Ueber die complexe Multiplication der elliptischen Functionen.

Von

G. PICK in Prag.

Das vorwiegende Ziel der folgenden Untersuchung ist, einen einfachen Beweis für jenen Hauptsatz aus der Theorie der complexen Multiplication zu geben, welcher gelegentlich von Abel*), angedeutet, späterhin von Herrn Kronecker**) nebst einer grossen Zahl weiterer Eigenschaften der Gleichungen für die singulären Moduln eingehend erörtert worden ist. Es hat jedoch bis heute an einer zusammenhängenden und systematischen Behandlung des Gegenstandes gefehlt. Nimmt man hinzu, dass die neueren Fortschritte der Theorie der elliptischen Functionen zu einer Umarbeitung jener Resultate in dem Sinne herausfordern, dass vor dem Eingehen auf κ^2 und höhere Functionen des Periodenquotienten zunächst die absolute Invariante $J^{***})$ in Betracht gezogen wird, so dürfte der nachfolgende Versuch gerechtfertigt erscheinen.

Es schien indess nicht blos der Vollständigkeit wegen passend, einige Angaben hinsichtlich der Aufstellung der Gleichungen der complexen Multiplication vorausgehen zu lassen. Denn obzwar, namentlich durch Hrn. Hermite†), in dieser Hinsicht alles Wünschenswerthe schon bekannt geworden ist, so konnte doch hier ein kürzeres Verfahren eingeschlagen werden, weil es heute unbedenklich erscheint, von den Modulargleichungen für J selbst den Ausgang zu nehmen.

Hinsichtlich der Voraussetzungen, welche zum Beweise des Hauptsatzes gemacht wurden, sei folgendes erwähnt. Die Theorie der Composition quadratischer Formen, wie sie in den Vorlesungen über Zahlentheorie von Dirichlet-Dedekind im X. Supplement dargestellt ist,

*) „Solution d'un problème etc.“ Oeuvres compl. I, S. 426.

**) Berliner Monatsberichte, Bdd. 1857, 1862, etc.

***) Nach der Bezeichnung von Hrn. Klein. Vgl. Math. Ann. Bd. XIV: „Ueber die Transformation der elliptischen Functionen etc.“

†) Comptes Rendus, t. 48, 49. (1859.)

wurde im Sinne der Anmerkung auf Seite 388 modificirt gedacht, um überall Formen erster und zweiter Art gemeinsam behandeln zu können.

Es darf ferner hervorgehoben werden, dass von einem Gebrauche des Satzes, dass durch jede Classe primitiver Formen Primzahlen dargestellt werden können, Umgang genommen worden ist.

Hinsichtlich der weiteren Ausführung der Theorie, namentlich in Hinblick auf die Irreducibilität und jene Zerlegung der Gleichungen complexer Multiplication, welche den Geschlechtern der quadratischen Formen entspricht, sei es gestattet, auf die Abhandlungen von Herrn Weber zu verweisen, welche nach der gütigen Mittheilung des Verfassers demnächst in den „Acta mathematica“ erscheinen sollen.

1.

Wenn für das Argument ω der elliptischen Modulfunction $J(\omega)$ die mit positivem imaginären Bestandtheil versehene Wurzel einer ganzzahligen quadratischen Gleichung

$$(1) \quad A + B\omega + C\omega^2 = 0$$

(von negativer Determinante) gesetzt wird, so kann $J(\omega)$ selbst als „singulärer Modul“ bezeichnet werden, analog der sonst für die Grösse κ^2 üblichen Sprechweise. Es empfiehlt sich indess anstatt $J(\omega)$ die Function

$$j(\omega) = 1728 J(\omega)$$

einzuführen, weil die singulären $j(\omega)$ ganze algebraische Zahlen sind, wie sich in der Folge zeigen wird.

Wir denken uns die Gleichungen von der Form (1) immer so geschrieben, dass A, B, C ohne gemeinsamen Theiler und dass A und C positiv sind. Wir werden uns dann des Ausdrucks bedienen, $j(\omega)$ gehöre zur Determinante

$$-\Delta = B^2 - 4AC,$$

und werden bisweilen zwischen singulären Moduln erster und zweiter Art unterscheiden, je nachdem die Form

$$[A, B, C] = A\omega_1^2 + B\omega_1\omega_2 + C\omega_2^2$$

von der ersten oder zweiten Art ist.

