# ELLIPTISCHE
# FUNCTIONEN
UND
# ALGEBRAISCHE ZAHLEN.

# ELLIPTISCHE
# FUNCTIONEN
UND
# ALGEBRAISCHE ZAHLEN.

ACADEMISCHE VORLESUNGEN

VON

## H. WEBER,

Professor der Mathematik an der Universität Marburg.

BRAUNSCHWEIG,
DRUCK UND VERLAG VON FRIEDRICH VIEWEG UND SOHN.
1891.

# VORREDE.

Das Werk, welches hiermit an die Oeffentlichkeit tritt, setzt sich zum Ziele, den Leser in die Lehre von den elliptischen Functionen und ihre Anwendungen, besonders auf Algebra und Zahlentheorie, einzuführen. Es setzt zwar einige Uebung und Schulung in der höheren Mathematik, nicht aber Kenntnisse in den elliptischen Functionen voraus. Es ist mein Bestreben gewesen, die Theorie vollständig und leicht verständlich, wenn auch in knapper Form zu entwickeln und dem Leser mitzutheilen, was für den Gebrauch der elliptischen Functionen nach irgend einer Richtung hin als wesentlich erschien. Wo Hülfsmittel aus anderen Gebieten der Mathematik nothwendig sind, war ich bemüht, diese dem Leser möglichst bequem an die Hand zu geben, und, wo es erforderlich war, besonders im dritten Theil, auf bekannte und leicht zugängliche Lehrbücher zu verweisen. Im Uebrigen sind Literaturangaben nur hin und wieder und ohne Anspruch auf Vollständigkeit gegeben.

Um den in Aussicht genommenen Umfang des Werkes nicht zu überschreiten und doch die Hauptaufgabe nicht zu kurz kommen zu lassen, konnte den Anwendungen der elliptischen Functionen auf Geometrie und Mechanik nur ein kleiner Platz eingeräumt werden; nur zwei Beispiele zur Belebung des Vortrages sind gegeben. Diese Beschränkung konnte um so eher eintreten, da in dem zweiten Bande von Halphen's „Traité des fonctions elliptiques“ diese Anwendungen in ausführlichster Weise behandelt sind. Auch zu diesem Werke wird, wie wir hoffen, trotz der Verschiedenheit der Darstellung der Leser durch das vorliegende Werk das Verständniss geebnet finden.

Der in Aussicht gestellte dritte Band von Halphen's Werk sollte ein ähnliches Ziel verfolgen wie unser Buch, und als ich die Ausarbeitung unternahm, freute ich mich eines solchen Mitstreiters. Tief ergriffen hat mich über der Arbeit die Nachricht von dem vorzeitigen Tode des trefflichen Mannes, der uns in den beiden ersten Bänden seines leider unvollendeten Werkes ein edles Denkmal seines Geistes und seiner Arbeitskraft hinterlassen hat.

Der leichteren Uebersicht wegen ist unser Werk in drei Theile getheilt, die in Rücksicht auf die hauptsächlich zur Anwendung kommenden Hülfsmittel als analytischer, algebraischer und zahlentheoretischer Theil bezeichnet sind, ohne dass damit eine scharfe Trennung ausgedrückt sein soll. Der verschiedene Standpunkt der drei Theile liesse sich auch so charakterisiren, dass im ersten Theil die elliptischen Functionen als Functionen von zwei Veränderlichen, des Arguments und des Moduls, betrachtet werden; der zweite Theil ist wesentlich solchen Functionen gewidmet, welche nur von einer Variablen, dem Modul, abhängen, während im dritten Theil die algebraischen Zahlen betrachtet werden, die man erhält, wenn der Modul einen besonderen ausgezeichneten Zahlenwerth hat.

Der Gegenstand, welchen der dritte Theil behandelt, gehört zu denen, welche noch nicht zum Gemeingut weiterer mathematischer Kreise geworden sind, und wir hoffen, dass unsere Arbeit zur Verbreitung und Belebung der Theilnahme an diesem weiten und schönen Gebiet beitragen möge. Diese Betrachtungen knüpfen an die von Abel bereits gekannte sogenannte complexe Multiplication der elliptischen Functionen an. Die Sätze, die Abel darüber in fragmentarischer Form und andeutungsweise hinterlassen hat, waren lange Zeit wenig bekannt und wenig verstanden. Die Arbeiten von Hermite und Joubert haben das Interesse und das Verständniss für diese Fragen gefördert. Am meisten aber verdankt die Theorie der complexen Multiplication den Forschungen von Kronecker, welche nicht nur die Sätze von Abel vollständig bewiesen, sondern auch die tieferen Beziehungen dieser Lehre zur Algebra und Zahlentheorie aufgedeckt haben. Die Kronecker'schen Arbeiten sind auch für unseren dritten Theil von maassgebendem Einfluss gewesen.

Während meiner langjährigen Beschäftigung mit den elliptischen Functionen in eigenen Arbeiten und in Lehrvorträgen habe ich die meisten Gegenstände, die den Inhalt des vorliegenden Werkes bilden, in mündlichem und schriftlichem Verkehr mit meinem Freunde Dedekind oft und eingehend besprochen. Seiner Anregung und Belehrung verdanke ich manchen Fortschritt und manchen neuen Gesichtspunkt. Besonders ist Dedekind's Theorie der algebraischen Zahlen, wie sie in der dritten Auflage von Dirichlet's Vorlesungen über Zahlentheorie dargestellt ist, mir ein werthvolles Hülfsmittel geworden. Auch bei der Correctur des Druckes stand mir Dedekind's unermüdliche Hülfe zur Seite, die mir von grossem Nutzen gewesen ist.

Es bleibt mir noch übrig, der Verlagsbuchhandlung für die Ausstattung des Werkes und für die Bereitwilligkeit, mit der sie meinen Wünschen entgegengekommen ist, meinen Dank auszusprechen.

Marburg, im November 1890.

**H. Weber.**

# INHALT.

---

## I. Analytischer Theil.

### Erster Abschnitt.

### Die elliptischen Integrale.

### Zweiter Abschnitt.

### Theta-Functionen.

## Dritter Abschnitt.

## Die Transformation der Theta-Functionen.

## Vierter Abschnitt.

## Die elliptischen Functionen.

## Fünfter Abschnitt.

## Die Modulfunctionen.

## Sechster Abschnitt.

## Einige Anwendungen der elliptischen Functionen.

# II. Algebraischer Theil.

## Siebenter Abschnitt.

## Hülfssätze aus der Algebra.

## Achter Abschnitt.

## Multiplication und Theilung der elliptischen Functionen.

## Neunter Abschnitt.

## Theorie der Transformationsgleichungen.

### Zehnter Abschnitt.

### Die Gruppe der Transformationsgleichungen und die Gleichung fünften Grades.

---

## III. Zahlentheoretischer Theil.

### Elfter Abschnitt.

### Complexe Multiplication.

### Zwölfter Abschnitt.

### Berechnung von Classeninvarianten.

## Dreizehnter Abschnitt.

## Die Multiplicatorgleichung in der complexen Multiplication und die Zerfällung der Classengleichung in Factoren.

## Vierzehnter Abschnitt.

## Galois'sche Gruppe der Classengleichung.

## Fünfzehnter Abschnitt.

## Die Normen der Classeninvarianten $f(\omega)$.

## Sechzehnter Abschnitt.

## Theilung der elliptischen Functionen mit singulären Moduln.

## Anhang.

---

# Berichtigungen.

Seite 8. In den beiden letzten Formeln (8) muss rechts das negative Zeichen stehen.

Seite 51. In der zweiten Formel (7) muss $e^{\pi i g_1}$ statt $e^{-\pi i g_1}$ stehen.

Seite 127. In der ersten Formel (15) muss $\frac{\operatorname{cn} v \operatorname{dn} v}{\operatorname{sn} v}$ statt $\frac{\operatorname{cn} v \operatorname{dn} v}{\operatorname{cn} v}$ stehen.

Seite 243. In der ersten Formel (6) muss $\frac{f(n\,\omega')}{f(\omega')^n}$ statt $\frac{f(n\,\omega')}{f(\omega')}$ stehen.

# I.

# ANALYTISCHER THEIL.

# Erster Abschnitt.

# Die elliptischen Integrale.

## §. 1. Definition der elliptischen Integrale.

Wenn in einer systematischen Darstellung der Integralrechnung die Entwickelung bis zu dem Punkte gelangt ist, wo algebraische Integrale, welche die Quadratwurzel aus einer Function ersten oder zweiten Grades enthalten, auf Integrale rationaler Functionen zurückgeführt werden, so tritt an dieser Stelle dem Lernenden eine Schranke entgegen, die er mit den ihm bis dahin zu Gebote stehenden Hülfsmitteln nicht zu übersteigen im Stande ist. Das Streben nach einer Erweiterung der Hülfsmittel, um auch noch die nächste Classe von Integralen der Forschung zugänglich zu machen, ist, wie es historisch der Anlass gewesen zu einem eingehenderen Studium der elliptischen Integrale und zur Einführung der elliptischen Functionen, auch der naturgemässeste und verständlichste Ausgangspunkt für den, der in die Theorie dieser Functionen zuerst eingeführt werden soll. Es soll daher auch unsere nächste Aufgabe sein, uns mit den elliptischen Integralen und ihren wichtigsten Eigenschaften bekannt zu machen.

Die Definition eines elliptischen Integrals, von der wir ausgehen wollen, ist die folgende. Es bedeute $f(x)$ eine ganze rationale Function dritten oder vierten Grades ohne quadratischen Theiler

(1) $$f(x) = a_0\, x^4 + 4\, a_1\, x^3 + 6\, a_2 x^2 + 4\, a_3\, x + a_4,$$

worin $a_0$ und $a_1$ nicht beide zugleich verschwinden, und $\Phi(x, y)$ eine beliebige ganze oder gebrochene rationale Function der beiden Argumente $x$, $y$. Dann ist

$$\int \Phi\left(x, \sqrt{f(x)}\right) dx$$

das allgemeinste von uns hier zu betrachtende elliptische Integral, und

$$\Phi\left(x, \sqrt{f(x)}\right) dx$$

heisst das elliptische Differential. Es lässt sich nun aber dies allgemeine Integral auf wesentlich einfachere zurückführen. Zunächst lässt sich $\Phi$ in die Form setzen:

$$\frac{A + B\sqrt{f(x)}}{C + D\sqrt{f(x)}},$$

worin $A$, $B$, $C$, $D$ ganze rationale Functionen von $x$ sind, und indem man diesen Bruch mit $C - D\sqrt{f(x)}$ erweitert, in die Form

$$\Psi(x) + \frac{\Phi(x)}{\sqrt{f(x)}},$$

worin $\Psi(x)$ und $\Phi(x)$ ganze oder gebrochene rationale Functionen von $x$ sind. Wir lassen nun das Integral

$$\int \Psi(x)\, dx,$$

welches auf Logarithmen und algebraische Functionen führt, ausser Betracht, und befassen uns nur noch mit dem elliptischen Integral

$$\int \frac{\Phi(x)\, dx}{\sqrt{f(x)}} \tag{2}$$

oder dem entsprechenden elliptischen Differential

$$\Phi(x)\frac{dx}{\sqrt{f(x)}}. \tag{3}$$

Es ist für viele Zwecke vortheilhaft, dies Differential in der homogenen Form zu betrachten; zu diesem Ende setzen wir für $x$ das Verhältniss zweier Variablen $x:y$ und demnach für $dx$

$$\frac{y\,dx - x\,dy}{y^2}.$$

Ist dann

$$f(x, y) = a_0 x^4 + 4a_1 x^3 y + 6a_2 x^2 y^2 + 4a_3 x y^3 + a_4 y^4$$

und $\Phi(x, y)$ eine homogene Function 0 ter Ordnung, so erhält unser elliptisches Differential die Gestalt

$$\Phi(x, y)\frac{y\,dx - x\,dy}{\sqrt{f(x, y)}}. \tag{4}$$

Die Aufgabe, die uns nun zunächst beschäftigen wird, ist eine doppelte: Es soll durch Einführung neuer Veränderlicher das Differential

$$(5)\qquad \frac{y\,dx - x\,dy}{\sqrt{f(x,y)}}$$

in ein anderes von derselben Form transformirt werden, worin aber die Function unter dem Quadratwurzelzeichen möglichst vereinfacht und besonders von einer möglichst kleinen Zahl von Parametern abhängig gemacht wird (§. 3, §. 4). Es soll zweitens das allgemeine Differential (3) oder (4) in andere ähnliche zerlegt werden, in welchen die Function $\Phi(x)$ oder $\Phi(x, y)$ möglichst einfach ist (§. 8).

Die Function $f(x)$ oder $f(x, y)$ wird bisweilen in ihre linearen Factoren aufgelöst vorausgesetzt, wo wir dann setzen werden:

$$f(x) = a_0\,(x-\alpha)\,(x-\beta)\,(x-\gamma)\,(x-\delta)$$

$$f(x, y) = (x y_1 - y x_1)\,(x y_2 - y x_2)\,(x y_3 - y x_3)\,(x y_4 - y x_4).$$

## §. 2. Doppelverhältnisse.

Um die Lage eines veränderlichen Punktes $X$ auf einer gegebenen geraden Linie zu bestimmen, nimmt man am einfachsten auf der Geraden einen festen Punkt $A$ an, und misst die Entfernung $(A, X)$ der Punkte $A$ und $X$, welche man positiv nennt, wenn $X$ auf der einen, etwa der rechten Seite von $A$ liegt, und negativ im entgegengesetzten Falle. Statt dessen ist es oft vorzuziehen, wie es in der analytischen Geometrie in neuerer Zeit vielfach und mit bestem Erfolg geschieht, auf unserer Geraden zwei feste Punkte $A$, $B$ anzunehmen, und mit $x$, $y$ die mit zwei beliebigen constanten Factoren multiplicirten, oder in zwei verschiedenen Maasseinheiten gemessenen Abstände des Punktes $X$ von $A$ und $B$ zu bezeichnen, so dass zwischen $x$, $y$ eine lineare Relation von der Form

$$a x + b y = 1$$

besteht, deren geometrische Bedeutung ist:

$$(A, X) - (B, X) = (A, B),$$

und die dazu verwandt werden kann, einen nicht homogenen Ausdruck in $x$, $y$ in einen homogenen zu verwandeln. Von dieser Bestimmungsweise des Punktes $X$ kommt man zu der zuerst erwähnten gewöhnlichen zurück, wenn man den Punkt $B$ ins

Unendliche rücken und die ihm entsprechende Maassconstante gleichzeitig unendlich abnehmen lässt, so dass $y$ sich einem constanten Werthe nähert und $= 1$ gesetzt werden kann. Die Grössen $x$, $y$ wollen wir die Coordinaten des Punktes $X$ nennen.

Wenn wir nun statt des Paares $A$, $B$ ein anderes Punktepaar $A'$, $B'$ auf der Geraden annehmen, und mit $\xi$, $\eta$ die Coordinaten desselben $X$, bezogen auf die Punkte $A'$, $B'$ bezeichnen, so ist, wie eine sehr einfache geometrische Betrachtung zeigt, die wir dem Leser überlassen,

$$\begin{aligned} x &= \alpha\xi + \beta\eta \\ y &= \gamma\xi + \delta\eta, \end{aligned} \tag{1}$$

worin $\alpha$, $\beta$, $\gamma$, $\delta$ Constanten sind, welche bei gehöriger Wahl der Punkte $A'$, $B'$ jedes beliebige Werthsystem erhalten können, dessen Determinante

$$r = \alpha\delta - \beta\gamma \tag{2}$$

von Null verschieden ist. Sind 1, 2 zwei Punkte mit den Coordinaten $x_1$, $y_1$; $x_2$, $y_2$, so ist

$$x_1\, y_2 - x_2\, y_1 = r(\xi_1\, \eta_2 - \xi_2\, \eta_1) \tag{3}$$

eine Grösse, welche von dem Abstande (1, 2) der beiden Punkte nur durch einen constanten Factor verschieden ist; hiernach ist, wenn 1, 2, 3, 4 irgend vier Punkte sind

$$\begin{aligned} \frac{x_1 y_3 - x_3 y_1}{x_1 y_4 - x_4 y_1} : \frac{x_2 y_3 - x_3 y_2}{x_2 y_4 - x_4 y_2} &= \frac{\xi_1 \eta_3 - \xi_3 \eta_1}{\xi_1 \eta_4 - \xi_4 \eta_1} : \frac{\xi_2 \eta_3 - \xi_3 \eta_2}{\xi_2 \eta_4 - \xi_4 \eta_2} \\ &= \frac{(1,3)}{(1,4)} : \frac{(2,3)}{(2,4)} \end{aligned} \tag{4}$$

eine von der Wahl des Coordinatensystems gänzlich unabhängige Grösse, und sie ist die einfachste Grösse dieser Art, welche zugleich der Bedingung genügt, nur von dem Verhältniss der Coordinaten sämmtlicher darin vorkommender Punkte abzuhängen. In der Geometrie ist dieser Ausdruck unter dem Namen des Doppelverhältnisses des Punktepaares 1, 2 zum Punktepaar 3, 4 wohl bekannt.

Homogene Functionen der Coordinaten eines oder mehrerer Punkte, welche beim Uebergang zu einem anderen Coordinatensystem ungeändert bleiben oder eine Potenz von $r$ als Factor annehmen, heissen Covarianten.

## §. 3. Die Legendre'sche Normalform.

Die einfachste Covariante, die sich bilden lässt, ist die Determinante

$$x_1 y_2 - x_2 y_1,$$

die in der Folge zur Abkürzung mit

$$(x_1 y_2)$$

bezeichnet sein soll. Dahin gehört auch das Differential

$$x\,dy - y\,dx = (x\,dy) = x^2 d\frac{y}{x}$$

und daher auch das elliptische Differential

$$(1)\quad du = \frac{x\,dy - y\,dx}{\sqrt{(xy_1)(xy_2)(xy_3)(xy_4)}} = \frac{1}{r}\,\frac{\xi\,d\eta - \eta\,d\xi}{\sqrt{(\xi\,\eta_1)\,(\xi\,\eta_2)\,(\xi\,\eta_3)\,(\xi\,\eta_4)}},$$

worin 1, 2, 3, 4 beliebig gegebene Punkte, $x$, $y$ ein veränderlicher Punkt. Hierin ist das Vorzeichen der einen Quadratwurzel durch das der anderen bestimmt aus der Gleichung

$$\sqrt{(x y_1)\,(x y_2)\,(x y_3)\,(x y_4)} = r^2 \sqrt{(\xi\,\eta_1)\,(\xi\,\eta_2)\,(\xi\,\eta_3)\,(\xi\,\eta_4)}.$$

Machen wir zur Vereinfachung des elliptischen Differentials die lineare Substitution

$$x = (\xi\,\eta_1),\quad y = (\xi\,\eta_2),\quad r = (\xi_1\,\eta_2),$$

so wird

$$\begin{aligned} x_1 &= 0, & x_2 &= -r, & x_3 &= (\xi_3\,\eta_1), & x_4 &= (\xi_4\,\eta_1) \\ y_1 &= r, & y_2 &= 0, & y_3 &= (\xi_3\,\eta_2), & y_4 &= (\xi_4\,\eta_2). \end{aligned}$$

Setzt man noch

$$(2)\qquad z = \frac{x_3\,y}{y_3\,x},$$

$$(3)\qquad \varkappa^2 = \frac{y_3\,x_4}{x_3\,y_4},$$

so ergiebt sich die Transformation des elliptischen Differentials in die Normalform:

$$(4)\qquad \frac{(\xi\,d\eta - \eta\,d\xi)\sqrt{(\xi_1\,\eta_3)\,(\xi_2\,\eta_4)}}{\sqrt{(\xi\,\eta_1)\,(\xi\,\eta_2)\,(\xi\,\eta_3)\,(\xi\,\eta_4)}} = \frac{dz}{\sqrt{z\,(1-z)\,(1-\varkappa^2 z)}}.$$

$$(5)\qquad \varkappa^2 = \frac{(\xi_1\,\eta_4)\,(\xi_2\,\eta_3)}{(\xi_1\,\eta_3)\,(\xi_2\,\eta_4)}.$$

$$(6)\qquad z = \frac{(\xi_1\,\eta_3)\,(\xi\,\eta_2)}{(\xi_2\,\eta_3)\,(\xi\,\eta_1)}.$$

Auf der linken Seite der beiden letzten Formeln stehen Doppelverhältnisse, und daher dürfen die Covarianten $(\xi_i\,\eta_h)$ durch die Entfernungen $(i, h)$ der beiden Punkte $i$, $h$ ersetzt werden, wenn gleichzeitig $(\xi\,\eta_i)$ durch die Entfernung $(x, i)$ des Punktes $X$ von $i$ ersetzt wird. Das Gleiche ist auch auf der linken Seite der Formel (4) gestattet, wenn für das Differential $(\xi\,d\eta)$ das Differential $dx$ der Entfernung des Punktes $X$ von einem festen Punkte gesetzt wird.

Danach lassen sich die Formeln (5), (6) in noch übersichtlicherer Weise schreiben, und wir fügen drei weitere Formeln hinzu, die aus der Gleichheit von Doppelverhältnissen oder mit Hülfe der Eigenschaft der Covarianten aus (2) und (3) sofort abzuleiten sind. Zu bemerken ist, dass die in diesen Ausdrücken vorkommenden Symbole $(i, h)$ nach Belieben Entfernungen von Punkten oder die bei irgend einer Coordinatenbestimmung aus den Coordinaten dieser Punkte gebildeten Determinanten $\xi_i\,\eta_h - \xi_h\,\eta_i$ bedeuten können.

$$\varkappa^2 = \frac{(1,4)\,(2,3)}{(1,3)\,(2,4)},\quad 1-\varkappa^2 = \frac{(1,2)\,(3,4)}{(1,3)\,(2,4)}, \tag{7}$$

$$z = \frac{(1,3)\,(x,2)}{(2,3)\,(x,1)},$$

$$1 - z = \frac{(1,2)\,(x,3)}{(2,3)\,(x,1)}, \tag{8}$$

$$1 - \varkappa^2 z = \frac{(1,2)\,(x,4)}{(2,4)\,(x,1)},$$

und die Formel (4) lautet in derselben Bezeichnung

$$\frac{dx\sqrt{(1,3)\,(2,4)}}{\sqrt{(x,1)\,(x,2)\,(x,3)\,(x,4)}} = \frac{dz}{\sqrt{z(1-z)\,(1-\varkappa^2 z)}}. \tag{9}$$

Diese Form des elliptischen Differentials nennen wir die Legendre'sche Normalform. Die Grösse $\varkappa$ heisst der Modul des elliptischen Differentials, $\sqrt{1-\varkappa^2}$, was auch mit $\varkappa'$ bezeichnet wird, das Complement des Moduls.

Da die vier Punkte 1, 2, 3, 4 sich auf 24 verschiedene Arten anordnen lassen, und jeder solchen Anordnung eine lineare Transformation auf die Normalform entspricht, so giebt es 24 solcher Transformationen; unter diesen sind vier, nämlich

$$(1, 2, 3, 4),\ (2, 1, 4, 3),\ (3, 4, 1, 2),\ (4, 3, 2, 1),$$

welche dasselbe Modulquadrat $\varkappa^2$ ergeben, während die übrigen in

Gruppen von je vieren zerfallen, welche je dasselbe Modulquadrat geben. Man erhält so bei allen diesen Transformationen sechs verschiedene Modulquadrate, die, wenn $\varkappa^2$ das erste ist, folgenden Ausdruck haben:

$$\varkappa^2,\quad 1-\varkappa^2,\quad \frac{1}{\varkappa^2},\quad \frac{1}{1-\varkappa^2},\quad \frac{\varkappa^2-1}{\varkappa^2},\quad \frac{\varkappa^2}{\varkappa^2-1}.$$

Ebenso besteht zwischen der Variablen $z$ einer beliebigen dieser Transformationen und der ersten ein linearer Zusammenhang.

Man übersieht am leichtesten diese Transformationen, wenn man annimmt, dass das zu transformirende Integral bereits die Normalform hat. Die auf diese Weise entstehenden 24 linearen Transformationen aus der Normalform in die Normalform heissen die Fundamentaltransformationen. Wir betrachten hier drei unter ihnen als Beispiele, aus denen, wie wir später sehen werden, die übrigen leicht hergeleitet werden können.

Es sei also

$$(x, 1)\,(x, 2)\,(x, 3)\,(x, 4) = x\,y\,(x-y)\,(x-\lambda^2 y).$$

Die Nullpunkte der vier Factoren $x, y, x-y, x-\lambda^2 y$ bezeichnen wir durch die Verhältnisse ihrer Coordinaten $\infty$, 0, 1, $1:\lambda^2$, und ordnen diesen die Punkte 1, 2, 3, 4 in den Formeln (7), (8), (9) in folgender Weise zu:

|  | $\infty$, | 0, | 1, | $\frac{1}{\lambda^2}$ |
|---|---|---|---|---|
| 1) | 3, | 2, | 1, | 4 |
| 2) | 1, | 2, | 4, | 3 |
| 3) | 4, | 3, | 2, | 1 |

Setzt man noch

$$\zeta = \frac{y}{x},$$

so ergeben die Formeln (7), (8), (9) in diesen drei Fällen die folgenden Resultate:

$$1)\qquad \varkappa^2 = \lambda'^2,\qquad z = \frac{-\zeta}{1-\zeta},$$

$$2)\qquad \varkappa^2 = \frac{1}{\lambda^2},\qquad z = \lambda^2\,\zeta,$$

$$3)\qquad \varkappa^2 = \lambda^2,\qquad z = \frac{1-\zeta}{1-\lambda^2\zeta},$$

während das Differential

$$\frac{dz}{\sqrt{z(1-z)(1-\varkappa^2 z)}}$$

in den drei Fällen in

$$\frac{i\,d\zeta}{\sqrt{\zeta(1-\zeta)\,(1-\lambda^2\zeta)}},\quad \frac{\lambda\,d\zeta}{\sqrt{\zeta\,(1-\zeta)\,(1-\lambda^2\zeta)}},\quad \frac{d\zeta}{\sqrt{\zeta(1-\zeta)\,(1-\lambda^2\zeta)}}$$

transformirt wird. Die Abhängigkeit der Vorzeichen dieser Quadratwurzeln ergiebt sich aus den Umformungen selbst, wenn für $dz : d\zeta$ der Werth eingesetzt wird.

Die hier betrachteten Umformungen sind in ihrem analytischen Charakter keineswegs von der Voraussetzung bedingt, dass die Punkte 1, 2, 3, 4 reelle Punkte seien. Wenn wir aber diese Annahme machen, so sind noch einige Bemerkungen hinzuzufügen.

Folgen sich die Punkte 1, 2, 3, 4 in dieser Reihenfolge auf der sie tragenden geraden Linie auf einander, etwa von links nach rechts, so werden $\varkappa^2$ und $\varkappa'^2$ beide positiv und folglich auch, da ihre Summe gleich Eins ist, echt gebrochen. Dieselbe Eigenschaft kommt acht unter den 24 Fundamentaltransformationen zu, nämlich denjenigen, welche $\varkappa^2$ ungeändert lassen oder $\varkappa^2$ mit $\varkappa'^2$ vertauschen. Die Werthreihe von 0 bis 1 der Variablen $z$ entspricht in diesen 8 Transformationen den Intervallen (2, 3), (3, 4), (4, 1), (1, 2) und (3, 2), (2, 1), (1, 4), (4, 3) (wobei der Uebergang von 4 zu 1 oder von 1 zu 4 durch das Unendliche stattfindet), wie man aus den Zählern in den beiden ersten Formeln (8) erkennt.

Durch eine quadratische Transformation lassen sich auf den Fall der reellen Punkte auch die beiden Fälle zurückführen, in welchen zwei der vier Punkte, etwa 1, 2, reell sind, während 3, 4 ein conjugirt imaginäres Paar bilden, oder wo 1, 2 und 3, 4 zwei conjugirt imaginäre Paare bilden. In diesen beiden Fällen existirt bekanntlich ein reelles zu den Punktepaaren 1, 2 und 3, 4 gleichzeitig harmonisches Punktepaar, und wenn wir dies Paar zu Grundpunkten $A$, $B$ machen, so erhalten die vier Punkte die Coordinaten

$$x_1,\ y_1;\quad x_1,\ -y_1;\quad x_3,\ y_3;\quad x_3,\ -y_3;$$

im ersten der erwähnten Fälle ist $y_3$, im zweiten $y_1$ und $y_3$ rein imaginär, also sind die Quadrate stets reell. Demnach wird das elliptische Differential (1)

$$du = \frac{x\,dy - y\,dx}{\sqrt{(x^2\,y_1^2 - y^2\,x_1^2)\,(x^2\,y_3^2 - y^2\,x_3^2)}},$$

welches durch die Substitution

$$z = \frac{y^2}{x^2}$$

in die Form übergeht:

$$du = \frac{dz}{2\sqrt{z(y_1^2 - x_1^2 z)(y_3^2 - x_3^2 z)}},$$

und hier stehen unter dem Wurzelzeichen drei reelle lineare Factoren.

## §. 4. Die Weierstrass'sche Normalform.

Eine zweite Normalform des elliptischen Differentials, welche besonders in den Weierstrass'schen Untersuchungen über elliptische Functionen eine wichtige Rolle spielt, und daher die Weierstrass'sche Normalform heissen soll, ist die folgende:

$$\frac{dz}{\sqrt{4z^3 - g_2 z - g_3}}. \tag{1}$$

Die Coëfficienten $g_2$, $g_3$ in dieser Form werden die Invarianten genannt und die Verbindung derselben $\varDelta = g_2^3 - 27 g_3^2$ die Discriminante des elliptischen Differentials. Wir haben nun zu untersuchen, wie die allgemeine Form in diese besondere zu transformiren ist. Eine Umformung, welche dies leistet, ist in unserer allgemeinen Formel (1) des vorigen Paragraphen enthalten. Setzen wir dort

$$\begin{aligned} x &= \xi\alpha + \eta\beta \\ y &= \xi\eta_1 - \eta\xi_1 \end{aligned} \tag{2}$$

$$r = \alpha\xi_1 + \beta\eta_1 \tag{3}$$

$$z = \frac{x}{y}, \tag{4}$$

so erhält die linke Seite von jener Formel die Gestalt

$$\frac{-dz}{\sqrt{-r\,(z y_2 - x_2)\,(z y_3 - x_3)\,(z y_4 - x_4)}},$$

worin

$$x_2 = \alpha\xi_2 + \beta\eta_2, \quad x_3 = \alpha\xi_3 + \beta\eta_3, \quad x_4 = \alpha\xi_4 + \beta\eta_4$$
$$y_2 = (\xi_2\,\eta_1), \quad y_3 = (\xi_3\,\eta_1), \quad y_4 = (\xi_4\,\eta_1).$$

Bestimmt man daher die Substitutionscoëfficienten $\alpha$, $\beta$ aus den Gleichungen

$$\frac{\alpha\xi_2+\beta\eta_2}{(\xi_2\eta_1)}+\frac{\alpha\xi_3+\beta\eta_3}{(\xi_3\eta_1)}+\frac{\alpha\xi_4+\beta\eta_4}{(\xi_4\eta_1)}=0, \tag{5}$$

$$y_2\,y_3\,y_4=-4r, \tag{6}$$

und definirt $g_2$, $g_3$ durch

$$\begin{aligned} y_2\,x_3\,x_4+y_3\,x_4\,x_2+y_4\,x_2\,x_3&=g_2\,r\\ x_2\,x_3\,x_4&=-g_3\,r, \end{aligned} \tag{7}$$

so ergiebt die Formel (1) §. 3

$$\frac{\xi\,d\eta-\eta\,d\xi}{\sqrt{(\xi\eta_1)(\xi\eta_2)(\xi\eta_3)(\xi\eta_4)}}=\frac{dz}{\sqrt{4z^3-g_2z-g_3}}. \tag{8}$$

Um die Legendre'sche Normalform in die Weierstrass'sche zu transformiren, setzt man in (8)

$$\zeta=\frac{\eta}{\xi},$$

und

$$\eta_1=0,\quad \xi_1=1,\quad \xi_2=0,\quad \xi_3=\eta_3,\quad \xi_4=\varkappa^2\eta_4,$$

$$\eta_2\,\eta_3\,\eta_4=-\mu^2,$$

worin $\mu$ willkürlich bleibt. Dadurch erhält die linke Seite von (8) die Gestalt

$$\frac{d\zeta}{\mu\sqrt{\zeta(1-\zeta)(1-\varkappa^2\zeta)}},$$

und die Gleichungen (5), (6), (7) ergeben

$$4r=4\alpha=-\mu^2\qquad \beta=\mu^2\,\frac{1+\varkappa^2}{12}$$

$$\begin{aligned} g_2&=\frac{\mu^4}{12}(1-\varkappa^2\varkappa'^2),\\ g_3&=\frac{\mu^6}{16\,.\,27}(2+\varkappa^2\varkappa'^2)(\varkappa^2-\varkappa'^2),\\ \varDelta&=\frac{\mu^{12}}{256}\varkappa^4\varkappa'^4, \end{aligned} \tag{9}$$

und es liefert also die aus (2) folgende Substitution

$$z=\frac{\mu^2}{4}\left(\frac{1}{\zeta}-\frac{1+\varkappa^2}{3}\right) \tag{10}$$

die Umformung

$$\frac{d\zeta}{\sqrt{\zeta(1-\zeta)(1-\varkappa^2\zeta)}}=\frac{\mu\,dz}{\sqrt{4z^3-g_2z-g_3}}. \tag{11}$$

Bei den bisherigen Umformungen des elliptischen Differentials ist stets die Voraussetzung gewesen, dass die unter dem

Wurzelzeichen stehende Function in lineare Factoren zerlegt sei; bei der linearen Reduction auf die Weierstrass'sche Normalform würde die Kenntniss eines Linearfactors dieser Function genügen. Man kann aber auch ganz ohne eine solche Zerlegung durch eine rationale, allerdings nicht lineare Substitution ein elliptisches Differential auf die Weierstrass'sche Normalform transformiren, wie jetzt noch gezeigt werden soll. Ist

$$f(x,y) = a_0 x^4 + 4 a_1 x^3 y + 6 a_2 x^2 y^2 + 4 a_3 x y^3 + a_4 y^4 \tag{12}$$

eine homogene Form vierten Grades, so heissen die beiden Functionen der Coëfficienten

$$g_2 = a_0 a_4 - 4 a_1 a_3 + 3 a_2^2 \tag{13}$$

$$g_3 = a_0 a_2 a_4 + 2 a_1 a_2 a_3 - a_0 a_3^2 - a_1^2 a_4 - a_2^3 \tag{14}$$

die erste und zweite Invariante und die Verbindung derselben

$$\varDelta = g_2^3 - 27 g_3^2 \tag{15}$$

die Discriminante der biquadratischen Form.

Ausserdem sind noch die beiden Covarianten

$$h = \frac{1}{144} \left[\frac{\partial^2 f}{\partial x^2} \frac{\partial^2 f}{\partial y^2} - \left(\frac{\partial^2 f}{\partial x \partial y}\right)^2\right], \tag{16}$$

$$t = \frac{1}{8} \left(\frac{\partial f}{\partial x} \frac{\partial h}{\partial y} - \frac{\partial f}{\partial y} \frac{\partial h}{\partial x}\right) \tag{17}$$

vom vierten und sechsten Grade in den Variablen $x$, $y$ in Betracht zu ziehen, zwischen welchen die identische Relation stattfindet:

$$t^2 = - 4 h^3 + g_2 h f^2 - g_3 f^3. \tag{18}$$

Nun ist nach dem Grundsatze über homogene Functionen

$$4 f = \frac{\partial f}{\partial x} x + \frac{\partial f}{\partial y} y, \quad df = \frac{\partial f}{\partial x} dx + \frac{\partial f}{\partial y} dy$$

$$4 h = \frac{\partial h}{\partial x} x + \frac{\partial h}{\partial y} y, \quad dh = \frac{\partial h}{\partial x} dx + \frac{\partial h}{\partial y} dy$$

und daraus nach (17)

$$f dh - h df = 2 (x dy - y dx) t$$

und nach (18)

$$\frac{2 (x dy - y dx)}{\sqrt{f(x,y)}} = \frac{f dh - h df}{\sqrt{f (- 4 h^3 + g_2 h f^2 - g_3 f^3)}}.$$

Führt man also die Variable $z$ ein durch die Gleichung

$$z = - \frac{h(x,y)}{f(x,y)}, \tag{19}$$

so erhält man

$$(20) \qquad \frac{2(x\,dy - y\,dx)}{\sqrt{f(x,y)}} = -\frac{dz}{\sqrt{4z^3 - g_2 z - g_3}},$$

worin der Zusammenhang in dem Vorzeichen der beiden Quadratwurzeln bestimmt ist durch die Gleichung

$$(21) \qquad \frac{t(x,y)\sqrt{f(x,y)}}{f(x,y)^2} = \sqrt{4z^3 - g_2 z - g_3} \; ^{*)}.$$

Es liegt nahe, diese Transformation auf ein Differential anzuwenden, welches bereits die Normalform hat. Dies geschieht, indem man

$$f(x,y) = 4x^3 y - g_2 x y^3 - g_3 y^4$$

setzt, also $a_0$, $a_1$, $a_2$, $a_3$, $a_4$ durch 0, 1, 0, $-{}^1\!/_4\, g_2$, $-g_3$ ersetzt, wodurch die Formeln (13), (14) in Identitäten übergehen. Es wird ferner

$$h = -x^4 - \frac{g_2}{2}x^2y^2 - 2g_3xy^3 - \frac{g_2^2}{16}y^4 = -\left(x^2 + \frac{g_2}{4}y^2\right)^2 - 2g_3xy^3,$$

$$t = 2x^6 - \frac{5}{2}g_2x^4y^2 + 10g_3x^3y^3 - \frac{5}{8}g_2^2x^2y^4$$

$$+ \frac{1}{2}g_2g_3xy^5 + \left(\frac{g_2^3}{16} - g_3^2\right)y^6.$$

Wendet man nun die Formeln (19), (20), (21) an, indem man $x$, $y$ durch $z$, 1, und $z$ durch $z'$ ersetzt, so folgt:

$$\frac{2\,dz}{\sqrt{4z^3 - g_2z - g_3}} = \frac{dz'}{\sqrt{4z'^3 - g_2z' - g_3}}$$

$$z' = \frac{\left(z^2 + \frac{g_2}{4}\right)^2 + 2g_3z}{4z^3 - g_2z - g_3}$$

$$\sqrt{4z'^3 - g_2z' - g_3}$$

$$= \frac{2z^6 - \frac{5}{2}g_2z^4 + 10g_3z^3 - \frac{5}{8}g_2^2z^2 + \frac{1}{2}g_2g_3z + \frac{g_2^3}{16} - g_3^2}{\left(\sqrt{4z^3 - g_2z - g_3}\right)^3}.$$

---

*) Ueber die Invarianten und Covarianten der binären quadratischen Formen vergl. man **Clebsch**, Theorie der binären algebraischen Formen (Leipzig 1872), §. 40 u. 42. Die hier mit $g_2$, $g_3$, $h$, $t$ bezeichneten Formen bezeichnet **Clebsch** mit $^1\!/_2\, i$, $^1\!/_6\, j$, $^1\!/_2\, H$, $T$. Die Transformation des elliptischen Differentials, die von **Hermite** herrührt **Crelle's** Journal, Bd. 52) findet sich in §. 62 des genannten Werkes.

Es ist also hierdurch das elliptische Differential vermittelst einer rationalen Substitution in ein mit 2 multiplicirtes Differential von derselben Form transformirt.

## §. 5. Das Jacobi'sche Transformationsprincip.

Die bisher betrachteten Umformungen des elliptischen Differentials sind specielle Fälle der allgemeinen Jacobi'schen Transformation, deren Grundlagen wir hier in der Kürze darlegen müssen.

Als Verallgemeinerung der in §. 3 benutzten linearen Substitution setze man für $x$, $y$ zwei ganze homogene Functionen ohne gemeinsamen Theiler gleichen aber beliebigen Grades $n$ zweier neuer Variablen $\xi$, $\eta$,

$$x = U(\xi, \eta),\; y = V(\xi, \eta). \tag{1}$$

Aus den Gleichungen

$$n\,U = \xi \frac{\partial U}{\partial \xi} + \eta \frac{\partial U}{\partial \eta} \qquad d\,U = d\xi \frac{\partial U}{\partial \xi} + d\eta \frac{\partial U}{\partial \eta}$$

$$n\,V = \xi \frac{\partial V}{\partial \xi} + \eta \frac{\partial V}{\partial \eta} \qquad d\,V = d\xi \frac{\partial V}{\partial \xi} + d\eta \frac{\partial V}{\partial \eta}$$

folgt sodann

$$U\,d\,V - V\,d\,U = H\,(\xi\,d\eta - \eta\,d\xi), \tag{2}$$

wenn $H$ die Functionaldeterminante

$$H = \frac{1}{n}\left(\frac{\partial U}{\partial \xi}\,\frac{\partial V}{\partial \eta} - \frac{\partial V}{\partial \xi}\,\frac{\partial U}{\partial \eta}\right) \tag{3}$$

bedeutet.

Danach geht das elliptische Differential

$$\frac{x\,dy - y\,dx}{\sqrt{f(x, y)}}$$

in das folgende über:

$$H\,\frac{\xi\,d\eta - \eta\,d\xi}{\sqrt{f(U, V)}}. \tag{5}$$

Damit nun dies Differential wieder die Form eines elliptischen erhält, ist erforderlich, dass von der Function $f(U, V)$, deren Grad der $4n$te ist, sich ein quadratischer Factor $T^2$ vom Grade $4n - 4$ absondern lasse, also, wenn $\varphi(\xi, \eta)$ eine Function vierten Grades bedeutet, dass

$$f(U, V) = T^2\,\varphi(\xi, \eta) \tag{6}$$

werde, wodurch, wenn

$$(7) \qquad \frac{T}{H} = M$$

gesetzt wird, das Differential (5) in

$$(8) \qquad \frac{1}{M}\,\frac{\xi\, d\eta - \eta\, d\xi}{\sqrt{\varphi(\xi,\eta)}}$$

übergeht. Es lässt sich nun nachweisen, dass, sobald die Bedingung (6) erfüllt ist, $H$ durch $T$ theilbar, und also, da der Grad beider Functionen derselbe ist, $M$ eine Constante wird, welche der Multiplicator der Transformation heisst.

Bemerken wir nämlich, dass, da $f(x,y)$ keinen quadratischen Factor enthält, die beiden Functionen

$$\frac{\partial f}{\partial x},\ \frac{\partial f}{\partial y}$$

keinen gemeinschaftlichen Theiler haben, und dass in Folge dessen, weil $U$ und $V$ theilerfremd sind, auch

$$\frac{\partial f}{\partial U},\ \frac{\partial f}{\partial V}.$$

keinen gemeinschaftlichen Theiler (in Beziehung auf $\xi$, $\eta$) haben, so lassen sich zwei Functionen $\alpha$, $\beta$ von $\xi$, $\eta$ so bestimmen, dass

$$\alpha\frac{\partial f}{\partial U} + \beta\frac{\partial f}{\partial V}$$

zu einer beliebig gegebenen Function $T$ theilerfremd ist. Man kann z. B. $\alpha$ theilerfremd zu $T$ und $\beta$ durch die in $\frac{\partial f}{\partial U}$ nicht aufgehenden Theiler von $T$ theilbar, dagegen durch die gemeinschaftlichen Theiler von $T$ und $\frac{\partial f}{\partial U}$ untheilbar annehmen. Wenn wir nun die Gleichung (6), die wir als erfüllt voraussetzen, nach $\xi$, $\eta$ differentiiren, so folgt:

$$\frac{\partial f}{\partial U}\frac{\partial U}{\partial \xi} + \frac{\partial f}{\partial V}\frac{\partial V}{\partial \xi} = TX$$
$$\frac{\partial f}{\partial U}\frac{\partial U}{\partial \eta} + \frac{\partial f}{\partial V}\frac{\partial V}{\partial \eta} = TY,$$

und daraus durch Auflösung in Bezug auf $\frac{\partial f}{\partial U}$, $\frac{\partial f}{\partial V}$:

$$H\left(\alpha\frac{\partial f}{\partial U} + \beta\frac{\partial f}{\partial V}\right) = TZ,$$

worin $X$, $Y$, $Z$ ganze homogene Functionen von $\xi$, $\eta$ sind. Aus der letzten Gleichung aber schliesst man, dass $H$ durch $T$ theilbar sein muss.

Demnach ist unser ganzes Problem enthalten in der Gleichung (6), welche nichts Anderes besagt, als dass die Function $4n$ten Grades, $f(U, V)$, $2n-2$ quadratische Factoren enthalten soll. Zur Befriedigung der hieraus folgenden $2n-2$ Bedingungen hat man die $2n+2$ in $U$, $V$ enthaltenen Coëfficienten zur Verfügung, so dass von diesen vier unbestimmt bleiben, was vorher zu sehen war, da für $\xi$, $\eta$ beliebige homogene lineare Functionen von $\xi$, $\eta$ eingeführt werden können. Man kann diese vier überzähligen Constanten dazu verwenden, um das Differential (8) in eine Normalform zu bringen. Da aber die Bedingungsgleichungen für die Coëfficienten von $U$, $V$ nicht linear sind, so giebt es für einen gegebenen Transformationsgrad mehrere Transformationen.

Wir werden diesem Transformationsproblem später von einer ganz anderen Seite her wieder begegnen und weit tiefer darauf eingehen müssen. Die einfachen algebraischen Principien desselben sind an dieser Stelle nur deshalb dargelegt, um später auf die Identität sehr verschiedenartig erscheinender Probleme hinweisen zu können. Es soll daher auf die Einzelheiten des algebraischen Problems hier nicht näher eingegangen werden, dagegen wollen wir durch zwei Beispiele das Gesagte veranschaulichen.

## §. 6. Die Transformation zweiten Grades.

Indem wir die Legendre'sche Normalform anwenden, setzen wir

$$f(x,y) = xy(x-y)(x-\lambda^2 y)$$
$$\varphi(\xi,\eta) = \xi\eta(\xi-\eta)(\xi-\varkappa^2\eta)$$

und es seien $U$, $V$ vom zweiten Grade.

Die Gleichung (6) wird jetzt, da $T$ vom zweiten Grade ist

$$(1)\quad \begin{aligned} &UV(U-V)(U-\lambda^2 V) \\ &\qquad = (a\xi+b\eta)^2(a'\xi+b'\eta)^2\xi\eta(\xi-\eta)(\xi-\varkappa^2\eta) \end{aligned}$$

und es müssen zwei der vier Factoren zweiten Grades auf der linken Seite dieser Gleichung Quadrate sein. Die grosse Zahl der hierin liegenden Möglichkeiten wollen wir dadurch noch beschränken, dass wir voraussetzen, $\eta$ und $y$ sollen gleichzeitig verschwinden, also $V$ durch $\eta$ theilbar sein. Dies giebt (von einem constanten Factor abgesehen) für $V$ die folgenden drei Möglichkeiten:

$$1)\quad V = \xi\eta \qquad 2)\quad V = \eta(\xi - \eta) \qquad 3)\quad V = \eta(\xi - \varkappa^2\eta).$$

Jeder dieser drei Fälle umfasst nun wieder drei Unterfälle, indem von den drei übrigen Factoren $U$, $U - V$, $U - \lambda^2 V$ irgend zwei als Quadrate angenommen werden können. Von diesen letzteren drei Fällen gehen zwei in einander über durch Vertauschung von $V$, $\lambda^2$ mit $V : \lambda^2$, $1 : \lambda^2$.

Wir wollen zwei für die Folge besonders wichtige unter diesen Transformationen vollständig durchführen.

### 1. Die Gauss'sche Transformation.

$$V = \xi\eta \qquad U = (a\xi + b\eta)^2.$$

Wenn nun noch $U - \lambda^2 V$ ein Quadrat sein soll, so ist

$$\lambda^2 = 4ab$$

zu setzen, und es wird

$$U - \lambda^2 V = (a\xi - b\eta)^2.$$

Da $U - V$ sodann durch $\xi - \eta$ und durch $\xi - \varkappa^2\eta$ theilbar sein muss, so ergeben sich, wenn man $\xi = \eta$, $\xi = \varkappa^2\eta$ setzt, aus $U = V$ die Bedingungen

$$a + b = 1, \qquad a\varkappa^2 + b = \pm\varkappa,$$

woraus, wenn das obere Zeichen genommen wird

$$a = \frac{1}{1+\varkappa}, \qquad b = \frac{\varkappa}{1+\varkappa}, \qquad \lambda = \frac{2\sqrt{\varkappa}}{1+\varkappa},$$

$$V = \xi\eta, \qquad U = \left(\frac{\xi + \varkappa\eta}{1+\varkappa}\right)^2, \qquad U - \lambda^2 V = \left(\frac{\xi - \varkappa\eta}{1 - \varkappa}\right)^2,$$

$$U - V = \frac{(\xi - \eta)(\xi - \varkappa^2\eta)}{(1+\varkappa)^2},$$

$$T = \frac{\xi^2 - \varkappa^2\eta^2}{(1+\varkappa)^3}, \qquad H = \frac{\xi^2 - \varkappa^2\eta^2}{(1+\varkappa)^2},$$

$$M = \frac{1}{1+\varkappa}.$$

Setzt man also wieder

$$\frac{y}{x} = z, \qquad \frac{\eta}{\xi} = \zeta,$$

so haben wir das Resultat, dass durch die Substitution

$$z = \frac{(1 + \varkappa)^2 \zeta}{(1 + \varkappa \zeta)^2}, \qquad \lambda^2 = \frac{4 \varkappa}{(1 + \varkappa)^2} \tag{2}$$

die Transformation

$$\frac{dz}{\sqrt{z(1 - z)(1 - \lambda^2 z)}} = \frac{(1 + \varkappa)\, d\zeta}{\sqrt{\zeta(1 - \zeta)(1 - \varkappa^2 \zeta)}} \tag{3}$$

geleistet wird.

### 2. Die Landen'sche Transformation.

$$V = a \eta (\xi - \eta), \qquad U = \xi (\xi - \varkappa^2 \eta).$$

Die Bedingungen, dass $U - V$, $U - \lambda^2 V$ Quadrate sind, lauten

$$4a = (\varkappa^2 + a)^2, \quad 4 a \lambda^2 = (\varkappa^2 + a \lambda^2)^2,$$

woraus

$$\lambda (\varkappa^2 + a) = \varkappa^2 + a \lambda^2,$$

oder durch $\lambda - 1$ dividirt

$$a \lambda = \varkappa^2;$$

dies in eine der obigen Gleichungen eingesetzt, giebt

$$4 \lambda = \varkappa^2 (1 + \lambda)^2,$$

und durch Auflösung dieser quadratischen Gleichung, wenn $\varkappa' = \sqrt{1 - \varkappa^2}$ gesetzt ist:

$$\begin{aligned}
\lambda &= \frac{1 - \varkappa'}{1 + \varkappa'}, \qquad a = (1 + \varkappa')^2, \\
U - V &= [\xi - (1 + \varkappa') \eta]^2, \\
U - \lambda^2 V &= [\xi - (1 - \varkappa') \eta]^2, \\
H &= (1 + \varkappa')^2 [\xi - (1 + \varkappa') \eta] [\xi - (1 - \varkappa') \eta], \\
T &= (1 + \varkappa') [(\xi - \eta)^2 - \varkappa'^2 \eta^2], \\
M &= \frac{1}{1 + \varkappa'},
\end{aligned}$$

also durch die Substitution

$$z = \frac{(1 + \varkappa')^2 \zeta (1 - \zeta)}{1 - \varkappa^2 \zeta}, \quad \lambda = \frac{1 - \varkappa'}{1 + \varkappa'}, \tag{4}$$

die Umformung

$$(5)\qquad \frac{dz}{\sqrt{z\,(1-z)\,(1-\lambda^2 z)}} = \frac{(1+\varkappa')\,d\xi}{\sqrt{\xi\,(1-\xi)\,(1-\varkappa^2\xi)}}.$$

## §. 7. Die Transformation dritten Grades.

Als zweites Beispiel betrachten wir die Transformation dritten Grades. Die Gleichung

$$(1)\qquad UV(U-V)(U-\lambda^2 V) = T^2\xi\eta\,(\xi-\eta)\,(\xi-\varkappa^2\eta)$$

fordert, dass jeder der vier Factoren dritten Grades $U$, $V$, $U-V$, $U-\lambda^2 V$ durch einen der Linearfactoren $\xi$, $\eta$, $\xi-\eta$, $\xi-\varkappa^2\eta$ theilbar sei, und dass der Quotient ein Quadrat sei. Wir setzen also

$$(2)\qquad U = \xi(a\xi+b\eta)^2, \qquad V = \eta(a'\xi+b'\eta)^2$$

und verlangen noch, dass

$$(3)\qquad \frac{U-V}{\xi-\eta},\quad \frac{U-\lambda^2 V}{\xi-\varkappa^2\eta}$$

die Quadrate linearer Functionen werden.

Von den beiden letzten Forderungen folgt die eine aus der anderen, wenn wir $U$, $V$ so einrichten, dass, von constanten Factoren abgesehen, $U$ und $V$ in einander übergehen durch die Vertauschung von $\xi$, $\eta$ mit $\varkappa^2\eta$, $\xi$. Durch diese Vertauschung geht aber

$$\xi(a\xi+b\eta)^2, \qquad \eta(a'\xi+b'\eta)^2$$

über in

$$\varkappa^2\eta\,(b\xi+a\varkappa^2\eta)^2, \qquad \xi(b'\xi+a'\varkappa^2\eta)^2,$$

und unsere Forderung ist erfüllt, wenn

$$(4)\qquad \varkappa^2 = \frac{bb'}{aa'}$$

ist. Wenn dann

$$(5)\qquad \lambda^2 = \varkappa^2\left(\frac{ab}{a'b'}\right)^2$$

ist, so geht durch diese Vertauschung

$$(6)\qquad \frac{U-V}{\xi-\eta} \quad\text{in}\quad \frac{b'^2}{a^2}\,\frac{U-\lambda^2 V}{\xi-\varkappa^2\eta}$$

über. Nachdem dies festgesetzt, ist nur noch die Bedingung zu erfüllen, dass die erste der beiden Grössen (3) das Quadrat einer linearen Function, die wir mit $(\alpha^2 \xi - \beta^2 \eta)$ bezeichnen, werde, also

$$(7) \qquad U - V = (\xi - \eta)(\alpha^2 \xi - \beta^2 \eta)^2$$

oder

$$U - \xi(\alpha^2 \xi - \beta^2 \eta)^2 = V - \eta(\alpha^2 \xi - \beta^2 \eta)^2,$$

und da $U$ durch $\xi$, $V$ durch $\eta$ theilbar ist, so muss diese Function durch $\xi\,\eta$ theilbar sein; setzen wir sie $= \xi\,\eta\,(m\,\xi + n\,\eta)$, so ergiebt sich aus (2)

$$\begin{aligned}(a\,\xi + b\,\eta)^2 &= (\alpha^2 \xi - \beta^2 \eta)^2 + \eta\,(m\,\xi + n\,\eta)\\ (a'\xi + b'\eta)^2 &= (\alpha^2 \xi - \beta^2 \eta)^2 + \xi\,(m\,\xi + n\,\eta).\end{aligned}$$

Die Vergleichung der Coëfficienten ergiebt

$$a = \alpha^2, \quad b = -\beta^2 + \frac{m}{2\,\alpha^2}, \qquad b^2 = \beta^4 + n,$$

$$b' = \beta^2, \quad a' = -\alpha^2 + \frac{n}{2\,\beta^2}, \qquad a'^2 = \alpha^4 + m,$$

und aus den beiden letzten Gleichungen jeder Reihe:

$$\begin{aligned}m^2 &= 4\,\alpha^2(n\,\alpha^2 + m\,\beta^2)\\ n^2 &= 4\,\beta^2(n\,\alpha^2 + m\,\beta^2).\end{aligned}$$

Wenn man also

$$m = h\,\alpha, \quad n = h\,\beta$$

setzt, so wird

$$h = 4\,\alpha\,\beta\,(\alpha + \beta).$$

Hiernach lassen sich $a, b, a', b'$ durch die beiden Grössen $\alpha, \beta$ ausdrücken in der Weise:

$$(8) \qquad \begin{aligned}a = \alpha^2, \quad b = \beta^2 + 2\,\alpha\,\beta,\\ a' = \alpha^2 + 2\,\alpha\,\beta, \quad b' = \beta^2\end{aligned}$$

und danach aus (4), (5)

$$(9) \qquad \varkappa^2 = \frac{\beta^3}{\alpha^3}\,\frac{\beta + 2\,\alpha}{\alpha + 2\,\beta}, \quad \frac{\lambda}{\varkappa} = \frac{\alpha}{\beta}\,\frac{\beta + 2\,\alpha}{\alpha + 2\,\beta},$$

oder durch Multiplication und Division dieser beiden Gleichungen:

$$(10) \qquad \sqrt{\lambda\,\varkappa} = \frac{\beta}{\alpha}\,\frac{\beta + 2\,\alpha}{\alpha + 2\,\beta}, \quad \frac{\varkappa^3}{\lambda} = \frac{\beta^4}{\alpha^4}.$$

Durch Elimination von $\beta : \alpha$ erhält man eine Gleichung zwischen $\varkappa$, $\lambda$, welche die Modulargleichung heisst, deren Grad die Anzahl der verschiedenen Transformationen dritten Grades angiebt. Sie nimmt die einfachste Gestalt an, wenn man setzt:

$$(11) \qquad \sqrt[4]{\varkappa} = u, \quad \sqrt[4]{\lambda} = v.$$

Dann werden die Gleichungen (10)

$$u^2 v^2 = \frac{\beta}{\alpha} \frac{\beta + 2\alpha}{\alpha + 2\beta}, \quad \frac{u^3}{v} = \frac{\beta}{\alpha},$$

also durch Einsetzen des Werthes von $\beta : \alpha$ in die erste Gleichung und Beseitigung des Factors $u^2$:

$$v^4 - u^4 + 2 u^3 v^3 - 2 u v = 0, \tag{12}$$

eine Gleichung vom vierten Grade.

Man erhält ferner

$$T = \frac{a}{b'} (a \xi + b \eta) (a' \xi + b' \eta) (\alpha^2 \xi - \beta^2 \eta) (\beta^2 \xi - \varkappa^2 \alpha^2 \eta)$$

$$H = \frac{1}{3} \left( \frac{\partial U}{\partial \xi} \frac{\partial V}{\partial \eta} - \frac{\partial V}{\partial \xi} \frac{\partial U}{\partial \eta} \right) = \frac{a'}{a} T,$$

woraus man leicht nach (8) findet

$$M = \frac{a}{a'} = \frac{\alpha}{\alpha + 2\beta} = \frac{v}{v + 2u^3}. \tag{13}$$

Setzt man den hieraus sich ergebenden Ausdruck

$$v = \frac{2 u^3 M}{1 - M}$$

in die Gleichung (12) ein, so ergiebt sich für $M$ eine Gleichung vierten Grades, die Multiplicatorgleichung, welche die Modulargleichung ersetzen kann. Man erhält aber diese Gleichung einfacher auf folgendem Wege. Nach (13) ist

$$\frac{1}{M} - 1 = 2 \frac{\beta}{\alpha}, \quad \frac{1}{M} + 3 = \frac{2 (\beta + 2\alpha)}{\alpha},$$

also nach (9):

$$\left(\frac{1}{M} - 1\right)^3 \left(\frac{1}{M} + 3\right) = 16 \varkappa^2 \frac{(\alpha + 2\beta)}{\alpha}$$

und folglich nach (13)

$$\frac{16 \varkappa^2}{M} = \left(\frac{1}{M} - 1\right)^3 \left(\frac{1}{M} + 3\right),$$

oder geordnet

$$\frac{1}{M^4} - \frac{6}{M^2} + \frac{8 (1 - 2\varkappa^2)}{M} - 3 = 0. \tag{14}$$

Drücken wir alle unsere Formeln durch $u$, $v$ aus, so ist also das Ergebniss dieser Betrachtung das folgende:

Durch die Substitution

$$z = \frac{\zeta\,[(v^2 + 2\,v\,u^3) + u^6\,\zeta]^2}{[v^2 + (u^6 + 2\,v\,u^3)\,\zeta]^2}$$

wird die Transformation bewirkt

$$\frac{d\,z}{\sqrt{z\,(1-z)\,(1-u^8\,z)}} = \frac{v + 2\,u^3}{v}\;\frac{d\,\zeta}{\sqrt{\zeta\,(1-\zeta)\,(1-v^8\,\zeta)}},$$

falls zwischen $u$, $v$ die Modulargleichung (12) besteht.

## §. 8. Die drei Gattungen elliptischer Integrale.

Wir haben oben (§. 1) gesehen, dass wir jedes elliptische Integral nach Absonderung des Integrals einer rationalen Function in der Form annehmen können:

$$(1) \qquad \int \frac{\varphi\,(x,y)}{\psi\,(x,y)}\,\frac{x\,d\,y - y\,d\,x}{\sqrt{f\,(x,y)}},$$

worin $\varphi$, $\psi$ ganze rationale und homogene Functionen gleichen Grades, aber ohne gemeinschaftlichen Theiler sind, während $f\,(x,y)$ eine ganze rationale homogene Function vierten Grades ohne quadratischen Theiler bedeutet. Dies Integral lässt sich nun in eine Reihe von einfacheren Integralen zerlegen. Zu diesem Ende machen wir von der Formel Gebrauch, welche gültig ist unter der Voraussetzung, dass $\Phi$ eine beliebige homogene Function vom $-2$ten Grade ist, und die sich aus dem Fundamentalsatz über homogene Functionen

$$x\,\frac{\partial f}{\partial x} + y\,\frac{\partial f}{\partial y} = 4\,f,\; x\,\frac{\partial \Phi}{\partial x} + y\,\frac{\partial \Phi}{\partial y} = -\,2\,\Phi$$

leicht ableiten lässt:

$$(2) \qquad d\big(\Phi\sqrt{f\,(x,y)}\big) = \frac{1}{4}\left(\frac{\partial f}{\partial x}\,\frac{\partial \Phi}{\partial y} - \frac{\partial f}{\partial y}\,\frac{\partial \Phi}{\partial x}\right)\frac{x\,d\,y - y\,d\,x}{\sqrt{f\,(x,y)}}.$$

Es seien $\xi$, $\eta$ zwei beliebige lineare Functionen von $x$, $y$:

$$\xi = \alpha\,x + \beta\,y, \qquad \eta = \gamma\,x + \delta\,y,$$

deren Determinante

$$r = \alpha\,\delta - \beta\,\gamma$$

von Null verschieden ist, und es werde

$$\Phi = \xi^{\lambda}\,\eta^{-\lambda-2}$$

gesetzt, worin $\lambda$ ein beliebiger Exponent. Dann ergiebt (2)

$$(3)\quad d\left(\xi^{\lambda}\,\eta^{-\lambda-2}\sqrt{f(x,y)}\right) = \frac{r}{4}\left(\frac{\partial f}{\partial \xi}\frac{\partial \Phi}{\partial \eta} - \frac{\partial f}{\partial \eta}\frac{\partial \Phi}{\partial \xi}\right)\frac{x\,dy - x\,dy}{\sqrt{f(x,y)}}$$

$$= \frac{-r}{4}\,\xi^{\lambda-1}\,\eta^{-\lambda-3}\left(\lambda\,\eta\,\frac{\partial f}{\partial \eta} + (\lambda+2)\,\xi\,\frac{\partial f}{\partial \xi}\right)\frac{x\,dy - y\,dx}{\sqrt{f(x,y)}},$$

worin

$$\lambda\,\eta\,\frac{\partial f}{\partial \eta} + (\lambda+2)\,\xi\,\frac{\partial f}{\partial \xi} = 4\,\lambda f + 2\,\xi\,\frac{\partial f}{\partial \xi}$$

$$= 4\,(\lambda+2)\,f - 2\,\eta\,\frac{\partial f}{\partial \eta}$$

gesetzt werden kann. Diese Function ist also dann und nur dann durch $\xi$ oder durch $\eta$ theilbar, wenn $\xi$ oder $\eta$ ein Theiler von $f$ ist, oder wenn $\lambda = 0$ oder $= -2$ ist, während sie niemals, wenigstens für ein ganzzahliges $\lambda$ durch $\xi^2$ oder $\eta^2$ theilbar ist. Sollte sie nämlich durch $\xi^2$ theilbar sein, so müsste auch ihre Ableitung nach $\xi$

$$(4\,\lambda + 2)\,\frac{\partial f}{\partial \xi} + 2\,\xi\,\frac{\partial^2 f}{\partial \xi^2}$$

durch $\xi$ theilbar sein, was, da $f$ und $\frac{\partial f}{\partial \xi}$ keinen gemeinsamen Theiler haben, unmöglich ist.

Es sei nun $\xi$ ein Factor von der im Integral (1) vorkommenden Function $\psi$, und zwar

$$(4)\qquad \psi = \xi^m\,\psi_1,$$

so dass $\psi_1$ nicht mehr durch $\xi$ theilbar ist. Ist zunächst $m = 1$, so kann man eine lineare homogene Function $q$ und eine homogene Function $\varphi_1$ vom Grade von $\psi_1$ so bestimmen, dass

$$\frac{\varphi}{\psi} = \frac{q}{\xi} + \frac{\varphi_1}{\psi_1}.$$

Man hat nämlich

$$\xi\,\varphi_1 = \varphi - q\,\psi_1,$$

und hat nur $q$ so zu wählen, dass die rechte Seite dieser Gleichung durch $\xi$ theilbar wird, wobei eine Constante willkürlich bleibt. Dadurch ist das Integral (1) in zwei andere von derselben Form zerlegt, in deren einem $\varphi$, $\psi$ linear sind, in deren zweitem der Grad dieser Functionen um 1 erniedrigt ist.

Denselben Zweck erreichen wir für jeden Werth von $m$ durch Hinzufügung einer algebraischen Function auf Grund der Gleichung (3). Wir bezeichnen mit $q$, $\varphi_1$ ganze homogene Functionen von $x$, $y$, deren erste linear ist, deren zweite einen um

1 niedrigeren Grad hat als $\psi$, mit $A$ eine Constante, und bestimmen diese Grössen, so dass

$$(5)\qquad \frac{\varphi}{\psi}\,\frac{y\,dx - x\,dy}{\sqrt{f(x,y)}} = \left(\frac{\varphi_1}{\psi_1\,\xi^{m-1}} + \frac{q}{\eta}\right)\frac{y\,dx - x\,dy}{\sqrt{f(x,y)}} + \frac{4\,A}{r}\,d\left(\xi^{\lambda}\,\eta^{-\lambda-2}\sqrt{f(x,y)}\right).$$

Ist dies gelungen, so ist der angegebene Zweck offenbar erreicht. Ueber die Function $\eta$ und den Exponenten $\lambda$ haben wir die Verfügung noch offen. Mit Hülfe von (3) leitet man aber aus der Gleichung (5) die folgende ab:

$$(6)\qquad \begin{aligned}\eta\,\xi\,\varphi_1 &= \eta\,\varphi - q\,\xi^m\,\psi_1\\ &+ A\,\xi^{m+\lambda-1}\,\eta^{-\lambda-2}\,\psi_1\left(\lambda\,\eta\,\frac{\partial f}{\partial \eta} + (\lambda+2)\,\xi\,\frac{\partial f}{\partial \xi}\right)\end{aligned}$$

und man hat nun über $q$, $A$, $\lambda$, $\eta$ so zu verfügen, dass die rechte Seite eine durch $\xi$, $\eta$ theilbare ganze Function wird; dann erhält man durch Ausführung der Division die Function $\varphi_1$.

Wenn nun zunächst $f$ durch $\xi$ nicht theilbar ist, so nehme man $\lambda = -m+1$. Ist $m \geqq 3$, so bleibt $\eta$ beliebig, man kann $q = 0$ setzen und $\eta$ fortheben, und $A$ ist dann so zu bestimmen, dass die ganze Function

$$\varphi - A\,\eta^{m-4}\,\psi_1\left[(m-1)\,\eta\,\frac{\partial f}{\partial \eta} + (m-3)\,\xi\,\frac{\partial f}{\partial \xi}\right]$$

durch $\xi$ theilbar wird, was immer möglich ist.

Ist dagegen $m = 2$, so muss man für $\eta$ einen der Lineartheiler von $f$ wählen. Darauf ist $q$ so zu bestimmen, dass

$$q\,\xi^2 + A\,\eta^{-1}\left(\eta\,\frac{\partial f}{\partial \eta} - \xi\,\frac{\partial f}{\partial \xi}\right),$$

welches in Folge der gemachten Voraussetzung eine ganze Function ist, durch $\eta$ theilbar wird. Dies ist immer möglich, und zwar so, dass $q$ den Factor $A$ erhält und überdies einer seiner Coëfficienten willkürlich bleibt. Darauf lässt sich $A$ noch so bestimmen, dass

$$\varphi - q\,\xi^2\,\eta^{-1}\,\psi_1 - A\,\eta^{-2}\,\psi_1\left(\eta\,\frac{\partial f}{\partial \eta} - \xi\,\frac{\partial f}{\partial \xi}\right)$$

durch $\xi$ theilbar wird.

Ist zweitens $\xi$ ein Theiler von $f$, so nehme man $\lambda = -m$; es kann dann $\eta$ beliebig angenommen und $q = 0$ gesetzt werden, so dass (6) durch $\eta$ theilbar wird, und es muss in

$$\xi \varphi_1 = \varphi - A \xi^{-1} \eta^{m-3} \psi_1 \left( m \eta \frac{\partial f}{\partial \eta} + (m-2) \xi \frac{\partial f}{\partial \xi} \right)$$

$A$ so bestimmt werden, dass die rechte Seite durch $\xi$ theilbar wird.

Indem man nun die in (5) enthaltene Reduction wiederholt anwendet, erkennt man, dass sich das elliptische Integral (1) stets darstellen lässt als ein Aggregat von algebraischen Functionen und Integralen von einer der beiden Formen

$$\int \frac{x\,dy - y\,dx}{\sqrt{f(x, y)}} \tag{7}$$

$$\int \frac{ax + by}{\alpha x + \beta y} \frac{x\,dy - y\,dx}{\sqrt{f(x, y)}}. \tag{8}$$

Die erste Form (7) sind die Integrale erster Gattung. Indem man (8) durch eine lineare Verbindung von (7) und (8) ersetzt, kann man in (8) den Constanten $a$, $b$ beliebige Werthe ertheilen.

Die Integrale (8) sind noch zu unterscheiden, je nachdem der Nenner $\alpha x + \beta y$ ein Theiler von $f(x,y)$ ist oder nicht. Die ersteren, deren vier wesentlich verschiedene sich ergeben, wenn für $\alpha x + \beta y$ jeder der Linearfactoren von $f(x,y)$ gesetzt wird, sind die Integrale zweiter Gattung. Ist aber $\alpha x + \beta y$ nicht in $f(x, y)$ enthalten, so ist (8) ein Integral dritter Gattung.

Die vier Integrale zweiter Gattung lassen sich aber durch Vermittelung algebraischer Functionen auf ein einziges zurückführen. Um dies nachzuweisen, seien $\xi_1, \xi_2, \xi_3, \xi_4$ die vier Linearfactoren von $f$, so dass

$$f = \xi_1 \xi_2 \xi_3 \xi_4,$$

und es sei

$$r = \frac{\partial \xi_1}{\partial x} \frac{\partial \xi_2}{\partial y} - \frac{\partial \xi_1}{\partial y} \frac{\partial \xi_2}{\partial x}.$$

Drücken wir $\xi_3, \xi_4$ durch $\xi_1, \xi_2$ aus, so mag sich ergeben

$$\xi_3 = \alpha \xi_1 + \beta \xi_2, \qquad \xi_4 = \alpha' \xi_1 + \beta' \xi_2.$$

Machen wir dann in der Formel (2) die Annahme

$$\Phi = \frac{1}{\xi_1 \xi_2},$$

so folgt, indem wir die Differentiation nach $x$, $y$ durch eine Differentiation nach $\xi_1$, $\xi_2$ ersetzen:

$$d\sqrt{\frac{\xi_3\,\xi_4}{\xi_1\,\xi_2}} = \frac{r}{2}\left(\alpha\alpha'\,\frac{\xi_1}{\xi_2} - \beta\beta'\,\frac{\xi_2}{\xi_1}\right)\frac{x\,dy - y\,dx}{\sqrt{f(x,y)}},$$

wodurch die beiden Integrale zweiter Gattung

$$\int\frac{\xi_1}{\xi_2}\,\frac{x\,dy - y\,dx}{\sqrt{f(x,y)}}, \qquad \int\frac{\xi_2}{\xi_1}\,\frac{x\,dy - y\,dx}{\sqrt{f(x,y)}}$$

auf einander zurückgeführt sind.

Um also die sämmtlichen zu einer Irrationalität $\sqrt{f}$ gehörigen elliptischen Integrale zusammenzusetzen, genügen drei Integrale der Formen (7), (8), von welchen das dritte von einem veränderlichen Parameter abhängig ist.

Wenden wir diese Ergebnisse auf die Legendre'sche Normalform an, so kann man, indem man über die Constanten $a$, $b$ in (8) noch verfügt, für diese drei Integrale die folgenden wählen:

$$\int\frac{dz}{\sqrt{z\,(1-z)\,(1-\varkappa^2 z)}}, \qquad \int\frac{(1-\varkappa^2 z)\,dz}{\sqrt{z\,(1-z)\,(1-\varkappa^2 z)}},$$

$$\int\frac{dz}{(z-\alpha)\sqrt{z\,(1-z)(1-\varkappa^2 z)}}.$$

Für die Weierstrass'sche Normalform würden die folgenden Integrale denselben Dienst leisten:

$$\int\frac{dz}{\sqrt{4z^3 - g_2 z - g_3}}, \qquad \int\frac{z\,dz}{\sqrt{4z^3 - g_2 z - g_3}},$$

$$\int\frac{dz}{(z-\alpha)\sqrt{4z^3 - g_2 z - g_3}}.$$

## §. 9. Das Additionstheorem.

Wir verlassen nun die Darstellung in homogenen Variablen, in welchen die folgenden Betrachtungen an Uebersichtlichkeit verlieren würden, und nehmen das elliptische Differential in der Form an

$$\frac{dx}{\sqrt{f(x)}},$$

worin $f(x)$ eine ganze rationale Function dritten oder vierten Grades von $x$ ist.

Das von Euler entdeckte Additionstheorem der elliptischen Integrale besteht in dem Satze, der für die ganze weitere Theorie von der fundamentalsten Bedeutung ist, dass, wenn von den drei Werthpaaren

$$x_1, \sqrt{f(x_1)}; \quad x_2, \sqrt{f(x_2)}; \quad x_3, \sqrt{f(x_3)}$$

zwei als gegeben vorausgesetzt werden, man auf algebraischem Wege das dritte so bestimmen kann, dass die Differentialgleichung

$$(1) \qquad \frac{dx_1}{\sqrt{f(x_1)}} + \frac{dx_2}{\sqrt{f(x_2)}} + \frac{dx_3}{\sqrt{f(x_3)}} = 0$$

befriedigt ist. Es ist dies ein specieller Fall des grossen Abel'schen Theorems und soll auch in dieser Weise hier aufgefasst und abgeleitet werden*). Dem Beweise schicken wir folgenden elementaren algebraischen Satz voraus:

Ist $F(x)$ eine ganze rationale Function $n$ten Grades ohne mehrfache Factoren, $F'(x)$ ihre Derivirte, ferner $x_1, x_2, \ldots x_n$ die Wurzeln der Gleichung $F(x) = 0$ und $\varphi(x)$ eine ganze Function von $x$, deren Grad höchstens $= n - 2$, so ist

$$(2) \qquad \frac{\varphi(x_1)}{F'(x_1)} + \frac{\varphi(x_2)}{F'(x_2)} + \cdots \frac{\varphi(x_n)}{F'(x_n)} = 0.$$

Der Beweis dieses Satzes ergiebt sich unmittelbar aus der Zerlegung des rationalen Bruches

$$\frac{x\,\varphi(x)}{F(x)}$$

in Partialbrüche

$$\frac{x_1\,\varphi(x_1)}{F'(x_1)\,(x - x_1)} + \frac{x_2\,\varphi(x_2)}{F'(x_2)\,(x - x_2)} + \cdots \frac{x_n\,\varphi(x_n)}{F'(x_n)\,(x - x_n)},$$

wenn darin $x = 0$ gesetzt wird.

