = C^2 + k^2x^2y^2z^2A^2, && n \equiv 0 \pmod 2 \\ D^2 &= x^2A^2 + y^2B^2 \quad = k^2x^2A^2 + z^2C^2, && n \equiv 1 \pmod 2, \end{aligned}$$

ferner wenn n ungerade ist:

$$(6)\qquad \begin{aligned} A(x^2) &= (-1)^{\frac{n-1}{2}}\left(\frac{z}{\sqrt{k'}}\right)^{n^2-1} B\left(\frac{y^2}{z^2}\right) \\ &= (-1)^{\frac{n-1}{2}}\left(\sqrt{\frac{k}{k'}}\,y\right)^{n^2-1} C\left(\frac{z^2}{k^2y^2}\right) \\ &= (-1)^{\frac{n-1}{2}}(\sqrt{k}\,x)^{n^2-1} D\left(\frac{1}{k^2x^2}\right), \end{aligned}$$

wie man nach § 2 (4) findet, wenn man in II u ersetzt durch $u+\frac{1}{2}$, $u+\frac{\omega}{2}$, $u+\frac{1}{2}+\frac{\omega}{2}$.

§ 10. *Teilung der elliptischen Functionen durch 2 und die Potenzen von 2.*

Die Teilungsaufgabe, d. h. die Berechnung von

$$\sin\mathrm{am}\frac{u}{n}, \qquad \cos\mathrm{am}\frac{u}{n}, \qquad \Delta\,\mathrm{am}\frac{u}{n}$$

aus den als bekannt vorausgesetzten Werten von $\sin\mathrm{am}\,u$, $\cos\mathrm{am}\,u$, $\Delta\,\mathrm{am}\,u$, besteht in der Auflösung der Gleichungen (1), (2) § 9 in Beziehung auf x, y, z. Diese Aufgabe erfordert eine andere Behandlung für ein gerades und für ein ungerades n. Wir behandeln zunächst die Teilung durch 2 [1] wofür, wenn

$$x = \sin\mathrm{am}\frac{v}{2}, \qquad y = \cos\mathrm{am}\frac{v}{2}, \qquad z = \Delta\,\mathrm{am}\frac{v}{2}$$

gesetzt wird, sich die Gleichungen ergeben:

$$(1)\qquad \begin{aligned} \sin\mathrm{am}\,v &= \frac{2xyz}{1-k^2x^4} \\ \cos\mathrm{am}\,v &= \frac{y^2-x^2z^2}{1-k^2x^4} \\ \Delta\,\mathrm{am}\,v &= \frac{z^2-k^2x^2y^2}{1-k^2x^4}, \end{aligned}$$

[1] Abel, Oeuvres éd. Sylow I, S. 292.

von denen die beiden letzten Gleichungen zweiten Grades für x^2 sind, die aber nur *eine* gemeinschaftliche Wurzel haben; denn die Wurzeln der ersteren sind

$$\sin\mathrm{am}\frac{v}{2}^2, \qquad \sin\mathrm{am}\left(\frac{v}{2}+K\right)^2$$

die der letzteren

$$\sin\mathrm{am}\frac{v}{2}^2, \qquad \sin\mathrm{am}\left(\frac{v}{2}+K+iK'\right)^2.$$

Man findet nun leicht:

$$\begin{aligned} 1+\cos\mathrm{am}\,v &= \frac{2y^2}{1-k^2x^4}, & 1+\Delta\mathrm{am}\,v &= \frac{2z^2}{1-k^2x^4} \\ 1-\cos\mathrm{am}\,v &= \frac{2x^2z^2}{1-k^2x^4}, & 1-\Delta\mathrm{am}\,v &= \frac{2k^2x^2y^2}{1-k^2x^4} \end{aligned} \tag{2}$$

und daraus

$$\begin{aligned} x &= \sqrt{\frac{1-\cos\mathrm{am}\,v}{1+\Delta\mathrm{am}\,v}} & &= \frac{1}{k}\sqrt{\frac{1-\Delta\mathrm{am}\,v}{1+\cos\mathrm{am}\,v}} \\ y &= \sqrt{\frac{\Delta\mathrm{am}\,v+\cos\mathrm{am}\,v}{1+\Delta\mathrm{am}\,v}}, & z &= \sqrt{\frac{\Delta\mathrm{am}\,v+\cos\mathrm{am}\,v}{1+\cos\mathrm{am}\,v}}. \end{aligned}$$

Jedem dieser drei Wurzelzeichen kann das doppelte Vorzeichen beigelegt werden; aber es besteht zwischen denselben nach der ersten Gleichung (1) noch eine Relation, durch welche eines der drei Zeichen durch die beiden andern bestimmt ist. Die so erhaltenen vier Wertsysteme haben die Bedeutung:

$\sin\mathrm{am}\frac{v}{2}$,	$\cos\mathrm{am}\frac{v}{2}$,	$\Delta\mathrm{am}\frac{v}{2}$
$\sin\mathrm{am}\left(\frac{v}{2}+2K\right)$,	$\cos\mathrm{am}\left(\frac{v}{2}+2K\right)$,	$\Delta\mathrm{am}\left(\frac{v}{2}+2K\right)$
$\sin\mathrm{am}\left(\frac{v}{2}+2iK'\right)$,	$\cos\mathrm{am}\left(\frac{v}{2}+2iK'\right)$,	$\Delta\mathrm{am}\left(\frac{v}{2}+2iK'\right)$
$\sin\mathrm{am}\left(\frac{v}{2}+2K+2iK'\right)$,	$\cos\mathrm{am}\left(\frac{v}{2}+2K+2iK'\right)$,	$\Delta\mathrm{am}\left(\frac{v}{2}+2K+2iK'\right)$.

Es ergiebt sich hieraus, dass man die Teilungsaufgabe für beliebige Potenzen von 2 durch eine *Kette von Quadratwurzeln* auflösen kann, und wenn man daher die Teilung durch ungerade Zahlen als gelöst voraussetzt, so erfordert die Teilung durch beliebige gerade Zahlen nur noch das Ausziehen von Quadratwurzeln. Wir beschäftigen uns daher im Folgenden nur noch mit der Teilung durch ungerade Zahlen.

§ 11. *Teilung durch eine ungerade Zahl.*

Setzt man

$$x = \sin\mathrm{am}\frac{v}{n}, \qquad y = \cos\mathrm{am}\frac{v}{n}, \qquad z = \Delta\mathrm{am}\frac{v}{n},$$

so ergeben sich zur Bestimmung dieser Grössen aus § 9 (2) die Gleichungen:

$$\begin{aligned} D(x^2)\sin\mathrm{am}\,v - xA(x^2) &= 0 \\ D(x^2)\cos\mathrm{am}\,v - yB(x^2) &= 0 \\ D(x^2)\ \Delta\mathrm{am}\,v - zC(x^2) &= 0, \end{aligned} \tag{2}$$

deren jede in Bezug auf die Unbekannte x, resp. y, z vom Grade n^2 ist. Durch die letzten dieser Gleichungen kann aber, *falls man nicht nur* $\sin\mathrm{am}\,v$ *sondern auch* $\cos\mathrm{am}\,v$ *und* $\Delta\,\mathrm{am}\,v$ *zu den gegebenen Grössen rechnet,* y, z *rational durch die Unbekannte* x *ausgedrückt werden,* [1] so dass man für die drei Unbekannten x, y, z nur n^2 verschiedene Wertsysteme erhält, welche die folgende Bedeutung haben:

$$\begin{aligned} x_{\mu,\mu'} &= \sin\mathrm{am}\left(\frac{v}{n} + \frac{4\mu K + 4\mu' iK'}{n}\right) \\ y_{\mu,\mu'} &= \cos\mathrm{am}\left(\frac{v}{n} + \frac{4\mu K + 4\mu' iK'}{n}\right) \\ z_{\mu,\mu'} &= \Delta\mathrm{am}\left(\frac{v}{n} + \frac{4\mu K + 4\mu' iK'}{n}\right), \end{aligned} \tag{3}$$

[1] Auf der Benutzung dieses Umstandes beruht der Fortschritt, den JACOBI gegen über der ersten ABEL'schen Lösung des Teilungsproblems gemacht hat. ABEL, Oeuvres éd. SYLOW I, S. 294. JACOBI, gesammelte Werke, S. 243, 403.

worin μ, μ' je ein vollständiges Restsystem (mod n) durchlaufen. Rechnet man nun die Grössen

$$(4) \qquad \sin\mathrm{am}\frac{4\mu K + 4\mu' iK'}{n}, \quad \cos\mathrm{am}\frac{4\mu K + 4\mu' iK'}{n}, \quad \Delta\,\mathrm{am}\frac{4\mu K + 4\mu' iK'}{n},$$

deren Bestimmung Gegenstand des nächsten Paragraphen sein wird, zu den bekannten Grössen, so kann man in Folge des Additionstheorems jede der Wurzeln $x_{\mu,\mu'}$ durch jede andere *rational* ausdrücken. Wenn aber

$$x_{\mu,\mu'} = F_{\mu,\mu'}(x_{0,0})$$

ist, so ergiebt sich aus der Bedeutung der Wurzeln (3)

$$x_{\mu+\nu,\mu'+\nu'} = F_{\mu,\mu'}(x_{\nu,\nu'}) = F_{\mu+\nu,\mu'+\nu'}(x_{0,0}),$$

und also

$$F_{\mu,\mu'}F_{\nu,\nu'}(x) = F_{\nu,\nu'}F_{\mu,\mu'}(x).$$

Die Gleichung vom Grade n^2, deren Wurzeln die $x_{\mu,\mu'}$ sind, ist also (nach Adjunction von $\sin\mathrm{am}\,v$, $\cos\mathrm{am}\,v$, $\Delta\,\mathrm{am}\,v$ und der Grössen (4)) eine ABEL'sche Gleichung und daher *algebraisch auflösbar.* (ABEL, Oeuvres éd. SYLOW. I, S. 132.)

§ 12. *Die Teilung der Perioden.*

Die noch zu lösende Aufgabe besteht nun in der algebraischen Bestimmung der Grössen

$$(1) \qquad x_{\mu,\mu'} = \sin\mathrm{am}\frac{4\mu K + 4\mu' iK'}{n}$$

oder in der *Teilung der Perioden.* Diese Grössen sind die Wurzeln der Gleichung

$$(2) \qquad xA(x^2) = 0$$

und die beiden anderen

$$y_{\mu,\mu'} = \cos\mathrm{am}\frac{4\mu K + 4\mu' iK'}{n}, \qquad z_{\mu,\mu'} = \Delta\,\mathrm{am}\frac{4\mu K + 4\mu' iK'}{n}$$

können durch diese rational ausgedrückt werden durch die Gleichungen

$$(3) \qquad y = \frac{D(x^2)}{B(x^2)}, \qquad z = \frac{D(x^2)}{C(x^2)}.$$

Aus den Wurzeln der Gleichung $A(x^2) = 0$ lassen sich ferner die Wurzeln der Gleichungen $B(x^2) = 0$, $C(x^2) = 0$, $D(x^2) = 0$ nach den Formeln (6) § 9 rational bestimmen, deren Bedeutung ist:

$$\sin\mathrm{am}\frac{(4\mu+1)K + 4\mu' iK'}{n}, \qquad \sin\mathrm{am}\frac{(4\mu+1)K + (4\mu'+1)iK'}{n}$$

$$\sin\mathrm{am}\frac{4\mu K + (4\mu'+1)iK'}{n},$$

und hiernach sind durch Auflösung der Gleichung $A(x^2) = 0$, welcher alle Functionen von der Form

$$x^2 = \left(\sin\mathrm{am}\frac{2\mu K + 2\mu' iK'}{n}\right)^2$$

genügen, die sämmtlichen Grössen

$$\left(\sin\mathrm{am}\frac{\mu K + \mu' iK'}{n}\right)^2$$

bestimmt, wenn μ, μ' irgend ganze Zahlen sind.

§ 13. *Die Galois'sche Gruppe und die irreductibeln Factoren der Teilungsgleichung.*

Die Grössen $x_{\mu,\mu'}$ sind algebraische Functionen von k^2, welche mit Ausnahme der Werte 0, 1 für alle endlichen Werte von k^2 endlich und stetig sind. Durch einen positiven Umlauf von k^2 um einen dieser singulären Punkte geht nach § 7

$$x_{\mu,\mu'} \quad \text{über in} \quad x_{\mu,2\mu+\mu'} \quad \text{resp. in} \quad x_{\mu+2\mu',\mu'}.$$

Also geht beim Durchlaufen irgend eines Kreisweges

$$x_{\mu,\mu'} \quad \text{in} \quad x_{\alpha\mu+2\beta\mu',\,2\gamma\mu+\delta\mu'}, \qquad \alpha\delta - 4\beta\gamma = 1$$

über, oder auch, da die Zahlen μ, μ' nur nach dem Modul n bestimmt sind

$$x_{\mu,\mu'} \quad \text{in} \quad x_{\alpha\mu+\beta\mu',\,\gamma\mu+\delta\mu'}, \qquad \alpha\delta - \beta\gamma \equiv 1 \pmod{n},$$

und es lässt sich der Weg so bestimmen, dass die vier Zahlen α, β, γ, δ irgend welche der Bedingung

$$\alpha\delta - \beta\gamma \equiv 1 \pmod{n} \tag{1}$$

genügende Werte haben.

Wenn daher eine rationale Function von k^2 und den Wurzeln $x_{\mu,\mu'}$ die Eigenschaft hat, durch alle Substitutionen

$$\begin{pmatrix} \mu & , & \mu' \\ \alpha\mu + \beta\mu', & & \gamma\mu + \delta\mu' \end{pmatrix}, \tag{2}$$

die wieder mit

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$$

bezeichnet sein sollen, ungeändert zu bleiben, so ist sie (nach § 7) rational durch k^2 ausdrückbar, und umgekehrt hat jede rational durch k^2 ausdrückbare Function diese Eigenschaft. *Der Inbegriff der Substitutionen* (2) *bildet also die* Galois'*sche Gruppe der Teilungsgleichung* $A(x^2) = 0$.

Es ist dies aber nur die sogenannte *Monodromie-Gruppe*, d. h. es ist nur dann die Gruppe der Gleichung, wenn als Rationalitätsbereich der Inbegriff *aller* rationalen Functionen von k^2 betrachtet wird. Es bleiben aber noch die beiden Fragen zu beantworten:

1. Welche Zahlenirrationalitäten müssen adjungirt werden, damit die Monodromiegruppe die wirkliche Gruppe der Gleichung sei.

2. Welches ist die Gruppe der Gleichung, wenn überhaupt irrationale Zahlen nicht adjungirt werden.

Zur Beantwortung dieser beiden Fragen bemerken wir zunächst Folgendes:

1°. Nach dem Additions- und Multiplicationstheorem kann man alle $x_{\mu,\mu'}$ ausdrücken durch die beiden

$$x_{1,0} = \operatorname{sin\,am}\frac{4K}{n}, \qquad x_{0,1} = \operatorname{sin\,am}\frac{4iK'}{n}$$

und zwar rational durch k^2 und rationale Zahlen. Wenn man in diesen Ausdrücken $x_{1,0}$ durch $x_{\lambda,0}$, d. h. K durch λK ersetzt, so geht $x_{\mu,\mu'}$ über in $x_{\lambda\mu,\mu'}$.