Einige Eigenschaften der Modulargleichungen sind für das folgende von Interesse. Bedeuten a, b, c, d vier ganze Zahlen ohne gemeinsamen Theiler von der Determinante

$$ad - bc = n > 0,$$

so besitzt die algebraische Gleichung $\Phi_n(j, \bar{j}) = 0$ zwischen

$$j = j(\omega)$$

und

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

folgende Beschaffenheit: Der Coefficient der höchsten vorkommenden Potenz von j' ist gleich Eins, während die Coefficienten der übrigen Potenzen ganze Functionen von j mit ganzzahligen Coefficienten sind. Ersetzt man ferner in

$$\Phi_n(j, j') = 0$$

j und j' durch denselben Buchstaben x , so erhält man eine ganzzahlige Gleichung für x , deren höchster Coefficient gleich Eins ist; und zwar ohne Weiteres im Allgemeinen, im Falle aber, dass n eine gerade Potenz einer Primzahl p ist, nach Weghebung des allen Gliedern gemeinsamen Factors p . Von der Richtigkeit dieser Behauptungen überzeugt man sich, wenn man die Form der Reihenentwicklung

$$j(\omega) = \frac{1}{q^2} \{1 + \gamma_1 q^2 + \gamma_2 q^4 + \dots\},$$

in welcher $\gamma_1, \gamma_2, \dots$ ganze Zahlen bedeuten, und die Rolle in Betracht zieht, welche dieselbe bei der wirklichen Aufstellung der Modulargleichungen spielt.

Zu jeder Classe primitiver Formen gehört ein bestimmter singulärer Werth von $j(\omega)$, und umgekehrt. Es ist daraus die Berechtigung des Ausdrucks klar, dass $j(\omega)$ mit einer bestimmten Classe componirt wird etc. In der That tritt für singuläre Moduln die Transformation in Beziehung zur Composition, wie genauer durch den folgenden Satz dargethan wird:

Durch Transformation n^{ter} Ordnung entstehen aus dem singulären Modul $j(\omega)$ von der Determinante $-\Delta$ alle und nur diejenigen zu derselben Determinante gehörigen Moduln, welche zahlentheoretisch aus $j(\omega)$ durch Composition mit denjenigen Formen der Determinante $-\Delta$ hervorgehen, durch welche n eigentlich darstellbar ist.

Um diesen für die Folge wichtigen Satz zu beweisen, erinnern wir daran, dass jedenfalls alle nicht äquivalenten Werthe des transformirten Periodenquotienten gefunden werden, indem man von den sämmtlichen mit dem ursprünglichen ω äquivalenten Werthen die n^{ten} Theile nimmt. Also sind in unserem Falle alle Formen der zu $j(\omega)$ gehörigen Classe hinsichtlich der Substitution

$$\begin{aligned} \omega_1 &= \omega'_1, \\ \omega_2 &= n \cdot \omega'_2 \end{aligned}$$

zu untersuchen. Es sei nun

$$[P, Q, R]$$

eine solche Form, so geht aus ihr die folgende

$$\left[\frac{P}{\tau}, \frac{nQ}{\tau}, \frac{n^2 R}{\tau} \right]$$

hervor, unter τ den grössten gemeinsamen Theiler von P, nQ, n^2R verstanden. Soll nun die neue Form zu derselben Determinante $-\Delta$ gehören, so ergibt sich $\tau = n$, so dass die Form lautet:

$$\left[\frac{P}{n}, Q, nR\right].$$

Es ist aber augenscheinlich das Resultat der Composition von

$$[P, Q, R] \quad \text{und} \quad \left[\frac{PR}{n}, Q, n\right]$$

ebenfalls

$$\left[\frac{P}{n}, Q, nR\right].$$

Umgekehrt, sei n durch eine Form der Determinante $-\Delta$ eigentlich darstellbar, so existirt eine Form der Gestalt

$$[P, Q, R],$$

worin P durch n theilbar ist und $\frac{P}{n}, Q, Rn$ ohne gemeinsamen Divisor sind, in jeder Classe der Determinante $-\Delta$. Denn um $[A, B, C]$ mit $[l, m, n]$ nach Dirichlet'scher Methode zu componiren, kann man zunächst eine zu $[A, B, C]$ äquivalente Form $[P, Q, R]$ so wählen, dass R gegen n relativ prim ist; dann aber wird nach Lösung der verträglichen Congruenzen

$$Q \equiv Q_1 \pmod{2R},$$

$$Q \equiv m \pmod{2n},$$

$$[P, Q, R] \text{ äquivalent mit } [P, Q, R],$$

$$[l, m, n] \text{ äquivalent mit } \left[\frac{PR}{n}, Q, n\right],$$

und das Resultat der Composition wird die Form

$$\left[\frac{P}{n}, Q, Rn\right],$$

deren Wurzel aus der von $[P, Q, R]$ auch durch Transformation n^{ter} Ordnung hervorgeht.