Es bedeuten nun $P$, $Q$ ganze Functionen von $x$ von den Graden $m$ und $m - 2$ und wir fragen nach den Werthen von $x$, $\sqrt{f(x)}$, für welche die Function

$$(3) \qquad P + Q\sqrt{f(x)}$$

verschwindet. Solcher Werthpaare giebt es $2m$, und zwar findet man die Werthe von $x$ als Wurzeln der Gleichung $2m$ten Grades

---

*) Dies weitumfassende Theorem findet sich in grossartiger Einfachheit abgeleitet in einem kaum zwei Seiten umfassenden Aufsatze im 4. Bande von Crelle's Journal „Démonstration d'une propriété générale d'une certaine classe de fonctions transcendentes"; Oeuvres complètes de N. H. Abel. Nouvelle édition T. I. p. 515.

$$(4) \qquad F(x) = P^2 - Q^2 f(x) = 0$$

und die zugehörigen Werthe $\sqrt{f(x)}$ aus

$$(5) \qquad P + Q\sqrt{f(x)} = 0.$$

Wir nehmen nun an, die Coëfficienten in den Functionen $P$, $Q$ seien veränderlich, entweder unabhängige Veränderliche, oder in irgend einer Weise von anderen Veränderlichen abhängig. Es werden dann auch die durch (4), (5) bestimmten Werthe $x$ und $\sqrt{f(x)}$ Functionen dieser Veränderlichen, und (5) lässt sich differentiiren.

Bezeichnen wir mit $\delta$ die Differentiation nach den in den Coëfficienten von $P$, $Q$ vorkommenden Veränderlichen, wobei $x$ als constant gilt, mit $dx$ das entsprechende Differential von $x$, wenn $x$ durch (4) oder (5) als Function dieser Coëfficienten bestimmt ist, so ergiebt die Differentiation von (4)

$$2P\delta P - 2Q\delta Q\, f(x) + F'(x)\,dx = 0,$$

woraus mit Benutzung von (5)

$$(6) \qquad \frac{Q\delta P - P\delta Q}{F'(x)} = \frac{dx}{2\sqrt{f(x)}},$$

und da der Zähler auf der linken Seite vom Grade $2m - 2$, $F(x)$ vom Grade $2m$ ist, so lässt sich die Formel (2) anwenden, und es folgt

$$(7) \qquad \sum \frac{dx}{\sqrt{f(x)}} = 0,$$

wenn die Summe auf sämmtliche Wurzeln der Gleichung (5) erstreckt ist.

Wir wenden dieses Theorem auf den einfachsten Fall, nämlich $m = 2$, an und erhalten dann folgenden Satz:

Wenn

$$(8) \qquad x_1, \sqrt{f(x_1)}; \quad x_2, \sqrt{f(x_2)}; \quad x_3, \sqrt{f(x_3)}; \quad x_4, \sqrt{f(x_4)}$$

vier Werthepaare sind, für welche irgend eine Function der Form

$$(9) \qquad a + bx + cx^2 + \sqrt{f(x)}$$

verschwindet, so sind diese Werthepaare nicht gänzlich von einander unabhängig, sondern es besteht zwischen ihnen die Differentialgleichung

$$(10) \qquad \frac{dx_1}{\sqrt{f(x_1)}} + \frac{dx_2}{\sqrt{f(x_2)}} + \frac{dx_3}{\sqrt{f(x_3)}} + \frac{dx_4}{\sqrt{f(x_4)}} = 0.$$

Die Abhängigkeit dieser vier Werthepaare, also eine Integration der Differentialgleichung (10). kann aber auch in algebraischer Weise ausgedrückt werden, indem man die Function (9) für $x = x_1, x_2, x_3, x_4$ gleich Null setzt und dann $a, b, c$ eliminirt. Man erhält so die Determinantengleichung

$$(11) \qquad \begin{vmatrix} 1, & x_1, & x_1^2, & \sqrt{f(x_1)} \\ 1, & x_2, & x_2^2, & \sqrt{f(x_2)} \\ 1, & x_3, & x_3^2, & \sqrt{f(x_3)} \\ 1, & x_4, & x_4^2, & \sqrt{f(x_4)} \end{vmatrix} = 0.$$

Aus dieser Gleichung kann man $x_1$ und $\sqrt{f(x_1)}$ rational durch $x_2, \sqrt{f(x_2)}$; $x_3, \sqrt{f(x_3)}$; $x_4, \sqrt{f(x_4)}$ ausdrücken; denn $x_1$ ist die Wurzel einer biquadratischen Gleichung, deren drei andere Wurzeln $x_2, x_3, x_4$ sind, und deren Coëfficienten rational von $x_2, \sqrt{f(x_2)}$; $x_3, \sqrt{f(x_3)}$; $x_4, \sqrt{f(x_4)}$ abhängen, und $\sqrt{f(x_1)}$ ist mittels (11) rational durch $x_1$ darstellbar. Setzt man $x_4$ einer beliebigen Constanten gleich, so geht die Differentialgleichung (10) in (1) über und (11) ergiebt ein Integral derselben.

Wir wenden dies Theorem zunächst an auf die Legendre'sche Normalform und setzen also

$$f(x) = x(1 - x)(1 - \varkappa^2 x).$$

Nehmen wir in (11) $x_4 = 0$ an, so reducirt sich diese Gleichung durch Division mit $\sqrt{x_1 x_2 x_3}$ auf:

$$(12) \qquad \begin{vmatrix} \sqrt{x_1}, & x_1\sqrt{x_1}, & \sqrt{(1 - x_1)(1 - \varkappa^2 x_1)} \\ \sqrt{x_2}, & x_2\sqrt{x_2}, & \sqrt{(1 - x_2)(1 - \varkappa^2 x_2)} \\ \sqrt{x_3}, & x_3\sqrt{x_3}, & \sqrt{(1 - x_3)(1 - \varkappa^2 x_3)} \end{vmatrix} = 0,$$

oder wenn wir die Determinante nach den Elementen der ersten Horizontalreihe entwickeln

$$(13) \qquad \sqrt{x_1}(a + b x_1) + c\sqrt{(1 - x_1)(1 - \varkappa^2 x_1)} = 0,$$

worin zur Abkürzung gesetzt ist

$$(14) \qquad \begin{aligned} a &= x_2\sqrt{x_2}\sqrt{(1-x_3)(1-\varkappa^2 x_3)} - x_3\sqrt{x_3}\sqrt{(1-x_2)(1-\varkappa^2 x_2)}, \\ b &= -\sqrt{x_2}\sqrt{(1-x_3)(1-\varkappa^2 x_3)} + \sqrt{x_3}\sqrt{(1-x_2)(1-\varkappa^2 x_2)}, \\ c &= -(x_2 - x_3)\sqrt{x_2}\sqrt{x_3}. \end{aligned}$$

Wenn wir (13) rational machen, so erhalten wir die cubische Gleichung

$$x\,(a + b\,x)^2 - c^2(1 - x)\,(1 - \varkappa^2 x) = 0,$$

deren drei Wurzeln $x_1$, $x_2$, $x_3$ sind. Es ist demnach identisch

$$(15)\quad b^2(x - x_1)(x - x_2)(x - x_3) = x\,(a + b\,x)^2 - c^2(1 - x)(1 - \varkappa^2 x),$$

und indem wir in dieser identischen Gleichung $x = 0,\ 1,\ 1 : \varkappa^2$ setzen, so folgt:

$$\sqrt{x_1\,x_2\,x_3} = -\frac{c}{b}$$

$$(16)\quad \sqrt{(1 - x_1)\,(1 - x_2)\,(1 - x_3)} = \frac{b + a}{b}$$

$$\sqrt{(1 - \varkappa^2 x_1)\,(1 - \varkappa^2 x_2)\,(1 - \varkappa^2 x_3)} = \frac{b + \varkappa^2 a}{b}.$$

Zur Bestimmung der Vorzeichen in diesen Gleichungen erhalten wir noch aus (13), wenn wir $x_1$ durch $x_2$ und $x_3$ ersetzen und die Ergebnisse multipliciren:

$$x_1\,x_2\,x_3\,(a + b\,x_1)\,(a + b\,x_2)\,(a + b\,x_3) = -c^3 \sqrt{f(x_1)}\,\sqrt{f(x_2)}\,\sqrt{f(x_3)}$$

und (15) ergiebt für $x = -a:b$

$$(a + b\,x_1)\,(a + b\,x_2)\,(a + b\,x_3) = \frac{c^2}{b}\,(b + a)\,(b + \varkappa^2 a).$$

Benutzt man noch das Quadrat der ersten Gleichung (16), so folgt hieraus

$$(17)\quad \sqrt{f(x_1)}\,\sqrt{f(x_2)}\,\sqrt{f(x_3)} = -\frac{c}{b^3}\,(b + a)\,(b + \varkappa^2 a),$$

so dass die Vorzeichen in (16) so gewählt sind, dass das Product der linken Seiten den durch die Differentialgleichung (1) geforderten Werth von $\sqrt{f(x_1)}$ ergiebt. Eine weitere Bestimmung der Vorzeichen ist in (16) der Natur der Sache nach nicht möglich, und diese Gleichungen dienen zur eindeutigen Definition von $\sqrt{x_1}$, $\sqrt{1 - x_1}$, $\sqrt{1 - \varkappa^2 x_1}$, wenn die $\sqrt{x_2}$, $\sqrt{1 - x_2}$, $\sqrt{1 - \varkappa^2 x_2}$, $\sqrt{x_3}$, $\sqrt{1 - x_3}$, $\sqrt{1 - \varkappa^2 x_3}$ als gegeben vorausgesetzt werden.

Um die Gleichungen (16) in die gebräuchliche Form zu bringen, machen wir zunächst in (14) den Zähler von $b$ rational und erhalten

$$b = -\frac{(x_2 - x_3)\,(1 - \varkappa^2 x_2\,x_3)}{\sqrt{x_2}\,\sqrt{(1 - x_3)\,(1 - \varkappa^2 x_3)} + \sqrt{x_3}\,\sqrt{(1 - x_2)\,(1 - \varkappa^2 x_2)}},$$

ferner:

$$b + a =$$
$$-\sqrt{(1-x_2)(1-x_3)}\left\{\sqrt{x_2(1-x_2)}\sqrt{1-\varkappa^2 x_3}-\sqrt{x_3(1-x_3)}\sqrt{1-\varkappa^2 x_2}\right\}$$

$$b + \varkappa^2 a =$$
$$-\sqrt{(1-\varkappa^2 x_2)(1-\varkappa^2 x_3)}\left\{\sqrt{x_2(1-\varkappa^2 x_2)}\sqrt{1-x_3}-\sqrt{x_3(1-\varkappa^2 x_3)}\sqrt{1-x_2}\right\},$$

wodurch die Gleichungen (16) leicht in die Form gebracht werden:

$$\sqrt{x_1} = -\frac{\sqrt{x_2}\sqrt{(1-x_3)(1-\varkappa^2 x_3)}+\sqrt{x_3}\sqrt{(1-x_2)(1-\varkappa^2 x_2)}}{1-\varkappa^2 x_2 x_3},$$

$$(17)\quad \sqrt{1-x_1} = \frac{\sqrt{1-x_2}\sqrt{1-x_3}-\sqrt{x_2 x_3}\sqrt{(1-\varkappa^2 x_2)(1-\varkappa^2 x_3)}}{1-\varkappa^2 x_2 x_3},$$

$$\sqrt{1-\varkappa^2 x_1} = \frac{\sqrt{1-\varkappa^2 x_2}\sqrt{1-\varkappa^2 x_3}-\varkappa^2\sqrt{x_2 x_3}\sqrt{(1-x_2)(1-x_3)}}{1-\varkappa^2 x_2 x_3},$$

und unsere Betrachtung lehrt, dass, wenn $x_1$ und die Wurzeln $\sqrt{x_1}$, $\sqrt{1-x_1}$, $\sqrt{1-\varkappa^2 x_1}$ durch diese Gleichungen als Functionen von $x_2$, $x_3$ bestimmt werden, die Differentialgleichung (1) identisch befriedigt ist.

---

Um auch für die Weierstrass'sche Normalform das Additionstheorem in möglichst einfacher Gestalt zu erhalten, setze man

$$f(x) = 4x^3 - g_2 x - g_3,$$

und lasse in der Gleichung (11) (nach Division mit $x_4^2$) $x_4$ unendlich gross werden. Es ergiebt sich alsdann das Integral der Differentialgleichung (1)

$$\frac{dx_1}{\sqrt{f(x_1)}}+\frac{dx_2}{\sqrt{f(x_2)}}+\frac{dx_3}{\sqrt{f(x_3)}}=0$$

in der Form

$$(18)\qquad \begin{vmatrix} 1, & x_1, & \sqrt{f(x_1)} \\ 1, & x_2, & \sqrt{f(x_2)} \\ 1, & x_3, & \sqrt{f(x_3)} \end{vmatrix} = 0,$$

oder

$$(19)\qquad a + b x_1 + c\sqrt{f(x_1)} = 0,$$

wenn

$$
\begin{aligned}
a &= x_2 \sqrt{f(x_3)} - x_3 \sqrt{f(x_2)} \\
b &= \sqrt{f(x_2)} - \sqrt{f(x_3)} \\
c &= x_3 - x_2.
\end{aligned}
\tag{20}
$$

Es werden dann $x_1$, $x_2$, $x_3$ die Wurzeln der cubischen Gleichung

$$(a + b x)^2 - c^2 f(x) = 0,$$

und wenn man hierin den Coëfficienten von $x^2$, getheilt durch den von $x^3$ gleich der negativen Summe der Wurzeln setzt, so erhält man

$$x_1 + x_2 + x_3 = \frac{1}{4}\left(\frac{\sqrt{f(x_2)} - \sqrt{f(x_3)}}{x_2 - x_3}\right)^2, \tag{21}$$

und aus (19)

$$\sqrt{f(x_1)} = \frac{1}{4}\left(\frac{\sqrt{f(x_2)} - \sqrt{f(x_3)}}{x_2 - x_3}\right)^3 - (x_2 + x_3)\frac{\sqrt{f(x_2)} - \sqrt{f(x_3)}}{x_2 - x_3} - \frac{x_3\sqrt{f(x_2)} - x_2\sqrt{f(x_3)}}{x_2 - x_3}. \tag{22}$$

## §. 10. Ursprung der elliptischen Functionen.

Wenn in dem elliptischen Differential erster Gattung in der Legendre'schen Normalform

$$\frac{1}{2}\,\frac{dz}{\sqrt{z(1-z)(1-\varkappa^2 z)}}$$

die Substitution

$$z = \sin^2\varphi$$

gemacht und sodann die Integration von $\varphi = 0$ an ausgeführt wird, so entsteht das elliptische Integral erster Gattung

$$\int_0^\varphi \frac{d\varphi}{\sqrt{1 - \varkappa^2 \sin^2\varphi}} = u.$$

Jacobi nennt die obere Grenze $\varphi$ dieses Integrals die Amplitude desselben und schreibt

$$\varphi = \operatorname{am} u.$$

Die trigonometrischen Functionen dieses Bogens

$$\sin\varphi,\ \cos\varphi,\ \sqrt{1 - \varkappa^2 \sin^2\varphi} = \Delta\varphi$$

sind es nun, welche, als Functionen von $u$ betrachtet, elliptische Functionen genannt und von Jacobi mit

$$\sin\!\text{am}\, u,\quad \cos\!\text{am}\, u,\quad \Delta\,\text{am}\, u,$$

oder, nach Gudermann, kürzer mit

$$\text{sn}\, u,\ \text{cn}\, u,\ \text{dn}\, u$$

bezeichnet werden. Die von Gauss, Abel, Jacobi begründete Theorie dieser Functionen zählt zu den bedeutsamsten und fruchtbarsten Fortschritten der neueren Mathematik. Diese Functionen stehen zu den elliptischen Integralen in einer analogen Beziehung, wie die trigonometrischen Functionen zu den Kreisfunctionen, und sind in mancher Hinsicht eine directe Verallgemeinerung der trigonometrischen Functionen. Unter den Eigenschaften dieser Functionen ist wohl die merkwürdigste die der doppelten Periodicität, eine Eigenschaft, welche in dem Gebiete der elementaren Functionen nirgends vorkommt, und so am deutlichsten zeigte, dass man es hier mit einer ganz neuen Functionenart zu thun habe. Die aus der doppelten Periodicität abgeleiteten Folgerungen sind es zugleich, welche, wie die Erfahrung gezeigt hat, weitaus am schnellsten mit befriedigender Strenge in das Innere der Theorie einführen, so dass hier der zweckmässigste Ausgangspunkt für eine methodische Entwickelung zu suchen ist. Unsere nächsten Betrachtungen werden daher den doppelt periodischen Functionen im Allgemeinen gewidmet sein.

## Zweiter Abschnitt.

# Theta-Functionen.

---

### §. 11. Voraussetzungen aus der Functionentheorie.

Der Begriff der doppelt periodischen Functionen kann nur dann richtig aufgefasst werden, wenn man dieselben als Functionen eines complexen Arguments $u = v + iw$ betrachtet, worin $i$ wie gewöhnlich die Bedeutung von $\sqrt{-1}$ hat. Die Variable $u$ gilt uns als unabhängige und unbeschränkt veränderliche Grösse, welche nach dem Vorgang von Gauss durch die Punkte einer Ebene in der Weise geometrisch veranschaulicht wird, dass der Punkt, dessen Coordinaten in einem rechtwinkligen System $v$, $w$ sind, als Träger des Werthes $u = v + iw$ angesehen und kurz als der Punkt $u$ bezeichnet wird.

Wir betrachten hier solche Functionen $\varphi(u)$ des complexen Arguments $u$, welche Weierstrass eindeutige analytische Functionen nennt, die durch folgende Eigenschaften charakterisirt sind.

1. In jedem endlichen Flächenstück liegt eine endliche Anzahl von Punkten, in welchen die Function $\varphi(u)$ nicht stetig ist, und die daher Unstetigkeitspunkte genannt werden.

2. Ist $u_0$ ein nicht zu den Unstetigkeitspunkten gehöriger Punkt, so ist die Function entwickelbar in eine nach ganzen aufsteigenden positiven Potenzen von $u - u_0$ fortschreitende Reihe, welche convergent ist in einem Kreise, der den Punkt $u_0$ zum Mittelpunkte hat und bis zum nächstgelegenen Unstetigkeitspunkte reicht. Man sagt, die Function habe in der Umgebung des Punktes $u_0$ den Charakter einer ganzen Function.

3. Ist $u_0$ ein Unstetigkeitspunkt, so giebt es eine ganze positive Zahl $m$, so dass $(u - u_0)^m \varphi(u)$ in dem Punkte $u_0$ endlich

und stetig bleibt und daher nach ganzen positiven Potenzen von $u - u_0$ entwickelbar ist. Der Unstetigkeitspunkt wird in diesem Falle von der $m$ten Ordnung genannt. Es ergiebt sich daraus eine Entwickelung von $\varphi(u)$ nach steigenden Potenzen von $u - u_0$, welche mit $(u - u_0)^{-m}$ anfängt und in einem um $u_0$ beschriebenen Kreise, der bis zum nächstgelegenen Unstetigkeitspunkte reicht, convergirt. Der Coëfficient von $(u - u_0)^{-1}$ in dieser Entwickelung heisst das Residuum dieser Function für den Punkt $u_0$.

4. Der Cauchy'sche Satz. Das Integral

$$\frac{1}{2\pi i}\int \varphi(u)\, du,$$

in positivem Sinne über die Begrenzung eines endlichen Flächenstücks erstreckt, welches auf der Randlinie keine Unstetigkeitspunkte enthält, ist gleich der Summe der Residuen für die im Inneren des Flächenstücks liegenden Unstetigkeitspunkte. Als positive Integrationsrichtung ist dabei diejenige anzusehen, welche gegen das Innere des Flächenstücks so liegt, wie die $v$-Axe zur $w$-Axe, so dass bei der üblichen Bestimmungsweise dieser Axen beim positiven Durchlaufen des Randes das Innere der Fläche zur Linken bleibt.

5. Die Function

$$\psi(u) = \frac{d \log \varphi(u)}{du} = \frac{1}{\varphi(u)} \frac{d\varphi(u)}{du}$$

hat nur Unstetigkeitspunkte erster Ordnung, und wenn in einem Punkte $u_0$ das Product $(u - u_0)^{-m}\varphi(u)$ endlich und von Null verschieden ist, so ist $m$ das Residuum von $\psi(u)$ für diesen Punkt. Ist $m$ positiv, so heisst $u_0$ ein Nullpunkt $m$ter Ordnung von $\varphi(u)$.

Hiernach ist eine unmittelbare Folgerung des Cauchy'schen Theorems:

6. Das Integral

$$\frac{1}{2\pi i}\int d \log \varphi(u),$$

ausgedehnt in positiver Richtung über die Begrenzung eines Flächenstücks, ist gleich der Anzahl der Nullpunkte, vermindert um die Anzahl der Unstetigkeitspunkte, welche in diesem Flächenstück liegen, wobei Nullpunkte und Unstetigkeitspunkte $m$ter Ordnung wie $m$ solche Punkte erster Ordnung zu zählen sind.

In gleichem Sinne ergiebt sich

7. Das Integral

$$\frac{1}{2\pi i}\int u\, d \log \varphi(u)$$

ist gleich der Summe der Werthe von $u$, für welche $\varphi(u)$ verschwindet, vermindert um die Summe der Werthe von $u$, in welchen $\varphi(u)$ unendlich wird.

8. Eine Function, welche im Endlichen gar keine Unstetigkeitspunkte besitzt, heisst eine ganze Function. Eine ganze Function, welche auch im Unendlichen endlich bleibt, ist eine Constante.

9. Als Corollar hieraus ergiebt sich, dass eine einwerthige Function, welche nur eine endliche Anzahl von Unendlichkeitspunkten endlicher Ordnung hat, eine rationale Function sein muss.

## §. 12. Das Periodenparallelogramm.

Eine Function $\varphi(u)$ von $u$, welche die Eigenschaft hat, dass für ein constantes $\omega$ und für jeden Werth von $u$

$$\varphi(u + \omega) = \varphi(u)$$

ist, heisst periodisch und $\omega$ heisst die Periode.

Der Gegenstand unserer Untersuchung sind Functionen $\varphi(u)$ mit zwei Perioden $\omega_1$, $\omega_2$, von denen wir ein- für allemal voraussetzen wollen, dass ihr Verhältniss $\omega_2 : \omega_1$ nicht reell und dass der imaginäre Theil dieses Verhältnisses positiv sei.

Jede Combination $m_1 \omega_1 + m_2 \omega_2$ ist, wenn $m_1$, $m_2$ ganze Zahlen sind, gleichfalls eine Periode.

Wir nehmen in der Ebene $u$ einen beliebigen Punkt $u_0$ an und bezeichnen die vier Punkte

$$u_0, \qquad u_0 + \omega_1, \qquad u_0 + \omega_1 + \omega_2, \qquad u_0 + \omega_2;$$

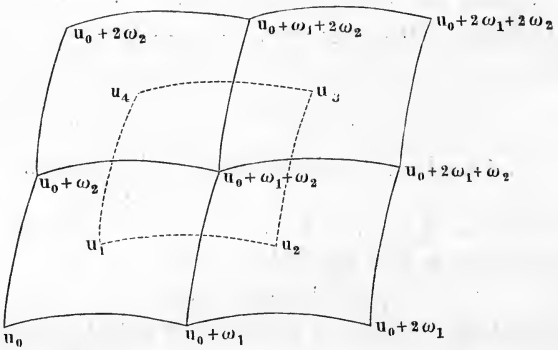
verbinden wir diese vier Punkte der Reihe nach durch gerade Linien, indem wir vom letzten zum ersten zurückkehren, so erhalten wir ein Parallelogramm, welches das Periodenparallelogramm genannt wird. Es können die geradlinigen Seiten des Periodenparallelogramms auch durch krummlinige Züge ersetzt werden, wenn nur die gegenüberliegenden durch Parallelverschiebung zur Deckung gelangen und die einzelnen Züge keine Schleifen bilden.

Durch Aneinanderreihen solcher congruenter Periodenparallelogramme lässt sich die ganze $u$-Ebene einfach und lückenlos überdecken. Entsprechende Punkte zweier verschiedener dieser Parallelogramme sind die Repräsentanten von $u$-Werthen, die sich um ganzzahlige Vielfache der Perioden unterscheiden und die nach dem Modul $(\omega_1, \omega_2)$ congruent oder, wenn kein Zweifel möglich ist, kurzweg congruent genannt werden. Das Zeichen der Congruenz ist nach Gauss

$$u \equiv u' \pmod{\omega_1, \omega_2},$$

und besagt, dass $u'$ die Form $u + m_1\omega_1 + m_2\omega_2$ hat, wenn $m_1$, $m_2$ ganze Zahlen sind.

Fig. 1.



So stellt die Figur 1 vier an einander gelagerte Periodenparallelogramme dar; die Punkte $u_1$, $u_2$, $u_3$, $u_4$ sind congruent:

$$u_2 = u_1 + \omega_1, \quad u_3 = u_1 + \omega_1 + \omega_2, \quad u_4 = u_1 + \omega_2,$$

und $u_1$, $u_2$, $u_3$, $u_4$ bilden ebenfalls die Ecken eines Periodenparallelogramms.

Die doppelt periodische Function $\varphi(u)$ hat in allen congruenten Punkten denselben Werth, so dass der ganze Werthvorrath dieser Function in einem Periodenparallelogramm sich erschöpft, wenn von zwei gegenüberliegenden Seiten nur die eine mit zum Parallelogramm gerechnet wird.

Wir ziehen aus unseren allgemeinen Voraussetzungen die Folgerung:

Es existirt (ausser der Constanten) keine doppelt periodische Function, welche im Periodenparallelogramm frei von Unstetigkeitspunkten ist; denn eine solche Function wäre in der ganzen $u$-Ebene endlich und müsste also nach §. 11, 8 eine Constante sein.

## §. 13. Die Functionen $T$.

Da nach dem zuletzt ausgesprochenen Satz keine ganzen doppelt periodischen Functionen existiren, so suchen wir solche als Quotienten zweier ganzer Functionen darzustellen, welche nicht doppelt periodisch sein können, sondern bei der Vermehrung des Arguments um die Perioden gewisse Factoren annehmen.

Um eine möglichst einfache Annahme zu machen, setzen wir voraus, dass diese Factoren Exponentialfunctionen sind mit in $u$ linearen Exponenten.

Wir bezeichnen hiernach als $T$-Function, $T(u)$, eine ganze Function von $u$, welche die folgenden beiden Gleichungen erfüllt:

$$(1)\qquad \begin{aligned} T(u+\omega_1) &= e^{-\pi i[a_1(2u+\omega_1)+b_1]}\, T(u) \\ T(u+\omega_2) &= e^{-\pi i[a_2(2u+\omega_2)+b_2]}\, T(u), \end{aligned}$$

worin $a_1$, $a_2$, $b_1$, $b_2$ constante, d. h. von $u$ unabhängige Grössen sind.

Die beiden Exponentialfactoren

$$e^{-\pi i[a_1(2u+\omega_1)+b_1]}, \qquad e^{-\pi i[a_2(2u+\omega_2)+b_2]},$$

die wir gleich in einer für die Folge zweckmässigen Form angenommen haben, sollen die Periodicitätsfactoren der $T$-Function genannt werden.

1. Man erkennt sofort, indem man in der ersten Gleichung (1) $u$ in $u+\omega_2$, in der zweiten $u$ in $u+\omega_1$ verwandelt und beide Werthe von $T(u+\omega_1+\omega_2)$ einander gleich setzt, dass die Gleichungen (1) nur unter der Bedingung mit einander verträglich sind, dass

$$(2)\qquad a_2\,\omega_1 - a_1\,\omega_2 = m$$

eine ganze Zahl ist. Diese Zahl wird die Ordnung der durch (1) definirten Function $T(u)$ genannt.

2. Wenn die Function $T(u)$ für irgend einen Werth von $u$ verschwindet, so verschwindet sie auch für alle congruenten Werthe, und man kennt alle Nullpunkte von $T(u)$ überhaupt, wenn man die in einem Periodenparallelogramm gelegenen kennt. Die Anzahl dieser Punkte ergiebt sich aber nach §. 11, 6

$$= \frac{1}{2\pi i}\int d\log T(u),$$

das Integral in positivem Sinne über die Begrenzung des Periodenparallelogramms erstreckt. Dies Integral lässt sich aber so darstellen:

$$\frac{1}{2\pi i}\int_{u_0}^{u_0+\omega_1} d\,[\log T(u) - \log T(u+\omega_2)]$$

$$-\frac{1}{2\pi i}\int_{u_0}^{u_0+\omega_2} d\,[\log T(u) - \log T(u+\omega_1)]$$

und ergiebt sich nach (1)

$$= a_2\,\omega_1 - a_1\,\omega_2 = m.$$

Die Ordnung einer $T$-Function ist also gleich der Anzahl der im Inneren eines Periodenparallelogramms gelegenen Nullpunkte und kann daher niemals negativ sein.

3. Nach dem Theorem 7. in §. 11 ist das in gleichem Sinne verstandene Integral über die Begrenzung des Periodenparallelogramms

$$\frac{1}{2\pi i}\int u\,d\log T(u) \tag{3}$$

gleich der Summe $\Sigma u^*$ der Werthe $u = u^*$, für welche $T(u)$ verschwindet. Dies Integral lässt sich aber wieder zerlegen in die beiden Bestandtheile:

$$\frac{1}{2\pi i}\int_{u_0}^{u_0+\omega_1} [u\,d\log T(u) - (u+\omega_2)\,d\log T(u+\omega_2)]$$

$$-\frac{1}{2\pi i}\int_{u_0}^{u_0+\omega_2} [u\,d\log T(u) - (u+\omega_1)\,d\log T(u+\omega_1)]$$

und dies ist nach (1)

$$a_2\int_{u_0}^{u_0+\omega_1}(u+\omega_2)\,du - a_1\int_{u_0}^{u_0+\omega_2}(u+\omega_1)\,du$$

$$-\frac{\omega_2}{2\pi i}\int_{u_0}^{u_0+\omega_1} d\log T(u) + \frac{\omega_1}{2\pi i}\int_{u_0}^{u_0+\omega_2} d\log T(u).$$

Jetzt lassen sich die Integrationen ausführen und es ist

$$\begin{aligned}\int_{u_0}^{u_0+\omega_1} d\,log\,T(u) &= log\,T(u_0+\omega_1) - log\,T(u_0)\\ &= -\pi i\,[a_1(2u_0+\omega_1)+b_1+2N_1]\\ \int_{u_0}^{u_0+\omega_2} d\,log\,T(u) &= log\,T(u_0+\omega_2) - log\,T(u_0)\\ &= -\pi i\,[a_2(2u_0+\omega_2)+b_2+2N_2],\end{aligned}$$

wenn $N_1$, $N_2$ unbestimmte ganze Zahlen sind. Ferner ist

$$\int_{u_0}^{u_0+\omega_1}(u+\omega_2)\,du = \omega_1\,(u_0+\omega_2)+\frac{1}{2}\omega_1^2$$

$$\int_{u_0}^{u_0+\omega_2}(u+\omega_1)\,du = \omega_2\,(u_0+\omega_1)+\frac{1}{2}\omega_2^2,$$

wonach unser Integral congruent wird mit

$$\Sigma u^* \equiv \frac{1}{2}\,\omega_1\,(m-b_2)+\frac{1}{2}\,\omega_2\,(m+b_1).$$

Es ist also die Summe der $u$-Werthe, für welche eine $T$-Function $m$ter Ordnung innerhalb eines Periodenparallelogramms verschwindet, congruent mit

$$\frac{m}{2}\,(\omega_1+\omega_2)+\frac{1}{2}\,(b_1\,\omega_2-b_2\,\omega_1).$$

4. Die einfachsten $T$-Functionen sind die von der nullten Ordnung. Wenn $T(u) = T^0(u)$ eine solche Function ist, so muss nach (2)

$$a_2\,\omega_1 - a_1\,\omega_2 = 0,$$

oder

(4) $$a_1 = \lambda\,\omega_1, \qquad a_2 = \lambda\,\omega_2,$$

worin $\lambda$ ein constanter Factor ist, ebenso nach 3, da hier gar keine Punkte $u^*$ vorhanden sind, also das Integral (3) den Werth Null hat,

$$\frac{1}{2}\,(b_1\,\omega_2 - b_2\,\omega_1)$$

congruent Null oder

(5) $$b_1 = \mu\,\omega_1 + 2\,n_1, \qquad b_2 = \mu\,\omega_2 + 2\,n_2,$$

wenn $\mu$ ein unbestimmter Factor, $n_1$, $n_2$ ganze Zahlen sind.

Daraus folgt, dass die Function

$$e^{\pi i(\lambda u^2+\mu u)}\,T^0(u)$$

die beiden Perioden $\omega_1$, $\omega_2$ hat, und da sie überdies eine ganze Function ist, so muss sie constant sein, also:

Die einzige $T$-Function nullter Ordnung ist, wenn $C$, $\lambda$, $\mu$ beliebige Constanten sind:

$$C e^{-\pi i (\lambda u^2 + \mu u)}. \tag{6}$$

Hieraus folgt noch:

Zwei $T$-Functionen mit denselben Perioden und den gleichen Nullpunkten unterscheiden sich nur durch einen Factor von der Form (6).

## §. 14. Die Charaktere der $T$-Function.

Nach 3., §. 13 hängt die Beziehung, welche zwischen den Nullpunkten einer $T$-Function stattfindet, wesentlich von der Grösse

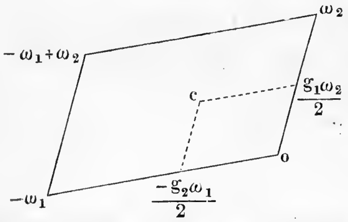
$$c = \frac{1}{2}(b_1 \omega_2 - b_2 \omega_1) + n_2 \omega_1 - n_1 \omega_2$$

ab, worin $n_1$, $n_2$ beliebige ganze Zahlen sind. Es lassen sich diese Zahlen so bestimmen, dass $c$ durch einen in einem beliebig gegebenen Periodenparallelogramm gelegenen Punkt dargestellt wird. Wählt man ein geradliniges Parallelogramm mit der Ecke 0, wie es Fig. 2 zeigt, so kann man $c$, und zwar nur auf eine Weise, in die Form setzen:

$$c = \frac{g_1 \omega_2 - g_2 \omega_1}{2},$$

worin $g_1$, $g_2$ reelle Zahlen zwischen 0 und 2, mit Einschluss von 0 und Ausschluss von 2, sind.

Fig. 2.



Den Punkt $c$ und alle mit ihm nach dem Modul $(\omega_1, \omega_2)$ congruenten Punkte nennen wir die charakteristischen Punkte der $T$-Function und das Zahlenpaar $(g_1, g_2)$ die Charakteristik derselben. Werden in einer Charakteristik die Zahlen $g_1$, $g_2$ um gerade Zahlen geändert, so soll die Charakteristik für ungeändert gelten. Danach wollen wir noch unter der Summe zweier Charakteristiken $(g_1, g_2)$ $(g_1', g_2')$ die Charakteristik $(g_1 + g_1', g_2 + g_2')$ verstehen.

Ist die Charakteristik $(g_1, g_2)$ gegeben, so ist

$$(1) \quad \begin{aligned} b_1 &= \mu\,\omega_1 + 2\,n_1 + g_1 \\ b_2 &= \mu\,\omega_2 + 2\,n_2 + g_2, \end{aligned}$$

worin $\mu$ eine beliebige Grösse ist. Werden $\mu$ und die ganzen Zahlen $n_1$, $n_2$ geändert, so bleibt die Charakteristik ungeändert.

Ist $c$ der charakteristische Punkt einer $T$-Function $m$ ter Ordnung, so ist die Summe der 0-Punkte dieser Function congruent mit $c$ oder mit $c + \frac{1}{2}(\omega_1 + \omega_2)$, je nachdem $m$ gerade oder ungerade ist.

Es ist also auch andererseits durch die Summe der Nullpunkte der $T$-Function $m$ ter Ordnung der charakteristische Punkt bestimmt.

Ist $T(u)$ eine $T$-Function $m$ ter Ordnung mit dem charakteristischen Punkte $c$, so ist, wenn $v$ eine beliebige Constante ist, $T(u + v)$ eine $T$-Function gleicher Ordnung mit dem charakteristischen Punkte

$$c' = c - v\,m.$$

Hiernach lassen sich, wenn $m > 0$ ist, die verschiedenen Charakteristiken durch Hinzufügung einer additiven Constanten zum Argument auf einander zurückführen.

## §. 15. Relationen zwischen verwandten $T$-Functionen.

Zwei $T$-Functionen von den gleichen Perioden, derselben Ordnung und derselben Charakteristik wollen wir verwandt nennen. Ist $T'(u)$ eine mit $T(u)$ verwandte $T$-Function und haben $a_1'$, $a_2'$, $b_1'$, $b_2'$ dieselbe Bedeutung für $T'$, wie $a_1$, $a_2$, $b_1$, $b_2$ für $T$, so ist in Folge der vorausgesetzten Verwandtschaft (§. 13, 14):

$$(2) \quad \begin{aligned} a_1' &= a_1 + \lambda\,\omega_1, & b_1' &= b_1 + 2\,n_1 + \mu\,\omega_1, \\ a_2' &= a_2 + \lambda\,\omega_2, & b_2' &= b_2 + 2\,n_2 + \mu\,\omega_2, \end{aligned}$$

worin $\lambda$, $\mu$ beliebige Grössen, $n_1$, $n_2$ ganze Zahlen.

Daher ist

$$e^{-\pi i (\lambda u^2 + \mu u)}\; T(u)$$

eine $T$-Function, welche dieselben Periodit\u00e4tsfactoren hat wie $T'(u)$, und daher der Satz:

1. Verwandte $T$-Functionen können durch Hinzufügung von Factoren der Form:

$$L = Ce^{-\pi i(\lambda u^2 + \mu u)}$$

($T^0$-Functionen) in solche verwandelt werden, welche dieselben Periodicitätsfactoren haben.

Ferner folgt unmittelbar aus §. 13, 3.

2. Wenn verwandte $T$-Functionen $m$ter Ordnung $m - 1$ gemeinsame Nullpunkte im Periodenparallelogramm haben, so haben sie auch den $m$ten gemeinsam;

und hieraus:

3. Zwischen höchstens $m + 1$ verwandten $T$-Functionen $m$ter Ordnung $T, T_1, \ldots T_m$ besteht eine identische Gleichung von der Form

$$L T + L_1 T_1 + \cdots L_m T_m = 0.$$

Denn besteht diese Relation nicht bereits für $L = 0$, so kann man von den in $L_1, L_2, \ldots L_m$ verfügbaren Constanten zunächst $\lambda_1, \lambda_2 \ldots \lambda_m, \mu_1, \mu_2 \ldots \mu_m$ so bestimmen, dass die sämmtlichen Producte $L_1 T_1, L_2 T_2 \ldots, L_m T_m$ dieselben Periodicitätsfactoren erhalten, und dann die $C_1, C_2 \ldots C_m$ so, dass $m - 1$ und folglich alle Nullpunkte der Function $L_1 T_1 + L_2 T_2 + \cdots L_m T_m$ mit den Nullpunkten der Function $T$ zusammen fallen. Daraus aber folgt nach §. 13, 4, dass das Verhältniss von $L_1 T_1 + L_2 T_2 + \cdots L_m T_m$ zu $T$ gleich einer $T^0$-Function $-L$ ist, was zu beweisen ist.

4. Die Quotienten verwandter $T$-Functionen können durch Hinzufügung eines Factors $L$ in doppelt periodische Functionen verwandelt werden.

5. Multiplicirt man zwei (verwandte oder nicht verwandte) $T$-Functionen $T, T'$ mit den gleichen Perioden, so entsteht eine neue $T$-Function, deren Periodicitätsfactoren die Producte der entsprechenden Periodicitätsfactoren von $T$ und $T'$ sind. Die Ordnung der neuen $T$-Function ist also gleich der Summe der Ordnungen der beiden Factoren, und die Charakteristik ist die Summe der Charakteristiken der beiden Factoren.

6. Setzen wir die Existenz einer $T$-Function erster Ordnung $t(u)$, voraus, so lässt sich daraus jede $T$-Function $m$ter Ordnung ableiten.

Es sei nämlich $c$ der charakteristische Punkt von $t(u)$ und $u_1, u_2, \ldots u_m$ beliebig gegebene Werthe. Es verschwindet dann die Function

$$t\left[(u - u_i + \frac{1}{2}(\omega_1 + \omega_2) + c\right] = t_i(u), \qquad i = 1, 2, \ldots m$$

in dem Punkte $u_i$ und allen mit $u_i$ congruenten Punkten, aber in keinem anderen. Nach §. 14 ist der charakteristische Punkt von $t_i(u)$ congruent mit $u_i + \frac{1}{2}(\omega_1 + \omega_2)$ und nach 5. ist das Product

$$T(u) = t_1(u)\, t_2(u) \ldots t_m(u)$$

eine $T$-Function $m$ter Ordnung mit den beliebig gegebenen Nullpunkten $u_1, u_2, \ldots u_m$, deren charakteristischer Punkt, wie es nach §. 14 sein muss, durch

$$\frac{m}{2}(\omega_1 + \omega_2) + u_1 + u_2 + \cdots u_m$$

bestimmt ist.

7. Hieraus lässt sich leicht beweisen, dass jede doppelt periodische Function, welche in einem Periodenparallelogramm nur eine endliche Anzahl von Unstetigkeitspunkten hat, als Quotient zweier $T$-Functionen darstellbar ist.

Es sei nämlich $\varphi(u)$ eine doppelt periodische Function mit den Perioden $\omega_1, \omega_2$ und den Unstetigkeitspunkten $u_1, u_2, \ldots u_m$, welche auch theilweise in Unstetigkeitspunkte höherer Ordnung zusammenfallen können.

Bestimmt man nach 6. eine Function $T(u)$ mit den Nullpunkten $u_1, u_2, \ldots u_m$, so ist:

$$T(u)\, \varphi(u) = T_1(u)$$

eine $T$-Function $m$ter Ordnung, und

$$\varphi(u) = \frac{T_1(u)}{T(u)} \qquad \textit{w. z. b. w.}$$

Die Functionen $T(u)$, $T_1(u)$ sind verwandt, da sie dieselben Periodicitätsfactoren und also auch dieselbe Charakteristik haben.

Die Nullpunkte von $T_1(u)$ sind zugleich die Nullpunkte von $\varphi(u)$ und die Summe dieser Nullwerthe ist also congruent mit der Summe der Unstetigkeitswerthe.

Ist nun $C$ ein beliebiger constanter Werth, so hat die Function

$$\varphi(u) - C$$

dieselben Unstetigkeitspunkte wie $\varphi(u)$ und hat also ebenso viele Nullpunkte.

Nennen wir daher $\varphi(u)$, wenn sie $m$ Unstetigkeitspunkte hat, eine doppelt periodische Function $m$ter Ordnung, so können wir das hiermit Bewiesene in folgende Sätze zusammenfassen:

8. Eine doppelt periodische Function $m$ter Ordnung nimmt jeden beliebigen Werth $C$ in $m$ Punkten des Periodenparallelogramms an; die Summe der Werthe des Arguments, für welche $\varphi(u) = C$ wird, ist einer constanten, d. h. von $C$ unabhängigen Grösse congruent. Doppelt periodische Functionen erster Ordnung existiren nicht.

## §. 16. $T$-Functionen erster Ordnung.

Wir gehen nun dazu über, die $T$-Functionen erster Ordnung, die wir mit $t(u)$ bezeichnen, und aus welchen sich die übrigen $T$-Functionen, wie wir gesehen haben, ableiten lassen, näher zu bestimmen.

Aus 3 des vorigen Paragraphen folgt, dass zwei $t$-Functionen derselben Charakteristik sich nur durch einen Factor von der Form

$$C e^{-\pi i(\lambda u^2 + \mu u)}$$

von einander unterscheiden, und wir wollen nun durch eine Erweiterung der Definition diesen Factor noch näher bestimmen.

Dies soll, was nach §. 14, 15, (1), (2) ohne Beschränkung der Allgemeinheit möglich ist, so geschehen, dass in den Periodicitätsfactoren

$$a_1 = 0, \quad b_1 = g_1, \quad b_2 = g_2$$

wird, wenn $(g_1, g_2)$ die Charakteristik ist; wegen der Relation

$$a_2\,\omega_1 - a_1\,\omega_2 = 1$$

ist dann

$$a_2 = \frac{1}{\omega_1};$$

und die Bedingungen für diese $t$-Function lauten alsdann (§. 13, 1):

$$\begin{aligned} t(u + \omega_1) &= e^{-\pi i g_1}\, t(u) \\ t(u + \omega_2) &= e^{-\pi i \frac{2u + \omega_2}{\omega_1}}\, e^{-\pi i g_2}\, t(u), \end{aligned} \tag{1}$$

und hierdurch ist die Function $t(u)$ bis auf einen von $u$ unabhängigen Factor bestimmt. Um diesen Factor noch näher zu bestimmen, fassen wir die Abhängigkeit der Function $t$ auch von $\omega_1$, $\omega_2$ ins Auge und bezeichnen sie, indem wir $g_1$, $g_2$ als gegebene von $\omega_1$, $\omega_2$ unabhängige Zahlen betrachten, mit $t(u, \omega_1, \omega_2)$. Es zeigt sich dann, dass, wenn $h$ ein willkürlicher Factor ist,

$$t(hu, h\omega_1, h\omega_2)$$

gleichfalls den Bedingungen (1) genügt, und dass demnach

$$\frac{t(hu, h\omega_1, h\omega_2)}{t(u, \omega_1, \omega_2)} = f(\omega_1, \omega_2) \tag{2}$$

von $u$ unabhängig ist.

Die Function $f(\omega_1, \omega_2)$ kann aber immer in die Form gesetzt werden:

$$f(\omega_1, \omega_2) = \frac{\varphi(h\omega_1, h\omega_1)}{\varphi(\omega_1, \omega_2)},$$

man hat nur, wenn $t(u)$ für $u = 0$ nicht verschwindet:

$$\varphi(\omega_1, \omega_2) = t(0, \omega_1, \omega_2)$$

und wenn $t(0) = 0$ ist, etwa

$$\varphi(\omega_1, \omega_2) = \omega_1 t'(0, \omega_1, \omega_2)$$

zu setzen, wenn $t'$ die Differentiation nach $u$ bezeichnet. Indem man also jetzt

$$\frac{t(u, \omega_1, \omega_2)}{\varphi(\omega_1, \omega_2)} \tag{3}$$

wieder mit $t(u, \omega_1, \omega_2)$ bezeichnet, kann man den Bedingungen (1) noch die hinzufügen, dass für ein beliebiges $h$

$$t(u, \omega_1, \omega_2) = t(hu, h\omega_1, h\omega_2). \tag{4}$$

Die Function $t$ hängt also jetzt nur noch von zwei Veränderlichen, nämlich den Verhältnissen $u : \omega_1 : \omega_2$, ab. Wir setzen in (4)

$$h = \frac{1}{\omega_1}, \quad \frac{u}{\omega_1} = v, \quad \frac{\omega_2}{\omega_1} = \omega,$$

und erhalten

$$t(u, \omega_1, \omega_2) = t\left(\frac{u}{\omega_1}, 1, \frac{\omega_2}{\omega_1}\right) = \vartheta(v, \omega), \tag{5}$$

worin $\vartheta$ ein neues Functionszeichen ist.

Hierdurch ist also eine neue Function $\vartheta(v)$ definirt von nur zwei Variablen $v$, $\omega$, deren erstere unbeschränkt veränderlich ist, während $\omega$ nach der im §. 12 gemachten Voraussetzung einen positiven imaginären Bestandtheil hat.

## §. 17. Die $\vartheta$-Function.

Die Function $\vartheta(v)$ ist eine ganze Function von $v$, welche den Bedingungen genügt:

$$(1) \qquad \begin{aligned} \vartheta(v+1) &= e^{-\pi i g_1}\, \vartheta(v) \\ \vartheta(v+\omega) &= e^{-\pi i (2v+\omega)}\, e^{-\pi i g_2}\, \vartheta(v), \end{aligned}$$

und ist dadurch bis auf einen von $v$ unabhängigen Factor bestimmt. Sie ist also unter den $t$-Functionen als Specialfall enthalten, während andererseits die allgemeine $t$-Function durch die $\vartheta$-Function ausgedrückt werden kann in der Weise:

$$t(u) = C e^{-\pi i (\lambda u^2 + \mu u)}\, \vartheta\left(\frac{u}{\omega_1}, \frac{\omega_2}{\omega_1}\right),$$

worin $C$, $\lambda$, $\mu$ beliebige constante oder von $\omega_1$, $\omega_2$ abhängige Grössen sind.

Die Function $\vartheta$ ist noch von den in der Charakteristik vorkommenden Zahlen $g_1$, $g_2$ abhängig, und wenn eine Bezeichnung dieser Abhängigkeit erforderlich ist, so soll für $\vartheta(v, \omega)$:

$$\vartheta_{g_1, g_2}(v, \omega)$$

gesetzt werden.

Entsprechend den $T$-Functionen höherer Ordnung werden wir auch $\Theta$-Functionen $m$ter Ordnung einführen und verstehen darunter eine ganze Function von $v$, welche den Bedingungen genügt:

$$(2) \qquad \begin{aligned} \Theta(v+1) &= e^{-\pi i g_1}\, \Theta(v) \\ \Theta(v+\omega) &= e^{-m\pi i (2v+\omega)}\, e^{-\pi i g_2}\, \Theta(v). \end{aligned}$$

Auch hierbei kann die Charakteristik $g_1, g_2$ in die Bezeichnung mit aufgenommen werden:

$$\Theta_{g_1, g_2}(v, \omega).$$

Diese Functionen sind als specielle Fälle unter den $T$-Functionen enthalten, und man kann allgemeine $T$-Functionen in der Weise bilden:

$$(3) \qquad C e^{-\pi i (\lambda u^2 + \mu u)} \, \Theta\left(\frac{u}{\omega_1}, \frac{\omega_2}{\omega_1}\right).$$

Es ergiebt sich also aus §. 15, 3 der Fundamentalsatz für die $\Theta$-Functionen, den wir folgendermaassen aussprechen:

Nennen wir $\Theta$-Functionen gleicher Ordnung und gleicher Charakteristik verwandt, und bezeichnen wir ferner ein System von Functionen als linear abhängig oder unabhängig, je nachdem eine homogene lineare Relation mit constanten (nicht sämmtlich verschwindenden) Coëfficienten zwischen diesen Functionen besteht oder nicht besteht, so gilt der Satz:

> $m + 1$ verwandte $\Theta$-Functionen $m$ter Ordnung sind immer linear abhängig;

oder:

> Aus $m$ linear unabhängigen verwandten $\Theta$-Functionen $m$ter Ordnung lässt sich jede andere verwandte $\Theta$-Function linear (mit constanten Coëfficienten) zusammensetzen.

Dieser Satz ist für unsere folgenden Betrachtungen von der fundamentalsten Bedeutung; es ergiebt sich daraus nach §. 15, 3, dass jede $T$-Function $m$ter Ordnung sich mit Anwendung der Formel (3) aus $m$ linear unabhängigen $\Theta$-Functionen zusammensetzen lässt.

Nach dem Satz 3, §. 13 ist die Summe der $m$ Argumentwerthe, für welche die Function $\Theta_{g_1, g_2}(v)$ im Periodenparallelogramm verschwindet, nach dem Modul $(1, \omega)$ congruent mit

$$m \, \frac{1 + \omega}{2} + \frac{g_1 \omega - g_2}{2}.$$

Die bis jetzt gegebene Definition der Function $\vartheta$ lässt einen Factor, welcher eine Function von $\omega$ sein kann, unbestimmt. Wir können aber noch eine Bestimmung hinzufügen, durch welche sich dieser Factor ergiebt.

Wenn man die Definitionsgleichungen (1) zweimal nach $v$ und einmal nach $\omega$ differentiirt, indem man $g_1, g_2$ als constant ansieht, so ergiebt sich nach einfacher Rechnung, dass die Function

$$\frac{\partial^2 \vartheta(v, \omega)}{\partial v^2} - 4\pi i \frac{\partial \vartheta(v, \omega)}{\partial \omega}$$

selbst den Bedingungen (1) genügt und also die Form

$$\varphi(\omega)\, \vartheta(v, \omega)$$

hat, worin $\varphi(\omega)$ in Bezug auf $v$ constant, also eine Function von $\omega$ allein ist. Wenn man also jetzt

$$e^{-\frac{1}{4\pi i}\int \varphi(\omega)\, d\omega}\, \vartheta(v, \omega)$$

gleich einem neuen $\vartheta$ setzt, so ergiebt sich für dieses die partielle Differentialgleichung

$$\frac{\partial^2 \vartheta(v, \omega)}{\partial v^2} - 4\pi i \frac{\partial \vartheta(v, \omega)}{\partial \omega} = 0, \tag{4}$$

und durch (1) und (4) ist jetzt die Function $\vartheta$ bis auf einen von $v$ und $\omega$, also nur noch von $g_1, g_2$ abhängigen Factor definirt.

## §. 18. Die Theta-Functionen verschiedener Charakteristiken. Hauptcharakteristiken.

Wir wollen jetzt, ehe wir zur Bestimmung des noch übrigen von $v$ und $\omega$ unabhängigen Factors in den $\vartheta$-Functionen gehen, die verschiedenen Charakteristiken auf einander zurückführen, was nach §. 14 immer möglich ist. Bezeichnet man mit $\vartheta(v)$ die zur Charakteristik (0, 0) gehörige $\vartheta$-Function, so ist

$$\Phi(v, \omega) = e^{-\pi i g_1 v}\, \vartheta\left(v - \frac{g_1 \omega - g_2}{2}\right)$$

eine den Bedingungen (1) §. 17 genügende Function. Es ist aber nun mit Rücksicht auf die Differentialgleichung (4):

$$\frac{\partial^2 \Phi}{\partial v^2} - 4\pi i \frac{\partial \Phi}{\partial \omega} = \pi^2 g_1^2 \Phi,$$

so dass, wenn wir

$$\vartheta_{g_1, g_2}(v) = e^{\frac{\pi i \omega g_1^2}{4} - \pi i g_1 v + \frac{g_1 g_2 \pi i}{2}}\, \vartheta\left(v - \frac{g_1 \omega - g_2}{2}\right) \tag{5}$$

setzen, die Differentialgleichung (4) durch alle diese Functionen befriedigt wird. Hierdurch also sind die Functionen $\vartheta_{g_1, g_2}$ bis auf einen allen gemeinschaftlichen numerischen Factor bestimmt.

Aus der Formel (5) lässt sich eine allgemeinere ableiten, indem man $v$ durch $v - \frac{g_1' \omega - g_2'}{2}$ ersetzt. Man erhält so

$$\begin{aligned}(6) \qquad &\vartheta_{g_1, g_2}\left(v - \frac{g_1' \omega - g_2'}{2}\right) \\ &= e^{-\frac{\pi i \omega}{4} g_1'^2 + \pi i g_1' v - \pi i g_1 g_2' - \frac{\pi i}{2} g_1' (g_2 + g_2')} \vartheta_{g_1 + g_1', g_2 + g_2'}(v).\end{aligned}$$

Aus (6) ergiebt sich noch, mit Benutzung von (1), wenn man $g_1' = 2$, $g_2' = 0$, oder $g_1' = 0$, $g_2' = 2$ setzt:

$$\begin{aligned}(7) \qquad \vartheta_{g_1 + 2, g_2}(v) &= \vartheta_{g_1, g_2}(v), \\ \vartheta_{g_1, g_2 + 2}(v) &= e^{+\pi i g_1} \vartheta_{g_1, g_2}(v),\end{aligned}$$

so dass durch (6) zugleich die Periodicität der Functionen $\vartheta_{g_1, g_2}(v)$ vollständig ausgedrückt ist; die Formel (6) ist gültig für ganz beliebige, selbst complexe Werthe von $g_1$, $g_2$.

Wenn man in den Definitionsformeln der $\vartheta$-Functionen [§. 17, (1)] $v$ durch $-v-1$, und durch $-v-\omega$, ferner $g_1$, $g_2$ durch $-g_1$, $-g_2$ ersetzt, so zeigt sich, dass $\vartheta_{-g_1, -g_2}(-v)$ denselben Bedingungen genügt, wie $\vartheta_{g_1, g_2}(v)$ und dass sonach

$$\vartheta_{g_1, g_2}(v), \quad \vartheta_{-g_1, -g_2}(-v)$$

bis auf einen constanten Factor identisch sind; es ist also insbesondere, wie aus $v = 0$ hervorgeht:

$$\vartheta_{0,0}(v) = \vartheta_{0,0}(-v),$$

und danach ergiebt die Formel (5), wenn man $v$, $g_1$, $g_2$ durch $-v$, $-g_1$, $-g_2$ ersetzt:

$$(8) \qquad \vartheta_{g_1, g_2}(v) = \vartheta_{-g_1, -g_2}(-v).$$

Sind die Elemente $g_1$, $g_2$ ganze Zahlen, so heisst $(g_1, g_2)$ eine Hauptcharakteristik. Es giebt deren vier wesentlich verschiedene, nämlich:

$$(0,0),\ (0,1),\ (1,0),\ (1,1),$$

und demnach auch vier wesentlich verschiedene Haupt-$\vartheta$-Functionen:

$$(9) \qquad \vartheta_{00}(v),\ \vartheta_{01}(v),\ \vartheta_{10}(v),\ \vartheta_{11}(v),$$

von denen die erste auch mit $\vartheta(v)$ bezeichnet wird.

In der Folge werden unter Charakteristiken und $\vartheta$-Functionen nur noch Hauptcharakteristiken und Hauptfunctionen verstanden.

Die Formel (6), auf dies Functionensystem angewandt, ergiebt die folgende, häufig angewandte Tabelle:

$$\begin{array}{l}
\vartheta_{01}(v) = \vartheta_{00}\left(v+\frac{1}{2}\right) \\
\vartheta_{10}(v) = e^{\frac{\pi i\omega}{4}+\pi i v}\,\vartheta_{00}\left(v+\frac{\omega}{2}\right) \\
\vartheta_{11}(v) = -\,i\,e^{\frac{\pi i\omega}{4}+\pi i v}\,\vartheta_{00}\left(v+\frac{1+\omega}{2}\right) \\
\hline
\vartheta_{00}(v) = \vartheta_{01}\left(v+\frac{1}{2}\right) \\
\vartheta_{11}(v) = -\,i\,e^{\frac{\pi i\omega}{4}+\pi i v}\,\vartheta_{01}\left(v+\frac{\omega}{2}\right) \\
\vartheta_{10}(v) = e^{\frac{\pi i\omega}{4}+\pi i v}\,\vartheta_{01}\left(v+\frac{1+\omega}{2}\right) \\
\hline
\vartheta_{11}(v) = -\,\vartheta_{10}\left(v+\frac{1}{2}\right) \\
\vartheta_{00}(v) = e^{\frac{\pi i\omega}{4}+\pi i v}\,\vartheta_{10}\left(v+\frac{\omega}{2}\right) \\
\vartheta_{01}(v) = i\,e^{\frac{\pi i\omega}{4}+\pi i v}\,\vartheta_{10}\left(v+\frac{1+\omega}{2}\right) \\
\hline
\vartheta_{10}(v) = \vartheta_{11}\left(v+\frac{1}{2}\right) \\
\vartheta_{01}(v) = -\,i\,e^{\frac{\pi i\omega}{4}+\pi i v}\,\vartheta_{11}\left(v+\frac{\omega}{2}\right) \\
\vartheta_{00}(v) = e^{\frac{\pi i\omega}{4}+\pi i v}\,\vartheta_{11}\left(v+\frac{1+\omega}{2}\right). \\
\hline
\end{array}\tag{10}$$

Nach (7), (8) ist

$$\begin{array}{ll}
\vartheta_{00}(-v) = \vartheta_{00}(v), & \vartheta_{01}(-v) = \vartheta_{01}(v), \\
\vartheta_{01}(-v) = \vartheta_{10}(v), & \vartheta_{11}(-v) = -\,\vartheta_{11}(v);
\end{array}\tag{11}$$

d. h. es sind $\vartheta_{00}(v)$, $\vartheta_{01}(v)$, $\vartheta_{10}(v)$ gerade Functionen, $\vartheta_{11}(v)$ ist eine ungerade Function.

Nach §. 17 verschwinden die vier Functionen (9), beziehungsweise für die folgenden Werthe des Arguments

$$\frac{1+\omega}{2},\ \frac{\omega}{2},\ \frac{1}{2},\ 0,$$

also für gewisse halbe Perioden. Von Wichtigkeit sind die Werthe, welche die sämmtlichen Functionen (9) für diese Argumentwerthe annehmen, und diese lassen sich mittelst der obigen Tabelle auf die drei

$$\vartheta_{00}(0)=\vartheta_{00},\quad \vartheta_{01}(0)=\vartheta_{01},\quad \vartheta_{10}(0)=\vartheta_{10}$$

zurückführen. Man erhält so das folgende System von 16 Formeln:

$$\begin{array}{ll@{\qquad}ll}
\vartheta_{00}(0) & =\vartheta_{00} & \vartheta_{01}(0) & =\vartheta_{01} \\
\vartheta_{00}\left(\frac{1}{2}\right) & =\vartheta_{01} & \vartheta_{01}\left(\frac{1}{2}\right) & =\vartheta_{00} \\
\vartheta_{00}\left(\frac{\omega}{2}\right) & =e^{-\frac{\pi i\omega}{4}}\vartheta_{10} & \vartheta_{01}\left(\frac{\omega}{2}\right) & =0 \\
\vartheta_{00}\left(\frac{1+\omega}{2}\right) & =0 & \vartheta_{01}\left(\frac{1+\omega}{2}\right) & =e^{-\frac{\pi i\omega}{4}}\vartheta_{10} \\
\hline
\vartheta_{10}(0) & =\vartheta_{10} & \vartheta_{11}(0) & =0 \\
\vartheta_{10}\left(\frac{1}{2}\right) & =0 & \vartheta_{11}\left(\frac{1}{2}\right) & =\vartheta_{10} \\
\vartheta_{10}\left(\frac{\omega}{2}\right) & =e^{-\frac{\pi i\omega}{4}}\vartheta_{00} & \vartheta_{11}\left(\frac{\omega}{2}\right) & =i\,e^{-\frac{\pi i\omega}{4}}\vartheta_{01} \\
\vartheta_{10}\left(\frac{1+\omega}{2}\right) & =-\,i\,e^{-\frac{\pi i\omega}{4}}\vartheta_{01} & \vartheta_{11}\left(\frac{1+\omega}{2}\right) & =e^{-\frac{\pi i\omega}{4}}\vartheta_{00}.
\end{array} \tag{12}$$

Die Quadrate der Functionen (9)

$$\vartheta_{00}^2(v),\ \vartheta_{01}^2(v),\ \vartheta_{10}^2(v),\ \vartheta_{11}^2(v) \tag{13}$$

sind $\Theta_{00}$-Functionen zweiter Ordnung, und folglich bestehen zwischen denselben zwei lineare Relationen. Nehmen wir diese Relationen in der Form an:

$$\begin{aligned}
\vartheta_{10}^2(v) &= A\,\vartheta_{01}^2(v)+B\,\vartheta_{11}^2(v),\\
\vartheta_{00}^2(v) &= A'\,\vartheta_{01}^2(v)+B'\,\vartheta_{11}^2(v),
\end{aligned}$$

so kann man die Coëfficienten auf Grund der Tabelle (12) leicht bestimmen, wenn man $v=0$ und $v=\frac{\omega}{2}$ setzt. Man erhält so

$$(14)\qquad \begin{aligned} \vartheta_{01}^2\, \vartheta_{10}^2(v) &= \vartheta_{10}^2\, \vartheta_{01}^2(v) - \vartheta_{00}^2\, \vartheta_{11}^2(v) \\ \vartheta_{01}^2\, \vartheta_{00}^2(v) &= \vartheta_{00}^2\, \vartheta_{01}^2(v) - \vartheta_{10}^2\, \vartheta_{11}^2(v), \end{aligned}$$

und daraus noch, indem man $v = \frac{1}{2}$ setzt:

$$(15)\qquad \vartheta_{00}^4 = \vartheta_{01}^4 + \vartheta_{10}^4.$$

Durch zwei beliebige von den Quadraten (13) können alle Functionen $\Theta_{00}$ der zweiten Ordnung linear dargestellt werden; aber auch die übrigen $\Theta$-Functionen zweiter Ordnung lassen sich durch die Functionen $\vartheta_{g_1, g_2}$ zusammensetzen, denn man erhält für jede Charakteristik zwei linear unabhängige Producte, von denen das eine eine gerade, das andere eine ungerade Function ist, nämlich:

$$(16)\qquad \begin{array}{llll} \vartheta_{00}(v)\, \vartheta_{01}(v), & \vartheta_{10}(v)\, \vartheta_{11}(v) & \text{Charakteristik} & (0,1) \\ \vartheta_{00}(v)\, \vartheta_{10}(v), & \vartheta_{01}(v)\, \vartheta_{11}(v) & \quad\text{„} & (1,0) \\ \vartheta_{10}(v)\, \vartheta_{01}(v), & \vartheta_{00}(v)\, \vartheta_{11}(v) & \quad\text{„} & (1,1) \end{array}$$

Nach demselben Princip lassen sich nun $\Theta$-Functionen beliebiger Ordnung und beliebiger Charakteristik aus den Functionen $\vartheta$ zusammensetzen. Um dies nachzuweisen, bezeichnen wir mit $\Theta_0$, $\Theta_1$ irgend zwei der $\vartheta$-Quadrate (13) und mit $F^{(n)}(\Theta_0, \Theta_1)$ eine ganze rationale und homogene Function $n$ter Ordnung der beiden Argumente $\Theta_0$, $\Theta_1$. Man erhält hiernach für die $\Theta$-Functionen $m$ter Ordnung $\Theta^{(m)}(v)$ folgende Ausdrücke:

$m$ gerade — gerade Functionen

$$\begin{aligned} \Theta_{00}^{(m)}(v) &= F^{\left(\frac{m}{2}\right)}(\Theta_0, \Theta_1) \\ \Theta_{01}^{(m)}(v) &= \vartheta_{00}(v)\, \vartheta_{01}(v)\, F^{\left(\frac{m}{2}-1\right)}(\Theta_0, \Theta_1) \\ \Theta_{10}^{(m)}(v) &= \vartheta_{00}(v)\, \vartheta_{10}(v)\, F^{\left(\frac{m}{2}-1\right)}(\Theta_0, \Theta_1) \\ \Theta_{11}^{(m)}(v) &= \vartheta_{10}(v)\, \vartheta_{01}(v)\, F^{\left(\frac{m}{2}-1\right)}(\Theta_0, \Theta_1) \end{aligned}$$

(17) ungerade Functionen

$$\begin{aligned} \Theta_{00}^{(m)}(v) &= \vartheta_{00}(v)\, \vartheta_{10}(v)\, \vartheta_{01}(v)\, \vartheta_{11}(v)\, F^{\left(\frac{m-4}{2}\right)}(\Theta_0, \Theta_1) \\ \Theta_{01}^{(m)}(v) &= \vartheta_{10}(v)\, \vartheta_{11}(v)\, F^{\left(\frac{m}{2}-1\right)}(\Theta_0, \Theta_1) \\ \Theta_{10}^{(m)}(v) &= \vartheta_{01}(v)\, \vartheta_{11}(v)\, F^{\left(\frac{m}{2}-1\right)}(\Theta_0, \Theta_1) \\ \Theta_{11}^{(m)}(v) &= \vartheta_{00}(v)\, \vartheta_{11}(v)\, F^{\left(\frac{m}{2}-1\right)}(\Theta_0. \Theta_1) \end{aligned}$$

$m$ ungerade gerade Functionen

$$\Theta_{00}^{(m)}(v) = \vartheta_{00}(v)\,F^{\left(\frac{m-1}{2}\right)}(\Theta_0, \Theta_1)$$
$$\Theta_{01}^{(m)}(v) = \vartheta_{01}(v)\,F^{\left(\frac{m-1}{2}\right)}(\Theta_0, \Theta_1)$$
$$\Theta_{10}^{(m)}(v) = \vartheta_{10}(v)\,F^{\left(\frac{m-1}{2}\right)}(\Theta_0, \Theta_1)$$
$$\Theta_{11}^{(m)}(v) = \vartheta_{00}(v)\,\vartheta_{01}(v)\,\vartheta_{10}(v)\,F^{\left(\frac{m-3}{2}\right)}(\Theta_0, \Theta_1)$$

(18) ungerade Functionen

$$\Theta_{00}^{(m)}(v) = \vartheta_{01}(v)\,\vartheta_{10}(v)\,\vartheta_{11}(v)\,F^{\left(\frac{m-3}{2}\right)}(\Theta_0, \Theta_1)$$
$$\Theta_{01}^{(m)}(v) = \vartheta_{00}(v)\,\vartheta_{10}(v)\,\vartheta_{11}(v)\,F^{\left(\frac{m-3}{2}\right)}(\Theta_0, \Theta_1)$$
$$\Theta_{10}^{(m)}(v) = \vartheta_{00}(v)\,\vartheta_{01}(v)\,\vartheta_{11}(v)\,F^{\left(\frac{m-3}{2}\right)}(\Theta_0, \Theta_1)$$
$$\Theta_{11}^{(m)}(v) = \vartheta_{11}(v)\,F^{\left(\frac{m-1}{2}\right)}(\Theta_0, \Theta_1).$$

Dass in dieser Form alle $\Theta$-Functionen darstellbar sind, ergiebt sich auf Grund von §. 17 aus folgenden drei Erwägungen.

1. Zwischen geraden und ungeraden Functionen kann keine lineare Abhängigkeit bestehen, wenn nicht schon zwischen den geraden Functionen für sich oder den ungeraden für sich eine lineare Abhängigkeit besteht.

2. Da zwei der $\vartheta$-Quadrate (13) nicht in constantem Verhältniss stehen, so besteht auch keine Gleichung von der Form $F^{(n)}(\Theta_0, \Theta_1) = 0$.

3. Die Gesammtzahl der Constanten, welche nach (17), (18) in den zu einer und derselben Charakteristik gehörenden geraden und ungeraden Functionen auftreten, ist genau gleich der Ordnung $m$.

## §. 19. Das Additionstheorem.

Sind $u$, $v$ zwei Veränderliche, so gehören die Producte

$$\vartheta_{g_1, g_2}(u + v)\,\vartheta_{g'_1, g'_2}(u - v)$$

zu den $\Theta$-Functionen zweiter Ordnung, mit der Charakteristik

$$(g_1 + g'_1,\ g_2 + g'_2),$$

und zwar für jede der beiden Variablen $u$, $v$; sie sind also als Functionen von $v$ linear darstellbar durch die Functionen (13) und (16) in §. 18, so dass die Variable $u$ in den Coëfficienten vorkommt. Diese Darstellung ist, wenn die Charakteristik (0, 0) ist, auf mehrfache Art möglich, da man zwei beliebige der Functionen (13) wählen kann, in den anderen Fällen nur auf eine Art. Man erhält so 16 Formeln, von welchen aber 6 durch blosse Vertauschung von $v$ mit $-v$ aus den anderen herzuleiten sind, so dass nur 10 wesentlich verschiedene bleiben. Man leitet diese Formeln sehr leicht ab, indem man dieselben zunächst mit unbestimmten Coëfficienten ansetzt und diese dann dadurch bestimmt, dass man für $v$ solche specielle Werthe setzt, für welche je eine der Functionen $\vartheta(v)$ verschwindet. So ist z. B.:

$$\vartheta_{00}(u+v)\,\vartheta_{00}(u-v) = A\,\vartheta_{00}^2(v) + B\,\vartheta_{11}^2(v),$$

und wenn man $v = 0$ und $v = \frac{1+\omega}{2}$ setzt, so erhält man mit Benutzung der Formeln des §. 18:

$$A\,\vartheta_{00}^2 = \vartheta_{00}^2(u),\quad B\,\vartheta_{00}^2 = \vartheta_{11}^2(u),$$

also

$$(1)\quad \vartheta_{00}^2\,\vartheta_{00}(u+v)\,\vartheta_{00}(u-v) = \vartheta_{00}^2(u)\,\vartheta_{00}^2(v) + \vartheta_{11}^2(u)\,\vartheta_{11}^2(v),$$

und wenn man hierin $u$ durch

$$u+\frac{1}{2},\quad u+\frac{\omega}{2},\quad u+\frac{1+\omega}{2}$$

ersetzt, so bildet man drei weitere Relationen, die man auf demselben Wege wie (1) auch direct hätte ableiten können:

$$(2)\quad \vartheta_{01}^2\,\vartheta_{01}(u+v)\,\vartheta_{01}(u-v) = \vartheta_{01}^2(u)\,\vartheta_{01}^2(v) - \vartheta_{11}^2(u)\,\vartheta_{11}^2(v)$$

$$(3)\quad \vartheta_{10}^2\,\vartheta_{10}(u+v)\,\vartheta_{10}(u-v) = \vartheta_{10}^2(u)\,\vartheta_{10}^2(v) - \vartheta_{11}^2(u)\,\vartheta_{11}^2(v)$$

$$(4)\quad \vartheta_{01}^2\,\vartheta_{11}(u+v)\,\vartheta_{11}(u-v) = \vartheta_{11}^2(u)\,\vartheta_{01}^2(v) - \vartheta_{01}^2(u)\,\vartheta_{11}^2(v).$$

Diese vier Gleichungen können, wie schon erwähnt, durch Anwendung der Formeln (14) des vorigen Paragraphen in mannigfacher Weise umgeformt werden. Die folgenden 6 Formeln haben nur eine Form. Es ist, um wieder mit einem beliebigen Beispiel zu beginnen:

$$\vartheta_{00}(u+v)\,\vartheta_{11}(u-v) = A\,\vartheta_{01}(v)\,\vartheta_{10}(v) + B\,\vartheta_{00}(v)\,\vartheta_{11}(v),$$

und wenn man $v = 0$ setzt:

$$A\,\vartheta_{01}\,\vartheta_{10} = \vartheta_{00}(u)\,\vartheta_{11}(u),$$

daraus erhält man $B$ durch Vertauschung von $u$ mit $v$. So sind die drei folgenden Formeln abgeleitet:

$$(5)\qquad \vartheta_{01}\vartheta_{10}\vartheta_{00}(u+v)\vartheta_{11}(u-v)$$
$$= \vartheta_{00}(u)\vartheta_{11}(u)\vartheta_{01}(v)\vartheta_{10}(v) - \vartheta_{01}(u)\vartheta_{10}(u)\vartheta_{00}(v)\vartheta_{11}(v),$$

$$(6)\qquad \vartheta_{00}\vartheta_{01}\vartheta_{10}(u+v)\vartheta_{11}(u-v)$$
$$= \vartheta_{10}(u)\vartheta_{11}(u)\vartheta_{00}(v)\vartheta_{01}(v) - \vartheta_{00}(u)\vartheta_{01}(u)\vartheta_{10}(v)\vartheta_{11}(v),$$

$$(7)\qquad \vartheta_{00}\vartheta_{10}\vartheta_{01}(u+v)\vartheta_{11}(u-v)$$
$$= \vartheta_{01}(u)\vartheta_{11}(u)\vartheta_{00}(v)\vartheta_{10}(v) - \vartheta_{00}(u)\vartheta_{10}(u)\vartheta_{01}(v)\vartheta_{11}(v),$$

welche sich unmittelbar verificiren lassen, indem man erst $u$, dann $v = 0$ setzt. Hieraus folgen die drei anderen durch Vermehrung von $u$ um

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

$$(8)\qquad \vartheta_{01}\vartheta_{10}\vartheta_{01}(u+v)\vartheta_{10}(u-v)$$
$$= \vartheta_{01}(u)\vartheta_{10}(u)\vartheta_{01}(v)\vartheta_{10}(v) + \vartheta_{00}(u)\vartheta_{11}(u)\vartheta_{00}(v)\vartheta_{11}(v),$$

$$(9)\qquad \vartheta_{00}\vartheta_{01}\vartheta_{00}(u+v)\vartheta_{01}(u-v)$$
$$= \vartheta_{00}(u)\vartheta_{01}(u)\vartheta_{00}(v)\vartheta_{01}(v) - \vartheta_{10}(u)\vartheta_{11}(u)\vartheta_{10}(v)\vartheta_{11}(v),$$

$$(10)\qquad \vartheta_{00}\vartheta_{10}\vartheta_{00}(u+v)\vartheta_{10}(u-v)$$
$$= \vartheta_{00}(u)\vartheta_{10}(u)\vartheta_{00}(v)\vartheta_{10}(v) + \vartheta_{01}(u)\vartheta_{11}(u)\vartheta_{01}(v)\vartheta_{11}(v).$$

Es lassen sich diese Formeln, deren Gesammtheit mit dem Namen des Additionstheorems bezeichnet wird, in mannigfacher Weise verallgemeinern, wovon das Folgende als Beispiel dienen möge.