2°. Aus den Entwickelungen

$$\frac{1}{2}\sqrt{k} = q^{\frac{1}{4}}\frac{1 + q^2 + q^6 + \ldots}{1 + 2q + 2q^4 + \ldots}$$

$$\sin\mathrm{am}\frac{4K}{n} = \frac{1}{i\sqrt{k}}\frac{\sum^{\nu}(-1)^{\nu}q^{\left(\nu+\frac{1}{2}\right)^2}e^{\frac{2\pi i}{n}(2\nu+1)}}{\sum^{\nu}(-1)^{\nu}q^{\nu^2}e^{\frac{4\pi i\nu}{n}}}$$

$$\sin\mathrm{am}\frac{4\lambda K}{n} = \frac{1}{i\sqrt{k}}\frac{\sum^{\nu}(-1)^{\nu}q^{\left(\nu+\frac{1}{2}\right)^2}e^{\frac{2\lambda\pi i}{n}(2\nu+1)}}{\sum^{\nu}(-1)^{\nu}q^{\nu^2}e^{\frac{4\lambda\pi i\nu}{n}}}$$

$$\sin\mathrm{am}\frac{4iK'}{n} = \frac{1}{i\sqrt{k}}\frac{\sum^{\nu}(-1)^{\nu}q^{\left(\nu+\frac{1}{2}\right)^2+\frac{4(\nu+\frac{1}{2})}{n}}}{\sum^{\nu}(-1)^{\nu}q^{\nu^2+\frac{4\nu}{n}}}$$

folgt zunächst, dass q in eine Reihe nach steigenden Potenzen von

$$\frac{k^2}{16}$$

entwickelbar ist, deren Coëfficienten *ganze Zahlen* sind, und deren erstes Glied $k^2:16$ den Coefficienten 1 hat. Daraus folgt dann weiter, dass

$$i\sin\mathrm{am}\frac{4iK'}{n}$$

sich in eine Reihe nach steigenden Potenzen von

$$\sqrt[n]{\frac{k^2}{16}}$$

mit *rationalen* Zahlencoëfficienten entwickeln lässt. Endlich lässt sich

$$i\sin\mathrm{am}\frac{4K}{n}$$

in eine Reihe nach steigenden Potenzen von $k^2 : 16$ entwickeln, deren Coëfficienten ausser rationalen Zahlen noch die n^{te} Einheitswurzel

$$\rho^{\frac{2\pi i}{n}}$$

enthalten.

3. Wenn nun eine rationale Function der Wurzeln $x_{\mu,\mu'}$, deren Coëfficienten rationale Functionen von k^2 und rationalen Zahlen sind, einer *rationalen Function* r von k^2 gleich ist, so genügt r (als Function der Wurzeln $x_{\mu,\mu'}$) jedenfalls einer algebraischen Gleichung, welche rational von k^2 und rationalen Zahlen abhängt, *und kann daher durch Multiplication mit einer ganzen rationalen Function von k^2 mit rationalen Zahlcoëfficienten in eine ganze Function von k^2 verwandelt werden.* Wir können also auch annehmen, dass r bereits eine *ganze* rationale Function von k^2 sei. Mit Anwendung von 1. ergiebt sich also daraus eine Gleichung von der Form

$$\Phi\left(k^2, \operatorname{sin\,am}\frac{4K}{n}, \operatorname{sin\,am}\frac{4iK'}{n}\right) = r, \tag{3}$$

worin Φ eine rationale Function seiner Argumente mit rationalen Zahlcoëfficienten, r eine ganze rationale Function von k^2 mit vorläufig noch unbestimmten Zahlcoëfficienten bedeutet. Da nun die Substitution

$$\begin{pmatrix} -1, & 0 \\ 0, & -1 \end{pmatrix}$$

zur Monodromiegruppe gehört, so bleibt die Gleichung (3) richtig, wenn in derselben die Vorzeichen von

$$\operatorname{sin\,am}\frac{4K}{n}, \qquad \operatorname{sin\,am}\frac{4iK'}{n}$$

zugleich geändert werden; und daher zerfällt die Gleichung (3) in zwei andere

$$\Phi_1 = r, \qquad \Phi_2 = 0, \tag{4}$$

so dass die Summen der Exponenten von

$$\operatorname{sin\,am}\frac{4K}{n}, \qquad \operatorname{sin\,am}\frac{4iK'}{n}$$

in der ersten gerade, in der zweiten ungerade Zahlen sind.

Nun lässt sich aber in Folge von (2) die Function Φ_1 in eine Potenzreihe entwickeln nach steigenden Potenzen von $\sqrt[n]{k^2 : 16}$, deren Coëfficienten ausser rationalen Zahlen nur n^{te} Einheitswurzeln enthalten, und daher kann auch die Function r keine anderen irrationalen Zahlen enthalten. Derselbe Schluss ist auch dann noch anwendbar, wenn die Function Φ in ihren Coëfficienten n^{te} Einheitswurzeln enthält. Damit ist die erste der oben gestellten Fragen dahin zu beantworten:

Die Monodromiegruppe ist die wahre Gruppe der Gleichung, wenn n^{te} Einheitswurzeln adjungirt werden.

4. Um die zweite Frage zu beantworten, müssen wir in (4) r mit *rationalen Coëfficienten* behaftet annehmen. Unter dieser Voraussetzung bleiben aber die beiden Gleichungen (4) bestehen, wenn die Einheitswurzel $e^{\frac{2\pi i}{n}}$, die in den Entwickelungen vorkommt, durch eine beliebige andere $e^{\frac{2\pi i\lambda}{n}}$ ersetzt wird, wenn wir λ zu n relativ prim voraussetzen. (Wegen der Irreductibilität der Gleichung, welcher die primitiven n^{ten} Einheitswurzeln genügen.) Dies bedeutet aber nichts anderes, als dass in allen rationalen Gleichungen zwischen den Wurzeln $x_{\mu,\mu'}$ die Substitution

$$\begin{pmatrix} \lambda, & 0 \\ 0, & 1 \end{pmatrix}$$

ausgeführt werden kann. Da man aber aus dieser Substitution und der Substitution (2) alle Substitutionen von der Form

$$\begin{pmatrix} \mu & , & \mu' \\ a\mu + b\mu', & c\mu + d\mu' \end{pmatrix} = \begin{pmatrix} a, & b \\ c, & d \end{pmatrix}, \tag{5}$$

in welchen $ad - bc$ zu n relativ prim ist, (würde $ad - bc$ einen Teiler mit n gemein haben, so würden die Ausdrucke $a\mu + b\mu'$, $c\mu + d\mu'$ nicht im Stande sein, alle Zahlenpaare μ, μ' (mod n) darzustellen und (5) würde nicht die Bedeutung einer Substitution haben) zusammensetzen kann, so folgt, *dass die Galois'sche Gruppe der Teilungsgleichung alle Substitutionen von der Form* (5) *enthält.*

5. Es bleibt noch zu zeigen, dass die Galois'sche Gruppe der Teilungsgleichung keine anderen als die durch (5) dargestellten Substitutionen enthält. Nach dem Additions- und Multiplicationstheorem ist, wenn

f und φ rationale Functionen bedeuten (welche k^2 und rationale Zahlen enthalten)

$$x_{\mu+\nu,\,\mu'+\nu'} = f(x_{\mu,\mu'},\ x_{\nu,\nu'}) \tag{6}$$

$$x_{m\mu,\,m\mu'} = \varphi(x_{\mu,\mu'}). \tag{7}$$

Auf diese Gleichungen kann man jede Substitution der Gruppe anwenden. Wenn nun durch irgend eine dieser Substitutionen (1, 0) in (a, c); (0, 1) in (b, d) übergeht, dann geht wegen (7) $(\mu, 0)$ in $(\mu a, \mu c)$, $(0, \mu')$ in $(\mu' b, \mu' d)$ über, und wegen (6) (μ, μ') in $(a\mu + b\mu', c\mu + d\mu')$; also sind alle Substitutionen der Gruppe in der Form (5) enthalten, *und der Inbegriff aller Substitutionen* (5) *ist die Galois'sche Gruppe der Teilungsgleichung.* (1)

6. Durch die Substitutionen (5) bleibt der grösste gemeinschaftliche Teiler der beiden Indices μ, μ' und n stets erhalten und daraus folgt, was auch leicht direct einzusehen ist, dass die Teilungsgleichung in rationale Factoren zerfällt, in der Weise, dass alle diejenigen Wurzeln $x_{\mu,\mu'}$, in welchen μ, μ' einen und denselben grössten gemeinschaftlichen Teiler mit n haben, einer besonderen rationalen Gleichung genügen. Diejenige unter diesen Gleichungen, für welche μ, μ', n ohne gemeinsamen Teiler sind, wollen wir die *eigentliche Teilungsgleichung* für den Divisor n nennen. Die anderen $x_{\mu,\mu'}$ sind zugleich Wurzeln von niedrigeren Teilungsgleichungen. Um den Grad der eigentlichen Teilungsgleichung zu bestimmen, hat man nur die Anzahl derjenigen Paare nach n incongruenter Zahlen μ, μ' zu bestimmen, für welche n, μ, μ' ohne gemeinsamen Teiler sind. Bezeichnen wir diesen Grad für den Augenblick mit $\chi(n)$, so ergiebt sich zunächst, wenn m, n relativ prim sind:

$$\chi(mn) = \chi(m)\chi(n),$$

(1) Die Monodromiegruppe der Teilungsgleichung ist von C. JORDAN untersucht, welcher auch den in No. 5 behandelten Teil der Frage, nach der algebraischen Gruppe zuerst erledigt hat. (*Traité des substitutions*, S. 342.) Die vollständige GALOIS sche Gruppe der Teilungsgleichung ist zuerst von SYLOW auf einem von dem unsrigen verschiedenen Weg bestimmt worden. (Forhandlinger i Videnskabs-Selskabet i Christiania, 1871.) Derselben Frage ist endlich eine Arbeit von KRONECKER in den Monatsberichten der Berliner Akademie vom 19 Juni 1875 gewidmet.

und wenn m eine Potenz einer Primzahl p ist:

$$\chi(m) = m^2\left(1 - \frac{1}{p^2}\right),$$

woraus allgemein folgt:

$$\chi(n) = n^2 \prod\left(1 - \frac{1}{p^2}\right) = \varphi(n)\psi(n), \tag{8}$$

wenn

$$\varphi(n) = n \prod\left(1 - \frac{1}{p}\right) \tag{9}$$

die Anzahl der Zahlclassen (mod n) bedeutet welche zu n teilerfremde Zahlen enthalten, und

$$\psi(n) = n \prod\left(1 + \frac{1}{p}\right) \tag{10}$$

ist, worin p jedesmal die sämmtlichen in n enthaltenen Primzahlen durchläuft.

7. Die Galois'sche Gruppe der eigentlichen Teilungsgleichung ist genau dieselbe wie die oben bestimmte der uneigentlichen; denn sie besteht aus denjenigen Substitutionen der letzteren, welche (μ, μ') verändern, wenn μ, μ', n ohne gemeinschaftlichen Teiler sind. Dies thut aber jede dieser Substitutionen (mit Ausnahme der identischen); denn die Substitution

$$\begin{pmatrix} a, & b \\ c, & d \end{pmatrix}$$

verändert (1, 0), (0, 1) in (a, c), (b, d).

Die Anzahl der Substitutionen dieser Gruppe ist

$$n\varphi(n)^2\psi(n).$$

8. *Die eigentliche Teilungsgleichung ist irreductibel in dem Gebiet der rationalen Functionen von k^2.* Denn man kann selbst in der Monodromiegruppe eine Substitution finden, welche eine beliebige Wurzel (μ, μ') der eigentlichen Teilungsgleichung in eine beliebige andere (ν, ν') überführt.

Denn wenn μ, μ' und ebenso ν, ν' ohne gemeinsamen Teiler mit n gegeben sind, so kann man immer die Zahlen α, β, γ, δ den Congruenzen

$$\alpha\mu + \beta\mu' \equiv \nu$$

$$\gamma\mu + \delta\mu' \equiv \nu' \qquad (\mathrm{mod}\ n)$$

$$\alpha\delta - \beta\gamma \equiv 1$$

entsprechend bestimmen. (Es genügt, $(\mu, \mu') = (1, 0)$ anzunehmen, wobei die Möglichkeit dieser Congruenzen sofort in die Augen springt.)

§ 14. *Zurückführung der Teilungsgleichung auf Transformationsgleichungen.*

Die Wurzeln der eigentlichen Teilungsgleichung lassen sich in folgender Weise in *Reihen* anordnen. Man wähle nach Belieben eine der Wurzeln

$$x_{\mu_1, \mu_1'} = \sin\mathrm{am}\left(\frac{4\mu_1 K + 4\mu_1' iK'}{n}\right) = \sin\mathrm{am}\, \Omega_1.$$

Unter den Wurzeln kommen auch die sämmtlichen $\varphi(n)$ Grössen

$$(\mathrm{R}_1) \qquad \sin\mathrm{am}\,(s\Omega_1)$$

vor, welche, wenn s ein vollständiges System incongruenter zu n teilerfremder Zahlen durchläuft, alle von einander verschieden sind. Das System (R_1) wollen wir die *erste Reihe* der Wurzeln nennen. Ist nun $\sin\mathrm{am}\,\Omega_2$ in (R_1) nicht enthalten, so bilden die $\varphi(n)$ Grössen

$$(\mathrm{R}_2) \qquad \sin\mathrm{am}\,(s\Omega_2),$$

welche sowohl von einander als von den Grössen der Reihe (R_1) verschieden sind, eine zweite Reihe; und auf diese Weise kann man fortfahren, bis die sämmtlichen $\varphi(n)\psi(n)$ Wurzeln in $\psi(n)$ Reihen von je $\varphi(n)$ Gliedern verteilt sind.

Diese Einteilung in Reihen ist von der Willkürlichkeit in der An-

nahme über Ω_1, Ω_2, ... unabhängig; denn es ist die notwendige und hinreichende Bedingung dafür, dass zwei Wurzeln

$$\sin\mathrm{am}\frac{4\mu K + 4\mu' iK'}{n}, \qquad \sin\mathrm{am}\frac{4\nu K + 4\nu' iK'}{n}$$

derselben Reihe angehören

$$\mu\nu' - \nu\mu' \equiv 0 \pmod{n}; \tag{1}$$

denn *erstens* wenn $\nu \equiv s\mu$, $\nu' \equiv s\mu' \pmod{n}$, so ist die Bedingung (1) erfüllt; und *zweitens* da μ, μ' keinen Teiler mit n gemein haben, so lassen sich ganze Zahlen α, β so bestimmen, dass

$$\alpha\mu - \beta\mu' \equiv 1 \pmod{n}$$

und daraus folgt mittels (1)

$$\nu \equiv (\nu\alpha - \nu'\beta)\mu, \qquad \nu' \equiv (\nu\alpha - \nu'\beta)\mu' \pmod{n}.$$

Die Congruenz (1) bleibt aber erhalten, wenn auf die beiden Wurzeln (μ, μ') und (ν, ν') gleichzeitig eine lineare Substitution angewandt wird, so dass die *Reihen nicht verändert sondern nur unter einander vertauscht werden durch die Substitutionen der Gruppe der Teilungsgleichung.*

Nach dem Multiplicationstheorem lässt sich jede Wurzel der Teilungsgleichung rational (in Bezug auf k^2 und rationale Zahlen) durch jede andere derselben Reihe ausdrücken. Es sei nämlich

$$\sin\mathrm{am}(sv) = f_s(\sin\mathrm{am}\, v); \tag{2}$$

dann ergiebt sich, wenn $\sin\mathrm{am}(s\Omega)$ die Wurzeln einer Reihe sind:

$$\sin\mathrm{am}(ss'\Omega) = f_s f_{s'}(\sin\mathrm{am}\,\Omega) = f_{s'} f_s(\sin\mathrm{am}\,\Omega), \tag{3}$$

woraus man mit Hülfe des schon oben benutzten ABEL'schen Satzes schliesst:

Wenn man die symmetrischen Functionen der Wurzeln einer Reihe als bekannt voraussetzt, so sind die Wurzeln dieser Reihe selbst durch Wurzelziehen zu bestimmen.