Zur Vervollständigung des auf solche Weise begründeten Satzes fragen wir noch, in welcher Multiplicität jede der so charakterisirten Wurzeln von

$$\Phi_n(j, j') = 0$$

auftritt. Versteht man unter ω das Argument von j , so stellen bekanntlich

$$\frac{1}{n} \omega \quad \text{und} \quad \frac{1}{n} \frac{\gamma + \delta \omega}{\alpha + \beta \omega}$$

dann und nur dann *verschiedene* Repräsentanten dar, wenn

$$\gamma \geq 0 \pmod{n}$$

ist. Sind also $[P, Q, R]$ und $[P', Q', R']$ zwei äquivalente Formen der Determinante $-\Delta$, worin P und P' durch n theilbar,

$$\left[\frac{PR}{n}, Q, n \right], \quad \left[\frac{P'R'}{n}, Q', n \right]$$

die zugehörigen transformirenden Compositionsformen, und endlich

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

die Substitution, welche $[P', Q', R']$ in $[P, Q, R]$ überführt, so hat man nur die Beschaffenheit von γ hinsichtlich des Moduls n zu untersuchen. Es ist aber

$$Q = 2P'\alpha\beta + Q'(\alpha\delta + \beta\gamma) + 2R'\gamma\delta,$$

oder

$$\begin{aligned} Q - Q' &= 2P'\alpha\beta + 2Q'\beta\gamma + 2R'\gamma\delta \\ &= 2P'\alpha\beta + 2\gamma(Q'\beta + R'\delta) \end{aligned}$$

und

$$P = P'\alpha^2 + \gamma(Q'\alpha + R'\gamma),$$

also

$$\left. \begin{aligned} Q - Q' &\equiv 2\gamma(Q'\beta + R'\delta) \\ 0 &\equiv 2\gamma(Q'\alpha + R'\gamma) \end{aligned} \right\} \pmod{2n}.$$

Aus der ersten dieser Congruenzen folgt, dass

$$Q' \equiv Q \pmod{2n},$$

falls γ durch n theilbar ist. Umgekehrt, ist $Q' - Q$ ein Multiplum von $2n$, so eliminire man aus den beiden Congruenzen einmal R' , das anderemal Q' , wodurch man erhält

$$\left. \begin{aligned} \gamma \cdot Q' &\equiv 0 \\ \gamma \cdot R' &\equiv 0 \end{aligned} \right\} \pmod{n}.$$

Da nun Q' und R' mit n (als Theiler von P') keinen Factor gemein haben können, so folgt nothwendig

$$\gamma \equiv 0 \pmod{n}.$$

Also liefert die Composition mit zwei Formen, welche n darstellen, denselben oder verschiedene Repräsentanten, jenachdem sie mit derselben oder mit verschiedenen Wurzeln der Congruenz

$$\xi^2 = -\Delta \pmod{2n}$$

gebildet sind.

2.

Sind

$$j_1, j_2, \dots, j_{h_A}$$

die sämmtlichen h_A zur Determinante $-\Delta$ gehörigen singulären Moduln, so wird die Gleichung

$$F_A(x) = (x - j_1)(x - j_2) \cdots (x - j_{n_A}) = 0$$

die zur Determinante $-\Delta$ gehörige „Gleichung der complexen Multiplication“ genannt. Die Mittel zur Aufstellung und einige elementare Eigenschaften dieser Gleichungen sollen zunächst erörtert werden.

Die Wurzeln der schon früher erwähnten Gleichungen

$$\Phi_n(x, x) = 0$$

sind sämtlich singuläre Moduln*). Denn soll ω mit $\frac{1}{n} \frac{\gamma + \delta \omega}{\alpha + \beta \omega}$ äquivalent sein, so muss es offenbar einer ganzzahligen quadratischen Gleichung genügen. Um zu entscheiden, durch welche singuläre Moduln $\Phi_n(x, x) = 0$ befriedigt wird, hat man nach dem früheren nur zu fragen, welches die Determinanten $-\Delta$ sind, durch deren Hauptclassen n darstellbar ist. Man erhält demnach als nothwendige und hinreichende Bedingung

$$n = \frac{\Delta}{4} t^2 + u^2,$$

bzw.

$$n = \frac{\Delta + 1}{4} t_1^2 + t_1 u_1 + u_1^2,$$

unter t, u , resp. t_1, u_1 ganze Zahlen ohne gemeinsamen Theiler verstanden, je nachdem es sich um Moduln erster Art [$\Delta \equiv 0 \pmod{4}$] oder solche zweiter Art [$\Delta \equiv -1 \pmod{4}$] handelt. Wir fragen ferner nach der Multiplicität der so bezeichneten Wurzeln von $\Phi(x, x) = 0$. Da nun

$$\begin{aligned} \frac{d\Phi_n(x, x)}{dx} &= \left[\frac{\partial \Phi_n(j, j')}{\partial j} + \frac{\partial \Phi_n(j, j')}{\partial j'} \right]_{j=j'=x} \\ &= 2 \left[\frac{\partial \Phi_n(j, j')}{\partial j'} \right]_{j=j'=x}, \end{aligned}$$

so sieht man, dass x dann und nur dann eine mehrfache Wurzel von $\Phi_n(x, x) = 0$ ist, wenn $j' = x$ eine mehrfache Wurzel von

$$\Phi_n(x, j') = 0$$

ist. Hier tritt nun das am Schlusse des vorigen Paragraphen angegebene Criterium in Kraft; und zwar ergibt eine ganz einfache Discussion der Gleichungen

$$\begin{cases} \alpha\delta - \beta\gamma = 1, \\ Q = 2 \frac{\Delta}{4} \alpha\beta + 2\gamma\delta, \\ n = \frac{\Delta}{4} \beta^2 + \delta^2, \end{cases}$$