Sind $u$, $v$ zwei Variable, so sind die vier Producte

$$\vartheta_{00}(u)\vartheta_{00}(u+v),\qquad \vartheta_{01}(u)\vartheta_{01}(u+v),$$
$$\vartheta_{10}(u)\vartheta_{10}(u+v),\qquad \vartheta_{11}(u)\vartheta_{11}(u+v),$$

als Functionen von $u$ betrachtet, verwandte $T$-Functionen zweiter Ordnung mit den gleichen Periodicitätsfactoren, so dass je drei derselben linear abhängig sind. Es ist also

$$A\vartheta_{00}(u)\vartheta_{00}(u+v) + B\vartheta_{10}(u)\vartheta_{10}(u+v) + C\vartheta_{11}(u)\vartheta_{11}(u+v)$$
$$= 0,$$

woraus für $u = 0$, $u = \frac{1}{2}$:

$$A\vartheta_{00}\vartheta_{00}(v) + B\vartheta_{10}\vartheta_{10}(v) = 0$$
$$A\vartheta_{01}\vartheta_{01}(v) + C\vartheta_{10}\vartheta_{10}(v) = 0$$

und daraus:

$$(11)\qquad \vartheta_{10}\,\vartheta_{10}(v)\,\vartheta_{00}(u)\,\vartheta_{00}(u+v) - \vartheta_{00}\,\vartheta_{00}(v)\,\vartheta_{10}(u)\,\vartheta_{10}(u+v) \\ - \vartheta_{01}\,\vartheta_{01}(v)\,\vartheta_{11}(u)\,\vartheta_{11}(u+v) = 0.$$

Ebenso sind nun auch, wenn $w$ eine dritte Variable ist, die in der Form

$$\vartheta_{g_1,g_2}(u+v)\,\vartheta_{g_1,g_2}(u+w), \quad \vartheta_{g_1,g_2}(u)\,\vartheta_{g_1,g_2}(u+v+w)$$

enthaltenen Producte, als Functionen von $u$ betrachtet, verwandte $T$-Functionen zweiter Ordnung mit den gleichen Periodicitätsfactoren, so dass zwischen je dreien unter ihnen eine lineare Abhängigkeit besteht. Die Coëfficienten bestimmt man wie oben durch specielle Werthe von $u$. So folgt das Formelsystem:

$$(12)\qquad \vartheta_{00}\,\vartheta_{00}(v+w)\,\vartheta_{00}(u+v)\,\vartheta_{00}(u+w) \\ = \vartheta_{00}(u)\,\vartheta_{00}(v)\,\vartheta_{00}(w)\,\vartheta_{00}(u+v+w) \\ - \vartheta_{11}(u)\,\vartheta_{11}(v)\,\vartheta_{11}(w)\,\vartheta_{11}(u+v+w).$$

$$(13)\qquad \vartheta_{01}\,\vartheta_{01}(v+w)\,\vartheta_{01}(u+v)\,\vartheta_{01}(u+w) \\ = \vartheta_{01}(u)\,\vartheta_{01}(v)\,\vartheta_{01}(w)\,\vartheta_{01}(u+v+w) \\ + \vartheta_{11}(u)\,\vartheta_{11}(v)\,\vartheta_{11}(w)\,\vartheta_{11}(u+v+w).$$

$$(14)\qquad \vartheta_{10}\,\vartheta_{10}(v+w)\,\vartheta_{10}(u+v)\,\vartheta_{10}(u+w) \\ = \vartheta_{10}(u)\,\vartheta_{10}(v)\,\vartheta_{10}(w)\,\vartheta_{10}(u+v+w) \\ + \vartheta_{11}(u)\,\vartheta_{11}(v)\,\vartheta_{11}(w)\,\vartheta_{11}(u+v+w).$$

## §. 20. Die Derivirten der $\vartheta$-Functionen.

Wir bezeichnen im Folgenden durch $\vartheta'_{g_1,g_2}(v)$, $\vartheta''_{g_1,g_2}(v)$ die nach $v$ genommenen Derivirten der Function $\vartheta_{g_1,g_2}(v)$ und mit $\vartheta'_{g_1,g_2}$, $\vartheta''_{g_1,g_2}$ die Werthe dieser Function für $v = 0$, so dass $\vartheta'_{01}$, $\vartheta'_{10}$, $\vartheta'_{00}$ verschwinden, weil $\vartheta_{01}(v)$, $\vartheta_{10}(v)$, $\vartheta_{00}(v)$ gerade Functionen von $v$ sind. Ebenso verschwindet $\vartheta''_{11}$.

Die sechs Functionen

$$\vartheta_{g_1,g_2}(v)\,\vartheta'_{g'_1,g'_2}(v) - \vartheta_{g'_1,g'_2}(v)\,\vartheta'_{g_1,g_2}(v)$$

sind, wie aus den Fundamentalgleichungen §. 17, (1) hervorgeht, $\vartheta$-Functionen zweiter Ordnung mit der Charakteristik

$$(g_1 + g'_1, \quad g_2 + g'_2),$$

und zugleich entweder gerade oder ungerade Functionen, wonach sich dieselben nach §. 18 sofort durch $\vartheta$-Functionen darstellen lassen. Ein constanter Factor wird durch einen speciellen Werth von $v$ ($v = 0$) bestimmt. So ist

$$\vartheta'_{11}(v)\,\vartheta_{01}(v) - \vartheta'_{01}(v)\,\vartheta_{11}(v) = A\,\vartheta_{10}(v)\,\vartheta_{00}(v). \tag{1}$$

$$A = \frac{\vartheta'_{11}\,\vartheta_{01}}{\vartheta_{10}\,\vartheta_{00}}. \tag{2}$$

Dieser Ausdruck für $A$ lässt sich aber noch vereinfachen.

Differentiiren wir (1) zweimal nach $v$ und setzen dann $v = 0$, so folgt

$$\vartheta'''_{11}\,\vartheta_{01} - \vartheta''_{01}\,\vartheta'_{11} = A\,(\vartheta''_{10}\,\vartheta_{00} + \vartheta_{10}\,\vartheta''_{00}),$$

und wenn man für $A$ den Werth (2) einführt:

$$\frac{\vartheta'''_{11}}{\vartheta'_{11}} = \frac{\vartheta''_{01}}{\vartheta_{01}} + \frac{\vartheta''_{10}}{\vartheta_{10}} + \frac{\vartheta''_{00}}{\vartheta_{00}}. \tag{3}$$

Nun genügen aber [nach §. 17, (4)] die vier Functionen $\vartheta'_{11}$, $\vartheta_{01}$, $\vartheta_{10}$, $\vartheta_{00}$ der Differentialgleichung

$$\vartheta'' = 4\,\pi i\,\frac{\partial \vartheta}{\partial \omega}, \tag{4}$$

wonach (3) sich schreiben lässt:

$$\frac{d \log \vartheta'_{11}}{d\omega} = \frac{d \log \vartheta_{00}\,\vartheta_{10}\,\vartheta_{01}}{d\omega},$$

oder durch Integration:

$$\vartheta'_{11} = c\,\vartheta_{00}\,\vartheta_{10}\,\vartheta_{01},$$

worin $c$ von $\omega$ unabhängig ist. Durch §. 17, 18 waren die $\vartheta$-Functionen bestimmt bis auf einen von $v$, $\omega$ unabhängigen, allen gemeinschaftlichen Factor. Ueber diesen Factor soll nun so verfügt werden, dass die Constante $c$ den Werth $\pi$ erhält, also die Formel besteht:

$$\vartheta'_{11} = \pi\,\vartheta_{00}\,\vartheta_{10}\,\vartheta_{01}, \tag{5}$$

und dadurch sind jetzt die $\vartheta$-Functionen bis auf das gemeinschaftliche Vorzeichen $\pm$ vollständig definirt. Durch Anwendung von (5) lässt sich der Formel (1) die Gestalt geben:

$$\vartheta'_{11}(v)\,\vartheta_{01}(v) - \vartheta'_{01}(v)\,\vartheta_{11}(v) = \pi\,\vartheta^2_{01}\,\vartheta_{10}(v)\,\vartheta_{00}(v), \tag{6}$$

und ebenso erhält man:

$$\vartheta'_{11}(v)\,\vartheta_{00}(v) - \vartheta'_{00}(v)\,\vartheta_{11}(v) = \pi\,\vartheta^2_{00}\,\vartheta_{10}(v)\,\vartheta_{01}(v), \tag{7}$$

$$\vartheta'_{11}(v)\,\vartheta_{10}(v) - \vartheta'_{10}(v)\,\vartheta_{11}(v) = \pi\,\vartheta^2_{10}\,\vartheta_{01}(v)\,\vartheta_{00}(v), \tag{8}$$

$$\vartheta'_{10}(v)\,\vartheta_{01}(v) - \vartheta'_{01}(v)\,\vartheta_{10}(v) = -\pi\,\vartheta^2_{00}\,\vartheta_{00}(v)\,\vartheta_{11}(v), \tag{9}$$

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

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

Differentiiren wir die Gleichungen (9), (10), (11) nach $v$ und setzen $v = 0$, so erhalten wir mittelst (4) und (5) die Relationen

$$4 \frac{d}{d\omega} \log \frac{\vartheta_{10}}{\vartheta_{01}} = i\pi \vartheta_{00}^4, \tag{12}$$

$$4 \frac{d}{d\omega} \log \frac{\vartheta_{00}}{\vartheta_{01}} = i\pi \vartheta_{10}^4, \tag{13}$$

$$4 \frac{d}{d\omega} \log \frac{\vartheta_{10}}{\vartheta_{00}} = i\pi \vartheta_{01}^4. \tag{14}$$

Wenn man die Fundamentalformeln für die $\vartheta$-Functionen zweimal logarithmisch differentiirt, so erkennt man, dass die Functionen

$$\vartheta^2(v) \frac{d^2 \log \vartheta(v)}{d v^2} = \vartheta''(v)\,\vartheta(v) - \vartheta'(v)\,\vartheta'(v)$$

$\Theta$-Functionen zweiter Ordnung mit der Charakteristik (0, 0) sind, und man kann sie daher durch die Functionen $\vartheta^2(v)$ linear ausdrücken. Auf diese Weise ergiebt sich

$$\vartheta_{00}^2\,\vartheta_{00}^2(v) \frac{d^2 \log \vartheta_{00}(v)}{d v^2} = \vartheta_{00}\,\vartheta_{00}''\,\vartheta_{00}^2(v) + \vartheta_{11}'^2\,\vartheta_{11}^2(v), \tag{15}$$

$$\vartheta_{01}^2\,\vartheta_{01}^2(v) \frac{d^2 \log \vartheta_{01}(v)}{d v^2} = \vartheta_{01}\,\vartheta_{01}''\,\vartheta_{01}^2(v) - \vartheta_{11}'^2\,\vartheta_{11}^2(v), \tag{16}$$

$$\vartheta_{10}^2\,\vartheta_{10}^2(v) \frac{d^2 \log \vartheta_{10}(v)}{d v^2} = \vartheta_{10}\,\vartheta_{10}''\,\vartheta_{10}^2(v) - \vartheta_{11}'^2\,\vartheta_{11}^2(v), \tag{17}$$

$$\vartheta_{00}^2\,\vartheta_{11}^2(v) \frac{d^2 \log \vartheta_{11}(v)}{d v^2} = \vartheta_{00}\,\vartheta_{00}''\,\vartheta_{11}^2(v) - \vartheta_{11}'^2\,\vartheta_{00}^2(v). \tag{18}$$

Hieraus lassen sich noch weitere Relationen herleiten durch fortgesetzte Differentiation. Wir führen noch eine dieser Formeln an, die sich ergiebt, wenn man (15) noch zweimal nach $v$ differentiirt und dann $v = 0$ setzt. Drückt man die Differentiationen nach $v$ durch solche nach $\omega$ aus mittelst der partiellen Differentialgleichung der $\vartheta$, so folgt

$$\frac{d^2 \log \vartheta_{00}}{d\omega^2} - 2\left(\frac{d \log \vartheta_{00}}{d\omega}\right)^2 = -\frac{\pi^2}{8}\,\vartheta_{10}^4\,\vartheta_{01}^4,$$

oder

$$\frac{d}{d\omega}\left(\frac{1}{\vartheta_{00}^4}\,\frac{d\,\vartheta_{00}^2}{d\omega}\right) = -\frac{\pi^2}{4}\,\frac{\vartheta_{10}^4\,\vartheta_{01}^4}{\vartheta_{00}^2}. \tag{19}$$

## §. 21. Darstellung der $\vartheta$-Functionen durch unendliche Producte.

Die Theorie der $\vartheta$-Functionen ist nun so weit gefördert, dass sich ihre Darstellung sehr leicht ergiebt. Damit wird dann die Existenz dieser Functionen nachgewiesen und die bisherigen Betrachtungen erhalten erst ihren sicheren Boden. Zwei Wege zu diesem Ziele stehen uns offen. Der erste geht aus von den uns schon bekannten Nullpunkten der $\vartheta$-Functionen, und setzt daraus unendliche Producte zusammen.

Die Function $\vartheta_{00}(v)$ verschwindet nach §. 18, wenn

$$2v = (2\nu - 1)\,\omega + (2\mu - 1)$$

ist, worin $\nu$, $\mu$ ganze Zahlen sind, oder wenn

$$e^{\pm 2\pi i v} = -\, e^{\pi i \omega (2\nu - 1)},$$

worin wir nun $\nu$ auf positive Zahlen beschränken können. Setzen wir also zur Abkürzung

$$e^{\pi i \omega} = q,$$

so ist $q$ eine Grösse, deren absoluter Werth ein echter Bruch ist. Das convergente unendliche Product

$$P(v) = \prod_{1,\infty}^{\nu} (1 + q^{2\nu-1} e^{2\pi i v})\,(1 + q^{2\nu-1} e^{-2\pi i v})$$

verschwindet also in allen und nur in den Punkten, in welchen $\vartheta_{00}(v)$ verschwindet, und es ist überdies

$$P(v+1) = P(v)$$

$$P(v+\omega) = \frac{1 + q^{-1} e^{-2\pi i v}}{1 + q\, e^{2\pi i v}}\, P(v) = q^{-1} e^{-2\pi i v} P(v),$$

so dass also nach §. 17

$$(1) \qquad \vartheta_{00}(v) = Q \prod_{1,\infty}^{\nu} (1 + q^{2\nu-1} e^{2\pi i v})\,(1 + q^{2\nu-1} e^{-2\pi i v}),$$

worin $Q$ ein von $v$ unabhängiger Factor ist. Nach den Formeln des §. 18 erhält man hieraus, indem man $v$ durch

$$v + \frac{1}{2}, \quad v + \frac{\omega}{2}, \quad v + \frac{1+\omega}{2}$$

ersetzt

$$\vartheta_{01}(v) = Q \prod_{1,\infty}^{\nu} (1 - q^{2\nu-1} e^{2\pi i v})(1 - q^{2v-1} e^{-2\pi i v}), \tag{2}$$

$$\vartheta_{10}(v) = Q q^{\frac{1}{4}} (e^{\pi i v} + e^{-\pi i v}) \prod_{1,\infty}^{\nu} (1 + q^{2\nu} e^{2\pi i v})(1 + q^{2\nu} e^{-2\pi i v}), \tag{3}$$

$$\vartheta_{11}(v) = - i Q q^{\frac{1}{4}} (e^{\pi i v} - e^{-\pi i v}) \prod_{1,\infty}^{\nu} (1 - q^{2\nu} e^{2\pi i v})(1 - q^{2\nu} e^{-2\pi i v}). \tag{4}$$

Setzt man in diesen Formeln $v = 0$, in der letzten nach einmaliger Differentiation, so folgt

$$\begin{aligned} \vartheta_{00} &= Q \prod_{1,\infty}^{\nu} (1 + q^{2\nu-1})^2 \\ \vartheta_{01} &= Q \prod_{1,\infty}^{\nu} (1 - q^{2\nu-1})^2 \\ \vartheta_{10} &= 2 Q q^{\frac{1}{4}} \prod_{1,\infty}^{\nu} (1 + q^{2\nu})^2 \\ \vartheta'_{11} &= 2 \pi Q q^{\frac{1}{4}} \prod_{1,\infty}^{\nu} (1 - q^{2\nu})^2. \end{aligned} \tag{5}$$

Hiernach lässt sich mittelst (5) §. 20:

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

der Factor $Q$ bestimmen. Man erhält zunächst

$$1 = Q^2 \prod^{\nu} \frac{(1 - q^{2\nu-1})^2 (1 + q^{2\nu-1})^2 (1 + q^{2\nu})^2}{(1 - q^{2\nu})^2},$$

oder, indem man das noch unbestimmte Vorzeichen von $Q$ jetzt bestimmt:

$$Q = \prod_{1,\infty}^{\nu} \frac{(1 - q^{2\nu})}{(1 + q^{2\nu})(1 + q^{2\nu-1})(1 - q^{2\nu-1})}.$$

Im Nenner kann man für $\Pi (1 + q^{2\nu})(1 + q^{2\nu-1})$ setzen $\Pi (1 + q^{\nu})$ und der Zähler $\Pi (1 - q^{2\nu})$ lässt sich zerlegen in

$$\Pi (1 - q^{\nu})(1 + q^{\nu}) = \Pi (1 - q^{2\nu})(1 - q^{2\nu-1})(1 + q^{\nu}).$$

Dadurch ergiebt sich endlich

$$Q = \prod^{\nu} (1 - q^{2\nu}). \tag{6}$$

Damit ist dann also auch das noch unbestimmte Vorzeichen der $\vartheta$-Functionen bestimmt.

Führen wir den Ausdruck (6) in die letzte Gleichung (5) ein, so ergiebt sich

$$\vartheta'_{11} = 2 \pi q^{\frac{1}{4}} \Pi (1 - q^{2\nu})^3,$$

und wenn wir also

$$\eta(\omega) = q^{\frac{1}{12}} \Pi (1 - q^{2\nu}) \tag{7}$$

setzen, so wird

$$\vartheta'_{11} = 2\pi\, \eta(\omega)^3. \tag{8}$$

Indem wir $Q$ mit Hülfe der Relation

$$Q = q^{-\frac{1}{12}} \eta(\omega)$$

aus (5) eliminiren, setzen wir

$$\begin{aligned} \vartheta_{00} &= \eta(\omega) f(\omega)^2, \\ \vartheta_{01} &= \eta(\omega) f_1(\omega)^2, \\ \vartheta_{10} &= \eta(\omega) f_2(\omega)^2, \end{aligned} \tag{9}$$

worin die Functionen $f(\omega)$, $f_1(\omega)$, $f_2(\omega)$ folgendermaassen definirt sind:

$$\begin{aligned} f(\omega) &= q^{-\frac{1}{24}} \overset{\nu}{\underset{1,\infty}{\Pi}} (1 + q^{2\nu-1}), \\ f_1(\omega) &= q^{-\frac{1}{24}} \overset{\nu}{\underset{1,\infty}{\Pi}} (1 - q^{2\nu-1}), \\ f_2(\omega) &= \sqrt{2}\, q^{\frac{1}{12}} \overset{\nu}{\underset{1,\infty}{\Pi}} (1 + q^{2\nu}). \end{aligned} \tag{10}$$

Die Functionen $\eta(\omega)$, $f(\omega)$, $f_1(\omega)$, $f_2(\omega)$ werden in unseren späteren Betrachtungen eine wichtige Rolle spielen. Aus §. 18 (15) ergiebt sich nach (9) die Relation

$$f(\omega)^8 = f_1(\omega)^8 + f_2(\omega)^8, \tag{11}$$

und aus §. 20 (5) nach (8)

$$f(\omega) f_1(\omega) f_2(\omega) = \sqrt{2}. \tag{12}$$

## §. 22. Darstellung der $\vartheta$-Functionen durch unendliche Reihen.

Der zweite Weg, um zur Darstellung der $\vartheta$-Functionen zu gelangen, besteht darin, dass man eine den Fundamentalgleichungen genügende convergente unendliche Reihe zu bilden sucht.

Bemerken wir zunächst, dass wegen der Bedingung

$$\vartheta_{00}(v + 1) = \vartheta_{00}(v)$$

die Function $\vartheta_{00}(v)$ als eindeutige Function von $e^{2\pi i v}$ angesehen werden kann, und setzen demgemäss

$$\vartheta_{00}(v) = \sum_{-\infty,\infty}^{\nu} A_\nu\, e^{2\pi i v \nu},$$

so ergiebt die Differentialgleichung §. 17 (4)

$$\frac{\partial^2 \vartheta}{\partial v^2} - 4\pi i \frac{\partial \vartheta}{\partial \omega} = 0$$

für $A_\nu$ die Bedingung

$$\frac{d A_\nu}{d\omega} = \pi i \nu^2 A_\nu, \quad A_\nu = c_\nu e^{\pi i \omega \nu^2} = c_\nu q^{\nu^2},$$

worin $c_\nu$ eine numerische Constante ist. Es wird also

$$\vartheta_{00}(v) = \Sigma\, c_\nu\, q^{\nu^2} e^{2\pi i v \nu}$$

und daraus

$$\vartheta_{00}(v+\omega) = \Sigma\, c_\nu\, q^{\nu^2+2\nu} e^{2\pi i v \nu}$$
$$= q^{-1} e^{-2\pi i v}\, \Sigma\, c_\nu\, q^{(\nu+1)^2} e^{2\pi i v(\nu+1)},$$

oder indem man $\nu - 1$ an Stelle von $\nu$ setzt, was, da $\nu$ von $-\infty$ bis $+\infty$ geht, gestattet ist

$$= q^{-1} e^{-2\pi i v}\, \Sigma\, c_{\nu-1}\, q^{\nu^2} e^{2\pi i v \nu}.$$

Nach der zweiten der Fundamentalgleichungen (§. 17, 1) müssen also die beiden Reihen

$$\Sigma\, c_\nu\, q^{\nu^2} e^{2\pi i v \nu} \text{ und } \Sigma\, c_{\nu-1}\, q^{\nu^2} e^{2\pi i v \nu}$$

mit einander übereinstimmen, d. h. es muss

$$c_{\nu-1} = c_\nu$$

sein. Die $c_\nu$ sind also alle einander gleich; dass sie den Werth 1 haben, ergiebt die Vergleichung der beiden Entwickelungen

$$\sum_{-\infty,\infty}^{\nu} q^{\nu^2} e^{2\pi i v \nu}, \quad \prod_{1,\infty}^{\nu} (1-q^{2\nu})(1+q^{2\nu-1} e^{2\pi i v})(1+q^{2\nu-1} e^{-2\pi i v})$$

für den Werth $q = 0$.

Der hiermit für $\vartheta_{00}(v)$ gefundenen Entwickelung kann man auch die reelle Form geben

$$(1) \qquad \vartheta_{00}(v) = \Sigma\, q^{\nu^2} e^{2\nu\pi i v}$$
$$= 1 + 2q \cos 2\pi v + 2q^4 \cos 4\pi v + 2q^9 \cos 6\pi v + \cdots,$$

und daraus erhält man nach §. 18, (10) durch Vermehrung von $v$ um $\frac{1}{2}, \frac{\omega}{2}, \frac{1+\omega}{2}$ die Entwickelungen für die drei übrigen $\vartheta$-Functionen:

$$(2) \qquad \vartheta_{01}(v) = \Sigma\, (-1)^\nu q^{\nu^2} e^{2\nu\pi i v}$$
$$= 1 - 2q \cos 2\pi v + 2q^4 \cos 4\pi v - 2q^9 \cos 6\pi v + \cdots$$

$$(3)\qquad \vartheta_{10}(v) = \Sigma\, q^{\frac{(2\nu+1)^2}{4}}\, e^{(2\nu+1)\pi i v}$$
$$= 2\, q^{\frac{1}{4}} \cos \pi v + 2\, q^{\frac{9}{4}} \cos 3\pi v + 2\, q^{\frac{25}{4}} \cos 5\pi v + \cdots$$

$$(4)\qquad \vartheta_{11}(v) = -i\, \Sigma\, (-1)^\nu\, q^{\frac{(2\nu+1)^2}{4}}\, e^{(2\nu+1)\pi i v}$$
$$= 2\, q^{\frac{1}{4}} \sin \pi v - 2\, q^{\frac{9}{4}} \sin 3\pi v + 2\, q^{\frac{25}{4}} \sin 5\pi v + \cdots$$

Ebenso kann man den unendlichen Producten eine reelle Form geben:

$$(5)\ \vartheta_{00}(v) = \overset{\nu}{\underset{1,\infty}{\Pi}} (1 - q^{2\nu})\, (1 + 2\, q^{2\nu-1} \cos 2\pi v + q^{4\nu-2})$$

$$(6)\ \vartheta_{01}(v) = \overset{\nu}{\underset{1,\infty}{\Pi}} (1 - q^{2\nu})\, (1 - 2\, q^{2\nu-1} \cos 2\pi v + q^{4\nu-2})$$

$$(7)\ \vartheta_{10}(v) = 2\, q^{\frac{1}{4}} \cos \pi v\ \overset{\nu}{\underset{1,\infty}{\Pi}} (1 - q^{2\nu})\, (1 + 2\, q^{2\nu} \cos 2\pi v + q^{4\nu})$$

$$(8)\ \vartheta_{11}(v) = 2\, q^{\frac{1}{4}} \sin \pi v\ \overset{\nu}{\underset{1,\infty}{\Pi}} (1 - q^{2\nu})\, (1 - 2\, q^{2\nu} \cos 2\pi v + q^{4\nu}).$$

Wir ziehen für spätere Anwendungen aus diesen Entwickelungen die Schlüsse:

Wenn der imaginäre Theil von $\omega$ ins Unendliche wächst, so dass der absolute Werth von $q$ verschwindet, so wird

$$\vartheta_{00}(v) = 1,\ \vartheta_{10}(v) = 1,\ q^{-\frac{1}{4}}\, \vartheta_{10}(v) = 2 \cos \pi v,$$
$$q^{-\frac{1}{4}}\, \vartheta_{11}(v) = 2 \sin \pi v.$$

Nehmen wir $\omega$ rein imaginär, also $q$ reell, positiv und echt gebrochen an, so sind für ein reelles $v$

1. $\vartheta_{00}(v)$, $\vartheta_{01}(v)$, $\vartheta_{10}(v)$, $\vartheta_{11}(v)$ reell, und wenn $v$ zwischen 0 und $\frac{1}{2}$ liegt, positiv, folglich auch $\vartheta_{00}$, $\vartheta_{01}$, $\vartheta_{10}$, $\vartheta'_{11}$ positiv;

2. $\vartheta_{00}(iv)$, $\vartheta_{01}(iv)$, $\vartheta_{10}(iv)$, $-i\vartheta_{11}(iv)$ reell, und so lange $v$ zwischen 0 und $\frac{-i\omega}{2}$ liegt, positiv; ferner mit Zuziehung der Formeln §. 18 (10)

3. $\vartheta_{00}\left(\frac{1}{2} + iv\right)$, $\vartheta_{01}\left(\frac{1}{2} + iv\right)$, $i\vartheta_{10}\left(\frac{1}{2} + iv\right)$, $\vartheta_{11}\left(\frac{1}{2} + iv\right)$ reell, und so lange $v$ zwischen 0 und $\frac{-i\omega}{2}$ liegt, positiv;

$$4.\quad q^{\frac{1}{4}}\, e^{\pi i v}\, \vartheta_{00}\left(\frac{\omega}{2}+v\right),\ -i\, q^{\frac{1}{4}}\, e^{\pi i v}\, \vartheta_{01}\left(\frac{\omega}{2}+v\right),$$

$$q^{\frac{1}{4}}\, e^{\pi i v}\, \vartheta_{10}\left(\frac{\omega}{2}+v\right),\ -i\, q^{\frac{1}{4}}\, e^{\pi i v}\, \vartheta_{11}\left(\frac{\omega}{2}+v\right)$$

reell, und so lange $v$ zwischen 0 und $\frac{1}{2}$ liegt, positiv.

# Dritter Abschnitt.

# Transformation der Theta-Functionen.

## §. 23. Das Transformationsprincip.

Wir kehren zurück zu den in §. 13 gegebenen Definitionsgleichungen der $T$-Functionen $m$ter Ordnung, und versehen darin aus einem gleich ersichtlichen Grunde die Buchstaben $\omega$, $a$, $b$, $m$ mit Accenten, so dass diese Gleichungen lauten:

$$
\begin{aligned}
T(u+\omega_1') &= e^{-\pi i(a_1'(2u+\omega_1')+b_1')}\,T(u) \\
T(u+\omega_2') &= e^{-\pi i a_1'(2u+\omega_2')+b_2'}\,T(u).
\end{aligned}
\tag{1}
$$

$$
a_2'\omega_1' - a_1'\omega_2' = m'. \tag{2}
$$

Sind $a$, $c$ irgend welche ganze (positive oder negative) Zahlen, so ergiebt die wiederholte Anwendung von (1)

$$
\begin{aligned}
&T(u - c\omega_1' + a\omega_2') \\
&= e^{-\pi i(-ca_1'+aa_2')(2u-c\omega_1'+a\omega_2')-\pi i(-cb_1'+ab_2'-m'ac)}\,T(u),
\end{aligned}
\tag{3}
$$

eine Gleichung, die auch aus einer der Gleichungen (1) hervorgeht, wenn man darin $a'$, $b'$, $\omega'$ durch

$$
-ca_1'+aa_2', \quad -cb_1'+ab_2'-m'ac, \quad -c\omega_1'+a\omega_2'
$$

ersetzt.

Hierin ist das Princip der Transformation der $T$-Functionen enthalten.

Es seien $b$, $\partial$ zwei andere ganze Zahlen, für welche die Determinante

$$
n = a\partial - bc \tag{4}
$$

einen positiven Werth hat. Wir setzen

$$
\begin{aligned}
\omega_1 &= +\partial\omega_1' - b\omega_2' \\
\omega_2 &= -c\omega_1' + a\omega_2',
\end{aligned}
\tag{5}
$$

und folglich

$$(6) \qquad \begin{aligned} n\,\omega_1' &= a\,\omega_1 + b\,\omega_2 \\ n\,\omega_2' &= c\,\omega_1 + \partial\,\omega_2. \end{aligned}$$

Es hat dann, wie man aus

$$\frac{\omega_2'}{\omega_1'} = \frac{c\,\omega_1 + \partial\,\omega_2}{a\,\omega_1 + b\,\omega_2}$$

durch Trennung des reellen vom imaginären Theil erkennt, der imaginäre Theil von $\omega_2 : \omega_1$ dasselbe Vorzeichen, wie der von $\omega_2' : \omega_1'$ (das positive).

Setzen wir

$$(7) \qquad \begin{aligned} a_1 &= \quad \partial\,a_1' - b\,a_2' \\ a_2 &= -\,c\,a_1' + a\,a_2' \end{aligned}$$

$$(8) \qquad \begin{aligned} b_1 &= \quad \partial\,b_1' - b\,b_2' - m'\,b\,\partial \\ b_2 &= -\,c\,b_1' + a\,b_2' - m'\,a\,c, \end{aligned}$$

so schliesst man aus (3), dass die Function $T(u)$ nicht nur den Bedingungen (1), sondern auch den aus (1) durch Vertauschung von $\omega_1'$, $\omega_2'$, $a_1'$, $a_2'$, $b_1'$, $b_2'$ mit $\omega_1$, $\omega_2$, $a_1$, $a_2$, $b_1$, $b_2$ hervorgehenden Gleichungen, d. h. den Gleichungen (1), §. 13, genügt. Sie ist also gleichzeitig eine $T$-Function der Perioden $\omega_1'$, $\omega_2'$ und der Perioden $\omega_1$, $\omega_2$, was wir durch folgende Gleichung andeuten:

$$(9) \qquad T'(u, \omega_1', \omega_2') = T(u, \omega_1, \omega_2).$$

Es ist aber nach (5) und (7)

$$a_2\,\omega_1 - a_1\,\omega_2 = (a_2'\,\omega_1' - a_1'\,\omega_2')\,(a\,\partial - b\,c),$$

also, wenn $m$ die Ordnung von $T$ ist,

$$(10) \qquad m = m'\,n.$$

Nach (8) ist die Charakteristik $(g_1, g_2)$ von $T$, wenn $(g_1', g_2')$ die von $T'$ ist, (§. 14),

$$(11) \quad (g_1, g_2) = (\partial\,g_1' - b\,g_2' - m'\,b\,\partial,\; -\,c\,g_1' + a\,g_2' - m'\,a\,c).$$

Unter der Transformation der $T$-Functionen versteht man die Darstellung der Functionen $T'$ mit den Perioden $\omega_1'$, $\omega_2'$ durch $T$-Functionen mit den Perioden $\omega_1$, $\omega_2$.

Die Zahlen $a$, $b$, $c$, $\partial$ heissen die Transformationszahlen und $n = a\,\partial - b\,c$ der Transformationsgrad.

Um die Form dieser Darstellung deutlicher zu übersehen, wollen wir die Bedingungen aufsuchen, unter welchen $T(u, \omega_1, \omega_2)$

eine $\Theta$-Function der $m$ten Ordnung $\Theta(u, \omega)$ wird (§. 17). Wir nehmen $b'_1$, $b'_2$ und folglich auch $b_1$, $b_2$ als ganze Zahlen, so dass $b_1$, $b_2$, $b'_1$, $b'_2$ durch $g_1$, $g_2$, $g'_1$, $g'_2$ ersetzt werden können. Es ist dann

$$\omega_1 = 1, \qquad \omega_2 = \omega, \qquad a_1 = 0, \qquad a_2 = m$$

zu setzen und demnach wird [nach (6), (7), (10)]

$$\omega'_1 = \frac{a + b\,\omega}{n}, \quad \omega'_2 = \frac{c + \partial\,\omega}{n},$$

$$a'_1 = m' b, \qquad a'_2 = m' \partial.$$

Die Function $T'(u, \omega'_1, \omega'_2)$ genügt also den Bedingungen (1):

$$T(u + \omega'_1) = (-1)^{g'_1}\, e^{-\pi i m' b (2u + \omega'_1)}\, T(u),$$

$$T(u + \omega'_2) = (-1)^{g'_2}\, e^{-\pi i m' \partial (2u + \omega'_2)}\, T(u),$$

und daraus ergiebt sich, dass das Product

$$e^{\frac{\pi i m' b u^2}{\omega'_1}}\, T'(u, \omega'_1, \omega'_2)$$

eine $\Theta$-Function der Ordnung $m'$ ist, mit den Argumenten

$$\frac{u}{\omega'_1}, \quad \frac{\omega'_2}{\omega'_1}$$

und der Charakteristik $(g'_1, g'_2)$. Wir können dies in der Gleichung ausdrücken:

$$e^{-\frac{\pi i m' n b u^2}{a + b\omega}}\, \Theta^{(m')}_{g'_1, g'_2}\left(\frac{n u}{a + b\,\omega}, \frac{c + \partial\,\omega}{a + b\,\omega}\right) = \Theta^{(m'n)}_{g_1, g_2}(u, \omega), \tag{12}$$

worin die Charakteristiken durch (11) bestimmt sind. Die Mittel zur Darstellung dieser Functionen sind in §. 18 enthalten.

## §. 24. Zusammensetzung der Transformationen.

Eine Transformation ist bestimmt durch die Transformationszahlen $a$, $b$, $c$, $\partial$ und wir bezeichnen sie daher symbolisch durch

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

oder auch durch einen einzelnen in Klammern gesetzten Buchstaben, wie $(S)$, so dass

$$(S) = \begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix} \tag{1}$$

eine Transformation bedeutet. Bisweilen soll auch, um den Uebergang (9) in §. 23 von den Functionen $T$ zu $T'$ anzudeuten, für $(S)$ das Symbol

$$(S) = (T', T), \tag{2}$$

oder, insofern nur die Einwirkung auf $\omega$ in Betracht kommt

$$\left(\omega, \frac{c + \partial\,\omega}{a + b\,\omega}\right)$$

gebraucht werden.

Eine Transformation, deren Grad $= 1$, heisst **linear**; für diese sollen zur Unterscheidung die Transformationszahlen durch die griechischen Buchstaben $\alpha$, $\beta$, $\gamma$, $\delta$ bezeichnet werden, so dass stets $\alpha\,\delta - \beta\,\gamma = 1$.

Wenn, wie es bei der Transformation mit den Grössen $\omega_1$, $\omega_2$, $\omega_1'$, $\omega_2'$ geschieht, aus irgend zwei Grössen $x_1$, $x_2$ zwei neue Grössen $x_1'$, $x_2'$ durch die Gleichungen

$$\begin{aligned} n\,x_1' &= a\,x_1 + b\,x_2 \\ n\,x_2' &= c\,x_2 + \partial\,x_2 \end{aligned} \tag{3}$$

abgeleitet werden, so sagen wir, die Substitution

$$(S) = \begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix}$$

werde auf das Grössensystem $(x_1, x_2)$ angewandt und schreiben abgekürzt

$$n\,(x_1', x_2') = (S)\,(x_1, x_2) = \begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix} (x_1, x_2) \tag{4}$$

Wenn nun

$$(S) = \begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix}, \quad S' = \begin{pmatrix} a', & b' \\ c', & \partial' \end{pmatrix} \tag{5}$$

zwei Transformationen der Grade $n$, $n'$ sind, so setzen wir

$$n\,(\omega_1', \omega_2') = \begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix} (\omega_1, \omega_2) \tag{6}$$

$$n'\,(\omega_1'', \omega_2'') = \begin{pmatrix} a', & b' \\ c', & \partial' \end{pmatrix} (\omega_1', \omega_2'). \tag{7}$$

Drückt man in (7) $\omega_1'$, $\omega_2'$ nach (6) durch $\omega_1$, $\omega_2$ aus, so erhält man einen Ausdruck von der Form

$$n\,n'\,(\omega_1'', \omega_2'') = \begin{pmatrix} a'', & b'' \\ c'', & \partial'' \end{pmatrix} (\omega_1, \omega_2) = (S'')\,(\omega_1, \omega_2) \tag{8}$$

und darin ist

$$(9) \qquad (S'') = \begin{pmatrix} a'', & b'' \\ c'', & \partial'' \end{pmatrix} = \begin{pmatrix} a'a + b'c, & a'b + b'\partial \\ c'a + \partial'c, & c'b + \partial'\partial \end{pmatrix},$$

und also

$$(10) \qquad a''\partial'' - b''c'' = n'' = nn'.$$

Wenden wir nun $(S')$ auf eine Function $T''$ an, und $(S)$ auf die Function $T'$, so erhalten wir nach (9) des vorigen Paragraphen

$$(11) \qquad T''(u, \omega_1'', \omega_2'') = T'(u, \omega_1', \omega_2') = T(u, \omega_1, \omega_2).$$

Hat man also durch die Transformation $(S')$ $T''$ durch $T'$-Functionen und durch $(S)$ $T'$ durch $T$-Functionen dargestellt, so ist damit auch zugleich $T''$ durch $T$-Functionen dargestellt. Dasselbe geschieht aber auch direct durch die Transformation

$$(S'') = \begin{pmatrix} a'', & b'' \\ c'', & \partial'' \end{pmatrix}.$$

Wir nennen daher die Transformation $(S'')$ aus $(S)$ und $(S')$ zusammengesetzt oder nennen $(S)$, $(S')$ die Componenten von $(S'')$, und schreiben symbolisch:

$$(12) \qquad \begin{pmatrix} a', & b' \\ c', & \partial' \end{pmatrix} \begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix} = \begin{pmatrix} a'', & b'' \\ c'', & \partial'' \end{pmatrix},$$

oder

$$(S')(S) = (S''),$$

oder endlich

$$(13) \qquad (T'', T')\ (T', T) = (T'', T).$$

Bei dieser durch eine symbolische Multiplication bezeichneten Zusammensetzung ist $(S)$ $(S')$ von $(S')$ $(S)$ im Allgemeinen verschieden. Man prägt die Regel für die Zusammensetzung zweier Transformationen (12), die in der Formel (9) enthalten ist, leicht dem Gedächtniss ein, wenn man an die Multiplicationsregel zweier Determinanten denkt, wobei im ersten Factor nach Horizontalreihen, im zweiten nach Verticalreihen summirt wird.

In gleicher Weise lassen sich auch drei und mehr Transformationen zusammensetzen, wobei das in der symbolischen Gleichung

$$[(S'')\ (S')]\ (S) = (S'')\ [(S')\ (S)] = (S'')\ (S')\ (S)$$

ausgedrückte associative Gesetz der Multiplication gilt. Letzteres ersieht man ohne Weiteres aus der Darstellung (13), wonach

$$[(T''', T'')\ (T'', T')]\ (T', T) = (T''', T'')\ [(T'', T')\ (T', T)] = (T''', T).$$

Wenn in einem besonderen Falle bei zwei Transformationen auch das commutative Gesetz $(S)(S') = (S')(S)$ gilt, so heissen die beiden Transformationen vertauschbar.

Der Grad einer zusammengesetzten Transformation ist gleich dem Product der Grade der einzelnen Componenten.

Sind die Componenten einer zusammengesetzten Transformation identisch, so wenden wir zur Bezeichnung symbolische Potenzen an, so dass

$$(S)^2 = (S)(S), \quad (S)^3 = (S)(S)(S) \ldots,$$

woraus allgemein

$$(S)^\lambda (S)^\mu = (S)^{\lambda+\mu}. \tag{14}$$

Die specielle Transformation vom Grade $n^2$

$$(N) = \begin{pmatrix} n, & 0 \\ 0, & n \end{pmatrix}, \tag{15}$$

durch welche die Perioden $\omega_1'$, $\omega_2'$ mit $n$ multiplicirt werden, heisst die **Multiplication.** Ist insbesondere $n = 1$, so lässt die Transformation

$$(1) = \begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix} \tag{16}$$

alles ungeändert und heisst die identische Transformation. Die Multiplication $(N)$ ist mit jeder anderen Transformation vertauschbar, und hat, mit einer anderen Transformation zusammengesetzt, den Erfolg, alle Transformationszahlen mit $n$ zu multipliciren.

Zu jeder Transformation $n$ten Grades $(S)$ giebt es eine vom gleichen Grade, die wir die complementäre Transformation oder (bei linearen Transformationen) auch die inverse Transformation nennen und mit $(S)^{-1}$ bezeichnen, welche dadurch charakterisirt ist, dass sie mit $(S)$ componirt zur Multiplication führt, in Zeichen

$$(S)(S)^{-1} = (N). \tag{17}$$

Dies ergiebt sich aus dem Anblick der folgenden Darstellung:

$$(S) = \begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix}, \quad (S)^{-1} = \begin{pmatrix} \partial, & -b \\ -c, & a \end{pmatrix}. \tag{18}$$

Die Beziehung von $(S)$ und $(S)^{-1}$ ist eine gegenseitige. Es ist auch leicht einzusehen, dass, wenn $(S)(S')$ oder $(S')(S) = (N)$ ist, $(S')$ nothwendig mit $(S)^{-1}$ identisch sein muss.

Hieraus ergiebt sich noch leicht, dass aus jeder der Gleichungen

$$(S)\,(S') = (S)\,(S''), \quad (S')\,(S) = (S'')\,(S)$$

die Gleichheit von $(S')$ und $(S'')$ folgt.

## §. 25. Zusammensetzung der Transformationen aus einfacheren.

Wir untersuchen nun noch, in welcher Weise sich gegebene Transformationen aus einfacheren zusammensetzen lassen.

Wenn zunächst die vier Transformationszahlen einen gemeinsamen Factor haben, so lässt sich dieser mittelst der Formel

$$(1) \qquad \begin{pmatrix} m, & 0 \\ 0, & m \end{pmatrix} \begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix} = \begin{pmatrix} m\,a, & m\,b \\ m\,c, & m\,\partial \end{pmatrix}$$

durch Zusammensetzung mit der Multiplication absondern, und wir setzen demnach jetzt voraus, dass $a$, $b$, $c$, $\partial$ keinen gemeinschaftlichen Theiler haben. Man kann dann immer die zwei ganzen Zahlen $\xi$, $\eta$ so bestimmen, dass

$$(2) \qquad \begin{aligned} a\,\eta - c\,\xi &= \alpha \\ b\,\eta - \partial\,\xi &= \beta \end{aligned}$$

ohne gemeinsamen Theiler sind.

Um dies einzusehen, setzen wir zunächst $\xi$, $\eta$ relativ prim voraus. Dann ist jeder gemeinsame Theiler von $\alpha$, $\beta$ nothwendig Theiler von $n$, wie man aus den Auflösungen von (2)

$$(3) \qquad \begin{aligned} n\,\xi &= b\,\alpha - a\,\beta \\ n\,\eta &= \partial\,\alpha - c\,\beta \end{aligned}$$

erkennt. Nimmt man also $\xi$ nicht theilbar durch alle in $a$ und $b$ zugleich aufgehenden Primzahlen, dagegen $\xi$ theilbar, $\eta$ untheilbar durch alle anderen in $n$ aufgehenden Primzahlen, und überdies $\xi$, $\eta$ relativ prim, was stets möglich ist, so haben $\alpha$ und $\beta$ keinen gemeinsamen Theiler. Hierauf bestimmt man $\gamma$, $\delta$ so, dass

$$(4) \qquad \alpha\,\delta - \beta\,\gamma = 1.$$

Es ist dann auch

$$(5) \qquad (a\,\delta - b\,\gamma)\;\eta - (c\,\delta - \partial\,\gamma)\;\xi = 1,$$

und es ergiebt sich die folgende Zusammensetzung, wie leicht mit Benutzung von (3) erkannt wird:

$$(6)\qquad \begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix} = \begin{pmatrix} a\delta - b\gamma, & \xi \\ c\delta - \partial\gamma, & \eta \end{pmatrix} \begin{pmatrix} 1, & 0 \\ 0, & n \end{pmatrix} \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}.$$

Nennen wir also

$$(7)\qquad \begin{pmatrix} 1, & 0 \\ 0, & n \end{pmatrix}$$

die Haupttransformation vom Grade $n$, so ist damit bewiesen, dass aus der Haupttransformation vom Grade $n$ und linearen Transformationen sich alle Transformationen vom Grade $n$ zusammensetzen lassen.

Aus der Zusammensetzung

$$(8)\qquad \begin{pmatrix} 1, & 0 \\ 0, & n \end{pmatrix} \begin{pmatrix} 1, & 0 \\ 0, & m \end{pmatrix} = \begin{pmatrix} 1, & 0 \\ 0, & mn \end{pmatrix}$$

können wir daher noch weiter schliessen, dass jede Transformation vom Grade $n$ aus solchen sich zusammensetzen lässt, deren Grad eine Primzahl ist. Die gleichen Schlüsse hätten wir auch machen können, wenn wir an Stelle von (7) die Transformation

$$(9)\qquad \begin{pmatrix} n, & 0 \\ 0, & 1 \end{pmatrix} = \begin{pmatrix} 0, & -1 \\ 1, & 0 \end{pmatrix} \begin{pmatrix} 1, & 0 \\ 0, & n \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix},$$

welche wir die zweite Haupttransformation nennen wollen, gesetzt hätten.

Wir heben noch den speciellen Fall der Zusammensetzung (6) hervor, wo $b = 0$, also $a\partial = n$ ist. Für diesen Fall ergiebt sich aus (3)

$$(10)\qquad \partial\xi = -\beta, \quad a\eta = \alpha + c\xi.$$

Wir können, wenn $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ eine beliebig gegebene lineare Transformation ist, $a, c, \partial$, immer so bestimmen, dass dieser Fall eintritt; denn $\partial$ ist nach (10) der grösste gemeinschaftliche Theiler von $n$ und $\beta$, so dass $a$ und $\xi$ zugleich mit bestimmt sind, und $c$ ergiebt sich nach dem Modul $a$ aus der Congruenz

$$(11)\qquad \alpha + c\xi \equiv 0 \pmod{a}.$$

Dann ergiebt sich aus (6)

$$\begin{pmatrix} a, & 0 \\ c, & \partial \end{pmatrix} = \begin{pmatrix} a\delta & \xi \\ c\delta - \partial\gamma, & \eta \end{pmatrix} \begin{pmatrix} 1, & 0 \\ 0, & n \end{pmatrix} \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix},$$

und die Vergleichung mit (6) führt zu folgendem Theorem:

Man kann jede Transformation vom Grade $n$ durch

Zusammensetzung mit **einer** linearen Transformation in Form

$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}\cdot\begin{pmatrix}a, & b\\ c, & \partial\end{pmatrix}$$

auf eine andere zurückführen, in welcher die Transformationszahl $b$ gleich Null ist.

Unter den linearen Transformationen nennen wir die beiden

$$(12)\qquad (A) = \begin{pmatrix}1, & 0\\ 1, & 1\end{pmatrix}, \quad (B) = \begin{pmatrix}0, & 1\\ -1, & 0\end{pmatrix}$$

die Fundamentaltransformationen. Durch wiederholte Zusammensetzung von $(A)^{\pm 1}$ und $(B)$ lässt sich, wie wir jetzt noch zeigen wollen, jede beliebige lineare Transformation $(S)$ bilden.

Zu diesem Zweck bemerken wir zunächst, dass

$$(13)\qquad (A)^\lambda = \begin{pmatrix}1, & 0\\ \lambda, & 1\end{pmatrix}, \quad (B)^2 = \begin{pmatrix}-1, & 0\\ 0, & -1\end{pmatrix},$$

$$(B)^3 = (B)^{-1}, \quad (B)^{-1}(A)^\lambda(B) = \begin{pmatrix}1, & -\lambda\\ 0, & 1\end{pmatrix} = (C)^\lambda,$$

wenn $(C)$ die Transformation

$$(C) = \begin{pmatrix}1, & -1\\ 0, & 1\end{pmatrix}$$

bedeutet. Es sei nun

$$(S) = \begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}, \; (S') = \begin{pmatrix}\alpha', & \beta'\\ \gamma', & \delta'\end{pmatrix}, \; (S'') = \begin{pmatrix}\alpha'', & \beta''\\ \gamma'', & \delta''\end{pmatrix}, \; (S''') = \begin{pmatrix}\alpha''', & \beta'''\\ \gamma''', & \delta'''\end{pmatrix} \ldots,$$

eine Reihe linearer Transformationen, deren erste gegeben ist, während die folgenden so gebildet sind:

$$(S') = (S)(A)^\lambda, \quad (S'') = (S')(C)^{\lambda'}, \quad (S''') = (S'')(A)^{\lambda''} \ldots,$$

so dass

$$\alpha' = \alpha + \beta\lambda, \quad \beta'' = \beta' - \alpha'\lambda', \quad \alpha''' = \alpha'' + \beta''\lambda'' \ldots,$$

und man kann daher über die Zahlen $\lambda, \lambda', \lambda'' \ldots$ so verfügen, dass, dem absoluten Werthe nach,

$$\alpha' \leqq \frac{1}{2}\beta, \quad \beta'' \leqq \frac{1}{2}\alpha', \quad \alpha''' \leqq \frac{1}{2}\beta'' \ldots,$$

so lange keine dieser Zahlen verschwindet, und dass also

$$\beta, \alpha', \beta'', \alpha''', \ldots$$

eine dem absoluten Werthe nach abnehmende Zahlenreihe bildet. Nach einer endlichen Anzahl von Zusammensetzungen dieser Art muss also eine Zahl dieser Reihe verschwinden.

Ist nun $\beta^{(\nu)} = 0$, so ist

$$(S^{(\nu)}) = \begin{pmatrix} \pm 1, & 0 \\ \gamma^{(\nu)}, & \pm 1 \end{pmatrix} = \begin{pmatrix} \pm 1, & 0 \\ 0, & \pm 1 \end{pmatrix} (A)^{\gamma^{(\nu)}},$$

und ist $\alpha^{(\nu)} = 0$, so ist

$$(S^{(\nu)}) = \begin{pmatrix} 0, & \pm 1 \\ \mp 1, & \delta^{(\nu)} \end{pmatrix} = (A)^{\pm \delta^{(\nu)}} (B)^{\pm 1},$$

und da

$$(S) = (S') (A)^{-\lambda} = (S'') (C)^{-\lambda'} (A)^{-\lambda}$$
$$= (S''') (A)^{-\lambda''} (C)^{-\lambda'} (A)^{-\lambda} = \ldots,$$

so ist der Satz damit erwiesen.

## §. 26. Die linearen Fundamentaltransformationen der $\vartheta$-Functionen.

Nach diesen Ergebnissen lässt sich das ganze System der Transformationen herleiten durch wiederholte Anwendung der drei Transformationen

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

und wir betrachten also zunächst die linearen Fundamentaltransformationen der $\vartheta$-Functionen.

I. $\begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix}$ oder $(\omega, \omega + 1)$.

Nach §. 23 (12) ist

$$(1) \qquad \vartheta_{11}(u, \omega + 1) = A\, \vartheta_{11}(u, \omega),$$

worin $A$ von $u$ unabhängig ist. Ersetzt man $u$ durch

$$u + \frac{1}{2}, \quad u + \frac{\omega}{2}, \quad u + \frac{1 + \omega}{2},$$

so ergeben die Formeln §. 18 (10)

$$(2) \qquad \vartheta_{10}(u, \omega + 1) = A\, \vartheta_{10}(u, \omega)$$

$$(3) \qquad e^{\frac{\pi i}{4}}\, \vartheta_{00}(u, \omega + 1) = A\, \vartheta_{01}(u, \omega)$$

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

Zur Bestimmung der Constanten $A$ wenden wir, wie in der Folge häufig, das Mittel an, dass wir $u = 0$ setzen, in (1) nach der Differentiation, und dann rechts und links von der Formel (5), §. 20

$$(5) \qquad \vartheta'_{11} = \pi\, \vartheta_{00}\, \vartheta_{10}\, \vartheta_{01}$$

Gebrauch machen, so folgt

$$A^2 = e^{\frac{\pi i}{2}}, \quad A = e^{\frac{\pi i}{4}};$$

dass bei $A$ das positive Zeichen steht, ergiebt sich aus einer der Formeln (3), (4) nach der Schlussbemerkung von §. 22, wenn man $\omega$ unendlich werden lässt.

Sonach erhält man

$$(6) \qquad \begin{aligned} \vartheta_{11}(u, \omega + 1) &= e^{\frac{\pi i}{4}}\, \vartheta_{11}(u) \\ \vartheta_{10}(u, \omega + 1) &= e^{\frac{\pi i}{4}}\, \vartheta_{10}(u) \\ \vartheta_{01}(u, \omega + 1) &= \vartheta_{00}(u) \\ \vartheta_{00}(u, \omega + 1) &= \vartheta_{01}(u). \end{aligned}$$

II. $\begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}$ oder $\left(\omega, \frac{-1}{\omega}\right)$.

Es ist wieder nach §. 23, (12)

$$(7) \qquad e^{-\frac{\pi i u^2}{\omega}}\, \vartheta_{11}\left(\frac{u}{\omega}, -\frac{1}{\omega}\right) = A\, \vartheta_{11}(u, \omega)$$

und durch Vermehrung von $u$ um $\frac{1}{2}, \frac{\omega}{2}, \frac{1+\omega}{2}$

$$(8) \qquad e^{-\frac{\pi i u^2}{\omega}}\, \vartheta_{01}\left(\frac{u}{\omega}, -\frac{1}{\omega}\right) = i A\, \vartheta_{10}(u, \omega)$$

$$(9) \qquad e^{-\frac{\pi i u^2}{\omega}}\, \vartheta_{10}\left(\frac{u}{\omega}, -\frac{1}{\omega}\right) = i A\, \vartheta_{01}(u, \omega)$$

$$(10) \qquad e^{-\frac{\pi i u^2}{\omega}}\, \vartheta_{00}\left(\frac{u}{\omega}, -\frac{1}{\omega}\right) = i A\, \vartheta_{00}(u, \omega)$$

und wie oben erhält man

$$A = \pm\, i \sqrt{-i\, \omega}.$$

Aus $u = 0$ und einem rein imaginären $\omega$ schliesst man, dass, wenn $\sqrt{-i\omega}$ so genommen wird, dass der reelle Theil positiv ist, das untere Zeichen stehen muss, so dass sich ergiebt

$$(11) \qquad \begin{aligned} e^{\frac{-\pi i u^2}{\omega}}\, \vartheta_{11}\left(\frac{u}{\omega}, -\frac{1}{\omega}\right) &= -i \sqrt{-i\omega}\, \vartheta_{11}(u) \\ e^{\frac{-\pi i u^2}{\omega}}\, \vartheta_{01}\left(\frac{u}{\omega}, -\frac{1}{\omega}\right) &= \sqrt{-i\omega}\, \vartheta_{10}(u) \end{aligned}$$

$$(11)\quad \begin{aligned} e^{-\frac{\pi i u^2}{\omega}}\, \vartheta_{10}\left(\frac{u}{\omega}, -\frac{1}{\omega}\right) &= \sqrt{-i\omega}\; \vartheta_{01}(u) \\ e^{-\frac{\pi i u^2}{\omega}}\, \vartheta_{00}\left(\frac{u}{\omega}, -\frac{1}{\omega}\right) &= \sqrt{-i\omega}\; \vartheta_{00}(u). \end{aligned}$$

## §. 27. Die Haupttransformationen zweiter Ordnung der $\vartheta$-Functionen.

Die beiden Haupttransformationen $n$ter Ordnung

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

verwandeln nach §. 23, (11) die Charakteristik $(g_1', g_2')$ in

$$(n g_1', \; g_2'), \; (g_1', \; n g_2'),$$

d. h. bei ungeradem $n$ bleibt die Charakteristik ungeändert, bei geradem $n$ geht sie über in

$$(1) \qquad (0, g_2') \text{ oder } (g_1', 0).$$

Da sich hiernach die Transformation geraden Grades wesentlich anders verhält als die ungeraden Grades, so betrachten wir zunächst den Fall $n = 2$. Die erste und zweite Haupttransformation zweiten Grades werden die Landen'sche und die Gauss'sche Transformation genannt.

Nach §. 23, (12) sind

$$(2)\quad \begin{aligned} \vartheta_{g_1, g_2}\left(u, \frac{\omega}{2}\right) &= \Theta_{g_1, 0}(u, \omega) \\ \vartheta_{g_1, g_2}(2u, 2\omega) &= \Theta_{0, g_2}(u, \omega) \end{aligned}$$

$\Theta$-Functionen zweiter Ordnung von $u$, $\omega$, welche sich nach §. 18 darstellen lassen.

Wir erhalten zunächst die zwei Formelpaare, in denen $A$, $B$ von $u$ unabhängig sind:

$$(3)\quad \begin{aligned} A\,\vartheta_{11}\left(u, \frac{\omega}{2}\right) &= \vartheta_{01}(u, \omega)\, \vartheta_{11}(u, \omega) \\ A\,\vartheta_{10}\left(u, \frac{\omega}{2}\right) &= \vartheta_{00}(u, \omega)\, \vartheta_{10}(u, \omega) \end{aligned}$$

$$(4)\quad \begin{aligned} B\,\vartheta_{11}(2u, 2\omega) &= \vartheta_{10}(u, \omega)\, \vartheta_{11}(u, \omega) \\ B\,\vartheta_{01}(2u, 2\omega) &= \vartheta_{00}(u, \omega)\, \vartheta_{01}(u, \omega), \end{aligned}$$

wovon nach §. 18 jedesmal die zweite aus der ersten abgeleitet werden kann durch Vermehrung des Arguments um eine halbe Periode.

Setzt man in diesen Gleichungen $u = 0$, so folgt

$$(5)\qquad \begin{aligned} A\vartheta'_{11}\left(0, \frac{\omega}{2}\right) &= \vartheta_{01}\,\vartheta'_{11}, \quad 2B\vartheta'_{11}\,(0, 2\omega) = \vartheta_{10}\,\vartheta'_{11}, \\ A\vartheta_{10}\left(0, \frac{\omega}{2}\right) &= \vartheta_{00}\,\vartheta_{10}, \quad B\vartheta_{01}\,(0, 2\omega) = \vartheta_{00}\,\vartheta_{01}, \end{aligned}$$

woraus durch Division, mit Benutzung der Relation [§. 20, (5)]

$$\vartheta'_{11} = \pi\,\vartheta_{00}\,\vartheta_{10}\,\vartheta_{01}$$

$$(6)\qquad \vartheta_{00}\left(0, \frac{\omega}{2}\right)\vartheta_{01}\left(0, \frac{\omega}{2}\right) = \vartheta_{01}^2,$$

$$(7)\qquad 2\vartheta_{00}\,(0, 2\omega)\,\vartheta_{10}\,(0, 2\omega) = \vartheta_{10}^2,$$

und wenn man in (6) $\omega$ durch $2\omega$, in (7) $\omega$ durch $\omega:2$ ersetzt:

$$(8)\qquad \vartheta_{01}\,(0, 2\omega)^2 = \vartheta_{00}\,\vartheta_{01},$$

$$(9)\qquad \vartheta_{10}\left(0, \frac{\omega}{2}\right)^2 = 2\vartheta_{00}\,\vartheta_{10}.$$

Nach (8) und (9) ergiebt sich aus den zweiten Gleichungen (5)

$$2A = \vartheta_{10}\left(0, \frac{\omega}{2}\right), \quad B = \vartheta_{01}\,(0, 2\omega),$$

und man erhält also für die Gauss'sche Transformation:

$$(10)\qquad \begin{aligned} \vartheta_{10}\left(0, \frac{\omega}{2}\right)\vartheta_{11}\left(u, \frac{\omega}{2}\right) &= 2\vartheta_{01}\,(u, \omega)\,\vartheta_{11}\,(u, \omega) \\ \vartheta_{10}\left(0, \frac{\omega}{2}\right)\vartheta_{10}\left(u, \frac{\omega}{2}\right) &= 2\vartheta_{00}\,(u, \omega)\,\vartheta_{10}\,(u, \omega), \end{aligned}$$

und für die Landen'sche Transformation:

$$(11)\qquad \begin{aligned} \vartheta_{01}\,(0, 2\omega)\,\vartheta_{11}\,(2u, 2\omega) &= \vartheta_{10}\,(u. \omega)\,\vartheta_{11}\,(u, \omega), \\ \vartheta_{01}\,(0, 2\omega)\,\vartheta_{01}\,(2u, 2\omega) &= \vartheta_{00}\,(u, \omega)\,\vartheta_{01}\,(u, \omega). \end{aligned}$$

Es bleiben für jede der beiden Transformationen noch zwei $\vartheta$-Functionen auszudrücken. Man kann diese Ausdrücke aus (10), (11) herleiten nach §. 18, (12), gelangt aber auch direct dazu auf folgende Weise. Die Functionen

$$(12)\qquad \vartheta_{01}\left(u, \frac{\omega}{2}\right), \quad \vartheta_{10}\,(2u, 2\omega)$$

verschwinden für

$$u = \frac{\omega}{4}, \quad u = \frac{1}{4}.$$

Andererseits ergiebt sich aus den Formeln (10) des §. 18, wenn dort $v = -\frac{\omega}{4}$ und $= -\frac{1}{4}$ gesetzt wird,

$$\vartheta_{11}\left(\frac{\omega}{4}\right) = i\,\vartheta_{01}\left(\frac{\omega}{4}\right)$$

$$\vartheta_{11}\left(\frac{1}{4}\right) = \vartheta_{10}\left(\frac{1}{4}\right)$$

und demnach sind die beiden Functionen (12), welche linear durch zwei $\vartheta$-Quadrate ausdrückbar sind, von constanten Factoren abgesehen, übereinstimmend mit

$$\vartheta_{01}^2(u) + \vartheta_{11}^2(u), \qquad \vartheta_{10}^2(u) - \vartheta_{11}^2(u).$$

Die constanten Factoren ergeben sich unmittelbar für $u = 0$ aus den Relationen (6), (7):

$$(13) \qquad \vartheta_{00}\left(0, \frac{\omega}{2}\right)\vartheta_{01}\left(u, \frac{\omega}{2}\right) = \vartheta_{01}^2(u) + \vartheta_{11}^2(u)$$

$$(14) \qquad 2\,\vartheta_{00}(0, 2\,\omega)\,\vartheta_{10}(2\,u, 2\,\omega) = \vartheta_{10}^2(u) - \vartheta_{11}^2(u).$$

Daraus erhält man die beiden letzten Formeln, wenn man $u$ in $u + \frac{1}{2}$ und $u + \frac{\omega}{2}$ verwandelt [oder auch auf demselben Wege wie (13), (14)]:

$$(15) \qquad \vartheta_{00}\left(0, \frac{\omega}{2}\right)\vartheta_{00}\left(u, \frac{\omega}{2}\right) = \vartheta_{00}^2(u) + \vartheta_{10}^2(u).$$

$$(16) \qquad 2\,\vartheta_{00}(0, 2\,\omega)\,\vartheta_{00}(2\,u, 2\,\omega) = \vartheta_{00}^2(u) + \vartheta_{01}^2(u).$$

Hieraus lassen sich mannigfache Relationen zwischen den Nullwerthen der $\vartheta$-Functionen herleiten, von denen wir nur die drei folgenden anführen, deren beide ersten aus (8), (9) folgen, während die letzte aus der ersten Gleichung (11) sich ergiebt, wenn man $\omega$ durch $\omega : 2$ ersetzt und $u = {}^1\!/_4$ annimmt und berücksichtigt, dass nach §. 18 (10) $\vartheta_{11}({}^1\!/_4) = \vartheta_{10}({}^1\!/_4)$ ist.

$$(17) \qquad \begin{aligned} \sqrt{\vartheta_{00}\,\vartheta_{01}} &= \vartheta_{01}(0, 2\,\omega) \\ \sqrt{\vartheta_{00}\,\vartheta_{10}} &= \frac{1}{\sqrt{2}}\,\vartheta_{10}\left(0, \frac{\omega}{2}\right) \\ \sqrt{\vartheta_{01}\,\vartheta_{10}} &= \vartheta_{10}\left(\frac{1}{4}, \frac{\omega}{2}\right). \end{aligned}$$

Diese Formeln sind darum von Interesse, weil sie die Quadratwurzeln als eindeutige Functionen von $\omega$ darstellen.

Wir machen von der Transformation zweiter Ordnung noch eine Anwendung auf den Beweis einer Formel, die für die Transformation ungerader Ordnung nothwendig ist.

Wir ersetzen in der zweiten Gleichung (10) $\omega$ durch $2\omega$ also:

$$2\vartheta_{00}(u, 2\omega)\,\vartheta_{10}(u, 2\omega) = \vartheta_{10}\,\vartheta_{10}(u).$$

Hiermit multipliciren wir die zweite Gleichung (11), so dass wir erhalten

$$\begin{aligned}2\vartheta_{01}(0, 2\omega)\,\vartheta_{01}(2u, 2\omega)\,\vartheta_{00}(u, 2\omega)\,\vartheta_{10}(u, 2\omega)\\ = \vartheta_{10}\,\vartheta_{10}(u)\,\vartheta_{00}(u)\,\vartheta_{01}(u).\end{aligned}$$

Dies dividiren wir durch das Product der beiden Gleichungen (7), (8):

$$2\vartheta_{00}(0, 2\omega)\,\vartheta_{10}(0, 2\omega)\,\vartheta_{01}(0, 2\omega)^2 = \vartheta_{10}^2\,\vartheta_{00}\,\vartheta_{01}$$

und erhalten

$$(18)\quad \frac{\vartheta_{00}(u, 2\omega)\,\vartheta_{10}(u, 2\omega)\,\vartheta_{01}(2u, 2\omega)}{\vartheta_{00}(0, 2\omega)\,\vartheta_{10}(0, 2\omega)\,\vartheta_{01}(0, 2\omega)} = \frac{\vartheta_{00}(u)\,\vartheta_{10}(u)\,\vartheta_{01}(u)}{\vartheta_{00}\,\vartheta_{10}\,\vartheta_{01}}.$$

Wenn nun $n$ irgend eine ungerade ganze Zahl bedeutet, so bleibt die Function

$$\vartheta_{01}\left(\frac{\nu}{n}\right),$$

wenn $\nu$ um ein Vielfaches von $n$ wächst, ungeändert, und folglich ist das Product

$$\overset{\nu}{\Pi}\,\vartheta_{01}\left(\frac{\nu}{n}\right),$$

wenn es über ein vollständiges Restsystem nach dem Modul $n$ genommen wird, unabhängig von der besonderen Wahl dieses Restsystems. Daher ist, da $2\nu$ zugleich mit $\nu$ ein solches Restsystem durchläuft,

$$(19)\qquad \overset{\nu}{\underset{1,\,n-1}{\Pi}}\,\vartheta_{01}\left(\frac{\nu}{n}\right) = \overset{\nu}{\underset{1,\,n-1}{\Pi}}\,\vartheta_{01}\left(\frac{2\nu}{n}\right).$$

Wenn wir also in (18) $u = \nu : n$ setzen, das Product bilden und im letzten Factor der linken Seite von der Formel (19) Gebrauch machen, so ergiebt sich, dass das Product

$$(20)\qquad \frac{\overset{\nu}{\underset{1,\,n-1}{\Pi}}\,\vartheta_{00}\left(\frac{\nu}{n}\right)\vartheta_{10}\left(\frac{\nu}{n}\right)\vartheta_{01}\left(\frac{\nu}{n}\right)}{\vartheta_{00}^{\,n-1}\;\vartheta_{10}^{\,n-1}\;\vartheta_{01}^{\,n-1}}$$

ungeändert bleibt, wenn $\omega$ durch $2\omega$ ersetzt wird.

Die in (20) vorkommenden Werthe von $\nu$ lassen sich in Paare anordnen derart:

$$2\nu,\quad n - 2\nu,\qquad \nu = 1, 2, \ldots \frac{n-1}{2},$$

und da

$$\vartheta_{00}\left(\frac{2\nu}{n}\right) = \vartheta_{00}\left(\frac{n-2\nu}{n}\right),\ \vartheta_{10}\left(\frac{2\nu}{n}\right) = -\vartheta_{10}\left(\frac{n-2\nu}{n}\right),$$

$$\vartheta_{01}\left(\frac{2\nu}{n}\right) = \vartheta_{01}\left(\frac{n-2\nu}{n}\right),$$

so stimmt (20) bis auf das Vorzeichen überein mit dem Quadrat von

$$(21)\qquad \frac{\overset{\nu}{\underset{1,\frac{n-1}{2}}{\Pi}}\ \vartheta_{00}\left(\frac{2\nu}{n}\right)\vartheta_{10}\left(\frac{2\nu}{n}\right)\vartheta_{01}\left(\frac{2\nu}{n}\right)}{\vartheta_{00}^{\frac{n-1}{2}}\ \vartheta_{10}^{\frac{n-1}{2}}\ \vartheta_{01}^{\frac{n-1}{2}}},$$

und der letztere Quotient, welcher eine stetige, von Null verschiedene Function von $\omega$ ist, so lange der imaginäre Theil von $\omega$ positiv ist, bleibt also gleichfalls ungeändert, wenn $\omega$ durch $2\omega$, also auch durch $4\omega$, $8\omega$, ... ersetzt wird. Man kann also den Werth dieses Ausdruckes dadurch bestimmen, dass man den imaginären Theil von $\omega$ unendlich, also $q = 0$ annimmt. Für $q = 0$ ist aber (nach §. 22):

$$\vartheta_{00}(v) = 1,\quad \vartheta_{01}(v) = 1,\quad \frac{\vartheta_{10}(v)}{\vartheta_{10}} = \cos \pi v$$

und daher der Werth von (21):

$$(22)\qquad \overset{\nu}{\underset{1,\frac{n-1}{2}}{\Pi}}\ \cos\frac{2\nu\pi}{n}.$$

Zunächst ist es einfach, den absoluten Werth dieses Productes zu finden. Sein Quadrat ist nämlich, wie bekannt

$$= \pm \overset{\nu}{\underset{1,\,n-1}{\Pi}}\ \cos\frac{\nu\pi}{n} = \frac{1}{2^{n-1}}.$$

Das Vorzeichen von (22) wird durch die Anzahl der negativen Factoren bestimmt, welche so gross ist, wie die Anzahl der ganzen Zahlen zwischen $\frac{n}{4}$ und $\frac{n}{2}$, also $= \frac{n \pm 1}{4}$, d. h. gerade, wenn $n \equiv \pm 1$, ungerade, wenn $n \equiv \pm 3 \pmod 8$ ist. Demnach ist der Werth von (22)

$$\frac{(-1)^{\frac{n^2-1}{8}}}{2^{\frac{n-1}{2}}},$$

oder nach der in der Theorie der quadratischen Reste gebräuchlichen Bezeichnung

$$\left(\frac{2}{n}\right)\frac{1}{2^{\frac{n-1}{2}}},$$

und es ist die Formel bewiesen:

$$(23)\qquad 2^{\frac{n-1}{2}}\prod_{1,\frac{n-1}{2}}^{\nu}\vartheta_{00}\left(\frac{2\nu}{n}\right)\vartheta_{10}\left(\frac{2\nu}{n}\right)\vartheta_{01}\left(\frac{2\nu}{n}\right) = \left(\frac{2}{n}\right)\vartheta_{00}^{\frac{n-1}{2}}\vartheta_{10}^{\frac{n-1}{2}}\vartheta_{01}^{\frac{n-1}{2}}.$$

## §. 28. Die Haupttransformationen ungerader Ordnung.

Die zuletzt bewiesene Formel ist uns von grossem Nutzen bei der Durchführung der Transformation ungerader Ordnung $n$, wobei wir uns hier auf die erste Haupttransformation beschränken. Nach §. 17 ist

$$(1)\qquad \vartheta_{11}(nu, n\omega)$$

eine $\Theta_{11}$-Function $n$ter Ordnung von $u$ und $\omega$ und diese lässt sich leicht bilden aus den Nullpunkten von (1), deren es im Periodenparallelogramm $n$ giebt. Die Nullpunkte von (1) sind nun die Werthe

$$u = \frac{\nu + \mu n\omega}{n} = \frac{\nu}{n} + \mu\omega,$$

wenn $\nu$ und $\mu$ ganze Zahlen sind, und man erhält also alle incongruenten unter diesen Werthen, wenn man $\mu$ festhält und $\nu$ ein vollständiges Restsystem nach dem Modul $n$ durchlaufen lässt. Wir wählen das Restsystem

$$0, \pm 2, \pm 4, \ldots, \pm(n-1),$$

und erhalten demnach, wenn $C$ einen von $u$ unabhängigen Factor bedeutet,

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

Eine Formel, die sich nach §. 19, (4) in folgender Weise auch durch die Functionen $\vartheta_{11}(u)$, $\vartheta_{01}(u)$ ausdrücken lässt:

$$C\vartheta_{01}^{n-1}\,\vartheta_{11}(n u,\, n\omega)$$
$$= \vartheta_{11}(u) \prod_{1,\frac{n-1}{2}}^{\nu} \left[\vartheta_{11}^{2}\left(\frac{2\nu}{n}\right)\vartheta_{01}^{2}(u) - \vartheta_{01}^{2}\left(\frac{2\nu}{n}\right)\vartheta_{11}^{2}(u)\right].$$

Wir ersetzen in (2) $u$ durch

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

und erhalten (§. 18):

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

$$C\vartheta_{01}(n u,\, n\omega) = \vartheta_{01}(u) \prod_{1,\frac{n-1}{2}}^{\nu} \vartheta_{01}\left(\frac{2\nu}{n} + u\right)\vartheta_{01}\left(\frac{2\nu}{n} - u\right). \tag{3}$$

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

Daraus aber ergiebt sich für $u = 0$ nach der Formel

$$\vartheta_{11}' = \pi\,\vartheta_{00}\,\vartheta_{01}\,\vartheta_{10} \text{ (§. 20):} \tag{4}$$

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

oder mit Benutzung von (23) des vorigen Paragraphen:

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

Das noch unbestimmte Vorzeichen ergiebt sich aus dem aus einer der Formeln (3) zu schliessenden Umstande, dass $C = 1$ wird für $q = 0$.