Die symmetrischen Functionen der Wurzeln *einer Reihe* lassen sich rational darstellen durch *eine* dieser Wurzeln vermittelst eines Ausdrucks,

der sich nicht ändert, wenn diese eine Wurzel durch eine beliebige andere derselben Reihe ersetzt wird. Jeder solche Ausdruck hat daher nur $\psi(n)$ verschiedene Werte und ist also die Wurzel einer rationalen Gleichung vom Grade

$$\psi(n) = \nu,$$

welche wir eine zum Transformationsgrad n (oder kurz zu n) gehörige *Transformationsgleichung* nennen wollen.

Jede Transformationsgleichung ist entweder irreductibel, oder sie ist eine Potenz einer irreductibeln Gleichung; denn da die Gruppe der Teilungsgleichung transitiv ist, so giebt es in derselben auch Substitutionen, welche die Wurzeln einer Reihe in die Wurzeln einer beliebigen anderen Reihe, und also eine Wurzel einer Transformationsgleichung in eine beliebige andere überführen. Sind also mehrere Wurzeln einer Transformationsgleichung einander gleich, so zerfallen die sämmtlichen Wurzeln derselben in Gruppen von gleich vielen unter einander gleichen. Sind aber die Wurzeln einer Transformationsgleichung von einander verschieden, so erhält man die GALOIS'sche Gruppe derselben, indem man die Substitutionen der Gruppe der Teilungsgleichung anwendet; diese Gruppe ist aber nach dem eben Bemerkten auch transitiv, und *folglich die Transformationsgleichung irreductibel.*

(Diese Sätze bleiben bestehen, wenn man die Gruppe der Teilungsgleichung auf die Monodromiegruppe beschränkt, d. h. wenn man den Inbegriff *aller* rationalen Functionen von k^2 als Rationalitätsbereich betrachtet.)

Durch die Wurzeln einer beliebigen irreductibeln Transformationsgleichung sind die entsprechenden Wurzeln aller Transformationsgleichungen rational darstellbar.

Sind nämlich $\pi_1, \pi_2, \ldots, \pi_\nu$ die Wurzeln einer irreductibeln, Ψ_1, $\Psi_2, \ldots, \Psi_\nu$ die einer beliebigen Transformationsgleichung, so gehören die Summen

$$(4)\qquad \begin{aligned} &\Psi_1 + \Psi_2 + \cdots + \Psi_\nu = a_0 \\ &\Psi_1\pi_1 + \Psi_2\pi_2 + \cdots + \Psi_\nu\pi_\nu = a_1 \\ &\cdots\cdots\cdots \\ &\Psi_1\pi_1^{\nu-1} + \Psi_2\pi_2^{\nu-1} + \cdots + \Psi_\nu\pi_\nu^{\nu-1} = a_{\nu-1} \end{aligned}$$

zum Rationalitätsbereich. Setzt man alsc

$$\Phi(\pi) = (\pi - \pi_1)(\pi - \pi_2) \ldots (\pi - \pi_\nu)$$

$$\frac{\Phi(\pi)}{\pi - \pi_1} = \Phi_0(\pi_1) + \pi\Phi_1(\pi_1) + \ldots + \pi^{\nu-1}\Phi_{\nu-1}(\pi_1),$$

so folgt:

$$(5) \qquad \Psi_1\Psi'(\pi_1) = a_0\Phi_0(\pi_1) + a_1\Phi_1(\pi_1) + \ldots + a_{\nu-1}\Phi_{\nu-1}(\pi_1),$$

worin $\Psi'(\pi_1)$ von Null verschieden ist.

§ 15. *Besondere Transformationsgleichungen.*

Die einfachsten Functionen, welche zur Bildung von Transformationsgleichungen benutzt werden können, sind, wenn Φ eine rationale Function bedeutet, Producte von der Form

$$(1) \qquad \prod_{1,\,n-1} \Phi(\sin\mathrm{am}\, s\Omega_t).\,(^1)$$

Diese Function bleibt offenbar ungeändert, wenn s statt der Werte $1, 2, \ldots, n-1$ ein anderes Restsystem $(\mathrm{mod}\, n)$ durchläuft, und also auch wenn Ω_t durch $h\Omega_t$ ersetzt wird, falls h zu n teilerfremd ist. Die Functionen $\sin\mathrm{am}\, s\Omega_t$ sind aber paarweise gleich und entgegengesetzt, und wenn s die Zahlen $1, 2, 3, \ldots, \frac{1}{2}(n-1)$ durchläuft, so haben die Zahlen sh, vom Vorzeichen abgesehen, dieselben Zahlen als absolut kleinste Reste. *Wenn daher $\Phi(x)$ eine gerade Function von x ist, so ist auch das Product*

$$(2) \qquad \prod_{1,\,\frac{n-1}{2}}^{s} \Phi(\sin\mathrm{am}\, s\Omega_t)$$

Wurzel einer Transformationsgleichung.

---

(1) Functionen dieser Art sind auch dann Wurzeln von Transformationsgleichungen, wenn s nur die zu n teilerfremden Zahlen der Reihe 1 bis $n-1$ durchläuft. Solche Transformationsgleichungen sind bis jetzt noch wenig oder nicht untersucht.

Ist aber $\Phi(x)$ eine ungerade Function und

$$\Pi(\Omega_t) = \prod_{1,\frac{n-1}{2}}^{s} \Phi(\sin\mathrm{am}\, s\Omega_t), \tag{3}$$

so ist in Folge eines zahlentheoretischen Satzes

$$\Pi(h\Omega_t) = \left(\frac{h}{n}\right)\Pi(\Omega_t)\,(^1); \tag{4}$$

also bleibt die Function $\Pi(\Omega_t)$ nicht ungeändert, sondern kann ihr Vorzeichen ändern, wenn die Wurzel $\sin\mathrm{am}\,\Omega_t$ durch eine andere Wurzel derselben Reihe ersetzt wird. Diese Vorzeichenänderung ist nur dann (für alle Werte von h) ausgeschlossen, wenn n *eine Quadratzahl* ist, und unter dieser Voraussetzung, aber auch nur unter dieser, ist auch diese Function Wurzel einer Transformationsgleichung. In anderen Fällen gilt dasselbe erst von dem Quadrat dieser Function.

Wir wollen ins Besondere die folgenden Functionen betrachten:

$$\prod_{1,\frac{n-1}{2}}^{s} \frac{\Delta\,\mathrm{am}(s\Omega)^2}{\cos\mathrm{am}(s\Omega)}, \qquad \prod_{1,\frac{n-1}{2}}^{s} \frac{\cos\mathrm{am}(s\Omega)^2}{\Delta\,\mathrm{am}(s\Omega)}, \qquad \prod_{1,\frac{n-1}{2}}^{s} \frac{1}{\Delta\,\mathrm{am}(s\Omega)\cos\mathrm{am}(s\Omega)},$$

$$(kk')^{\frac{n-1}{2}} \prod_{1,\frac{n-1}{2}}^{s} \frac{\sin\mathrm{am}\,(s\Omega)^2}{\cos\mathrm{am}(s\Omega)\,\Delta\,\mathrm{am}(s\Omega)}, \tag{5}$$

die nach § 12 in der Form (2) darstellbar sind, von welchen die drei

---

(1) Vgl. über diesen Satz: SCHERING und KRONECKER Monatsberichte der Berliner Akademie v. 22ten Juni 1876, ferner den ganz elementaren Beweis von SCHERING in den Acta mathematica I. Der Satz selbst lautet: Sind h, n relative Primzahlen, die letztere ungerade, und ist μ die Anzahl derjenigen unter den Zahlen

$$h,\ 2h,\ 3h,\ \ldots,\ \frac{n-1}{2}h$$

deren absolut kleinster Rest (mod n) negativ ist, so ist

$$(-1)^{\mu} = \left(\frac{h}{n}\right).$$

ersten allgemein, die letzte falls n eine Quadratzahl ist (sonst deren Quadrat), Wurzeln von Transformationsgleichungen sind.

Nimmt man, was erlaubt ist, in

$$\Omega = \frac{4\mu K + 4\mu' iK'}{n}$$

μ, μ' nicht nur ohne gemeinschaftlichen Teiler mit n, sondern überhaupt relativ prim an, und ersetzt die elliptischen Functionen durch ihre Ausdrücke in den ϑ-Functionen, so kann man die Formeln (25) § 5 anwenden, und erhält für die vier Functionen (5) die Ausdrücke:

$$(6)\quad (-1)^{\frac{n^2-1}{8}} 2^{\frac{n-1}{2}} P_{00}^3,\quad (-1)^{\frac{n^2-1}{8}} 2^{\frac{n-1}{2}} P_{10}^3,\quad (-1)^{\frac{n^2-1}{8}} 2^{\frac{n-1}{2}} P_{01}^3,\quad (-1)^{\frac{n^2-1}{8}} P_{11}^3$$

wenn zur Abkürzung gesetzt ist:

$$(7)\qquad \tilde{\omega} = \frac{\mu + \mu'\omega}{n}$$

$$(8)\qquad \begin{aligned}
P_{00}\vartheta_{00}^{\frac{n-1}{2}} &= e^{\frac{\pi i}{6}\mu'(\mu+\mu'\omega)\frac{n^2-1}{n}} \prod_{1,\frac{n-1}{2}}^{s} \vartheta_{00}(2s\tilde{\omega}) \\
P_{10}\vartheta_{10}^{\frac{n-1}{2}} &= e^{\frac{\pi i}{6}\mu'(\mu+\mu'\omega)\frac{n^2-1}{n}} \prod_{1,\frac{n-1}{2}}^{s} \vartheta_{10}(2s\tilde{\omega}) \\
P_{01}\vartheta_{01}^{\frac{n-1}{2}} &= e^{\frac{\pi i}{6}\mu'(\mu+\mu'\omega)\frac{n^2-1}{n}} \prod_{1,\frac{n-1}{2}}^{s} \vartheta_{01}(2s\tilde{\omega}) \\
P_{11}\eta(\omega)^{\frac{n-1}{2}} &= e^{\frac{\pi i}{6}\mu'(\mu+\mu'\omega)\frac{n^2-1}{n}} \prod_{1,\frac{n-1}{2}}^{s} \vartheta_{11}(2s\tilde{\omega}),
\end{aligned}$$

woraus also zu schliessen, dass P_{00}^3, P_{10}^3, P_{01}^3, P_{11}^6, und, falls n ein Quadrat, auch P_{11}^3 Wurzeln von Transformationsgleichungen sind. Dasselbe folgt aber auch aus

$$(9)\qquad \frac{P_{10}}{P_{00}} = \prod \frac{\cos \operatorname{am}(s\Omega)}{\Delta \operatorname{am}(s\Omega)}, \qquad \frac{P_{01}}{P_{00}} = \prod \frac{1}{\Delta \operatorname{am}(s\Omega)}$$

für diese beiden Quotienten, und aus

$$(10) \qquad (-1)^{\frac{n^2-1}{8}} (\sqrt[3]{2})^{n-1} \frac{P_{11} P_{00}^2}{\sqrt[3]{kk'}^{\frac{n-1}{2}}} = \prod^{s} \frac{\sin \operatorname{am}(s\Omega)\, \Delta \operatorname{am}(s\Omega)}{\cos \operatorname{am}(s\Omega)}$$

für das Quadrat dieser letzteren Grösse, und falls n ein Quadrat ist, für diese selbst.

Nun ergiebt sich aber noch aus der Multiplication, indem man in der letzten Formel IV § 9 $u = 2s\tilde{\omega}$ setzt und das Product über alle s von 1 bis $\frac{1}{2}(n-1)$ nimmt:

$$(11) \qquad P_{00}^{n^2} = \prod_{1, \frac{n-1}{2}}^{s} \frac{\Delta \operatorname{am}(s\Omega)^{n^2}}{D(\sin \operatorname{am} s\Omega^2)},$$

und hieraus schliesst man, dass auch $P_{00}^{n^2}$ Wurzel einer Transformationsgleichung ist. Dies lehrt nichts neues wenn n durch 3 teilbar ist; ist aber n nicht durch 3 teilbar, also $n^2 \equiv 1 \pmod 3$ so folgt daraus unmittelbar durch Zusammenhalten mit dem vorigen Satz, und mit Rücksicht auf (9), (11), dass auch P_{00}, P_{10}, P_{01}, P_{11}^2 und falls n ein Quadrat ist, auch P_{11} die Wurzeln von Transformationsgleichungen sind.

§ 16. *Zweite Darstellung der Wurzeln der Transformationsgleichungen.*

Die Wurzeln der eigentlichen Teilungsgleichung sind charakterisirt durch zwei nach dem Modul n bestimmte Zahlen μ, μ', welche mit n keinen Teiler gemein haben, und die auch unter einander relativ prim vorausgesetzt werden können. Es kommt nun darauf an, die verschiedenen *Reihen,* die, wie wir oben gesehen haben, durch eine Gleichung $\psi(n)^{\text{ten}}$ Grades bestimmt sind, durch Zahlen zu charakterisiren.

Aus der Definition der Reihen geht hervor, dass der grösste gemeinschaftliche Teiler d von μ' und n für alle Wurzeln einer Reihe derselbe ist. Sei also

$$(1) \qquad \mu' = dy, \qquad n = ad,$$

worin a und d als positiv vorausgesetzt sind, und den grössten gemeinschaftlichen Teiler e haben mögen, dessen Quadrat also in n aufgeht. Da nun y relativ prim zu a ist, so kann man die Zahlen c und x so bestimmen, dass

$$\mu = ax + cy, \tag{2}$$

worin c jedoch nur nach dem Modul a bestimmt ist, und z. B. durch eine beliebige Potenz von 2, oder, wenn a nicht durch 3 teilbar ist, durch eine beliebige Potenz von 3 teilbar angenommen werden kann. Aus der Bedingung (1) § 14 folgt nun, *dass zwei Wurzeln der eigentlichen Teilungsgleichung dann und nur dann derselben Reihe angehören wenn in*

$$\begin{aligned} \mu &= ax + cy \\ \mu' &= dy \end{aligned} \tag{3}$$

die drei Zahlen a, d, c, *letztere modulo* a, *denselben Wert haben.* Da μ, μ', n ohne gemeinsamen Teiler sind, so muss c relativ prim zu e sein und kann daher nur

$$\frac{a}{e}\varphi(e)$$

verschiedene Werte annehmen. Jeder dieser Zahlenwerte ist aber auch zulässig, und führt bei passender Bestimmung von x, y zu einem eine Reihe bestimmenden Zahlenpaar μ, μ', woraus sich ergiebt

$$\sum \frac{a}{e}\varphi(e) = \psi(n)\,(^1),$$

wenn die Summe sich auf alle Divisoren a von n erstreckt. In jeder Reihe giebt es wenigstens eine Wurzel, für welche $\mu \equiv d \pmod{n}$ ist, so dass $y = 1$ gesetzt werden kann. Wir wählen also als repräsentirendes Glied der Reihe ein solches aus, für welches

$$\begin{aligned} \mu &= ax + c \\ \mu' &= d, \end{aligned} \tag{4}$$

(1) Diese Gleichung lässt sich leicht auch direct beweisen. (Vgl. DEDEKIND, *Modulfunctionen*, l. c. S. 288.)