*) Vgl. hiezu und wegen des folgenden auch Gierster, Math. Ann. XXI. „Ueber Classenzahlrelationen“.

resp.

$$\begin{cases} \alpha\delta - \beta\gamma = 1, \\ Q = 2 \frac{\Delta+1}{4} \alpha\beta + (\alpha\delta + \beta\gamma) + 2\gamma\delta, \\ n = \frac{\Delta+1}{4} \beta^2 + \beta\delta + \delta^2, \end{cases}$$

welche aussagen, dass $\left[\frac{Q^2 + \Delta}{4n}, Q, n\right]$ der bezüglichen Hauptklasse angehört, folgendes: Die *einfachen* Wurzeln von $\Phi_n(x, x) = 0$ sind

- 1) Die zur Determinante $-4n$ gehörigen singulären Moduln (erster Art),
- 2) wenn $n \equiv -1 \pmod{4}$, die zur Determinante $-n$ gehörigen Moduln (zweiter Art); hievon ist jedoch der Fall auszunehmen, dass n das dreifache eines vollständigen Quadrates ist, in welchem nämlich diese Moduln *dreifache* Wurzeln von $\Phi_n(x, x) = 0$ sind.

Hieraus ergeben sich folgende Regeln zur Gewinnung der Gleichungen der complexen Multiplication:*)

- 1) Wenn $\Delta \equiv 0, 4, 8 \pmod{16}$, erhält man das Polynom $F_{\frac{\Delta}{4}}(x)$, indem man in bekannter Weise aus $\Phi_{\frac{\Delta}{4}}(x, x)$ das Product der *einfachen* Linearfactoren abscheidet.
- 2) Wenn $\Delta \equiv -4 \pmod{16}$, ergibt eben dieses Verfahren zunächst $F_{\frac{\Delta}{4}}(x) \cdot F_{\frac{\Delta}{4}}(x)$; hier ist dann das Polynom $\Phi_{\frac{\Delta+4}{16}}(x, x)$ zu Hilfe zu nehmen, welches durch $F_{\frac{\Delta}{4}}(x)$ theilbar, gegen $F_{\frac{\Delta}{4}}(x)$ jedoch theilerfremd ist. Hierdurch ist auch zugleich
- 3) Der Fall $\Delta \equiv -1 \pmod{4}$ erledigt, wofern nicht
- 4) $\Delta \equiv -1 \pmod{4}$ das dreifache eines vollständigen Quadrats ist. Dann aber erhält man $F_{\frac{\Delta}{4}}(x)$ als Product der in $\Phi^d(x, x)$ *dreifach* auftretenden Linearfactoren, wie leicht zu sehen ist.

Aus einer früher angegebenen Eigenschaft der Gleichungen $\Phi_n(x, x) = 0$ folgt, dass die *singulären Moduln ganze algebraische Zahlen sind*.

Die Gleichungen $F_{\frac{\Delta}{4}}(x) = 0$ lassen sich demnach so schreiben, dass der Coefficient der höchsten vorkommenden Potenz von x gleich Eins, die übrigen ganze rationale Zahlen sind.

Hinsichtlich der Realität der singulären Moduln lässt sich noch ein sehr einfaches Gesetz angeben. Ist nämlich $j(\omega)$ reell, so liegt einer der zugehörigen Werthe des Arguments ω auf der Axe der imaginären Zahlen oder auf einer zu ihr im Abstände $-\frac{1}{2}$ parallelen Geraden. Die zugehörige Form $[P, Q, R]$ besitzt dann offenbar die Eigenschaft, dass

*, Wobei jedoch von den Werthen $j = 1728$ und 0 abgesehen ist.

$$Q \equiv 0 \pmod{R}$$

ist. Umgekehrt giebt es in jeder ambigen Classe Formen, welche diese Eigenschaft besitzen. Es folgt somit:

Die reellen singulären Moduln gehören zu den ambigen Classen und umgekehrt.

3.

Wir unterwerfen nun irgend eine Wurzel j_0 der Gleichung

$$F_A(x) = 0$$

einer Transformation von dem ungeraden Primzahlgrade p , wobei p nicht in Δ enthalten und $\left(\frac{-\Delta}{p}\right) = +1$ sein soll. Unter den Wurzeln j' der Gleichung

$$\Phi_p(j_0, j') = 0$$

befinden sich nach den Ausführungen des ersten Paragraphen zwei welche zugleich der Gleichung

$$F_A(j') = 0$$

genügen, nämlich diejenigen, welche aus j_0 durch Composition mit den Formen

$$\left[\frac{Q^2 + \Delta}{4p}, \pm Q, p \right]$$

hervorgehen, wo selbstverständlich

$$Q^2 \equiv -\Delta \pmod{2p}.$$

Wenn nun erstens eine dieser Formen (und folglich beide) der ambigen Classe P angehört, so sind jene beiden Wurzeln j' einander gleich und die Gleichungen

$$\begin{aligned} F_A(j') &= 0, \\ \Phi_p(j_0, j') &= 0 \end{aligned}$$

besitzen nur eine gemeinsame Lösung j_1 , welche sich folglich als rationale Function von j_0 mit rationalen Zahlencoefficienten darstellen lässt:

$$j_1 = P(j_0).$$

Die Berechtigung diese Relation so zu bezeichnen ist klar; denn die beiden Gleichungen, deren gemeinsamer Linearfactor

$$j' - P(j_0)$$

ist, sind ganz unabhängig von der Wahl des Moduls j_0 , und nur bestimmt durch Angabe von p , oder, was hier dasselbe ist, der Form P .