Nach dieser Bestimmung von $C$ lassen sich die Formeln (2), (3) so schreiben:

$$\sqrt{n}\;\vartheta_{11}(n u,\, n\omega)\,\vartheta_{00}^{\frac{n-1}{2}}\,\vartheta_{10}^{\frac{n-1}{2}}\,\vartheta_{01}^{\frac{n-1}{2}} \tag{6}$$
$$= 2^{\frac{n-1}{2}}\,\vartheta_{11}(u) \prod_{1,\frac{n-1}{2}}^{\nu} \vartheta_{11}\left(\frac{2\nu}{n}\right)\vartheta_{11}\left(\frac{2\nu}{n} + u\right)\vartheta_{11}\left(\frac{2\nu}{n} - u\right).$$

$$(7)\qquad \sqrt{n}\,\vartheta_{10}(n u, n\omega)\,\vartheta_{00}^{\frac{n-1}{2}}\,\vartheta_{10}^{\frac{n-1}{2}}\,\vartheta_{01}^{\frac{n-1}{2}}$$

$$= 2^{\frac{n-1}{2}}\,\vartheta_{10}(u)\prod_{1,\frac{n-1}{2}}^{\nu}\vartheta_{11}\left(\frac{2\nu}{n}\right)\vartheta_{10}\left(\frac{2\nu}{n}+u\right)\vartheta_{10}\left(\frac{2\nu}{n}-u\right).$$

$$(8)\qquad \sqrt{n}\,\vartheta_{01}(n u, n\omega)\,\vartheta_{00}^{\frac{n-1}{2}}\,\vartheta_{10}^{\frac{n-1}{2}}\,\vartheta_{01}^{\frac{n-1}{2}}$$

$$= 2^{\frac{n-1}{2}}\,\vartheta_{01}(u)\prod_{1,\frac{n-1}{2}}^{\nu}\vartheta_{11}\left(\frac{2\nu}{n}\right)\vartheta_{01}\left(\frac{2\nu}{n}+u\right)\vartheta_{01}\left(\frac{2\nu}{n}-u\right).$$

$$(9)\qquad \sqrt{n}\,\vartheta_{00}(n u, n\omega)\,\vartheta_{00}^{\frac{n-1}{2}}\,\vartheta_{10}^{\frac{n-1}{2}}\,\vartheta_{01}^{\frac{n-1}{2}}$$

$$= 2^{\frac{n-1}{2}}\,\vartheta_{00}(u)\prod_{1,\frac{n-1}{2}}^{\nu}\vartheta_{11}\left(\frac{2\nu}{n}\right)\vartheta_{00}\left(\frac{2\nu}{n}+u\right)\vartheta_{00}\left(\frac{2\nu}{n}-u\right)$$

## §. 29. Die Functionen $\eta(\omega)$, $f(\omega)$, $f_1(\omega)$, $f_2(\omega)$.

Es sind bereits im §. 21 die Functionen $\eta(\omega)$, $f(\omega)$, $f_1(\omega)$, $f_2(\omega)$ erwähnt, die sich dort, als einwerthige Functionen von $\omega$ bei der Darstellung der $\vartheta$-Functionen durch unendliche Producte fast von selbst einstellten, die aber nicht sich ergaben bei der zweiten Darstellung durch unendliche Reihen. Damit im Zusammenhang steht ein bemerkenswerther Umstand, dass viele unserer Formeln, z. B. die zur Transformation zweiter Ordnung gehörigen (17) oder die Formel (23), §. 27 leicht verificirt werden können durch die unendlichen Producte, dagegen schwer oder gar nicht durch die unendlichen Reihen. Darum war es für uns von Interesse, diese Resultate ohne die Benutzung des einen oder anderen dieser Ausdrücke aus der Transformationstheorie herzuleiten, und ebenso sollen nun auch aus dieser Quelle die Functionen $\eta(\omega)$, $f(\omega)$, $f_1(\omega)$, $f_2(\omega)$ und ihre Grundeigenschaften gewonnen werden.

Wenden wir die Formel (6) des vorigen Paragraphen auf den einfachsten Fall $n = 3$ an, so ergiebt sich durch Differentiation und Nullsetzen von $u$ mit Rücksicht auf (4)

$$3\sqrt{3}\,\vartheta'_{11}(0, 3\omega) = 2\pi\,\vartheta_{11}\left(\frac{2}{3}\right)^{3},$$

oder indem man $\omega$ durch $\frac{\omega}{3}$ ersetzt,

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

Setzt man also

(1) $$\eta(\omega) = \frac{1}{\sqrt{3}}\,\vartheta_{11}\left(\frac{2}{3}, \frac{\omega}{3}\right),$$

so folgt in Uebereinstimmung mit §. 21:

(2) $$\vartheta'_{11} = \pi\,\vartheta_{00}\,\vartheta_{01}\,\vartheta_{10} = 2\pi\,\eta(\omega)^3$$

und aus §. 22, (4) erhält man für $\eta(\omega)$ die Reihenentwickelung

(3) $$\eta(\omega) = q^{\frac{1}{12}} \sum_{-\infty,\infty}^{\nu} (-1)^\nu\, q^{3\nu^2+\nu}.$$

Die Function $\eta(\omega)$ ist nach (1) für ein rein imaginäres $\omega$ reell, und für ein unendlich grosses $\omega$ (d. h. verschwindendes $q$) ist

$$q^{-\frac{1}{12}}\,\eta(\omega) = 1.$$

Hiernach findet man leicht aus §. 26, (6), (11) für die linearen Fundamentaltransformationen von $\eta(\omega)$

(4) $$\eta(\omega+1) = e^{\frac{\pi i}{12}}\,\eta(\omega).$$

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

Wir gehen über zur Betrachtung der beiden Haupttransformationen zweiter Ordnung der $\eta$-Function.

Aus §. 27, (11) erhält man durch Differentiation und Nullsetzen von $u$

$$2\,\vartheta_{01}(0, 2\omega)\ \eta(2\omega)^3 = \vartheta_{10}\ \eta(\omega)^3,$$

also wenn man ins Quadrat erhebt und §. 27, (8) anwendet:

$$4\,\vartheta_{00}\ \vartheta_{10}\ \vartheta_{01}\ \eta\ (2\omega)^6 = \vartheta_{10}^3\,\eta(\omega)^6,$$

und mit Anwendung von (2) und Ausziehen der Cubikwurzel:

(6) $$2\,\eta\,(2\omega)^2 = \vartheta_{10}\,\eta(\omega).$$

Ebenso findet man aus der Gauss'schen Transformation [§. 27, (10)]:

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

und durch Verwandlung von $\omega$ in $\omega + 1$ [(4) und §. 26, (6)]:

(8)
$$e^{-\frac{\pi i}{12}}\,\eta\left(\frac{\omega+1}{2}\right)^2 = \vartheta_{00}\,\eta(\omega).$$

Hiernach führen wir die drei Functionen ein:

(9)
$$\begin{aligned} f(\omega) &= e^{-\frac{\pi i}{24}}\frac{\eta\left(\frac{\omega+1}{2}\right)}{\eta(\omega)} \\ f_1(\omega) &= \frac{\eta\left(\frac{\omega}{2}\right)}{\eta(\omega)} \\ f_2(\omega) &= \sqrt{2}\,\frac{\eta(2\omega)}{\eta(\omega)}, \end{aligned}$$

so dass

(10)
$$\begin{aligned} \vartheta_{00} &= \eta(\omega)\,f(\omega)^2 \\ \vartheta_{01} &= \eta(\omega)\,f_1(\omega)^2 \\ \vartheta_{10} &= \eta(\omega)\,f_2(\omega)^2, \end{aligned}$$

woraus zu schliessen ist, dass $f(\omega)$, $f_1(\omega)$, $f_2(\omega)$ für ein rein imaginäres $\omega$ reell und positiv sind. (10) stimmt überein mit §. 21, (9), so dass die dort eingeführten Functionen $f, f_1, f_2$ dieselben sind wie diese. Aus (10) folgen aber leicht die Relationen [(2) und §. 18 (15)]:

(11)
$$f(\omega)^8 = f_1(\omega)^8 + f_2(\omega)^8.$$

(12)
$$\sqrt{2} = f(\omega)\,f_1(\omega)\,f_2(\omega).$$

Für die linearen Fundamentaltransformationen der Functionen $f$ erhält man zunächst aus (4) und (9):

(13)
$$\begin{aligned} f(\omega+1) &= e^{-\frac{\pi i}{24}} f_1(\omega) \\ f_1(\omega+1) &= e^{-\frac{\pi i}{24}} f(\omega) \\ f_2(\omega+1) &= e^{\frac{\pi i}{12}} f_2(\omega). \end{aligned}$$

Ferner ergiebt sich aus (5) und den beiden letzten Gleichungen (9):

(14)
$$f_1\left(-\frac{1}{\omega}\right) = f_2(\omega), \quad f_2\left(-\frac{1}{\omega}\right) = f_1(\omega)$$

und wenn man hiervon in (12) Gebrauch macht:

(15)
$$f\left(-\frac{1}{\omega}\right) = f(\omega).$$

Für die Transformation zweiter Ordnung ergiebt sich unmittelbar aus den beiden letzten Gleichungen (9):

(16)
$$f_1(2\omega)\, f_2(\omega) = \sqrt{2},$$

woraus durch einfache Rechnung folgt:

(17)
$$f_2(\omega)^4\, [f(2\omega)^8 + f_2(2\omega)^8] = 2\,[f(\omega)^8 + f_1(\omega)^8],$$

eine Formel, die sich durch Quadriren nach (11), (12), (16) leicht verificiren lässt.

Setzt man in (16) nach (13), (14)

$$f_1(2\omega) = e^{-\frac{\pi i}{24}} f(2\omega - 1)$$

$$f_2(\omega) = e^{\frac{\pi i}{24}} f\left(1 - \frac{1}{\omega}\right),$$

so kann man, indem man $\omega$ an Stelle von $2\omega - 1$ setzt, für (16) auch schreiben:

(18)
$$f(\omega)\, f\left(\frac{\omega - 1}{\omega + 1}\right) = \sqrt{2},$$

und indem man in (16) $\omega$ durch $\frac{\omega}{2}$ und $\frac{\omega + 1}{2}$ ersetzt:

(19)
$$f_1(\omega)\, f_2\left(\frac{\omega}{2}\right) = \sqrt{2}$$
$$f(\omega)\, f_2\left(\frac{\omega + 1}{2}\right) = e^{\frac{\pi i}{24}} \sqrt{2}.$$

Wir stellen endlich noch für ein ungerades $n$ die Formeln für die Haupttransformation $n$ter Ordnung der Functionen $\eta$, $f$ auf. Für $\eta\,(n\omega)$ ergiebt sich leicht, wenn man in den Formeln (6), §. 28 nach der Differentiation $u = 0$ setzt, und die dritte Wurzel zieht:

(20)
$$\sqrt{n}\;\eta\,(n\omega)\;\eta(\omega)^{\frac{n-3}{2}} = \prod_{1,\frac{n-1}{2}}^{\nu} \vartheta_{11}\left(\frac{2\nu}{n}\right).$$

Setzt man ferner $u = 0$ in (7), (8), (9), §. 28, benutzt alsdann die Relationen (10) und (20) und zieht die Quadratwurzel, so findet sich

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

$$f_1(n\omega)\,\eta(\omega)^{\frac{n-1}{2}} = f_1(\omega) \prod_{1,\frac{n-1}{2}}^{\nu} \vartheta_{01}\left(\frac{2\nu}{n}\right), \tag{21}$$

$$f_2(n\omega)\,\eta(\omega)^{\frac{n-1}{2}} = \left(\frac{2}{n}\right) f_2(\omega) \prod_{1,\frac{n-1}{2}}^{\nu} \vartheta_{10}\left(\frac{2\nu}{n}\right),$$

wo das Vorzeichen in den beiden ersten Formeln direct aus der Annahme eines rein imaginären $\omega$ geschlossen wird, während das Vorzeichen in der dritten entweder nach der Endformel von §. 27 durch Multiplication der drei Formeln (21), oder auch direct nach der in §. 27 angewandten Methode durch Abzählung der Anzahl der negativen Factoren bestimmt wird.

## §. 30. Die Weierstrass'sche σ-Function.

Wenn auch aus den bis jetzt betrachteten besonderen Transformationen alle anderen sich durch wiederholte Anwendung ableiten lassen, so ist es doch nothwendig, die Gesetze, die bei der allgemeinen Transformation herrschen, so weit als möglich zu ergründen, und wir wenden uns daher zunächst zur allgemeinen linearen Transformation

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

Ist $(g_1, g_2)$ die Charakteristik einer zu transformirenden $t$-Function, so wird nach §. 23, (11) die Charakteristik der transformirten Function bestimmt durch

$$(g_1, g_2) = (\delta g'_1 - \beta g'_2 - \beta\delta, \; -\gamma g'_1 + \alpha g'_2 - \alpha\gamma),$$

oder

$$(g'_1, g'_2) = (\alpha g_1 + \beta g_2 + \alpha\beta, \; \gamma g_1 + \delta g_2 + \gamma\delta) \tag{1}$$

[da die beiden Producte $\alpha\beta(\gamma + \delta + 1)$ und $\gamma\delta(\alpha + \beta + 1)$ immer gerade Zahlen sind]; und daraus ergiebt sich, dass unter den vier Charakteristiken (0, 0), (0, 1), (1, 0), (1, 1), die letzte (1, 1), und nur diese, die Eigenschaft hat, durch alle linearen Transformationen ungeändert zu bleiben; denn weder $\alpha$ und $\beta$ noch $\gamma$ und $\delta$ können zugleich gerade Zahlen sein, wenn

$\alpha\delta - \beta\gamma = 1$ ist. Die zu dieser Charakteristik gehörige $t$-Function hat zugleich die Eigenschaft, für $u = 0$ zu verschwinden. Diese $t$-Function betrachten wir also zunächst.

Ist

$$(\omega_1', \omega_2') = \begin{pmatrix} \alpha, \beta \\ \gamma, \delta \end{pmatrix} (\omega_1, \omega_2),$$

so sind nach unserem Transformationsprincip

$$t(u, \omega_1, \omega_2) \text{ und } t(u, \omega_1', \omega_2')$$

verwandte $T$-Functionen erster Ordnung und folglich ist, wenn $C$, $\lambda$, $\mu$ von $u$ unabhängige Grössen sind,

$$t(u, \omega_1', \omega_2') = C e^{\lambda u^2 + \mu u}\, t(u, \omega_1, \omega_2). \tag{2}$$

Es ergiebt sich hieraus durch logarithmische Differentiation

$$2\lambda u + \mu = \frac{d \log t(u, \omega_1', \omega_2')}{du} - \frac{d \log t(u, \omega_1, \omega_2)}{du}. \tag{3}$$

Nun ist, wenn wir nach Potenzen von $u$ nach dem Taylor'schen Lehrsatz entwickeln, und mit $t'$, $t''$ $t'''$ die erste, zweite, dritte Derivirte von $t$ nach $u$ für $u = 0$ bezeichnen,

$$\frac{d \log t(u, \omega_1, \omega_2)}{du} = \frac{1}{u} + \frac{t''}{2t'} + u\left(\frac{t'''}{3t'} - \frac{t''^2}{4t'^2}\right) + \cdots,$$

woraus sich durch Vergleichung mit (3) ergiebt, dass $\lambda$ und $\mu$ in die Form gesetzt werden können:

$$\lambda = \varphi(\omega_1', \omega_2') - \varphi(\omega_1, \omega_2)$$
$$\mu = \psi(\omega_1', \omega_2') - \psi(\omega_1, \omega_2),$$

worin

$$\varphi(\omega_1, \omega_2) = \frac{t'''}{6t'} - \frac{t''^2}{8t'^2}, \quad \psi(\omega_1, \omega_2) = \frac{t''}{2t'}. \tag{4}$$

Bestimmt man ferner noch den Factor $C$ in (2) durch den speciellen Werth $u = 0$, so folgt

$$C = \frac{t'(\omega_1', \omega_2')}{t'(\omega_1, \omega_2)}. \tag{5}$$

Hiernach lässt sich die Formel (2) in folgendem Lehrsatz aussprechen:

Die Function

$$\sigma(u, \omega_1, \omega_2) = e^{-u^2\left(\frac{t'''}{6t'} - \frac{t''^2}{8t'^2}\right) - u\frac{t''}{2t'}}\, \frac{t(u, \omega_1, \omega_2)}{t'} \tag{6}$$

bleibt ungeändert, wenn man $\omega_1$, $\omega_2$, durch $\omega_1'$, $\omega_2'$ ersetzt, d. h. wenn man irgend eine lineare Transformation anwendet, oder:

(7) $$\sigma(u, \omega_1', \omega_2') = \sigma(u, \omega_1, \omega_2).$$

Die durch (6) definirte Function bleibt, wie eine einfache Rechnung zeigt, ungeändert, wenn man $t$ durch irgend eine verwandte $t$-Function ersetzt.

Wenn die Periodicitätsfactoren der Function $t(u)$

(8) $$e^{-\pi i a_1 (2u + \omega_1) - \pi i b_1}, \quad e^{-\pi i a_2 (2u + \omega_2) - \pi i b_2}$$

sind, so ist, da die Charakteristik von $t = (1, 1)$ vorausgetzt war nach §. 14, (1)

(9) $$e^{-\pi i b_1} = - e^{-\mu \pi i \omega_1}, \quad e^{-\pi i b_2} = - e^{-\mu \pi i \omega_2},$$

worin $\mu$ jeder Werth sein kann, der sich durch $t$ selbst in folgender Weise ausdrücken lässt.

Aus
$$t(u + \omega_1) = - e^{-\pi i a_1 (2u + \omega_1) - \pi i \mu \omega_1}\, t(u)$$
folgt durch Vertauschung von $u$ mit $-u - \omega_1$:
$$t(-u - \omega_1) = - e^{-\pi i a_1 (2u + \omega_1) + \pi i \mu \omega_1}\, t(-u),$$
und entsprechend für $t(-u - \omega_2)$, so dass $t(u)$ und $t(-u)$ verwandte $T$-Functionen sind. Sie unterscheiden sich also nur durch einen Exponentialfactor von einander, und es ergiebt sich leicht, wenn man einen constanten Factor aus $u = 0$ bestimmt:

(10) $$t(-u) = - e^{2 \pi i \mu u}\, t(u).$$

Differentiirt man diese Gleichung zweimal nach $u$ und setzt dann $u = 0$, so folgt

(11) $$2 \pi i \mu = - \frac{t''}{t'}.$$

Mit Benutzung dieser Relation findet man nun nach (6) die Periodicitätsfactoren der $\sigma$-Function folgendermaassen:
$$- e^{- \left[\pi i a_1 + \omega_1 \left(\frac{t'''}{6t} - \frac{t''^2}{8t'^2}\right)\right] (2u + \omega_1)}$$
$$- e^{- \left[\pi i a_2 + \omega_2 \left(\frac{t'''}{6t'} - \frac{t''^2}{8t'^2}\right)\right] (2u + \omega_2)},$$
so dass, wenn man zur Abkürzung

(12) $$\begin{aligned} \pi i a_1 + \omega_1 \left(\frac{t'''}{6t'} - \frac{t''^2}{8t'^2}\right) &= - \eta_1 \\ \pi i a_2 + \omega_2 \left(\frac{t'''}{6t'} - \frac{t''^2}{8t'^2}\right) &= - \eta_2 \end{aligned}$$

setzt, man für $\sigma(u)$ die fundamentalen Relationen erhält:

$$\begin{aligned} \sigma(u + \omega_1) &= -\, e^{\eta_1 (2u + \omega_1)}\, \sigma(u) \\ \sigma(u + \omega_2) &= -\, e^{\eta_2 (2u + \omega_2)}\, \sigma(u). \end{aligned} \tag{13}$$

Die durch (12) eingeführten $\eta_1$, $\eta_2$ sind Functionen von $\omega_1$, $\omega_2$, welche nach der Relation §. 13, (2) die Gleichung befriedigen:

$$\eta_1 \omega_2 - \eta_2 \omega_1 = \pi i. \tag{14}$$

Durch wiederholte Anwendung von (13) ergiebt sich, wenn $a$, $b$ ganze Zahlen sind [vergl. §. 23, (3)]:

$$\begin{gathered} \sigma(u + a\omega_1 + b\omega_2) = \\ (-1)^{a + b + ab}\, e^{(a\eta_1 + b\eta_2)(2u + a\omega_1 + b\omega_2)}\, \sigma(u). \end{gathered} \tag{15}$$

Wenn man die Formeln (7) bis (11) auf die Function $\sigma$ selbst, welche ja unter den Functionen $t$ mit enthalten ist, anwendet, so ist zu setzen

$$-\pi i a_1 = \eta_1, \quad -\pi i a_2 = \eta_2, \quad \mu = 0,$$

folglich:

$$\begin{gathered} \sigma(-u) = -\,\sigma(u) \\ \sigma(0) = 0,\ \sigma'(0) = 1,\ \sigma''(0) = 0,\ \sigma'''(0) = 0 \end{gathered} \tag{16}$$

[nach (6), (11) und (12)].

Die Function $\sigma(u)$ ist also eine ungerade Function.

Wenn auf $\omega_1$, $\omega_2$ eine lineare Substitution

$$(\omega_1', \omega_2') = \begin{pmatrix} \alpha, \beta \\ \gamma, \delta \end{pmatrix} (\omega_1, \omega_2) \tag{17}$$

angewendet wird, so erfahren die Grössen $\eta_1$, $\eta_2$ die entsprechende Substitution

$$(\eta_1', \eta_2') = \begin{pmatrix} \alpha, \beta \\ \gamma, \delta \end{pmatrix} (\eta_1, \eta_2), \tag{18}$$

was eine unmittelbare Folge der Relationen (7) und (15) ist.

Differentiirt man die Formeln (13) logarithmisch nach $u$, so folgt

$$\begin{aligned} \frac{\sigma'(u + \omega_1)}{\sigma(u + \omega_1)} &= \frac{\sigma'(u)}{\sigma(u)} + 2\eta_1 \\ \frac{\sigma'(u + \omega_2)}{\sigma(u + \omega_2)} &= \frac{\sigma'(u)}{\sigma(u)} + 2\eta_2, \end{aligned} \tag{19}$$

und indem man in der ersten $u = -\frac{\omega_1}{2}$, in der zweiten $u = -\frac{\omega_2}{2}$ setzt, und beachtet, dass $\sigma(u)$ eine ungerade und folglich $\sigma'(u)$ eine gerade Function von $u$ ist:

$$(20) \qquad \eta_1 = \frac{\sigma'\left(\frac{\omega_1}{2}\right)}{\sigma\left(\frac{\omega_1}{2}\right)}, \qquad \eta_2 = \frac{\sigma'\left(\frac{\omega_2}{2}\right)}{\sigma\left(\frac{\omega_2}{2}\right)}.$$

## §. 31. Die Functionen $\sigma_{00}$, $\sigma_{01}$, $\sigma_{10}$.

Es bleibt uns noch übrig, die analogen Resultate für die übrigen Charakteristiken zu gewinnen. Wir gehen aus von der folgenden Bemerkung: Sind $x_1, x_2$; $y_1, y_2$ irgend zwei Paare von Grössen, welche durch dieselbe lineare Substitution ($S$) in $x'_1, x'_2$; $y'_1, y'_2$ transformirt werden, ist also:

$$(x'_1, x'_2) = \begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix}(x_1, x_2); \quad (y'_1, y'_2) = \begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix}(y_1, y_2),$$

so ist auch

$$x_1 y_2 - x_2 y_1 = x'_1 y'_2 - x'_2 y'_1,$$

wie aus der Multiplication der Determinanten hervorgeht. Demnach ist, was auch $x_1, x_2$ sei, nach (7), §. 30:

$$(1) \quad \sigma(u + x_2\omega_1 - x_1\omega_2, \omega_1, \omega_2) = \sigma(u + x'_2\omega'_1 - x'_1\omega'_2, \omega'_1, \omega'_2).$$

Diese Function ändert sich der Formel (15) des vorigen Paragraphen gemäss, wenn $x_1$, $x_2$ um ganze Zahlen geändert werden. Diese Aenderung kann man aber vermeiden, wenn man statt dessen die Function

$$e^{-2(\eta_1 x_2 - \eta_2 x_1)u}\, \frac{\sigma(u + x_2\omega_1 - x_1\omega_2)}{\sigma(x_2\omega_1 - x_1\omega_2)}$$

betrachtet, welche wir (für den Augenblick) mit $\sigma(u, x_1, x_2, \omega_1, \omega_2)$ bezeichnen wollen. Diese Function genügt den Bedingungen:

$$(2) \qquad \sigma(u, x'_1, x'_2, \omega'_1, \omega'_2) = \sigma(u, x_1, x_2, \omega_1, \omega_2)$$

$$(3) \qquad \begin{aligned} \sigma(u, x_1 + 1, x_2, \omega_1, \omega_2) &= \sigma(u, x_1, x_2, \omega_1, \omega_2) \\ \sigma(u, x_1, x_2 + 1, \omega_1, \omega_2) &= \sigma(u, x_1, x_2, \omega_1, \omega_2) \end{aligned}$$

$$(4) \qquad \begin{aligned} \sigma(u + \omega_1) &= -\, e^{-2\pi i x_1}\; e^{\eta_1(2u + \omega_1)}\, \sigma(u) \\ \sigma(u + \omega_2) &= -\, e^{-2\pi i x_2}\; e^{\eta_2(2u + \omega_2)}\, \sigma(u). \end{aligned}$$

Indem wir uns nun wieder auf die Hauptcharakteristiken beschränken, setzen wir $(x_1, x_2) = \left(-\frac{1}{2}, \frac{1}{2}\right), \left(0, \frac{1}{2}\right), \left(-\frac{1}{2}, 0\right)$ und erhalten so die folgenden drei Functionen:

$$\sigma_{00}(u) = \sigma\left(u, -\frac{1}{2}, \frac{1}{2}, \omega_1, \omega_2\right) = e^{-(\eta_1+\eta_2)u} \frac{\sigma\left(u + \frac{\omega_1+\omega_2}{2}\right)}{\sigma\left(\frac{\omega_1+\omega_2}{2}\right)}$$

$$\sigma_{01}(u) = \sigma\left(u, 0, \frac{1}{2}, \omega_1, \omega_2\right) = e^{-\eta_1 u} \frac{\sigma\left(u + \frac{\omega_1}{2}\right)}{\sigma\left(\frac{\omega_1}{2}\right)} \tag{5}$$

$$\sigma_{10}(u) = \sigma\left(u, -\frac{1}{2}, 0, \omega_1, \omega_2\right) = e^{-\eta_2 u} \frac{\sigma\left(u + \frac{\omega_2}{2}\right)}{\sigma\left(\frac{\omega_2}{2}\right)}$$

und die Function $\sigma(u)$ selbst kann entsprechend auch mit $\sigma_{11}(u)$ bezeichnet werden.

Für diese Functionen ergeben sich nach (4) die charakteristischen Periodengleichungen

$$\begin{gathered} \sigma_{g_1, g_2}(u + \omega_1) = (-1)^{g_1} e^{\eta_1(2u+\omega_1)} \sigma_{g_1, g_2}(u) \\ \sigma_{g_1, g_2}(u + \omega_2) = (-1)^{g_2} e^{\eta_2(2u+\omega_2)} \sigma_{g_1, g_2}(u) \\ \sigma_{g_1, g_2}(u + a\omega_1 + b\omega_2) = \\ (-1)^{g_1 a + g_2 b + ab} \; e^{(a\eta_1 + b\eta_2)(2u + a\omega_1 + b\omega_2)} \sigma_{g_1, g_2}(u). \end{gathered} \tag{6}$$

Durch Anwendung einer linearen Transformation werden die drei Functionen $\sigma_{00}$, $\sigma_{01}$, $\sigma_{10}$ unter einander permutirt, wie die Formel (2) lehrt [oder §. 30, (1)]. Je nach dieser Permutation zerfallen die linearen Transformationen in sechs Classen, deren erste alle diejenigen Transformationen umfasst, welche die Functionen $\sigma_{00}$, $\sigma_{01}$, $\sigma_{10}$ ungeändert lassen. Diese sind dadurch charakterisirt, dass $\alpha$, $\delta$ ungerade, $\beta$, $\gamma$ gerade Zahlen sind, was wir kurz so schreiben:

$$\begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix} \equiv \begin{pmatrix}1, 0 \\ 0, 1\end{pmatrix} \pmod{2}.$$

Hiernach sind die sechs Classen der linearen Transformationen folgendermaassen zu charakterisiren:

$$\text{I.} \quad \begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix} \equiv \begin{pmatrix}1, 0 \\ 0, 1\end{pmatrix} \text{(mod. 2)} \quad (00,\ 01,\ 10)$$

$$\text{II.} \quad \text{„} \quad \equiv \begin{pmatrix}0, 1 \\ -1, 0\end{pmatrix} \quad \text{„} \quad (00,\ 10,\ 01)$$

$$\text{III.}\quad \begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} \equiv \begin{pmatrix}1, & 1\\ -1, & 0\end{pmatrix} \;(\text{mod. } 2.)\quad (10,\ 00,\ 01)$$

$$\text{IV.}\quad ,, \equiv \begin{pmatrix}1, & 1\\ 0, & 1\end{pmatrix} \quad ,, \quad (10,\ 01,\ 00)$$

$$\text{V.}\quad ,, \equiv \begin{pmatrix}1, & 0\\ 1, & 1\end{pmatrix} \quad ,, \quad (01,\ 00,\ 10)$$

$$\text{VI.}\quad ,, \equiv \begin{pmatrix}0, & 1\\ -1, & 1\end{pmatrix} \quad ,, \quad (01,\ 10,\ 00),$$

wo in der letzten Columne die jedesmalige Permutation der Charakteristiken 00, 01, 10 aufgeführt ist.

Die Transformationen der ersten Classe bilden eine sogenannte Gruppe, insofern eine aus zwei Transformationen der ersten Classe zusammengesetzte Transformation wieder der ersten Classe angehört. Bei den übrigen Classen ist dies nicht der Fall.

So wie sämmtliche lineare Transformationen aus den beiden Fundamentaltransformationen, so lassen sich die Transformationen der ersten Classe aus wiederholter Anwendung von

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

ableiten, was sich auf dem Wege des §. 25 beweisen lässt.

## §. 32. Darstellung der $\sigma$-Functionen durch $\vartheta$-Functionen.

Um die Function $\sigma(u)$ als $\vartheta$-Function darzustellen, kann man einfach die Formel (6) des §. 30 auf die Function

$$t(u) = \vartheta_{11}\left(\frac{u}{\omega_1}, \frac{\omega_2}{\omega_1}\right)$$

anwenden, also

$$(1)\qquad \sigma(u, \omega_1, \omega_2) = \omega_1\, e^{-\frac{u^2}{6\omega_1^2}\frac{\vartheta'''_{11}}{\vartheta'_{11}}}\, \frac{\vartheta_{11}\left(\frac{u}{\omega_1}, \frac{\omega_2}{\omega_1}\right)}{\vartheta'_{11}}$$

setzen. Es ist aber in Folge der Differentialgleichung §. 17, (4):

$$\vartheta'''_{11} = 4\pi i\,\frac{d\vartheta'_{11}}{d\omega}$$

und also nach §. 29, (2):

$$\frac{\vartheta'''_{11}}{\vartheta'_{11}} = 4\pi i \frac{d \log \vartheta'_{11}}{d\omega} = 12\pi i \frac{d \log \eta(\omega)}{d\omega}. \tag{2}$$

Durch logarithmische Differentiation von (1) erhält man mittelst (2):

$$\frac{d \log \sigma(u)}{du} = -\frac{4\pi i u}{\omega_1^2} \frac{d \log \eta(\omega)}{d\omega} + \frac{d \log \vartheta_{11}\left(\frac{u}{\omega_1}, \frac{\omega_2}{\omega_1}\right)}{du}$$

und wenn man hierin $u = \frac{\omega_1}{2}, \frac{\omega_2}{2}$ setzt und die Formeln (10) des §. 18 anwendet nach §. 30, (20):

$$\begin{aligned} \eta_1 &= -\frac{2\pi i}{\omega_1} \frac{d \log \eta(\omega)}{d\omega} \\ \eta_2 &= -\frac{2\pi i \omega_2}{\omega_1^2} \frac{d \log \eta(\omega)}{d\omega} - \frac{\pi i}{\omega_1} \end{aligned} \tag{3}$$

Hiernach kann man für $\sigma$ setzen:

$$\sigma(u) = \omega_1 e^{\frac{\eta_1 u^2}{\omega_1}} \frac{\vartheta_{11}\left(\frac{u}{\omega_1}, \frac{\omega_2}{\omega_1}\right)}{\vartheta'_{11}}, \tag{4}$$

und für die drei Functionen $\sigma_{00}$, $\sigma_{01}$, $\sigma_{10}$ erhält man nach §. 31 (5) mit Benutzung von §. 30 (14):

$$\begin{aligned} \sigma_{00}(u) &= e^{\frac{\eta_1 u^2}{\omega_1}} \frac{\vartheta_{00}\left(\frac{u}{\omega_1}, \frac{\omega_2}{\omega_1}\right)}{\vartheta_{00}}, \\ \sigma_{01}(u) &= e^{\frac{\eta_1 u^2}{\omega_1}} \frac{\vartheta_{01}\left(\frac{u}{\omega_1}, \frac{\omega_2}{\omega_1}\right)}{\vartheta_{01}}, \\ \sigma_{10}(u) &= e^{\frac{\eta_1 u^2}{\omega_1}} \frac{\vartheta_{10}\left(\frac{u}{\omega_1}, \frac{\omega_2}{\omega_1}\right)}{\vartheta_{10}}. \end{aligned} \tag{5}$$

Die Functionen $\sigma_{00}(u)$, $\sigma_{01}(u)$, $\sigma_{10}(u)$ sind also gerade Functionen von $u$, welche den Bedingungen

$$\sigma_{00}(0) = 1, \quad \sigma_{01}(0) = 1, \quad \sigma_{10}(0) = 1 \tag{6}$$

genügen, und durch zweimalige logarithmische Differentiation ergiebt sich noch [nach (3) und §. 29, (2)]:

$$\sigma''_{00}(0) + \sigma''_{01}(0) + \sigma''_{10}(0) = 0. \tag{7}$$

Die Ausdrücke (4), (5) für die $\sigma$-Functionen lassen auf den ersten Blick eine wichtige Eigenschaft derselben erkennen, dass nämlich $\sigma_{00}$, $\sigma_{01}$, $\sigma_{10}$ nur von den Verhältnissen $u : \omega_1 : \omega_2$ abhängen, während bei $\sigma$ dasselbe, abgesehen von dem Factor $\omega_1$, gilt. Es sind also $\sigma$, $\sigma_{00}$, $\sigma_{01}$, $\sigma_{10}$ homogene Functionen der drei Variablen $u$, $\omega_1$, $\omega_2$ erstere von der ersten, die drei anderen von der nullten Ordnung, oder, in Zeichen, wenn $\lambda$ einen willkürlichen Factor bedeutet:

$$(8)\quad \begin{aligned} \sigma\;(\lambda u_1, \lambda\omega_1, \lambda\omega_2) &= \lambda\,\sigma\,(u, \omega_1, \omega_2) \\ \sigma_{00}\,(\lambda u_1, \lambda\omega_1, \lambda\omega_2) &= \sigma_{00}\,(u, \omega_1, \omega_2) \\ \sigma_{01}\,(\lambda u_1, \lambda\omega_1, \lambda\omega_2) &= \sigma_{01}\,(u, \omega_1, \omega_2) \\ \sigma_{10}\,(\lambda u_1, \lambda\omega_1, \lambda\omega_2) &= \sigma_{10}\,(u, \omega_1, \omega_2). \end{aligned}$$

## §. 33. Lineare Transformation der Function $\eta(\omega)$.

Die Formeln (3) §. 32 führen zur linearen Transformation der Function $\eta(\omega)$. Wird nämlich

$$(1)\qquad (\omega_1', \omega_2') = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} (\omega_1, \omega_2)$$

gesetzt, so geht $(\eta_1, \eta_2)$ über in

$$(2)\qquad (\eta_1', \eta_2') = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} (\eta_1, \eta_2)$$

[§. 30, (18)] und $\omega = \omega_2 : \omega_1$ in

$$(3)\qquad \omega' = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}.$$

Nun folgt aus (2) mit Rücksicht auf (3) des vorigen Paragraphen:

$$\eta_1' = -\frac{2\pi i}{\omega_1'}\frac{d\,log\,\eta(\omega')}{d\omega'} = -\frac{2\pi i\,\omega_1'}{\omega_1^2}\frac{d\,log\,\eta(\omega)}{d\omega} - \frac{\pi i\beta}{\omega_1}$$

$$\eta_2' = -\frac{2\pi i\,\omega_2'}{\omega_1'^2}\frac{d\,log\,\eta(\omega')}{d\omega'} - \frac{\pi i}{\omega_1'} = -\frac{2\pi i\,\omega_2}{\omega_1^2}\frac{d\,log\,\eta(\omega)}{d\omega} - \frac{\pi i\delta}{\omega_1},$$

und diese beiden Relationen geben übereinstimmend

$$\frac{d\,log\,\eta(\omega')}{\omega_1'^2\,d\omega'} = \frac{d\,log\,\eta(\omega)}{\omega_1^2\,d\omega} + \frac{\beta}{2\,\omega_1\,\omega_1'},$$

oder endlich, da nach (3)

$$d\omega' = \frac{d\omega}{(\alpha + \beta\omega)^2},$$

$$\frac{d\log\eta(\omega')}{d\omega} = \frac{d\log\eta(\omega)}{d\omega} + \frac{\beta}{2(\alpha + \beta\omega)}.$$

Hieraus folgt durch Integration:

$$(4) \qquad \eta\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right) = \varepsilon\sqrt{\alpha + \beta\omega}\,\eta(\omega),$$

worin $\varepsilon$ eine von $\omega$ unabhängige, also nur von den Zahlen $\alpha$, $\beta$, $\gamma$, $\delta$ abhängige Grösse ist.

Die genaue Bestimmung dieser Constanten $\varepsilon$, namentlich auch mit Rücksicht auf das Vorzeichen ist ein bekanntes wichtiges Problem, welches eigenthümliche Schwierigkeiten bietet, dessen Lösung aber für uns unerlässlich ist. Lösungen desselben haben auf verschiedenen Wegen Hermite[1]) und Dedekind[2]) gegeben. Wir wollen hier einen Weg gehen, welcher den Vorzug grosser Einfachheit hat, dafür freilich nicht eine Ableitung, sondern einen Beweis der fertigen Formel enthält.

Für zwei specielle Fälle haben wir schon früher [§. 29, (4), (5)] diese Bestimmung ausgeführt und auf dies Ergebniss werden wir uns hier stützen. Es sind die Formeln

$$(5) \qquad \eta(\omega \pm 1) = e^{\pm\frac{\pi i}{12}}\,\eta(\omega)$$

und

$$(6) \qquad \eta\left(-\frac{1}{\omega}\right) = \sqrt{-i\omega}\,\eta(\omega),$$

worin $\sqrt{-i\omega}$ mit positivem reellem Theil zu nehmen ist.

Wir setzen nun

$$(7) \qquad \frac{\eta\left(\dfrac{\gamma + \delta\omega}{\alpha + \beta\omega}\right)}{\eta(\omega)} = E\left(\begin{matrix}\alpha, \beta\\ \gamma, \delta\end{matrix}, \omega\right),$$

und haben den Werth dieses Symbols zu bestimmen. Nach (5), (6), (7) haben wir:

$$(8) \qquad E\left(\begin{matrix}-\alpha, -\beta\\ -\gamma, -\delta\end{matrix}, \omega\right) = E\left(\begin{matrix}\alpha, \beta\\ \gamma, \delta\end{matrix}, \omega\right),$$

---

[1]) Liouville's Journal, Ser. II, T. III, 1858.

[2]) Erläuterungen zum XXVII. Fragment in Riemann's Werken und „Ueber die elliptischen Modulfunctionen", Crelle's Journal, Bd. 83, S. 265. Vgl. auch des Verfassers Abhandlung „Zur Theorie der elliptischen Functionen", Acta Mathematica, Bd. 6, S. 341 ff.

(9) $$E\begin{pmatrix}1, 0\\ 0, 1\end{pmatrix}, \omega) = 1,$$

(10) $$E\begin{pmatrix}1, 0\\ \pm 1, 1\end{pmatrix}, \omega) = e^{\pm\frac{\pi i}{12}},$$

(11) $$E\begin{pmatrix}0, 1\\ -1, 0\end{pmatrix}, \omega) = \sqrt{-i\omega}.$$

Wir betrachten jetzt zwei Substitutionen und die aus beiden zusammengesetzte, also:

$$\begin{pmatrix}\alpha'', \beta''\\ \gamma'', \delta''\end{pmatrix} = \begin{pmatrix}\alpha', \beta'\\ \gamma', \delta'\end{pmatrix}\begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix}.$$

Ist dann

$$\omega' = \frac{\gamma + \delta\omega}{\alpha + \beta\omega},$$

so ergiebt sich unmittelbar aus der Definition (7):

(12) $$E\left(\begin{matrix}\alpha'', \beta''\\ \gamma'', \delta''\end{matrix}, \omega\right) = E\left(\begin{matrix}\alpha', \beta'\\ \gamma', \delta'\end{matrix}, \omega'\right) E\left(\begin{matrix}\alpha, \beta\\ \gamma, \delta\end{matrix}, \omega\right),$$

und davon zwei besondere Fälle, indem man

$$\begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix} = \begin{pmatrix}1, 0\\ \pm 1, 1\end{pmatrix}, \begin{pmatrix}0, 1\\ -1, 0\end{pmatrix}$$

setzt und an Stelle von $\alpha', \beta', \gamma', \delta'$ wieder $\alpha, \beta, \gamma, \delta$ schreibt, also

$$\begin{pmatrix}\alpha'', \beta''\\ \gamma'', \delta''\end{pmatrix} = \begin{pmatrix}\alpha \pm \beta, \beta\\ \gamma \pm \delta, \delta\end{pmatrix}, \begin{pmatrix}-\beta, \alpha\\ -\delta, \gamma\end{pmatrix}:$$

(13) $$E\left(\begin{matrix}\alpha \pm \beta, \beta\\ \gamma \pm \delta, \delta\end{matrix}, \omega\right) = e^{\pm\frac{\pi i}{12}} E\left(\begin{matrix}\alpha, \beta\\ \gamma, \delta\end{matrix}, \omega \pm 1\right)$$

(14) $$E\left(\begin{matrix}\pm\beta, \mp\alpha\\ \pm\delta, \mp\gamma\end{matrix}, \omega\right) = \sqrt{-i\omega}\, E\left(\begin{matrix}\alpha, \beta\\ \gamma, \delta\end{matrix}, \frac{-1}{\omega}\right).$$

Es hat sich nun in §. 25 gezeigt, dass durch wiederholte Anwendung der beiden Fundamentaltransformationen

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

und ihrer inversen Transformationen sich alle linearen Transformationen zusammensetzen lassen, und daraus folgt auf Grund von (12), dass durch die Formeln (8) bis (14) das Symbol $E$ vollständig definirt ist. Von den in (10), (13), (14) enthaltenen je zwei Formeln kann übrigens die eine als Folge aus der anderen hergeleitet werden.

Wenn wir also einen diesen Bedingungen genügenden Ausdruck kennen, so muss derselbe mit $E$ übereinstimmen. Um einen solchen aufzustellen, unterscheiden wir zwei Fälle. Da $\alpha$, $\beta$ relative Primzahlen sind, so ist eine von ihnen sicher ungerade. Wir setzen:

1. $\alpha$ ungerade und positiv:

$$E\begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix}, \omega\Big) = \left(\frac{\beta}{\alpha}\right) i^{\frac{\alpha-1}{2}} e^{\frac{\pi i}{12}[\alpha(\gamma-\beta)-(\alpha^2-1)\beta\delta]} \sqrt{(\alpha+\beta\omega)};$$

(15)

2. $\beta$ ungerade und positiv:

$$E\begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix}, \omega\Big) = \left(\frac{\alpha}{\beta}\right) i^{\frac{1-\beta}{2}} e^{\frac{\pi i}{12}[\beta(\alpha+\delta)-(\beta^2-1)\alpha\gamma]} \sqrt{-i(\alpha+\beta\omega)},$$

wozu noch Folgendes zu bemerken ist: Die Wurzeln $\sqrt{\alpha+\beta\omega}$, $\sqrt{-i(\alpha+\beta\omega)}$ sind mit positivem reellem Theil zu nehmen. Dass eine derselben rein imaginär sei, ist durch die Annahme, dass $\omega$ einen positiven imaginären Theil hat, und $\alpha$ resp. $\beta$ positiv sei, ausgeschlossen. $\left(\frac{\beta}{\alpha}\right)$ und $\left(\frac{\alpha}{\beta}\right)$ ist das Legendre-Jacobi'sche Symbol aus der Theorie der quadratischen Reste, mit der Erweiterung, dass $\left(\frac{\beta}{1}\right)$ und $\left(\frac{0}{1}\right) = 1$ sein soll. Wenn im ersten Falle $\alpha$ oder im zweiten $\beta$ negativ ist, so müssen rechts die sämmtlichen Vorzeichen von $\alpha$, $\beta$, $\gamma$, $\delta$ umgekehrt werden. Wenn sowohl $\alpha$ als $\beta$ ungerade sind, so kann sowohl (15) 1. als (15) 2. angewandt werden, und beides ergiebt, wie man leicht auf Grund des Reciprocitätsgesetzes der quadratischen Reste nachweist, dasselbe Resultat. Es ist nämlich, wenn $\alpha$ und $\beta$ ungerade sind, $\alpha$ positiv angenommen wird, und das obere oder untere Zeichen gilt, je nachdem $\beta$ positiv oder negativ ist:

$$\left(\frac{\beta}{\alpha}\right)\left(\frac{\pm\alpha}{\pm\beta}\right) = \pm e^{-\frac{\pi i}{4}(\alpha\mp 1)(\beta-1)}$$

$$\sqrt{\mp i(\alpha+\beta\omega)} = e^{\mp\frac{\pi i}{4}} \sqrt{\alpha+\beta\omega}$$

und die Identität von (15) 1., 2. ergiebt sich dann aus der Congruenz

$$-3\alpha\beta+\beta(\alpha+\delta)-(\beta^2-1)\alpha\gamma \equiv \alpha(\gamma-\beta)-(\alpha^2-1)\beta\delta \pmod{24}.$$

Dass durch (15) die Formeln (8) bis (11) befriedigt sind, ist unmittelbar einzusehen, und es bleibt noch zu zeigen, dass (13) und (14) erfüllt sind. Wir beginnen mit (14), wobei angenommen werden kann, dass $\alpha$ ungerade (und positiv) sei; denn vertauscht man in (14) $\omega$ mit $-1:\omega$, so vertauschen sich $\alpha$ und $-\beta$, und diese können nicht beide gerade sein.

Es ist

$$\sqrt{-i\omega}\;\sqrt{\alpha-\frac{\beta}{\omega}}=\sqrt{-i\,(-\beta+\alpha\,\omega)},$$

da beide Seiten dieser Gleichung einen positiven reellen Theil haben, und danach ergiebt sich aus (15) 1:

$$\sqrt{-i\,\omega}\;E\left(\begin{matrix}\alpha, & \beta\\ \gamma, & \delta\end{matrix},\frac{-1}{\omega}\right)$$

$$=\left(\frac{\beta}{\alpha}\right)i^{\frac{\alpha-1}{2}}\;e^{\frac{\pi i}{12}[\alpha(\gamma-\beta)-(\alpha^2-1)\beta\delta]}\;\sqrt{-i\,(-\beta+\alpha\,\omega)}.$$

Dieselbe Formel aber erhält man, da $\left(\frac{-\beta}{\alpha}\right)=i^{(\alpha-1)}\left(\frac{\beta}{\alpha}\right)$, aus (15) 2. für

$$E\left(\begin{matrix}-\beta, & \alpha\\ -\delta, & \gamma\end{matrix},\omega\right)$$

und damit ist (14) bewiesen.

Es bleibt noch die Formel (13). Ist zunächst $\beta$ ungerade (und positiv), so ergiebt sich (13) unmittelbar aus (15) 2. auf Grund der Congruenz

$$(\beta^2-1)(1-\beta\gamma-\alpha\delta-\beta\delta)\equiv-\beta(\beta^2-1)(2\gamma+\delta)\equiv 0\;(\mathrm{mod}\;24).$$

Ist $\beta$ gerade, so ist $\alpha$ ungerade. Nehmen wir $\alpha$ positiv, so kann $\alpha+\beta$ positiv oder negativ sein. Gelten im ersten Falle die oberen, im zweiten die unteren Zeichen, so ergiebt uns (15) 1:

$$(16)\qquad e^{\frac{i\pi}{12}}\,E\left(\begin{matrix}\alpha, & \beta\\ \gamma, & \delta\end{matrix},\omega+1\right)=$$

$$\left(\frac{\beta}{\alpha}\right)i^{-\frac{1-\alpha}{2}}\;e^{\frac{\pi i}{12}[1+\alpha(\gamma-\beta)-(\alpha^2-1)\beta\delta]}\;\sqrt{\alpha+\beta+\beta\,\omega},$$

$$(17)\qquad E\left(\begin{matrix}\alpha+\beta, & \beta\\ \gamma+\delta, & \delta\end{matrix},\omega\right)=$$

$$\left(\frac{\pm\beta}{(\alpha+\beta)}\right)i^{-\frac{1\mp(\alpha+\beta)}{2}}\;e^{\frac{\pi i}{12}\{(\alpha+\beta)(\gamma+\delta-\beta)-[(\alpha+\beta)^2-1]\beta\delta\}}\;\sqrt{\pm(\alpha+\beta+\beta\,\omega)}.$$

Nun ist, wenn die unteren Zeichen gelten,

$$\sqrt{-(\alpha+\beta+\beta\,\omega)}=i\,\sqrt{\alpha+\beta+\beta\,\omega},$$

ferner nach dem Reciprocitätsgesetz der quadratischen Reste:

$$\left(\frac{\beta}{\alpha+\beta}\right) = (-1)^{\frac{\beta(\alpha+1)}{4}} \left(\frac{\beta}{\alpha}\right),$$

$$\left(\frac{-\beta}{-(\alpha+\beta)}\right) = (-1)^{\frac{\alpha-1}{2}} (-1)^{\frac{\beta(\alpha-1)}{4}} \left(\frac{\beta}{\alpha}\right)$$[1],

und daraus folgt leicht die Uebereinstimmung der beiden Ausdrücke (16), (17) und mithin die Richtigkeit der Formel (13) nach der Congruenz

$$\beta(3\alpha - 2\gamma + \beta - \delta + \beta^2\delta + 2\alpha\beta\delta) \equiv 0 \pmod{24},$$

die sich, da $\beta$ gerade vorausgesetzt ist, aus $\alpha\delta - \beta\gamma = 1$ ergiebt.

Somit sind also die Formeln (15) als richtig erwiesen.

Setzen wir

$$E\left(\begin{matrix}\alpha, \beta \\ \gamma, \delta\end{matrix}, \omega\right) = \varepsilon\sqrt{\alpha + \beta\omega}, \tag{18}$$

so ist $\varepsilon$ eine 24te Einheitswurzel, deren Product mit $\sqrt{\alpha+\beta\omega}$ durch (15) vollständig bestimmt ist, und es ergiebt sich die Transformation der $\eta$-Function

$$\eta\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right) = \varepsilon\sqrt{\alpha + \beta\omega}\;\eta(\omega). \tag{19}$$

Für $\varepsilon^{12}$ findet man

$$\varepsilon^{12} = (-1)^{\alpha\beta + \gamma\delta + \beta\gamma}. \tag{20}$$

---

[1] Nach dem Reciprocitätsgesetz ist, wenn $\beta = \pm 2^\lambda \beta'$ gesetzt und $\beta'$ ungerade und positiv angenommen wird, wenn $\alpha + \beta$ positiv ist

$$\left(\frac{\beta}{\alpha+\beta}\right) = \left(\frac{\pm 2^\lambda}{\alpha+\beta}\right)\left(\frac{\alpha}{\beta'}\right)(-1)^{\frac{(\alpha+\beta-1)(\beta'-1)}{4}}$$

$$\left(\frac{\beta}{\alpha}\right) = \left(\frac{\pm 2^\lambda}{\alpha}\right)\left(\frac{\alpha}{\beta'}\right)(-1)^{\frac{(\alpha-1)(\beta'-1)}{4}}.$$

Ist $\lambda \geqq 2$, so sind diese beiden Werthe einander gleich, ist $\lambda = 1$, so unterscheiden sie sich durch den Factor $(-1)^{\frac{\alpha+1}{2}}$, in Uebereinstimmung mit der ersten der obigen Eormeln. Die Richtigkeit der zweiten Formel ergiebt sich, wenn $\alpha + \beta$ negativ ist, aus

$$\left(\frac{-\beta}{-(\alpha+\beta)}\right) = \left(\frac{2^\lambda}{\alpha+\beta}\right)\left(\frac{\alpha}{\beta'}\right)(-1)^{\frac{(\alpha+\beta-1)(\beta'-1)}{4}}$$

$$\left(\frac{\beta}{\alpha}\right) = \left(\frac{2^\lambda}{\alpha}\right)\left(\frac{\alpha}{\beta'}\right)(-1)^{\frac{\alpha-1}{2}}(-1)^{\frac{(\alpha-1)(\beta'-1)}{4}}.$$

## §. 34. Lineare Transformation der $\vartheta$-Functionen.

Hiernach sind die Transformationsformeln der $\vartheta$-Functionen einfache Folgen der Grundeigenschaften der $\sigma$-Function, durch die Substitution

$$(\omega_1', \omega_2') = \begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix} (\omega_1, \omega_2)$$

ungeändert zu bleiben. Beachtet man, dass

$$\vartheta_{11}' = 2\pi\,\eta(\omega)^3$$

ist, so giebt die Formel (4), §. 32, mit Rücksicht auf §. 30, (14), wenn man $\omega_1$, $\omega_2$, $\eta_1$ durch $\omega_1'$, $\omega_2'$, $\eta_1'$ ersetzt und

$$(1) \qquad v = \frac{u}{\omega_1}, \qquad \omega = \frac{\omega_2}{\omega_1},$$

$$(2) \qquad v' = \frac{u}{\omega_1'} = \frac{v}{\alpha + \beta\omega}, \qquad \omega' = \frac{\omega_2'}{\omega_1'} = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}$$

setzt:

$$(3) \qquad e^{-\pi i \beta v v'}\, \vartheta_{11}(v', \omega') = \varepsilon^3 \sqrt{\alpha + \beta\omega}\, \vartheta_{11}(v, \omega).$$

Die Transformationsformeln der drei übrigen Functionen $\vartheta_{00}$, $\vartheta_{01}$, $\vartheta_{10}$ sind verschieden in den sechs Classen des §. 31, und können aus den Formeln (5), §. 32 in derselben Weise hergeleitet werden. Man kann die sechs Fälle aber auch in ein einziges Formelsystem zusammenfassen, welches man aus (3) erhält, wenn man $v$ ersetzt durch

$$v + \frac{\alpha + \beta\omega}{2}, \qquad v + \frac{\gamma + \delta\omega}{2}, \qquad v + \frac{\alpha + \gamma + (\beta + \delta)\omega}{2},$$

also $v'$ durch

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

und dann auf der rechten und linken Seite von (3) die Formeln (6), (7), (10) des §. 18 anwendet. So kommt:

$$(4) \qquad e^{-\pi i \beta v v'}\, \vartheta_{10}(v', \omega')$$

$$= i^{\beta} e^{-\frac{\pi i \alpha\beta}{4}} \varepsilon^3 \sqrt{\alpha + \beta\omega}\, \vartheta_{1+\beta,\, 1-\alpha}(v, \omega),$$

$$(5) \qquad e^{-\pi i \beta v v'}\, \vartheta_{01}(v', \omega')$$

$$= i^{\delta-1} e^{-\frac{\pi i \gamma\delta}{4}} \varepsilon^3 \sqrt{\alpha + \beta\omega}\, \vartheta_{1+\delta,\, 1-\gamma}(v, \omega),$$

$$(6) \qquad e^{-\pi i \beta v v'} \vartheta_{00}(v', \omega')$$
$$= i^{\delta + \beta - \alpha\delta} e^{-\frac{\pi i}{4}(\alpha\beta + \gamma\delta)} \varepsilon^3 \sqrt{\alpha + \beta\omega}\, \vartheta_{1+\beta+\delta,\, 1-\alpha-\gamma}(v, \omega).$$

Die vierten Potenzen dieser Functionen lassen sich einfacher ausdrücken durch

$$(7)\ e^{-4\pi i \beta v v'} \vartheta^4_{g_1, g_2}(v', \omega') = (-1)^{g_2 \alpha\beta + g_1 \gamma\delta + \beta\gamma} (\alpha + \beta\,\omega)^2 \vartheta^4_{g'_1, g'_2}(v),$$

worin in den sechs Classen die Charakteristiken $(g_1, g_2)$ und $(g'_1, g'_2)$ der in §. 31 gegebenen Tabelle entsprechen.

Eine einfachere Transformationsformel erhält man aus den $\sigma$-Functionen für das Product der drei $\vartheta$-Functionen (4), (5), (6). Es ist nämlich, wenn man das Product der drei Functionen §. 32, (5) bildet:

$$\sigma_{00}(u)\ \sigma_{01}(u)\ \sigma_{10}(u)$$
$$= e^{\frac{3\eta_1 u^2}{\omega_1}} \frac{\vartheta_{00}\left(\frac{u}{\omega_1}, \frac{\omega_2}{\omega_1}\right) \vartheta_{01}\left(\frac{u}{\omega_1}, \frac{\omega_2}{\omega_1}\right) \vartheta_{10}\left(\frac{u}{\omega_1}, \frac{\omega_2}{\omega_1}\right)}{\vartheta_{00}\,\vartheta_{01}\,\vartheta_{10}}$$

eine Function, welche bei linearer Transformation völlig ungeändert bleibt. Macht man noch Gebrauch von der Relation

$$\eta'_1\,\omega_1 - \eta_1\,\omega'_1 = -\pi i \beta,$$

die sich aus §. 30, (14) ergiebt, so folgt

$$(8) \qquad \frac{\vartheta_{00}(v, \omega)\,\vartheta_{01}(v, \omega)\,\vartheta_{10}(v, \omega)}{\vartheta_{00}\,\vartheta_{01}\,\vartheta_{10}}$$
$$= e^{-3\pi i \beta v v'} \frac{\vartheta_{00}(v', \omega')\,\vartheta_{01}(v', \omega')\,\vartheta_{10}(v', \omega')}{\vartheta_{00}(0, \omega')\,\vartheta_{01}(0, \omega')\,\vartheta_{10}(0, \omega')},$$

worin man noch nach (19) des vorigen Paragraphen

$$\vartheta_{00}(0, \omega')\,\vartheta_{01}(0, \omega')\,\vartheta_{10}(0, \omega') = \varepsilon^3 \sqrt{\alpha + \beta\omega}^{\,3}\ \vartheta_{00}\,\vartheta_{01}\,\vartheta_{10}$$

setzen kann.

Wir ziehen aber aus (8) einen anderen Schluss: Setzt man nämlich

$$v' = \frac{2h}{n}, \qquad v = \frac{2h(\alpha + \beta\omega)}{n},$$

und nimmt das Product für $h = 1, 2, \cdot\cdot \frac{n-1}{2}$, so ergiebt sich mittelst der bekannten Relation

$$\sum_{1,\ \frac{n-1}{2}}^{h} h^2 = n\,\frac{n^2-1}{24},$$

wenn man auf der rechten Seite von (8) die Formel (23), §. 27 anwendet:

$$(9)\ 2^{\frac{n-1}{2}} \prod_{1,\frac{n-1}{2}}^{h} \vartheta_{00}\left(\frac{2h(\alpha+\beta\omega)}{n}\right) \vartheta_{01}\left(\frac{2h(\alpha+\beta\omega)}{n}\right) \vartheta_{10}\left(\frac{2h(\alpha+\beta\omega)}{n}\right)$$

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

worin nun $\alpha, \beta$ irgend ein Paar relativer Primzahlen sein kann.

## §. 35. Lineare Transformation der Functionen $f(\omega)$, $f_1(\omega)$, $f_2(\omega)$.

Die Formeln für die lineare Transformation der $f$-Functionen sind nach §. 29, (9) eine einfache Folge der Transformation der $\eta$-Function.

Setzen wir in der linearen Transformation

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

zunächst $\beta$ als gerade und folglich $\alpha$, $\delta$ als ungerade voraus, so ist

$$(1)\qquad \begin{pmatrix} 1, & 0 \\ 0, & 2 \end{pmatrix} \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} = \begin{pmatrix} \alpha, & \frac{1}{2}\beta \\ 2\gamma, & \delta \end{pmatrix} \begin{pmatrix} 1, & 0 \\ 0, & 2 \end{pmatrix}.$$

Es ist aber nach §. 29, (9):

$$f_2(\omega) = \sqrt{2}\,\frac{\eta(2\omega)}{\eta(\omega)},$$

und wenn wir also die Substitution

$$\frac{\gamma+\delta\omega}{\alpha+\beta\omega}$$

machen, so ergiebt sich, mit Benutzung der Bezeichnung des §. 33

$$(2)\qquad f_2\left(\frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right) = \frac{E\begin{pmatrix} \alpha, & \frac{1}{2}\beta \\ 2\gamma, & \delta \end{pmatrix}, 2\omega}{E\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}, \omega} f_2(\omega),$$

worin (15) 1, §. 33 zu beachten ist. Diese Formel giebt

$$\frac{E\begin{pmatrix}\alpha, \frac{1}{2}\beta \\ 2\gamma, \delta\end{pmatrix}, 2\omega}{E\begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix}, \omega} = \left(\frac{2}{\alpha}\right) e^{\frac{\pi i}{12}\left(\alpha\gamma + \frac{\alpha\beta}{2} + (\alpha^2 - 1)\frac{\beta\delta}{2}\right)}$$

Es ist aber

$$\alpha\gamma + \frac{\alpha\beta}{2} + (\alpha^2 - 1)\frac{\beta\delta}{2} \equiv 9\,\frac{\alpha(2\gamma + \beta)}{2} \pmod 8$$

$$\equiv -8\,[\alpha(\gamma - \beta) - (\alpha^2 - 1)\beta\delta] \pmod 3,$$

und wenn wir also zur Abkürzung

$$(3) \qquad \varrho = e^{-\frac{2\pi i}{8}[\alpha(\gamma - \beta) - (\alpha^2 - 1)\beta\delta]}$$

setzen, so ergiebt sich aus (2):

$$(4)\ f_2\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right) = \left(\frac{2}{\alpha}\right) \varrho\, e^{\frac{3\pi i}{8}\alpha(2\gamma + \beta)} f_2(\omega), \qquad \beta \equiv 0 \pmod 2.$$

In derselben Weise lassen sich alle anderen Formeln dieser Art herleiten; man erhält sie aber einfacher aus (4) selbst mit Benutzung der Fundamentaltransformationen §. 29, (13), (14), (15). So ergiebt sich, wenn man in (4) $\omega$ durch $-1:\omega$ ersetzt und dann $\alpha, \beta, \gamma, \delta$ mit $\beta, -\alpha, \delta, -\gamma$ vertauscht (wodurch $\varrho$ ungeändert bleibt):

$$(5)\ f_2\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right) = \left(\frac{2}{\beta}\right) \varrho\, e^{\frac{3\pi i}{8}\beta(2\delta - \alpha)} f_1(\omega), \qquad \alpha \equiv 0 \pmod 2,$$

und ersetzt man hierin $\omega$ durch $\omega + 3$ und $\gamma, \alpha$ durch $\gamma - 3\delta$, $\alpha - 3\beta$, so folgt

$$(6)\ f_2\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right) = -\ \varrho\, e^{\frac{3\pi i}{8}\beta(2\delta - \alpha)} f(\omega), \qquad \alpha - \beta \equiv 0 \pmod 2.$$

Setzt man in (4), (5), (6)

$$f_2\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right) = f_1\left(-\frac{\alpha + \beta\omega}{\gamma + \delta\omega}\right),$$

und vertauscht dann $\alpha, \beta, \gamma, \delta$ mit $-\gamma, -\delta, \alpha, \beta$, so ergiebt sich

$$(7)\ f_1\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right) = \left(\frac{2}{\gamma}\right) \varrho\, e^{-\frac{3\pi i}{8}\gamma(2\alpha - \delta)} f_2(\omega), \qquad \delta \equiv 0 \pmod 2$$

$$(8) \qquad = \left(\frac{2}{\delta}\right) \varrho\, e^{-\frac{3\pi i}{8}\delta(2\beta + \gamma)} f_1(\omega), \qquad \gamma \equiv 0 \pmod 2$$

$$(9) \qquad = -\ \varrho\, e^{-\frac{3\pi i}{8}\delta(2\beta + \gamma)} f(\omega), \quad \gamma - \delta \equiv 0 \pmod 2$$

Aus (9) und (6) erhält man, indem man $\omega$ durch $\frac{-\gamma+\alpha\omega}{\delta-\beta\omega}$ und dann $\alpha, \beta, \gamma, \delta$ durch $\delta, -\beta, -\gamma, \alpha$ ersetzt:

$$(10)\ f\left(\frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right) = -\varrho\, e^{-\frac{3\pi i}{8}\alpha(2\beta+\gamma)} f_1(\omega),\quad \alpha-\gamma \equiv 0 \pmod 2,$$

$$(11)\ f\left(\frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right) = -\varrho\, e^{\frac{3\pi i}{8}\beta(2\alpha-\delta)} f_2(\omega),\quad \beta-\delta \equiv 0 \pmod 2,$$

und wenn man endlich in (10) $\omega$ durch $\omega+9$ und $\gamma, \alpha$ durch $\gamma-9\delta, \alpha-9\beta$ ersetzt:

$$(11)\quad f\left(\frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right) = \varrho\left(\frac{2}{\alpha-\beta}\right) e^{-\frac{3\pi i}{8}(\alpha-\beta)(\alpha+\beta+\gamma-\delta)} f(\omega),$$
$$\alpha+\beta+\gamma-\delta \equiv 0 \pmod 2)\,[1].$$

---

[1] Die von Hermite (Sur la théorie des équations modulaires, Paris 1859) eingeführten Functionen $\varphi(\omega)$, $\psi(\omega)$, $\chi(\omega)$ hängen mit den Functionen $f(\omega)$, $f_1(\omega)$, $f_2(\omega)$ durch die Gleichungen

$$f(\omega) = \frac{\sqrt[6]{2}}{\chi(\omega)},\quad f_1(\omega) = \sqrt[6]{2}\,\frac{\psi(\omega)}{\chi(\omega)},\quad f_2(\omega) = \sqrt[6]{2}\,\frac{\varphi(\omega)}{\chi(\omega)}$$

zusammen. Die Transformationsformeln der $f$-Functionen lassen sich mit Benutzung der Relation $\alpha\delta-\beta\gamma=1$ auf mannigfaltige Weise umgestalten. So sind die von Hermite a. a. O. angegebenen Formeln nicht ohne Weiteres mit den unserigen als identisch zu erkennen. Eine einfache Rechnung zeigt aber ihre Uebereinstimmung. Die oben gegebenen Formeln haben den Vorzug, dass sie, ohne an Einfachheit zu verlieren, je zwei der sechs Transformationsclassen in einen Ausdruck zusammenfassen.

# Vierter Abschnitt.

## Die elliptischen Functionen.

### §. 36. Zusammenhang der $\vartheta$-Functionen mit den elliptischen Integralen.

In Folge von §. 18 bestehen zwischen den Quadraten der vier $\vartheta$-Functionen zwei von einander unabhängige lineare Gleichungen, so dass man zwei von diesen Quadraten durch die beiden anderen oder auch alle vier durch zwei unabhängige Variable $\xi$, $\eta$ ausdrücken kann. Indem wir das Letztere thun, bezeichnen wir mit $\xi_1$, $\eta_1$; $\xi_2$, $\eta_2$; $\xi_3$, $\eta_3$; $\xi_4$, $\eta_4$ Constanten und setzen, indem wir an die Bezeichnungsweise des ersten Abschnitts (§. 3) anknüpfen:

$$\begin{aligned}
\vartheta_{01}^2(u) &= \xi\,\eta_1 - \eta\,\xi_1 = (\xi\;\eta_1),\\
\vartheta_{11}^2(u) &= \xi\,\eta_2 - \eta\,\xi_2 = (\xi\;\eta_2),\\
\vartheta_{10}^2(u) &= \xi\,\eta_3 - \eta\,\xi_3 = (\xi\;\eta_3),\\
\vartheta_{00}^2(u) &= \xi\,\eta_4 - \eta\,\xi_4 = (\xi\;\eta_4).
\end{aligned} \tag{1}$$

Zwischen den Constanten $\xi_i$, $\eta_i$ und den Werthen $\vartheta_{01}$, $\vartheta_{10}$, $\vartheta_{00}$ bestehen vier Relationen, die sich aus den Gleichungen (14) des §. 18

$$\begin{aligned}
(\xi\;\eta_3)\,\vartheta_{01}^2 &= (\xi\;\eta_1)\,\vartheta_{10}^2 - (\xi\;\eta_2)\,\vartheta_{00}^2\\
(\xi\;\eta_4)\,\vartheta_{01}^2 &= (\xi\;\eta_1)\,\vartheta_{00}^2 - (\xi\;\eta_2)\,\vartheta_{10}^2
\end{aligned} \tag{2}$$

herleiten lassen. Man kann diesen Relationen, indem man in (2) $\xi$, $\eta = \xi_1$, $\eta_1$ und $= \xi_2$, $\eta_2$ setzt, die Form geben:

$$(3)\qquad \begin{aligned}(\xi_1\ \eta_3)\ \vartheta_{01}^2 &= (\xi_2\ \eta_1)\ \vartheta_{00}^2,\\ (\xi_2\ \eta_3)\ \vartheta_{01}^2 &= (\xi_2\ \eta_1)\ \vartheta_{10}^2,\\ (\xi_1\ \eta_4)\ \vartheta_{01}^2 &= (\xi_2\ \eta_1)\ \vartheta_{10}^2,\\ (\xi_2\ \eta_4)\ \vartheta_{01}^2 &= (\xi_2\ \eta_1)\ \vartheta_{00}^2,\end{aligned}$$

wozu man noch fügen kann, indem man in (2) $\xi, \eta = \xi_4, \eta_4$ setzt und §. 18, (15) benutzt:

$$(4)\qquad (\xi_4\ \eta_3) = (\xi_2\ \eta_1),$$

und aus (3) und (4) folgt für die Doppelverhältnisse:

$$(5)\qquad \frac{(\xi_2\ \eta_3)\ (\xi_1\ \eta_4)}{(\xi_1\ \eta_3)\ (\xi_2\ \eta_4)} = \frac{\vartheta_{10}^4}{\vartheta_{00}^4},$$

$$(6)\qquad \frac{(\xi_1\ \eta_2)\ (\xi_3\ \eta_4)}{(\xi_1\ \eta_3)\ (\xi_2\ \eta_4)} = \frac{\vartheta_{01}^4}{\vartheta_{00}^4}.$$

Wenn wir nun zwei der Gleichungen (1), etwa die beiden ersten, differentiiren, so folgt:

$$\begin{aligned}2\,\vartheta_{01}(u)\ \vartheta_{01}'(u)\ du &= \eta_1\ d\xi - \xi_1\ d\eta\\ 2\,\vartheta_{11}(u)\ \vartheta_{11}'(u)\ du &= \eta_2\ d\xi - \xi_2\ d\eta\end{aligned}$$

und daraus mit Benutzung von (1)

$$\begin{aligned}2\,\vartheta_{01}(u)\ \vartheta_{11}(u)\ [\vartheta_{01}'(u)\ \vartheta_{11}(u) - \vartheta_{11}'(u)\ \vartheta_{01}(u)]\ du&\\ = (\xi_2\,\eta_1 - \eta_2\,\xi_1)\ (\xi\ d\eta - \eta\ d\xi) &= (\xi_2\ \eta_1)\ (\xi\ d\eta)\end{aligned}$$

und mit Benutzung von §. 20 (6):

$$(7)\qquad 2\pi\ \vartheta_{01}^2\,\vartheta_{00}(u)\ \vartheta_{11}(u)\ \vartheta_{10}(u)\ \vartheta_{01}(u)\ du = (\xi_1\,\eta_2)\ (\xi\,d\eta).$$

Führt man hierin nach (3)

$$(8)\qquad (\xi_1\ \eta_2)\ \vartheta_{00}^2 = \sqrt{(\xi_1\,\eta_3)\ (\xi_2\,\eta_4)}\ \vartheta_{01}^2$$

ein, und setzt für die ϑ-Functionen die Ausdrücke (1), so folgt schliesslich

$$(9)\qquad 2\pi\ \vartheta_{00}^2\,du = \frac{\sqrt{(\xi_1\ \eta_3)\ (\xi_2\ \eta_4)}\ (\xi\ d\eta)}{\sqrt{(\xi\ \eta_1)\ (\xi\ \eta_2)\ (\xi\ \eta_3)\ (\xi\ \eta_4)}},$$

so dass $du$ durch ein elliptisches Differential erster Gattung ausgedrückt ist.

Es ist durch (1) das Verhältniss $\xi:\eta$ als doppeltperiodische Function von $u$ bestimmt. Desgleichen sind aber auch die Verhältnisse der Quadratwurzeln

$$(10)\qquad \sqrt{(\xi\ \eta_1)},\quad \sqrt{(\xi\ \eta_2)},\quad \sqrt{(\xi\ \eta_3)},\quad \sqrt{(\xi\ \eta_4)}$$

als eindeutige doppeltperiodische Functionen erklärt, und das Vorzeichen der Quadratwurzeln in (9) ist hierdurch und durch (8) ebenfalls eindeutig bestimmt.

Wir bemerken noch die folgenden zusammengehörigen Werthe:

$$(11)\qquad \begin{aligned} u &= \frac{1}{2}\omega, & \xi:\eta &= \xi_1:\eta_1, \\ u &= 0, & \xi:\eta &= \xi_2:\eta_2, \\ u &= \frac{1}{2}, & \xi:\eta &= \xi_3:\eta_3, \\ u &= \frac{1+\omega}{2}, & \xi:\eta &= \xi_4:\eta_4, \end{aligned}$$

wie aus (1) sofort hervorgeht.