so dass μ, μ' relativ prim sind. Wenn wir nun zwei Zahlen ν, ν' so bestimmen, dass

$$\mu\nu' - \nu\mu' = 1 \tag{5}$$

wird, so können wir nach § 5 die zusammengesetzte Transformation bilden

$$\begin{pmatrix} a, & 0 \\ c, & d \end{pmatrix} = \begin{pmatrix} -a\nu', & 1 \\ -c\nu' + d\nu, & -x \end{pmatrix} \begin{pmatrix} 1, & 0 \\ 0, & n \end{pmatrix} \begin{pmatrix} \mu, & \mu' \\ \nu, & \nu' \end{pmatrix}, \tag{6}$$

und die Anwendung der dortigen Formel (28) ergiebt

$$P_{11} = i^{\frac{n-1}{2}} e^{-\frac{\pi i}{12}(n\lambda+\lambda')} \sqrt{d}\, \frac{\eta\left(\frac{c+d\omega}{a}\right)}{\eta(\omega)}. \tag{7}$$

Behufs einfacherer Berechnung von $n\lambda + \lambda'$ kann man

$$\mu \equiv 0, \qquad \nu' \equiv 0, \qquad c \equiv 0 \pmod 8$$

annehmen und erhält (§ 5)

$$\begin{aligned} n\lambda + \lambda' &\equiv 2a\left(\frac{\mu}{\mu'}\right) - a(d+1) \pmod 8 \\ &\equiv ac \pmod 3, \qquad n \equiv \pm 1 \pmod 3 \\ &\equiv -a\nu' - x \pmod 3, \qquad n \equiv 0 \pmod 3; \end{aligned} \tag{8}$$

die beiden letzteren Fälle lassen sich auch so zusammenfassen:

$$n\lambda + \lambda' \equiv (x + a\nu')(n^2 - 1) + ncd \pmod 3.$$

Setzen wir also:

$$\rho = e^{\frac{2\pi i}{3}[(x+a\nu')(n^2-1)+ncd]} \tag{9}$$

so folgt

$$P_{11} = \rho\left(\frac{\mu}{\mu'}\right) i^{\frac{a-1}{2}} \sqrt{d}\, \frac{\eta\left(\frac{c+d\omega}{a}\right)}{\eta(\omega)} \tag{10}$$

worin, falls n nicht durch 3 teilbar ist, $c \equiv 0 \pmod{24}$ angenommen werden kann, wodurch $\rho = 1$ wird. Ist n eine Quadratzahl, in welchem

Falle allein die Bestimmung des Vorzeichens in (10) von Interesse ist, so ist auch $d:e$ eine Quadratzahl und mithin ist

$$\left(\frac{\mu}{\mu'}\right) = \left(\frac{ax + c}{d}\right) = \left(\frac{c}{e}\right). \tag{11}$$

Auf demselben Wege leitet man aus den drei letzten Formeln (1) § 4 die Gleichungen her:

$$\sqrt[3]{2}^{n-1}\frac{P_{11}P_{00}^2}{\sqrt[3]{kk'}^{\frac{n-1}{2}}} = i^{\frac{a-1}{2}}\left(\frac{\mu}{\mu'}\right)\sqrt{d}\,\frac{\vartheta_{00}\left(0, \frac{c + d\omega}{a}\right)}{\vartheta_{00}}$$

$$k^{\frac{n-1}{2}}\sqrt[3]{2}^{n-1}\frac{P_{11}P_{10}^2}{\sqrt[3]{kk'}^{\frac{n-1}{2}}} = i^{\frac{a-1}{2}}\left(\frac{\mu}{\mu'}\right)\sqrt{d}\,\frac{\vartheta_{10}\left(0, \frac{c + d\omega}{a}\right)}{\vartheta_{10}} \tag{12}$$

$$k'^{\frac{n-1}{2}}\sqrt[3]{2}^{n-1}\frac{P_{11}P_{01}^2}{\sqrt[3]{kk'}^{\frac{n-1}{2}}} = i^{\frac{a-1}{2}}\left(\frac{\mu}{\mu'}\right)\sqrt{d}\,\frac{\vartheta_{01}\left(0, \frac{c + d\omega}{a}\right)}{\vartheta_{01}}.$$

Aus (10) und (12) ergiebt sich aber:

$$\sqrt[3]{2}^{n-1}P_{00}^2 = \rho^2\frac{\chi(\omega)^{2n}}{\chi\left(\frac{c + d\omega}{a}\right)^2}$$

$$\frac{P_{10}^2}{P_{00}^2} = \frac{\varphi\left(\frac{c + d\omega}{a}\right)^2}{\varphi(\omega)^{2n}} \tag{13}$$

$$\frac{P_{01}^2}{P_{00}^2} = \frac{\psi\left(\frac{c + d\omega}{a}\right)^2}{\psi(\omega)^{2n}}.$$

Aus diesen Ausdrücken kann auch die Wurzel gezogen werden, und durch Anwendung der HERMITE'schen Formeln für die lineare Transformation der Functionen φ, ψ, χ lassen sich die Vorzeichen bestimmen:

$$\sqrt[3]{2}^{\frac{n-1}{2}} P_{00} = \rho \frac{\chi(\omega)^n}{\chi\left(\frac{c+d\omega}{a}\right)}$$

$$\frac{P_{10}}{P_{00}} = \left(\frac{2}{d}\right) \frac{\varphi\left(\frac{c+d\omega}{a}\right)}{\varphi(\omega)^n} \tag{14}$$

$$\frac{P_{01}}{P_{00}} = \left(\frac{2}{d}\right) \frac{\psi\left(\frac{c+d\omega}{a}\right)}{\psi(\omega)^n}.$$ [1]

Aus (13) ergiebt sich, dass auch die ν Functionen

$$j\left(\frac{c+d\omega}{a}\right) \tag{15}$$

(worin c an keine Congruenz gebunden zu werden braucht) Wurzeln einer Transformationsgleichung sind, die wir die *Invariantengleichung* nennen wollen.

Dass alle die hier betrachteten Transformationsgleichungen verschiedene Wurzeln haben und mithin irreductibel sind, ergiebt sich sehr einfach aus dem Verhalten der Wurzeln für $q = 0$.

Die Invariantengleichung hat die Eigenschaft, dass ihre Coëfficienten alle ganze rationale Functionen von $j(\omega)$ sind. Denn ersetzt man ω durch $\omega + 1$ und $-1:\omega$, so geht $j(n\omega)$ über in $j(n\omega)$ und $j\left(\frac{\omega}{n}\right)$; und da auch letzteres eine Wurzel der (irreductibeln) Invariantengleichung ist, so können sich die Coëfficienten derselben durch diese beiden Substitutionen nicht ändern und sind daher (nach § 7) rationale Functionen von $j(\omega)$. Da ferner keine der Grössen (15) für einen endlichen Wert von $j(\omega)$ unendlich wird so sind sie auch ganze Functionen von j (wenn der Coëfficient der höchsten Potenz der Unbekannten $= 1$ ist).

Wir werden ausser der Invariantengleichung noch diejenigen Trans-

---

[1] Die Transformationsgleichung für P_{00} ist zuerst von SCHLÄFLI untersucht (Journal für Mathematik, Bd. 72, S. 368).

Die Function $P_{10}:P_{00}$ führt auf die JACOBI'sche Modulargleichung. Die Bestimmung der Vorzeichen in diesen Formeln führen wir hier nicht weiter aus, da wir keinen Gebrauch von denselben machen werden.

formationsgleichungen betrachten, deren Wurzeln Potenzen von P_{11} sind.(1) Diese Gleichungen sind nicht alle nur von $j(\omega)$ abhängig, sondern zum Teil auch von g_2 und g_3. Die Form dieser Abhängigkeit ergiebt sich leicht aus den Sätzen des § 7. Wir heben hier nur diejenigen Fälle hervor, in welchen die Coëfficienten rationale Functionen von j werden, die man ebenso wie oben findet, indem man ω in $\omega + 1$ und in $-1:\omega$ verwandelt. Nennen wir diese Art von Transformationsgleichungen *invariante Multiplicatorgleichungen*, so haben wir die folgenden Sätze.

Es sind Wurzeln von invarianten Multiplicatorgleichungen:

(16)

P_{11}^{12}	für jedes ungerade n
P_{11}^{6}	$n \equiv 1 \pmod 4$
P_{11}^{4}	$n \equiv 1 \pmod 6$
P_{11}^{2}	$n \equiv 1 \pmod{12}$
P_{11}^{3}	n eine ungerade Quadratzahl
P_{11}	n eine weder durch 2 noch durch 3 teilbare Quadratzahl.

Da P_{11} für einen endlichen Wert von ω weder Null noch unendlich wird, so sind die Coëfficienten der invarianten Multiplicatorgleichung *ganze rationale* Functionen von j und der letzte derselben ist von j unabhängig; oder mit andern Worten: es ist sowohl P_{11} als $1:P_{11}$ eine *ganze* algebraische Function von j.(2) Aus dem Schluss des § 14 geht hervor, dass die in (16) zusammengestellten Potenzen von P_{11} rational durch

$$j\left(\frac{c + d\omega}{a}\right)$$

ausgedrückt werden können, und zwar als ganze rationale Functionen, höchstens vom Grade $\nu - 1$. Die Coëfficienten dieser Ausdrücke sind rationale Functionen von k^2 mit rationalen Zahlencoëfficienten, und die

---

(1) Gleichungen dieser Art sind von F. KLEIN (l. c.) und KIEPERT (Journal für Mathematik, Bd. 87, 88, 95) untersucht.

(2) Nach Analogie der Zahlentheorie würde eine solche algebraische Function als eine *Einheit* zu bezeichnen sein.

Veränderung von ω in $\omega + 1$ und $-1:\omega$ zeigt, dass dieselben rational von $j(\omega)$ abhängen. Dass auch in der Darstellung durch $j(\omega)$ nur *rationale Zahlencoëfficienten* vorkommen, ergiebt sich leicht daraus, dass $j(\omega)$ nach aufsteigenden Potenzen von k^2 mit rationalen Coëfficienten entwickelbar ist.

§ 17. *Die Invariantengleichung.*

Die Wurzeln der Invariantengleichung sind, wie wir oben gesehen haben, die Grössen

$$j\left(\frac{c + d\omega}{a}\right).$$

Da nun, wenn a, b, c, d vier beliebige ganze Zahlen ohne gemeinsamen Teiler sind, deren Determinante $ad - bc = n$ ist, eine Substitution

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$$

mit der Determinante $\alpha\delta - \beta\gamma = 1$ so bestimmt werden kann, dass

$$\begin{pmatrix} a, & b \\ c, & d \end{pmatrix} = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}\begin{pmatrix} a', & 0 \\ c', & d' \end{pmatrix},$$[1]

so folgt, dass die sämmtlichen Grössen

$$j\left(\frac{c + d\omega}{a + b\omega}\right)$$

Wurzeln der Invariantengleichung sind, dass unter diesen aber nur ν von einander verschiedene sich finden.

Es sei nun

$$F_n(v, u) \tag{1}$$

diejenige ganze rationale Function der beiden Variablen u, v vom Grade

---

[1] Vgl. DEDEKIND, *Modulfunctionen*, § 7, l. c.

$\psi(n) = \nu$ in Bezug auf v, in welcher die höchste Potenz v^ν den Coëfficienten (1) hat, welche für

$$u = j(\omega), \qquad v = j\left(\frac{c + d\omega}{a + b\omega}\right) \tag{2}$$

verschwindet, und $v_1, v_2, \ldots, v_\nu$ seien die Wurzeln der Gleichung

$$F_n[v, j(\omega)] = 0. \tag{3}$$

Ist n' zu n relativ prim so ist $\psi(n)\psi(n') = \psi(nn')$ und das Product

$$F_{n'}(v, v_1)F_{n'}(v, v_2)\ldots F_{n'}(v, v_\nu) \tag{4}$$

vom Grade $\psi(nn')$ hängt als symmetrische Function der Wurzeln von (3) rational von $j(\omega)$ ab. Zugleich verschwindet dieses Product für

$$v = j\left(\frac{\omega}{nn'}\right),$$

und daher ist dasselbe, wenn man wieder $j(\omega)$ durch u ersetzt, identisch mit

$$F_{nn'}(v, u) \tag{5}$$

(mit Rücksicht auf die Irreductibilität der letzteren Function). Hiernach kann man die Lösung der allgemeinen Gleichung $F_n(v, u) = 0$ auf den Fall zurückführen, wo n eine Primzahlpotenz ist.

Betrachten wir ferner die Gleichung

$$F_{p^{\pi-1}}(v, u) = 0$$

vom Grade $\nu = p^{\pi-2}(p + 1)$, worin p eine Primzahl ist, deren Wurzeln $v_1, v_2, \ldots, v_\nu$ seien. Das Product

$$P = F_p(v, v_1)F_p(v, v_2)\ldots F_p(v, v_\nu) \tag{6}$$

ist in Bezug auf v vom Grade $p^{\pi-2}(p + 1)^2$ und verschwindet für

$$u = j(\omega), \qquad v_1 = j\left(\frac{\omega}{p^{\pi-1}}\right), \qquad v = j\left(\frac{\omega}{p^\pi}\right). \tag{7}$$

Es muss daher P durch $F_{p^\pi}(v, u)$ teilbar sein.

Ist ferner

$$u = j(\omega), \qquad v_1 = j\left(\frac{p^{\pi-2}c + \omega}{p^{\pi-1}}\right), \tag{8}$$

so verschwindet $F_p(v, v_1)$ auch für

$$v = j\left(\frac{\omega}{p^{\pi-2}}\right), \tag{9}$$

und da c in (8) p verschiedene Werte haben kann, so ist P teilbar durch

$$[F_{p^{\pi-2}}(v, u)]^p.$$

Die Vergleichung der Grade giebt alsdann

$$F_{p^\pi}(v, u) = \frac{F_p(v, v_1) F_p(v, v_2) \ldots F_p(v, v_\nu)}{[F_{p^{\pi-2}}(v, u)]^{p^2}}. \tag{10}$$

Für $\pi = 2$ tritt an Stelle dieser Gleichung die folgende:

$$F_{p^2}(v, u) = \frac{F_p(v, v_1) F_p(v, v_2) \ldots F_p(v, v_{p+1})}{(v - u)^{p+1}}. \tag{10'}$$

Da die drei Functionen

$$j(2\omega), \qquad j\left(\frac{\omega}{2}\right), \qquad j\left(\frac{1+\omega}{2}\right) \tag{11}$$

durch die beiden Substitutionen $\omega + 1$, $-1 : \omega$ für ω nur in einander übergehen, so sind die symmetrischen Functionen dieser Grössen rationale Functionen von $j(\omega)$, woraus hervorgeht, dass auch für den Transformationsgrad 2 die Grössen (11) die Wurzeln einer Invariantengleichung sind. Die Formeln (10), (10') sind darnach auch auf den Fall $p = 2$ anwendbar, und es ergiebt sich durch die obige Schlussweise, dass auch für ein gerades n eine Invariantengleichung $\psi(n)^{\text{ten}}$ Grades besteht, deren eine Wurzel $j(n\omega)$ ist. Da nun nach § 5 (27) jede Substitution mit der Determinante n

$$\begin{pmatrix} a, & b \\ c, & d \end{pmatrix}$$

durch Vermittelung linearer Substitutionen aus

$$\begin{pmatrix} 1, & 0 \\ 0, & n \end{pmatrix}$$

abgeleitet werden kann, so folgt, dass die sämmtlichen Functionen

$$j\left(\frac{c + d\omega}{a + b\omega}\right)$$

derselben Gleichung genügen. Diese Functionen werden daher durch die $\psi(n)$ *verschiedenen* Functionen

$$j\left(\frac{c + d\omega}{a}\right)$$

erschöpft und zugleich folgt hieraus auch für diesen Fall die *Irreductibilität der Invariantengleichung.*

Die Function $F_n(v, u)$ *ist symmetrisch in Bezug auf* u *und* v. Denn aus der identischen Gleichung

$$F_n[j(n\omega), j(\omega)] = 0$$

folgt, indem man ω durch $\omega : n$ ersetzt:

$$F_n\left[j(\omega), j\left(\frac{\omega}{n}\right)\right] = 0,$$

und es ergiebt sich also aus der Irreductibilität, dass $F_n(u, v)$ durch $F_n(v, u)$ teilbar sein muss. Da man die beiden unabhängigen Variablen vertauschen kann, so folgt dasselbe umgekehrt, und daraus ergiebt sich

$$F_n(u, v) = \pm F_n(v, u). \tag{12}$$

Darin ist aber (ausser für $n = 1$) nur das obere Zeichen zulässig, da sonst $F_n(v, u)$ für $v = u$ verschwinden würde, was der Irreductibilität wiederspricht.