Ist zweitens keine der beiden p darstellenden Formenklassen ambig, so sind dieselben verschieden und können mit den Symbolen

$$P \text{ und } P^{-1}$$

bezeichnet werden. Dann ist der grösste gemeinsame Theiler von $F_{\mathcal{A}}(j')$ und $\Phi_p(j_0, j')$ ein Polynom zweiten Grades in j' mit rationalen ganzzahligen Functionen von j_0 als Coefficienten:

$$j'^2 + A(j_0)j' + B(j_0);$$

setzt man dieses Polynom gleich Null, so besitzt die entstandene Gleichung die Wurzeln j_1, j_{-1} , welche symbolisch durch

$$\begin{aligned} j_1 &= P \cdot j_0, \\ j_{-1} &= P^{-1} \cdot j_0 \end{aligned}$$

zu bezeichnen sind.

Es folgt nun unmittelbar, dass die Wurzeln der Gleichung

$$j'^2 + A(j_1)j' + B(j_1) = 0$$

folgende Grössen sind:

$$\begin{aligned} P \cdot P \cdot j_0 &= j_2 = P^2 \cdot j_0, \\ P^{-1} \cdot P \cdot j_0 &= j_0, \end{aligned}$$

und so fort. Wir können also sagen, dass aus der Reihe der Grössen

$$(I) \quad \dots j_{-2}, j_{-1}, j_0, j_1, j_2, \dots, ^*)$$

welche aus einer von ihnen, etwa j_0 , durch wiederholte Composition mit der Form P hervorgehen:

$$j_r = P^r \cdot j_0,$$

je zwei, deren Index um Zwei verschieden ist, Wurzeln einer Gleichung sind, deren Coefficienten rational mittelst rationalen Zahlen in der dazwischenliegenden Grösse darstellbar sind. Offenbar folgt ferner, dass durch zwei aufeinanderfolgende Glieder jener Reihe jedes andere rational (und mit rationalen Zahlencoefficienten) ausgedrückt werden kann:

$$j_{\kappa+r} = C_r(j_{\kappa}, j_{\kappa+1}),$$

wobei die Form der Function C_r einzig von dem Index r abhängig ist.

Die quadratischen Gleichungen, welche auf solche Weise erhalten sind, lassen sich nun durch ein eigenthümliches Verfahren auflösen. Es sei p^{λ} die niedrigste Potenz von p , welche durch die Hauptklasse darstellbar ist, so dass also P zum Exponenten λ gehört. Unter dieser Voraussetzung wiederholen sich die Grössen der Reihe (I) immer nach je λ Gliedern. Es ist also

$$j_{\kappa+\lambda} = j_{\kappa},$$

und nützlich zu bemerken, dass $\lambda > 2$ ist, weil andernfalls die Form P ambig wäre. Zu jeder Transformation p^{λ} ten Grades, durch welche aus j_r wieder $j_{\kappa}(=j_{\kappa+\lambda})$ hervorgeht, gehört ein bestimmter Multiplikator, auf dessen Berechnung es für die Erledigung unserer Absicht

*) Wegen dieses Arrangements vgl. Joubert, Comptes Rendus, t. 50 (1860).

ankommt. Bezeichnet man allgemein mit M den Multiplicator einer Transformation n ten Grades

$$\omega_1' = a\omega_1 + b\omega_2,$$

$$\omega_2' = c\omega_1 + d\omega_2,$$

bei welcher

$$\frac{\omega_2'}{\omega_1'} = \frac{\omega_2}{\omega_1} = \omega$$

ein zulässiges Werthesystem bildet, so ist

$$M\omega_1 = \omega_1',$$

$$M\omega_2 = \omega_2',$$

also zunächst

$$M = a + b\omega.$$

Bildet man nun mit Hülfe der Modulargleichung

$$\Phi_n(j, j') = 0$$

den Differentialquotienten $\frac{dj'}{dj}$ für die betrachteten Specialwerthe

$$j = j' = j(\omega),$$

so ergibt sich mit Rücksicht auf

$$\omega' = \frac{c + d\omega}{a + b\omega},$$

an welche Relation ja auch die benachbarten Werthe gebunden sind,

$$\left(\frac{dj'}{dj}\right)_{j'=j} = \frac{d\omega'}{d\omega},$$

oder

$$(M) \quad \left(\frac{dj'}{dj}\right)_{j'=j} = \frac{n}{M^2} *).$$

In dem speciellen Falle unserer Transformation von der Ordnung p^2 , stellt nun das Werthesystem $j = j_*$, $j' = j_*$ einen Doppelpunkt der Curve