## §. 37. Jacobi's elliptische Functionen.

Die letzten Betrachtungen haben einen bemerkenswerthen Zusammenhang zwischen den doppeltperiodischen Functionen und den elliptischen Integralen erster Gattung ergeben. Um diesen Zusammenhang tiefer zu ergründen, gehen wir zunächst auf die Legendre'sche Normalform über. Wir setzen:

$$(1)\qquad \eta:\xi=\zeta,\ \xi_1=0,\ \eta_2=0,\ \xi_3=\eta_3,\ \xi_4=\varkappa^2\eta_4,\ \varkappa'^2=1-\varkappa^2$$

und erhalten aus (3), §. 36

$$(2)\qquad \frac{\xi_2}{\eta_1}=-\frac{\vartheta_{10}^2}{\vartheta_{00}^2},\qquad \frac{\eta_3}{\eta_1}=\frac{\vartheta_{10}^2}{\vartheta_{01}^2},\qquad \frac{\eta_4}{\eta_1}=\frac{\vartheta_{00}^2}{\vartheta_{01}^2}.$$

$$(3)\qquad \sqrt{\varkappa}=\frac{\vartheta_{10}}{\vartheta_{00}},\qquad \sqrt{\varkappa'}=\frac{\vartheta_{01}}{\vartheta_{00}}.$$

Aus (1) und (9) des vorigen Paragraphen findet sich

$$(4)\qquad \begin{aligned} \frac{\vartheta_{00}}{\vartheta_{10}}\,\frac{\vartheta_{11}(u)}{\vartheta_{01}(u)} &= \sqrt{\zeta} \\ \frac{\vartheta_{01}}{\vartheta_{10}}\,\frac{\vartheta_{10}(u)}{\vartheta_{01}(u)} &= \sqrt{1-\zeta} \\ \frac{\vartheta_{01}}{\vartheta_{00}}\,\frac{\vartheta_{00}(u)}{\vartheta_{01}(u)} &= \sqrt{1-\varkappa^2\zeta}. \end{aligned}$$

$$(5)\qquad 2\pi\vartheta_{00}^2 u=\int_0^{\zeta}\frac{d\zeta}{\sqrt{\zeta(1-\zeta)(1-\varkappa^2\zeta)}},$$

worin der Integrationsweg und die Bedeutung der Wurzelzeichen durch die Formeln (4) selbst bestimmt ist, wenn der Uebergang von 0 zu $u$ in der $u$-Ebene gegeben ist. Es darf aber dann auch der Integrationsweg in (5) geändert werden, wenn dabei nur keiner der singulären Punkte $\infty$, 1, $\frac{1}{\varkappa^2}$ überschritten wird.

Die Gleichung (5) lässt sich in folgenden drei Formen schreiben:

$$
\begin{aligned}
d\sqrt{\zeta} &= \pi\,\vartheta_{00}^2 \sqrt{(1-\zeta)(1-\varkappa^2\zeta)}\,du,\\
d\sqrt{1-\zeta} &= -\pi\,\vartheta_{00}^2 \sqrt{\zeta(1-\varkappa^2\zeta)}\,du, \qquad (6)\\
d\sqrt{1-\varkappa^2\zeta} &= -\pi\,\vartheta_{00}^2\,\varkappa^2 \sqrt{\zeta(1-\zeta)}\,du.
\end{aligned}
$$

Führen wir eine neue Variable $v$ ein durch die Gleichung

$$\pi\,\vartheta_{00}^2 u = v, \tag{7}$$

so werden die Gleichungen (5), (6):

$$v = \frac{1}{2}\int_0^{\zeta} \frac{d\zeta}{\sqrt{\zeta(1-\zeta)(1-\varkappa^2\zeta)}}, \tag{8}$$

$$
\begin{aligned}
d\sqrt{\zeta} &= \sqrt{(1-\zeta)(1-\varkappa^2\zeta)}\,dv\\
d\sqrt{1-\zeta} &= -\sqrt{\zeta(1-\varkappa^2\zeta)}\,dv \qquad (9)\\
d\sqrt{1-\varkappa^2\zeta} &= -\varkappa^2\sqrt{\zeta(1-\zeta)}\,dv
\end{aligned}
$$

und nun betrachten wir die drei Grössen $\sqrt{\zeta} = x$, $\sqrt{1-\zeta} = y$, $\sqrt{1-\varkappa^2\zeta} = z$, durch (4) und (7) definirt, als Functionen der Variablen $v$. Nach (4) sind es eindeutige, doppeltperiodische und, abgesehen von einzelnen Punkten, in denen sie unendlich werden, stetige Functionen von $v$. Sie werden nach Jacobi sinus amplitudinis, cosinus amplitudinis, $\Delta$ amplitudinis von $v$ genannt und mit $\operatorname{sinam} v$, $\operatorname{cosam} v$, $\Delta \operatorname{am} v$ bezeichnet. Wir wollen uns hier der schon im §. 10 erwähnten kürzeren Gudermann'schen Bezeichnung $\operatorname{sn} v$, $\operatorname{cn} v$, $\operatorname{dn} v$ bedienen, so dass

$$
\begin{aligned}
\frac{\vartheta_{11}(u)}{\vartheta_{01}(u)} &= \sqrt{\varkappa}\,\operatorname{sn} v,\\
\frac{\vartheta_{10}(u)}{\vartheta_{01}(u)} &= \sqrt{\frac{\varkappa}{\varkappa'}}\,\operatorname{cn} v, \qquad (10)\\
\frac{\vartheta_{00}(u)}{\vartheta_{01}(u)} &= \frac{1}{\sqrt{\varkappa'}}\,\operatorname{dn} v.
\end{aligned}
$$

Diese Functionen genügen nach (9) den Differentialgleichungen

$$(11)\qquad \begin{aligned} \frac{dx}{dv} &= y\,z \\ \frac{dy}{dv} &= -\,z\,x \\ \frac{dz}{dv} &= -\,\varkappa^2 x\,y \end{aligned}$$

und den Nebenbedingungen

$$(12)\qquad \operatorname{sn} 0 = 0, \qquad \operatorname{cn} 0 = 1, \qquad \operatorname{dn} 0 = 1.$$

Es bestehen zwischen ihnen die Relationen

$$(13)\qquad y^2 = 1 - x^2, \qquad z^2 = 1 - \varkappa^2 x^2.$$

Aus den Fundamentaleigenschaften der $\vartheta$-Functionen ergeben sich die ersten Eigenschaften der elliptischen Functionen:

$$(14)\quad \operatorname{sn} v = -\operatorname{sn}(-v), \quad \operatorname{cn} v = \operatorname{cn}(-v), \quad \operatorname{dn} v = \operatorname{dn}(-v),$$

d. h. $\operatorname{sn} v$ ist eine ungerade, $\operatorname{cn} v$, $\operatorname{dn} v$ sind gerade Functionen.

Setzen wir noch

$$(15)\qquad \pi\,\vartheta_{00}^2 = 2K, \qquad \pi\,\vartheta_{00}^2\,\omega = 2\,i\,K',$$

so erhält $v$ die Werthe $K$, $i\,K'$, $K + i\,K'$, wenn $u = \frac{1}{2}, \frac{\omega}{2}, \frac{1+\omega}{2}$ wird, und es folgt aus (4) mit Rücksicht auf §. 18:

$$(16)\qquad \begin{aligned} &\operatorname{sn} K = 1, \quad \operatorname{sn}(K + i\,K') = \frac{1}{\varkappa} \\ &\operatorname{cn} K = 0, \quad \operatorname{cn}(K + i\,K') = -\,\frac{i\,\varkappa'}{\varkappa} \\ &\operatorname{dn} K = \varkappa', \quad \operatorname{dn}(K + i\,K') = 0 \\ &\operatorname{sn} i\,K', \quad \operatorname{cn} i\,K', \quad \operatorname{dn} i\,K' = \infty. \end{aligned}$$

Nun lassen sich $K$, $K'$ vermittelst (8) durch bestimmte Integrale ausdrücken und man erhält, wenn man $v$ von einem Eckpunkte des Parallelogramms $0, K, K + i\,K', i\,K'$ bis zum folgenden längs der Peripherie sich bewegen lässt, also $u$ längs

$$0, \quad \frac{1}{2}, \quad \frac{1+\omega}{2}, \quad \frac{\omega}{2}.$$

$$(17)\qquad K = \frac{1}{2} \int_0^1 \frac{d\zeta}{\sqrt{\zeta(1-\zeta)(1-\varkappa^2\zeta)}},$$

$$(18)\qquad i\,K' = \frac{1}{2} \int_1^{\frac{1}{\varkappa^2}} \frac{d\zeta}{\sqrt{\zeta(1-\zeta)(1-\varkappa^2\zeta)}},$$

$$-K = \frac{1}{2}\int\limits_{\frac{1}{\varkappa^2}}^{\infty} \frac{d\zeta}{\sqrt{\zeta(1-\zeta)(1-\varkappa^2\zeta)}}, \tag{19}$$

$$-iK' = \frac{1}{2}\int\limits_{\infty}^{0} \frac{d\zeta}{\sqrt{\zeta(1-\zeta)(1-\varkappa^2\zeta)}}. \tag{20}$$

Die Werthe von $\sqrt{\zeta}$, $\sqrt{1-\zeta}$, $\sqrt{1-\varkappa^2\zeta}$ sind bei diesen Integrationen durch die Formeln (4) bestimmt. Wenn aber $\omega$ rein imaginär und in Folge dessen $\varkappa^2$ ein positiver echter Bruch und $K$, $K'$ reell und positiv sind, so sind die Wege für $v$ der reellen und imaginären Axe parallel, und mit Rücksicht auf die Bemerkungen am Schluss des §. 22 zeigen die Formeln (4) Folgendes:

In (17) sind $\sqrt{\zeta}$, $\sqrt{1-\zeta}$, $\sqrt{1-\varkappa^2\zeta}$ reell und positiv,
„ (18) „ $\sqrt{\zeta}$, $i\sqrt{1-\zeta}$, $\sqrt{1-\varkappa^2\zeta}$ „ „ „
„ (19) „ $\sqrt{\zeta}$, $i\sqrt{1-\zeta}$, $i\sqrt{1-\varkappa^2\zeta}$ „ „ „
„ (20) „ $-i\sqrt{\zeta}$, $\sqrt{1-\zeta}$, $\sqrt{1-\varkappa^2\zeta}$ „ „ „

und $\sqrt{\zeta}$ hat auf keinem der Integrationswege ein Maximum oder Minimum. Es können daher $K$, $K'$ durch die vier folgenden reellen Integrale mit positiver Quadratwurzel erklärt werden:

$$K = \frac{1}{2}\int\limits_{0}^{1} \frac{d\zeta}{\sqrt{\zeta(1-\zeta)(1-\varkappa^2\zeta)}} = \frac{1}{2}\int\limits_{\frac{1}{\varkappa^2}}^{\infty} \frac{d\zeta}{\sqrt{\zeta(\zeta-1)(\varkappa^2\zeta-1)}}$$

$$K' = \frac{1}{2}\int\limits_{-\infty}^{0} \frac{d\zeta}{\sqrt{-\zeta(1-\zeta)(1-\varkappa^2\zeta)}} = \frac{1}{2}\int\limits_{1}^{\frac{1}{\varkappa^2}} \frac{d\zeta}{\sqrt{\zeta(\zeta-1)(1-\varkappa^2\zeta)}}.$$

## §. 38. Die Jacobi'schen Functionen $\Theta(v)$, $H(v)$.

Wenn man die $\vartheta$-Functionen der Variablen $u$ als Functionen von $v$ betrachtet, so erhält man die Jacobi'schen $\Theta$-Functionen. Wir setzen mit Rücksicht auf (7) und (15) des vorigen Paragraphen

$$\begin{aligned} \vartheta_{01}\left(\frac{v}{2K}, \omega\right) &= \Theta(v) \\ \vartheta_{11}\left(\frac{v}{2K}, \omega\right) &= H(v), \end{aligned} \tag{1}$$

so dass $\Theta(v)$, $H(v)$ als Functionen $t(v, 2K, 2K')$ zu bezeichnen sind, und nach §. 22 ist

$$\begin{aligned}\Theta(v) &= 1 - 2q\cos\frac{\pi v}{K} + 2q^4\cos\frac{2\pi v}{K} - 2q^9\cos\frac{3\pi v}{K} + \cdots\\ H(v) &= \phantom{1 - {}} 2q^{\frac{1}{4}}\sin\frac{\pi v}{2K} - 2q^{\frac{9}{4}}\sin\frac{3\pi v}{2K} + 2q^{\frac{25}{4}}\sin\frac{5\pi v}{2K} - \cdots\end{aligned} \tag{2}$$

$$q = e^{-\frac{\pi K'}{K}}.$$

Nach §. 18 (10) ist

$$\begin{aligned}H(v) &= -i e^{-\frac{\pi K'}{4K} + \frac{\pi i v}{2K}}\,\Theta(v + iK')\\ \Theta(v) &= -i e^{-\frac{\pi K'}{4K} + \frac{\pi i v}{2K}}\,H(v + iK').\end{aligned} \tag{3}$$

Ferner:

$$\begin{aligned}\vartheta_{00}\left(\frac{v}{2K}, \omega\right) &= \Theta(v + K)\\ \vartheta_{10}\left(\frac{v}{2K}, \omega\right) &= H(v + K),\end{aligned} \tag{4}$$

wonach, mittelst der Formeln (3), (10), (15) des vorigen Paragraphen:

$$\begin{aligned}&\sqrt{\varkappa} = \frac{H(K)}{\Theta(K)}, \quad \sqrt{\varkappa'} = \frac{\Theta(0)}{\Theta(K)},\\ &\Theta(K) = \sqrt{\frac{2K}{\pi}}, \quad \Theta(0) = \sqrt{\frac{2\varkappa' K}{\pi}}, \quad H(K) = \sqrt{\frac{2\varkappa K}{\pi}};\end{aligned} \tag{5}$$

endlich die Darstellung der elliptischen Functionen:

$$\begin{aligned}\frac{H(v)}{\Theta(v)} &= \sqrt{\varkappa}\,\mathrm{sn}\,v\\ \frac{H(v+K)}{\Theta(v)} &= \sqrt{\frac{\varkappa}{\varkappa'}}\,\mathrm{cn}\,v\\ \frac{\Theta(v+K)}{\Theta(v)} &= \frac{1}{\sqrt{\varkappa'}}\,\mathrm{dn}\,v.\end{aligned} \tag{6}$$

Die Functionen $\Theta$, $H$ haben, wie aus (3) leicht folgt, die durch die folgenden Gleichungen ausgedrückte Periodicität:

$$\begin{aligned}\Theta(v + 2nK) &= \Theta(v)\\ \Theta(v + 2niK') &= (-1)^n e^{\frac{n^2\pi K'}{K} - \frac{\pi i n v}{K}}\,\Theta(v),\end{aligned} \tag{7}$$

$$\begin{aligned}H(v + 2nK) &= (-1)^n H(v)\\ H(v + 2niK') &= (-1)^n e^{\frac{n^2\pi K'}{K} - \frac{\pi i n v}{K}}\,H(v).\end{aligned} \tag{8}$$

Es ist bisweilen nützlich, die Gleichungen (3), (7), (8) folgendermaassen zusammenzufassen:

$$(9)\qquad \Phi(v + niK') = i^n e^{\frac{n^2\pi i}{4}\frac{K'}{K} - \frac{\pi i n v}{2K}}\,\Psi(v),$$

worin, wenn $n$ gerade, $\Phi$ und $\Psi$ beide gleich $\Theta$ oder beide gleich $H$, wenn $n$ ungerade, $\Phi = \Theta$, $\Psi = H$ oder $\Phi = H$, $\Psi = \Theta$ zu setzen ist.

Aus §. 19, (2), (4) ergeben sich die Additionsformeln:

$$(10)\qquad \begin{aligned} \Theta^2(0)\,\Theta(u+v)\,\Theta(u-v) &= \Theta^2(u)\,\Theta^2(v) - H^2(u)\,H^2(v) \\ \Theta^2(0)\,H(u+v)\,H(u-v) &= H^2(u)\,\Theta^2(v) - \Theta^2(u)\,H^2(v), \end{aligned}$$

wofür man auch schreiben kann:

$$(11)\qquad \begin{aligned} \Theta^2(0)\,\Theta(u+v)\,\Theta(u-v) &= \Theta^2(u)\,\Theta^2(v)\,(1 - \varkappa^2\,\mathrm{sn}^2 u\,\mathrm{sn}^2 v) \\ \Theta^2(0)\,H(u+v)\,H(u-v) &= \Theta^2(u)\,\Theta^2(v)\,\varkappa\,(\mathrm{sn}^2 u - \mathrm{sn}^2 v). \end{aligned}$$

Wir gehen nun dazu über, die Sätze über die $\vartheta$-Functionen auf die elliptischen Functionen zu übertragen und beginnen mit dem Additionstheorem.

## §. 39. Additionstheorem der elliptischen Functionen.

Aus den vier $\vartheta$-Functionen lassen sich im Ganzen zwölf Quotienten bilden, welche nach §. 37 durch elliptische Functionen ausdrückbar sind. Bildet man diese Quotienten für das Argument $u + v$, so kann man dieselben nach §. 19 durch $\vartheta$-Functionen von $u$ und von $v$ einzeln, also auch durch die entsprechenden elliptischen Functionen darstellen, und zwar immer so, dass der Nenner nur Quadrate von $\vartheta$ enthält, also rational durch $\mathrm{sn}^2 u$, $\mathrm{sn}^2 v$ ausgedrückt wird. Nehmen wir, um ein Beispiel durchzuführen, die Formel (5), §. 19, und dividiren sie einmal durch (1) und dann durch (4) (indem wir das erste Mal in (5) $v$ in $-v$ verwandeln), so folgt:

$$\frac{\vartheta_{01}\,\vartheta_{10}}{\vartheta_{00}^2}\,\frac{\vartheta_{11}(u+v)}{\vartheta_{00}(u+v)}$$

$$= \frac{\vartheta_{00}(u)\,\vartheta_{11}(u)\,\vartheta_{01}(v)\,\vartheta_{10}(v) + \vartheta_{01}(u)\,\vartheta_{10}(u)\,\vartheta_{00}(v)\,\vartheta_{11}(v)}{\vartheta_{00}^2(u)\,\vartheta_{00}^2(v) + \vartheta_{11}^2(u)\,\vartheta_{11}^2(v)},$$

$$\frac{\vartheta_{10}}{\vartheta_{01}}\,\frac{\vartheta_{00}(u+v)}{\vartheta_{11}(u+v)}$$

$$= \frac{\vartheta_{00}(u)\,\vartheta_{11}(u)\,\vartheta_{01}(v)\,\vartheta_{10}(v) - \vartheta_{01}(u)\,\vartheta_{10}(u)\,\vartheta_{00}(v)\,\vartheta_{11}(v)}{\vartheta_{11}^2(u)\,\vartheta_{01}^2(v) - \vartheta_{01}^2(u)\,\vartheta_{11}^2(v)},$$

und wenn man $u$, $v$ ersetzt durch $u:2K$, $v:2K$, so kann man nach §. 37, (10) Alles durch elliptische Functionen ausdrücken. Man erhält so

$$\frac{\operatorname{sn}(u+v)}{\operatorname{dn}(u+v)} = \frac{\operatorname{dn} u \operatorname{sn} u \operatorname{cn} v + \operatorname{dn} v \operatorname{sn} v \operatorname{cn} u}{\operatorname{dn}^2 u \operatorname{dn}^2 v + \varkappa^2 \varkappa'^2 \operatorname{sn}^2 u \operatorname{sn}^2 v}, \tag{1}$$

$$\frac{\operatorname{dn}(u+v)}{\operatorname{sn}(u+v)} = \frac{\operatorname{dn} u \operatorname{sn} u \operatorname{cn} v - \operatorname{dn} v \operatorname{sn} v \operatorname{cn} u}{\operatorname{sn}^2 u - \operatorname{sn}^2 v}. \tag{2}$$

Auf demselben Wege erhält man aus den Formeln (6), (3), (4); (7), (2), (4); (8), (2), (3); (9), (1), (2); (10), (1), (3) des §. 19:

$$\frac{\operatorname{sn}(u+v)}{\operatorname{cn}(u+v)} = \frac{\operatorname{cn} u \operatorname{sn} u \operatorname{dn} v + \operatorname{cn} v \operatorname{sn} v \operatorname{dn} u}{\operatorname{cn}^2 u \operatorname{cn}^2 v - \varkappa'^2 \operatorname{sn}^2 u \operatorname{sn}^2 v}, \tag{3}$$

$$\frac{\operatorname{cn}(u+v)}{\operatorname{sn}(u+v)} = \frac{\operatorname{cn} u \operatorname{sn} u \operatorname{dn} v - \operatorname{cn} v \operatorname{sn} v \operatorname{dn} u}{\operatorname{sn}^2 u - \operatorname{sn}^2 v}, \tag{4}$$

$$\operatorname{sn}(u+v) = \frac{\operatorname{sn} u \operatorname{cn} v \operatorname{dn} v + \operatorname{sn} v \operatorname{cn} u \operatorname{dn} u}{1 - \varkappa^2 \operatorname{sn}^2 u \operatorname{sn}^2 v}, \tag{5}$$

$$\frac{1}{\operatorname{sn}(u+v)} = \frac{\operatorname{sn} u \operatorname{cn} v \operatorname{dn} v - \operatorname{sn} v \operatorname{cn} u \operatorname{dn} u}{\operatorname{sn}^2 u - \operatorname{sn}^2 v}, \tag{6}$$

$$\operatorname{cn}(u+v) = \frac{\operatorname{cn} u \operatorname{cn} v - \operatorname{sn} u \operatorname{sn} v \operatorname{dn} u \operatorname{dn} v}{1 - \varkappa^2 \operatorname{sn}^2 u \operatorname{sn}^2 v}, \tag{7}$$

$$\frac{1}{\operatorname{cn}(u+v)} = \frac{\operatorname{cn} u \operatorname{cn} v + \operatorname{sn} u \operatorname{sn} v \operatorname{dn} u \operatorname{dn} v}{\operatorname{cn}^2 u \operatorname{cn}^2 v - \varkappa'^2 \operatorname{sn}^2 u \operatorname{sn}^2 v}, \tag{8}$$

$$\operatorname{dn}(u+v) = \frac{\operatorname{dn} u \operatorname{dn} v - \varkappa^2 \operatorname{sn} u \operatorname{sn} v \operatorname{cn} u \operatorname{cn} v}{1 - \varkappa^2 \operatorname{sn}^2 u \operatorname{sn}^2 v}, \tag{9}$$

$$\frac{1}{\operatorname{dn}(u+v)} = \frac{\operatorname{dn} u \operatorname{dn} v + \varkappa^2 \operatorname{sn} u \operatorname{sn} v \operatorname{cn} u \operatorname{cn} v}{\operatorname{dn}^2 u \operatorname{dn}^2 v + \varkappa^2 \varkappa'^2 \operatorname{sn}^2 u \operatorname{sn}^2 v}, \tag{10}$$

$$\frac{\operatorname{dn}(u+v)}{\operatorname{cn}(u+v)} = \frac{\operatorname{dn} u \operatorname{dn} v \operatorname{cn} u \operatorname{cn} v + \varkappa'^2 \operatorname{sn} u \operatorname{sn} v}{\operatorname{cn}^2 u \operatorname{cn}^2 v - \varkappa'^2 \operatorname{sn}^2 u \operatorname{sn}^2 v}, \tag{11}$$

$$\frac{\operatorname{cn}(u+v)}{\operatorname{dn}(u+v)} = \frac{\operatorname{dn} u \operatorname{dn} v \operatorname{cn} u \operatorname{cn} v - \varkappa'^2 \operatorname{sn} u \operatorname{sn} v}{\operatorname{dn}^2 u \operatorname{dn}^2 v + \varkappa^2 \varkappa'^2 \operatorname{sn}^2 u \operatorname{sn}^2 v}. \tag{12}$$

Man kann noch mannigfache andere Formeln auf dieselbe Weise herleiten, unter denen wir die folgenden drei anführen, die durch Division von §. 19, (4), (3), (1) durch (2) sich ergeben.

$$\operatorname{sn}(u+v) \operatorname{sn}(u-v) = \frac{\operatorname{sn}^2 u - \operatorname{sn}^2 v}{1 - \varkappa^2 \operatorname{sn}^2 u \operatorname{sn}^2 v}, \tag{13}$$

$$\operatorname{cn}(u+v) \operatorname{cn}(u-v) = \frac{\operatorname{cn}^2 u \operatorname{cn}^2 v - \varkappa'^2 \operatorname{sn}^2 u \operatorname{sn}^2 v}{1 - \varkappa^2 \operatorname{sn}^2 u \operatorname{sn}^2 v}, \tag{14}$$

$$(15)\qquad \mathrm{dn}(u+v)\,\mathrm{dn}(u-v) = \frac{\mathrm{dn}^2 u\,\mathrm{dn}^2 v + \varkappa^2\varkappa'^2\,\mathrm{sn}^2 u\,\mathrm{sn}^2 v}{1-\varkappa^2\,\mathrm{sn}^2 u\,\mathrm{sn}^2 v}.$$

Die wichtigsten unter diesen Formeln sind (5), (7), (9), aus welchen sich, wenn auch durch weitläufige Rechnungen, die übrigen alle herleiten lassen. Der Uebersicht halber setzen wir sie noch einmal her:

$$(16)\qquad \begin{aligned} \mathrm{sn}(u+v) &= \frac{\mathrm{sn}\,u\,\mathrm{cn}\,v\,\mathrm{dn}\,v + \mathrm{sn}\,v\,\mathrm{cn}\,u\,\mathrm{dn}\,u}{1-\varkappa^2\,\mathrm{sn}^2 u\,\mathrm{sn}^2 v} \\ \mathrm{cn}(u+v) &= \frac{\mathrm{cn}\,u\,\mathrm{cn}\,v - \mathrm{sn}\,u\,\mathrm{sn}\,v\,\mathrm{dn}\,u\,\mathrm{dn}\,v}{1-\varkappa^2\,\mathrm{sn}^2 u\,\mathrm{sn}^2 v} \\ \mathrm{dn}(u+v) &= \frac{\mathrm{dn}\,u\,\mathrm{dn}\,v - \varkappa^2\,\mathrm{sn}\,u\,\mathrm{sn}\,v\,\mathrm{cn}\,u\,\mathrm{cn}\,v}{1-\varkappa^2\,\mathrm{sn}^2 u\,\mathrm{sn}^2 v}. \end{aligned}$$

Indem man je zwei dieser Gleichungen combinirt, kann man ihnen unter anderen die Formen geben:

$$(17)\qquad \begin{aligned} \mathrm{cn}(u+v)\,\mathrm{dn}\,u\,\mathrm{dn}\,v - \mathrm{dn}(u+v)\,\mathrm{cn}\,u\,\mathrm{cn}\,v &= -\varkappa'^2\,\mathrm{sn}\,u\,\mathrm{sn}\,v \\ \mathrm{dn}(u+v)\,\mathrm{sn}\,u\,\mathrm{cn}\,v - \mathrm{sn}(u+v)\,\mathrm{dn}\,u &= -\,\mathrm{cn}\,u\,\mathrm{sn}\,v \\ \mathrm{sn}(u+v)\,\mathrm{cn}\,u - \mathrm{cn}(u+v)\,\mathrm{sn}\,u\,\mathrm{dn}\,v &= \mathrm{dn}\,u\,\mathrm{sn}\,v \\ \mathrm{cn}(u+v)\,\mathrm{cn}\,u + \mathrm{sn}(u+v)\,\mathrm{sn}\,u\,\mathrm{dn}\,v &= \mathrm{cn}\,v. \end{aligned}$$

Wir wenden die Formeln (16) zunächst an zur Feststellung der Periodicität der elliptischen Functionen, die sich natürlich auch aus §. 18 herleiten lässt. Setzt man in (16) $v = \pm K$, $v = K + iK'$ so folgt aus §. 37, (16):

$$\begin{aligned} &\mathrm{sn}(u\pm K) = \pm\frac{\mathrm{cn}\,u}{\mathrm{dn}\,u}, &&\mathrm{sn}(u+K+iK') = \frac{1}{\varkappa}\frac{\mathrm{dn}\,u}{\mathrm{cn}\,u}, \\ (18)\quad &\mathrm{cn}(u\pm K) = \mp\frac{\varkappa'\,\mathrm{sn}\,u}{\mathrm{dn}\,u}, \quad &(19)\quad &\mathrm{cn}(u+K+iK') = -\frac{i\varkappa'}{\varkappa}\frac{1}{\mathrm{cn}\,u}, \\ &\mathrm{dn}(u\pm K) = \frac{\varkappa'}{\mathrm{dn}\,u}, &&\mathrm{dn}(u+K+iK') = \frac{i\varkappa'\,\mathrm{sn}\,u}{\mathrm{cn}\,u}, \end{aligned}$$

und wenn man in (19) $u$ in $u - K$ verwandelt:

$$(20)\qquad \begin{aligned} \mathrm{sn}(u+iK') &= \frac{1}{\varkappa}\frac{1}{\mathrm{sn}\,u}, \\ \mathrm{cn}(u+iK') &= -\frac{i}{\varkappa}\frac{\mathrm{dn}\,u}{\mathrm{sn}\,u}, \\ \mathrm{dn}(u+iK') &= -i\,\frac{\mathrm{cn}\,u}{\mathrm{sn}\,u}. \end{aligned}$$

Wendet man dieselben Formeln nochmals an, so folgt:

$$
(21)\quad \begin{aligned} \operatorname{sn}(u+2K) &= -\operatorname{sn} u, \\ \operatorname{cn}(u+2K) &= -\operatorname{cn} u, \\ \operatorname{dn}(u+2K) &= \operatorname{dn} u, \end{aligned} \qquad (22)\quad \begin{aligned} \operatorname{sn}(u+2iK') &= \operatorname{sn} u \\ \operatorname{cn}(u+2iK') &= -\operatorname{cn} u \\ \operatorname{dn}(u+2iK') &= -\operatorname{dn} u. \end{aligned}
$$

Die gemeinschaftlichen Perioden dieser drei Functionen sind also $4K$, $4iK'$; ausserdem hat aber $\operatorname{sn} u$ die Periode $2iK'$, $\operatorname{dn} u$ die Periode $2K$, $\operatorname{cn} u$ die Periode $2K + 2iK'$.

Wir geben nur dem Satz über $\Theta$-Functionen (§. 18) einen anderen Ausdruck, indem wir den folgenden Satz aussprechen:

Jede doppelt periodische Function von $v$ mit den Perioden $2K$, $2iK'$ (welche überall den Charakter einer rationalen Function hat) ist, wenn sie eine gerade Function ist, eine rationale Function von $\operatorname{sn}^2 v$, und wenn sie eine ungerade Function ist, das Product von $\operatorname{sn} v \operatorname{cn} v \operatorname{dn} v$ mit einer rationalen Function von $\operatorname{sn}^2 v$.

So kann man jeden Satz, der sich auf homogene Functionen nullter Ordnung von $\vartheta$-Functionen bezieht, in einen Satz über elliptische Functionen verwandeln, und erhält daraus wieder entsprechende Sätze über elliptische Integrale. Man erkennt sofort, dass die Additionsformeln (16) keine anderen sind, als die Formeln des §. 9 im ersten Abschnitt. In derselben Weise liefert uns die Transformationstheorie der $\vartheta$-Functionen eine Lösung des Jacobi'schen Transformationsproblems der elliptischen Integrale, wie wir es im §. 5 dargelegt haben.

Wir wollen dies an den beiden Haupttransformationen zweiter Ordnung nachweisen, die wir im §. 27 ebenso wie im §. 6 als Gauss'sche und Landen'sche Transformation bezeichnet haben. Nach §. 27 ist für die Gauss'sche Transformation

$$
(23)\qquad \frac{\vartheta_{10}\left(0, \frac{\omega}{2}\right)\ \vartheta_{11}\left(u, \frac{\omega}{2}\right)}{\vartheta_{00}\left(0, \frac{\omega}{2}\right)\ \vartheta_{01}\left(u, \frac{\omega}{2}\right)} = \frac{2\,\vartheta_{01}(u)\,\vartheta_{11}(u)}{\vartheta_{01}^2(u) + \vartheta_{11}^2(u)},
$$

$$
(24)\qquad \frac{\vartheta_{10}\left(0, \frac{\omega}{2}\right)^2}{\vartheta_{00}\left(0, \frac{\omega}{2}\right)^2} = \frac{2\,\vartheta_{10}\,\vartheta_{00}}{\vartheta_{00}^2 + \vartheta_{10}^2} = \frac{2\sqrt{\varkappa}}{1+\varkappa},
$$

$$
(25)\qquad \vartheta_{00}^2\left(0, \frac{\omega}{2}\right) = (1+\varkappa)\,\vartheta_{00}^2.
$$

Nach §. 37 erhalten wir also eine Beziehung zwischen elliptischen Functionen mit zwei verschiedenen Moduln, und es ist, wenn $\lambda$, $L$, $L'$ aus $\varkappa$, $K$, $K'$ durch die Vertauschung $\left(\omega, \frac{\omega}{2}\right)$ hervorgehen nach (23), (24), (25)

$$(26) \quad \lambda = \frac{2\sqrt{\varkappa}}{1+\varkappa}, \quad L = (1+\varkappa)K, \quad L' = 2(1+\varkappa)K',$$

$$(27) \quad \operatorname{sn}[(1+\varkappa)v;\, \lambda] = \frac{(1+\varkappa)\operatorname{sn} v}{1+\varkappa \operatorname{sn}^2 v},$$

wenn der Deutlichkeit halber der Modul unter dem Functionszeichen sn als zweites Argument mit aufgeführt ist.

Für die Landen'sche Transformation ist

$$\frac{\vartheta_{11}(2u, 2\omega)}{\vartheta_{01}(2u, 2\omega)} = \frac{\vartheta_{10}(u)\vartheta_{11}(u)}{\vartheta_{00}(u)\vartheta_{01}(u)},$$

$$\frac{\vartheta_{01}(0, 2\omega)^2}{\vartheta_{00}(0, 2\omega)^2} = \frac{2\vartheta_{00}\vartheta_{01}}{\vartheta_{00}^2+\vartheta_{01}^2} = \frac{2\sqrt{\varkappa'}}{1+\varkappa'},$$

$$2\vartheta_{00}^2(0, 2\omega) = (1+\varkappa')\vartheta_{00}^2,$$

daraus, wenn $\lambda$, $\lambda'$, $L$, $L'$ durch die Vertauschung $(\omega, 2\omega)$ aus $\varkappa$, $\varkappa'$ $K$, $K'$ entstehen:

$$(28) \quad \lambda' = \frac{2\sqrt{\varkappa'}}{1+\varkappa'}, \quad \sqrt{\lambda} = \frac{\varkappa}{1+\varkappa'}, \quad \lambda = \frac{1-\varkappa'}{1+\varkappa'},$$

$$2L = (1+\varkappa')K, \qquad L' = (1+\varkappa')K',$$

$$(29) \quad \operatorname{sn}[(1+\varkappa')v,\, \lambda] = \frac{(1+\varkappa')\operatorname{sn} v \operatorname{cn} v}{\operatorname{dn} v},$$

und in (26) bis (29) erkennt man nach §. 37 die Formeln (2) und (4) des §. 6.

## §. 40. Die lineare Transformation der elliptischen Functionen.

Die Einwirkung der linearen Transformation auf die elliptischen Functionen übersieht man am besten aus der Darstellung durch die $\sigma$-Functionen. Man erhält aus (4) oder (10), §. 37 und den Formeln des §. 32:

$$
(1)\qquad
\begin{aligned}
\frac{\omega_1}{2K}\,\mathrm{sn}\,\frac{2Ku}{\omega_1} &= \frac{\sigma(u)}{\sigma_{01}(u)}\\
\mathrm{cn}\,\frac{2Ku}{\omega_1} &= \frac{\sigma_{10}(u)}{\sigma_{01}(u)}\\
\mathrm{dn}\,\frac{2Ku}{\omega_1} &= \frac{\sigma_{00}(u)}{\sigma_{01}(u)},
\end{aligned}
$$

oder auch, indem man von der Homogeneität der $\sigma$-Function Gebrauch macht:

$$
(2)\qquad
\begin{aligned}
\mathrm{sn}\,v &= \frac{\sigma(v,\,2K,\,2iK')}{\sigma_{01}(v,\,2K,\,2iK')}\\
\mathrm{cn}\,v &= \frac{\sigma_{10}(v,\,2K,\,2iK')}{\sigma_{01}(v,\,2K,\,2iK')}\\
\mathrm{dn}\,v &= \frac{\sigma_{00}(v,\,2K,\,2iK')}{\sigma_{01}(v,\,2K,\,2iK')}.
\end{aligned}
$$

Die auf der rechten Seite von (2) vorkommenden $\sigma$-Functionen hängen nur von den beiden Variablen $v$, $\omega$ ab und es kommt zunächst darauf an, die Aenderung dieser Functionen bei Anwendung der Fundamentaltransformationen

$$(\omega,\ \omega+1),\qquad \left(\omega,\ -\frac{1}{\omega}\right)$$

zu bestimmen. Wegen

$$\pi\,\vartheta_{00}^2 = 2K,\qquad 2iK' = 2\omega K$$

erhält man aus §. 26 die entsprechenden Aenderungen:

$$
\begin{array}{ccccc}
\omega, & 2K, & 2iK', & \varkappa, & \varkappa',\\[1ex]
\omega+1, & 2\varkappa' K, & 2\varkappa'(K+iK'), & \dfrac{i\varkappa}{\varkappa'}, & \dfrac{1}{\varkappa'},\\[2ex]
-\dfrac{1}{\omega}, & 2K', & 2iK, & \varkappa', & \varkappa.
\end{array}
$$

Danach ergeben sich für die $\sigma$-Functionen folgende entsprechende Aenderungen (§. 31):

$$
(3)\qquad
\begin{array}{ccccc}
\omega, & \sigma(v), & \sigma_{00}(v), & \sigma_{01}(v), & \sigma_{10}(v),\\[1ex]
\omega+1, & \varkappa'\,\sigma\!\left(\dfrac{v}{\varkappa'}\right), & \sigma_{01}\!\left(\dfrac{v}{\varkappa'}\right), & \sigma_{00}\!\left(\dfrac{v}{\varkappa'}\right), & \sigma_{10}\!\left(\dfrac{v}{\varkappa'}\right),\\[2ex]
-\dfrac{1}{\omega}, & -i\,\sigma(iv), & \sigma_{00}(iv), & \sigma_{10}(iv), & \sigma_{01}(iv),
\end{array}
$$

worin die Perioden $2K$, $2iK'$ sind. Daraus folgen nach (2) die beiden ersten linearen Transformationen der elliptischen Functionen:

$$
\begin{aligned}
&\operatorname{sn}\left(\varkappa' v, \frac{i\varkappa}{\varkappa'}\right) = \varkappa' \frac{\operatorname{sn} v}{\operatorname{dn} v}\\
(4)\qquad &\operatorname{cn}\left(\varkappa' v, \frac{i\varkappa}{\varkappa'}\right) = \frac{\operatorname{cn} v}{\operatorname{dn} v}\\
&\operatorname{dn}\left(\varkappa' v, \frac{i\varkappa}{\varkappa'}\right) = \frac{1}{\operatorname{dn} v}.
\end{aligned}
$$

$$
\begin{aligned}
&\operatorname{sn}(i v, \varkappa') = i \frac{\operatorname{sn} v}{\operatorname{cn} v}\\
(5)\qquad &\operatorname{cn}(i v, \varkappa') = \frac{1}{\operatorname{cn} v}\\
&\operatorname{dn}(i v, \varkappa') = \frac{\operatorname{dn} v}{\operatorname{cn} v}.
\end{aligned}
$$

Man erhält hiernach die zweite häufig gebrauchte Darstellung für $K'$ [§. 37, (17)]:

$$
(6)\qquad K' = \frac{1}{2}\int_0^1 \frac{d\zeta}{\sqrt{\zeta(1-\zeta)(1-\varkappa'^2\zeta)}}.
$$

Aus (4), (5) erhält man die übrigen Fälle der linearen Transformation durch wiederholte Anwendung. Setzt man in (4) $i v$, $\varkappa'$ an Stelle von $v$, $\varkappa$ und wendet (5) an, so folgt

$$
\begin{aligned}
&\operatorname{sn}\left(i\varkappa v, \frac{i\varkappa'}{\varkappa}\right) = i\varkappa \frac{\operatorname{sn} v}{\operatorname{dn} v}\\
(7)\qquad &\operatorname{cn}\left(i\varkappa v, \frac{i\varkappa'}{\varkappa}\right) = \frac{1}{\operatorname{dn} v}\\
&\operatorname{dn}\left(i\varkappa v, \frac{i\varkappa'}{\varkappa}\right) = \frac{\operatorname{cn} v}{\operatorname{dn} v}.
\end{aligned}
$$

Ersetzt man umgekehrt in (5) $v$, $\varkappa$, $\varkappa'$ durch $\varkappa' v$, $\frac{i\varkappa}{\varkappa'}$, $\frac{1}{\varkappa'}$ und wendet (4) an, so folgt:

$$
\begin{aligned}
&\operatorname{sn}\left(i\varkappa' v, \frac{1}{\varkappa'}\right) = i\varkappa' \frac{\operatorname{sn} v}{\operatorname{cn} v}\\
(8)\qquad &\operatorname{cn}\left(i\varkappa' v, \frac{1}{\varkappa'}\right) = \frac{\operatorname{dn} v}{\operatorname{cn} v}\\
&\operatorname{dn}\left(i\varkappa' v, \frac{1}{\varkappa'}\right) = \frac{1}{\operatorname{cn} v}.
\end{aligned}
$$

Ersetzt man hierin wieder $v$ durch $i v$ und $\varkappa$, $\varkappa'$ durch $\varkappa'$, $\varkappa$ und wendet (5) an, so findet man:

$$\begin{aligned} &\operatorname{sn}\left(\varkappa v, \frac{1}{\varkappa}\right) = \varkappa \operatorname{sn} v \\ (9)\qquad &\operatorname{cn}\left(\varkappa v, \frac{1}{\varkappa}\right) = \operatorname{dn} v \\ &\operatorname{dn}\left(\varkappa v, \frac{1}{\varkappa}\right) = \operatorname{cn} v, \end{aligned}$$

womit die sechs Classen der linearen Transformationen erschöpft sind, da eine noch mehrmalige Wiederholung zu keinen neuen Formeln Anlass giebt.

## §. 41. Die Weierstrass'sche $\wp$-Function.

Die linearen Transformationen der elliptischen Functionen legen es nahe, eine elliptische Function zu suchen, welche, wie die $\sigma$-Function selbst, den linearen Transformationen gegenüber unveränderlich ist. Um eine solche Function zu bilden, setzen wir zunächst die Gleichungen (1) des vorigen Paragraphen in folgende Form:

$$\begin{aligned} &\frac{\sigma_{10}(u)}{\sigma(u)} = \frac{2K}{\omega_1}\frac{\operatorname{cn} v}{\operatorname{sn} v} \\ (1)\qquad &\frac{\sigma_{00}(u)}{\sigma(u)} = \frac{2K}{\omega_1}\frac{\operatorname{dn} v}{\operatorname{sn} v} \\ &\frac{\sigma_{01}(u)}{\sigma(u)} = \frac{2K}{\omega_1}\frac{1}{\operatorname{sn} v}, \end{aligned}$$

worin zur Abkürzung

$$(2)\qquad v = \frac{2Ku}{\omega_1}$$

gesetzt ist. Hieraus schliesst man mit Hülfe der Relationen

$$\operatorname{cn}^2 v = 1 - \operatorname{sn}^2 v, \qquad \operatorname{dn}^2 v = 1 - \varkappa^2 \operatorname{sn}^2 v,$$

$$\frac{\sigma_{01}^2(u)}{\sigma^2(u)} - \frac{\sigma_{10}^2(u)}{\sigma^2(u)} = \frac{4K^2}{\omega_1^2}$$

$$\frac{\sigma_{01}^2(u)}{\sigma^2(u)} - \frac{\sigma_{00}^2(u)}{\sigma^2(u)} = \frac{4K^2}{\omega_1^2}\varkappa^2.$$

Es lassen sich daher drei von $u$ unabhängige (also von $\omega_1$, $\omega_2$ abhängige) Grössen $e_1, e_2, e_3$ so bestimmen, dass

$$(3)\qquad \frac{\sigma_{10}^2(u)}{\sigma^2(u)} + e_1 = \frac{\sigma_{00}^2(u)}{\sigma^2(u)} + e_2 = \frac{\sigma_{01}^2(u)}{\sigma^2(u)} + e_3 = \wp(u),$$

worin $\wp(u)$ eine durch (3) neu definirte, doppelt periodische Function ist. Die Grössen $e_1$, $e_2$, $e_3$ können irgend welche sein, wenn sie nur den Bedingungen

$$e_1 - e_3 = \frac{4K^2}{\omega_1^2}, \quad e_2 - e_3 = \frac{4K^2}{\omega_1^2}\varkappa^2 \tag{4}$$

genügen. Es steht uns also frei, zur völligen Bestimmung derselben noch die Bedingung

$$e_1 + e_2 + e_3 = 0 \tag{5}$$

hinzuzufügen. Dann ergeben sich für $e_1$, $e_2$, $e_3$ folgende Ausdrücke:

$$\begin{aligned} e_1 &= \frac{4K^2}{\omega_1^2}\,\frac{1+\varkappa'^2}{3} \\ e_2 &= -\frac{4K^2}{\omega_1^2}\,\frac{\varkappa'^2-\varkappa^2}{3} \\ e_3 &= -\frac{4K^2}{\omega_1^2}\,\frac{1+\varkappa^2}{3}. \end{aligned} \tag{6}$$

Die Function $\wp(u)$, welche die Perioden $\omega_1$, $\omega_2$ besitzt, wird hiernach durch (1) ausgedrückt:

$$\wp(u) = \frac{4K^2}{\omega_1^2}\left(\frac{1}{\operatorname{sn}^2 v} - \frac{1+\varkappa^2}{3}\right). \tag{7}$$

Die Function $\wp(u)$ hat die gewünschte Eigenschaft der Unveränderlichkeit bei linearen Transformationen, wie man aus dem Ausdruck

$$\wp(u) = \frac{1}{3}\,\frac{\sigma_{00}^2(u) + \sigma_{01}^2(u) + \sigma_{10}^2(u)}{\sigma^2(u)} \tag{8}$$

erkennt.

In Folge von (3) vertauschen sich die $e_1$, $e_2$, $e_3$ bei einer linearen Transformation in derselben Weise wie die $\sigma_{10}$, $\sigma_{01}$, $\sigma_{00}$; eine symmetrische Function derselben ist daher bei einer linearen Transformation ungeändert und wird eine Invariante genannt. Es giebt deren zwei fundamentale, die wir mit $g_2$, $g_3$ bezeichnen:

$$\begin{aligned} g_2 &= -4(e_2 e_3 + e_3 e_1 + e_1 e_2) = 2(e_1^2 + e_2^2 + e_3^2) \\ &= \frac{64}{3}\,\frac{K^4}{\omega_1^4}\,(1 - \varkappa^2\varkappa'^2), \end{aligned} \tag{9}$$

$$g_3 = 4 e_1 e_2 e_3 = \frac{2^8}{27}\,\frac{K^6}{\omega_1^6}\,(2 + \varkappa^2\varkappa'^2)(\varkappa'^2 - \varkappa^2), \tag{10}$$

und wir fügen noch die unter dem Namen der Discriminante bekannte Function bei:

$$(11)\qquad G = (e_2 - e_3)^2 (e_3 - e_1)^2 (e_1 - e_2)^2 = \frac{1}{16} (g_2^3 - 27\, g_2^2)$$
$$= \frac{(2K)^{12}}{\omega_1^{12}} \varkappa^4 \varkappa'^4,$$

wofür nach §. 37, (3), (15) und §. 29, (2) auch gesetzt werden kann:

$$(12)\qquad G = \frac{2^8 \pi^{12} \eta(\omega)^{24}}{\omega_1^{12}}.$$

$\wp(u)$, $g_2$, $g_3$, $G$ sind homogene Functionen, wie folgende Relationen zeigen, worin $\lambda$ ein willkürlicher Factor ist.

$$(13)\qquad \begin{aligned} \wp(\lambda u, \lambda \omega_1, \lambda \omega_2) &= \lambda^{-2} \wp(u, \omega_1, \omega_2) \\ g_2(\lambda \omega_1, \lambda \omega_2) &= \lambda^{-4} g_2(\omega_1, \omega_2) \\ g_3(\lambda \omega_1, \lambda \omega_2) &= \lambda^{-6} g_3(\omega_1, \omega_2) \\ G(\lambda \omega_1, \lambda \omega_2) &= \lambda^{-12} G(\omega_1, \omega_2). \end{aligned}$$

Setzen wir, wie in §. 40, (2)

$$\omega_1 = 2K, \qquad \omega_2 = 2iK',$$

so wird

$$(14)\qquad \begin{gathered} e_1 = \frac{1 + \varkappa'^2}{3}, \quad e_2 = -\frac{\varkappa'^2 - \varkappa^2}{3}, \quad e_3 = -\frac{1 + \varkappa^2}{3} \\ g_2 = \frac{4}{3}(1 - \varkappa^2 \varkappa'^2), \quad g_3 = \frac{4}{27}(\varkappa'^2 - \varkappa^2)(2 + \varkappa^2 \varkappa'^2), \\ G = \varkappa^4 \varkappa'^4. \end{gathered}$$

Wenn wir $\omega_1$ aus den allgemeinen Ausdrücken (9), (10), (11) für $g_2, g_3, G$ eliminiren, so erhalten wir homogene Functionen nullter Ordnung, also Functionen von $\omega$ allein, welche bei linearen Transformationen ungeändert bleiben. Solche Functionen sind $g_2^3 : G$, $g_3^2 : G$. Wir heben unter diesen Functionen, die sich alle auf einander zurückführen lassen, eine hervor, die wir mit $j(\omega)$ bezeichnen und schlechtweg die Invariante nennen und so definiren:

$$(15)\qquad j(\omega) = 2^8 \frac{(1 - \varkappa^2 \varkappa'^2)^3}{\varkappa^4 \varkappa'^4},$$

so dass wir erhalten:

$$(16)\qquad \begin{gathered} \frac{4 \,.\, 27\, g_2^3}{G} = j(\omega) \\ \frac{4 \,.\, 27 \,.\, 27\, g_3^2}{G} = j(\omega) - 27 \,.\, 64 = \frac{64 \,.\, (2 + \varkappa^2 \varkappa'^2)^2 (\varkappa'^2 - \varkappa^2)^2}{\varkappa^4 \varkappa'^4}. \end{gathered}$$

Als Function von $\varkappa^2$ betrachtet, hat die Function $j(\omega)$ die Eigenschaft, ungeändert zu bleiben, wenn $\varkappa^2$ durch einen der sechs Werthe

$$\varkappa^2, \quad \varkappa'^2, \quad \frac{1}{\varkappa^2}, \quad \frac{1}{\varkappa'^2}, \quad -\frac{\varkappa^2}{\varkappa'^2}, \quad -\frac{\varkappa'^2}{\varkappa^2}$$

ersetzt wird.

Wenn wir nach (7) den Differentialquotienten der Function $\wp(u)$ bilden, so erhalten wir

$$(17) \quad \wp'(u) = -\frac{16\,K^3}{\omega_1^3}\frac{\operatorname{cn} v \operatorname{dn} v}{\operatorname{sn}^3 v} = -2\,\frac{\sigma_{00}(u)\,\sigma_{10}(u)\,\sigma_{01}(u)}{\sigma(u)^3}$$

und daraus nach (3):

$$(18) \quad \begin{aligned} \wp'(u)^2 &= 4(\wp(u)-e_1)(\wp(u)-e_2)(\wp(u)-e_3) \\ &= 4\wp(u)^3 - g_2\,\wp(u) - g_3, \end{aligned}$$

oder endlich:

$$(19) \quad du = \frac{d\wp}{\sqrt{4\wp^3 - g_2\wp - g_3}},$$

woraus man ersieht, dass die Function $\wp(u)$ in derselben Beziehung zur Weierstrass'schen Normalform des elliptischen Differentials steht, wie die Function $\operatorname{sn} v$ zu der Legendre'schen.

## §. 42. Die elliptischen Transcendenten zweiter Gattung.

Jacobi hat als Transcendente zweiter Gattung die Function

$$(1) \quad Z(v) = \frac{\Theta'(v)}{\Theta(v)} = \frac{d\log\Theta(v)}{dv}$$

eingeführt. Die Beziehung dieser Function zu den elliptischen Integralen zweiter Gattung ergiebt sich aus der Formel (16) des §. 20, wobei gleich bemerkt sei, dass ganz ähnliche Betrachtungen an die dortigen Formeln (15), (17), (18) anzuknüpfen wären, die aber nicht zu wesentlich neuen Resultaten führen.

Setzen wir dort $v:2K$ an Stelle von $v$, so ergiebt sich aus §§. 37 und 38:

$$(2) \quad \begin{aligned} \frac{d^2\log\Theta(v)}{dv^2} &= \frac{1}{4K^2}\frac{\vartheta''_{01}}{\vartheta_{01}} - \varkappa^2\operatorname{sn}^2 v \\ &= \frac{1}{4K^2}\frac{\vartheta''_{01}}{\vartheta_{01}} - 1 + \operatorname{dn}^2 v. \end{aligned}$$

Wir setzen

$$(3) \quad 1 - \frac{\vartheta''_{01}}{4K^2\vartheta_{01}} = \frac{E}{K},$$

und erhalten durch Integration von (2)

$$\frac{d \log \Theta(v)}{d v} = Z(v) = -\frac{E}{K} v + \int_0^v \mathrm{dn}^2 v \, d v,$$

oder indem wir

$$(4) \qquad E(v) = \int_0^v \mathrm{dn}^2 v \, d v$$

setzen:

$$(5) \qquad Z(v) = E(v) - \frac{E}{K} v.$$

Die Functionen $\Theta(v)$ und $\Theta(v+K)$ sind gerade Functionen und daher ist $\Theta'(0)$ und $\Theta'(K) = 0$. Wenn wir also in (5) $v = K$ setzen, so folgt:

$$(6) \qquad E = \int_0^K \mathrm{dn}^2 v \, d v.$$

Führt man noch für $d v$ das Differential

$$\frac{1}{2} \frac{d \zeta}{\sqrt{\zeta(1-\zeta)(1-\varkappa^2 \zeta)}}$$

ein, [§. 37, (8)], so erhält man für $E(v)$ ein elliptisches Integral zweiter Gattung (§. 8):

$$(7) \qquad E(v) = \frac{1}{2} \int_0^\zeta \frac{d \zeta (1-\varkappa^2 \zeta)}{\sqrt{\zeta(1-\zeta)(1-\varkappa^2 \zeta)}},$$

$$(8) \qquad E = \frac{1}{2} \int_0^1 \frac{d \zeta (1-\varkappa^2 \zeta)}{\sqrt{\zeta(1-\zeta)(1-\varkappa^2 \zeta)}},$$

wo letzteres in demselben Sinne zu nehmen ist, wie §. 37, (17).

$E(v)$ und $Z(v)$ sind ungerade Functionen des Arguments.

Aus dem Additionstheorem der $\Theta$-Function [§. 38, (11)] ergiebt sich durch logarithmische Differentiation:

$$(9) \quad Z(u+v) + Z(u-v) = 2 Z(u) - \frac{2 \varkappa^2 \, \mathrm{sn}^2 v \, \mathrm{sn}\, u \, \mathrm{cn}\, u \, \mathrm{dn}\, u}{1 - \varkappa^2 \, \mathrm{sn}^2 u \, \mathrm{sn}^2 v},$$

$$(10) \quad Z(u+v) - Z(u-v) = 2 Z(v) - \frac{2 \varkappa^2 \, \mathrm{sn}^2 u \, \mathrm{sn}\, v \, \mathrm{cn}\, v \, \mathrm{dn}\, v}{1 - \varkappa^2 \, \mathrm{sn}^2 u \, \mathrm{sn}^2 v}.$$

Hierin kann $Z$ auch durch $E$ ersetzt werden und durch Addition ergiebt sich [§. 39, (16)]:

$$(11) \quad E(u) + E(v) - E(u+v) = \varkappa^2 \, \mathrm{sn}\, u \, \mathrm{sn}\, v \, \mathrm{sn}(u+v).$$

Hieraus erhält man die Periodeneigenschaften der Function $E(u)$, wenn man $v = \pm K,\ K + iK'$ setzt. Man kommt aber auch auf folgendem Wege dazu.

Aus der ersten Gleichung §. 38, (3) folgt:

$$\frac{d \log H(v)}{dv} = Z(v + iK') + \frac{i\pi}{2K}, \tag{12}$$

und demnach aus §. 38, (6) und §. 37, (11):

$$\begin{aligned} Z(v + iK') &= Z(v) + \frac{\operatorname{cn} v \operatorname{dn} v}{\operatorname{sn} v} - \frac{i\pi}{2K} \\ Z(v + K) &= Z(v) - \frac{\varkappa^2 \operatorname{sn} v \operatorname{cn} v}{\operatorname{dn} v}. \end{aligned} \tag{13}$$

Durch zweimalige Anwendung derselben Formeln [mit Rücksicht auf §. 39, (18), (20)]:

$$\begin{aligned} Z(v + 2iK') &= Z(v) - \frac{i\pi}{K} \\ Z(v + 2K) &= Z(v). \end{aligned} \tag{14}$$

Ueberträgt man diese Gleichungen auf die Function $E(v)$, so folgt:

$$\begin{aligned} E(v + iK') &= E(v) + \frac{\operatorname{cn} v \operatorname{dn} v}{\cancel{\operatorname{cn} v}} + \frac{iEK'}{K} - \frac{i\pi}{2K} \\ E(v + K) &= E(v) + E - \frac{\varkappa^2 \operatorname{sn} v \operatorname{cn} v}{\operatorname{dn} v}. \end{aligned} \tag{15}$$

sn

$$\begin{aligned} E(v + 2iK') &= E(v) + \frac{2iEK'}{K} - \frac{i\pi}{K} \\ E(v + 2K) &= E(v) + 2E. \end{aligned} \tag{16}$$

Wenn wir in (15) $v = K$ setzen und eine Grösse $E'$ durch die Gleichung definiren:

$$E(K + iK') = E + i(K' - E'), \tag{17}$$

so erhält man die unter dem Namen der Legendre'schen Relation bekannte Formel

$$EK' + KE' - KK' = \frac{\pi}{2}. \tag{18}$$

Die wahre Bedeutung der hier eingeführten Grösse $E'$ erkennt man, wenn man die Legendre'sche Relation auf einem zweiten Wege ableitet, mit Benutzung einer der linearen Transformationen.

Es ergiebt sich, wenn man wie in §. 40 verfährt und in §. 26, (11) setzt:

$$u = \frac{v}{2K}, \qquad \omega = \frac{iK'}{K}, \qquad \frac{u}{\omega} = \frac{v}{2iK'},$$

$$(19) \qquad \sqrt{K}\, e^{-\frac{\pi v^2}{4KK'}}\, \Theta(iv, \varkappa') = \sqrt{K'}\, H(v + K),$$

und daraus durch logarithmische Differentiation

$$(20) \qquad i Z(iv, \varkappa') = \frac{\pi v}{2KK'} + \frac{H'(v + K)}{H(v + K)}$$

oder nach §. 38, (6)

$$(21) \qquad i Z(iv, \varkappa') = \frac{\pi v}{2KK'} + Z(v) + \frac{d \log \operatorname{cn} v}{dv}.$$

Es ist aber nach (4), (5)

$$i \frac{dZ(iv, \varkappa')}{dv} = - \operatorname{dn}^2(iv, \varkappa') + \frac{E'}{K'},$$

wenn jetzt $E'$ die Bedeutung hat:

$$(22) \qquad E' = \int_v^{K'} \operatorname{dn}^2(v, \varkappa')\, dv,$$

also aus $E$ durch Vertauschung von $\varkappa$ mit $\varkappa'$ hervorgeht. Setzt man also in (21) $v = 0$, nachdem man zuvor differentiirt hat, so ergiebt sich wiederum die Relation (18), woraus folgt, dass $E'$ beide Male dieselbe Grösse ist.

## §. 43. Die elliptische Transcendente dritter Gattung.

Wenn wir die Formel (10) des vorigen Paragraphen:

$$\frac{\Theta'(u + v)}{\Theta(u + v)} - \frac{\Theta'(u - v)}{\Theta(u - v)} = 2 Z(v) - \frac{2 \varkappa^2 \operatorname{sn}^2 u \operatorname{sn} v \operatorname{cn} v \operatorname{dn} v}{1 - \varkappa^2 \operatorname{sn}^2 u \operatorname{sn}^2 v}$$

in Bezug auf $u$ integriren, so folgt:

$$(1) \quad \frac{1}{2} \log \frac{\Theta(u - v)}{\Theta(u + v)} + u Z(v) = \int_0^u \frac{\varkappa^2 \operatorname{sn}^2 u \operatorname{sn} v \operatorname{cn} v \operatorname{dn} v}{1 - \varkappa^2 \operatorname{sn}^2 u \operatorname{sn}^2 v}\, du,$$

und wir können noch die auf gleiche Weise [aus §. 38, (11)] herzuleitende Formel:

$$(2) \qquad \frac{1}{2} \log \frac{H(v - u)}{H(v + u)} + u Z(v) = \int_0^u \frac{\operatorname{sn} v \operatorname{cn} v \operatorname{dn} v\, du}{\operatorname{sn}^2 u - \operatorname{sn}^2 v}$$

hinzufügen, die übrigens auch aus (1) abgeleitet werden kann. Wir setzen nun mit Jacobi

$$(3)\qquad \Pi(u,v) = \int\limits_0^u \frac{\varkappa^2 \operatorname{sn}^2 u \operatorname{sn} v \operatorname{cn} v \operatorname{dn} v}{1 - \varkappa^2 \operatorname{sn}^2 u \operatorname{sn}^2 v}\, du,$$

und nennen $\Pi(u, v)$ die Transcendente dritter Gattung mit dem Argument $u$ und dem Parameter $v$. Ersetzt man $du$ durch den Ausdruck:

$$\frac{d\zeta}{2\sqrt{\zeta(1-\zeta)(1-\varkappa^2\zeta)}}$$

und $\operatorname{sn}^2 u$ durch $\zeta$, so ergiebt sowohl (1) als (2) ein elliptisches Integral dritter Gattung, wie wir es in §. 8 kennen gelernt haben.

Aus (1) folgt zunächst

$$(4)\qquad \Pi(u, v) - u Z(v) = \Pi(v, u) - v Z(u),$$

oder der Jacobi'sche Satz über die Vertauschung von Argument und Parameter.

Die Function $\Pi(u, v)$ verschwindet, wenn $v = K$ oder $v = K + iK'$ ist. Setzen wir daher diese Werthe für $u$ in (4) ein, so folgt

$$(5)\qquad \begin{aligned} \Pi(K, v) &= K Z(v) \\ \Pi(K + iK', v) &= (K + iK') Z(v) + \frac{i\pi v}{2K} \text{ [§. 42, (13)],} \end{aligned}$$

wodurch die vollständigen Integrale dritter Gattung auf die zweite Gattung zurückgeführt sind.

Wir wollen noch das Additionstheorem der $\Pi$-Function ableiten, welches Jacobi in den Fund. nova art. 53—55 [1]) in verschiedenen Formen giebt, die nur mühsam auf einander zurückführbar sind. Zunächst erhalten wir aus der Definition (1), wenn wir den Parameter jetzt mit $a$ bezeichnen:

$$(6)\qquad \begin{aligned} &\Pi(u + v, a) - \Pi(u, a) - \Pi(v, a) \\ &= \frac{1}{2} \log \frac{\Theta(u + v - a)}{\Theta(u + v + a)} \frac{\Theta(u + a)\,\Theta(v + a)}{\Theta(u - a)\,\Theta(v - a)}, \end{aligned}$$

und es handelt sich noch darum, den unter dem Logarithmus stehenden Ausdruck durch elliptische Functionen darzustellen.

Dies geschieht zunächst leicht, wie an der erwähnten Stelle der Fundamenta, mittelst der Formel [§. 38, (11)]:

$$\Theta^2(0)\,\Theta(u + v)\,\Theta(u - v) = \Theta^2(u)\,\Theta^2(v)\,[1 - \varkappa^2 \operatorname{sn}^2 u \operatorname{sn}^2 v],$$

wenn man in derselben für $u$, $v$ setzt $u \pm a$, $v \pm a$, dann $\pm a$, $u + v \pm a$. Man erhält so:

---

[1]) C. G. J. Jacobi's gesammelte Werke, Berlin 1881, Bd. I, S. 204.

$$\Theta^2(0)\,\Theta(u+v\pm 2a)\,\Theta(u-v)$$
$$= \Theta^2(u\pm a)\,\Theta^2(v\pm a)\,[1-\varkappa^2\,\mathrm{sn}^2(u\pm a)\,\mathrm{sn}^2(v\pm a)]$$
$$\Theta^2(0)\,\Theta(u+v\pm 2a)\,\Theta(u+v)$$
$$= \Theta^2(a)\,\Theta^2(u+v\pm a)\,[1-\varkappa^2\,\mathrm{sn}^2 a\,\mathrm{sn}^2(u+v\pm a)],$$

woraus folgt:

$$(7)\qquad \frac{\Theta(u+v-a)\,\Theta(u+a)\,\Theta(v+a)}{\Theta(u+v+a)\,\Theta(u-a)\,\Theta(v-a)}$$
$$= \sqrt{\frac{[1-\varkappa^2\,\mathrm{sn}^2(u-a)\,\mathrm{sn}^2(v-a)]\,[1-\varkappa^2\,\mathrm{sn}^2 a\,\mathrm{sn}^2(u+v+a)]}{[1-\varkappa^2\,\mathrm{sn}^2(u+a)\,\mathrm{sn}^2(v+a)]\,[1-\varkappa^2\,\mathrm{sn}^2 a\,\mathrm{sn}^2(u+v-a)]}}.$$

Einen zweiten Ausdruck erhält man aus der Additionsformel (13), §. 19, welche man so darstellen kann:

$$\Theta(0)\,\Theta(u\pm a)\,\Theta(v\pm a)\,\Theta(u+v)$$
$$= \Theta(u)\Theta(v)\Theta(a)\Theta(u+v\pm a)\;[1\pm\varkappa^2\,\mathrm{sn}\,a\,\mathrm{sn}\,u\,\mathrm{sn}\,v\,\mathrm{sn}\,(u+v\pm a)],$$

woraus durch Division:

$$(8)\quad \frac{\Theta(u+v-a)\Theta(u+a)\Theta(v+a)}{\Theta(u+v+a)\Theta(u-a)\Theta(v-a)} = \frac{1+\varkappa^2\,\mathrm{sn}a\,\mathrm{sn}u\,\mathrm{sn}v\,\mathrm{sn}(u+v+a)}{1-\varkappa^2\,\mathrm{sn}a\,\mathrm{sn}u\,\mathrm{sn}v\,\mathrm{sn}(u+v-a)}.$$

## §. 44. Die Transcendenten zweiter und dritter Gattung von Weierstrass.

Es sind nun noch die Transcendenten zweiter und dritter Gattung in der Weierstrass'schen Form aufzustellen. Zu der ersteren gelangen wir ähnlich wie in §. 42 durch zweimalige Differentiation von *log* $\sigma(u)$. Es ergiebt sich so aus

$$(1)\qquad \sigma(u) = \omega_1\, e^{\frac{\eta_1 u^2}{\omega_1}}\,\frac{\vartheta_{11}\left(\frac{u}{\omega_1}\right)}{\vartheta'_{11}}\qquad [\text{§. 32, (4)}],$$

$$\frac{d^2 \log \sigma(u)}{d u^2} = \frac{2\,\eta_1}{\omega_1} + \frac{d^2 \log \vartheta_{11}\left(\frac{u}{\omega_1}\right)}{d u^2},$$

$$= \frac{2\,\eta_1}{\omega_1} + \frac{1}{\omega_1^2}\,\frac{\vartheta''_{00}}{\vartheta_{00}} - \frac{1}{\omega_1^2}\,\frac{\vartheta'^2_{11}}{\vartheta^2_{00}}\,\frac{\vartheta^2_{00}\left(\frac{u}{\omega_1}\right)}{\vartheta^2_{11}\left(\frac{u}{\omega_1}\right)}\qquad [\text{§. 20, (18)}]$$

und also nach §. 37 und §. 41:

$$\frac{d^2 \log \sigma(u)}{d u^2} = A - \wp(u),$$

worin $A$ eine Constante ist. Diese findet man aber, wenn man die Gleichung nach §. 41 (8) so schreibt:

$$\sigma''(u)\sigma(u) - \sigma'(u)\sigma'(u) = A\sigma(u)\sigma(u) - \frac{1}{3}[\sigma_{00}^2(u) + \sigma_{01}^2(u) + \sigma_{10}^2(u)].$$

Wenn man hierin zweimal differentiirt und dann $u = 0$ setzt, so ergiebt sich $A = 0$ [§. 30 (16), §. 32 (6), (7)], so dass wir erhalten:

$$(2) \qquad \frac{d^2 \log \sigma(u)}{du^2} = -\wp(u),$$

eine Formel, welche bei Weierstrass zur Definition der $\wp$-Function dient.

Wird also

$$(3) \qquad \frac{\sigma'(u)}{\sigma(u)} = \zeta(u)$$

gesetzt, so ist $\zeta(u)$ ein elliptisches Integral zweiter Gattung:

$$(4) \quad \zeta(u) = -\int \wp(u)\,du = -\int \frac{\wp\, d\wp}{\sqrt{4\wp^3 - g_2\wp - g_3}} \quad [\text{§. 41 (19)}],$$

worin die additive Constante dadurch bestimmt ist, dass $\zeta(u)$ eine ungerade Function sein muss. Die Periodicität der $\zeta$-Function ergiebt sich aus den Periodengleichungen der $\sigma$-Function [§. 30, (19)]:

$$(5) \qquad \begin{aligned} \zeta(u + \omega_1) - \zeta(u) &= 2\eta_1 \\ \zeta(u + \omega_2) - \zeta(u) &= 2\eta_2, \end{aligned}$$

so dass $2\eta_1$ und $2\eta_2$ als vollständige Integrale zweiter Gattung (analog den $E$, $E'$) dargestellt sind:

$$(6) \qquad 2\eta_1 = -\int_u^{u+\omega_1} \wp(u)\,du, \quad 2\eta_2 = -\int_u^{u+\omega_2} \wp(u)\,du$$

mit der der Legendre'schen Relation entsprechenden Gleichung

$$(7) \qquad \eta_1\omega_2 - \eta_2\omega_1 = \pi i.$$

Um die Additionstheoreme für die Weierstrass'schen Transcendenten zu bilden, gehen wir von der $\sigma$-Function aus. Für diese erhalten wir aus (1) mit Benutzung der Additionsformel für $\vartheta_{11}$, §. 19 (4):

$$(8) \qquad \frac{\sigma(u+v)\,\sigma(u-v)}{\sigma(u)^2\,\sigma(v)^2} = \wp(v) - \wp(u),$$

daraus durch logarithmische Differentiation:

$$
(9)\quad
\begin{aligned}
\zeta(u+v)+\zeta(u-v)-2\zeta(u) &= \frac{\wp'(u)}{\wp(u)-\wp(v)}\\
\zeta(u+v)-\zeta(u-v)-2\zeta(v) &= \frac{-\wp'(v)}{\wp(u)-\wp(v)}
\end{aligned}
$$

$$
(10)\quad \zeta(u+v)=\zeta(u)+\zeta(v)+\frac{1}{2}\frac{\wp'(u)-\wp'(v)}{\wp(u)-\wp(v)}.
$$

Hieraus leitet man durch abermalige Differentation das Additionstheorem für die $\wp$-Function her. Man erhält aus (9) durch Differentiation nach $u$ und $v$:

$$
\wp(u+v)+\wp(u-v)-2\wp(u)=-\frac{\wp''(u)}{\wp(u)-\wp(v)}+\frac{\wp'(u)^2}{[\wp(u)-\wp(v)]^2}
$$

$$
2\wp(u+v)-2\wp(u-v)=-\frac{2\wp'(u)\wp'(v)}{[\wp(u)-\wp(v)]^2}
$$

$$
\wp(u+v)+\wp(u-v)-2\wp(v)=\frac{\wp''(v)}{\wp(u)-\wp(v)}+\frac{\wp'(v)^2}{[\wp(u)-\wp(v)]^2}
$$

und indem man addirt:

$$
4\wp(u+v)-2\wp(u)-2\wp(v)=\left(\frac{\wp'(u)-\wp'(v)}{\wp(u)-\wp(v)}\right)^2-\frac{\wp''(u)-\wp''(v)}{\wp(u)-\wp(v)}.
$$

Es ist aber

$$
\begin{aligned}
\wp'(u)^2 &= 4\wp(u)^3-g_2\wp(u)-g_3\\
\wp''(u) &= 6\wp(u)^2-\frac{1}{2}g_2\\
\wp''(u)-\wp''(v) &= 6[\wp^2(u)-\wp^2(v)],
\end{aligned}
$$

so dass man erhält:

$$
(11)\quad \wp(u+v)+\wp(u)+\wp(v)=\frac{1}{4}\left(\frac{\wp'(u)-\wp'(v)}{\wp(u)-\wp(v)}\right)^2,
$$

was mit der Formel (21), §. 9 übereinstimmt.

Endlich erhält man noch durch Integration der zweiten Gleichung (9) in Bezug auf $u$:

$$
(12)\quad \frac{1}{2}\log\frac{\sigma(v-u)}{\sigma(v+u)}+u\,\zeta(v)=\frac{1}{2}\int_0^u\frac{\wp'(v)\,du}{\wp(u)-\wp(v)},
$$

wodurch ein Integral dritter Gattung vom Argument $u$ und dem Parameter $v$ durch die $\sigma$-Function ausgedrückt ist.

Eine andere Form des Integrals dritter Gattung erhält man durch Integration von (10):

$$
(13)\quad \log\frac{\sigma(u+v)}{\sigma(u)\sigma(v)}-u\,\zeta(v)=\frac{1}{2}\int\frac{\wp'(u)-\wp'(v)}{\wp(u)-\wp(v)}\,du.
$$

## §. 45. Entwickelungen der elliptischen Functionen.

Um für den Gebrauch unserer Darstellung keine wesentliche Lücke zu lassen, sollen hier noch die Entwickelungen der elliptischen Functionen abgeleitet und zusammengestellt werden. Diese Entwickelungen sind zweierlei Art, von denen die erste, die Partialbruchentwickelung, eine allgemein gültige Darstellung der elliptischen Functionen liefert, während die zweite Art, die Entwickelung in trigonometrische Reihen, nur einen beschränkten Gültigkeitsbereich hat.

Zur Ableitung der ersteren wählen wir den functionentheoretischen Weg, der wohl am einfachsten zum Ziele führt.

Die Functionen $\operatorname{sn} v$, $\operatorname{cn} v$, $\operatorname{dn} v$ werden, wenn wir zur Abkürzung

$$z = e^{\frac{\pi i}{2K} v}$$

setzen, nur unendlich für die Werthe:

$$v = 2 h_1 K + (2h - 1) i K',$$

oder

$$z = \pm q^{\frac{2h-1}{2}},$$

worin $h$ und $h_1$ beliebige ganze Zahlen sind.

Wir machen daher für die drei Functionen $\operatorname{sn} v$, $\operatorname{cn} v$, $\operatorname{dn} v$ den Ansatz:

$$C + \sum^h \frac{A_h}{z - q^{\frac{2h-1}{2}}} + \sum^h \frac{B_h}{z + q^{\frac{2h-1}{2}}}$$
$$+ \sum^h \frac{A'_h}{z^{-1} - q^{\frac{2h-1}{2}}} + \sum^h \frac{B'_h}{z^{-1} + q^{\frac{2h-1}{2}}},$$

worin die Summen sich auf alle positiven Werthe von $h$ erstrecken und die $C, A_h, B_h, A'_h, B'_h$ noch zu bestimmende Coëfficienten sind.