Wir schliessen hier noch den Beweis eines wichtigen Satzes über die Zahlencoëfficienten der Invariantengleichung an unter der Voraussetzung, dass der Transformationsgrad n eine Primzahl sei.

Die Invariante lässt sich nach ihrer Definition (§ 6) in eine nach-

aufsteigenden Potenzen von q fortschreitende Reihe entwickeln von der Form

$$(13) \qquad j(\omega) = q^{-2}(1 + a_1 q^2 + a_2 q^4 + \ldots) = q^{-2} \sum_{0,\infty}^{s} a_s q^{2s},$$

worin die Coëfficienten a_s *ganze Zahlen* sind ($a_0 = 1$, $a_1 = 744$) und in eine ähnliche Reihe lässt sich jede Potenz von $j(\omega)$ entwickeln. Es ergiebt sich ins Besondere durch Anwendung des polynomischen Lehrsatzes und des für jedes a gültigen FERMAT'schen Satzes

$$a^p \equiv a \pmod{p}:$$

$$(14) \qquad j(\omega)^p = q^{-2p} \sum_{0,\infty}^{s} a_s q^{2sp} + pq^{-2(p-1)} \sum_{0,\infty}^{s} b_s q^{2s}$$

worin die b_s ebenfalls ganze Zahlen sind. Und aus (13) erhält man

$$(15) \qquad j(p\omega) = q^{-2p} \sum_{0,\infty}^{s} a_s q^{2sp}.$$

Setzt man also

$$j(\omega) = u, \qquad j(p\omega) = v,$$

so folgt

$$(16) \qquad u^p - v = pq^{-2(p-1)} \sum_{0,\infty}^{s} b_s q^{2s},$$

und wenn c_s andere ganze Zahlen sind:

$$(17) \qquad (u - v^p)(u^p - v) = v^{p+1} + u^{p+1} - u^p v^p - uv = pq^{-2(p^2+p-1)} \sum_{0,\infty}^{s} c_s q^{2s}.$$

Es lässt sich aber nach (12) die Invariantengleichung in die Form setzen

$$(18) \qquad (u - v^p)(u^p - v) = \sum_{0,p}^{r,s} c_{r,s} v^r u^s$$

worin die $c_{r,s}$ die zu bestimmenden Zahlencoëfficienten sind, welche der Bedingung

$$(19) \qquad c_{r,s} = c_{s,r}, \qquad c_{p,p} = 0$$

genügen (letzteres weil in der Entwicklung (17) die Potenz $q^{-2(p^2+p)}$ nicht vorkommt).

Zur Bestimmung der Coëfficienten $c_{r,s}$ kann man hiernach die Gleichungen (18) auch so schreiben:

$$(20) \qquad (u - v^p)(u^p - v) = \sum_{0,p}^{r} \sum_{0,r-1}^{s} c_{r,s}(v^r u^s + v^s u^r) + \sum_{0,p-1}^{s} c_{s,s} u^s v^s.$$

Hierin setzt man nun die aus (13), (15) sich ergebenden Entwickelungen von $v^r u^s + v^s u^r$, $u^s v^s$ nach Potenzen von q ein, welche mit den Anfangsgliedern

$$q^{-2(rp+s)}, \qquad q^{-2s(p+1)}$$

und mit dem Coëfficienten 1 beginnen. *Auf der rechten Seite von* (20) *kommen aber nicht zwei Glieder mit demselben Anfang der Entwicklung vor,* denn aus

$$rp + s = r'p' + s'$$

folgt $s \equiv s' \pmod{p}$ und mithin, da in (20) $s < p$ ist, $s = s'$, $r = r'$. Wenn man daher die Coëfficienten derselben Potenzen von q auf beiden Seiten der Gleichung (20) einander gleich setzt, so erhält man eine Reihe linearer Gleichungen, deren jede folgende nur *eine* neue Unbekannte $c_{r,s}$ mit dem Coëfficienten 1 enthält, so dass alle diese Coëfficienten sich als *ganze durch p teilbare Zahlen* ergeben.

Es hat also die Invariantengleichung die Form

$$(21) \qquad (u - v^p)(u^p - v) = p \sum_{0,p}^{r,s} a_{r,s} v^r u^s$$

worin die $a_{r,s}$ den Bedingungen $a_{r,s} = a_{s,r}$; $a_{p,p} = 0$ genügende ganze Zahlen sind.

Hieraus ergiebt sich noch mittelst der zu Anfang dieses Paragraphen gegebenen Darstellung der Invariantengleichung für einen zusammengesetzten Transformationsgrad ((4) und (10)), dass auch im allgemeinen Fall die Coëfficienten der Invariantengleichung *ganze Zahlen sind.*

IV. Abschnitt.

§ 18. *Die complexe Multiplication.*

Die Multiplicationstheorie der elliptischen Functionen haben wir in § 9 auf den Satz gegründet dass

$$\theta_{g,h}(\mu u,\ \omega) \tag{1}$$

für ein *ganzzahliges* μ θ-Functionen von μ und ω sind. Ähnliche Betrachtungen werden sich immer dann durchführen lassen, wenn μ und $\mu\omega$ Perioden der Function $\theta(u,\ \omega)$ sind. Damit dies aber stattfinde, ist notwendig und hinreichend, dass vier ganze Zahlen a, b, c, d sich so bestimmen lassen, dass

$$\begin{aligned} \mu &= a + b\omega \\ \mu\omega &= c + d\omega \end{aligned} \tag{2}$$

und dies ist, *so lange* ω *variabel ist*, nur möglich für $b = 0$, $c = 0$, also für ein ganzzahliges μ. Ausserdem aber können die Bedingungen (2) auch dann erfüllt werden, wenn ω einer Gleichung zweiten Grades mit ganzzahligen Coëfficienten und *negativer Determinante* genügt:

$$\omega(a + b\omega) = c + d\omega. \tag{3}$$

In diesem Fall wird μ eine complexe Zahl von der Form $M + N\sqrt{-n}$, worin n eine ganze positive, M, N rationale Zahlen sind, deren letzte nicht verschwindet. Diese Art der Multiplication heisst aus diesem Grunde die *complexe Multiplication.* Die Werte welche in diesem Falle der Modul k oder die Invariante $j(\omega)$ annehmen, sind *algebraische Zahlen*, welche mit den quadratischen Formen von negativer Determinante im innigsten Zusammenhang stehen. Die Existenz solcher *singulärer Moduln* ist zuerst von Abel erkannt, der auch bereits den Satz ausgesprochen hat, dass dieselben durch Wurzelziehen aus dem Gebiete der rationalen Zahlen abgeleitet werden können (Abel, Oeuvres, éd. Sylow I, S. 377 u. folg., 426).

Die vollständige Theorie der singulären Moduln ist sodann von KRONECKER in einer längeren Reihe ausgezeichneter Untersuchungen begründet worden, die in den Monatsberichten der Berliner Akademie(1) veröffentlicht sind. Auch die Untersuchungen von DEDEKIND über die elliptischen Modulfunctionen zielen auf eine Anwendung auf die complexe Multiplication, welche durch die Einführung der Valenz (die sich von der absoluten Invariante $j(\omega)$ nur durch einen rationalen Zahlenfactor unterscheidet) eine sehr elegante Gestalt annimmt. Im Folgenden soll eine Anwendung der Transformationstheorie der elliptischen Functionen auf die Ableitung einiger Sätze aus der Theorie der complexen Multiplication gemacht werden, wobei nur der *elementare* Teil der Theorie der quadratischen Formen vorausgesetzt werden soll, während andere Sätze aus dieser Theorie, die von GAUSS und DIRICHLET durch tiefer liegende Hilfsmittel bewiesen sind, aus der complexen Multiplication selbst hergeleitet werden sollen.

Aus den am Eingang dieses Paragraphen gemachten Bemerkungen (Formel (3)) ergiebt sich, dass diejenigen Werte von ω, für welche die complexe Multiplication statt hat, imaginäre Wurzeln von Gleichungen zweiten Grades mit rationalen Coëfficienten sind, und zwar diejenigen, deren imaginärer Teil positiv ist.

Auch das Umgekehrte ist der Fall, denn es sei

$$A\omega^2 + B\omega + C = 0 \tag{4}$$

eine solche Gleichung, in welcher A, B, C ganze Zahlen ohne gemeinsamen Teiler sind und

$$4AC - B^2 = \Delta \tag{5}$$

sei positiv; so kann man hieraus in mannigfaltiger Weise Gleichungen von der Form (3) herleiten, indem man setzt

$$b = Ax, \qquad a - d = Bx, \qquad c = -Cx, \qquad a + d = y. \tag{6}$$

Hieraus folgt

$$2a = y + Bx, \qquad b = Ax, \qquad c = -Cx, \qquad 2d = y - Bx, \tag{7}$$

(1) 29 Oct. 1857, 26 Juni 1862, 22 Januar 1863, 1 Dec. 1870, 19 Juli 1875, 16 Apr. 1877, 2 Febr. 1880, 7 Dec. 1882.

und man kann über die ganzen Zahlen x, y so verfügen, dass a, b, c, d ganze Zahlen ohne gemeinsamen Teiler sind. Es ist dann

$$4(ad - bc) = 4n = y^2 + \Delta x^2, \tag{8}$$

und x, y können keinen andern gemeinsamen Teiler haben als 2. Setzt man umgekehrt für x, y irgend zwei der Bedingung (8) genügende Zahlen *ohne gemeinschaftlichen Teiler*, so erhält man aus (7) vier Zahlen a, b, c, d mit der Determinante n, welche keinen Teiler gemein haben. Dasselbe gilt auch noch für ein ungerades n, wenn x, y den grössten gemeinsamen Teiler 2 haben.

Unter diesen Voraussetzungen ist aber

$$j\left(\frac{c + d\omega}{a + b\omega}\right) = j(\omega). \tag{9}$$

und es genügt daher dieser Wert von j der Gleichung

$$F_n(u, u) = 0. \tag{10}$$

Wenn umgekehrt $u = j(\omega)$ eine Wurzel der Gleichung (10) ist, so folgt daraus nach § 16 eine Gleichung von der Form (9), woraus wieder die Gleichungen (7) und (8) folgen. (Vgl. § 6.)

Der quadratischen Gleichung (4) entspricht eine primitive quadratische Form erster oder zweiter Art, je nachdem B gerade oder ungerade, also $\Delta \equiv 0$ oder $\equiv -1 \pmod 4$ ist:

$$\left(A, \tfrac{1}{2}B, C\right) \quad \text{oder} \quad (2A, B, 2C) \tag{11}$$

von der Determinante $-\frac{1}{4}\Delta$ oder $-\Delta$; und umgekehrt entspricht jeder primitiven quadratischen Form von *negativer Determinante* eine Gleichung von der Form (4), also *ein* Wert von ω und von $j(\omega)$, für welchen complexe Multiplication stattfindet.

Ersetzt man eine Form (11) durch eine äquivalente Form, so geht auch ω in eine äquivalente Zahl über, und $j(\omega)$ bleibt ungeändert. Ein solcher singulärer Wert von $j(\omega)$ entspricht also nicht nur einer Form, sondern einer ganzen Formenclasse. *Dagegen entsprechen nicht äquivalenten Formen immer verschiedene Werte von* $j(\omega)$.

Wir können daher passend die Zahl $j(\omega)$ als *Invariante der durch*
(11) *repräsentirten Formenclasse* oder kurz als *Classeninvariante* bezeichnen.

Die Classeninvarianten sind *ganze algebraische Zahlen*. Als Wurzeln von Gleichungen (10) sind sie zunächst algebraische Zahlen. Der Grad der Gleichung (10) wird bestimmt aus

$$F_n[j(\omega),\ j(\omega)] = \prod\left[j(\omega) - j\left(\frac{c + d\omega}{a}\right)\right], \tag{12}$$

indem man ω unendlich, $q = 0$ werden lässt. (Vgl. § 16.) Es ergiebt sich hieraus leicht für den Grad μ von $F_n(u, v)$ falls n kein Quadrat ist

$$\mu = 2\sum_{d>\sqrt{n}} \frac{d}{e}\varphi(e), \tag{13}$$

und falls n ein Quadrat ist

$$\mu = 2\sum_{d>\sqrt{n}} \frac{d}{e}\varphi(e) + \varphi(\sqrt{n}). \tag{14}$$

Der Coëfficient der höchsten Potenz von u in $F_n(u, v)$ wird durch dasselbe Verfahren bestimmt, und ergiebt sich, wenn n kein Quadrat ist, $= \pm 1$. Da man nun über x, y in (8) stets so verfügen kann, dass n kein Quadrat wird,(1) und da, wie früher bewiesen, die Coëfficienten in $F_n(v, u)$ ganze Zahlen sind, so folgt dass die Classeninvarianten *ganze* algebraische Zahlen sind. (Dedekind, Suppl. XI zur dritten Auflage von Dirichlet's *Vorlesungen über Zahlentheorie*, § 160 ff.)

Wir bezeichnen nun das Product

$$\prod[u - j(\omega)],$$

ausgedehnt über alle zu einer bestimmten negativen Determinante $-n$ gehörigen Invarianten eigentlich primitiver Classen mit

$$H_n(u),$$

---

(1) Ist z. B. $x^2 + \Delta y^2 = u^2$ ein Quadrat und p eine in n aber nicht in x und folglich auch nicht in y aufgehende Primzahl und ξ relativ prim zu p, so ist $(x + \xi p)^2 + \Delta y^2$ durch p, aber nicht durch p^2 teilbar und also gewiss kein Quadrat, und man kann über ξ noch so verfügen, dass $x + \xi p$ und y relativ prim sind.

und dasselbe Product, erstreckt über alle zur Determinante $-n$ gehörigen Invarianten uneigentlich primitiver Classen mit

$$H'_n(u).$$

(H'_n existirt natürlich nur dann wenn $n \equiv -1 \pmod 4$). H_n, H'_n sind ganze rationale Functionen der unbestimmten Grösse u, deren Grade h, h' gleich den Classenzahlen der Formen erster und zweiter Art von der Determinante $-n$ sind. Der Hauptsatz, dessen Nachweis zu führen ist, besteht darin, dass die Functionen H_n, H'_n rationale Coëfficienten haben, woraus schon von selbst folgt, dass diese Coëfficienten, als ganze algebraische Zahlen, auch *ganze* rationale Zahlen sind.

Zunächst ist leicht einzusehen, dass der Satz richtig ist für H_1 und H'_3; denn für diese beiden Fälle hat man beziehungsweise

$$\omega = -\frac{1}{\omega} \quad \text{und} \quad \omega = -1 - \frac{1}{\omega}, \tag{15}$$

und folglich (nach § 6 (15), (16)) $g_3(\omega) = 0$ resp. $g_2(\omega) = 0$; also ist

$$H_1(u) = u - 27.64, \qquad H'_3(u) = u. \tag{16}$$

Wir nehmen nun an, es sei unser Satz als richtig erwiesen für H_m so lange $m < n$, und für H'_m so lange $m < 4n - 1$, und zeigen dass er auch gilt für H_n und H'_{4n-1}.