$$\Phi_{p^2}(j, j') = 0$$

dar, weil nach den im ersten Paragraphen entwickelten Kriterien $x = j_*$ eine doppelt zählende Wurzel jeder der beiden Gleichungen

$$\Phi_{p^2}(x, j_*) = 0, \quad \Phi_{p^2}(j_*, x) = 0$$

bildet. Hier besitzt also die linke Seite der Gleichung (M) zwei Werthe, und entsprechend muss auch M^2 für diesen Fall eine zweideutige Grösse sein. Es kommt nun alles darauf an, jene Gleichung durch genaue

*) Vgl. die allgemeine Formel z. B. bei Hurwitz, Math. Ann. Bd. XVIII, „Independent Theorie der Modulfunctionen etc.“ Sie ist hier von Anfang hergeleitet worden, weil ohnedies über eine eventuell hinzutretende 6te Wurzel der Einheit Zweifel entstehen könnten.

Bestimmung beider Seiten aus einer scheinbar vierdeutigen Beziehung in zwei eindeutige zu verwandeln. Zu diesem Zwecke zerlegen wir die in Rede stehende Transformation $p^{\lambda\text{ter}}$ Ordnung in jene λ Transformationen p^{ter} Ordnung, welche λ aufeinanderfolgenden Compositionen mit der Form P äquivalent sind. Die Grösse j_x geht dann durch die Reihe der Zwischengrössen

$$j_{x+1}, j_{x+2}, \dots, j_{x+\lambda-1}$$

in $j_{x+\lambda} = j_x$ selbst über. Die im Sinne der Gleichung

$$\Phi_p(j, j') = 0$$

gebildeten Differentialquotienten

$$\left(\frac{dj'}{dj}\right)_{j=j_{x+q}} \\ j'=j_{x+q+1}$$

sind *eindeutig* durch die jeweils beteiligten Argumente bestimmt, und das Product

$$\prod_{q=0}^{\lambda-1} \left(\frac{dj'}{dj}\right)_{j=j_{x+q}} \\ j'=j_{x+q+1}$$

stellt einen der beiden Werthe der linken Seite von (M) dar. Den zugehörigen Werth von M^2 erhält man wohl am kürzesten durch das folgende Verfahren. Es sei

$$[MNp^{\lambda-1}, Q, p]$$

eine Form der Classe P ,

$$[Mp^{\lambda}, Q, N]$$

eine der zu j_x gehörigen Formen. In solche Gestalt lassen sich Formen der betreffenden Classen stets bringen, wie eine ganz elementare Ueberlegung zeigt. Es geht $[Mp^{\lambda}, Q, N]$ in die äquivalente Form über durch λ -malige Composition mit $[MNp^{\lambda-1}, Q, p]$, oder durch einmalige Composition mit $[M, N, Q, p^{\lambda}]$. Man erhält durch Zusammenziehung aller bei diesen Compositionen auftretenden Identitäten:

$$\left\{ \begin{array}{l} \left(\omega_1 - \frac{\omega_2}{\omega^{(x)}}\right) \cdot \left[\frac{Q - \sqrt{-\Delta}}{2} \Omega_1 + p^{\lambda} \Omega_2\right] \\ \qquad \qquad \qquad = \left(\omega_1' - \frac{\omega_2'}{\omega^{(x)'}}\right) \cdot \left[\frac{Q - \sqrt{-\Delta}}{2} \Omega_1' + p \Omega_2'\right]^{\lambda}, \\ \left(\omega_1 - \frac{\omega_2}{\omega^{(x)}}\right) \cdot \left[\frac{Q + \sqrt{-\Delta}}{2} \Omega_1 + p^{\lambda} \Omega_2\right] \\ \qquad \qquad \qquad = \left(\omega_1' - \frac{\omega_2'}{\omega^{(x)'}}\right) \cdot \left[\frac{Q + \sqrt{-\Delta}}{2} \Omega_1' + p \Omega_2'\right]^{\lambda}, \end{array} \right.$$

wo $\omega^{(x)}$, $\bar{\omega}^{(x)}$ die beiden Wurzeln der Form

$$[Mp^2, Q, N]$$

$\omega_1, \omega_2; \omega_1', \omega_2'; \Omega_1, \Omega_2; \Omega_1', \Omega_2'$ dagegen Veränderliche bedeuten, welche an die folgenden Relationen gebunden sind. Es ist erstens aus ω_1', ω_2' mittelst der Grössen Ω_1', Ω_2' ein neues Zahlenpaar

$$\begin{aligned}\omega_1'' &= (Q\Omega_1 + p\Omega_2) \omega_1' + N\Omega_1 \cdot \omega_2', \\ \omega_2'' &= -Mp^{\lambda-1}\Omega_1 \cdot \omega_1' + \Omega_2 \cdot \omega_2'\end{aligned}$$