Lassen wir $v$ in $-v$ übergehen, so folgt, dass für die Function $\operatorname{sn} v$, $A_h = -A'_h$, $B_h = -B'_h$, $C = 0$, für $\operatorname{cn} v$, $\operatorname{dn} v$ dagegen $A_h = A'_h$, $B_h = B'_h$ sein muss. Aendern wir $v$ um $2K$, so geht $z$ in $-z$ über; dabei ändern $\operatorname{sn} v$, $\operatorname{cn} v$ das Vorzeichen, $\operatorname{dn} v$ bleibt ungeändert. Also ist für $\operatorname{sn} v$, $\operatorname{cn} v$ $A_h = B_h$, $C = 0$ für $\operatorname{dn} v$ $A_h = -B_h$; um nun $A_h$ zu bestimmen, setzen wir

$$v = (2h - 1) i K' + u$$

und lassen $u$ in Null übergehen. Nach §. 39, (20) ist:

$$\operatorname{sn} v = \frac{1}{\varkappa \operatorname{sn} u}, \quad \operatorname{cn} v = \frac{(-1)^h i}{\varkappa}\,\frac{\operatorname{dn} u}{\operatorname{sn} u}, \quad \operatorname{dn} v = \frac{(-1)^h i \operatorname{cn} u}{\operatorname{sn} u},$$

$$z - q^{\frac{2h-1}{2}} = q^{\frac{2h-1}{2}}\left(e^{\frac{\pi i u}{2K}} - 1\right).$$

Es ergiebt sich also durch Multiplication mit $z - q^{\frac{2h-1}{2}}$ und Uebergang zur Grenze $u = 0$ für die drei Functionen der Werth:

$$A_h = \frac{\pi i}{2\varkappa K}\, q^{\frac{2h-1}{2}}, \quad -\frac{(-1)^h \pi}{2\varkappa K}\, q^{\frac{2h-1}{2}}, \quad -\frac{(-1)^h \pi}{2K}\, q^{\frac{2h-1}{2}}.$$

Vereinigt man je zwei oder je vier Glieder der obigen Reihen, setzt die gefundenen Werthe von $A_h$ ein, und bestimmt für $\operatorname{dn} v$ den Werth der Constanten $C$ aus der Annahme $v = K + iK'$, so erhält man folgende Darstellungen, worin zur Abkürzung $v = 2Ku$ gesetzt ist:

$$(1)\quad \frac{\varkappa K}{\pi} \operatorname{sn} 2Ku = -i \sum_{1,\infty}^{h} \left( \frac{q^{\frac{2h-1}{2}}\, e^{\pi i u}}{1 - q^{2h-1}\, e^{2\pi i u}} - \frac{q^{\frac{2h-1}{2}}\, e^{-\pi i u}}{1 - q^{2h-1}\, e^{-2\pi i u}} \right)$$

$$= 2 \sin \pi u \sum_{1,\infty}^{h} \frac{q^{\frac{2h-1}{2}}\,(1 + q^{2h-1})}{1 - 2q^{2h-1} \cos 2\pi u + q^{4h-2}},$$

$$(2)\quad \frac{\varkappa K}{\pi} \operatorname{cn} 2Ku = -\sum_{1,\infty}^{h} (-1)^h \left( \frac{q^{\frac{2h-1}{2}}\, e^{\pi i u}}{1 - q^{2h-1}\, e^{2\pi i u}} + \frac{q^{\frac{2h-1}{2}}\, e^{-\pi i u}}{1 - q^{2h-1}\, e^{-2\pi i u}} \right)$$

$$= -2 \cos \pi u \sum_{1,\infty}^{h} (-1)^h \frac{q^{\frac{2h-1}{2}}\,(1 - q^{2h-1})}{1 - 2q^{2h-1} \cos 2\pi u + q^{4h-2}},$$

$$(3)\quad \frac{K}{\pi} \operatorname{dn} 2Ku = \frac{1}{2} - \sum_{1,\infty}^{h} (-1)^h \left( \frac{q^{2h-1}\, e^{2\pi i u}}{1 - q^{2h-1}\, e^{2\pi i u}} + \frac{q^{2h-1}\, e^{-2\pi i u}}{1 - q^{2h-1}\, e^{-2\pi i u}} \right)$$

$$= \frac{1}{2} - 2 \sum_{1,\infty}^{h} (-1)^h \frac{(q^{2h-1} \cos 2\pi u - q^{4h-2})}{1 - 2q^{2h-1} \cos 2\pi u + q^{4h-2}}.$$

Dass die Summen auf der rechten Seite die Functionen, denen sie gleich gesetzt sind, wirklich darstellen, ist eine Folge der Convergenz der Reihen für alle Werthe von $u$. Die Differenz zwischen der rechten und linken Seite ist eine Function von $u$, welche für keinen Werth der Variablen unendlich wird und muss folglich eine Constante sein.

Aus diesem System kann man neun andere Entwickelungen (für die Quotienten je zweier der elliptischen Grundfunctionen und die reciproken Werthe) herleiten, indem man $v$ durch $v + K$,

$v + iK'$, $v + K + iK'$ ersetzt. Diese Formeln wollen wir nicht hersetzen, da ihre Ableitung keinerlei Schwierigkeit bietet. Dagegen wollen wir noch die Formeln anführen, die sich aus den vorstehenden für $v = 0$ und $v = K$ ergeben:

$$\begin{aligned}
\frac{\varkappa K^2}{\pi^2} &= \sum_{1,\infty}^{h} \frac{q^{\frac{2h-1}{2}}(1+q^{2h-1})}{(1-q^{2h-1})^2} \\
\frac{\varkappa K}{\pi} &= -2\sum_{1,\infty}^{h}(-1)^h \frac{q^{\frac{2h-1}{2}}}{1-q^{2h-1}} \\
\frac{K}{\pi} &= \frac{1}{2} - 2\sum_{1,\infty}^{h}(-1)^h \frac{q^{2h-1}}{1-q^{2h-1}} \\
\frac{\varkappa' K}{\pi} &= \frac{1}{2} + 2\sum_{1,\infty}^{h}(-1)^h \frac{q^{2h-1}}{1+q^{2h-1}}.
\end{aligned}\tag{4}$$

Um nun die trigonometrischen Reihen für die Functionen $\operatorname{sn} v$, $\operatorname{cn} v$, $\operatorname{dn} v$ zu erhalten, entwickeln wir in den vorstehenden Summen die einzelnen Glieder nach Potenzen von $q$, indem wir setzen:

$$\frac{1}{1-q^{2h-1}e^{\pm 2\pi i u}} = \sum_{0,\infty}^{\lambda} q^{(2h-1)\lambda}\, e^{\pm 2\lambda\pi i u}.\tag{5}$$

Diese Entwickelung ist für jedes $h$ erlaubt, so lange der absolute Werth von $q e^{\pm 2\pi i u}$ ein echter Bruch ist, so lange also der reelle Theil von

$$\frac{K'}{K} \pm 2iu,$$

für beide Zeichen positiv ist, oder so lange der imaginäre Theil von $u$ absolut kleiner ist als der reelle Theil von $\pm K' : 2K$ (sicher also für reelle Werthe von $u$).

Setzt man unter dieser Voraussetzung die Entwickelung (5) in die Formeln (1), (2), (3) ein und führt dann wieder die Summation nach $h$ aus, so folgt, wenn man wieder $h$ an Stelle von $\lambda$ setzt:

$$\begin{aligned}
\frac{\varkappa K}{\pi} \operatorname{sn} 2Ku &= 2\sum_{1,\infty}^{h} \frac{q^{\frac{2h-1}{2}}}{1-q^{2h-1}} \sin(2h-1)\pi u \\
\frac{\varkappa K}{\pi} \operatorname{cn} 2Ku &= 2\sum_{1,\infty}^{h} \frac{q^{\frac{2h-1}{2}}}{1+q^{2h-1}} \cos(2h-1)\pi u \\
\frac{K}{\pi} \operatorname{dn} 2Ku &= \frac{1}{2} + 2\sum_{1,\infty}^{h} \frac{q^h}{1+q^{2h}} \cos 2h\pi u,
\end{aligned}\tag{6}$$

woraus man noch für $u = 0$, $u = \frac{1}{2}$ die Entwickelungen erhält:

$$
(7)\qquad
\begin{aligned}
\frac{\varkappa K}{\pi} &= 2 \sum_{1,\infty}^{h} \frac{q^{\frac{2h-1}{2}}}{1 + q^{2h-1}} \\
\frac{K}{\pi} &= \frac{1}{2} + 2 \sum_{1,\infty}^{h} \frac{q^h}{1 + q^{2h}} \\
\frac{\varkappa' K}{\pi} &= \frac{1}{2} + 2 \sum_{1,\infty}^{h} (-1)^h \frac{q^h}{1 + q^{2n}}.
\end{aligned}
$$

Aehnliche Entwickelungen lassen sich auch für die Transscendenten zweiter und dritter Gattung geben. So erhält man für die Function $Z$ entweder auf demselben functionentheoretischen Wege oder einfacher noch durch Ausführung der in der Formel

$$
Z(v) = \frac{d \log \Theta(v)}{dv}
$$

angedeuteten Differentiation [§. 21 (2)] die unbedingt gültige Reihe (Partialbruchentwickelung):

$$
(8)\quad \frac{K}{\pi} Z(2Ku) = -i \sum_{1,\infty}^{h} \left( \frac{q^{2h-1} e^{2\pi i u}}{1 - q^{2h-1} e^{2\pi i u}} - \frac{q^{2h-1} e^{-2\pi i u}}{1 - q^{2h-1} e^{-2\pi i u}} \right)
$$

$$
= 2 \sum_{1,\infty}^{h} \frac{q^{2h-1} \sin 2\pi u}{1 - 2 q^{2h-1} \cos 2\pi u + q^{4h-2}},
$$

und daraus eine in demselben Umfange wie oben gültige Reihenentwickelung:

$$
(9)\qquad \frac{K}{\pi} Z(2Ku) = 2 \sum_{1,\infty}^{h} \frac{q^h}{1 - q^{2h}} \sin 2\pi h u.
$$

Differentiiren wir diese Formel noch nach $u$ und setzen dann $u = 0$, so folgt mit Rücksicht auf die Gleichung

$$
Z(v) = E(v) - \frac{E}{K} v, \quad Z'(0) = \frac{K - E}{K}
$$

eine Entwickelung für $E$:

$$
(10)\qquad E = K - \frac{2\pi^2}{K} \sum_{1,\infty}^{h} \frac{h q^h}{1 - q^{2h}}.
$$

Um für die Transcendente dritter Gattung:

$$
\Pi(u, v) = u Z(v) + \frac{1}{2} \log \frac{\Theta(u - v)}{\Theta(u + v)}
$$

eine Reihenentwickelung zu finden, setzen wir für die $\Theta$-Functionen die unendlichen Producte und entwickeln die Logarithmen der einzelnen Factoren:

$$log\,[1 - q^{2h-1}\, e^{\pm 2\pi i(u \mp v)}] = -\sum_{1,\infty}^{\lambda} \frac{1}{\lambda}\, q^{\lambda(2h-1)}\, e^{\pm 2\pi i\lambda(u \mp v)},$$

was jedoch nur erlaubt ist, so lange die imaginären Theile von $u + v$ und $u - v$ innerhalb der oben angegebenen Grenzen liegen. Wir erhalten so:

(11)
$$\Pi(2\,Ku,\ 2\,Kv) =$$
$$2\,Ku\,Z(2\,Kv) - 2\sum_{1,\infty}^{h} \frac{q^h}{h\,(1-q^{2h})} \sin 2\,\pi\,u \sin 2\,\pi\,v.$$

---

## Fünfter Abschnitt.

## Die Modulfunctionen.

### §. 46. Die elliptischen Differentialgleichungen.

Die bisher definirten elliptischen Functionen sind Functionen der beiden Variablen $v$, $\omega$, und von dem Periodenverhältniss $\omega$, welches einen positiv imaginären Bestandtheil haben muss, sind die Moduln $\varkappa$, $\varkappa'$, ferner $j(\omega)$, $K$, $K'$ abhängig. Ebenso ist die Function $\wp(u)$ eine Function der drei Variablen $u$, $\omega_1$, $\omega_2$ und von $\omega_1$, $\omega_2$ sind die Invarianten $g_2$, $g_3$ abhängig. Die Aufgabe der Umkehrung der elliptischen Integrale, wie wir sie in §. 10 formulirt haben, setzt aber voraus, dass in den elliptischen Functionen $\varkappa^2$ (oder bei der Weierstrass'schen Normalform $g_2$, $g_3$) beliebig gegebene Werthe haben, und die vollständige Lösung dieser Aufgabe verlangt also, dass nicht $\omega$, sondern $\varkappa^2$ (resp. $g_2$, $g_3$) als zweite unabhängige Variable auftritt, und dass $\omega$ durch diese ausgedrückt werde. Dieser Aufgabe werden die nächsten Betrachtungen gewidmet sein.

Wir gehen aus von der Aufgabe, ein System von Differentialgleichungen, welches wir das der elliptischen Differentialgleichungen nennen, zu integriren:

$$\frac{dx}{dv} = yz$$

$$(1) \qquad \frac{dy}{dv} = -zx$$

$$\frac{dz}{dv} = -\varkappa^2 xy,$$

unter den Nebenbedingungen:

(2) für $v = 0$ soll $x = 0$, $y = 1$, $z = 1$ sein.

Wir haben im vorigen Abschnitt gesehen, dass, wenn

$$\varkappa^2 = \frac{\vartheta_{10}^4}{\vartheta_{00}^4} \tag{3}$$

ist, diese Aufgabe durch die elliptischen Functionen gelöst wird, und zwar in der Weise, dass $x$, $y$, $z$ in der ganzen $v$-Ebene eindeutige und, ausser wo sie unendlich sind, stetige Functionen von $v$ werden. Ist nun aber $\varkappa^2$ gegeben, so entsteht die Frage, ob es zu jedem Werth von $\varkappa^2$ einen der Bedingung (3) genügenden Werth von $\omega$ giebt und ob es mehrere solche giebt.

Wir beweisen zunächst, dass durch die Differentialgleichungen (1) mit den Nebenbedingungen die Functionen $x, y, z$ eindeutig bestimmt sind.

Es ergiebt sich zunächst aus (1), dass $x^2 + y^2$, $\varkappa^2 x^2 + z^2$ constant sind, und aus den Nebenbedingungen folgt:

$$y^2 = 1 - x^2, \qquad z^2 = 1 - \varkappa^2 x^2. \tag{4}$$

Angenommen, es existire ein zweites System denselben Bedingungen genügender Functionen $x_1$, $y_1$, $z_1$, so ist zunächst

$$y_1^2 = 1 - x_1^2, \qquad z_1^2 = 1 - \varkappa^2 x_1^2$$

und eine einfache Differentiation ergiebt, dass

$$\frac{x y_1 z_1 - x_1 y z}{1 - \varkappa^2 x^2 x_1^2}$$

constant ist. (Das Additionstheorem der elliptischen Integrale, welches die Form dieses Ausdruckes liefert, wird unmittelbar durch Differentiation bestätigt.) Aus den Nebenbedingungen folgt aber, dass diese Constante verschwindet, also:

$$x y_1 z_1 = x_1 y z,$$

woraus man leicht schliesst, indem man beiderseits quadrirt:

$$x = x_1, \quad y = y_1, \quad z = z_1.$$

## §. 47. Die Lösungen der Gleichung $j(\omega) = j(\omega')$.

Dies Resultat genügt zunächst, um die Beziehungen der verschiedenen Werthe von $\omega$ festzustellen, welche zu demselben Werth von $\varkappa^2$ führen. Sei also:

$$(1)\qquad \frac{\vartheta_{10}^4(0,\omega')}{\vartheta_{00}^4(0,\omega')} = \frac{\vartheta_{10}^4(0,\omega)}{\vartheta_{00}^4(0,\omega)} = \varkappa^2,$$

und setzen wir

$$(2)\qquad v = \pi\,\vartheta_{00}^2(0,\omega)\,u = \pi\,\vartheta_{00}^2(0,\omega')\,u',$$

so genügen (nach §. 37) sowohl die Functionen

$$(3)\quad \frac{\vartheta_{00}(0,\omega)\,\vartheta_{11}(u,\omega)}{\vartheta_{10}(0,\omega)\,\vartheta_{01}(u,\omega)},\quad \frac{\vartheta_{01}(0,\omega)\,\vartheta_{10}(u,\omega)}{\vartheta_{10}(0,\omega)\,\vartheta_{01}(u,\omega)},\quad \frac{\vartheta_{01}(0,\omega)\,\vartheta_{00}(u,\omega)}{\vartheta_{00}(0,\omega)\,\vartheta_{01}(u,\omega)},$$

als auch

$$(4)\quad \frac{\vartheta_{00}(0,\omega')\,\vartheta_{11}(u',\omega')}{\vartheta_{10}(0,\omega')\,\vartheta_{01}(u',\omega')},\quad \frac{\vartheta_{01}(0,\omega')\,\vartheta_{10}(u',\omega')}{\vartheta_{10}(0,\omega')\,\vartheta_{01}(u',\omega')},\quad \frac{\vartheta_{01}(0,\omega')\,\vartheta_{00}(u',\omega')}{\vartheta_{00}(0,\omega')\,\vartheta_{01}(u',\omega')},$$

für $x$, $y$, $z$ gesetzt, den Differentialgleichungen (1) des vorigen Paragraphen, und die entsprechenden sind also identisch. Wenn nun $u' = \frac{1}{2}$ ist, so verschwindet $\vartheta_{10}(u', \omega')$ und es muss dann auch $\vartheta_{10}(u, \omega)$ verschwinden. Demnach folgt aus (2) mit Rücksicht auf §. 18:

$$(5)\qquad \vartheta_{00}^2(0,\omega') = \vartheta_{00}^2(0,\omega)\,(\alpha + \beta\,\omega),$$

worin $\alpha$, $\beta$ ganze Zahlen sind, welche der Bedingung

$$(6)\qquad \alpha \equiv 1,\quad \beta \equiv 0 \pmod 2$$

genügen. Ist $u' = \omega' : 2$, so verschwinden $\vartheta_{01}(u', \omega')$ und $\vartheta_{01}(u, \omega)$ und daher ist wie oben

$$(7)\qquad \vartheta_{00}^2(0,\omega')\,\omega' = \vartheta_{00}^2(0,\omega)\,(\gamma + \delta\,\omega),$$

worin

$$(8)\qquad \gamma \equiv 0,\quad \delta \equiv 1 \pmod 2.$$

Daraus folgt:

$$(9)\qquad \omega' = \frac{\gamma + \delta\,\omega}{\alpha + \beta\,\omega}.$$

Da aber in gleicher Weise geschlossen werden kann:

$$\vartheta_{00}^2(0,\omega) = \vartheta_{00}^2(0,\omega')\,(\alpha' + \beta'\,\omega')$$
$$\vartheta_{00}^2(0,\omega)\,\omega = \vartheta_{00}^2(0,\omega')\,(\gamma' + \delta'\,\omega'),$$

worin $\alpha'$, $\beta'$, $\gamma'$, $\delta'$ gleichfalls ganze Zahlen sind, so ergiebt die Substitution (5) in diesen Gleichungen:

$$1 = (\alpha + \beta\,\omega)(\alpha' + \beta'\,\omega')$$
$$\omega = (\alpha + \beta\,\omega)(\gamma' + \delta'\,\omega'),$$

also nach (9):

$$\alpha\alpha' + \gamma\beta' = 1, \quad \beta\alpha' + \delta\beta' = 0,$$
$$\alpha\gamma' + \gamma\delta' = 0, \quad \beta\gamma' + \delta\delta' = 1,$$

und mithin

$$(\alpha\delta - \beta\gamma)(\alpha'\delta' - \beta'\gamma') = 1,$$

und daher, da $\omega$, $\omega'$ beide einen positiven imaginären Theil haben müssen:

$$\alpha\delta - \beta\gamma = 1,$$
$$\alpha = \delta', \quad \delta = \alpha', \quad \gamma = -\gamma', \quad \beta = -\beta'.$$

1. Es hängen also $\omega$, $\omega'$ durch eine lineare Transformation und zwar [nach (6), (8)] durch eine der ersten Classe (§. 31) mit einander zusammen. Dass auch umgekehrt zwei solche Werthe $\omega$, $\omega'$ denselben Werth $\varkappa^2$ ergeben, ist bereits oben nachgewiesen.

Ein ähnlicher Satz ergiebt sich als unmittelbare Consequenz hieraus, für die Invariante $j(\omega)$ (§. 41).

2. Die Gleichung:

$$j(\omega') = j(\omega) \tag{10}$$

ist dann und nur dann befriedigt, wenn $\omega'$ mit $\omega$ durch irgend eine lineare Transformation

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

zusammenhängt.

Denn bezeichnen wir die zu $\omega'$ gehörigen Werthe von $\varkappa^2$, $\varkappa'^2$ mit $\lambda^2$, $\lambda'^2$, so kann die Gleichung (10) so geschrieben werden:

$$\frac{(1 - \lambda^2\lambda'^2)^3}{\lambda^4\lambda'^4} = \frac{(1 - \varkappa^2\varkappa'^2)^3}{\varkappa^4\varkappa'^4},$$

und ist in Bezug auf $\lambda^2$ eine Gleichung sechsten Grades, deren Wurzeln

$$\varkappa^2, \quad \varkappa'^2, \quad \frac{1}{\varkappa^2}, \quad \frac{1}{\varkappa'^2}, \quad -\frac{\varkappa'^2}{\varkappa^2}, \quad -\frac{\varkappa^2}{\varkappa'^2}$$

sind. Es findet daher (mit Rücksicht auf §. 40) eine der folgenden Beziehungen statt:

$$\lambda^2 = \varkappa^2(\omega), \quad \varkappa^2\left(-\frac{1}{\omega}\right), \quad \varkappa^2(\omega + 1), \quad \varkappa^2\left(\frac{1-\omega}{\omega}\right),$$
$$\varkappa^2\left(-\frac{1}{\omega+1}\right), \quad \varkappa^2\left(\frac{\omega}{\omega-1}\right),$$

wonach aus dem ersten Satze die Richtigkeit des zweiten folgt.

## §. 48. Die unabhängige Variable $\varkappa^2$. Lineare Differentialgleichung für $K$.

Nach dem zuletzt Bewiesenen bleibt noch übrig, zu zeigen, dass und wie man zu einem beliebig gegebenen Werth von $\varkappa^2$ wenigstens *einen* der Bedingung

$$\varkappa^2 = \frac{\vartheta_{10}^4}{\vartheta_{00}^4} \tag{1}$$

genügenden Werth von $\omega$ finden kann. Diese Frage wird am vollständigsten beantwortet durch Zurückführung auf eine lineare Differentialgleichung zweiter Ordnung.

Eine solche Differentialgleichung ist aber in den Formeln des §. 20 bereits enthalten.

Es folgt zunächst aus §. 20, (14):

$$d \log \varkappa^2 = i \pi \vartheta_{01}^4 d \omega,$$

oder mit Rücksicht auf

$$\pi \vartheta_{00}^2 = 2K, \quad \pi \vartheta_{10}^2 = 2 \varkappa K, \quad \pi \vartheta_{01}^2 = 2 \varkappa' K: \tag{2}$$

$$\pi d(\varkappa^2) = 4 i \varkappa^2 \varkappa'^2 K^2 d \omega, \tag{3}$$

und aus §. 20, (19):

$$\frac{d}{d\omega} \frac{dK}{K^2 d\omega} = -\frac{4}{\pi^2} \varkappa^2 \varkappa'^2 K^3.$$

Führt man vermittelst (3) für $\omega$ die Variable $\varkappa^2$ ein, so folgt

$$\frac{d}{d(\varkappa^2)} \left( \varkappa^2 \varkappa'^2 \frac{dK}{d(\varkappa^2)} \right) = \frac{1}{4} K, \tag{4}$$

welches die gesuchte Differentialgleichung ist.

Setzen wir weiter

$$- i \omega = \frac{K'}{K}, \tag{5}$$

$$- i K^2 d \omega = K dK' - K' dK, \tag{6}$$

so ergiebt sich nach (3):

$$\varkappa^2 \varkappa'^2 \left( K \frac{dK'}{d(\varkappa^2)} - K' \frac{dK}{d(\varkappa^2)} \right) = -\frac{\pi}{4}, \tag{7}$$

also durch abermalige Differentiation:

$$\frac{1}{K} \frac{d}{d(\varkappa^2)} \left( \varkappa^2 \varkappa'^2 \frac{dK}{d(\varkappa^2)} \right) = \frac{1}{K'} \frac{d}{d(\varkappa^2)} \left( \varkappa^2 \varkappa'^2 \frac{dK'}{d(\varkappa^2)} \right),$$

woraus zu ersehen, dass $K'$ das zweite particulare Integral der Differentialgleichung (4) ist.

Diese Differentialgleichung lässt sich durch hypergeometrische Reihen integriren. Das eine particulare Integral derselben ist die Reihe

$$(8) \qquad F\left(\frac{1}{2}, \frac{1}{2}, 1, \varkappa^2\right) = 1 + \sum_{1,\infty}^{\nu} \left(\frac{1.3\,..\,2\nu - 1}{2.4\,..\,2\nu}\right)^2 \varkappa^{2\nu},$$

welche convergent ist, so lange der absolute Werth von $\varkappa^2$ kleiner als 1 ist. Als das zweite particulare Integral kann man wählen

$$(9) \qquad F\left(\frac{1}{2}, \frac{1}{2}, 1, \varkappa'^2\right),$$

welches aber einen anderen Convergenzbereich hat. Denken wir uns $\varkappa^2$ als complexe Variable in einer Ebene dargestellt, so convergirt (8) in einem mit dem Radius 1 um den Nullpunkt beschriebenen Kreise, (9) in einem gleichen Kreise um den Punkt 1 beschrieben, so dass der gemeinsame Convergenzbereich aus einem Zweieck besteht, welches den zwischen 0 und 1 gelegenen Theil der reellen Achse enthält. Man kann aber auch, was für uns wichtig ist, das zweite particulare Integral in einer Form aufstellen, welche in demselben Kreise wie die Reihe (8) convergirt, wobei jedoch zu beachten ist, dass das zweite particulare Integral für $\varkappa^2 = 0$ unendlich wird.

Dies zweite particulare Integral lautet, wenn wir nach Gauss (Disq. circa seriem infinitam etc., Werke, Bd. III, S. 125) $\Pi(n)$ und $\Psi(n)$ durch die Gleichungen

$$\Pi(n) = 1.2.3\,...\,n$$

$$\Psi(n) - \Psi(0) = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$$

definiren:

$$(10) \sum_{1,\infty}^{\nu} 2[\Psi(\nu) - \Psi(0)] \frac{\Pi(2\nu)^2}{\Pi(\nu)^4} \left(\frac{\varkappa^2}{16}\right)^{\nu} - log\,\frac{\varkappa^2}{16\varkappa'^2}\, F\left(\frac{1}{2}, \frac{1}{2}, 1, \varkappa^2\right),$$

wie man leicht durch Einsetzen in die Differentialgleichung (4) verificirt.

Wir setzen zur Abkürzung die Reihe (8):

$$(11) \qquad \sum_{0,\infty}^{\nu} \frac{\Pi(2\nu)^2}{\Pi(\nu)^4} \left(\frac{\varkappa^2}{16}\right)^{\nu} = F(\varkappa^2),$$

und den ersten Theil des Ausdruckes (10):

$$(12) \qquad \sum_{1,\infty}^{\nu} 2[\Psi(\nu) - \Psi(0)] \frac{\Pi(2\nu)^2}{\Pi(\nu)^4} \left(\frac{\varkappa^2}{16}\right)^{\nu} = G(\varkappa^2).$$

Um nun aber $K$ und $K'$ durch diese particularen Integrale wirklich darzustellen, müssen wir das Verhalten von $K, K'$ für $q = 0$ untersuchen, wofür zugleich $\varkappa^2 = 0$ wird.

Es ist aber für $q = 0$ nach §. 22 und §. 37:

$$q^{-1}\varkappa^2 = 16, \quad 2K = \pi, \tag{13}$$

also:

$$\operatorname{Lim}\left(\log\frac{\varkappa^2}{16} - i\pi\omega\right) = 0,$$

andererseits:

$$2K' + \log\frac{\varkappa^2}{16} = \left(\log\frac{\varkappa^2}{16} - i\pi\omega\right) + i\pi\omega(1 - \vartheta_{00}^2),$$

woraus:

$$\operatorname*{Lim}_{\varkappa^2 = 0}\left(2K' + \log\frac{\varkappa^2}{16}\right) = 0, \tag{14}$$

$$K = \frac{\pi}{2}F(\varkappa^2), \quad K' = \frac{1}{2}G(\varkappa^2) - \frac{1}{2}\log\frac{\varkappa^2}{16\varkappa'^2}F(\varkappa^2) \tag{15}$$

und

$$q = \frac{\varkappa^2}{16\varkappa'^2}e^{-\frac{G(\varkappa^2)}{F(\varkappa^2)}}, \tag{16}$$

worin, wie schon bemerkt, die Reihen $G(\varkappa^2)$, $F(\varkappa^2)$ convergent sind, so lange der absolute Werth von $\varkappa^2$ ein echter Bruch ist. In der Differentialgleichung (4) liegen nun freilich die Mittel, die gefundenen Ausdrücke für $K, K', q$ über dies Convergenzbereich hinaus fortzusetzen. Einfacher gelangt man dazu aber durch die Anwendung der Landen'schen Transformation.

Wir begrenzen die Ebene der complexen Werthe $\varkappa^2$, indem wir längs der reellen Achse zwei Schnitte von 0 bis $-\infty$ und von 1 bis $\infty$ legen. In der so begrenzten Ebene sind dann alle Wurzeln aus $\varkappa^2$, $\varkappa'^2$ eindeutig dadurch bestimmt, dass sie für positive echt gebrochene $\varkappa^2$ reell und positiv sein sollen. Es ist nun nach den Formeln der Landen'schen Transformation [§. 39, (23)], wenn wir mit $\varkappa_1, \varkappa_1', K_1, K_1'$ die Functionen von $\omega$ bezeichnen, die sich aus $\varkappa, \varkappa', K, K'$ ergeben, wenn $\omega$ durch $2\omega$ ersetzt wird:

$$\varkappa_1 = \frac{1-\varkappa'}{1+\varkappa'}, \qquad \varkappa_1' = \frac{2\sqrt{\varkappa'}}{1+\varkappa'} \tag{17}$$

$$2K_1 = (1+\varkappa')K, \quad K_1' = (1+\varkappa')K'.$$

Wenn wir also in (16) $\omega$ durch $2\omega$ ersetzen, so folgt:

$$q = \frac{1}{4} \frac{\varkappa_1}{\varkappa_1'} e^{-\frac{1}{2} \frac{G(\varkappa_1^2)}{F(\varkappa_1^2)}}. \tag{18}$$

Hierin erstreckt sich nun der Convergenzbereich über den in der Ebene $\varkappa_1^2$ gelegenen Einheitskreis. Dieser aber entspricht nach der ersten Formel (17) der ganzen Ebene $\varkappa^2$, so dass die Kreisperipherie den rein imaginären Werthen von $\varkappa'$, d. h. beiden Ufern des von 1 nach $\infty$ laufenden Schnittes, entspricht.

Man kann aber die Convergenz dieser Ausdrücke noch verbessern durch eine abermalige Anwendung der Landen'schen Transformation. Bezeichnen wir das Resultat einer nochmaligen Verdoppelung von $\omega$ durch den Index 2, so folgt:

$$\sqrt{\varkappa_2} = \frac{1 - \sqrt{\varkappa'}}{1 + \sqrt{\varkappa'}}, \qquad 4 K_2 = (1 + \sqrt{\varkappa'})^2 K, \tag{19}$$

$$K_2' = (1 + \sqrt{\varkappa'})^2 K',$$

$$q = \sqrt{\frac{\varkappa_2}{4 \varkappa_2'}}\, e^{-\frac{1}{4} \frac{G(\varkappa_2^2)}{F(\varkappa_2^2)}}, \tag{20}$$

worin nun der Convergenzbereich die Ebene der $\varkappa^2$ zweimal (mit einer Verzweigung im Punkte $\varkappa^2 = 1$) bedeckt.

Diese Operation kann man fortsetzen, indem man nach der Formel (17) aus $\varkappa_2$ durch Verdoppelung von $\omega$ eine neue Grösse $\varkappa_3$, daraus ebenso $\varkappa_4$ u. s. f. herleitet. Man bekommt dann eine Reihe von Ausdrücken für $q$, deren Convergenz eine immer bessere wird. Für ein beliebiges $\nu$ ist:

$$q = \sqrt[2^{\nu-1}]{\frac{\varkappa_\nu}{4 \varkappa_\nu'}}\, e^{-\frac{G(\varkappa_\nu^2)}{2^\nu F(\varkappa_\nu^2)}}. \tag{21}$$

Die erste Gleichung (17)

$$\varkappa_1 = \frac{\varkappa^2}{(1 + \varkappa')^2}$$

zeigt, dass, so lange der absolute Werth von $\varkappa^2$ kleiner als 1 ist, und folglich der absolute Werth von $1 + \varkappa'$ grösser als 1, der absolute Werth von $\varkappa_1$ kleiner ist als der von $\varkappa^2$, und folglich nähert sich $\varkappa_\nu$ mit unendlich wachsendem $\nu$ der Grenze Null. Daraus erhält man für $q$ die Darstellung:

$$q = \lim_{\nu = \infty} \sqrt[2^{\nu-1}]{\frac{\varkappa_\nu}{4 \varkappa_\nu'}} = \lim \sqrt[2^{\nu-1}]{\frac{\varkappa_\nu}{4}}, \tag{22}$$

welche bei reellen Werthen von $\varkappa$ zur Berechnung geeignet ist.

Aus jeder der Formeln (21) kann man eine Reihenentwickelung von $q$ nach den steigenden Potenzen von $\varkappa_\nu$ herleiten, deren Convergenz mit wachsendem $\nu$ zunimmt. Wendet man insbesondere die Formel (20) an, so erhält man eine Entwickelung, welche Weierstrass in den Monatsberichten der Berliner Akademie vom Jahre 1883 mitgetheilt hat, deren Convergenzbereich die Ebene $\varkappa^2$ zweimal ausfüllt.

Die Coëfficienten dieser Entwickelung berechnet man am einfachsten aus:

$$(23) \qquad \sqrt{\varkappa_2} = \frac{\vartheta_{10}(0, 4\omega)}{\vartheta_{00}(0, 4\omega)} = \frac{2q + 2q^9 + 2q^{25} + \cdots}{1 + 2q^4 + 2q^{16} + \cdots},$$

und erhält so nach der Methode der unbestimmten Coëfficienten:

$$(24) \quad q = \frac{\sqrt{\varkappa_2}}{2} + 2\left(\frac{\sqrt{\varkappa_2}}{2}\right)^5 + 15\left(\frac{\sqrt{\varkappa_2}}{2}\right)^9 + 150\left(\frac{\sqrt{\varkappa_2}}{2}\right)^{13} + 1701\left(\frac{\sqrt{\varkappa_2}}{2}\right)^{17} + \cdots$$

Ebenso lässt sich nach (23) auch umgekehrt $\sqrt{\varkappa_2}$ in eine nach Potenzen von $q$ fortschreitende Reihe entwickeln:

$$(25) \qquad \frac{1}{2}\sqrt{\varkappa_2} = q - 2q^5 + 5q^9 - 10q^{13} + 18q^{17} \cdots,$$

welches die Umkehrung der Reihe (24) ist.

Damit ist die am Anfang dieses Paragraphen gestellte Frage vollständig beantwortet.

Bezüglich der Anwendung der hier entwickelten Formeln zu numerischer Berechnung von $q$ sei noch bemerkt, dass, wenn $\varkappa^2$ näher an 1 liegt, man ein besser convergentes Verfahren erhält, wenn man $\varkappa^2$ mit $\varkappa'^2$ vertauscht. Die Rechnung ergiebt dann zunächst nicht $q$, sondern

$$q' = e^{-\frac{\pi i}{\omega}},$$

woraus man aber $q$ aus der Formel erhält:

$$q \log q' = \pi^2.$$

## §. 49. Die Modulfunctionen.

Unter einer Modulfunction wollen wir eine solche eindeutige Function von $\omega$ verstehen, welche ungeändert bleibt, wenn $\omega$ entweder der Gesammtheit oder auch nur einem Theil der linearen Transformationen

$$S = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \tag{1}$$

unterworfen wird, so dass, wenn $\psi(\omega)$ eine solche Function ist:

$$\psi\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right) = \psi(\omega).$$

Alle linearen Transformationen, durch welche eine solche Function $\psi(\omega)$ ungeändert bleibt, bilden eine Gruppe $\mathfrak{G}$ in dem Sinne, wie dieser Ausdruck am Schluss des §. 31 gebraucht ist; denn, wenn $\psi(\omega)$ durch $(S)$ und durch $(S')$ ungeändert bleibt, so bleibt sie auch durch $(S)(S')$ ungeändert. Diese Gruppe $\mathfrak{G}$ ist enthalten in der Gruppe $\mathfrak{G}_0$, welche aus allen Transformationen $(S)$ besteht.

Wenn eine solche Gruppe $\mathfrak{G}$ **alle** Transformationen und nur diejenigen enthält, durch welche $\psi(\omega)$ ungeändert bleibt in dem Sinne, dass die Gleichung

$$\psi(\omega) = \psi(\omega')$$

eine Gleichung

$$\omega' = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}$$

nach sich zieht, so dass

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

in $\mathfrak{G}$ enthalten ist, so sagen wir, $\psi(\omega)$ gehöre zur Gruppe $\mathfrak{G}$.

Wir beschränken uns auf die Betrachtung solcher Modulfunctionen, welche mit dem Modul $\varkappa^2$ in einem algebraischen Zusammenhange stehen.

Unter dieser Voraussetzung lässt sich der folgende allgemeine Satz aussprechen:

Wenn $\psi(\omega)$ zur Gruppe $\mathfrak{G}$ gehört und $\chi(\omega)$ durch die Transformationen von $\mathfrak{G}$ ungeändert bleibt, so ist $\chi(\omega)$ **rational** durch $\psi(\omega)$ ausdrückbar.

Denn zunächst ist $\chi(\omega)$ eine algebraische Function von $\psi(\omega)$, und $\psi(\omega)$ kann als algebraische Function von $\varkappa^2$ jeden Werth annehmen. Zu jedem Werth von $\psi(\omega)$ gehört aber nach Voraussetzung nur ein Werth von $\chi(\omega)$ und daher ist $\chi(\omega)$ als einwerthige algebraische Function von $\psi(\omega)$ rational [§. 11, (9)].

Es ist eine grosse, noch nicht vollständig gelöste Aufgabe, alle in $\mathfrak{G}_0$ enthaltenen Gruppen zu ermitteln, zu welchen Modulfunctionen gehören. F. Klein hat in mehreren Abhandlungen eine grosse Classe derselben, die er Congruenzgruppen nennt, untersucht, deren Transformationen dadurch charakterisirt sind, dass für irgend einen ganzzahligen Modul $m$

$$\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix} \equiv \begin{pmatrix}1, & 0 \\ 0, & 1\end{pmatrix} \pmod{m}.$$

Für $m = 2$ ist diese Gruppe die erste unserer sechs Classen. Wir wollen hier nur diejenigen Modulfunctionen näher betrachten, auf welche wir im Verlaufe unserer Untersuchung gestossen sind, und einige nahe damit verwandte.

1. Der Modul $\varkappa^2$ ist nach §. 47 eine zu der ersten Classe der linearen Transformationen gehörige Modulfunction; da nach §. 31 alle diese Transformationen aus den beiden

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

zusammensetzbar sind, so können wir den Satz aussprechen:

Jede Modulfunction, welche durch die beiden Vertauschungen

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

ungeändert bleibt, ist eine rationale Function von $\varkappa^2$.

2. Die Function $\varkappa^2 \varkappa'^2$ gehört zu der aus der ersten und zweiten Classe des §. 31 gemeinschaftlich gebildeten Gruppe. Diese Gruppe lässt sich durch Wiederholung der beiden Transformationen

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

ableiten, und wir können daher den Satz aussprechen:

Jede Modulfunction, welche durch die beiden Vertauschungen

$$(\omega,\ \omega + 2), \qquad \left(\omega,\ -\frac{1}{\omega}\right)$$

ungeändert bleibt, ist eine rationale Function von $\varkappa^2 \varkappa'^2$. Hieraus folgt noch:

3. Jede Modulfunction, die durch $(\omega, \omega + 2)$ ungeändert bleibt und durch $\left(\omega, -\frac{1}{\omega}\right)$ ihr Zeichen ändert, ist das Product von $(\varkappa'^2 - \varkappa^2)$ mit einer rationalen Function von $\varkappa^2 \varkappa'^2$.

4. Die Invariante $j(\omega)$ gehört zur Gruppe $\mathfrak{G}_0$ (§. 47) und daher der Satz:

Jede Modulfunction, welche durch die beiden Vertauschungen

$$(\omega,\ \omega + 1), \qquad \left(\omega,\ -\frac{1}{\omega}\right)$$

ungeändert bleibt, ist eine rationale Function von $j(\omega)$.

Ausser diesen führen wir noch zwei andere Modulfunctionen ein.

Aus der Definition der Functionen $f(\omega)$, $f_1(\omega)$, $f_2(\omega)$ [§. 29, (10), (2)] ergiebt sich, wenn man die beiden Gleichungen §. 37, (3) mit einander multiplicirt:

$$(2) \quad f(\omega) = \frac{\sqrt[6]{2}}{\sqrt[12]{\varkappa \varkappa'}}, \quad f_1(\omega) = \sqrt[6]{2}\sqrt[12]{\frac{\varkappa'^2}{\varkappa}}, \quad f_2(\omega) = \sqrt[6]{2}\sqrt[12]{\frac{\varkappa^2}{\varkappa'}},$$

$$(3) \qquad \frac{f_1(\omega)}{f(\omega)} = \sqrt[4]{\varkappa'}, \qquad \frac{f_2(\omega)}{f(\omega)} = \sqrt[4]{\varkappa}.$$

Auf Grund von §. 41, (15), (16) definiren wir zwei Functionen $\gamma_2(\omega)$, $\gamma_3(\omega)$:

$$(4) \quad \begin{aligned} \gamma_2(\omega) &= \sqrt[3]{j(\omega)} = \sqrt[3]{2}^{\,8}\, \frac{1 - \varkappa^2 \varkappa'^2}{\sqrt[3]{\varkappa^4 \varkappa'^4}} \\ \gamma_3(\omega) &= \sqrt{j(\omega) - 27 \cdot 64} = \frac{8\,(2 + \varkappa^2 \varkappa'^2)\,(\varkappa'^2 - \varkappa^2)}{\varkappa^2 \varkappa'^2}, \end{aligned}$$

welche nach (2) und (3) als eindeutige Functionen von $\omega$ folgendermaassen darstellbar sind:

$$(5) \quad \begin{aligned} \gamma_2(\omega) &= \frac{f(\omega)^{24} - 16}{f(\omega)^8} \\ \gamma_3(\omega) &= \frac{[f(\omega)^{24} + 8]\,[f_1(\omega)^8 - f_2(\omega)^8]}{f(\omega)^8} \end{aligned}$$

wofür man nach den Grundformeln für die $f$-Functionen [§. 29, (11), (12)] auch setzen kann:

$$(6)\qquad \gamma_2(\omega) = f(\omega)^8 f_1(\omega)^8 + f(\omega)^8 f_2(\omega)^8 - f_1(\omega)^8 f_2(\omega)^8,$$

$$(7)\qquad \gamma_3(\omega) = \frac{1}{2}\,[f(\omega)^8 + f_1(\omega)^8]\,[f(\omega)^8 + f_2(\omega)^8]\,[f_1(\omega)^8 - f_2(\omega)^8].$$

Es sind also $f^8$, $-f_1^8$, $-f_2^8$ die Wurzeln der cubischen Gleichung

$$(8)\qquad f^{24} - \gamma_2 f^8 - 16 = 0$$

und $4\gamma_3^2$ ist die Discriminante dieser Gleichung.

Bemerkenswerth sind auch die aus §. 48 für diese Functionen folgenden Differentialgleichungen:

$$(9)\qquad d\varkappa^2 = -\,d\varkappa'^2 = \pi i\,\vartheta_{00}^4\,\varkappa^2\varkappa'^2\,d\omega,$$

$$(10)\qquad d\varkappa^2\varkappa'^2 = -\,\pi i\,\vartheta_{00}^4\,(\varkappa^2 - \varkappa'^2)\,\varkappa^2\varkappa'^2\,d\omega,$$

$$(11)\qquad df(\omega)^8 = \frac{\pi i}{3}\,\vartheta_{00}^4\,[f_2(\omega)^8 - f_1(\omega)^8]\,d\omega,$$

$$(12)\qquad d\gamma_2(\omega) = -\,\frac{2\pi i}{3}\,\gamma_3(\omega)\,\eta(\omega)^4\,d\omega \quad [\text{§. 29 (10)}],$$

$$(13)\qquad dj(\omega) = -\,2\pi i\,\gamma_2(\omega)^2\,\gamma_3(\omega)\,\eta(\omega)^4\,d\omega.$$

Man erhält sodann für die linearen Fundamentaltransformationen aus §. 29, (13), (14), (15):

$$(14)\qquad \begin{aligned} \gamma_2(\omega+1) &= e^{-\frac{2\pi i}{3}}\,\gamma_2(\omega), & \gamma_2\left(-\frac{1}{\omega}\right) &= \gamma_2(\omega),\\ \gamma_3(\omega+1) &= -\,\gamma_3(\omega), & \gamma_3\left(-\frac{1}{\omega}\right) &= -\,\gamma_3(\omega), \end{aligned}$$

und aus §. 35 findet man allgemein:

$$(15)\qquad \begin{aligned} \gamma_2\left(\frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right) &= e^{-\frac{2\pi i}{3}(\alpha\beta+\alpha\gamma+\beta\delta-\alpha\beta^2\gamma)}\,\gamma_2(\omega)\\ \gamma_3\left(\frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right) &= (-1)^{\alpha\gamma+\beta\gamma+\beta\delta}\,\gamma_3(\omega). \end{aligned}$$

Es sind dies also Modulfunctionen, und die Gruppen, zu welchen sie gehören, sind durch die beiden Congruenzen charakterisirt:

$$\begin{aligned} \alpha\beta + \alpha\gamma + \beta\delta - \alpha\beta^2\gamma &\equiv 0 \pmod 3\\ \alpha\gamma + \beta\gamma + \beta\delta &\equiv 0 \pmod 2). \end{aligned}$$

Wir geben hiernach unserem Satz 4. die folgende Ergänzung, die sich aus den Formeln (14) ergiebt.

5. Eine Modulfunction, welche durch die beiden Substitutionen

$$(\omega, \omega + 1), \quad \left(\omega, -\frac{1}{\omega}\right)$$

das Zeichen ändert, ist das Product von $\gamma_3(\omega)$ mit einer rationalen Function von $j(\omega)$.

6. Eine Modulfunction, welche durch die Substitution $\left(\omega, -\frac{1}{\omega}\right)$ ungeändert bleibt und durch $(\omega, \omega + 1)$ den Factor $e^{\mp\frac{2\pi i}{3}}$ annimmt, ist das Product von $\gamma_3(\omega)^{\pm 1}$ mit einer rationalen Function von $j(\omega)$.

7. Eine Modulfunction, welche durch die Substitutionen $\left(\omega, -\frac{1}{\omega}\right)$ das Zeichen ändert und durch $(\omega, \omega + 1)$ den Factor $-e^{\mp\frac{2\pi i}{3}}$ annimmt, ist das Product von $\gamma_2(\omega)\gamma_3(\omega)^{\pm 1}$ mit einer rationalen Function von $j(\omega)$.

## §. 50. Darstellung der elliptischen Functionen durch $v$ und $\varkappa^2$.

Wenn wir das Umkehrproblem der elliptischen Integrale so wie in §. 46 als die Aufgabe der Integration der elliptischen Differentialgleichungen fassen, so verlangt es die Darstellung der drei Functionen $\operatorname{sn} v$, $\operatorname{cn} v$, $\operatorname{dn} v$ durch die beiden unabhängigen Variablen $v$, $\varkappa^2$. Diese Aufgabe ist durch §. 48 gelöst, aber bezüglich der Variablen $\varkappa^2$ nur implicite. Man kann aber auch Darstellungen finden, welche $\varkappa^2$ explicite enthalten, und zwar durch Reihen, welche nach Potenzen von $v$ fortschreiten, deren Coëfficienten rationale Functionen von $\varkappa^2$ sind. Die Coëfficienten dieser Reihen können freilich nicht durch ein allgemeines Gesetz dargestellt, sondern nur successive berechnet werden. Diese Darstellungen verdankt man hauptsächlich Weierstrass¹).

---

1) Ueber die Weierstrass'sche Theorie der elliptischen Functionen vgl. man besonders die von H. A. Schwarz herausgegebenen „Formeln und Lehrsätze zum Gebrauch der elliptischen Functionen". Ueber die Reihenentwickelungen vgl. man auch Königsberger „Vorlesungen über die Theorie der elliptischen Functionen", 25. Vorlesung.

Die $\sigma$-Functionen können, da sie durchaus endliche und stetige Functionen von $u$ sind, in unbedingt convergente Potenzreihen nach $u$ entwickelt werden, und wenn wir daher die in §. 40, (2) vorkommenden $\sigma$-Functionen in dieser Weise entwickeln, so bekommen wir eine Lösung unserer Aufgabe. Wir setzen daher

$$(1)\quad \begin{aligned}
\sigma(v,\ 2K,\ 2iK') &= \sum_{0,\infty}^{\nu} A_\nu \frac{v^{2\nu+1}}{(2\nu+1)!} \\
\sigma_{00}(v,\ 2K,\ 2iK') &= \sum_{0,\infty}^{\nu} B_\nu \frac{v^{2\nu}}{(2\nu)!} \\
\sigma_{01}(v,\ 2K,\ 2iK') &= \sum_{0,\infty}^{\nu} C_\nu \frac{v^{2\nu}}{(2\nu)!} \\
\sigma_{10}(v,\ 2K,\ 2iK') &= \sum_{0,\infty}^{\nu} D_\nu \frac{v^{2\nu}}{(2\nu)!},
\end{aligned}$$

und die $A_\nu$, $B_\nu$, $C_\nu$, $D_\nu$ sind die zu bestimmenden Functionen von $\varkappa^2$ oder von $\omega$. Fassen wir sie zunächst als Functionen von $\omega$ auf, so ergeben die linearen Transformationen [§. 40, (3)]:

$$(2)\quad \begin{aligned}
A_\nu\left(-\frac{1}{\omega}\right) &= (-1)^\nu A_\nu(\omega) \\
B_\nu\left(-\frac{1}{\omega}\right) &= (-1)^\nu B_\nu(\omega) \\
C_\nu\left(-\frac{1}{\omega}\right) &= (-1)^\nu D_\nu(\omega) \\
D_\nu\left(-\frac{1}{\omega}\right) &= (-1)^\nu C_\nu(\omega).
\end{aligned}$$

$$(3)\quad \begin{aligned}
\varkappa'^{2\nu} A_\nu(\omega+1) &= A_\nu(\omega) \\
\varkappa'^{2\nu} B_\nu(\omega+1) &= C_\nu(\omega) \\
\varkappa'^{2\nu} C_\nu(\omega+1) &= B_\nu(\omega) \\
\varkappa'^{2\nu} D_\nu(\omega+1) &= D_\nu(\omega).
\end{aligned}$$

$$(4)\quad \begin{aligned}
A_\nu(\omega+2) &= A_\nu(\omega) \\
B_\nu(\omega+2) &= B_\nu(\omega) \\
C_\nu(\omega+2) &= C_\nu(\omega) \\
D_\nu(\omega+2) &= D_\nu(\omega).
\end{aligned}$$

Hieraus schliessen wir auf die charakteristischen Eigenschaften dieser Coëfficienten als Functionen von $\varkappa^2$. Zunächst erhellt aus der Bedeutung der Coëfficienten, dass für jeden Werth von $\varkappa^2$ mit etwaiger Ausnahme von $\varkappa^2 = 0,\ 1,\ \infty$ die Coëfficienten $A_\nu(\varkappa^2)$, $B_\nu(\varkappa^2)$, $C_\nu(\varkappa^2)$, $D_\nu(\varkappa^2)$ endliche und stetige Functionen von $\varkappa^2$ sind.

Aber auch für $\varkappa^2 = 0$ bleiben diese Functionen endlich und man kann ihre Werthe leicht finden, wenn man in den Darstellungen des §. 32 $q$ und mithin $\varkappa^2$ in Null übergehen lässt. Man erhält dann aus den Entwickelungen in §. 22 mit Rücksicht darauf, dass nach §§. 29, 37 für ein verschwindendes $q$

$$\eta(\omega) = q^{\frac{1}{12}}, \qquad 2K = \pi$$

wird

$$\begin{aligned} e^{\frac{v^2}{6}} \sin v &= \sum_{0,\infty}^{\nu} A_\nu(0) \frac{v^{2\nu+1}}{(2\nu+1)!} \\ e^{\frac{v^2}{6}} &= \sum_{0,\infty}^{\nu} B_\nu(0) \frac{v^{2\nu}}{(2\nu)!} \\ e^{\frac{v^2}{6}} &= \sum_{0,\infty}^{\nu} C_\nu(0) \frac{v^{2\nu+1}}{(2\nu)!} \\ e^{\frac{v^2}{6}} \cos v &= \sum_{0,\infty}^{\nu} D_\nu(0) \frac{v^{2\nu}}{(2\nu)!} \end{aligned} \tag{5}$$

Die Formeln (2) ergeben nun:

$$\begin{aligned} A_\nu(\varkappa'^2) &= (-1)^\nu A_\nu(\varkappa^2) \\ B_\nu(\varkappa'^2) &= (-1)^\nu B_\nu(\varkappa^2) \\ C_\nu(\varkappa'^2) &= (-1)^\nu D_\nu(\varkappa^2) \\ D_\nu(\varkappa'^2) &= (-1)^\nu C_\nu(\varkappa^2). \end{aligned} \tag{6}$$

woraus folgt, dass auch für $\varkappa^2 = 1$ diese Functionen endlich bleiben, nämlich:

$$\begin{aligned} A_\nu(1) &= (-1)^\nu A_\nu(0) \\ B_\nu(1) &= (-1)^\nu B_\nu(0) \\ C_\nu(1) &= (-1)^\nu D_\nu(0) \\ D_\nu(1) &= (-1)^\nu C_\nu(0). \end{aligned} \tag{7}$$

Das System (3) lässt sich ferner so schreiben:

$$\begin{aligned} \varkappa'^{2\nu} A_\nu\left(\frac{-\varkappa^2}{\varkappa'^2}\right) &= A_\nu(\varkappa^2) \\ \varkappa'^{2\nu} B_\nu\left(\frac{-\varkappa^2}{\varkappa'^2}\right) &= C_\nu(\varkappa^2) \\ \varkappa'^{2\nu} C_\nu\left(\frac{-\varkappa^2}{\varkappa'^2}\right) &= B_\nu(\varkappa^2) \\ \varkappa'^{2\nu} D_\nu\left(\frac{-\varkappa^2}{\varkappa'^2}\right) &= D_\nu(\varkappa^2), \end{aligned} \tag{8}$$

woraus für ein unendliches $\varkappa^2$:

$$
(9) \qquad
\begin{aligned}
A_\nu(\varkappa^2) &= \varkappa^{2\nu} A_\nu(0),\\
B_\nu(\varkappa^2) &= \varkappa^{2\nu} D_\nu(0),\\
C_\nu(\varkappa^2) &= \varkappa^{2\nu} B_\nu(0),\\
D_\nu(\varkappa^2) &= \varkappa^{2\nu} C_\nu(0),
\end{aligned}
$$

und hieraus wird geschlossen, dass die Coëfficienten $A_\nu, B_\nu, C_\nu, D_\nu$ ganze rationale Functionen von $\varkappa^2$ vom Grade $\nu$ sind, und aus §. 49, 2, 3, folgt überdies noch, dass $A_\nu$, $B_\nu$ bei geradem $\nu$ rational durch $\varkappa^2\varkappa'^2$ ausgedrückt sind, während sie bei ungeradem $\nu$ gleich dem Product von $(\varkappa'^2 - \varkappa^2)$ mit einer rationalen Function von $\varkappa^2\varkappa'^2$ sind.

Aus $B_\nu$ findet man $C_\nu$ mittelst der Formel:

$$
(10) \qquad C_\nu(\varkappa^2) = \varkappa'^{2\nu} B_\nu\left(\frac{-\varkappa^2}{\varkappa'^2}\right)
$$

und $D_\nu$ durch Anwendung von (6) und (8):

$$
(11) \qquad D_\nu(\varkappa^2) = (-1)^\nu C_\nu(\varkappa'^2) = (-1)^\nu \varkappa^{2\nu} B_\nu\left(\frac{-\varkappa'^2}{\varkappa^2}\right).
$$

Da man aus (5) die Coëfficienten $A_\nu(0)$, $B_\nu(0)$, $C_\nu(0)$, $D_\nu(0)$ leicht bestimmen kann, so ergeben sich aus dem hier entwickelten Formelsystem die Coëfficienten $A_\nu$, $B_\nu$, $C_\nu$, $D_\nu$ ohne weitere Rechnung bis $\nu = 3$ einschliesslich.

Man findet:

$$
\begin{aligned}
&A_0 = 1, \quad A_1 = 0 && A_2 = -\frac{2}{3}(1 - \varkappa^2\varkappa'^2)\\
&B_0 = 1, \quad B_1 = \frac{1}{3}(\varkappa'^2 - \varkappa^2), && B_2 = \frac{1}{3}(1 + 2\varkappa^2\varkappa'^2)\\
&C_0 = 1, \quad C_1 = \frac{1}{3}(1 + \varkappa^2), && C_2 = \frac{1}{3}(\varkappa'^4 - 2\varkappa^2)\\
&D_0 = 1, \quad D_1 = -\frac{1}{3}(1 + \varkappa'^2), && D_2 = \frac{1}{3}(\varkappa^4 - 2\varkappa'^2).
\end{aligned}
$$

$$
\begin{aligned}
A_3 &= -\frac{8}{9}(\varkappa'^2 - \varkappa^2)(2 + \varkappa^2\varkappa'^2)\\
B_3 &= \frac{1}{9}(\varkappa'^2 - \varkappa^2)(5 - 2\varkappa^2\varkappa'^2)\\
C_3 &= \frac{1}{9}(1 + \varkappa^2)(5\varkappa'^4 + 2\varkappa^2)\\
D_3 &= -\frac{1}{9}(1 + \varkappa'^2)(5\varkappa^4 + 2\varkappa'^2).
\end{aligned}
$$

Weitere Coëfficienten lassen sich auf demselben Wege, wenn auch weitläufiger berechnen, indem man die Ausdrücke für die $\sigma$-Functionen in §. 32 nach Potenzen von $q$ entwickelt und, wie hier die niedrigste Potenz von $q$, so die höheren benutzt. Weierstrass bedient sich zur recurrenten Berechnung der Coëfficienten gewisser partieller Differentialgleichungen. Darauf soll hier nicht weiter eingegangen werden.

# Sechster Abschnitt.

## Einige Anwendungen der elliptischen Functionen.

### §. 51. Oberfläche des Ellipsoids.

Wir wollen hier den Fortgang unserer Betrachtungen unterbrechen, um durch zwei Anwendungen das bisher Entwickelte zu beleben. Wir wählen zuerst ein berühmtes Problem, die Bestimmung der Oberfläche des dreiachsigen Ellipsoids, von welchem hier eine neue Lösung gegeben werden soll.

Wir drücken die Punkte der Oberfläche des Ellipsoids, dessen Gleichung in rechtwinkeligen Coordinaten

$$\frac{x^2}{a} + \frac{y^2}{b} + \frac{z^2}{c} = 1 \tag{1}$$

lautet, durch elliptische Coordinaten aus, indem wir setzen:

$$\begin{aligned} x^2 &= \frac{a(\lambda - a)(\mu - a)}{(b - a)(c - a)} \\ y^2 &= \frac{b(\lambda - b)(\mu - b)}{(c - b)(a - b)} \\ z^2 &= \frac{c(\lambda - c)(\mu - c)}{(a - c)(b - c)}, \end{aligned} \tag{2}$$

worin $\lambda$, $\mu$ die elliptischen Coordinaten sind, welche an die Bedingung

$$0 < a < \lambda < b < \mu < c \tag{3}$$

gebunden sind.

Man hat, in diesen Variablen ausgedrückt, für die gesammte Oberfläche des Ellipsoids (1) den Ausdruck

$$F = 2\int_a^b\int_b^c \frac{(\mu - \lambda)\,\mu\,\lambda\,d\mu\,d\lambda}{\sqrt{\lambda(\lambda - a)(\lambda - b)(\lambda - c)}\,\sqrt{-\mu(\mu - a)(\mu - b)(\mu - c)}}, \tag{4}$$

worin die Quadratwurzeln mit positiven Zeichen zu nehmen sind[1]).

Wir setzen zur Abkürzung:

$$(5)\quad f(\lambda) = \lambda(\lambda - a)(\lambda - b)(\lambda - c) = \lambda^4 - a_1\lambda^3 + a_2\lambda^2 - a_3\lambda$$

und können dann das Doppelintegral $F$ durch die folgenden vier einfachen elliptischen Integrale ausdrücken:

$$(6)\quad \begin{aligned} &\int_a^b \frac{\lambda\, d\lambda}{\sqrt{f(\lambda)}} = A, \qquad &&\int_b^c \frac{\mu\, d\mu}{\sqrt{-f(\mu)}} = B, \\ &\int_a^b \frac{\lambda^2\, d\lambda}{\sqrt{f(\lambda)}} = A', \qquad &&\int_b^c \frac{\mu^2\, d\mu}{\sqrt{-f(\mu)}} = B', \end{aligned}$$

$$(7)\quad F = 2\,(AB' - BA').$$

Wir wenden nun die Ergebnisse des §. 36 auf diesen Fall an, und setzen

$$(8)\quad du = \frac{d\lambda}{\sqrt{f(\lambda)}}.$$

Es sind alsdann $\lambda$ und $\sqrt{f(\lambda)}$ einwerthige, doppeltperiodische Functionen von $u$ mit den beiden Perioden:

$$(9)\quad \omega_1 = 2\int_a^b \frac{d\lambda}{\sqrt{f(\lambda)}}, \qquad \omega_2 = 2i\int_b^c \frac{d\mu}{\sqrt{-f(\mu)}},$$

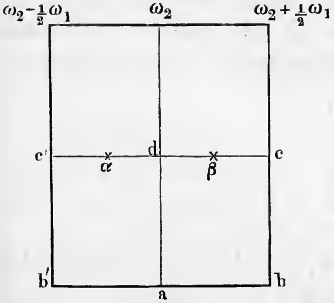
und wenn wir noch festsetzen, dass $\lambda - a$ für $u = 0$ verschwinden soll, so ist $\lambda$ eine gerade, $\sqrt{f(\lambda)}$ eine ungerade Function des Arguments $u$. In beistehender Fig. 3 ist das Periodenparallelogramm dargestellt. In den mit $a$, $b$, $c$, $d$ bezeichneten Punkten hat $u$ die Werthe:

$$0, \quad \frac{\omega_1}{2}, \quad \frac{(\omega_1 + \omega_2)}{2}, \quad \frac{\omega_2}{2}$$

und $\lambda$ die Werthe:

$$a, \; b, \; c, \; 0.$$

Fig. 3.



---

[1]) Vgl. Hesse, Vorlesungen über analytische Geometrie des Raumes, 22. Vorlesung.

Führt man also $u$ als Integrationsvariable in $A$, $A'$, $B$, $B'$ ein, so folgt:

$$(10)\qquad \begin{aligned} 2A &= \int\limits_{-\frac{1}{2}\omega_1}^{+\frac{1}{2}\omega_1} \lambda\, du, & 2iB &= \int\limits_{\frac{1}{2}\omega_1}^{\frac{1}{2}\omega_1+\omega_2} \lambda\, du, \\ 2A' &= \int\limits_{-\frac{1}{2}\omega_1}^{+\frac{1}{2}\omega_1} \lambda^2\, du, & 2iB' &= \int\limits_{\frac{1}{2}\omega_1}^{\frac{1}{2}\omega_1+\omega_2} \lambda^2\, du. \end{aligned}$$

Die Function $\lambda$ wird in zwei Punkten $\alpha$, $\beta$ des Periodenparallelogramms unendlich, welche durch

$$(11)\qquad \alpha = \frac{1}{2}\omega_2 - \int\limits_{-\infty}^{0} \frac{d\lambda}{\sqrt{f(\lambda)}}, \qquad \beta = \frac{1}{2}\omega_2 + \int\limits_{-\infty}^{0} \frac{d\lambda}{\sqrt{f(\lambda)}}$$

bestimmt sind, wobei $\sqrt{f(\lambda)}$ positiv ist. Um das Verhalten der Function $\lambda$ in der Umgebung von $\alpha$, $\beta$ zu erkennen, lassen wir $u$ sich von $d$ aus den Punkten $\alpha$, $\beta$ geradlinig annähern und erhalten:

$$u - \alpha = \int\limits_{-\infty}^{\lambda} \frac{d\lambda}{\sqrt{f(\lambda)}}, \qquad u - \beta = -\int\limits_{-\infty}^{\lambda} \frac{d\lambda}{\sqrt{f(\lambda)}},$$

worin $\lambda$ reell und $\sqrt{f(\lambda)}$ positiv ist. Aus der Entwickelung

$$\frac{1}{\sqrt{f(\lambda)}} = \frac{1}{\lambda^2} + \frac{a_1}{2}\frac{1}{\lambda^3} + \cdots$$

ergeben sich durch Integration und Umkehrung der Reihe für die Umgebung der beiden Punkte $\alpha$, $\beta$ die nach steigenden Potenzen von $u - \alpha$, $u - \beta$ fortschreitenden Entwickelungen:

$$(12)\qquad \begin{aligned} \lambda &= \frac{-1}{u-\alpha} + \frac{a_1}{4} + \cdots \\ \lambda &= \frac{+1}{u-\beta,} + \frac{a_1}{4} + \cdots \end{aligned}$$

woraus zu ersehen, dass $\left(\lambda^2 - \frac{1}{2}a_1\lambda\right)$ kein Glied mit der $-1$ ten Potenz von $u - \alpha$ oder $u - \beta$ enthält. Es ist daher

$$\psi(u) = \int\limits_0^u \left(\lambda^2 - \frac{1}{2}a_1\lambda\right) du$$

eine einwerthige ungerade Function von $u$ (eine Transscendente zweiter Gattung).

Da der Differentialquotient von $\psi(u)$ die Perioden $\omega_1$, $\omega_2$ hat, so sind die Differenzen $\psi(u+\omega_1)-\psi(u)$, $\psi(u+\omega_2)-\psi(u)$ von $u$ unabhängig und man erhält:

$$\begin{aligned}
\psi(u+\omega_1)-\psi(u) &= \int\limits_{-\frac{1}{2}\omega_1}^{+\frac{1}{2}\omega_1}\left(\lambda^2-\frac{1}{2}a_1\lambda\right)du = 2\left(A'-\frac{1}{2}a_1 A\right)\\
\psi(u+\omega_2)-\psi(u) &= \int\limits_{\frac{1}{2}\omega_1}^{\frac{1}{2}\omega_1+\omega_2}\left(\lambda^2-\frac{1}{2}a_1\lambda\right)du = 2i\left(B'-\frac{1}{2}a_1 B\right).
\end{aligned}\tag{13}$$

Nun ist nach dem Residuensatz [§. 11, (4)] das Integral

$$\frac{1}{2\pi i}\int \lambda\,\psi(u)\,du,\tag{14}$$

über die Begrenzung des Periodenparallelogramms erstreckt, gleich der Summe der Residuen der Function $\lambda\,\psi(u)$ für die Punkte $\alpha$, $\beta$. Wir bestimmen zuerst das Begrenzungsintegral, welches gleich ist

$$\frac{1}{2\pi i}\int\limits_{-\frac{1}{2}\omega_1}^{+\frac{1}{2}\omega_1}\lambda[\psi(u)-\psi(u+\omega_2)]\,du+\frac{1}{2\pi i}\int\limits_{\frac{1}{2}\omega_1}^{\frac{1}{2}\omega_1+\omega_2}\lambda\,[\psi(u)-\psi(u-\omega_1)]\,du,$$

also mit Rücksicht auf (13), (10), (7), indem man in der ersten Gleichung (13) $u-\omega_1$ an Stelle von $u$ setzt:

$$\frac{2}{\pi}(A'B-B'A)=-\frac{1}{\pi}F.\tag{15}$$

Es bleibt also noch übrig, die Residuen der Function $\lambda\,\psi(u)$, d. h. die Coëfficienten der $(-1)$ten Potenz in den Entwickelungen nach steigenden Potenzen von $u-\alpha$, $u-\beta$ zu bestimmen. Zu diesem Zweck müssen wir $\psi(u)$ durch partielle Integration so umformen, dass der unendlich werdende Theil in einer algebraischen Function von $\lambda$ abgesondert wird. Wir gehen aus von der Formel

$$d\,\frac{\sqrt{f(\lambda)}}{\lambda-a}=\frac{du}{(\lambda-a)^2}\left(\frac{1}{2}(\lambda-a)f'(\lambda)-f(\lambda)\right)$$

$$= du\left\{\lambda^2 - \frac{1}{2}a_1\lambda + \frac{a(b+c-a)}{2} - \frac{1}{2}\frac{a(b-a)(c-a)}{\lambda-a}\right\},$$

woraus folgt:

$$(16)\quad \psi(u) - \psi\left(\frac{\omega_1}{2}\right) = \frac{\sqrt{f(\lambda)}}{\lambda-a} - \frac{a(b+c-a)}{2}\left(u - \frac{\omega_1}{2}\right)$$

$$+ \frac{a(b-a)(c-a)}{2}\int\limits_{\frac{1}{2}\omega_1}^{u}\frac{du}{\lambda-a}.$$

Wenn wir nun nach fallenden Potenzen von $\lambda$ entwickeln, so ist

$$(17)\qquad \frac{\pm\sqrt{f(\lambda)}}{\lambda-a} = \lambda - \frac{b+c-a}{2}\cdots$$

Geht man im Periodenparallelogramm von $d$ nach $\alpha$ und von $d$ nach $\beta$, so erkennt man nach (8), dass in (17) das obere Zeichen in der Umgebung von $\alpha$, das untere in der Umgebung von $\beta$ gilt, und daraus ergiebt sich nach (12) und (16) die Summe der Residuen von $\lambda\,\psi(u)$:

$$-2a - \frac{a(b+c-a)}{2}(\beta-\alpha) + \frac{a(b-a)(c-a)}{2}\int\limits_{\alpha}^{\beta}\frac{du}{\lambda-a}$$

$$= -2a - \frac{a}{2}\int\limits_{\alpha}^{\beta}[\lambda(b+c-a) - bc]\frac{du}{\lambda-a}.$$

Das hier vorkommende Integral

$$\int\frac{\lambda(b+c-a)-bc}{\lambda-a}\,du$$

ist eine einwerthige Function von $u$, und daher der Integrationsweg von $\alpha$ nach $\beta$ beliebig. Integrirt man geradlinig und führt die Integrationsvariable $\lambda$ ein, so folgt:

$$(18)\qquad F = 2\pi a + \pi a\int\limits_{-\infty}^{0}\frac{\lambda(b+c-a)-bc}{(\lambda-a)\sqrt{f(\lambda)}}\,d\lambda.$$

Diese Formel ist auch auf das Rotationsellipsoid und die Kugel anwendbar, wobei das Integral ausführbar wird. Die Transformation auf die Legendre'sche Normalform führt zu dem gewöhnlichen Ausdruck.

## §. 52. Theorie der Rotation eines Körpers um seinen Schwerpunkt.

Die Bewegung eines starren Körpers um einen festen Punkt wird analytisch dargestellt durch die gegenseitige Lage zweier rechtwinkeliger Coordinatensysteme mit demselben Anfangspunkte, deren eines im Raume fest ist, während das andere mit dem bewegten Körper in fester Verbindung gedacht wird. Bezeichnen wir die Coordinaten irgend eines Punktes in Bezug auf das erste System mit $x$, $y$, $z$, auf das zweite mit $\xi$, $\eta$, $\zeta$, so bestehen die Relationen

$$(1) \qquad \begin{aligned} x &= a\,\xi + b\,\eta + c\,\zeta \\ y &= a'\,\xi + b'\,\eta + c'\,\zeta \\ z &= a''\,\xi + b''\,\eta + c''\,\zeta \end{aligned}$$

und die Bewegung ist bestimmt, sobald die neun Coëfficienten

$$(2) \qquad \begin{matrix} a, & b, & c \\ a', & b', & c' \\ a'', & b'', & c'', \end{matrix}$$

zwischen welchen die sechs bekannten Relationen

$$(3) \qquad \begin{aligned} a^2 + b^2 + c^2 &= 1, & a'\,a'' + b'\,b'' + c'\,c'' &= 0 \\ a'^2 + b'^2 + c'^2 &= 1, & a''\,a + b''\,b + c''\,c &= 0 \\ a''^2 + b''^2 + c''^2 &= 1, & a\,a' + b\,b' + c\,c' &= 0 \end{aligned}$$

stattfinden, als Functionen der Zeit $t$ gegeben sind. Hierin sind $a$, $b$, $c$ die Richtungscosinus der $x$-Achse gegen die Achsen $\xi$, $\eta$, $\zeta$, und entsprechend die übrigen. Wenn $p$, $q$, $r$ die Componenten der Rotationsgeschwindigkeit nach den Achsen $\xi$, $\eta$, $\zeta$ bedeuten, so bestehen die aus der Mechanik bekannten Gleichungen

$$(4) \qquad \begin{aligned} \frac{da}{dt} &= b\,r - c\,q \\ \frac{db}{dt} &= c\,p - a\,r \\ \frac{dc}{dt} &= a\,q - b\,p, \end{aligned}$$

welche gültig bleiben, wenn $a$, $b$, $c$ durch jedes der drei Systeme (2) ersetzt wird, so dass durch (4) neun Gleichungen dargestellt sind. Nehmen wir an, dass der feste Punkt der Schwerpunkt sei und ausser der Schwerkraft keine weiteren Kräfte auf den Körper wirken, so bestehen für die drei Grössen $p$, $q$, $r$, wie die Mechanik lehrt, die Differentialgleichungen

$$(5)\qquad \begin{aligned} A\frac{dp}{dt} &= (B - C)\,qr \\ B\frac{dq}{dt} &= (C - A)\,rp \\ C\frac{dr}{dt} &= (A - B)\,pq, \end{aligned}$$

vorausgesetzt, dass die Achsen $\xi$, $\eta$, $\zeta$ die Hauptträgheitsachsen des Körpers und dass $A$, $B$, $C$ die Hauptträgheitsmomente sind.

Hat man durch Integration von (5) $p$, $q$, $r$ gefunden, so hat man, um die drei Systeme (2) zu finden, noch drei particulare Lösungen des Systems linearer Differentialgleichungen (4) zu bestimmen.

Nach den allgemeinen mechanischen Principien kennen wir vier Integrale, nämlich die drei Flächensätze und den Satz von der Erhaltung der lebendigen Kraft, wodurch nach dem Satz vom letzten Multiplicator das Problem auf Quadraturen zurückführbar ist.

Nach den drei ersteren Integralen sind die über sämmtliche Massenpunkte $m$ des Körpers ausgedehnten Summen

$$\Sigma m\left(y\frac{dz}{dt} - z\frac{dy}{dt}\right),\qquad \Sigma m\left(z\frac{dx}{dt} - x\frac{dz}{dt}\right),$$
$$\Sigma m\left(x\frac{dy}{dt} - y\frac{dx}{dt}\right)$$

Constanten gleich, von denen wir zwei, etwa die beiden ersten, durch Verfügung über die Lage des Coordinatensystems $x$, $y$, $z$ gleich Null annehmen können. Bezeichnen wir die dritte Constante, die wir als positiv voraussetzen, mit $l$, so werden diese Gleichungen

$$(6)\qquad \begin{aligned} Apa + Bqb + Crc &= 0 \\ Apa' + Bqb' + Crc' &= 0 \\ Apa'' + Bqb'' + Crc'' &= l, \end{aligned}$$

und hieraus durch Auflösung nach $Ap$, $Bq$, $Cr$, wenn wir statt der Constanten $A$, $B$, $C$ die Constanten

$$\alpha = \frac{l}{A}, \qquad \beta = \frac{l}{B}, \qquad \gamma = \frac{l}{C}\,^{1)}$$

einführen:

$$(7) \qquad p = \alpha a'', \qquad q = \beta b'', \qquad r = \gamma c''.$$

Der Satz von der Erhaltung der lebendigen Kraft lautet, wenn $h$ die Constante der Integration ist:

$$(8) \qquad A p^2 + B q^2 + C r^2 = h.$$

Führen wir noch für $h$ die Constante

$$\delta = \frac{h}{l}$$

ein, so können wir (6) und (8) in die Form setzen:

$$\frac{p^2}{\alpha^2} + \frac{q^2}{\beta^2} + \frac{r^2}{\gamma^2} = 1$$

$$\frac{p^2}{\alpha} + \frac{q^2}{\beta} + \frac{r^2}{\gamma} = \delta,$$

woraus:

$$(9) \qquad \frac{(\alpha - \delta) p^2}{\alpha^2} + \frac{(\beta - \delta) q^2}{\beta^2} + \frac{(\gamma - \delta) r^2}{\gamma^2} = 0.$$

Hierin sind $p, q, r$ den Richtungscosinus der augenblicklichen Drehungsachse proportional und (9) ist daher die Gleichung des Kegels zweiter Ordnung, den diese Linie in dem Körper beschreibt. Es folgt aus (9), dass bei einer reellen Bewegung $\delta$ zwischen der grössten und der kleinsten der drei Grössen $\alpha, \beta, \gamma$ liegen muss und wir können danach, wenn wir annehmen, dass $\beta$ die mittlere dieser drei Grössen sei, zwei Fälle der Bewegung unterscheiden:

I. $\alpha > \beta > \delta > \gamma$

II. $\alpha < \beta < \delta < \gamma$,

so dass immer die $\zeta$-Achse die Achse dieses Kegels ist; im ersten Falle aber ist sie die Achse des grössten, im zweiten die des kleinsten Trägheitsmomentes.