Wenn die Gleichung (10) $F_n(u, u) = 0$ irgend eine Classeninvariante zur Wurzel hat, so genügen derselben, wie die Gleichungen (7), (8) zeigen alle zu derselben Determinante und derselben Art gehörigen Classeninvarianten. Die Gleichung (8) ist aber erfüllt für

$$\begin{aligned} &\Delta = 4n, && y = 0, && x = \pm 1 \\ &\Delta = 4n - 1, && y = 1, && x = \pm 1, \end{aligned} \tag{17}$$

und alle andern Werte von Δ, für welche (8) noch befriedigt werden kann, sind kleiner als diese. Es ist daher $F_n(u, u)$ teilbar durch $H_n(u)$, $H'_{4n-1}(u)$ und ausserdem nur noch durch solche Functionen $H_m(u)$, $H'_m(u)$, deren Indices kleiner sind als n, resp. $4n - 1$, und die daher nach Voraussetzung rationale Coëfficienten haben.

Daraus folgt also, dass das Product

$$(18) \qquad H_n(u)\,H'_{4n-1}(u)$$

rationale Coëfficienten hat. (Man erhält nämlich dies Product, indem man $F_n(u, u)$ von mehrfachen Factoren und von solchen Teilern befreit, die es mit niedrigeren Functionen $H_m(u)$, $H'_m(u)$ gemein hat.)

Es ist nun ferner

$$4(4n - 1) = y^2 + (4n - 1)x^2$$

lösbar ($y = 0$, $x = \pm 2$),

$$4(4n - 1) = y^2 + 4nx^2$$

nicht lösbar. (Denn aus letzterer Gleichung würde folgen $4n(4 - x^2) = y^2 + 4$. Es könnte also wegen der positiven rechten Seite x nur $= \pm 1$ sein; dies ist aber nicht möglich, weil $y^2 + 4$ nicht durch 3 teilbar sein kann.) Hieraus folgt, dass

$$F_{4n-1}(u, u)$$

durch $H'_{4n-1}(u)$ teilbar, dagegen zu $H_n(u)$ relativ prim ist. Und daraus ergiebt sich, dass auch $H_n(u)$ und $H'_{4n-1}(u)$ rationale Coëfficienten haben. Die Gleichungen $H_m(u) = 0$, $H'_m(u) = 0$ wollen wir die zur Determinante $-m$ gehörige *Classengleichung erster und zweiter Art* nennen.

§ 19. *Über die Beziehungen zwischen den Classeninvarianten der verschiedenen Ordnungen.*

A) *Classeninvarianten erster und zweiter Art.*

Es seien

$$(1) \qquad H_m(u) = 0, \qquad (2) \qquad H'_m(u) = 0$$

die zur Determinante $-m$ (welche $\equiv 1 \pmod 4$ vorausgesetzt ist) gehörigen Classengleichungen erster und zweiter Art und $u = j(\omega)$ eine Wurzel der ersteren. Dann ist

$$(3) \qquad A\omega^2 + 2B\omega + C = 0, \qquad B^2 - AC = -m \equiv 1 \pmod 4,$$

und man kann B und C ungerade voraussetzen, was zur Folge hat, dass A durch 4 teilbar ist. Die cubische Invariantengleichung

$$F_2(v, u) = 0 \tag{4}$$

hat zu Wurzeln

$$v = j(2\omega), \quad j\left(\frac{\omega}{2}\right), \quad j\left(\frac{1+\omega}{2}\right), \tag{5}$$

und wenn

$$\omega' = 2\omega, \quad \frac{\omega}{2}, \quad \frac{1+\omega}{2} \tag{6}$$

gesetzt wird, so hat man respective:

$$\omega' = 2\omega, \quad \frac{1}{4}A\omega'^2 + B\omega' + C = 0, \qquad \text{Det: } B^2 - AC = -m, \text{ zweite Art}$$

$$\omega' = \frac{1}{2}\omega, \quad 4A\omega'^2 + 4B\omega' + C = 0, \qquad \text{Det: } 4(B^2 - AC) = -4m \tag{7}$$

$$\omega' = \frac{1+\omega}{2}, \quad 4A\omega'^2 + 4(B-A)\omega' + (A - 2B + C) = 0.$$

$$\text{Det: } 4(B^2 - AC) = -4m$$

Es ist also nur die erste der drei Grössen (5) zugleich Wurzel der Gleichung (2), und dieselbe kann daher *rational* durch $j(\omega)$ ausgedrückt werden. Es sei dieser Ausdruck

$$v = R(u). \tag{8}$$

Ersetzt man hierin u durch die sämmtlichen Wurzeln der Gleichung (1), so ergeben sich daraus die sämmtlichen Wurzeln $v = j(\omega')$ der Gleichung (2). Denn ist $v = j(\omega')$ eine beliebige Classeninvariante zweiter Art und

$$A\omega'^2 + B\omega' + C = 0, \qquad B^2 - 4AC = -m \equiv 1 \pmod 4 \tag{9}$$

und sind wieder B, C als ungerade vorausgesetzt, so ist $j\left(\frac{1}{2}\omega'\right)$ eine zur

Determinante $-m$ gehörige Classeninvariante erster Art, weil $\omega = \omega' : 2$ der Gleichung genügt:

$$4A\omega^2 + 2B\omega + C = 0$$

Es frägt sich nun, ob unter den so erhaltenen Werten von v derselbe mehrmals vorkommen kann.

Um dies zu entscheiden, bemerken wir, dass die Werte von u, welche nach (8) denselben Wert von v hervorbringen, sämmtlich der Gleichung (1) und der Gleichung (4) genügen müssen, und dass daher höchstens je drei dieser Werte einander gleich sein können.

Ist nun $j(\omega')$ irgend einer der Werte v, in welchem ω' einer Gleichung (9) genügt, so sind die drei Wurzeln der Gleichung (4)

$$(10) \qquad u = j(2\omega'), \qquad j\left(\frac{\omega'}{2}\right), \qquad j\left(\frac{\omega' + 1}{2}\right),$$

und man hat nach (9) die Gleichungen:

$$\omega = 2\omega', \qquad A\omega^2 + 2B\omega + 4C = 0$$

$$(11) \qquad \omega = \frac{1}{2}\omega', \qquad 4A\omega^2 + 2B\omega + C = 0$$

$$\omega = \frac{1 + \omega'}{2}, \qquad 4A\omega^2 + 2(B - 2A)\omega + (A - B + C) = 0,$$

welche alle die Determinante $-m$ haben. Wenn nun

$$(12) \qquad -m \equiv 1 \pmod 8,$$

so ist A gerade, und unter den drei den Gleichungen (11) entsprechenden quadratischen Formen

$$(13) \qquad (A, B, 4C), \qquad (4A, B, C), \qquad (4A, B - 2A, A - B + C)$$

ist nur die mittlere eigentlich primitiv. Daher genügt von den drei Grössen (10) nur die mittlere der Gleichung (1) und die Grössen (8) sind alle unter einander verschieden. Daher ist in diesem Falle

$$(14) \qquad h' = h.$$

Wenn aber

$$-m \equiv 5 \pmod 8, \tag{15}$$

so ist A ungerade, und die quadratischen Formen (13) sind alle drei eigentlich primitiv. Wenn daher die drei Grössen (10) von einander verschieden sind, so ergeben je drei der Grössen u nach (8) denselben Wert von v, und es folgt:

$$h' = \frac{1}{3} h. \tag{16}$$

Es handelt sich also nur noch um die Frage, ob unter den drei Grössen (10) gleiche vorkommen, oder ob zwei der Zahlen

$$2\omega', \qquad \frac{1}{2}\omega', \qquad \frac{1+\omega'}{2} \tag{17}$$

äquivalent sein können. Nehmen wir etwa an, es sei

$$2\omega' = \frac{2\gamma + \delta\omega'}{2\alpha + \beta\omega'}, \qquad \alpha\delta - \beta\gamma = 1,$$

so folgt wegen (9)

$$2\beta = Ax, \qquad -2\gamma = Cx, \qquad 4\alpha - \delta = Bx, \quad 4\alpha + \delta = y$$

$$16 = y^2 + mx^2,$$

worin x und y gerade sind. Dies ist aber nur möglich wenn $m = 3$ ist, was in der That eine Ausnahme bildet, da in diesem Falle

$$h = h' = 1. \tag{18}$$

In diesem Falle sind die *drei* Grössen (17) äquivalent, und zu demselben Resultat kommt man, wenn man von der Annahme der Äquivalenz zweier anderer unter den Zahlen (17) ausgeht.

Da sich bei dieser Untersuchung ergeben hat, dass die Classeninvarianten der zweiten Art rational durch die der ersten Art ausdrückbar sind, so werden wir uns in der Folge auf die Betrachtung der Classeninvarianten und Classengleichungen erster Art beschränken, auch ohne dies immer ausdrücklich hervorzuheben.

B) Es sei p eine beliebige (gerade oder ungerade) Primzahl und

$$m = p^2 m', \tag{1}$$

$$H_m(u) = 0. \qquad (3) \quad H_{m'}(v) = 0 \tag{2}$$

die zu den Determinanten $-m$, $-m'$ gehörigen Classengleichungen erster Art. Es sei $u = j(\omega)$ eine beliebige Wurzel der ersteren und

$$A\omega^2 + 2B\omega + C = 0, \qquad AC - B^2 = m = p^2 m' \tag{4}$$

und A durch p nicht teilbar angenommen, was stets zulässig ist. Die Invariantengleichung

$$F_p(u, v) = 0 \tag{5}$$

hat zu Wurzeln

$$v = j(p\omega), \qquad j\left(\frac{\omega + c}{p}\right). \qquad (c = 0, 1, 2, \ldots, p-1) \tag{6}$$

Setz man nun

$$\omega' = p\omega, \ \frac{\omega + c}{p},$$

so genügt ω' beziehungsweise den Gleichungen

$$\begin{gathered} A\omega'^2 + 2Bp\omega' + Cp^2 = 0 \\ Ap^2\omega'^2 + 2(B - Ac)p\omega' + (Ac^2 - 2Bc + C) = 0. \end{gathered} \tag{7}$$

Diese Gleichungen haben die Determinante $-p^2 m$ und sind alle primitiv, ausser wenn $Ac^2 - 2Bc + C$ durch p teilbar ist. Dies findet aber nur für einen einzigen Wert von c statt, den man aus der Congruenz

$$Ac - B \equiv 0 \pmod{p}$$

erhält: denn es ist

$$A(Ac^2 - 2Bc + C) = (Ac - B)^2 + m,$$

und es ist für diesen $Ac^2 - 2Bc + C$ durch p^2 teilbar. Dieser eine Wert von ω' genügt daher der Gleichung

$$A\omega'^2 + 2\frac{B - Ac}{p}\omega' + \frac{Ac^2 - 2Bc + C}{p^2} = 0, \tag{8}$$

deren Determinante $-m'$ ist. Daraus ergiebt sich also, dass die beiden Gleichungen (3) und (5) *eine und nur eine Wurzel gemeinschaftlich haben, welche sich rational durch u ausdrücken lässt:*

$$v = R(u). \tag{9}$$

Ist zweitens $v = j(\omega')$ eine beliebige Wurzel der Gleichung (3) und

$$A\omega'^2 + 2B\omega' + C = 0, \qquad AC - B^2 = m', \tag{10}$$

und A wieder unteilbar durch p, so genügt $\omega = p\omega'$ der Gleichung

$$A\omega^2 + 2Bp\omega + Cp^2 = 0, \tag{11}$$

welche primitiv ist und zur Determinante $-m = -p^2m'$ gehört. Es ist also $j(\omega)$ eine Wurzel von (2), aus welcher man nach (9) $j(\omega')$ erhält. Daraus ergiebt sich also, dass durch (9) *alle* Wurzeln der Gleichung (3) dargestellt werden, wenn man für u *alle* Wurzeln der Gleichung (1) setzt. Man hat nun genau wie oben zu untersuchen, wie viele unter den Ausdrücken (9) denselben Wert v ergeben. Die verschiedenen Werte von u, welche dies leisten, müssen zugleich den beiden Gleichungen (2) und (5) genügen. Die Werte von u aber, welche für $v = j(\omega')$ der Gleichung (5) genügen sind

$$j(p\omega'), \qquad j\left(\frac{\omega' + c}{p}\right), \tag{12}$$

und wenn man

$$\omega = p\omega', \ \frac{\omega' + c}{p} \tag{13}$$

setzt, so gelten für diese Werte von ω beziehlich die Gleichungen

$$\begin{gathered} A\omega^2 + 2Bp\omega + Cp^2 = 0 \\ Ap^2\omega^2 + 2(B - Ac)p\omega + (Ac^2 - 2Bc + C) = 0, \end{gathered} \tag{14}$$

welche sämmtlich die Determinante $-m$ haben. Unter den Grössen (12) werden also diejenigen der Gleichung (2) genügen, für welche die entsprechende Gleichung (14) primitiv ist. Dabei sind drei Fälle zu unterscheiden:

a) Wenn p in m' aufgeht, so kommt unter den Gleichungen (14) nur eine nicht primitive vor, nämlich diejenige, für welche

$$Ac - B \equiv 0 \pmod{p}.$$

b) Wenn $-m'$ quadratischer Rest von p ist, so sind zwei der Gleichungen (14) nicht primitiv, nämlich diejenigen für welche

$$Ac - B \equiv \pm \sqrt{-m'} \pmod{p}.$$

c) Wenn $-m'$ Nichtrest von p ist, so sind sämmtliche Gleichungen (14) primitiv.

d) Für $p = 2$ sind die beiden aus der Congruenz

$$Ac - B \equiv \pm \sqrt{-m'} \pmod{2}$$

gefolgerten Werte von c mit einander identisch und folglich ist für $p = 2$ immer eine unter den Gleichungen (14) nicht primitiv.

Nehmen wir also vorläufig an, was wir gleich weiter untersuchen werden, dass unter den Grössen (13) nicht zwei äquivalente sind, so erhalten wir, wenn wir mit h, h' die Grade der Gleichungen (2), (3) bezeichnen, das folgende Resultat

$$\begin{aligned} &h = ph' && \text{falls} \quad m' \equiv 0 \pmod{p} \quad \text{oder} \quad p = 2 \\ (15) \qquad &h = (p-1)h' && \text{»} \quad \left(\frac{-m'}{p}\right) = +1 \\ &h = (p+1)h' && \text{»} \quad \left(\frac{-m'}{p}\right) = -1. \end{aligned}$$

Es handelt sich also noch darum, ob unter den Grössen (13) nach Ausschluss der wegen a), b) oder d) wegfallenden zwei äquivalente vorkommen können.

α) Sei also zunächst

$$\frac{\omega' + c}{p} = \frac{\gamma + \partial p\omega'}{\alpha + \beta p\omega'}, \qquad \alpha\partial - \beta\gamma = 1$$

$$\beta p\omega'^2 + (\alpha + \beta pc - \partial p^2)\omega' + \alpha c - \gamma p = 0,$$

so muss wegen (10)

$$(16) \qquad \beta p = Ax, \qquad \alpha + \beta pc - \partial p^2 = 2Bx, \qquad \alpha c - \gamma p = Cx$$

sein, und wenn man also

$$\alpha - \beta pc + \delta p^2 = 2y$$

setzt, so folgt

$$y^2 + m'x^2 = p^2. \tag{17}$$

Hierin ist aber wegen (16) x und folglich auch y durch p teilbar, und (17) kann *nur* für $m' = 1$ befriedigt werden (da x nicht $= 0$ sein kann). Ist aber $m' = 1$, so ist $y = 0$, $x = \pm p$

$$\alpha = \pm pB, \qquad \beta = \pm A, \qquad \gamma = \pm Bc \mp C, \qquad \delta p = \mp B \pm Ac,$$

und es sind also für $m' = 1$, $p\omega'$ und $(\omega' + c) : p$ äquivalent, wenn c aus der Congruenz $Ac - B \equiv 0 \pmod p$ bestimmt wird (gilt auch für $p = 2$).