zu bilden, dann aus diesem ein weiteres

$$\begin{aligned}\omega_1''' &= (Q\Omega_1 + p\Omega_2) \omega_1'' + Np\Omega_1 \cdot \omega_2'', \\ \omega_2''' &= -Mp^{\lambda-2}\Omega_1 \cdot \omega_1'' + \Omega_2 \cdot \omega_2'',\end{aligned}$$

und ähnlich fortzufahren; das auf solche Weise erhaltene Zahlenpaar $\omega_1^{(\lambda+1)}, \omega_2^{(\lambda+1)}$ ist nun gleich zu setzen den Ausdrücken

$$\begin{aligned}(Q\Omega_1 + p^\lambda\Omega_2) \cdot \omega_1 + N\Omega_1 \cdot \omega_2, \\ -M\Omega_1 \cdot \omega_1 + \Omega_2 \cdot \omega_2.\end{aligned}$$

Es sei jetzt

$$\Omega_1' = 0, \quad \Omega_2' = 1,$$

und für Ω_1, Ω_2 ein Zahlenpaar t, u genommen, welches eine Darstellung der Zahl 1 durch die Form $[MN, Q, p^\lambda]$ vermittelt. Dann gehen die Identitäten über in

$$\left\{ \begin{aligned} \left(\omega_1 - \frac{\omega_2}{\omega^{(x)}} \right) \cdot \left[\frac{Q - \sqrt{-\Delta}}{2} t + p^\lambda u \right] &= p^\lambda \left(\omega_1' - \frac{\omega_2'}{\omega^{(x)}} \right), \\ \left(\omega_1 - \frac{\omega_2}{\omega^{(x)}} \right) \cdot \left[\frac{Q + \sqrt{-\Delta}}{2} t + p^\lambda u \right] &= p^\lambda \left(\omega_1' - \frac{\omega_2'}{\omega^{(x)}} \right), \end{aligned} \right.$$

während die zugehörigen Relationen jetzt einfach lauten

$$\begin{aligned}p^\lambda \cdot \omega_1' &= (Qt + p^\lambda t) \omega_1 + Nt \cdot \omega_2, \\ \omega_2' &= -Mt \cdot \omega_1 + u \cdot \omega_2.\end{aligned}$$

Da nun

$$(Qt + p^\lambda u) \cdot u - Nt (-Mt) = MNt^2 + Qtu + p^\lambda u^2$$

den Werth Eins besitzt, so stellen diese Relationen nichts anderes als eine Transformation $p^{\lambda \text{ter}}$ Ordnung vor. Es zeigt ferner die erste der Identitäten, dass für

$$\frac{\omega_2'}{\omega_1'} = \omega^{(x)},$$

auch

$$\frac{\omega_2}{\omega_1} = \omega^{(x)}$$

wird. Setzt man endlich, diese Specialwerthe im Auge behaltend,

$$\begin{aligned}\omega_1 &= M \cdot \omega_1', \\ \omega_2 &= M \cdot \omega_2'\end{aligned}$$

in die zweite Identität ein, so erhält man für den Multiplikator

$$M = \frac{p^2}{\frac{Q + \sqrt{-\Delta}}{2} t + p^2 u}.$$

Dieser Werth ist nun in der That bis auf sein Vorzeichen unveränderlich, wenn auch für Ω_1', Ω_2' ein anderes Zahlenpaar, welches eine Darstellung von p durch die Form $[MNp^{2-1}, Q, p]$ bildet, für t, u ein anderes Zahlenpaar, welches eine Darstellung von 1 durch $[MN, Q, p^2]$ bildet, eingesetzt wird. Und ferner ist unmittelbar ersichtlich, dass der gefundene Multiplikator einzig und allein von den Zahlen p, Q , das heisst von der Form P abhängig ist, und zwar so, dass er, vom Vorzeichen abgesehen, in den conjugirten Werth übergeht, wenn man das Vorzeichen von Q ändert, also P in P^{-1} übergehen lässt.

Man drücke nun in der Gleichung

$$(M') \quad \prod_{q=0}^{\lambda-1} \left(\frac{dj'}{dj} \right)_{j=j_x+q}^{j=j_x+q+1} = p^{-\lambda} \left(\frac{Q + \sqrt{-\Delta}}{2} t + p^2 u \right)^2$$

die Grössen $j_{x+2}, j_{x+3}, \dots, j_{x+\lambda-1}$ in der früher besprochenen Weise durch j_x und j_{x+1} aus. Dann stellt diese Gleichung eine Bestimmungsgleichung für

$$j_{x+1} = P \cdot j_x$$

vor, welcher nicht zugleich durch

$$j_{x-1} = P^{-1} \cdot j_x$$

genügt wird, weil nach der obigen Auseinandersetzung mit dem Uebergange von P in P^{-1} auch die rechte Seite der Gleichung in den conjugirten Werth sich verwandelt. Daher kann man mit Zuhilfenahme von

$$j_{x+1}^2 + A(j_x) j_{x+1} + B(j_x) = 0$$

j_{x+1} rational durch j_x ausdrücken, wobei aber die Coefficienten mit der Irrationalität $\sqrt{-\Delta}$ behaftet erscheinen:

Wir sind nun in der Lage folgendermassen zusammenzufassen:

Jeder symbolischen Relation

$$j' = P \cdot j$$

entspricht eine wirkliche

$$j' = P(j),$$

wobei $P(z)$ eine durch die Formenclasse P vollständig bestimmte*) rationale Function bedeutet, deren Coefficienten dem Zahlenkörper angehören, welcher durch $\sqrt{-\Delta}$ bezeichnet ist.