Nach diesen Annahmen kann im Verlaufe der Bewegung $p$ und $q$ verschwinden, nicht aber $r$. Wenn wir vermittelst (7) $p, q, r$ eliminiren, so ergeben die Gleichungen (4) und (9):

---

1) Wir folgen der Bezeichnung, die Hermite in seiner Arbeit: „Sur quelques applications des fonctions elliptiques", Paris 1885, gebraucht.

$$(10)\qquad \begin{aligned} \frac{d\,a''}{d\,t} &= (\gamma - \beta)\,b''c'' \\ \frac{d\,b''}{d\,t} &= (\alpha - \gamma)\,c''a'' \\ \frac{d\,c''}{d\,t} &= (\beta - \alpha)\,a''b''. \end{aligned}$$

$$(11)\qquad \begin{aligned} \frac{d\,a}{d\,t} &= \gamma\,b\,c'' - \beta\,c\,b'' \\ \frac{d\,b}{d\,t} &= \alpha\,c\,a'' - \gamma\,a\,c'' \\ \frac{d\,c}{d\,t} &= \beta\,a\,b'' - \alpha\,b\,a''. \end{aligned}$$

$$(12)\qquad (\alpha - \delta)\,a''^2 + (\beta - \delta)\,b''^2 + (\gamma - \delta)\,c''^2 = 0.$$

Dazu kommt die Gleichung:

$$(13)\qquad a''^2 + b''^2 + c''^2 = 1$$

und (12) und (13) sind zwei Integrale von (10).

Haben wir (10) integrirt, so sind von (11) ausser der evidenten Lösung $a = a''$, $b = b''$, $c = c''$ noch zwei particulare Lösungen zu ermitteln.

Die Aehnlichkeit des Systems (10) mit dem System der elliptischen Differentialgleichungen (§. 46) fällt in die Augen. Um beide Systeme auf einander zurückzuführen, setzen wir:

$$(14)\qquad \begin{gathered} u = n\,(t - t_0) \\ a'' = \lambda\,\mathrm{cn}\,u, \qquad b'' = \mu\,\mathrm{sn}\,u, \qquad c'' = \nu\,\mathrm{dn}\,u, \end{gathered}$$

wo über die Constanten $\lambda$, $\mu$, $\nu$, $n$ und den Modul $\varkappa$ noch verfügt werden kann.

Die Gleichungen (10) werden befriedigt, wenn

$$(15)\qquad \begin{aligned} n &= (\beta - \gamma)\,\frac{\mu\,\nu}{\lambda} \\ n &= (\alpha - \gamma)\,\frac{\nu\,\lambda}{\mu} \\ \varkappa^2\,n &= (\alpha - \beta)\,\frac{\lambda\,\mu}{\nu}, \end{aligned}$$

woraus:

$$(16)\qquad \lambda^2 + \varkappa^2\,\nu^2 = \mu^2.$$

$t_0$ ist so gewählt, dass $b''$ und also auch $q$ für $t = t_0$ verschwindet, also die momentane Drehungsachse in der $\xi$, $\zeta$-Ebene liegt. $\lambda$, $\nu$ sind die Werthe von $a''$, $c''$ für $t = t_0$ und können ohne Beschränkung der Allgemeinheit positiv vorausgesetzt werden. Für sie ergeben sich aus (12), (13) die beiden Gleichungen:

$$\begin{aligned} \lambda^2(\alpha - \delta) + \nu^2(\gamma - \delta) &= 0 \\ \lambda^2 \quad + \nu^2 \quad &= 1, \end{aligned}$$

also

$$(17) \qquad \lambda = \sqrt{\frac{\gamma - \delta}{\gamma - \alpha}}, \qquad \nu = \sqrt{\frac{\delta - \alpha}{\gamma - \alpha}}.$$

Eine Vorzeichenänderung von $n$ bedingt nur eine Vorzeichenänderung von $u$ und daher kann auch $n$ positiv vorausgesetzt werden und die Gleichungen (15) zeigen dann, dass $\mu$ positiv ist im Falle I, negativ im Falle II, und es folgt aus (15):

$$(18) \quad \varkappa^2 = \frac{(\beta - \alpha)(\gamma - \delta)}{(\gamma - \beta)(\delta - \alpha)}, \quad \varkappa'^2 = 1 - \varkappa^2 = \frac{(\delta - \beta)(\gamma - \alpha)}{(\gamma - \beta)(\delta - \alpha)},$$

so dass $\varkappa^2$, $\varkappa'^2$ positive echte Brüche sind, ferner

$$(19) \qquad n = \sqrt{(\gamma - \beta)(\delta - \alpha)}, \qquad \mu = \pm\sqrt{\frac{\gamma - \delta}{\gamma - \beta}},$$

wo das obere oder untere Zeichen die Fälle I, II unterscheidet.

Nachdem so $a''$, $b''$, $c''$ vollständig bestimmt sind, suchen wir noch die beiden Systeme von Particularlösungen von (11). Wir suchen aber nur solche Lösungen $a$, $b$, $c$, welche der in (3) enthaltenen Bedingung

$$a a'' + b b'' + c c'' = 0$$

genügen.

Setzen wir daher

$$(20) \qquad a = W U, \qquad b = W V, \qquad c = W,$$

so müssen die beiden Functionen $U$, $V$ die Bedingung erfüllen:

$$(21) \qquad U a'' + V b'' + c'' = 0,$$

und die Einführung von (20) in die Differentialgleichungen (11) ergiebt:

$$(22) \qquad \begin{aligned} U \frac{d \log W}{d t} + \frac{d U}{d t} &= \gamma c'' V - \beta b'' \\ V \frac{d \log W}{d t} + \frac{d V}{d t} &= - \gamma c'' U + \alpha a'', \end{aligned}$$

$$(23) \qquad \frac{d \log W}{d t} = \beta b'' U - \alpha a'' V.$$

Eliminiren wir $W$, so ergeben sich für $U$, $V$ die Gleichungen

$$(24)\quad \begin{aligned} \frac{dU}{dt} &= -\beta b'' U^2 + \alpha a'' VU + \gamma c'' V - \beta b'' \\ \frac{dV}{dt} &= -\beta b'' UV + \alpha a'' V^2 - \gamma c'' U + \alpha a'', \end{aligned}$$

und daraus

$$U \frac{dU}{dt} + V \frac{dV}{dt} = (\alpha a'' V - \beta b'' U)(U^2 + V^2 + 1).$$

Diese Gleichung ist befriedigt, wenn

$$(25)\qquad U^2 + V^2 + 1 = 0$$

gesetzt wird, und da wir nur eine particulare Lösung suchen, so genügt diese Annahme.

Durch (21) und (25) sind aber die Gleichungen (24) befriedigt und wir können $U$, $V$ daraus bestimmen. Wir setzen, um (25) identisch zu befriedigen, indem wir einen noch näher zu bestimmenden Parameter $\omega$ einführen:

$$(26)\qquad U = i \operatorname{sn}(u + i\omega), \qquad V = \mp i \operatorname{cn}(u + i\omega),$$

was, in (21) eingeführt, nach (14) ergiebt:

$$(27)\quad i\lambda \operatorname{sn}(u + i\omega) \operatorname{cn} u \mp i\mu \operatorname{cn}(u + i\omega) \operatorname{sn} u + \nu \operatorname{dn} u = 0.$$

Diese Formel ist aber nach dem Additionstheorem der elliptischen Functionen [§. 39, (17)] befriedigt, wenn

$$\frac{\mu}{\lambda} = \pm \operatorname{dn} i\omega, \qquad \frac{i\nu}{\lambda} = \operatorname{sn} i\omega$$

gesetzt wird, zwei Gleichungen, von denen in der That nach (16) die eine aus der anderen folgt, und die drei Constanten $\lambda$, $\mu$, $\nu$ drücken sich in folgender Weise durch $\omega$ aus (§. 40, 5):

$$(28)\quad \begin{aligned} \lambda &= \operatorname{cn}(\omega, \varkappa') &&= \frac{1}{\operatorname{cn}(i\omega, \varkappa)} \\ \mu &= \pm \operatorname{dn}(\omega, \varkappa') &&= \pm \frac{\operatorname{dn}(i\omega, \varkappa)}{\operatorname{cn}(i\omega, \varkappa)} \\ \nu &= \operatorname{sn}(\omega, \varkappa') &&= -\frac{i \operatorname{sn}(i\omega, \varkappa)}{\operatorname{cn}(i\omega, \varkappa)}. \end{aligned}$$

Es kann also, wenn im Falle I das obere, im Falle II das untere Zeichen gilt, $\omega$ als eine reelle Constante angenommen werden, die zwischen 0 und $K'$ liegt.

Ehe wir zur Bestimmung von $W$ übergehen, leiten wir aus (14), (26), (28) nach den gefundenen Ausdrücken aus dem Additionstheorem [§. 39, (17)] noch die Formel ab:

$$Va'' - Ub'' = \mp i,$$

wodurch (23) die Form erhält:

$$\begin{aligned}\frac{d \log W}{dt} \mp i\alpha &= (\beta - \alpha) b'' U \\ &= i(\beta - \alpha)\, \mu \operatorname{sn} u \operatorname{sn}(u + i\omega) \\ &= \frac{(\beta - \alpha)\lambda\mu}{\nu} \operatorname{sn} u \operatorname{sn} i\omega \operatorname{sn}(u + i\omega),\end{aligned}$$

also nach (15):

$$\frac{d \log W}{dt} = \pm i\alpha - n\varkappa^2 \operatorname{sn} u \operatorname{sn} i\omega \operatorname{sn}(u + i\omega). \tag{29}$$

Nun ist aber nach dem Additionstheorem der Transcendenten zweiter Gattung (§. 42):

$$\varkappa^2 \operatorname{sn} u \operatorname{sn} i\omega \operatorname{sn}(u + i\omega) = \frac{\Theta'(u)}{\Theta(u)} + \frac{\Theta'(i\omega)}{\Theta(i\omega)} - \frac{\Theta'(u + i\omega)}{\Theta(u + i\omega)}$$

und wenn wir zur Abkürzung

$$\pm \alpha - n \frac{\Theta'(i\omega)}{i\,\Theta(i\omega)} = \varepsilon \tag{30}$$

setzen, was eine reelle Constante ist, so folgt durch Integration von (29) bei geeigneter Bestimmung der Integrationsconstanten

$$W = -i e^{i\varepsilon t} \frac{\Theta(u + i\omega)}{\Theta(u)}. \tag{31}$$

Hierdurch sind die gesuchten particularen Lösungen des Systems (11) gefunden in der Form:

$$e^{i\varepsilon t} \frac{\Theta(u + i\omega)}{\Theta(u)} \operatorname{sn}(u + i\omega),$$

$$\mp e^{i\varepsilon t} \frac{\Theta(u + i\omega)}{\Theta(u)} \operatorname{cn}(u + i\omega),$$

$$- i e^{i\varepsilon t} \frac{\Theta(u + i\omega)}{\Theta(u)},$$

und ein zweites System particularer Lösungen erhält man durch Vertauschung von $i$ mit $-i$.

Die Summe der Quadrate dieser drei Functionen verschwindet identisch, und wenn wir also setzen:

$$\begin{aligned} a + ia' &= \phantom{\mp i} M e^{i\varepsilon(t-\tau)} \frac{\Theta(u + i\omega)}{\Theta(u)} \operatorname{sn}(u + i\omega) \\ b + ib' &= \mp M e^{i\varepsilon(t-\tau)} \frac{\Theta(u + i\omega)}{\Theta(u)} \operatorname{cn}(u + i\omega) \\ c + ic' &= - i M e^{i\varepsilon(t-\tau)} \frac{\Theta(u + i\omega)}{\Theta(u)} \end{aligned} \tag{32}$$

wenn $M$ und $\tau$ reelle Constanten bedeuten, so genügen die hieraus bestimmten reellen Werthe $a$, $a'$, $b$, $b'$ $c$, $c'$ den Bedingungen

$$a^2 + b^2 + c^2 = a'^2 + b'^2 + c'^2, \qquad a a' + b b' + c c' = 0,$$

und es bleibt nur noch übrig, die Constante $M$ so zu bestimmen, dass

$$a^2 + b^2 + c^2 = 1$$

wird; denn die Constante $\tau$ bleibt der Natur der Sache nach unbestimmt; sie ändert sich mit einer Drehung des Coordinatensystems $x$, $y$, $z$ um die $z$-Achse.

Um nun $M$ zu bestimmen, ersetzen wir in (32) $i$ durch $-i$ und bilden die Summe $(a + i a')(a - i a') + (b + i b')(b - i b') + (c + i c')(c - i c') = 2$.

Dadurch ergiebt sich:

$$2 = M^2 \frac{\Theta(u + i\omega)\,\Theta(u - i\omega)}{\Theta^2(u)} \times$$

$$[\operatorname{sn}(u + i\omega)\operatorname{sn}(u - i\omega) + \operatorname{cn}(u + i\omega)\operatorname{cn}(u - i\omega) + 1],$$

und dies giebt mit Benutzung der Additionstheoreme §. 38 (11), §. 39 (13), (14):

$$M = \frac{\Theta(0)}{\Theta(i\omega)}\,\frac{1}{\operatorname{cn} i\omega}.$$

Danach erhalten wir also folgende Resultate:

$$a + i a' = \quad e^{i\varepsilon(t-\tau)}\,\frac{\Theta(0)\,\Theta(u + i\omega)}{\Theta(i\omega)\,\Theta(u)}\,\frac{\operatorname{sn}(u + i\omega)}{\operatorname{cn} i\omega},$$

$$a'' = \frac{\operatorname{cn} u}{\operatorname{cn} i\omega}$$

$$(33) \quad b + i b' = \mp e^{i\varepsilon(t-\tau)}\,\frac{\Theta(0)\,\Theta(u + i\omega)}{\Theta(i\omega)\,\Theta(u)}\,\frac{\operatorname{cn}(u + i\omega)}{\operatorname{cn} i\omega},$$

$$b'' = \pm\,\frac{\operatorname{dn} i\omega \operatorname{sn} u}{\operatorname{cn} i\omega}$$

$$c + i c' = - i\, e^{i\varepsilon(t-\tau)}\,\frac{\Theta(0)\,\Theta(u + i\omega)}{\Theta(i\omega)\,\Theta(u)}\,\frac{1}{\operatorname{cn} i\omega},$$

$$c'' = - i\,\frac{\operatorname{sn} i\omega \operatorname{dn} u}{\operatorname{cn} i\omega}.$$

Bezeichnen wir mit $P$, $Q$, $R$ die Componenten der momentanen Drehung nach den Achsen der $x$, $y$, $z$, also:

$$\begin{aligned} P &= a\,p + b\,q + c\,r \\ Q &= a'\,p + b'\,q + c'\,r \\ R &= a''p + b''q + c''r, \end{aligned}$$

so erhält man $R = \delta$, also constant, und aus den beiden ersteren Gleichungen ergiebt sich

$$\begin{gathered} P + Qi = \\ (a + ia')p + (b + ib')q + (c + ic')r = \\ \alpha(a + ia')a'' + \beta(b + ib')b'' + \gamma(c + ic')c'' = \\ (\alpha - \gamma)(a + ia')a'' + (\beta - \gamma)(b + ib')b''. \end{gathered}$$

Es folgt aber aus (15) und (28):

$$\begin{aligned} \alpha - \gamma &= \pm\, i n \frac{\operatorname{dn} i\omega \operatorname{cn} i\omega}{\operatorname{sn} i\omega} \\ \beta - \gamma &= \pm\, i n \frac{\operatorname{cn} i\omega}{\operatorname{dn} i\omega \operatorname{cn} i\omega}, \end{aligned}$$

also nach (33):

$$\begin{gathered} P + iQ = \\ \pm\, i n e^{i\varepsilon(t-\tau)} \frac{\Theta(0)\,\Theta(u + i\omega)}{\Theta(i\omega)\,\Theta(u)} \frac{\operatorname{sn}(u + i\omega) \operatorname{cn} u \operatorname{dn} i\omega - \operatorname{sn} u \operatorname{cn}(u + i\omega)}{\operatorname{cn} i\omega \,.\, \operatorname{sn} i\omega}. \end{gathered}$$

Wendet man im Zähler dieses Ausdruckes das Additionstheorem an, indem man in der dritten Formel (17) des §. 39 $u$ durch $u + i\omega$ und $v$ durch $- i\omega$ ersetzt, so erhält man schliesslich:

$$P + Qi = \pm\, i n e^{i\varepsilon(t-\tau)} \frac{\Theta(0)\,\Theta(u + i\omega)}{\Theta(i\omega)\,\Theta(u)} \frac{\operatorname{dn}(u + i\omega)}{\operatorname{cn} i\omega}.$$

# II.

# ALGEBRAISCHER THEIL.

## Siebenter Abschnitt.

# Hülfssätze aus der Algebra.

## §. 53. Endliche Gruppen.

Wir geben hier, zur Erleichterung des Verständnisses einen Ueberblick über den Theil der Algebra, auf welchen sich die weitere Theorie der elliptischen Functionen und ihre Anwendung zu stützen hat. Wir beschränken uns auf das für uns Nothwendige und verweisen den Leser bezüglich einer breiteren Ausführung auf die algebraischen Lehrbücher, besonders auf Serret, „Cours d'algèbre supérieure“ (deutsch von Wertheim).

Es ist uns bereits oben, bei der Zusammensetzung der Transformationen, der Begriff der Gruppe begegnet. Es ist zunächst erforderlich, diesen Begriff etwas schärfer zu kennzeichnen.

1. Definition. Ein System $\mathfrak{G}$ von Elementen irgend welcher Art, $A_1$, $A_2$, $A_3$ . . ., heisst eine Gruppe, wenn es den folgenden Bedingungen genügt:

I. Durch irgend eine Vorschrift, welche als Composition oder Multiplication bezeichnet wird, leitet man in eindeutiger Weise aus zwei Elementen ein neues Element desselben Systems her, in Zeichen:

$$A_i A_k = A_h.$$

II. Es ist stets

$$(A_i A_k) A_h = A_i (A_k A_h) = A_i A_k A_h$$

(associatives Gesetz, das commutative Gesetz der Multiplication wird im Allgemeinen nicht vorausgesetzt).

III. Aus $A A_i = A A_k$ und aus $A_i A = A_k A$ folgt $A_i = A_k$.

Besteht das System aus einer endlichen Zahl von Elementen, so heisst die Gruppe eine endliche, und die Anzahl der Elemente heisst der Grad der Gruppe. Die Gruppe der Transformationen der $\vartheta$-Functionen war eine unendliche. Hier beschäftigen wir uns nur mit endlichen Gruppen.

Als Beispiel einer endlichen Gruppe mag die Gruppe der Vertauschungen (Substitutionen) von $n$ Elementen dienen. Die Operation $A$ möge darin bestehen, dass an Stelle von $n$ Elementen $1, 2, \ldots n$ dieselben Elemente in einer anderen Ordnung $a_1, a_2, \ldots a_n$ gesetzt werden, was wir so ausdrücken:

$$A = \begin{pmatrix} 1, & 2, & \ldots & n \\ a_1, & a_2, & \ldots & a_n \end{pmatrix}.$$

Ist nun

$$B = \begin{pmatrix} 1, & 2, & \ldots & n \\ b_1, & b_2, & \ldots & b_n \end{pmatrix}$$

eine Operation derselben Art, so ist, wenn erst $A$, dann $B$ ausgeführt wird, dies gleichbedeutend mit:

$$A\,B = \begin{pmatrix} 1, & 2, & \ldots & n \\ b_{a_1}, & b_{a_2}, & \ldots & b_{a_n} \end{pmatrix}.$$

Hieraus ersieht man leicht, dass auch II, III erfüllt sind, und diese Vertauschungen bilden also eine Gruppe. Da die Anzahl aller möglichen Vertauschungen von $n$ Elementen $\Pi(n) = 1.\,2.\ldots n$ beträgt, so ist diese Gruppe eine endliche. $B\,A$ ist hier im Allgemeinen von $A\,B$ verschieden.

2. In jeder endlichen Gruppe $\mathfrak{G}$:

$$(\mathfrak{G}) \qquad A_1, A_2, \ldots A_n$$

giebt es ein und nur ein Element $A^0$, welches der Bedingung genügt, dass für jedes $A_i$:

$$A_i\,A^0 = A^0\,A_i = A_i.$$

Ist nämlich $A$ irgend ein Element in $\mathfrak{G}$, so sind nach III die Elemente

$$A\,A_{.}, A\,A_2, \ldots A\,A_n$$

von einander verschieden und müssen demnach die ganze Gruppe $\mathfrak{G}$ erschöpfen. Es muss daher auch $A$ darunter vorkommen; sei also

$$A = A\,A^0.$$

Daraus folgt für jedes beliebige $A_i$:

$$A_i\,A = A_i\,A\,A^0,$$

oder, da $A_i\,A$ zugleich mit $A_i$ die ganze Gruppe durchläuft, indem man $A_i$ an Stelle von $A_i\,A$ setzt:

$$(1) \qquad A_i = A_i A^0,$$

und dass es nur ein solches Element giebt, ist eine Folge von III.

Ebenso schliesst man auf die Existenz eines Elementes $A_0$, für welches

$$(2) \qquad A_i = A_0 A_i$$

und aus (1) und (2) folgt:

$$A^0 = A_0 = A_0 A^0,$$

also die Identität von $A_0$ und $A^0$.

Zu jedem Element $A$ kann man ein anderes $A^{-1}$ bestimmen, so dass

$$(3) \qquad A A^{-1} = A^{-1} A = A^0.$$

Denn zunächst folgt daraus, dass $A A_i$ und $A_i A$ zugleich mit $A_i$ die vollständige Gruppe durchlaufen, die Existenz eines Elementes $A^{-1}$, für welches

$$A A^{-1} = A^0;$$

daraus folgt dann weiter:

$$A^{-1} A A^{-1} = A^{-1} A^0 = A^0 A^{-1} = A^{-1},$$

also nach III:

$$A^{-1} A = A^0.$$

Damit ist die Bedeutung der Potenzen $A^m$ von $A$ mit positiven und negativen Exponenten gegeben als wiederholte Zusammensetzung des Elementes $A$ oder $A^{-1}$ mit sich selbst. Die Potenzen werden multiplicirt, indem man ihre Exponenten addirt. Das Element $A^0$ heisst das Hauptelement und wird als Einheit in der Gruppe mit 1 bezeichnet.

3. Wenn die Elemente $B_1, B_2, \ldots B_\nu$ einer Gruppe $\mathfrak{H}$ sämmtlich unter den Elementen der Gruppe $\mathfrak{G}$ enthalten sind, so heisst $\mathfrak{H}$ ein Theiler oder Divisor von $\mathfrak{G}$.

Der Grad $\nu$ eines Divisors von $\mathfrak{G}$ ist immer ein Theiler des Grades $n$ von $\mathfrak{G}$.

Denn wenn die Gruppe

$$\mathfrak{H} = B_1, B_2, \ldots B_\nu$$

nicht die ganze Gruppe $\mathfrak{G}$ erschöpft, und also nicht $\nu = n$ ist, so wähle man ein nicht in $\mathfrak{H}$ enthaltenes Element $A$. Es sind dann die Elemente des Systems

$$\mathfrak{H} A = B_1 A, B_2 A, \ldots B_\nu A$$

sowohl unter einander als von denen in $\mathfrak{H}$ verschieden. Ist damit $\mathfrak{G}$ noch nicht erschöpft, so wähle man $A'$, so dass es weder in $\mathfrak{H}$ noch in $\mathfrak{H}A$ enthalten ist, und bilde

$$\mathfrak{H}A' = B_1 A',\ B_2 A',\ \ldots\ B_\nu A'.$$

Diese sind unter sich sowohl als von denen in $\mathfrak{H}$ und $\mathfrak{H}A$ verschieden; und so kann man fortfahren, bis die ganze Gruppe $\mathfrak{G}$ in Reihen $\mathfrak{H}$, $\mathfrak{H}A$, $\mathfrak{H}A'$ ... von je $\nu$ Elementen zerlegt ist. Ist $p$ die Anzahl dieser Reihen, so ist

$$n = \nu p.$$

Die Zahl $p$ wollen wir den Index des Theilers $\mathfrak{H}$ nennen.

Die Reihe $\mathfrak{H}A$ bildet keine Gruppe, wohl aber das System

$$A^{-1}\mathfrak{H}A = A^{-1}B_1 A,\ A^{-1}B_2 A,\ \ldots\ A^{-1}B_\nu A.$$

Alle auf diese Weise aus einem und demselben $\mathfrak{H}$ abgeleiteten Gruppen $A^{-1}\mathfrak{H}A$ heissen conjugirte Theiler von $\mathfrak{G}$.

Ein Theiler von $\mathfrak{G}$, der mit allen seinen conjugirten Theilern identisch ist, heisst (nach Galois) ein eigentlicher Theiler von $\mathfrak{G}$.

Nennen wir den Inbegriff aller derjenigen Elemente, welche zwei oder mehreren Gruppen gemeinsam sind, welcher stets eine Gruppe bildet, ihren grössten gemeinsamen Theiler, so ergiebt sich, dass der grösste gemeinsame Theiler aller mit einander conjugirten Divisoren einer Gruppe $\mathfrak{G}$ stets ein eigentlicher Divisor von $\mathfrak{G}$ ist.

4. Ist $\mathfrak{H}$ ein eigentlicher Divisor von $\mathfrak{G}$ vom Index $p$ und $\mathfrak{G}'$ ein beliebiger Divisor von $\mathfrak{G}$, so ist der grösste gemeinschaftliche Theiler $\mathfrak{H}'$ von $\mathfrak{G}'$ und $\mathfrak{H}$ ein eigentlicher Divisor von $\mathfrak{G}'$, dessen Index $q$ ein Theiler von $p$ ist.

Um dies einzusehen, zerlege man $\mathfrak{G}'$ in die Reihen:

$$\mathfrak{G}' = \mathfrak{H}',\ \mathfrak{H}' S_1,\ \ldots\ \mathfrak{H}' S_{q-1},$$

worin die $S_i$ in $\mathfrak{G}'$, aber nicht in $\mathfrak{H}'$ und also auch nicht in $\mathfrak{H}$ enthaltene Elemente sind. Da $\mathfrak{H}$ ein eigentlicher Divisor von $\mathfrak{G}$ ist, so ist $S_i^{-1}\mathfrak{H}' S_i$ in $\mathfrak{H}$ und in $\mathfrak{G}'$, also auch in $\mathfrak{H}'$ enthalten, und da $S_i^{-1}\mathfrak{H}' S_i$ auch von gleichem Grade mit $\mathfrak{H}'$ ist, so ist es mit $\mathfrak{H}'$ identisch, d. h. $\mathfrak{H}'$ ist ein eigentlicher Divisor von $\mathfrak{G}'$. Daraus folgt aber, da $\mathfrak{G}'$ eine Gruppe ist, dass, wenn $S_1$, $S_2$ irgend zwei der Elemente $S$ sind, ein drittes dieser Elemente, $S_3$, und ein Element $H'$ aus $\mathfrak{H}'$ gefunden werden kann, so dass

$$S_1 S_2 = H' S_3.$$

Hieraus schliesst man weiter mit Hülfe der Relation:

$$S_i \mathfrak{H} = \mathfrak{H} S_i,$$

dass der Inbegriff der Elemente:

$$\mathfrak{L} = \mathfrak{H}, \mathfrak{H} S_1, \ldots \mathfrak{H} S_{q-1}$$

eine (in $\mathfrak{G}$ enthaltene) Gruppe bildet. Denn wenn $H_1 S_1$, $H_2 S_2$ irgend zwei Elemente in $\mathfrak{L}$ sind, so kann man $H_3$ in $\mathfrak{H}$ so bestimmen, dass

$$H_1 S_1 H_2 S_2 = H_1 H_3 S_1 S_2 = H_1 H_3 H' S_3$$

wird, und also ebenfalls in $\mathfrak{L}$ enthalten ist. Ist $\nu$ der Grad von $\mathfrak{H}$, so ist $\nu p$ der Grad von $\mathfrak{G}$ und $\nu q$ der Grad von $\mathfrak{L}$, also $\nu p$ durch $\nu q$ und folglich $p$ durch $q$ theilbar.

5. Ist $S$ ein beliebiges Element einer Gruppe $\mathfrak{G}$, deren Grad $n$ ist, so giebt es, da die Anzahl der verschiedenen Elemente endlich ist, unter den auf einander folgenden Potenzen von $S$ gewiss zwei identische, etwa $S^{\nu}$ und $S^{\nu+q}$, so dass $S^q = 1$ für irgend ein von Null verschiedenes $q$. Ist $q$ die kleinste positive Zahl, welche dieser Bedingung genügt, so heisst $q$ der Grad des Elementes $S$, und jeder andere Exponent $\mu$, für welchen $S^{\mu} = 1$ ist, muss durch $q$ theilbar sein; denn ist $q'$ der Rest von $\mu$ bei der Division mit $q$, so ist auch $S^{q'} = 1$, und folglich muss $q'$, welches kleiner als $q$ ist, Null sein. Da die Potenzen von $S$ eine in $\mathfrak{G}$ enthaltene Gruppe bilden, so ist (nach 3.) der Grad eines jeden Elementes $S$ ein Theiler des Grades der Gruppe, und es ist $S^n = 1$ für jedes Element $S$ in $\mathfrak{G}$.

## §. 54. Abel'sche Gruppen.

Wenn in einer Gruppe $\mathfrak{G}$ für je zwei Elemente $A$, $B$ das commutative Gesetz gilt:

$$AB = BA,$$

so heisst die Gruppe eine **Abel'sche**.

Eine Abel'sche Gruppe hat nur eigentliche Theiler und jeder ihrer Theiler ist selbst eine Abel'sche Gruppe.

Wir wollen hier nur die eine fundamentale Eigenschaft der Abel'schen Gruppen beweisen, dass sie sich durch eine Basis darstellen lassen. Darunter ist zu verstehen:

In einer Abel'schen Gruppe vom Grade $n$ kann man die Elemente $A$, $B$, $C$ ... von den Graden $a$, $b$, $c$ ... so auswählen, dass in der Form

$$S = A^\alpha B^\beta C^\gamma \ldots$$

jedes Element von $\mathfrak{G}$ und jedes nur einmal enthalten ist, wenn $\alpha$, $\beta$, $\gamma$ ... vollständige Restsysteme nach den Moduln $a$, $b$, $c$ ... durchlaufen, so dass

$$n = abc \ldots$$

Dieser Satz wird folgendermaassen bewiesen:

1. Ist $r$ irgend eine im Grade $n$ von $\mathfrak{G}$ aufgehende Primzahl, so giebt es in $\mathfrak{G}$ Elemente, deren Grad durch $r$ theilbar ist.

Bezeichnet man nämlich mit $S_1$, $S_2$ ... $S_n$ die sämmtlichen Elemente von $\mathfrak{G}$ und mit $m_1$, $m_2$ ... $m_n$ ihre Grade, so ist in der Form

$$S = S_1^{\mu_1} S_2^{\mu_2} \ldots S_n^{\mu_n} \tag{1}$$

jedes Element und jedes gleich oft enthalten, wenn $\mu_1$, $\mu_2$ ... $\mu_n$ vollständige Restsysteme nach den Moduln $m_1$, $m_2$ ... $m_n$ durchlaufen. Es lässt sich nämlich jedes Element genau ebenso oft in der Form (1) darstellen, wie sich das Element „1" in dieser Form darstellen lässt. Bezeichnen wir diese Zahl mit $h$, so folgt:

$$m_1 m_2 \ldots m_n = h\,n,$$

also muss unter den Graden $m_1$, $m_2$, ... $m_n$ wenigstens einer durch $r$ theilbar sein, wie z. b. w.

2. Der Grad des Productes aus mehreren Elementen $S_1, S_2$ ... einer Abel'schen Gruppe ist stets ein Theiler des kleinsten gemeinschaftlichen Vielfachen der Grade von $S_1$, $S_2$ ...; denn ist $m$ dies kleinste gemeinschaftliche Vielfache, so ist

$$(S_1 S_2 \ldots)^m = S_1^m S_2^m \ldots = 1,$$

also $m$ durch den Grad von $S_1 S_2$ ... theilbar (5. des vorigen Paragraphen).

3. Ist $n = ab$ und $a$ relativ prim zu $b$, so existiren in $\mathfrak{G}$ genau $a$ Elemente $A$, deren Grad ein Theiler von $a$, und $b$ Elemente $B$, deren Grad ein Theiler von $b$ ist, und in der Form $AB$ sind sämmtliche Elemente von $\mathfrak{G}$ und jedes nur einmal enthalten.

Beweis. Der Inbegriff $\mathfrak{A}$ aller Elemente $A$ bildet wegen 2. eine Abel'sche Gruppe; ebenso der Inbegriff $\mathfrak{B}$ aller Elemente $B$. Sind $a'$, $b'$ die Grade dieser Gruppen, so ist $a'$ relativ prim zu $b$ und $b'$ relativ prim zu $a$; denn ist $r$ eine in $a'$ aufgehende Primzahl, so giebt es nach 1. Elemente in $\mathfrak{A}$, deren Grad durch $r$ theilbar ist und also kann $r$ nicht in $b$ aufgehen.

Bestimmt man nun die ganzen Zahlen $x$, $y$ so, dass

$$ax + by = 1,$$

so ist für ein beliebiges Element $S$:

$$S = S^{ax} S^{by} = BA,$$

da $S^{ax}$ in $\mathfrak{B}$, $S^{by}$ in $\mathfrak{A}$ enthalten ist. Daher lässt sich jedes Element $S$ in der Form $AB$ darstellen. Eine solche Darstellung ist aber auch nur auf eine Art möglich, denn aus $AB = A'B'$ folgt, indem man zur Potenz $by$ erhebt, $A = A'$ und mithin $B = B'$. Demnach ist

$$n = ab = a'b'$$

und folglich, da $a$ mit $b'$ und $b$ mit $a'$ keinen Theiler gemein hat:

$$a = a', \; b = b',$$

wie z. b. w.

4. Hiernach ist unser Satz allgemein bewiesen, wenn er noch für solche Abel'sche Gruppen als richtig erwiesen ist, deren Grad eine Potenz einer Primzahl $p$ ist.

Es sei also jetzt der Grad $n$ der Gruppe eine Potenz der Primzahl $p$ und $A$, $B$, $C$ ... von den Graden $a$, $b$, $c$ ... so ausgewählt, dass in der Form

$$S = A^{\alpha} B^{\beta} C^{\gamma} \ldots \tag{2}$$

jedes Element von $\mathfrak{G}$ überhaupt, wenn auch mehrmals, enthalten ist, wenn die Exponenten $\alpha$, $\beta$, $\gamma$ ... kleiner als $a$, $b$, $c$ ... und nicht negativ angenommen werden. Dies ist stets möglich, da man für $A$, $B$, $C$ ... nöthigenfalls alle Elemente von $\mathfrak{G}$ (mit Ausnahme des Hauptelementes) nehmen kann. Wie in 1. schliesst man, dass in der Form (2) jedes Element gleich oft, etwa $h$ mal, enthalten ist, und es ist

$$hn = abc \ldots$$

Hierin sind $a$, $b$, $c$ ... gleichfalls Potenzen von $p$.

Es sei nun

$$1 = A^{\alpha_0} B^{\beta_0} C^{\gamma_0} \ldots \tag{3}$$

irgend eine Darstellung des Hauptelementes in der Form (2), in welcher nicht alle Exponenten $\alpha_0$, $\beta_0$, $\gamma_0$ ... verschwinden; ferner sei

$$\alpha_0 = a_0 \alpha_1, \quad \beta_0 = b_0 \beta_1, \quad \gamma_0 = c_0 \gamma_1 \ldots,$$

worin $a_0, b_0, c_0 \ldots$ Potenzen von $p$ sind, während $\alpha_1, \beta_1, \gamma_1 \ldots$ durch $p$ untheilbar sind.

Man nehme an, es seien in (3) die $A, B, C \ldots$ so angeordnet, dass $\alpha_0$ von Null verschieden ist, und dass $b_0, c_0 \ldots$ durch $a_0$ theilbar sind. Setzen wir dann:

$$A' = A^{\alpha_1} B^{\frac{b_0}{a_0}\beta_1} C^{\frac{c_0}{a_0}\gamma_1} \ldots,$$

so ist $A'^{a_0} = 1$ und daher der Grad $a'$ von $A'$ ein Theiler von $a_0$, also gewiss kleiner als $a$; da ferner $\alpha_1$ durch $p$ nicht theilbar ist, so kann man $x$ so bestimmen, dass

$$\alpha_1 x \equiv 1 \pmod{a}$$

und daher

$$A = A'^x B^{-\frac{b_0}{a_0}\beta_1 x} C^{-\frac{c_0}{a_0}\gamma_1 x} \ldots,$$

also $A$ und mithin jedes Element $S$ darstellbar in der Form:

$$A'^{\alpha'} B^{\beta'} C^{\gamma'} \ldots$$

Ist $h'$ die Anzahl dieser Darstellungen, so ist

$$h'n = a' b c \ldots$$

und folglich

$$h' < h.$$

Man kann auf diese Weise so lange fortfahren, die Anzahl der Darstellungen zu verkleinern, als diese Anzahl noch grösser als 1 ist, woraus der Beweis des Satzes sich ergiebt.

Wenn die Abel'sche Gruppe durch die Potenzen eines einzigen Elementes sich erschöpfen lässt, wenn sie also aus den Elementen

$$1, A, A^2, \ldots A^{a-1}$$

besteht, so heisst sie regulär.

## §. 55. Algebraische Grundbegriffe.

1. Rationalitätsbereich. Wenn von Eigenschaften algebraischer Grössen die Rede ist, so ist es vor Allem erforderlich, eine Festsetzung darüber zu treffen, welche Grössen als bekannt, gegeben oder rational angesehen werden sollen. Die Festsetzung darüber ist zunächst eine willkürliche, jedoch ist festzuhalten, dass alle durch die vier Species (Addition, Subtraction, Multiplication, Division) aus rationalen Grössen abgeleiteten wieder rational sind. Hieraus entspringt der Begriff des Ratio-

nalitätsbereichs, worunter der Inbegriff aller als bekannt betrachteten Grössen verstanden wird.

Ein Grössensystem, welches die Ausführung der vier Species (mit Ausnahme der Division durch Null) unbeschränkt gestattet, wird ein Körper genannt, und daher ist jeder Rationalitätsbereich ein Körper.

Jeder Körper muss, wenn er nicht aus dem einzigen Element Null besteht, als Quotient zweier gleicher Elemente die Zahl 1 und mithin alle rationalen Zahlen enthalten.

Der aus allen rationalen Zahlen bestehende Rationalitätsbereich heisst der absolute Rationalitätsbereich. Es kann aber auch der Rationalitätsbereich gewisse irrationale oder variable Grössen enthalten.

Der Rationalitätsbereich kann durch Hinzufügung gewisser nicht darin enthaltener Grössen erweitert werden. Eine solche Hinzufügung nennt man Adjunction.

Wir bezeichnen den Rationalitätsbereich durch $\mathfrak{R}$ und verstehen unter rationalen Functionen oder Gleichungen solche, deren Coëfficienten in $\mathfrak{R}$ enthalten sind.

Eine ganze rationale Function (einer oder mehrerer Variablen) heisst reducibel oder irreducibel, je nachdem sie in ganze rationale Factoren zerlegt werden kann oder nicht. Eine irreducible Function kann reducibel werden durch Erweiterung des Rationalitätsbereichs. Man unterscheidet dem entsprechend auch reducible und irreducible Gleichungen, je nachdem sie durch Nullsetzen einer reduciblen oder irreduciblen Function entstehen.

Eine algebraische Grösse in $\mathfrak{R}$ ist eine solche, welche die Wurzel einer in $\mathfrak{R}$ rationalen Gleichung ist.

2. Sind $x, y \dots$ algebraische Grössen in $\mathfrak{R}$ in beliebiger Anzahl und

$$f(x) = 0,\ \varphi(y) = 0 \dots$$

rationale Gleichungen vom Grade $m, n \dots$, welchen sie genügen, von denen wir nur voraussetzen wollen, dass sie keine mehrfachen Wurzeln haben, so kann man über die rationalen Grössen $a, b \dots$ so verfügen, dass die $mn \dots$ Werthe $r, r', r'' \dots$, die man erhält, wenn man in

$$r = ax + by + \cdots$$

für $x, y \dots$ die sämmtlichen Wurzeln von $f = 0, \varphi = 0 \dots$ setzt, alle unter einander verschieden sind. Die Differenzen

$r - r'$, $r - r''$, $r' - r''$ ... sind nämlich lineare Functionen der Veränderlichen $a, b \ldots$, in deren keiner die Coëfficienten sämmtlich verschwinden. Man kann also über die $a, b \ldots$ so verfügen, dass keine dieser Differenzen verschwindet (wie man in der Geometrie des Raumes einen Punkt, selbst mit rationalen Coordinaten, so wählen kann, dass er auf keiner von einer beliebigen Anzahl gegebener Ebenen liegt). Dann sind $r, r', r'' \ldots$ die Wurzeln einer rationalen Gleichung vom Grade $mn \ldots$

$$\Phi(t) = (t - r)(t - r')(t - r'') \ldots = 0,$$

und es lässt sich jede rationale Function von $x, y \ldots$, also auch die $x, y \ldots$ selbst, rational durch $r$ ausdrücken. Der erste Theil der Behauptung folgt nach dem Satze, dass die symmetrischen Functionen der Wurzeln einer algebraischen Gleichung rational durch die Coëfficienten ausgedrückt werden können, einfach daraus, dass, wenn $t$ eine beliebige Veränderliche bedeutet, $\Phi(t)$ ungeändert bleibt, wenn darin die Wurzeln von $f(x) = 0$ oder von $\varphi(y) = 0 \ldots$ beliebig unter einander vertauscht werden.

Bedeutet aber $\varrho$ eine beliebige rationale Function von $x, y \ldots$, welche, entsprechend den Werthen $r, r', r'' \ldots$, die Werthe $\varrho, \varrho', \varrho'' \ldots$ erhält (die zum Theil auch einander gleich sein können), so ist aus demselben Grunde

$$\left(\frac{\varrho}{t - r} + \frac{\varrho'}{t - r'} + \cdots\right) \Phi(t) = X(t)$$

eine ganze rationale Function von $t$. Setzt man $t = r$, so folgt

$$\varrho = \frac{X(r)}{\Phi'(r)},$$

womit auch der zweite Theil der Behauptung erwiesen ist. Es ist hierbei keineswegs ausgeschlossen, dass die Gleichungen $f = 0$, $\varphi = 0 \ldots$ gemeinschaftliche Factoren haben oder sogar mit einander identisch sind.

3. Algebraischer Körper. Der Inbegriff aller rationalen Functionen einer algebraischen Function $x$ in $\mathfrak{R}$ heisst ein algebraischer Körper und wird mit $\mathfrak{K}(x)$ oder kurz mit $\mathfrak{K}$ bezeichnet. Nach 2. ist der Inbegriff aller rationalen Functionen mehrerer algebraischer Grössen $\mathfrak{K}(x, y \ldots)$ unter dem so definirten Körperbegriff enthalten.

Es sei also

$$f(x) = 0 \tag{1}$$

die Gleichung $m$ten Grades für $x$, von der wieder vorausgesetzt sei, dass sie keine mehrfachen Wurzeln habe, und

(2) $$x, x_1, x_2 \ldots, x_{m-1}$$

seien ihre Wurzeln. Indem man $x$ durch $x_1, x_2 \ldots x_{m-1}$ ersetzt, entspringen aus $\mathfrak{K}(x)$ die $m$ conjugirten Körper

$$\mathfrak{K}(x), \mathfrak{K}(x_1), \ldots, \mathfrak{K}(x_{m-1}),$$

so dass jeder Grösse $y$ in $\mathfrak{K}$ eine ganz bestimmte Grösse $y_h$ in jedem der conjugirten Körper $\mathfrak{K}(x_h)$ entspricht.

Diese Grössen $y, y_1, \ldots y_{m-1}$ heissen mit einander conjugirt. Symmetrische Functionen von conjugirten Grössen sind rational. Von besonderer Wichtigkeit ist unter diesen das Product aller mit einander conjugirten Grössen $y$, welches die Norm von $y$ genannt wird.

4. Der Grad des Körpers. Wenn $f(x)$ reducibel ist, so sei

(3) $$\varphi(x) = 0$$

die irreducible Gleichung, welcher $x$ genügt, vom Grade $n$, und

(4) $$x, x_1 \ldots, x_{n-1}$$

seien ihre Wurzeln. Die Zahl $n$ heisst der Grad des Körpers $\mathfrak{K}(x)$. Jeder rationalen Gleichung, welche durch eine der Grössen (4) befriedigt wird, müssen auch die übrigen genügen.

Denn wenn $\psi(x) = 0$ und $\varphi(x) = 0$ eine gemeinsame Wurzel haben, so muss wegen der Irreducibilität von $\varphi(x)$ die Function $\psi(x)$ durch $\varphi(x)$ theilbar sein.

5. Jede Grösse $y$ des Körpers $\mathfrak{K}(x)$ genügt einer rationalen Gleichung $n$ten Grades:

(5) $$\chi(y) = 0,$$

worin für ein veränderliches $t$

$$\chi(t) = (t - y)(t - y_1) \ldots (t - y_{n-1}),$$

entweder irreducibel oder eine Potenz einer irreducibeln Function ist.

Denn lösen wir $\chi(t)$ in seine irreducibeln Factoren

$$\chi_1(t), \chi_2(t) \ldots$$

auf, so verschwindet jede dieser Functionen wenigstens für einen der Werthe

(6) $$t = y, y_1 \ldots, y_{n-1},$$

und mithin nach 4., da $y$ eine rationale Function von $x$ ist, für alle diese Werthe. Die Functionen $\chi_1(t)$, $\chi_2(t)$ . . . haben daher alle dieselben Wurzeln, nämlich die von einander verschiedenen unter den Grössen (6) und sind also mit einander identisch. Die Grössen (6) zerfallen in Gruppen von gleichvielen unter einander gleichen.

7. Wenn die Gleichung (5) irreducibel ist, so heisst $y$ eine primitive Grösse des Körpers $\mathfrak{K}$ (weil sie keinem Körper niedrigeren Grades angehört). Jede Grösse des Körpers $\mathfrak{K}$ ist dann durch $y$ rational ausdrückbar und also $\mathfrak{K}(x)$ mit $\mathfrak{K}(y)$ identisch.

Der Beweis ist derselbe wie in Nr. 2.

Wenn umgekehrt $x$ durch eine Grösse $y$ des Körpers $\mathfrak{K}(x)$ rational ausdrückbar ist, so ist $y$ eine primitive Grösse des Körpers $\mathfrak{K}$.

8. Wir kehren jetzt zurück zur Gleichung

$$f(x) = 0$$

vom $m$ten Grade und betrachten neben dem Körper $\mathfrak{K}(x)$ den Körper

$$\mathfrak{K}(x, x_1, x_2 \ldots, x_{m-1}) = \mathfrak{N},$$

welcher die Norm des Körpers $\mathfrak{K}(x)$ heisst, und dessen Grad wir mit $\nu$ bezeichnen wollen. Ist $r$ eine primitive Grösse des Körpers $\mathfrak{N}$, so sind $x, x_1, x_2 \ldots, x_{m-1}$ rationale Functionen von $r$ (nach 7) und der Körper $\mathfrak{N}$ ist identisch mit $\mathfrak{K}(r)$; $r$ ist eine rationale Function der Grössen (2) und die mit $r$ conjugirten Grössen

$$r, r_1, r_2 \ldots, r_{\nu-1} \tag{7}$$

entstehen alle durch gewisse Vertauschungen der $x$, sind also ebenfalls rationale Functionen der Grössen (2) und daher auch von $r$. Der Körper $\mathfrak{N}$ hat also die Eigenschaft, alle seine conjugirten Körper zu enthalten, und da dasselbe für jeden anderen der Körper $\mathfrak{K}(r_1)$, $\mathfrak{K}(r_2)$ . . . gilt, so sind alle diese Körper mit einander und mit ihrer Norm $\mathfrak{K}(r, r_1 \ldots, r_{\nu-1})$ identisch. Ein solcher Körper heisst ein Normalkörper oder ein Galois'scher Körper. Die Grössen (7) genügen einer irreducibeln Gleichung $\nu$ten Grades

$$F(r) = 0, \tag{8}$$

welche die Eigenschaft hat, dass durch eine ihrer Wurzeln alle übrigen und auch alle Wurzeln der ursprünglichen Gleichung $f(x) = 0$ rational ausdrückbar sind. Wir nennen eine solche Gleichung eine Galois'sche Resolvente der Gleichung $f(x) = 0$.

## §. 56. Die Galois'sche Gruppe der Gleichung $f(x) = 0$.

Drückt man die sämmtlichen Grössen des Körpers $\mathfrak{R}$ rational durch $r$ aus und ersetzt dann $r$ durch $r_1$, oder macht man, wie wir uns ausdrücken wollen, die Substitution

$$S = (r, r_1),$$

so gehen die sämmtlichen Grössen in $\mathfrak{R}$ in bestimmte andere Grössen desselben Körpers über, und niemals zwei verschiedene Grössen in ein und dieselbe [denn aus $\psi_1(r_1) = \psi_2(r_1)$ würde nach 4. folgen $\psi_1(r) = \psi_2(r)$].

Jede Gleichung, die zwischen Grössen des Körpers $\mathfrak{R}$ besteht, bleibt richtig, wenn die Substitution $S$ darin ausgeführt wird. Die Grössen (7) und ebenso die Grössen (2) in §. 55 werden daher durch die Substitution $S$ in bestimmter Weise unter einander vertauscht.

Die $\nu$ Substitutionen $S_k$

$$(r, r), (r, r_1), (r, r_2) \ldots, (r, r_{\nu-1}), \tag{9}$$

worin $(r, r) = S_0$ die identische Substitution bedeutet, durch welche nichts geändert wird, bilden eine Gruppe $\mathfrak{G}$ in folgendem Sinne:

Wir wollen zwei der Substitutionen (9), etwa $S_1$, $S_2$, nach einander ausführen. Durch $S_2 = (r, r_2)$ wird $r_1$ in eine bestimmte der Grössen (7), etwa $r_3$, übergehen, so dass $S_2$ auch $= (r_1, r_3)$ gesetzt werden kann. Dann ist das Resultat der successiven Ausführung von $S_1$, $S_2$ offenbar $(r, r_3) = S_3$, und wir setzen daher:

$$(r, r_1)(r, r_2) = (r, r_1)(r_1, r_3) = (r, r_3), \tag{10}$$

wodurch die Composition der Elemente von $\mathfrak{G}$ erklärt ist, welche $\mathfrak{G}$ zur Gruppe macht. Die Zahl $\nu$ ist der Grad dieser Gruppe.

Die Gruppe $\mathfrak{G}$ hat die doppelte Eigenschaft:

a) Jede Grösse in $\mathfrak{R}$, welche durch die Substitutionen der Gruppe $\mathfrak{G}$ ungeändert bleibt, ist rational.

Denn ist

$$\psi(r) = \psi(r_1) = \cdots \psi(r_{\nu-1}),$$

so ist

$$\nu\psi(r) = \psi(r) + \psi(r_1) + \cdots \psi(r_{\nu-1})$$

als symmetrische Function der Wurzeln von (8) rational.

b) Jede rationale Gleichung zwischen Grössen in $\mathfrak{R}$ bleibt richtig, wenn irgend eine Substitution der Gruppe $\mathfrak{G}$ angewandt wird.

Denn ist $\psi(r) = 0$, so ist, da $F(t)$ irreducibel ist, $\psi(t)$ theilbar durch $F(t)$ und also auch $\psi(r_1) = 0, \dots \psi(r_{\nu-1}) = 0$.

Wenn man eine Substitution der Gruppe $\mathfrak{G}$ auf die Grössenreihe $x, x_1, x_2 \dots, x_{m-1}$ anwendet, so erleiden diese eine gewisse Permutation. Jeder Substitution $S$ entspricht daher eine gewisse Substitution der Wurzeln $x$:

$$S = \begin{pmatrix} x, & x_1, & x_2 \dots, & x_{m-1} \\ x', & x'_1, & x'_2 \dots, & x'_{m-1} \end{pmatrix}, \tag{11}$$

welche sich nach der Regel (10) zusammensetzen lassen und daher eine mit $\mathfrak{G}$ „isomorphe"[1] Gruppe bilden, die wir gleichfalls mit $\mathfrak{G}$ bezeichnen wollen.

Sie heisst die Galois'sche Gruppe der Gleichung $f = 0$ und hat die beiden folgenden Eigenschaften, die nur ein anderer Ausdruck für a) b) sind:

a') Jede rationale Function der Wurzeln $x, x_1 \dots, x_{m-1}$, welche durch die sämmtlichen Substitutionen $\mathfrak{G}$ ungeändert bleibt, ist eine rationale Grösse.

b') Jede rationale Gleichung zwischen den Wurzeln $x, x_1 \dots, x_{m-1}$ bleibt richtig, wenn eine der Substitutionen $\mathfrak{G}$ angewandt wird.

Dem fügen wir noch hinzu:

c') Wenn irgend eine Substitution $S$ der Wurzeln $x$ auf sämmtliche rationale Gleichungen zwischen den Wurzeln anwendbar ist, so gehört sie zur Galois'schen Gruppe der Gleichung.

Denn eine solche Substitution ist auf die Gleichung (8) anwendbar und ist daher mit einer der Substitutionen $(r, r_k)$ gleichbedeutend.

Daraus folgt noch, dass die Eigenschaften a') b') für die Galois'sche Gruppe vollständig charakteristisch sind, d. h. dass es keine zweite Gruppe von Substitutionen giebt, welche dieselben Eigenschaften besitzt, und man kann die Gruppe der

---

[1] Zwei Gruppen von gleich vielen Elementen heissen isomorph, wenn jedem Element der einen Gruppe ein Element der anderen Gruppe in der Weise entspricht, dass auch dem Compositum aus zwei Elementen der einen Gruppe das Compositum aus entsprechenden Elementen der anderen entspricht.

Gleichung auch definiren als den Inbegriff aller derjenigen Substitutionen, welche in sämmtlichen rationalen Gleichungen zwischen den Wurzeln gestattet sind.

Denn hat eine Gruppe $\mathfrak{G}'$ die beiden Eigenschaften a') b'), so ist sie nach c') ein Theiler von $\mathfrak{G}$. Ist aber $\mathfrak{G}$ durch $\mathfrak{G}'$ nicht erschöpft, so geht durch $\mathfrak{G}'$ ein Theil der Grössen $r$, etwa $r, r_1 \ldots, r_{\mu-1}$, nur in einander über;

$$(t - r)(t - r_1) \ldots (t - r_{\mu-1})$$

wäre aber dann rational und $F(t)$ reducibel, gegen die Voraussetzung.

Die Gruppe $\mathfrak{G}$ heisst transitiv, wenn es in ihr wenigstens eine Substitution giebt, durch welche $x$ in eine beliebige andere Wurzel $x_k$ übergeht, im entgegengesetzten Falle intransitiv.

Ist $\mathfrak{G}$ transitiv, so ist $f(x)$ irreducibel; dann alsdann muss nach b') jede Gleichung $\varphi(x) = 0$ für sämmtliche Wurzeln von $f(x) = 0$ erfüllt sein.

Ist aber $\mathfrak{G}$ intransitiv, so wird $f(x)$ reducibel sein; dann giebt es einen gewissen Theil der Grössen $x$, etwa $x, x_1 \ldots, x_{n-1}$, worin $n < m$, welche durch $\mathfrak{G}$ nur unter einander vertauscht werden, und daher ist nach a') bereits $\varphi(t) = (t - x) \ldots (t - x_{n-1})$ rational, also $\varphi(x) = 0$ rational und nur vom Grade $n$.

Die Gruppe der Gleichung $\varphi(x) = 0$ besteht dann neben der identischen Substitution aus allen durch die Substitutionen von $\mathfrak{G}$ bewirkten Vertauschungen der Wurzeln $x, x_1, x_2 \ldots, x_{n-1}$.

## §. 57. Reduction der Galois'schen Gruppe durch Adjunction.

Es sei $\xi$ irgend eine Grösse des Körpers $\mathfrak{N}$ und $\mathfrak{H}$ der Inbegriff aller derjenigen Substitutionen von $\mathfrak{G}$, durch welche $\xi$ ungeändert bleibt. Es ist dann $\mathfrak{H}$ eine Gruppe, und zwar ein Divisor von $\mathfrak{G}$ (welcher, falls $\xi$ im Körper $\mathfrak{N}$ primitiv ist, nur die einzige identische Substitution enthält und, falls $\xi$ rational ist, mit $\mathfrak{G}$ identisch ist). Der Grad von $\mathfrak{H}$ sei $\mu$ und der Index $n_1$, so dass

$$(12) \qquad \nu = \mu n_1.$$

Ist $n_1 < \nu$ und $S_1$ eine nicht in $\mathfrak{H}$ enthaltene Substitution von $\mathfrak{G}$, so geht durch die sämmtlichen Substitutionen

$$\mathfrak{H}\, S_1$$

$\xi$ in ein und denselben, von $\xi$ verschiedenen Werth $\xi_1$ über, und es entsprechen also den $n_1$ Reihen (§. 53, 3):

$$\mathfrak{H},\ \mathfrak{H}\, S_1 \ldots,\ \mathfrak{H}\, S_{n_1 - 1}, \tag{13}$$

$n_1$ verschiedene Werthe von $\xi$:

$$\xi,\ \xi_1 \ldots,\ \xi_{n_1 - 1}. \tag{14}$$

Die Anwendung irgend einer Substitution $T$ von $\mathfrak{G}$ auf $\xi_1$ hat denselben Effect, wie die Anwendung von $S_1\, T$ auf $\xi$, und da $S_1\, T$ in einer der Reihen (13) enthalten ist, so werden durch jede Substitution $T$ die Grössen (14) nur unter einander permutirt. Hieraus folgt, dass, wenn $t$ eine Veränderliche bedeutet, das Product

$$(t - \xi)\,(t - \xi_1) \ldots (t - \xi_{n_1 - 1}) = \varphi(t)$$

rational ist und dass mithin $\xi$ durch eine Gleichung vom Grade $n_1$:

$$\varphi(\xi) = 0 \tag{15}$$

bestimmt wird. Die Gleichung (15) ist irreducibel, da jede rationale Gleichung $\varphi(\xi) = 0$ richtig bleiben muss, wenn irgend eine Substitution (13) gemacht, also $\xi$ durch eine der anderen Grössen (14) ersetzt wird.

Jede Grösse in $\mathfrak{R}$, welche durch die Substitutionen der Gruppe $\mathfrak{H}$ ungeändert bleibt, kann rational durch $\xi$ ausgedrückt werden (Beweis wie in §. 55, 2).

Die Gruppe $\mathfrak{H}$ besteht aus $\mu$ Substitutionen der Form:

$$(r,\ r),\ (r,\ r_1), \ldots (r,\ r_{\mu - 1}),$$

und daher werden durch $\mathfrak{H}$ die $\mu$ Grössen:

$$r,\ r_1,\ r_2, \ldots r_{\mu - 1}$$

nur unter einander vertauscht. Denn sind $H = (r, r_1), H_1 = (r_1, r_2)$ zwei Substitutionen in $\mathfrak{H}$, so gehört $H H_1 = (r, r_2)$ gleichfalls zu $\mathfrak{H}$. Das Product:

$$F(t,\ \xi) = (t - r)\,(t - r_1) \ldots (t - r_{\mu - 1})$$

ist daher rational durch $\xi$ ausdrückbar, und wenn also $\xi$ dem Rationalitätsbereich adjungirt wird, so fordert die Bestimmung von $r$, also die vollständige Lösung der Gleichung $f(x) = 0$, nur noch die Kenntniss einer Wurzel $r$ der Gleichung $\mu$ten Grades:

$$F(r,\ \xi) = 0. \tag{16}$$

Wir wollen noch umgekehrt zeigen, dass, wenn $\mathfrak{H}$ irgend ein Divisor von $\mathfrak{G}$ ist, immer eine Grösse in $\mathfrak{N}$ gefunden werden kann, welche durch die Substitutionen $\mathfrak{H}$ und nur durch diese ungeändert bleibt. Von einer solchen Function sagt man, sie gehöre zu der Gruppe $\mathfrak{H}$.

Besteht die Gruppe $\mathfrak{H}$ aus den Substitutionen

$$(r, r), (r, r_1), \ldots (r, r_{\mu-1}),$$

so bleibt das Product

$$\xi = (\alpha - r)(\alpha - r_1) \ldots (\alpha - r_{\mu-1}),$$

worin $\alpha$ eine willkürliche rationale Grösse ist, ungeändert durch $\mathfrak{H}$. Macht man aber in dem so gebildeten Ausdruck $\xi$ alle Substitutionen $S, S_1 \ldots, S_{n_1-1}$, so entstehen $n_1$-Grössen, von denen keine zwei in Bezug auf $\alpha$ identisch sind, und von denen also nur für eine endliche Anzahl von Werthen $\alpha$ zwei einander gleich werden können. Man kann also über $\alpha$ so verfügen, dass sie alle verschieden sind, und dass also $\xi$ sich durch jede nicht in $\mathfrak{H}$ enthaltene Substitution ändert, und mithin zu $\mathfrak{H}$ gehört.

Wenn man also darauf ausgeht, die Auflösung der Gleichung $f(x) = 0$ auf eine Gleichung möglichst niedrigen Grades zurückzuführen, so wird man einen Divisor $\mathfrak{H}$ von $\mathfrak{G}$ suchen von möglichst hohem Grade. Beurtheilt man aber die Schwierigkeit der Lösung einer algebraischen Aufgabe nach dem Grade der Gruppe, so wird es zunächst darauf ankommen, den Grad der Gruppe der Gleichung (15) zu ermitteln. Wir betrachten also den Körper (§. 55, 8):

$$\mathfrak{N}_1 = \mathfrak{K}(\xi, \xi_1 \ldots, \xi_{n_1-1})$$

und bezeichnen mit $\varrho$ eine primitive Grösse dieses Körpers. Eine solche Grösse bleibt nur durch solche Substitutionen ungeändert, welche gleichzeitig alle $\xi, \xi_1 \ldots, \xi_{n_1-1}$ ungeändert lassen. Wenn nun $\xi$ durch $S$ in $\xi_1$ übergeht, so geht $\xi_1$ durch $S^{-1}$ in $\xi$ über, und daher gehört $\xi_1$ zu $S^{-1}\mathfrak{H}S$. Daraus folgt, dass $\varrho$ zu dem grössten gemeinschaftlichen Theiler $\mathfrak{H}_1$ aller mit $\mathfrak{H}$ conjugirten Theiler von $\mathfrak{G}$ gehört.

Die Gruppe $\mathfrak{H}_1$ ist ein eigentlicher Divisor von $\mathfrak{G}$, dessen Grad und Index wir mit $\mu_1, \nu_1$ bezeichnen, so dass

$$\nu = \mu_1 \nu_1.$$

Es genügt also $\varrho$ einer irreducibeln Gleichung $\nu_1$ten Grades und $\nu_1$ ist also der Grad des Körpers $\mathfrak{N}_1$ oder der Grad der Gruppe der Gleichung $\varphi(\xi) = 0$.

Eine Reduction der Gruppe von $f(x) = 0$ kann also nur durch solche Grössen eintreten, welche durch die Substitutionen eines eigentlichen Divisors von $\mathfrak{G}$ ungeändert bleiben. Wenn $\mathfrak{G}$ gar keinen eigentlichen Divisor besitzt, so kann wohl eine Reduction des Grades, aber nicht eine Reduction der Gruppe eintreten. In diesem Falle enthält $\mathfrak{H}_1$ nur die eine identische Substitution und es kann $r$ rational durch $\varrho$ ausgedrückt werden, so dass durch die Kenntniss von $\varrho$ oder, was dasselbe ist, der sämmtlichen Wurzeln $\xi, \xi_1 \ldots, \xi_{n_1-1}$ die Gleichung $f(x) = 0$ vollständig gelöst ist.

Wenn die Galois'sche Resolvente $F(r) = 0$ nach Adjunction irgend welcher algebraischer Grössen reducirt wird und es ist

$$F_1(t) = (t - r)(t - r_1) \ldots (t - r_{\nu_1-1})$$

ein irreducibler Factor von $F(t)$, so bilden die Substitutionen

$$(r, r), (r, r_1), \ldots (r, r_{\nu_1-1})$$

eine (in $\mathfrak{G}$ enthaltene) Gruppe $\mathfrak{H}$. Denn wenn

$$(r, r_1)(r, r_2) = (r, r_3),$$

also

$$(r, r_2) = (r_1, r_3)$$

ist, so folgt, dass, wenn $r_1, r_2$ der Gleichung $F_1(t) = 0$ genügen, ihr auch $r_3$ genügt, weil in $F_1(r_1) = 0$ wegen der Irreducibilität von $F_1(r) = 0$ die Substitution $(r, r_2)$ ausgeführt werden darf, so dass also auch $F_1(r_3) = 0$ ist. Es ist also $(r, r_3)$ in $\mathfrak{H}$ enthalten. Suchen wir also eine zu dieser Gruppe $\mathfrak{H}$ gehörige Grösse $\xi$ in $\mathfrak{N}$, so folgt, dass $F_1(t)$ (für ein unbestimmtes $t$) rational durch $\xi$ ausdrückbar ist. Wir haben also nicht nöthig, bei der successiven Reduction der Galois'schen Resolvente andere Irrationalitäten als solche zu Hülfe zu nehmen, welche in $\mathfrak{N}$ enthalten, also rational durch die Wurzeln von $f(x)$ ausdrückbar sind.

## §. 58. Reduction durch Wurzeln reiner Gleichungen. Abel'sche Gleichungen.

1. Wir wollen noch die Frage erörtern, unter welchen Umständen die Gleichung $F(r) = 0$ durch Adjunction der Wurzel einer reinen Gleichung reducirt werden kann. Es genügt hierbei die Annahme, dass der Grad der reinen Gleichung eine

Primzahl $p$ sei, weil jedes Wurzelziehen sich auf eine Kette von Wurzeln mit Primzahlgraden zurückführen lässt.

Wir machen hierbei die Annahme, dass die $p$ten Einheitswurzeln zum Rationalitätsbereich gehören, bemerken aber, dass die Frage, ob durch Adjunction der $p$ten Einheitswurzeln die Gleichung $F(r) = 0$ reducirt wird, keine andere ist als die, die wir hier gestellt haben, weil, wie aus der Kreistheilungstheorie bekannt ist, die $p$ten Einheitswurzeln ausgedrückt werden können durch die Wurzeln reiner Gleichungen, deren Grade Divisoren von $p - 1$, also kleiner als $p$ sind.

Die Function

$$\psi(t) = t^p - A \tag{17}$$

ist, wenn $A$ rational, aber nicht die $p$te Potenz einer rationalen Grösse ist, irreducibel; denn wäre (17) reducibel, so wäre ein Product aus weniger als $p$ seiner Wurzeln rational, also $\sqrt[p]{A^q}$ für ein $q < p$ rational. Bestimmt man also die ganze Zahl $x$ so, dass $xq \equiv 1 \pmod{p}$, so folgt, dass auch $\sqrt[p]{A^{qx}}$ und folglich $\sqrt[p]{A}$ rational ist, gegen die Voraussetzung.

Wenn nun durch Adjunction einer Wurzel $\varrho$ von (17) die Gleichung $F(r) = 0$ reducirt wird, so giebt es einen Factor $F(t, \varrho)$ von $F(t)$, der $\varrho$ wirklich enthält, und zwar höchstens im Grade $p - 1$, so dass $F(r, \varrho) = 0$ ist. Es hat daher $F(r, t) = 0$ und $\psi(t) = 0$ eine gemeinschaftliche Wurzel, und folglich ist $\psi(t)$ nach Adjunction von $r$ reducibel. Es sei $\psi(t, r)$ ein Factor von (17) von möglichst niedrigem Grade und

$$\psi(t) = \psi(t, r)\, \psi_1(t, r).$$

Diese Gleichung ist in $t$ identisch und gestattet daher die Substitutionen der Gruppe $\mathfrak{G}$, d. h. sie gilt für alle Wurzeln der Gleichung $F(r) = 0$. Bilden wir also das Product über alle diese Wurzeln, so folgt:

$$\psi(t)^\nu = \overset{r}{\Pi}\, \psi(t, r)\, \overset{r}{\Pi}\, \psi_1(t, r),$$

worin $\overset{r}{\Pi}\, \psi(t, r)$ rational ist; und da $\psi(t)$ irreducibel ist, so ist dies Product durch eine Potenz von $\psi(t)$ theilbar, und da es keine anderen Factoren enthalten kann, mit einer solchen Potenz identisch; also

$$\psi(t)^\lambda = \overset{r}{\Pi}\, \psi(t, r).$$

Da $\psi(t, r)$ irreducibel ist, und daher keine mehrfachen Factoren enthält, da ferner zwei der Factoren $\psi(t, r)$ entweder ganz identisch oder relativ prim sind, so müssen in dem Product der rechten Seite je $\lambda$ von den $\nu$ Factoren einander gleich sein, und es zerfällt also $\psi(t)$ in Factoren $\psi(t, r)$, $\psi(t, r_1) \dots$, die alle von gleichem Grade sind. Dieser Grad ist also ein Theiler von $p$ und ist daher $= 1$, d. h. $\psi(t, r)$ ist in Bezug auf $t$ linear. Daraus folgt, dass die Wurzeln $\varrho$ im Körper $\mathfrak{N}$ enthalten, oder rational durch $r$ ausdrückbar sind. Die Gruppe $\mathfrak{H}$, zu welcher $\varrho$ gehört, ist daher ein Theiler von $\mathfrak{G}$ vom Index $p$, und zwar ein eigentlicher Theiler.

Denn ist $S$ eine nicht in $\mathfrak{H}$ enthaltene Substitution, durch welche $\varrho$ in $\varrho_1 = \varepsilon\varrho$ übergeht (wenn $\varepsilon$ eine $p$te Einheitswurzel bedeutet), so geht $\varrho$ durch $S^{-1}$ in $\varepsilon^{-1}\varrho$ über. Es bleibt also $\varrho$ ungeändert durch $S\mathfrak{H}S^{-1}$ und letztere Gruppe ist also mit $\mathfrak{H}$ identisch.

2. Es gilt die Umkehrung dieses Satzes in folgendem Sinne: Wenn $\mathfrak{G}$ einen eigentlichen Divisor $\mathfrak{H}$ vom Primzahl-Index $p$ besitzt, so wird die Gleichung $F(r) = 0$ durch Adjunction der $p$ten Wurzel aus einer rationalen Grösse reducirt.

Man adjungire zunächst dem Rationalitätsbereich die $p$ten Einheitswurzeln, wenn sie nicht schon darin enthalten sind. Es kann der Fall eintreten, dass schon durch diese Adjunction die Gruppe $\mathfrak{G}$ reducirt wird, und zwar auf einen Theiler von $\mathfrak{G}$, dessen Index $\leqq p - 1$ ist.

Wenn aber $\mathfrak{G}$ einen eigentlichen Theiler $\mathfrak{H}$ vom Primzahlindex $p$ besitzt, so muss nach §. 53, 4 auch jeder andere Theiler von $\mathfrak{G}$, der nicht mit $\mathfrak{H}$ identisch ist, einen ebensolchen Theiler haben. Wenn daher unsere Voraussetzung vor der Adjunction der $p$ten Einheitswurzeln erfüllt war, so ist sie es auch nachher und wir nehmen daher an, die $p$ten Einheitswurzeln gehören zum Rationalitätsbereich.

Ist nun $S$ eine nicht in $\mathfrak{H}$ enthaltene Substitution von $\mathfrak{G}$, und $S^\lambda$ die niedrigste Potenz von $S$, welche in $\mathfrak{H}$ enthalten ist, so ist das System

$$\mathfrak{H},\ \mathfrak{H}S \dots,\ \mathfrak{H}S^{\lambda-1}$$

eine Gruppe, welche in $\mathfrak{G}$ enthalten ist. Es ist also $\lambda$ ein Theiler von $p$ und, da $p$ eine Primzahl ist, $\lambda = p$. Die Gruppe $\mathfrak{G}$ ist also in die Reihen zerlegt:

$$\mathfrak{H},\ \mathfrak{H}S \dots,\ \mathfrak{H}S^{p-1},$$

und wenn $\xi$ eine zu $\mathfrak{H}$ gehörige Grösse ist, welche durch $S, S^2 \ldots, S^{p-1}$ in $\xi_1, \xi_2 \ldots, \xi_{p-1}$ übergeht, so ist, wenn $\varepsilon$ eine imaginäre $p$te Einheitswurzel bedeutet,

$$\varrho = \xi + \varepsilon \xi_1 + \varepsilon^2 \xi_2 \ldots \varepsilon^{p-1} \xi_{p-1}$$

gleichfalls eine zu $\mathfrak{H}$ gehörige Grösse, welche durch $S$ in $\varepsilon^{-1} \varrho$ übergeht, deren $p$te Potenz also durch $S$ ungeändert bleibt und daher rational ist.

3. Die Gleichung $F(r) = 0$ ist algebraisch auflösbar, wenn die Gruppe $\mathfrak{H}$ wiederum einen eigentlichen Divisor vom Primzahl-Index besitzt, und so fort, bis man schliesslich zu einer Gruppe kommt, deren Grad eine Primzahl ist.

In diesem Falle befinden sich die Abel'schen Gleichungen, d. h. diejenigen Gleichungen, deren Gruppe eine Abel'sche ist.

Wenn nämlich die Gruppe $\mathfrak{G}$ durch die Basis $(A, B, C \ldots)$ darstellbar ist, so ist, wenn $p$ eine im Grade von $A$ aufgehende Primzahl bedeutet, die durch die Basis $(A^p, B, C \ldots)$ dargestellte Gruppe $\mathfrak{H}$ ein eigentlicher Divisor von $\mathfrak{G}$ vom Index $p$; und da $\mathfrak{H}$ wieder eine Abel'sche Gruppe ist, so lässt sich dieser Schluss fortsetzen.

Bei den Abel'schen Gleichungen lässt sich die Auflösbarkeit auch auf folgendem directem Wege zeigen.

Wenn durch die Substitution

$$S = A^\alpha B^\beta \ldots$$

$r$ in $r_{\alpha, \beta \ldots}$ übergeht, so geht durch dieselbe Substitution $r_{\alpha', \beta' \ldots}$ in $r_{\alpha' + \alpha, \beta' + \beta \ldots}$ über, oder es ist

$$S = (r, r_{\alpha, \beta \ldots}) = (r_{\alpha', \beta' \ldots}, r_{\alpha' + \alpha, \beta' + \beta \ldots}),$$

wie man erkennt, wenn man auf $r_{\alpha', \beta' \ldots}$ nach einander die Substitutionen $A^{-\alpha'} B^{-\beta'} \ldots$ und $A^{\alpha + \alpha'} B^{\beta + \beta'} \ldots$ anwendet. Bezeichnet man also mit $(a), (b) \ldots$ irgend welche Einheitswurzeln der Grade $a, b \ldots$, so ist die über je ein vollständiges Restsystem nach den Moduln $a, b \ldots$ ausgedehnte Summe

$$\left( \sum^{\alpha, \beta \ldots} (a)^\alpha (b)^\beta \ldots r_{\alpha, \beta \ldots} \right)^n = \psi_{a, b \ldots}$$

durch die Substitutionen $S$ ungeändert und daher rational. Daraus folgt aber

$$n r = \sum^{(a), (b) \ldots} \sqrt[n]{\psi_{a, b \ldots}},$$

wo die Summe rechts über sämmtliche $a$te, $b$te $\ldots$ Einheitswurzeln $(a), (b) \ldots$ auszudehnen ist.