β) Es seien sodann

$$\frac{\omega' + c}{p}, \qquad \frac{\omega' + c'}{p}$$

äquivalent, also

$$\frac{\omega' + c}{p} = \frac{\gamma p + \delta(\omega' + c')}{\alpha p + \beta(\omega' + c')},$$

woraus wie oben folgt:

$$\beta = Ax, \qquad \alpha pc + \beta cc' - \gamma p^2 - \delta pc' = Cx$$

$$\alpha p + \beta c + \beta c' - \delta p = 2Bx \tag{18}$$

$$\alpha p - \beta c + \beta c' + \delta p = 2y$$

$$y^2 + m'x^2 = p^2 \tag{19}$$

Aus (18) ergiebt sich

$$Cx \equiv \beta cc', \qquad Ax \equiv \beta, \qquad 2Bx \equiv \beta(c + c') \pmod p. \tag{20}$$

Ist nun x nicht durch p teilbar, so folgt hieraus

$$C \equiv Acc'$$

$$2B \equiv A(c + c') \pmod p. \tag{21}$$

$$A^2(c - c')^2 \equiv -4m'$$

Die letztere Congruenz ist aber nur dann möglich, wenn entweder m' durch p teilbar, und dann ist $c = c'$, oder wenn $-m'$ quadratischer Rest von p ist, und dann ist

$$Ac - B \equiv \sqrt{-m'}, \qquad Ac' - B \equiv -\sqrt{-m'} \pmod{p}.$$

Diese beiden Werte von c sind aber in Folge von b) von dem System (12) oder (13) ohnehin auszuschliessen. Für $p = 2$ ergiebt sich ohne Weiteres nach der zweiten Congruenz (21) $c \equiv c' \pmod 2$.

Es bleibt also nur übrig, dass in (18), (19), (20) x durch p teilbar sei und folglich nach (19) $m' = 1$, $y = 0$, $x = \pm p$. Dann folgt aber

$$\alpha = \pm (B - Ac'), \qquad \gamma p = \mp (Acc' - Bc - Bc' + C)$$

$$\beta = \pm pA, \qquad \delta = \mp (B - Ac).$$

Es ergiebt sich also aus der Congruenz

$$Acc' - Bc - Bc' + C \equiv 0 \pmod{p} \tag{22}$$

zu jedem c *ein* c' (und umgekehrt), ausser wenn $Ac - B \equiv 0 \pmod p$ (in welchem Falle die Congruenz (22) unmöglich ist). Dieser Fall ist aber bereits unter α) erledigt. Die beiden nach (22) bestimmten Werte von c, c' sind nur dann einander gleich, wenn

$$(Ac - B)^2 \equiv -m' \pmod{p},$$

was aber nach b) ausgeschlossen ist. Das Ergebniss dieser Betrachtung ist also, dass unter den Grössen (13) (nach Ausschluss der wegen a), b), d) auszuschliessenden) nur dann äquivalente vorkommen, wenn $m' = 1$ ist, und dass in diesem Falle *je zwei* derselben äquivalent sind. Die Formeln (15) sind also richtig, ausser für $m' = 1$, und in diesem Falle treten an deren Stelle die folgenden:

$$\begin{aligned} h &= h' && \text{für} && p = 2 \\ h &= \frac{p-1}{2} h' && && \left(\frac{-1}{p}\right) = +1 \\ h &= \frac{p+1}{2} h' && && \left(\frac{-1}{p}\right) = -1. \end{aligned} \tag{23}$$

Hierdurch sind für den Fall negativer Determinanten die Verhältnisse der Classenzahlen abgeleitet für solche Determinanten, die in quadratischem Verhältniss stehen. (Vgl. DIRICHLET-DEDEKIND, *Vorl. über Zahlentheorie*, § 100.)

§ 20. *Hilfssätze aus der Theorie der algebraischen Functionen.*

Behufs einer weiteren Anwendung auf die complexe Multiplication schalte ich hier die Beweise einiger einfacher algebraischer Lehrsätze ein, wobei ich mich bezüglich der Terminologie und allgemeinen Voraussetzungen auf die ersten Paragraphen der von DEDEKIND und mir gemeinsam verfassten *Theorie der algebraischen Functionen* (Journal für Mathematik, Bd. 92, S. 181) berufen kann, ohne jedoch aus jener Theorie selbst etwas vorauszusetzen.

1°. Es sei v eine *ganze algebraische* Function von u, definirt durch die irreductible Gleichung

$$F(v, u) = v^\nu + a_1 v^{\nu-1} + a_2 v^{\nu-2} + \ldots + a_\nu = 0 \tag{1}$$

in welcher die $a_1, a_2, \ldots, a_\nu$ *ganze rationale* Functionen von u sind. Jede *ganze* Function M des durch (1) bestimmten Körpers algebraischer Functionen ist dann in der Form darstellbar

$$M = \frac{\psi(v, u)}{F'(v)} \tag{2}$$

worin ψ eine ganze rationale Function von v und u ist. Der Beweis dieser Behauptung ergiebt sich aus Folgendem. Beziehen wir das Zeichen Σ auf die sämmtlichen Wurzeln der Gleichung (1), so ist nach bekannten Sätzen

$$\begin{aligned} &\sum \frac{v^k}{F'(v)} = 0, \quad (0 \leqq k \leqq \nu - 2) \qquad \sum \frac{v^{\nu-1}}{F'(v)} = 1 \\ &\sum \frac{v^\nu}{F'(v)} = -a_1, \qquad \sum \frac{v^{\nu+1}}{F'(v)} = a_1^2 - a_2, \quad \ldots \end{aligned} \tag{3}$$

und allgemein, wenn $k \lessgtr \nu$

$$\sum \frac{v^k}{F'(v)}$$

eine ganze rationale Function von u.

Nun kann man immer, wenn $\alpha_0, \alpha_1, \ldots$ (ganze oder gebrochene) rationale Functionen von u bedeuten

$$M = \frac{\alpha_0 v^{\nu-1} + \alpha_1 v^{\nu-2} + \ldots + \alpha_{\nu-1}}{F'(v)} \tag{4}$$

setzen und aus (3) erhält man zur Bestimmung der $\alpha_0, \alpha_1, \ldots, \alpha_{\nu-1}$

$$\Sigma M = \alpha_0, \quad \Sigma vM = -\alpha_0 a_1 + \alpha_1, \quad \Sigma v^2 M = \alpha_0(a_1^2 - a_2) - \alpha_1 a_1 + \alpha_2, \ldots \tag{5}$$

Da nun die ΣM, ΣvM, $\Sigma v^2 M$, ... als ganze algebraische und zugleich rationale Functionen von u auch *ganze rationale* Functionen von u sind, so folgt dasselbe für die Coëfficienten $\alpha_0, \alpha_1, \alpha_2, \ldots$ w. z. b. w.

Auf Grund dieses Satzes kann man also auch setzen

$$M = \frac{\psi_1}{F'(v)}, \qquad M^2 = \frac{\psi_2}{F'(v)}, \qquad M^3 = \frac{\psi_3}{F'(v)}, \ldots \tag{6}$$

worin die $\psi_1, \psi_2, \psi_3, \ldots$ ganze rationale Functionen von u und v sind.

2°. Es sei die Function (1) in zwei Factoren zerlegt

$$F(v, u) = F_1(v) F_2(v) \tag{7}$$

$$\begin{aligned} F_1(v) &= (v - v_1)(v - v_2) \ldots (v - v_\lambda) = v^\lambda + \alpha_1 v^{\lambda-1} + \ldots + \alpha_\lambda \\ F_2(v) &= (v - v_{\lambda+1})(v - v_{\lambda+2}) \ldots (v - v_\nu) = v^{\nu-\lambda} + \beta_1 v^{\nu-\lambda-1} + \ldots + \beta_{\nu-\lambda}. \end{aligned} \tag{8}$$

Auf Grund von (6) kann man dann, wenn v einen der Werte $v_1, v_2, \ldots, v_\lambda$ hat, setzen:

$$M = \frac{\psi_1}{F_1'(v) F_2(v)}, \qquad M^2 = \frac{\psi_2}{F_1'(v) F_2(v)}, \qquad M^3 = \frac{\psi_3}{F_1'(v) F_2(v)}, \ldots$$

Setz man nun

$$F_2(v_1) F_2(v_2) \ldots F_2(v_\lambda) = P,$$

so ist P zunächst eine ganze rationale Function der α_ι, β_ι; und da (durch Ausführung der Division $F:F_1$) die β_ι ganz und rational durch die α_ι und a_ι bestimmbar sind, so kann P auch als *ganze rationale* Function der a_ι und α_ι, also auch als *ganze rationale* Function von u, α_1, α_2, ..., α_λ dargestellt werden. Ebenso schliesst man, dass das Product

$$P_1 = F_2(v_2) \ldots F_2(v_\lambda)$$

als symmetrische Function der Wurzeln der Gleichung

$$\frac{F_1(v)}{v - v_1} = 0$$

ganz und rational durch v_1, α_ι, a_ι ausgedrückt werden kann. Wenn also $\varphi_1(v)$, $\varphi_2(v)$, $\varphi_3(v)$, ... ganze rationale Functionen von u, v, α_1, α_2, ..., α_λ bedeuten, so hat man für $v = v_1, v_2, \ldots, v_\lambda$

$$(9) \qquad M = \frac{\varphi_1(v)}{PF_1'(v)}, \qquad M^2 = \frac{\varphi_2(v)}{PF_1'(v)}, \qquad M^3 = \frac{\varphi_3(v)}{PF_1'(v)}, \ \ldots$$

Die Functionen φ können vermittelst der Gleichung $F_1 = 0$ in die Form gesetzt werden

$$(10) \qquad \varphi_k = c_0^{(k)} v^{\lambda-1} + c_1^{(k)} v^{\lambda-2} + \ldots + c_{\lambda-1}^{(k)},$$

worin die $c_0^{(k)}$, $c_1^{(k)}$, ..., $c_{\lambda-1}^{(k)}$ ganze rationale Functionen von u, α_0, α_1, ..., α_λ sind. Aus (9) und (10) erhält man aber (mit Rücksicht auf (3)) die über $v_1, v_2, \ldots, v_\lambda$ erstreckten Summen:

$$(11) \qquad \Sigma M = \frac{c_0^{(1)}}{P}, \qquad \Sigma M^2 = \frac{c_0^{(2)}}{P}, \qquad \Sigma M^3 = \frac{c_0^{(3)}}{P}, \ \ldots,$$

und es genügen daher die Werte $M_1, M_2, \ldots, M_\lambda$ einer Gleichung λ^{ten} Grades

$$(12) \qquad \gamma_0 M^\lambda + \gamma_1 M^{\lambda-1} + \ldots + \gamma_{\lambda-1} M + \gamma_\lambda = 0,$$

in welcher die Coëfficienten $\gamma_0, \gamma_1, \ldots, \gamma_\lambda$ *ganze rationale* Functionen von $u, \alpha_1, \alpha_2, \ldots, \alpha_\lambda$ sind, und γ_0 *eine Potenz von* P. Die Zahlencoëfficienten in allen hier vorkommenden Functionen sind *rationale Zahlen*, wenn sie es in der ursprünglich gegebenen Gleichung (1) sind.

Wenn nun für einen speciellen Wert u_0 von u die λ Werte $v_1, v_2, \ldots, v_\lambda$ einander gleich, $= v_0$ werden, während $v_{\lambda+1}, v_{\lambda+2}, \ldots, v_\nu$ von v_0 verschieden sind, so wird P und folglich γ_0 für $u = u_0$ nicht verschwinden, und die zu $v = v_1, v_2, \ldots, v_\lambda$ gehörigen Werte der ganzen Function M, (die gleich oder verschieden sein können) werden durch eine Gleichung λ^{ten} Grades bestimmt, deren Coëfficienten rationale Functionen von u_0, v_0 sind. Ist ins Besondere $v_0 = u_0$, so sind die Coëfficienten dieser Gleichung rationale Functionen von u_0.

§ 21. *Zerfällung der Classengleichung in Factoren.*

Wir beschliessen diese Betrachtungen mit dem Beweise des schönen von KRONECKER entdeckten Satzes, dass die Classengleichung $H_m(u)$ nach Adjunction der Quadratwurzeln aus den in m aufgehenden Primzahlen in Factoren zerlegt werden kann, deren jeder die zu *einem Geschlecht* gehörigen Classeninvarianten zu Wurzeln hat. Es wird sich daraus zugleich ein neuer Beweis des zahlentheoretischen Satzes ergeben, dass in jedem der möglichen Geschlechter eine gleich grosse Anzahl von Classen enthalten ist.

1°. Es sei n eine *ungerade Quadratzahl* > 1, und

$$F_n(v, u) = 0 \tag{1}$$

die zu n gehörige Invariantengleichung. Die Wurzeln derselben sind, wenn $u = j(\omega)$ gesetzt wird

$$v = j\left(\frac{c + d\omega}{a}\right) \tag{2}$$

(auch wenn ω variabel ist), $ad = n$, und c möge $\equiv 0 \pmod 8$ angenommen werden.

Nach der Schlussbetrachtung der § 16 können die Functionen

$$M = \left(\frac{c}{e}\right) i^{3\frac{a-1}{2}} \sqrt{d^3} \left(\frac{\eta\left(\frac{c + d\omega}{a}\right)}{\eta(\omega)}\right)^3 \tag{3}$$

rational durch u, v ausgedrückt werden, und zwar mit rationalen Zahlencoëfficienten.

2°. Wir wollen nun in (1) für u eine zur Determinante $-m$ gehörige Classeninvariante, d. h. irgend eine Wurzel der Classengleichung

$$H_m(u) = 0 \tag{4}$$

setzen, also ω einer Gleichung unterwerfen

$$A\omega^2 + 2B\omega + C = 0, \qquad AC - B^2 = m, \tag{5}$$

und wollen darin, was stets erlaubt ist, A positiv und relativ prim zu $2m$ und zu n voraussetzen. Es ist zu untersuchen, welche von den Werten (2) gleich u werden. Dazu ist notwendig und hinreichend, dass die ganzen Zahlen α, β, γ, δ sich so bestimmen lassen, dass

$$\frac{c + d\omega}{a} = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}, \qquad \alpha\delta - \beta\gamma = 1. \tag{6}$$

Die Vergleichung von (5) und (6) liefert aber, wenn x, y ganze Zahlen *ohne gemeinsamen Teiler* sind, deren erste positiv genommen werden kann, (da α, β, γ, δ gleichzeitig mit entgegengesetztem Zeichen genommen werden können, ohne dass (6) sich ändert)

$$\begin{aligned} d\beta &= Ax, & c\beta - a\delta &= Bx + y \\ d\alpha &= Bx - y, & c\alpha - a\gamma &= Cx, \end{aligned} \tag{7}$$

und daraus

$$n = y^2 + mx^2. \tag{8}$$

Aus unserer Annahme über A folgt aber

$$d = 1, \qquad a = n, \tag{9}$$

und so können für jedes der Gleichung (8) genügende Wertpaar x, y (ohne gemeinsamen Teiler) α, β, γ, δ und c, und zwar letzteres eindeutig nach dem Modul n, durch die Gleichungen (7) bestimmt werden.

Es lässt sich auch leicht einsehen, dass zwei verschiedene Lösungen der Gleichung (8) nicht zu demselben c führen können; denn durch α, β, γ, δ, c sind nach (7) die beiden Zahlen x, y völlig bestimmt, x als

der grösste gemeinschaftliche Teiler von β, $\alpha + c\beta - n\delta$, $c\alpha - n\gamma$, und die Annahme einer Gleichung

$$\frac{\gamma + \delta\omega}{\alpha + \beta\omega} = \frac{\gamma' + \delta'\omega}{\alpha' + \beta'\omega}$$

führt, wenn der interesselose Fall $m = 1$ ausgeschlossen wird, zu $\alpha = \pm\alpha'$ $\beta = \pm\beta'$, $\gamma = \pm\gamma'$, $\delta = \pm\delta'$.