*) Bis auf Veränderungen mittelst der Gleichung $F_{\mathcal{A}}(j) = 0$.

4.

Es seien nun j und j' zwei beliebig ausgewählte Wurzeln von

$$F_A(x) = 0,$$

und es sei A die Formenklasse, mit welcher j zu componiren ist, um in j' überzugehen:

$$j' = A \cdot j$$

in symbolischer Schreibweise. Es sei ferner die der Classe A angehörige Form

$$[M, Q, a]$$

so ausgewählt, dass

$$a = p^\pi \cdot p'^{\pi'} \dots$$

eine ungerade gegen Δ theilerfremde Zahl ist. Man hat dann

$$\left[\frac{Ma}{p}, Q, p\right]^\pi \cdot \left[\frac{Ma}{p'}, Q, p'\right]^{\pi'} \dots = [M, Q, a],$$

oder

$$A = P^\pi \cdot P'^{\pi'} \dots,$$

wo somit $P, P', \dots$ Formenklassen bezeichnen, durch welche beziehungsweise die Primzahlen $p, p', \dots$ darstellbar sind. Durch wiederholte Anwendung des im vorigen Paragraphen bewiesenen Satzes ist es nun offenbar möglich, die Grösse

$$j' = P^\pi \cdot P'^{\pi'} \dots j$$

rational mit in $\sqrt{-\Delta}$ rationalen Coefficienten durch j auszudrücken:

$$j' = A(j).$$

Zugleich wird ersichtlich, dass die Function $A(z)$ nur von der Formenklasse A und nicht von j abhängig ist, weil auch die Functionen $P(z), P'(z), \dots$, aus welchen sie sich zusammensetzt, den Formenklassen $P, P', \dots$ correspondiren, und von den jeweiligen Argumenten unabhängig sind. Die verschiedenen Zerlegungen der Classe A , welche durch verschiedene Auswahl der darstellbaren Zahl a erhalten werden können, führen nothwendig zu identischen Resultaten hinsichtlich der rationalen Function $A(z)$. Denn alle auf solche Weise sich ergebenden Functionen bewirken bei den *sämmtlichen* Wurzeln von

$$F_A(x) = 0$$

immer dieselben Wertänderungen, und sind also mit Rücksicht auf die Gleichung identisch.

Das System der Functionen $A_1(z), A_2(z), \dots$, welches durch die vorigen Betrachtungen gefunden ist, bildet eine Gruppe, welche mit der „Gruppe der Composition“ für die Determinante $-\Delta$ holodrisch isomorph ist. Denn offenbar folgt aus der Relation

$$A_r \cdot A_s = A_t$$

zwischen drei Formenklassen, die gleichbedeutende zwischen den entsprechenden rationalen Functionen.

Es übertragen sich somit alle Eigenschaften der Gruppe der Composition auf die Gruppe jener Functionen. Für die Gleichungen der complexen Multiplication kann man somit etwa folgenden Satz aussprechen:

Die Gleichung

$$F_A(x) = 0$$

wird durch Adjunction der Quadratwurzel aus $-\Delta$ zu einer Abel'schen Gleichung.

Das ist gleichbedeutend mit dem Satze, welchen Abel in der Form ausspricht:

„Toutes ces valeurs sont exprimables par des radicaux).*“

Prag, im November 1884.

*) Während des Druckes vorliegender Untersuchung ist eine erste Abhandlung von Hrn. Weber erschienen (Acta math. VI, 4), in welcher die Zerlegung der in Rede stehenden Gleichungen nach den Geschlechtern der Formen gelehrt wird; hingegen sind die Bestimmung der Gruppe jener Gleichungen und fernere algebraisch-zahlentheoretische Sätze für eine zweite Abhandlung in Aussicht gestellt. Durch briefliche Mittheilung von Hrn. Weber war ich in der angenehmen Lage die im Texte verwendeten Bezeichnungen mit den seinigen insofern in Uebereinstimmung zu bringen, als $j(\omega)$ an beiden Orten dieselbe Bedeutung besitzt.

Es sei noch erlaubt, auf eine inzwischen erschienene Note in den Berichten der sächsischen Gesellschaft d. Wissenschaften zu verweisen (Sitzung vom 12. Januar 1885), in welcher ich einen Beweis für die Irreducibilität der Gleichungen der complexen Multiplication in seinen Grundzügen zu geben versucht habe.

[Febr. 1885.]