Die Anzahl der Werte v, die nach dieser Annahme $= u$ werden, ist also ebenso gross wie die Anzahl der eigentlichen Lösungen der Gleichung (8), wobei x positiv angenommen werden kann, y aber, wenn es nicht verschwindet, mit beiden Zeichen genommen werden muss.

3°. Die Werte von M, welche zu den gleich u werdenden Wurzeln v gehören, sind nach § 20 Wurzeln einer Gleichung

$$\Phi(M, u) = 0, \tag{10}$$

welche rational von u und rationalen Zahlen abhängt, deren Grad (in Bezug auf M) gleich der Anzahl der eigentlichen Lösungen der Gleichung (8) ist. Diese Werte von M können aber in Folge der Gleichung (6) nach § 5 (6) leicht bestimmt werden, und es ergiebt sich, wenn λ die dort (§ 5 (16)) angegebene Bedeutung hat, nach (3), (5), (7)

$$M = e^{\frac{\pi i(\lambda-3)}{4}} \left(\sqrt{ix\sqrt{m} - y}\right)^3, \tag{11}$$

worin die Quadratwurzel mit positivem reellem Teil zu nehmen ist. (In diesem Ausdruck ist von der speciellen Wahl der Classeninvariante u nur die Zahl λ abhängig.)

Es ist nun von Wichtigkeit, zu entscheiden, ob unter den Werten (11) solche sind, welche dieselbe 8^{te} Potenz haben. Dazu wäre erforderlich, dass für zwei verschiedene Paare x, y; x', y' von Lösungen der Gleichung (8)

$$(ix\sqrt{m} - y)^{12} = (ix'\sqrt{m} - y')^{12}$$

oder, wenn ρ eine zwölfte Einheitswurzel bedeutet

$$yy' + xx'm - i\sqrt{m}(xy' - yx') = \rho n. \tag{12}$$

Ist nun

a) $\rho = \pm 1$, so folgt hieraus sofort

$$x = x', \qquad y = y', \qquad \rho = 1$$

b) $\rho = \pm i\left(\frac{-1 \pm i\sqrt{3}}{2}\right)$ erweist sich sofort als unmöglich, da in (12) der reelle Teil auf der rechten Seite irrational, auf der linken rational wäre.

c) $\rho = \pm \frac{-1 \pm i\sqrt{3}}{2}$, $\sqrt{m}(yx' - xy') = \pm \frac{1}{2} n \sqrt{3}$, was unmöglich ist, da n ungerade vorausgesetzt war; es bleibt also noch

d) $\rho = \pm i$; $xx'm + yy' = 0$, $\sqrt{m}(yx' - xy') = \pm n$.

Dies ist also nur dann möglich, wenn m ein Quadrat und $\sqrt{m}$ in n enthalten ist. Aus der letzten Gleichung ergiebt sich aber noch durch Quadriren, mit Benutzung der Gleichungen

$$x^2m + y^2 = n, \qquad x'^2m + y'^2 = n, \qquad xx'm + yy' = 0:$$

$$n = m(x^2 + x'^2),$$

woraus hervorgeht, dass n auch durch m teilbar sein muss, und

$$y = \pm x'\sqrt{m}, \qquad y' = \mp x\sqrt{m}, \qquad x^2 + x'^2 = \frac{n}{m}.$$

Unter dieser Voraussetzung wird aber in Folge vom (7):

$$\begin{aligned} (Ac - B)x &\equiv y \\ (Ac' - B)x' &\equiv y' \end{aligned} \pmod{n},$$

woraus, wenn k, k' ganze Zahlen bedeuten

$$Ac - B = k\sqrt{m}, \qquad Ac' - B = k'\sqrt{m}$$

$$k - k' \equiv 0 \pmod{8A}$$

$$kx \equiv \pm x', \qquad k'x' \equiv \mp x \left(\mathrm{mod}\ \frac{n}{\sqrt{m}}\right)$$

$$(k - k')xx' \equiv \pm \frac{n}{m} \equiv 0 \left(\mathrm{mod}\ \frac{n}{\sqrt{m}}\right)$$

und da x, x' relativ prim zu n sein müssen, so folgt

$$k \equiv k' \left(\mathrm{mod}\ 8A\frac{n}{\sqrt{m}}\right).$$

Hiernach ist nun

$$\frac{c+\omega}{n} = \frac{Ac - B + i\sqrt{m}}{An} = \frac{k+i}{A\frac{n}{\sqrt{m}}}$$

$$\frac{c'+\omega}{n} = \frac{Ac' - B + i\sqrt{m}}{An} = \frac{k'+i}{A\frac{n}{\sqrt{m}}}$$

und folglich ist $M = M'$.

Hieraus ergiebt sich also, dass für keinen der Gleichung (4) *genügenden Wert von u zwei der vier Functionen*

$$\psi(M, u), \qquad \Phi(-M, u), \qquad \Phi(iM, u), \qquad \Phi(-iM, u)$$

zugleich verschwinden können.

4°. Wir zerlegen nun die als gegeben vorausgesetzte Zahl m in zwei Factoren

$$m = m'm'', \tag{13}$$

so dass m'' *ungerade und durch kein Quadrat* teilbar ist und setzen

$$x = 4, \qquad y = 4m' - m'' \tag{14}$$

$$\sqrt{ix\sqrt{m} - y} = 2i\sqrt{m'} + \sqrt{m''} \tag{15}$$

$$n = mx^2 + y^2 = (4m' + m'')^2, \tag{16}$$

und haben unter dieser Voraussetzung λ in der Formel (11) zu bestimmen (wobei zur Vereinfachung B gerade angenommen werden kann). Eine einfache Rechnung ergiebt

$$M = -\left(\frac{A}{m''}\right)\left(i^{\frac{m''+1}{2}}\, 2\sqrt{m'} + i^{\frac{m''-1}{2}}\sqrt{m''}\right)^3. \tag{17}$$

Setzt man den so gefundenen Wert von M in $\Phi(\pm M, u)$ ein, so muss für jede Wurzel der Gleichung $H_m(u) = 0$

$$\Phi(M, u) = 0 \quad \text{oder} \quad \Phi(-M, u) = 0$$

sein. Für keinen dieser Werte von u können aber diese beiden Gleichungen zugleich bestehen (nach 3°). Sucht man also den grössten gemeinschaftlichen Teiler $\Psi(M, u)$ von $H_m(u)$ und $\Phi(M, u)$, so ist dieser relativ prim zu $\Psi(-M, u)$.

Ist nun m' kein Quadrat und $m'' > 1$, so sind $\sqrt{m'}$, $\sqrt{m''}$ beide irrational und M ändert (nach (17)) sein Zeichen, wenn $\sqrt{m'}$, $\sqrt{m''}$, gleichzeitig die entgegengesetzten Werte erhalten. Da nun $H_m(u)$ rationale Coëfficienten hat, so ist es nicht nur durch $\Psi(M, u)$, sondern auch durch $\Psi(-M, u)$, und also auch durch das Product beider teilbar. Da überdies für jede Wurzel von $H_m(u) = 0$ eine der beiden Functionen $\Psi(\pm M, u)$ verschwinden muss, so ist

$$H_m(u) = \Psi(M, u)\Psi(-M, u) \tag{18}$$

und es folgt, *dass unter den sämmtlichen zur Determinante $-m$ gehörigen eigentlich primitiven Formenclassen jeder der beiden Charactere*

$$\left(\frac{A}{m''}\right) = \pm 1 \tag{19}$$

gleich oft vorkommt.

Ist m' ein Quadrat, also nach der Voraussetzung über m'' die grösste in m aufgehende Quadratzahl, und $m \equiv m'' \equiv 3 \pmod 4$ so ist

$$i^{\frac{m''+1}{2}}\sqrt{m'} \tag{20}$$

rational, und dieser Schluss ist nicht mehr anwendbar. In der That ist in diesem Falle für alle Formen der Determinante $-m$

$$\left(\frac{A}{m''}\right) = \left(\frac{A}{m}\right) = \left(\frac{-m}{A}\right) = 1. \tag{21}$$

In diesem Falle sind alle Charactere in der From

$$\left(\frac{A}{m''}\right) \tag{22}$$

enthalten, und die Zerlegung (18) genügt, um alle Geschlechter zu trennen.

Die Factorenzerfällung (18) gilt für *jede* Zerlegung von m in zwei Factoren m', m'', wenn

$$m \equiv 1 \pmod 4, \qquad m \equiv 2, 6 \pmod 8, \qquad m \equiv 4 \pmod{16}$$

weil im ersten und letzten dieser Fälle, auch wenn m' ein Quadrat ist, die Grösse (20) irrational ist, und in den beiden andern m' überhaupt kein Quadrat sein kann.

Da in diesen vier Fällen resp. die Characteren

$$(-1)^{\frac{1}{2}(A-1)}, \qquad (-1)^{\frac{1}{2}(A-1)+\frac{1}{8}(A^2-1)}, \qquad (-1)^{\frac{1}{8}(A^2-1)}, \qquad (-1)^{\frac{1}{2}(A-1)}$$

sich aus den Characteren von der Form (22) zusammensetzen lassen, so genügt die Zerfällung (18) zur vollständigen Trennung aller Geschlechter. Dagegen reicht für die Fälle $m \equiv 12 \pmod{16}$, $m \equiv 0 \pmod 8$ die Formel (17) nicht aus, um alle Geschlechter von einander zu trennen.

Man leitet daher auf dem gleichen Wege aus der Annahme

$$\begin{aligned} &x = 2, \qquad y = m' - m'', \qquad m' \equiv 0 \pmod 4 \\ &n = (m' + m'')^2, \qquad \sqrt{2i\sqrt{m} - y} = i\sqrt{m'} + \sqrt{m''} \end{aligned} \tag{23}$$

die Formel her:

$$M = (-1)^{\frac{1}{4}m}\left(\frac{2}{m''}\right)\left(\frac{A}{m''}\right)(-1)^{\frac{A-1}{2}}\left(i^{-\frac{m''-1}{2}}\sqrt{m'} + i^{-\frac{m''+1}{2}}\sqrt{m''}\right)^3 \tag{24}$$

welche für den Fall $m \equiv 12 \pmod{16}$ dasselbe leistet, wie die Formel (17) in der übrigen Fällen (wobei auch die Annahme $m'' = 1$ zu berücksichtigen ist).

Ist endlich $m \equiv 0 \pmod 8$, so setze man, indem man unter S^2 die grösste in m aufgehende Quadratzahl versteht

$$m = S^2P.$$

Ist dann $P \equiv 2$ oder $\equiv 6 \pmod 8$ so ist stets

$$(-1)^{\frac{A-1}{2}+\frac{A^2-1}{8}}\left(\frac{A}{P}\right) = 1, \qquad (-1)^{\frac{A^2-1}{8}}\left(\frac{A}{P}\right) = 1$$

und mit Hilfe dieser Relationen können alle Characteren auf eine der beiden Formen

$$\left(\frac{A}{m''}\right), \qquad (-1)^{\frac{A-1}{2}}\left(\frac{A}{m''}\right)$$

zurückgeführt werden. Da m' in diesen Fällen niemals ein Quadrat ist, so genügen die Formeln (17), (24) zur vollständigen Trennung der Ge-

schlechter und gestatten die früheren Schlüsse. Um aber für den Fall $m \equiv 0 \pmod 8$ eine stets ausreichende Formel zu erhalten, nehme man

$$x = 1, \qquad y = \frac{1}{4}m' - m'', \qquad n = \left(\frac{1}{4}m' + m''\right)^2 \cdot \tag{25}$$

$$\sqrt{ix\sqrt{m} - y} = \frac{1}{2}i\sqrt{m'} + \sqrt{m''},$$

woraus sich ergiebt

$$M = (-1)^{\frac{m}{8}} e^{-\frac{\pi i}{4}m''A}\left(\frac{A}{m''}\right)\left(i^{\frac{m''+1}{2}}\frac{1}{2}\sqrt{m'} + i^{\frac{m''-1}{2}}\sqrt{m''}\right)^3. \tag{26}$$

Nachdem die Zerlegung nach den Characteren $\left(\frac{A}{m''}\right)$ vermittelst der Formel (17) erledigt ist, handelt es sich nur noch um die Unterscheidung der dargestellten Zahlen A nach dem Modul 8. Dazu genügt es, in (26) $m'' = 1$, $m' = m$ zu setzen, wodurch sie in den vier Fällen die folgende Form annimmt:

$$\begin{aligned}
M &= (-1)^{\frac{m}{8}}\frac{1-i}{\sqrt{2}}\left(\frac{1}{2}i\sqrt{m}+1\right)^3 && A \equiv 1 \pmod 8\\
M &= (-1)^{\frac{m}{8}}\frac{-1-i}{\sqrt{2}}\left(\frac{1}{2}i\sqrt{m}+1\right)^3 = M', && A \equiv 3 \pmod 8\\
M &= (-1)^{\frac{m}{8}}\frac{-1+i}{\sqrt{2}}\left(\frac{1}{2}i\sqrt{m}+1\right)^3 = M'', && A \equiv 5 \pmod 8\\
M &= (-1)^{\frac{m}{8}}\frac{1+i}{\sqrt{2}}\left(\frac{1}{2}i\sqrt{m}+1\right)^3 = M''', && A \equiv 7 \pmod 8.
\end{aligned} \tag{27}$$

Die vier Werte von M gehen in einander über durch die Vertauschungen

$$\begin{array}{llll}
M, & \sqrt{2}, & i, & \sqrt{m}\\
M', & -\sqrt{2}, & -i, & -\sqrt{m}\\
M'', & -\sqrt{2}, & i, & \sqrt{m}\\
M''', & \sqrt{2}, & -i, & -\sqrt{m}.
\end{array} \tag{28}$$

Ist nun $\Psi(M, u)$ wie oben der grösste gemeinschaftliche Teiler von $H_{-}(u)$ und $\Phi(M, u)$, so folgt aus 3° dass die vier Functionen $\Psi(M, u)$,

$\Psi(M', u)$, $\Psi(M'', u)$, $\Psi(M''', u)$ zu einander relativ prim sind, und wenn die Vertauschungen (28) zulässig sind, so schliesst man wie oben

$$H_m(u) = \Psi(M, u)\Psi(M', u)\Psi(M'', u)\Psi(M''', u), \tag{29}$$

woraus also folgt, dass jeder der vier Fälle

$$A \equiv 1, \qquad A \equiv 3, \qquad A \equiv 5, \qquad A \equiv 7 \pmod 8$$

in gleich vielen Formenclassen der Determinante $-m$ vorkommt.

Die Vertauschungen (28) sind aber nur dann nicht alle zulässig, wenn m ein Quadrat oder das doppelte eines Quadrats ist. Im ersten Fall ist nur die Vertauschung (M, M''), im zweiten die (M, M') zulässig, und in diesen Fällen kommen auch in der That nur die Characteren vor

$$A \equiv 1, 5 \quad \text{resp.} \quad A \equiv 1, 3 \pmod 8,$$

und zwar wieder jeder derselben in gleich vielen Classen.

Da die Invarianten zweier entgegengesetzter Classen conjugirt imaginär, die der ambigen Classen reell sind, und da ferner zwei entgegengesetzte Classen zu demselben Geschlecht gehören, so haben alle die hier gefundenen Teilgleichungen reelle oder conjugirt imaginäre Wurzeln und folglich muss $\sqrt{-1}$ aus den Coëfficienten derselben sich fortheben.