4. Für die Auflösbarkeit einer Gleichung durch Wurzelzeichen hat Abel folgendes Kennzeichen gegeben:

Eine Gleichung ist algebraisch auflösbar, wenn alle Wurzeln durch eine unter ihnen, die mit $x$ bezeichnet sei, rational darstellbar sind, und wenn überdies, falls $f(x)$, $f_1(x)$ irgend zwei andere der Wurzeln sind, die Bedingung erfüllt ist

$$f f_1(x) = f_1 f(x).$$

Dies Kennzeichen kann aus dem vorigen hergeleitet werden. Es seien

$$x_1 = f_1(x), \quad x_2 = f_2(x), \quad x_3 = f_3(x) \ldots$$

die sämmtlichen Wurzeln der fraglichen Gleichung, die wir als von einander verschieden voraussetzen, darunter $x$; es seien ferner $x$, $x'$, $x''$ ... diejenigen unter diesen Wurzeln, welche einer irreducibeln Gleichung $\Phi = 0$ genügen. Nach Voraussetzung ist, wenn $\varphi'$, $\varphi''$ ... rationale Functionen sind,

$$x' = \varphi'(x), \quad x'' = \varphi''(x) \ldots$$

Wenn dann $x_i = f_i(x)$ eine Wurzel der gegebenen Gleichung ist, so sind auch $x'_i = f_i(x')$, $x''_i = f_i(x'')$ ... Wurzeln (wegen der Irreducibilität der Gleichung $\Phi = 0$), und die $x'_i$, $x''_i$ repräsentiren für $i = 1, 2, 3 \ldots$ nur zwei andere Anordnungen der Wurzeln $x_i$.

Die Gruppe $\mathfrak{G}$ der gegebenen Gleichung besteht ausser der identischen Substitution aus den sämmtlichen Vertauschungen

$$S' = (x, x'), \quad S'' = (x, x'') \ldots,$$

welche gleichbedeutend sind mit den Vertauschungen:

$$\begin{pmatrix} x_1, & x_2, & x_3 & \ldots \\ x'_1, & x'_2, & x'_3 & \ldots \end{pmatrix}, \quad \begin{pmatrix} x_1, & x_2, & x_3 & \ldots \\ x''_1, & x''_2, & x''_3 & \ldots \end{pmatrix} \ldots$$

Denn jede rationale Gleichung zwischen den Wurzeln kann nach Voraussetzung als eine rationale Gleichung für $x$ ausgedrückt werden, und gestattet also, wegen der Irreducibilität von $\Phi = 0$, die Vertauschungen $S'$, $S''$ ...; und wenn umgekehrt eine Function von $x$ diese Vertauschungen gestattet, so kann sie als symmetrische Function von $x$, $x'$, $x''$ ... dargestellt werden und ist also rational. Nun ist aber

$$S' S'' = (x, \varphi' \varphi''(x)), \quad S'' S' = (x, \varphi'' \varphi'(x)),$$

also, nach Voraussetzung, $S' S'' = S'' S'$ und mithin $\mathfrak{G}$ eine Abel'sche Gruppe.

## §. 59. Ganze algebraische Zahlen und ganze algebraische Functionen einer Veränderlichen.

Bisher haben wir über den Rationalitätsbereich eine specielle Voraussetzung nicht gemacht. Setzen wir den absoluten Rationalitätsbereich (den der rationalen Zahlen) voraus, so erhalten wir aus der allgemeinen Definition des algebraischen Körpers (§. 55, 3) den Begriff der algebraischen Zahlkörper. Verstehen wir aber unter dem Rationalitätsbereich den der rationalen Functionen einer Variablen, so erhalten wir die Körper der algebraischen Functionen einer Variablen. In letzterem Falle können noch die Constanten entweder unbeschränkt oder auch auf einen beliebigen Zahlkörper beschränkt sein. Bezüglich der Theorie der algebraischen Zahlkörper verweisen wir auf Dedekind's Darstellung (Dirichlet-Dedekind, Zahlentheorie, Supplement XI). Es sollen hier nur wenige der einfachsten Sätze erwähnt werden, die sich auf die beiden oben erwähnten Arten von Körpern, und besonders auf den Uebergang von dem einen zum anderen beziehen, von denen wir später Gebrauch machen müssen.

Genügt $y$ einer algebraischen Gleichung $n$ten Grades

$$(1) \quad F(y) = y^n + a_1 y^{n-1} + \cdots + a_{n-1} y + a_n = 0,$$

so ist, je nachdem die $a_1 \ldots, a_{n-1}, a_n$ rationale Zahlen oder rationale Functionen einer Veränderlichen $x$ sind, $y$ eine algebraische Zahl oder eine algebraische Function von $x$. Den Coëfficienten der höchsten Potenz der Unbekannten nehmen wir immer $= 1$ an.

Eine und dieselbe Grösse $y$ genügt unendlich vielen Gleichungen von der Form (1). Unter diesen ist eine und nur eine vom niedrigsten Grade, und diese ist irreducibel. Ist $F(y) = 0$ selbst diese irreducible Gleichung und $\Phi(y) = 0$ eine andere Gleichung von der Form (1), so ist $\Phi(t)$ durch $F(t)$ (mit variablem $t$) theilbar.

Sind in (1) die Coëfficienten $a_1, \ldots a_n$ ganze rationale Zahlen oder ganze rationale Functionen von $x$, so heisst $y$ eine ganze algebraische Zahl oder eine ganze algebraische Function von $x$. Wir wollen, um beide Fälle zusammenzufassen, $y$ als ganze algebraische Grösse bezeichnen. Es gelten folgende Sätze:

1. Ganze algebraische Grössen, die zugleich rational sind, sind ganze rationale Grössen (Zahlen oder Functionen).

Ist nämlich

$$y = \frac{u}{v},$$

und sind $u$, $v$ ganze rationale Grössen ohne gemeinsamen Theiler, so folgt aus (1):

$$u^n + a_1 u^{n-1} v + \cdots a_{n-1} u v^{n-1} + a_n v^n = 0.$$

Daraus ist zu schliessen, dass ein Primtheiler von $v$, d. h. eine in $v$ aufgehende Primzahl im Falle der Zahlen, und ein in $v$ aufgehender linearer Factor im Falle der Functionen, auch in $u^n$ und mithin in $u$ aufgehen müsste. Es kann also $y$ keinen anderen Nenner haben als 1 oder eine Constante.

2. Summe, Differenz und Product zweier ganzer algebraischer Grössen sind wieder ganze algebraische Grössen.

Sind nämlich $y$, $z$ zwei ganze algebraische Grössen, welche den beiden Gleichungen

$$(2) \qquad \begin{aligned} y^n + a_1 y^{n-1} + \cdots a_{n-1} y + a_n &= 0 \\ z^m + b_1 z^{m-1} + \cdots b_{m-1} z + b_m &= 0 \end{aligned}$$

genügen, so kann man, wenn $\mu = mn$ gesetzt wird und unter $u_1, u_2 \ldots u_\mu$ die $\mu$-Producte

$$y^r z^s;\ r = 0, 1, \ldots n-1;\ s = 0, 1, \ldots m-1$$

verstanden werden, und wenn endlich $u$ eine der drei Grössen $y+z$, $y-z$, $yz$ bedeutet, mit Hülfe der Gleichungen (2) setzen:

$$\begin{aligned} u u_1 &= a_{1,1} u_1 + \cdots a_{1,\mu} u_\mu \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ u u_\mu &= a_{\mu,1} u_1 + \cdots a_{\mu,\mu} u_\mu, \end{aligned}$$

worin $a_{i,\varkappa}$ ganze rationale Grössen sind. Daraus folgt aber, dass $u$ eine Wurzel der Gleichung:

$$\begin{vmatrix} a_{1,1} - u \ldots, a_{1,\mu} \\ a_{\mu,1} \ldots, a_{\mu,\mu} - u \end{vmatrix} = 0$$

ist, welche ebenfalls ganze Coëfficienten hat. Es ist daher $u$ auch eine ganze Grösse. Durch wiederholte Anwendung dieses Satzes folgt, dass jede ganze rationale Function von ganzen Grössen mit ganzen rationalen Coëfficienten ebenfalls eine ganze Grösse ist.

3. Wenn eine algebraische Grösse $y$ einer Gleichung genügt von der Form

$$(3)\qquad y^\nu + \alpha_1 y^{\nu-1} + \alpha_{\nu-1} y + \alpha_\nu = 0,$$

deren Coëfficienten $\alpha_1 \ldots \alpha_\nu$ ganze algebraische Grössen sind, so ist auch $y$ eine ganze algebraische Grösse.

Denn nach Voraussetzung genügen die $\alpha_1, \ldots \alpha_\nu$ gewissen Gleichungen mit ganzen rationalen Coëfficienten. Denkt man sich auf der linken Seite von (3) für die Coëfficienten alle möglichen Combinationen der Wurzeln dieser Gleichungen gesetzt und die so gewonnenen Ausdrücke mit einander multiplicirt, so entsteht eine ganze rationale Function von $y$, deren Coëfficienten als symmetrische Functionen der Wurzeln jener Gleichungen rational sind. Sie sind aber auch, da sie aus ganzen Grössen, nämlich den verschiedenen Werthen der $\alpha$ durch Addition und Multiplication zusammengesetzt sind, nach 2. ganze algebraische, und mithin ganze rationale Grössen. $y$ erscheint somit als Wurzel einer rationalen Gleichung mit ganzen Coëfficienten und ist also eine ganze algebraische Grösse.

4. Ist $F(y) = 0$ die rationale Gleichung niedrigsten Grades, welcher die ganze Grösse $y$ genügt, so hat $F$ ganze Coëfficienten. Denn es genügt $y$ irgend einer rationalen Gleichung $\Phi(y) = 0$, mit ganzen Coëfficienten und $\Phi(t)$ muss durch $F(t)$ theilbar sein. Folglich sind alle Wurzeln von $F$ unter denen von $\Phi$ enthalten und sind also ganze algebraische Grössen. Aus diesen setzen sich aber die Coëfficienten von $F$ durch Addition und Multiplication zusammen und sind daher ebenfalls ganze Grössen.

5. Es sei jetzt

$$(4)\qquad F(y) = y^n + a_1 y^{n-1} + \cdots a_{n-1} y + a_n = 0$$

eine Gleichung mit ganzen rationalen Coëfficienten, von der wir nur vorauszusetzen brauchen, dass sie keine mehrfachen Wurzeln habe, dass also nicht $F'(y)$ gleichzeitig mit $F(y)$ verschwinde.

Die Grösse $y$ giebt Anlass zu einem algebraischen Körper $\mathfrak{K}(y)$, dessen Elemente in der Form ausdrückbar sind:

$$(5)\qquad \omega = b_0 + b_1 y + \cdots b_{n-1} y^{n-1},$$

worin die $b$ ganze oder gebrochene rationale Grössen sind. Unter den Grössen dieses Körpers sind unendlich viele ganze enthalten, unter anderen alle die, in welchen die $b_0, b_1, \ldots b_n$ selbst ganze rationale Grössen sind. Es ist aber keineswegs immer nothwendig, dass diese Coëfficienten ganz seien, damit $\omega$ eine ganze Grösse sei.

Es ist dies eine in der Theorie der algebraischen Grössen fundamental wichtige Frage, auf die näher einzugehen hier nicht der Ort ist. Nur einen hierauf bezüglichen Satz, von dem wir später mehrfach Gebrauch zu machen haben, müssen wir hier ableiten.

Jede ganze Grösse $\mu$ des Körpers $\mathfrak{K}(y)$ kann dargestellt werden in der Form:

$$\mu = \frac{\psi(y)}{F'(y)}, \tag{6}$$

so dass

$$\psi(y) = b_0 + b_1 y + \cdots b_{n-1} y^{n-1} \tag{7}$$

ganze rationale Coëfficienten hat.

Beim Beweise setzen wir zunächst voraus, es sei $F(y)$ irreducibel, so dass zugleich mit $\mu$ die mit $\mu$ conjugirten Grössen ganze Grössen der mit $\mathfrak{K}(y)$ conjugirten Körper sind. Beziehen wir das Zeichen $\Sigma$ auf diese conjugirten Werthe, so ist, wie aus elementaren Sätzen über Partialbruchzerlegung folgt [vgl. §. 9 (2)]:

$$\Sigma \frac{y^\varkappa}{F'(y)} = 0, \text{ wenn } 0 \leqq \varkappa \leqq n - 2, \tag{8}$$

ferner folgt:

$$\Sigma \frac{y^{n-1}}{F'(y)} = 1, \tag{9}$$

und dann aus (4):

$$\Sigma \frac{y^n}{F'(y)} = -a_1, \quad \Sigma \frac{y^{n+1}}{F'(y)} = a_1^2 - a_2 \ldots, \tag{10}$$

und allgemein ist

$$\Sigma \frac{y^\varkappa}{F'(y)} = s_\varkappa, \tag{11}$$

wenn $\varkappa \geqq n - 1$, eine ganze rationale Grösse, wie man aus (4) durch den Schluss von $\varkappa$ auf $\varkappa + 1$ findet. Nun lässt sich das Product $\mu F'(y)$ gewiss in der Form $\psi(y)$ darstellen, nur bleibt noch nachzuweisen, dass die Coëfficienten $b_0, \ldots b_{n-1}$ ganze Grössen sind. Dies ergiebt sich aber leicht mit Hülfe der letzten Formeln aus 2., denn es ist nach (8) bis (11):

$$\begin{aligned} \Sigma \mu &= b_{n-1} \\ \Sigma y \mu &= s_n b_{n-1} + b_{n-2} \\ \Sigma y^2 \mu &= s_{n+1} b_{n-1} + s_n b_{n-2} + b_{n-3} \\ &\cdots\cdots\cdots\cdots\cdots \end{aligned}$$

und daher $b_{n-1}, b_{n-2}, b_{n-3}, \ldots$ ganze Grössen.

Ist aber $F(t)$ nicht irreducibel, sondern in

$$F(t) = F_1(t)\, F_2(t)$$

zerlegbar und ist $F_1(t)$ der irreducible Factor, der für $t = y$ verschwindet, so ist

$$F'(y) = F_1'(y)\, F_2(y).$$

Nach dem Bewiesenen ist $\mu$ zunächst in der Form darstellbar:

$$\mu = \frac{\psi_1(y)}{F_1'(y)}$$

und dies geht, indem man Zähler und Nenner mit $F_2(y)$ multiplicirt und dann mittelst $F(y) = 0$ den Grad des Zählers erniedrigt, in die Form (6) über.

Es ist kaum nöthig, zu erwähnen, dass man nicht etwa umgekehrt schliessen darf, dass jede Grösse der Form (6) eine ganze Grösse sei.

6. Der letzte Satz, den wir hier ableiten wollen, bezieht sich auf algebraische Functionen einer Veränderlichen $x$, und den Uebergang von diesen zu Zahlen durch Einsetzen eines speciellen Werthes von $x$.

Es sollen jetzt in (4) die Coëfficienten $a_1, a_2, \ldots a_n$ ganze rationale Functionen einer Veränderlichen $x$ sein. Die numerischen Coëfficienten können irgend einem festgesetzten Rationalitätsbereich, z. B. dem der rationalen Zahlen, angehören.

Eine ganze algebraische Function von $x$ kann, wie aus ihrer Definition unmittelbar hervorgeht, für keinen endlichen Werth von $x$ unendlich werden. Nun ist in der Darstellung (6) einer ganzen Function des Körpers $\mathfrak{K}(y)$ nur vorausgesetzt, dass $F'(y)$ nicht identisch verschwindet; es ist aber nicht ausgeschlossen, dass $F'(y)$ für einen besonderen Werth $x_0$ von $x$, für welchen $y = y_0$ wird, verschwinde, und da $\mu$ für einen solchen nicht unendlich werden kann, so muss auch der Zähler von (6) für denselben Werth von $x$ verschwinden.

Der Ausdruck (6) giebt dann den Werth von $\mu$ in unbestimmter Form, und es handelt sich darum, ihn zu bestimmen. Die Werthe $x_0$, $y_0$ werden im Allgemeinen nicht dem ursprünglich festgesetzten Rationalitätsbereich der Coëfficienten der $a_1, \ldots a_n$ angehören.

Wir machen zunächst folgende allgemeine Erwägung. Die in (4) vorkommende Function:

$$(13) \qquad F(t) = (t - y)(t - y_1) \ldots (t - y_{n-1})$$

sei irgendwie in die zwei Factoren $F_1(t)$ und $F_2(t)$ zerlegt, so dass

$$(14)\qquad \begin{aligned} F_1(t) &= (t-y)(t-y_1)\dots(t-y_{\lambda-1}) \\ &= t^\lambda + \alpha_1 t^{\lambda-1} + \dots + \alpha_\lambda, \end{aligned}$$

$$(15)\qquad \begin{aligned} F_2(t) &= (t-y_\lambda)(t-y_{\lambda+1})\dots(t-y_{n-1}) \\ &= t^{n-\lambda} + \beta_1 t^{n-\lambda-1} + \dots + \beta_{n-\lambda}, \end{aligned}$$

worin die Coëfficienten $\alpha$, $\beta$ algebraische (natürlich nicht rationale) Functionen von $x$ sind.

Indem wir die Division $F(t):F_1(t)$ ausführen, können wir die $\beta$ als ganze rationale Functionen der $\alpha$ und der $a$ darstellen. Da $F_1(y) = 0$ ist, so können wir nach (6) setzen:

$$(16)\qquad \mu = \frac{\psi(y)}{F_2(y)F_1'(y)}$$

und da alle Potenzen von $\mu$ gleichfalls ganze Functionen sind:

$$(17)\qquad \mu^2 = \frac{\psi_2(y)}{F_2(y)F_1'(y)},\quad \mu^3 = \frac{\psi_3(y)}{F_2(y)F_1'(y)}\dots$$

Wir setzen nun

$$(18)\qquad F_2(y)F_2(y_1)\dots F_2(y_{\lambda-1}) = P$$

und können, da $P$ eine symmetrische Function der Wurzeln von (14) ist, $P$ ausdrücken als ganze rationale Function der $\alpha$, der $\beta$ und der $a$, also auch der $\alpha$ und der $a$ allein.

Ebenso ist

$$P_1 = F_2(y_1)\dots F_2(y_{\lambda-1}) = \frac{P}{F_2(y)}$$

als ganze symmetrische Function der Wurzeln der Gleichung

$$\frac{F_1(t)}{t-y} = 0$$

eine ganze rationale Function von $y$, $\alpha$, $a$. Hiernach können wir, wenn wir mit $\varphi_1(y)$, $\varphi_2(y)$, $\varphi_3(y)\dots$ ganze rationale Functionen von $x$, $y$, $\alpha_1$, $\alpha_2\dots$, $\alpha_\lambda$ bezeichnen, deren Zahlencoëfficienten im ursprünglichen Rationalitätsbereich enthalten sind, setzen

$$(19)\qquad \mu = \frac{\varphi_1(y)}{PF_1'(y)},\quad \mu^2 = \frac{\varphi_2(y)}{PF_1'(y)},\quad \mu^3 = \frac{\varphi_3(y)}{PF_1'(y)}\dots,$$

und hierin kann $y$ auch durch $y_1$, $y_2\dots$, $y_{\lambda-1}$ ersetzt werden, wenn gleichzeitig für $\mu$ die entsprechenden conjugirten Werthe $\mu_1$, $\mu_2\dots$, $\mu_{\lambda-1}$ gesetzt werden.

Setzen wir die Functionen $\varphi_\varkappa$ in die Form:

$$\varphi_\varkappa(y) = c_0^{(\varkappa)}\, y^{\lambda-1} + c_1^{(\varkappa)}\, y^{\lambda-2} + \cdots c_{\lambda-1}^{(\varkappa)},$$

so ergiebt sich aus (8), (9), wenn die Summe $\Sigma$ auf die $\lambda$ Werthe $y, y_1 \ldots, y_{\lambda-1}$ erstreckt wird:

$$(20) \qquad \Sigma\mu = \frac{c_0^{(1)}}{P}, \quad \Sigma\mu^2 = \frac{c_0^{(2)}}{P}, \ldots \quad \Sigma\mu^3 = \frac{c_0^{(3)}}{P} \ldots,$$

und da man aus den Potenzsummen der Wurzeln einer Gleichung die Coëfficienten ganz und rational zusammensetzen kann, so ergiebt sich aus (20) eine Gleichung $\lambda$ten Grades, deren Wurzeln $\mu, \mu_1 \ldots, \mu_{\lambda-1}$ sind, von der Form

$$(21) \qquad C_0\,\mu^\lambda + C_1\,\mu^{\lambda-1} + \cdots C_{\lambda-1}\,\mu + C_\lambda = 0,$$

deren Coëfficienten ganze rationale Functionen von $x, \alpha_1, \alpha_2 \ldots, \alpha_{\lambda-1}$ sind, und worin $C_0$ eine Potenz von $P$ ist. Die numerischen Coëfficienten in den Functionen $C$ gehören dem ursprünglichen Rationalitätsbereich an.

Diese ganze Betrachtung ist nur in dem Falle für uns von Interesse, dass für einen besonderen Werth $x_0$ von $x$ die Werthe $y, y_1 \ldots, y_{\lambda-1}$ einander gleich und gleich $y_0$ werden, während die übrigen $y_\lambda, y_{\lambda+1} \ldots, y_{n-1}$ von $y_0$ verschieden sind.

Dann wird für $x = x_0$:

$$F_1(t) = (t - y_0)^\lambda,$$

also

$$\alpha_1 = -\lambda y_0, \quad \alpha_2 = \frac{\lambda(\lambda-1)}{1.2}\, y_0^2 \ldots, \quad \alpha_\lambda = (-1)^\lambda\, y_0^\lambda.$$

Die Coëfficienten von (21) gehen über in ganze rationale Functionen von $x_0$, $y_0$ und der Coëfficient $C_0$ der höchsten Potenz von $\mu$ ist als Potenz von $P$ nach der Bedeutung dieser letzteren Grösse von Null verschieden. Für ein solches Werthpaar $x_0$, $y_0$ erhält man also $\lambda$ Werthe für $\mu$, welche Wurzeln der Gleichung (21) sind, die im Allgemeinen von einander verschieden sind, in besonderen Fällen aber auch theilweise oder alle einander gleich werden können.

## Achter Abschnitt.

# Multiplication und Theilung der elliptischen Functionen.

---

### §. 60. Multiplication der elliptischen Functionen.

Unter der Multiplication der elliptischen Functionen versteht man die Darstellung der Functionen $\operatorname{sn} n v$, $\operatorname{cn} n v$, $\operatorname{dn} n v$ für ein ganzzahliges $n$ als rationale Functionen von $\operatorname{sn} v$, $\operatorname{cn} v$, $\operatorname{dn} v$, eine Aufgabe, die, wie aus dem Additionstheorem ersichtlich ist, immer gelöst werden kann.

Die Form der Lösung ergiebt sich leicht aus der Betrachtung der $\vartheta$-Functionen.

Es sind, wie aus §. 18 unmittelbar zu ersehen, die Functionen $\vartheta_{g_1, g_2}(n u)$ $\Theta$-Functionen der Ordnung $n^2$, deren Charakteristik $(0, 0)$ bei geradem $n$, $(g_1, g_2)$ bei ungeradem $n$ ist. Ueberdies ist $\vartheta_{11}(n u)$ eine ungerade, $\vartheta_{00}(n u)$, $\vartheta_{10}(n u)$, $\vartheta_{01}(n u)$ sind gerade Functionen von $u$. Es lassen sich also diese Functionen rational durch die $\vartheta$-Functionen darstellen und die Sätze des §. 18 ergeben die Form dieser Ausdrücke. Es wird, wenn wir wieder mit $F^{(\nu)}(x, y)$ eine ganze, rationale, homogene Function $\nu$ter Ordnung bezeichnen:

bei geradem $n$:

$$(1)\quad \begin{aligned} \vartheta_{11}(n u) &= \vartheta_{00}(u)\, \vartheta_{01}(u)\, \vartheta_{10}(u)\, \vartheta_{11}(u)\, F^{\left(\frac{n^2}{2} - 2\right)}\left(\vartheta_{11}^2(u), \vartheta_{01}^2(u)\right) \\ \vartheta_{g_1, g_2}(n u) &= F^{\left(\frac{n^2}{2}\right)}\left(\vartheta_{11}^2(u), \vartheta_{01}^2(u)\right), \quad (g_1, g_2) = (10), (01), (00), \end{aligned}$$

bei ungeradem $n$:

$$(2) \qquad \vartheta_{g_1, g_2}(n u) = \vartheta_{g_1, g_2}(u)\, F^{\left(\frac{n^2-1}{2}\right)}\left(\vartheta_{11}^2(u),\, \vartheta_{01}^2(u)\right).$$

Wenn wir diese Formeln durch $\vartheta_{01}(u)^{n^2}$ dividiren, so lassen sich die rechten Seiten als ganze rationale Functionen von den elliptischen Functionen $\operatorname{sn} v$, $\operatorname{cn} v$, $\operatorname{dn} v$ darstellen (§. 37). Wenn wir die linken Seiten alsdann durch die Jacobi'schen Functionen $\Theta(v)$, $H(v)$ (§. 38) ausdrücken, und zur Abkürzung:

$$(3) \qquad \operatorname{sn} v = x, \qquad \operatorname{cn} v = y, \qquad \operatorname{dn} v = z$$

setzen, so können wir die Formeln (1), (2), indem wir einen constanten Factor passend bestimmen, so schreiben:

I. bei geradem $n$:

$$\frac{\Theta(K)\,\Theta(0)^{n^2-1}}{H(K)}\,\frac{H(n v)}{\Theta(v)^{n^2}} = x y z\, A(x^2), \qquad A(0) = n$$

$$\frac{\Theta(0)^{n^2}}{H(K)}\,\frac{H(n v + K)}{\Theta(v)^{n^2}} = B(x^2), \qquad B(0) = 1$$

$$\frac{\Theta(0)^{n^2}}{\Theta(K)}\,\frac{\Theta(n v + K)}{\Theta(v)^{n^2}} = C(x^2), \qquad C(0) = 1$$

$$\Theta(0)^{n^2-1}\,\frac{\Theta(n v)}{\Theta(v)^{n^2}} = D(x^2), \qquad D(0) = 1.$$

II. bei ungeradem $n$:

$$\frac{\Theta(K)\,\Theta(0)^{n^2-1}}{H(K)}\,\frac{H(n v)}{\Theta(v)^{n^2}} = x\, A(x^2), \qquad A(0) = n$$

$$\frac{\Theta(0)^{n^2}}{H(K)}\,\frac{H(n v + K)}{\Theta(v)^{n^2}} = y\, B(x^2), \qquad B(0) = 1$$

$$\frac{\Theta(0)^{n^2}}{\Theta(K)}\,\frac{\Theta(n v + K)}{\Theta(v)^{n^2}} = z\, C(x^2), \qquad C(0) = 1$$

$$\Theta(0)^{n^2-1}\,\frac{\Theta(n v)}{\Theta(v)^{n^2}} = D(x^2), \qquad D(0) = 1,$$

worin $A$, $B$, $C$, $D$ ganze rationale Functionen von $x^2$ sind, deren Grade aus den Formeln (1), (2) abzulesen sind. Da zwei verschiedene der vier Functionen $\vartheta_{g, g_2}(n u)$ niemals für denselben Werth des Arguments verschwinden, so haben keine zwei der vier Functionen $A$, $B$, $C$, $D$ einen gemeinsamen Theiler.

Wenn man von diesen Formeln je die drei ersten durch die letzte dividirt, so erhält man die Multiplication der elliptischen Functionen.

III. Bei geradem $n$:

$$\operatorname{sn} n v = \frac{x y z A(x^2)}{D(x^2)},$$

$$\operatorname{cn} n v = \frac{B(x^2)}{D(x^2)},$$

$$\operatorname{dn} n v = \frac{C(x^2)}{D(x^2)},$$

IV. Bei ungeradem $n$:

$$\operatorname{sn} n v = \frac{x A(x^2)}{D(x^2)},$$

$$\operatorname{cn} n v = \frac{y B(x^2)}{D(x^2)},$$

$$\operatorname{dn} n v = \frac{z C(x^2)}{D(x^2)}.$$

Die Coëfficienten von $A$, $B$, $C$, $D$ hängen noch von $\omega$ oder von $\varkappa^2$ ab. Ueber die Art dieser Abhängigkeit geben die Recursionsformeln Aufschluss, die man zur successiven Berechnung von $A$, $B$, $C$, $D$ aus dem Additionstheorem folgert. Wenn wir den Werth des Multiplicators $n$, zu welchem diese Functionen gehören, durch einen Index andeuten, so haben wir zunächst

$$A_1 = 1, \quad B_1 = 1, \quad C_1 = 1, \quad D_1 = 1; \tag{4}$$

ferner aus den Additionsformeln [§. 39, (16), für $u = v$]:

$$\begin{aligned} \operatorname{sn} 2v &= \frac{2 \operatorname{sn} v \operatorname{cn} v \operatorname{dn} v}{1 - \varkappa^2 \operatorname{sn}^4 v} \\ \operatorname{cn} 2v &= \frac{\operatorname{cn}^2 v - \operatorname{sn}^2 v \operatorname{dn}^2 v}{1 - \varkappa^2 \operatorname{sn}^4 v} \\ \operatorname{dn} 2v &= \frac{\operatorname{dn}^2 v - \varkappa^2 \operatorname{sn}^2 v \operatorname{cn}^2 v}{1 - \varkappa^2 \operatorname{sn}^4 v} \end{aligned} \tag{5}$$

$$\begin{aligned} A_2 &= 2 \\ B_2 &= 1 - 2x^2 + \varkappa^2 x^4 \\ C_2 &= 1 - 2\varkappa^2 x^2 + \varkappa^2 x^4 \\ D_2 &= 1 - \varkappa^2 x^4. \end{aligned} \tag{6}$$

Wenn wir in (5) $v$ durch $nv$ ersetzen, so folgt:

$$\begin{aligned} A_{2n} &= 2 A_n B_n C_n D_n \\ B_{2n} &= B_n^2 D_n^2 - x^2 y^2 z^2 A_n^2 C_n^2, && n \text{ gerade}, \\ &= y^2 B_n^2 D_n^2 - x^2 z^2 A_n^2 C_n^2, && n \text{ ungerade}, \\ C_{2n} &= C_n^2 D_n^2 - \varkappa^2 x^2 y^2 z^2 A_n^2 B_n^2, && n \text{ gerade}, \\ &= z^2 C_n^2 D_n^2 - \varkappa^2 x^2 y^2 A_n^2 B_n^2, && n \text{ ungerade}, \\ D_{2n} &= D_n^4 - \varkappa^2 x^4 y^4 z^4 A_n^4, && n \text{ gerade}, \\ &= D_n^4 - \varkappa^2 x^4 A_n^4, && n \text{ ungerade}, \end{aligned} \tag{7}$$

und wenn man in den Additionsformeln des §. 39 $u = nv$, $v = (n + 1)v$ setzt:

$$
\begin{aligned}
A_{2n+1} &= y^2 z^2 A_n D_n B_{n+1} C_{n+1} + A_{n+1} D_{n+1} C_n B_n, \quad n \text{ gerade},\\
&= A_n D_n B_{n+1} C_{n+1} + y^2 z^2 A_{n+1} D_{n+1} C_n B_n, \quad n \text{ ungerade},\\
(8)\quad B_{2n+1} &= B_n B_{n+1} D_n D_{n+1} - x^2 z^2 A_n A_{n+1} C_n C_{n+1}\\
C_{2n+1} &= C_n C_{n+1} D_n D_{n+1} - \varkappa^2 x^2 y^2 A_n A_{n+1} B_n B_{n+1}\\
D_{2n+1} &= D_n^2 D_{n+1}^2 - \varkappa^2 x^4 y^2 z^2 A_n^2 A_{n+1}^2.
\end{aligned}
$$

Aus diesen Formeln schliesst man, dass die $A$, $B$, $C$, $D$ ganze rationale Functionen von $\varkappa^2$ sind, und dass die Zahlcoëfficienten ganze rationale Zahlen sind.

Denn nach (4), (6) hat diese Eigenschaft für $n = 1, 2$ statt und folglich nach (7), (8) allgemein.

Ueber den Grad, bis zu welchem $\varkappa^2$ ansteigt, lässt sich noch schliessen, dass die Coëfficienten von $x^{2\nu}$ den Grad $\nu$ in Bezug auf $\varkappa^2$ nicht übersteigen. Denn ist diese Regel richtig für $n$ und $n + 1$, so folgt ihre Richtigkeit für $2n$ und $2n + 1$, und für $n = 1$, $n = 2$ trifft sie zu.

Aus den Grundgleichungen zwischen den drei elliptischen Functionen:

$$1 = \operatorname{cn}^2 v + \operatorname{sn}^2 v = \operatorname{dn}^2 v + \varkappa^2 \operatorname{sn}^2 x$$

ergeben sich noch die Relationen:

$$
(9)\quad
\begin{aligned}
D^2 &= B^2 + x^2 y^2 z^2 A^2 = C^2 + \varkappa^2 x^2 y^2 z^2 A^2, \quad n \text{ gerade},\\
D^2 &= y^2 B + x^2 A^2 \qquad = z^2 C^2 + \varkappa^2 x^2 A^2, \quad n \text{ ungerade}.
\end{aligned}
$$

Die ersten Coëfficienten in den Functionen $A$, $B$, $C$, $D$ sind schon oben durch die Formeln

$$A(0) = n, \qquad B(0) = C(0) = D(0) = 1$$

bestimmt.

Um auch die Coëfficienten der höchsten Potenzen von $x$ in $A$, $B$, $C$, $D$ zu finden, setze man in I. II., $v + iK'$ an Stelle von $v$ und wende die Formeln der §§. 38, 39 an.

Es ergiebt sich so für ein gerades $n$:

$$
(10)\quad
\begin{aligned}
A(x^2) &= (-1)^{\frac{n-2}{2}} (\sqrt{\varkappa}\, x)^{n^2-4}\, A\left(\frac{1}{\varkappa^2 x^2}\right)\\
B(x^2) &= (\sqrt{\varkappa}\, x)^{n^2}\, B\left(\frac{1}{\varkappa^2 x^2}\right)\\
C(x^2) &= (\sqrt{\varkappa}\, x)^{n^2}\, C\left(\frac{1}{\varkappa^2 x^2}\right)\\
D(x^2) &= (-1)^{\frac{n}{2}} (\sqrt{\varkappa}\, x)^{n^2}\, D\left(\frac{1}{\varkappa^2 x^2}\right),
\end{aligned}
$$

und daraus finden sich, wenn man $x$ unendlich setzt, die Coëfficienten der höchsten Potenzen von $x$ in $A, B, C, D$:

$$(-1)^{\frac{n-2}{2}}\, n \sqrt{\varkappa}^{\,n^2-4}, \quad \sqrt{\varkappa}^{\,n^2}, \quad \sqrt{\varkappa}^{\,n^2}, \quad (-1)^{\frac{n}{2}} \sqrt{\varkappa}^{\,n^2};$$

und für ein ungerades $n$:

$$\begin{aligned} A(x^2) &= (-1)^{\frac{n-1}{2}} (\sqrt{\varkappa}\, x)^{n^2-1} D\left(\frac{1}{\varkappa^2 x^2}\right) \\ B(x^2) &= \phantom{(-1)^{\frac{n-1}{2}}} (\sqrt{\varkappa}\, x)^{n^2-1} C\left(\frac{1}{\varkappa^2 x^2}\right) \\ C(x^2) &= \phantom{(-1)^{\frac{n-1}{2}}} (\sqrt{\varkappa}\, x)^{n^2-1} B\left(\frac{1}{\varkappa^2 x^2}\right) \\ D(x^2) &= (-1)^{\frac{n-1}{2}} (\sqrt{\varkappa}\, x)^{n^2-1} A\left(\frac{1}{\varkappa^2 x^2}\right), \end{aligned} \tag{11}$$

also die Coëfficienten der höchsten Potenzen von $x$ in $A, B, C, D$:

$$(-1)^{\frac{n-1}{2}} \sqrt{\varkappa}^{\,n^2-1}, \quad \sqrt{\varkappa}^{\,n^2-1}, \quad \sqrt{\varkappa}^{\,n^2-1}, \quad (-1)^{\frac{n-1}{2}}\, n \sqrt{\varkappa}^{\,n^2-1}.$$

Im Falle eines ungeraden $n$ kann man die vier Polynome $A, B, C, D$ auf eines zurückführen, wie man findet, wenn man in II. $v$ um $K$ und um $iK'$ vermehrt:

$$\begin{aligned} A(x^2) &= (-1)^{\frac{n-1}{2}} \left(\frac{z}{\sqrt{\varkappa'}}\right)^{n^2-1} B\left(\frac{y^2}{z^2}\right) \\ &= (-1)^{\frac{n-1}{2}} \left(\sqrt{\frac{\varkappa}{\varkappa'}}\, y\right)^{n^2-1} C\left(\frac{z^2}{y^2}\right) \\ &= (-1)^{\frac{n-1}{2}} (\sqrt{\varkappa}\, x)^{n^2-1} D\left(\frac{1}{\varkappa^2 x^2}\right). \end{aligned} \tag{12}$$

Die der Multiplication entgegengesetzte Aufgabe ist die der Theilung, d. h. die der Darstellung der Functionen:

$$\operatorname{sn}\frac{v}{n}, \quad \operatorname{cn}\frac{v}{n}, \quad \operatorname{dn}\frac{v}{n},$$

durch $\operatorname{sn} v$, $\operatorname{cn} v$, $\operatorname{dn} v$.

Die Lösung dieser Aufgabe ist durch III., IV. auf die Auflösung einer algebraischen Gleichung, der Theilungsgleichung, zurückgeführt, deren algebraische Eigenschaften in unseren ferneren Betrachtungen das hauptsächlichste Interesse in Anspruch nehmen.

## §. 61. Multiplication der Function $\wp(u)$.

Eine sehr elegante Form erhält die Multiplicationstheorie für die Weierstrass'sche Function $\wp(u)$ mit den beiden Perioden $\omega_1, \omega_2$.

Betrachten wir die doppelt periodische Function

$$\wp(nu) - \wp(u), \tag{1}$$

worin $n$ eine beliebige positive ganze Zahl sein mag. Diese Function wird unendlich für $u = 0$, und zwar so, dass

$$\wp(nu) - \wp(u) + \frac{n^2 - 1}{n^2} \frac{1}{u^2} \tag{2}$$

für $u = 0$ endlich bleibt. Ausserdem wird sie aber unendlich für alle Werthe $u^*$ von $u$, welche der Bedingung

$$n u^* \equiv 0 \pmod{\omega_1, \omega_2}$$

genügen, also von der Form sind:

$$u^* = \frac{\nu_1 \omega_1 + \nu_2 \omega_2}{n}, \tag{3}$$

worin $\nu_1, \nu_2$ beliebige ganze Zahlen bedeuten. Wir erhalten alle in (3) enthaltenen incongruenten Werthe, wenn wir $\nu_1$ und $\nu_2$ je ein vollständiges Restsystem nach dem Modul $n$ durchlaufen lassen.

Die Function (1) verschwindet für alle diejenigen Werthe $u^0$ von $u$, welche von Null verschieden sind und der Bedingung

$$\pm n u^0 \equiv u^0 \pmod{\omega_1, \omega_2}$$

genügen, also für

$$u^0 = \frac{\nu_1 \omega_1 + \nu_2 \omega_2}{n \pm 1}, \tag{4}$$

wenn wieder $\nu_1, \nu_2$ beliebige ganze Zahlen sind. Die Nullpunkte sind von der ersten, die Unendlichkeitspunkte von der zweiten Ordnung.

Wir führen daher jetzt eine Function $\psi_n(u)$ ein, die wir folgendermaassen erklären:

$$\psi_n(u)^2 = n^2 \prod^{\nu_1, \nu_2} \left[\wp(u) - \wp\left(\frac{\nu_1 \omega_1 + \nu_2 \omega_2}{n}\right)\right], \tag{5}$$

wobei $\nu_1, \nu_2$ je ein vollständiges Restsystem nach dem Modul $n$, mit alleinigem Ausschluss des Werthepaares 0, 0 durchlaufen, und fügen noch die Bestimmung hinzu, dass $\psi_1 = 1$ sein soll.

Wenn $n$ ungerade ist, so kommt in dem Product (5) jeder Linearfactor zweimal vor, da die beiden incongruenten Werthe

$$u = \pm \frac{\nu_1 \omega_1 + \nu_2 \omega_2}{n}$$

den gleichen Werth von $\wp(u)$ ergeben. Ist aber $n$ gerade, so kommen wieder in (5) alle Linearfactoren zweimal vor, mit Ausnahme der drei

$$\wp(u) - \wp\left(\frac{\omega_1}{2}\right), \quad \wp(u) - \wp\left(\frac{\omega_2}{2}\right), \quad \wp(u) - \wp\left(\frac{\omega_1 + \omega_2}{2}\right),$$

welche nur einfach vorkommen. Beachtet man nun, dass nach §. 31 und §. 41

$$\wp'(u)^2 = 4\left[\wp(u) - \wp\left(\frac{\omega_1}{2}\right)\right]\left[\wp(u) - \wp\left(\frac{\omega_2}{2}\right)\right]\left[\wp(u) - \wp\left(\frac{\omega_1 + \omega_2}{2}\right)\right]$$

ist, so ergiebt sich das Resultat:

$$\begin{aligned} &n \text{ ungerade:} \quad \psi_n = P_n \\ &n \text{ gerade:} \quad \psi_n = \wp'(u) P_n, \end{aligned} \tag{6}$$

wenn $P_n$ eine ganze rationale Function von $\wp(u)$ bedeutet, welche bei ungeradem $n$ vom Grade $\frac{1}{2}(n^2 - 1)$ und bei geradem $n$ vom Grade $\frac{1}{2}(n^2 - 4)$ ist, und in welcher das Glied höchster Ordnung bezw. gleich

$$n\, \wp(u)^{\frac{n^2-1}{2}}, \qquad -\frac{n}{2}\, \wp(u)^{\frac{n^2-4}{2}}$$

ist, wodurch zugleich das nach (5) noch unbestimmte Vorzeichen bestimmt ist. Bei dieser Bestimmung der Vorzeichen ist das Anfangsglied in der Entwickelung von $\psi_n(u)$ nach steigenden Potenzen von $u$ in beiden Fällen:

$$\frac{n}{u^{n^2-1}}. \tag{7}$$

Erwägt man nun, dass die Unendlichkeitspunkte der Function (1) mit den Nullpunkten von $\psi_n(u)$ zusammenfallen und die Nullpunkte von (1) mit den Nullpunkten von $\psi_{n \pm 1}(u)$, dass also

$$\frac{\psi_n(u)^2 [\wp(nu) - \wp(u)]}{\psi_{n+1}(u)\, \psi_{n-1}(u)}$$

eine überall endliche doppelt periodische Function und daher eine Constante ist, deren Werth sich aus $u = 0$ gleich $-1$ ergiebt, so folgt

$$\wp(n u) = \wp(u) - \frac{\psi_{n+1}(u)\,\psi_{n-1}(u)}{\psi_n(u)^2}. \tag{9}$$

Wir bestimmen zunächst die Function $P_n$ in den ersten Fällen $n = 1, 2, 3, 4$. Dazu bilden wir nach dem Additionstheorem der $\wp$-Function (§. 44):

$$4\,[\wp(u) + \wp(v) + \wp(u + v)] = \left(\frac{\wp'(u) - \wp'(v)}{\wp(u) - \wp(v)}\right)^2,$$

indem wir $u = v$ setzen und den Grenzwerth rechts durch Differentiation bestimmen:

$$\wp(2 u) + 2\wp(u) = \frac{1}{4}\left(\frac{\wp''(u)}{\wp'(u)}\right)^2 = \frac{1}{4}\,\frac{\left(6\wp(u)^2 - \frac{1}{2}\,g_2\right)^2}{4\wp(u)^3 - g_2\wp(u) - g_3},$$

oder

$$\wp(2 u) = \wp(u) - \frac{3\wp(u)^4 - \frac{3}{2}\,g_2\wp(u)^2 - 3\,g_3\wp(u) - \frac{g_2^2}{16}}{\wp'(u)^2}, \tag{10}$$

so dass

$$\psi_1 = 1, \quad \psi_2 = -\wp'(u), \quad \psi_3 = P_3,$$

$$P_1 = 1, \quad P_2 = -1, \quad P_3 = 3\wp(u)^4 - \frac{3}{2}\,g_2\wp(u)^2 - 3\,g_3\wp(u) - \frac{g_2^2}{16} \tag{11}$$

wird. Wir erhalten ferner aus der Additionsformel, (§. 44):

$$\wp(v + u) - \wp(v - u) = -\frac{\wp'(u)\,\wp'(v)}{[\wp(v) - \wp(u)]^2},$$

indem wir $v = 2u$ setzen:

$$\wp(3 u) - \wp(u) = -\frac{\wp'(u)\,\wp'(2 u)}{[\wp(2 u) - \wp(u)]^2} = -\frac{\wp'(u)^5\;\wp'(2 u)}{\psi_3(u)^2},$$

$$= -\frac{\psi_2(u)\;\psi_4(u)}{\psi_3(u)^2},$$

also:

$$\psi_4(u) = \wp'(u)\,P_4 = -\wp'(u)^4\,\wp'(2 u),$$

und wenn man aus (10) den Werth $\wp'(2 u)$ bildet:

$$P_4 = -2\wp(u)^6 + \frac{5}{2}\,g_2\,\wp(u)^4 + 10\,g_3\,\wp(u)^3 + \frac{5}{8}\,g_2^2\wp(u)^2 + \frac{1}{2}\,g_2\,g_3\,\wp(u) + g_3^2 - \frac{g_2^3}{32}. \tag{12}$$

Für grössere Werthe von $n$ leiten wir Recursionsformeln ab. Zu diesem Zweck wenden wir die Formel (9) auf zwei verschiedene Zahlen $m$, $n$ an und erhalten:

$$\wp(u) - \wp(mu) = \frac{\psi_{m+1}(u)\,\psi_{m-1}(u)}{\psi_m(u)^2}$$

$$\wp(u) - \wp(nu) = \frac{\psi_{n+1}(u)\,\psi_{n-1}(u)}{\psi_n(u)^2},$$

woraus zu ersehen ist, dass die rechten Seiten einander gleich werden für solche Werthe $u^0$ von $u$, welche von Null verschieden sind und der Bedingung genügen

$$m u^0 \equiv \pm n u^0 \pmod{\omega_1, \omega_2},$$

oder

$$(m \pm n) u^0 \equiv 0 \pmod{\omega_1, \omega_2};$$

für dieselben Werthe $u^0$ verschwinden aber auch die Functionen

$$\psi_{m \pm n}(u),$$

so dass die beiden Functionen:

$$\psi_{m+1}(u)\,\psi_{m-1}(u)\,\psi_n(u)^2 - \psi_{n+1}(u)\,\psi_{n-1}(u)\,\psi_m(u)^2$$
$$\psi_{m+n}(u)\,\psi_{m-n}(u),$$

welches nach (6) ganze rationale Functionen von $\wp(u)$ sind, für die nämlichen endlichen Werthe von $\wp(u)$ verschwinden. Sie unterscheiden sich also nur durch einen constanten Factor von einander, der sich aus (7) gleich 1 ergiebt. Wir haben daher

$$(12) \qquad \psi_{m+n}(u)\,\psi_{m-n}(u) =$$
$$\psi_{m+1}(u)\,\psi_{m-1}(u)\,\psi_n(u)^2 - \psi_{n+1}(u)\,\psi_{n-1}(u)\,\psi_m(u)^2.$$

Diese Formel wenden wir auf zwei specielle Fälle an, indem wir $n+1$, $n$ oder $n+1$, $n-1$ an Stelle von $m$, $n$ setzen, und erhalten so:

$$\psi_{2n+1}(u) = \psi_{n+2}(u)\,\psi_n(u)^3 - \psi_{n+1}(u)^3\,\psi_{n-1}(u)$$

$$\wp'(u)\,\psi_{2n}(u) = -\psi_n(u)[\psi_{n+2}(u)\,\psi_{n-1}(u)^2 - \psi_{n+1}(u)^2\,\psi_{n-2}(u)],$$

und daraus erhält man nach (6) die Recursionsformeln für $P_n$:

$$(13) \qquad P_{2n+1} = \wp'(u)^4 P_{n+2} P_n^3 - P_{n+1}^3 P_{n-1}, \; n \text{ gerade},$$
$$= P_{n+2} P_n^3 - \wp'(u)^4 P_{n+1}^3 P_{n-1}, \; n \text{ ungerade}.$$

$$(14) \qquad P_{2n} = -P_n(P_{n+2} P_{n-1}^2 - P_{n+1}^2 P_{n-2}).$$

Da sich die Functionen $P_n$ alle hiernach aus $P_1$, $P_2$, $P_3$, $P_4$ berechnen lassen, so folgt, dass die Coëfficienten von $P_n$ rational aus $g_2$, $g_3$ und rationalen Zahlen zusammengesetzt sind.

Unsere ferneren Betrachtungen über die Theilung knüpfen wir aber an die Multiplicationsformeln der Functionen $\mathrm{sn}\, u$, $\mathrm{cn}\, u$, $\mathrm{dn}\, u$, welche Vortheile bieten, die erst im dritten Theil vollständig zur Geltung kommen werden.

## §. 62. Die Theilung durch 2.

Indem wir uns zunächst zur Betrachtung des einfachsten Falles wenden, setzen wir in den Gleichungen III des §. 60 $n = 2$ und schreiben $v$ an Stelle von $2v$. Dann ist:

$$(1) \qquad x = \mathrm{sn}\,\frac{v}{2}, \qquad y = \mathrm{cn}\,\frac{v}{2}, \qquad z = \mathrm{dn}\,\frac{v}{2},$$

und wir erhalten

$$(2) \qquad \begin{aligned} \mathrm{sn}\, v &= \frac{2xyz}{1 - \varkappa^2 x^4} \\ \mathrm{cn}\, v &= \frac{y^2 - x^2 z^2}{1 - \varkappa^2 x^4} \\ \mathrm{dn}\, v &= \frac{z^2 - \varkappa^2 x^2 y^2}{1 - \varkappa^2 x^4}. \end{aligned}$$

Die beiden letzten dieser Gleichungen sind quadratisch in Bezug auf $x^2$, sie haben aber nur eine gemeinschaftliche Wurzel, denn die Wurzeln der zweiten der Gleichungen (2) sind

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

und die der dritten

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

Man findet nun leicht aus (2):

$$1 + \mathrm{cn}\, v = \frac{2y^2}{1 - \varkappa^2 x^4}, \qquad 1 + \mathrm{dn}\, v = \frac{2z^2}{1 - \varkappa^2 x^4},$$

$$1 - \mathrm{cn}\, v = \frac{2x^2 z^2}{1 - \varkappa^2 x^4}, \qquad 1 - \mathrm{dn}\, v = \frac{2\varkappa^2 x^2 y^2}{1 - \varkappa^2 x^4},$$

$$\mathrm{dn}\, v + \mathrm{cn}\, v = \frac{2y^2 z^2}{1 - \varkappa^2 x^4},$$

also

$$(3)\qquad \begin{aligned} x &= \sqrt{\frac{1-\operatorname{cn} v}{1+\operatorname{dn} v}} = \frac{1}{\varkappa}\sqrt{\frac{1-\operatorname{dn} v}{1+\operatorname{cn} v}}, \\ y &= \sqrt{\frac{\operatorname{dn} v+\operatorname{cn} v}{1+\operatorname{dn} v}},\quad z = \sqrt{\frac{\operatorname{dn} v+\operatorname{cn} v}{1+\operatorname{cn} v}}; \end{aligned}$$

zwischen den Vorzeichen dieser drei Grössen besteht nach der ersten Gleichung (2) noch eine Relation, so dass man nur vier verschiedene Werthsysteme erhält, welche folgende Bedeutung haben:

$$\begin{array}{lll} \operatorname{sn}\left(\frac{v}{2}\right), & \operatorname{cn}\left(\frac{v}{2}\right), & \operatorname{dn}\left(\frac{v}{2}\right), \\ \operatorname{sn}\left(\frac{v}{2}+2K\right), & \operatorname{cn}\left(\frac{v}{2}+2K\right), & \operatorname{dn}\left(\frac{v}{2}+2K\right), \\ \operatorname{sn}\left(\frac{v}{2}+2iK'\right), & \operatorname{cn}\left(\frac{v}{2}+2iK'\right), & \operatorname{dn}\left(\frac{v}{2}+2iK'\right), \\ \operatorname{sn}\left(\frac{v}{2}+2K+2iK'\right), & \operatorname{cn}\left(\frac{v}{2}+2K+2iK'\right), & \operatorname{dn}\left(\frac{v}{2}+2K+2iK'\right). \end{array}$$

Wir führen noch die aus (3) sich ergebenden speciellen Fälle an:

$$\begin{array}{lll} \operatorname{sn}\frac{K}{2} = \frac{1}{\sqrt{1+\varkappa'}}, & \operatorname{sn}\frac{iK'}{2} = \frac{i}{\sqrt{\varkappa}}, & \operatorname{sn}\frac{K+iK'}{2} = \sqrt{\frac{\varkappa+i\varkappa'}{\varkappa}}, \\ \operatorname{cn}\frac{K}{2} = \sqrt{\frac{\varkappa'}{1+\varkappa'}}, & \operatorname{cn}\frac{iK'}{2} = \sqrt{\frac{1+\varkappa}{\varkappa}}, & \operatorname{cn}\frac{K+iK'}{2} = \sqrt{\frac{-i\varkappa'}{\varkappa}}, \\ \operatorname{dn}\frac{K}{2} = \sqrt{\varkappa'}, & \operatorname{dn}\frac{iK'}{2} = \sqrt{1+\varkappa}, & \operatorname{dn}\frac{K+iK'}{2} = \sqrt{\frac{-i\varkappa'}{\varkappa-i\varkappa'}}. \end{array}$$

Hieraus folgt nun, dass man die Theilung durch 2 und mithin auch durch jede Potenz von 2 durch eine Kette von Quadratwurzeln ausführen kann. Setzt man daher die Aufgabe der Theilung durch eine ungerade Zahl als gelöst voraus, so ist die Theilung durch eine gerade Zahl auf Quadratwurzeln zurückgeführt. Im Folgenden beschäftigen wir uns ausschliesslich mit der Theilung durch ungerade Zahlen.

## §. 63. Die Theilung durch eine ungerade Zahl.

Setzt man, wenn $n$ eine ungerade Zahl ist

$$(1)\qquad x = \operatorname{sn}\frac{v}{n},\qquad y = \operatorname{cn}\frac{v}{n},\qquad z = \operatorname{dn}\frac{v}{n},$$

so erhält man aus den Gleichungen IV, §. 60:

$$
\begin{aligned}
&D(x^2)\,\mathrm{sn}\,v - x\,A(x^2) = 0\\
(2)\qquad &D(x^2)\,\mathrm{cn}\,v - y\,B(x^2) = 0\\
&D(x^2)\,\mathrm{dn}\,v - z\,C(x^2) = 0.
\end{aligned}
$$

Die erste dieser Gleichungen ist in Bezug auf die Unbekannte $x$ vom Grade $n^2$; durch die zweite und dritte werden $y$ und $z$ rational durch $x$ (und durch $\mathrm{cn}\,v$, $\mathrm{dn}\,v$) ausgedrückt. Es ergeben sich also $n^2$ Werthsysteme für die drei Unbekannten $x$, $y$, $z$, welche folgende Bedeutung haben:

$$
\begin{aligned}
&x_{\mu,\,\mu'} = \mathrm{sn}\left(\frac{v}{n} + \frac{4\,\mu\,K + 4\,\mu'\,i\,K'}{n}\right)\\
(3)\qquad &y_{\mu,\,\mu'} = \mathrm{cn}\left(\frac{v}{n} + \frac{4\,\mu\,K + 4\,\mu'\,i\,K'}{n}\right)\\
&z_{\mu,\,\mu'} = \mathrm{dn}\left(\frac{v}{n} + \frac{4\,\mu\,K + 4\,\mu'\,i\,K'}{n}\right),
\end{aligned}
$$

worin $\mu$, $\mu'$ je ein vollständiges Restsystem (mod $n$) durchlaufen.

Die erste Gleichung (2):

$$(4)\qquad D(x^2)\,\mathrm{sn}\,v - x\,A(x^2) = 0,$$

vom Grade $n^2$ heisst die allgemeine Theilungsgleichung. Sie ist in dem Sinne irreducibel, dass sie nicht in Factoren zerlegbar ist, welche in Bezug auf $\mathrm{sn}\,v$, $\mathrm{cn}\,v$, $\mathrm{dn}\,v$ rational sind und beliebige von $v$ unabhängige Coëfficienten haben.

Denn zunächst sind die $n^2$ Werthe $x_{\mu,\,\mu'}$ alle von einander verschieden, und wenn irgend eine rationale Gleichung:

$$F\left(\mathrm{sn}\,\frac{v}{n},\ \mathrm{sn}\,v,\ \mathrm{cn}\,v,\ \mathrm{dn}\,v\right) = 0$$

besteht, so kann darin die Variable $v$ durch $v + 4\,\mu\,K + 4\,\mu'\,i\,K'$ ersetzt werden. Wegen der Periodicität von $\mathrm{sn}\,v$, $\mathrm{cn}\,v$, $\mathrm{dn}\,v$ folgt aber daraus, dass die Gleichung

$$F(x,\ \mathrm{sn}\,v,\ \mathrm{cn}\,v,\ \mathrm{dn}\,v) = 0$$

für alle Wurzeln der Gleichung (4) erfüllt ist. Um ihre Galois'sche Gruppe zu ermitteln, setzen wir zunächst den Rationalitätsbereich fest. Er soll folgende Grössen umfassen:

1. rationale Zahlen,
2. rationale Functionen von $\varkappa^2$,
3. die drei Functionen $\mathrm{sn}\,v$, $\mathrm{cn}\,v$, $\mathrm{dn}\,v$,
4. die Grössen $\mathrm{sn}\left(\frac{4\,\mu\,K' + 4\,\mu'\,i\,K'}{n}\right)$.

Aus (2) folgt dann, dass auch

$$\operatorname{cn}\left(\frac{4\mu K + 4\mu' i K'}{n}\right), \qquad \operatorname{dn}\left(\frac{4\mu K + 4\mu' i K'}{n}\right)$$

zum Rationalitätsbereich gehören.

Wir bemerken nun, dass nach dem Additionstheorem jede der Grössen $x_{\mu, \mu'}$ durch jede andere unter ihnen rational ausdrückbar ist. Wenn insbesondere

$$(5) \qquad x_{\mu, \mu'} = F_{\mu, \mu'}(x_{0, 0})$$

ist, so ist

$$(6) \qquad x_{\mu + \nu, \mu' + \nu'} = F_{\mu, \mu'}(x_{\nu, \nu'}) = F_{\mu + \nu, \mu' + \nu'}(x_{0, 0}).$$

Daraus folgt, dass die Galois'sche Gruppe unserer Gleichung aus den $n^2$ Vertauschungen $S_{\nu, \nu'}$ besteht, die man erhält, wenn man in den Wurzeln $x_{\mu, \mu'}$ die Indices $\mu$, $\mu'$ alle um dasselbe Zahlenpaar $\nu$, $\nu'$ vermehrt (wobei jeder Index nach dem Modul $n$ zu nehmen ist).

Denn nach (5) kann jede rationale Function der Wurzeln $x_{\mu, \mu'}$ rational durch $x_{0, 0}$ in der Form

$$\Phi(x_{0, 0})$$

ausgedrückt werden und geht also nach (6) durch die Substitution $S_{\nu, \nu'}$ in $\Phi(x_{\nu, \nu'})$ über; bleibt sie also durch diese Substitution ungeändert, so ist sie rational. Umgekehrt folgt aus der Irreducibilität, dass jede rationale Gleichung zwischen den Wurzeln, da sie in die Form gesetzt werden kann

$$\psi(x_{0, 0}) = 0,$$

und also

$$\psi(x_{\nu, \nu'}) = 0$$

zur Folge hat, die Substitution $S_{\nu, \nu'}$ gestattet. Die Gruppe der $S_{\nu, \nu'}$ ist aber wegen

$$S_{\nu, \nu'} S_{\mu, \mu'} = S_{\nu + \mu, \nu' + \mu'}$$

eine Abel'sche, welche nach der Formel

$$S_{\nu, \nu'} = S_{1,0}^{\nu} S_{0,1}^{\nu'}$$

durch die Basis $S_{1,0}$, $S_{0,1}$ darstellbar ist, und also ist nach §. 58 die allgemeine Theilungsgleichung algebraisch lösbar.

## §. 64. Die Theilung der Perioden.

Die weiter noch zu lösende Aufgabe besteht nun darin, auf algebraischem Wege die Grössen

$$(1) \qquad x_{\mu,\mu'} = \operatorname{sn}\left(\frac{4\mu K + 4\mu' i K'}{n}\right)$$

zu bestimmen. Man erhält alle Werthe dieser Grösse, wenn man $\mu$, $\mu'$ von einander unabhängig, je ein vollständiges Restsystem nach dem Modul $n$ durchlaufen lässt. Diese Werthe sind aber auch alle von einander verschieden, denn $\operatorname{sn} v$ kann nur dann $= \operatorname{sn} v'$ sein, wenn $v'$ congruent $v$ oder congruent $2K - v$ modulo $4K$, $2iK'$, und beides kann für zwei verschiedene der Argumente von (1) nicht eintreten.

Die $n^2$ Grössen (1) sind die Wurzeln der Gleichung

$$(2) \qquad x A(x^2) = 0,$$

und nach den Formeln

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

können auch

$$y_{\mu,\mu'} = \operatorname{cn}\left(\frac{4\mu K + 4\mu' i K'}{n}\right)$$

$$z_{\mu,\mu'} = \operatorname{dn}\left(\frac{4\mu K + 4\mu' i K'}{n}\right)$$

rational durch $x_{\mu,\mu'}$ ausgedrückt werden, wenn der Rationalitätsbereich aus rationalen Zahlen und rationalen Functionen von $\varkappa^2$ besteht.

Aus den Wurzeln $x^2$ der Gleichung $A = 0$ lassen sich nach (12), §. 60 die Wurzeln von $B = 0$, $C = 0$, $D = 0$ rational ableiten; wenn nämlich $x^2$ eine Wurzel von $A = 0$ ist, so sind

$$\frac{1 - x^2}{1 - \varkappa^2 x^2}, \qquad \frac{1 - \varkappa^2 x^2}{1 - x^2}, \qquad \frac{1}{\varkappa^2 x^2}$$

die Wurzeln von $B = 0$, $C = 0$, $D = 0$. Die Bedeutung dieser letzteren Wurzeln ist aber

$$\operatorname{sn}\left(\frac{(4\mu+1)K+4\mu' iK'}{n}\right)^2,$$

$$\operatorname{sn}\left(\frac{(4\mu+1)K+(4\mu'+1)iK'}{n}\right)^2,$$

$$\operatorname{sn}\left(\frac{4\mu K+(4\mu'+1)iK'}{n}\right)^2,$$

und hiernach sind durch Auflösung der Gleichung $A = 0$ alle Grössen von der Form

$$\operatorname{sn}\left(\frac{\mu K+\mu' iK'}{n}\right)^2,$$

worin $\mu$, $\mu'$ beliebige ganze Zahlen sind, rational bestimmt.

## §. 65. Die Abel'schen Relationen.

Für eine nähere Untersuchung der algebraischen Natur der Periodentheilungsgleichung ist ein System von Relationen zwischen ihren Wurzeln von grosser Wichtigkeit, zu dessen Ableitung wir jetzt übergehen[1].

Wir betrachten die Summe:

$$(1) \qquad \sum^{\nu} e^{\frac{8\nu\nu'\pi i}{n}} \frac{\vartheta_{11}\left(u+\frac{2\nu}{n}\right)}{\vartheta_{g_1,g_2}\left(u+\frac{2\nu}{n}\right)},$$

genommen nach $\nu$ über ein vollständiges Restsystem für den (ungeraden) Modul $n$. $\nu'$ ist eine beliebige ganze Zahl und $g_1, g_2$ eine der drei geraden Charakteristiken (0, 0), (0, 1), (1, 0). Diese Summe ist unabhängig von dem besonderen Restsystem, welches $\nu$ durchläuft.

Der Hauptnenner der in (1) vorkommenden Brüche:

$$\prod^{\nu} \vartheta_{g_1,g_2}\left(u+\frac{2\nu}{n}\right)$$

---

[1] Diese Relationen rühren von **Abel** her (Oeuvres complètes, Bd. I, S. 523; Bd. II, S. 251 der neuen Ausgabe). Der oben gegebene Beweis dieser Relationen schliesst sich an **Hermite** an (Crelle's Journal, Bd. 32, S. 283). Zu erwähnen ist noch **Sylow**, Christiania Videnskabsselskabs Forhandlinger 1864 und 1871. **Kronecker**, Berichte der Berliner Akademie, 19. Juli 1875. **Engel**, Berichte der Sächsischen Gesellschaft der Wissenschaften, 31. Juli 1884.

ist nach den letzten Formeln des §. 28, von einem constanten Factor abgesehen, gleich

$$\vartheta_{g_1, g_2}(n u, n \omega),$$

und wenn wir also die Summe (1) gleich

$$\frac{\Phi(u)}{\vartheta_{g_1, g_2}(n u, n \omega)} \tag{2}$$

setzen, so ist $\Phi(u)$ eine ganze transcendente Function von $u$.

Vermehrt man $u$ um $\frac{1}{n}$, so ergiebt sich mit Rücksicht auf

$$\frac{\vartheta_{11}\left(u + \frac{2\nu + 1}{n}\right)}{\vartheta_{g_1, g_2}\left(u + \frac{2\nu + 1}{n}\right)} = (-1)^{g_1 + 1} \frac{\vartheta_{11}\left(u + \frac{2\nu + n + 1}{n}\right)}{\vartheta_{g_1, g_2}\left(u + \frac{2\nu + n + 1}{n}\right)},$$

und da $\nu$ und $\nu + \frac{n+1}{2}$ gleichzeitig ein vollständiges Restsystem modulo $n$ durchlaufen

$$\Phi\left(u + \frac{1}{n}\right) = -e^{-\frac{4\nu'\pi i}{n}} \Phi(u), \tag{3}$$

und durch Vermehrung von $u$ um $\omega$:

$$\Phi(u + \omega) = -e^{-n\pi i(2u + \omega)} \Phi(u). \tag{4}$$

Daraus ergiebt sich, dass die Function $\Phi(u)$ eine $t$-Function ist mit den Perioden $\frac{1}{n}$, $\omega$, welche durch die Bedingungen (3), (4) bis auf einen von $u$ unabhängigen Factor bestimmt und durch eine $\vartheta$-Function ausdrückbar ist (§. 17). Man sieht leicht, dass die Bedingungen (3), (4) durch die Function

$$e^{-4\pi i\nu' u} \vartheta_{11}(n u - 2\nu'\omega, n\omega)$$

befriedigt sind, so dass sich ergiebt:

$$\sum^{\nu} e^{\frac{8\nu\nu'\pi i}{n}} \frac{\vartheta_{11}\left(u + \frac{2\nu}{n}\right)}{\vartheta_{g_1, g_2}\left(u + \frac{2\nu}{n}\right)} = C e^{-4\pi i\nu' u} \frac{\vartheta_{11}(n u - 2\nu'\omega, n\omega)}{\vartheta_{g_1, g_2}(n u, n\omega)}. \tag{5}$$

Die Bestimmung der Constanten $C$ kann man leicht ausführen, wenn man rechts und links mit

$$\vartheta_{g_1, g_2}(u)$$

multiplicirt und dann

$$u = \frac{(1 - g_2) + (1 - g_1)\omega}{2}$$

setzt. Die Formel (6) des §. 18 ergiebt dann:

$$(6)\qquad C = (-1)^{(g_1+1)\frac{n-1}{2}}\, n\, \frac{\vartheta_{g_1, g_2}(0, \omega)}{\vartheta_{g_1, g_2}(2\nu'\omega, n\omega)}\, \frac{\vartheta'_{11}(0, n\omega)}{\vartheta'_{11}(0, \omega)}.$$

Die Abel'schen Relationen erhält man einfach, indem man in (5) $n u = 2\nu'\omega$ setzt, wodurch die rechte Seite verschwindet:

$$(7)\qquad \sum^{\nu} e^{\frac{8\nu\nu'\pi i}{n}} \frac{\vartheta_{11}\left(\dfrac{2\nu'\omega + 2\nu}{n}\right)}{\vartheta_{g_1, g_2}\left(\dfrac{2\nu'\omega + 2\nu}{n}\right)} = 0.$$

Wendet man auf die hier vorkommenden $\vartheta$-Functionen eine lineare Transformation

$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}, \qquad \alpha\delta - \beta\gamma = 1$$

an, so erhält man nach §. 34 die allgemeine Formel:

$$(8)\qquad \sum^{\nu} e^{\frac{8\nu\nu'\pi i}{n}} \frac{\vartheta_{11}\left(\dfrac{2(\nu\alpha + \nu'\gamma) + 2(\nu\beta + \nu'\delta)\omega}{n}\right)}{\vartheta_{g_1, g_2}\left(\dfrac{2(\nu\alpha + \nu'\gamma) + 2(\nu\beta + \nu'\delta)\omega}{n}\right)} = 0.$$

Diese Gleichungen gehen nun, wenn man $g_1, g_2 = 0, 1$ setzt und die Bezeichnungen des vierten Abschnittes einführt, unmittelbar in Relationen zwischen den Wurzeln $x_{\nu, \nu'}$ (§. 64) über:

$$(9)\qquad \sum^{\nu} e^{\frac{8\nu\nu'\pi i}{n}} x_{\nu\alpha + \nu'\gamma,\, \nu\beta + \nu'\delta} = 0,$$

und den beiden speciellen Fällen:

$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} = \begin{pmatrix}1, & 0\\ 0, & 1\end{pmatrix}, \qquad \begin{pmatrix}0, & 1\\ -1, & 0\end{pmatrix}$$

entsprechend

$$(10)\qquad \sum^{\nu} e^{\frac{8\nu\nu'\pi i}{n}} x_{\nu, \nu'} = 0,$$

$$(11)\qquad \sum^{\nu'} e^{\frac{8\nu\nu'\pi i}{n}} x_{\nu, \nu'} = 0.$$

Nach (5), (6) kann man auch den Werth dieser Summen bestimmen, wenn darin die Einheitswurzel

$$e^{\frac{8\pi i}{n}}$$

durch eine andere ersetzt wird, indem man in (5) $\nu'$ durch ein anderes Zeichen, $m$, ersetzt und dann $n u = 2\nu'\omega$ setzt. Beschränken wir uns auf den Fall $(g_1, g_2) = (0, 1)$ und multiplicirt (5) noch mit $\vartheta_{00} : \vartheta_{10}$, so folgt:

$$\sum^{\nu} e^{\frac{8 m \nu \pi i}{n}} x_{\nu, \nu'} = \tag{12}$$

$$(-1)^{\frac{n-1}{2}} n e^{\frac{-4 \pi i m \nu' \omega}{n}} \frac{\vartheta_{00} \vartheta_{01} \vartheta'_{11}(0, n\omega) \vartheta_{11}(2(\nu' - m)\omega, n\omega)}{\vartheta_{10} \vartheta'_{11} \vartheta_{01}(2 m\omega, m\omega) \vartheta_{01}(2\nu'\omega, n\omega)},$$

wo die linke Seite dann, aber auch nur dann verschwindet, wenn $m \equiv \nu' \pmod{n}$ ist.

## §. 66. Die Galois'sche Gruppe der Theilungsgleichung.

Um die Galois'sche Gruppe $\mathfrak{G}$ der Theilungsgleichung zu ermitteln, setzen wir als Rationalitätsbereich fest den Inbegriff aller rationalen Zahlen und rationalen Functionen von $\varkappa^2$.

Nach dem Additions- und Multiplicationstheorem (vgl. §. 60, 64) ist, wenn $f$ und $\varphi_m$ rationale Functionen bedeuten, welche von $\mu, \mu', \nu, \nu'$ unabhängig sind,

$$x_{\mu + \nu, \mu' + \nu'} = f(x_{\mu, \mu'}, x_{\nu, \nu'}), \tag{1}$$

$$x_{m\mu, m\mu'} = \varphi_m(x_{\mu, \mu'}). \tag{2}$$

Ist nun $S$ irgend eine Substitution der Gruppe $\mathfrak{G}$, durch welche, wenn $a, b, c, \partial$ ganze Zahlen bedeuten, die nach dem Modul $n$ genommen sind,

$$x_{1, 0}, x_{0, 1} \quad \text{in} \quad x_{\partial, -c}, x_{-b, a}$$

übergeht, so können wir $S$ auf jede der Formeln (1), (2) anwenden. Es ist aber nach (2):

$$x_{\mu, 0} = \varphi_\mu(x_{1, 0}),$$

woraus zu schliessen, dass durch die Substitution $S$

$$x_{\mu, 0} \quad \text{in} \quad \varphi_\mu(x_{\partial, -c}) = x_{\partial\mu, -c\mu}$$

übergeht. Ebenso findet man, dass durch $S$

$$x_{0, \mu'} \quad \text{in} \quad \varphi_{\mu'}(x_{-b, a}) = x_{-b\mu', a\mu}$$

übergeht.

Wenden wir dies auf die aus (1) hervorgehende Gleichung

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

an, so folgt, dass durch $S$

$$x_{\mu, \mu'} \quad \text{in} \quad x_{\partial\mu - b\mu', -c\mu + a\mu'} \tag{3}$$

übergeht.

Hieraus schliessen wir zunächst, dass die Zahlen $a, b, c, \partial$ so beschaffen sein müssen, dass ihre Determinante

(4) $$m = a\partial - bc$$

mit $n$ keinen Theiler gemeint hat. Denn wäre ein solcher Theiler vorhanden, so würden $\mu$, $\mu'$, ohne dass beide durch $n$ theilbar sind, so bestimmt werden können, dass

$$\partial\mu - b\mu' \equiv 0, \quad -c\mu + a\mu' \equiv 0 \pmod{n},$$

so dass mehrere von einander verschiedene Wurzeln $x_{\mu,\mu'}$ durch $S$ in ein und dieselbe Wurzel übergehen würden, was unmöglich ist. Bezeichnen wir abgekürzt die Vertauschung (3) mit

$$(x_{\mu,\mu'}, x_{\nu,\nu'}),$$

so ist

$$\left.\begin{array}{l} \nu \equiv \phantom{-}\partial\mu - b\mu' \\ \nu' \equiv -c\mu + a\mu' \end{array}\right. \pmod{n},$$

und daraus, durch Auflösung, mit Benutzung der Bezeichnung §. 24, (4):

(5) $$m(\mu, \mu') \equiv \begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix} (\nu, \nu').$$

Es ist daher

(6) $$\begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix}$$

ein zweckmässiges Zeichen für die Vertauschung $S$ und aus (5) ersieht man, dass sich zwei solche Vertauschungen:

$$S = \begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix}, \qquad S' = \begin{pmatrix} a', & b' \\ c', & \partial' \end{pmatrix}$$

genau nach der in §. 24 gegebenen Regel:

(7) $$SS' = S'' = \begin{pmatrix} aa' + bc', & ab' + b\partial' \\ ca' + \partial c', & cb' + \partial\partial' \end{pmatrix}$$

zusammensetzen, so dass die Vertauschung $S''$ der Wurzeln entsteht, wenn zuerst die Vertauschung $S$, sodann die Vertauschung $S'$ unter den Wurzeln der Theilungsgleichung vorgenommen wird. Zu beachten ist aber immer, dass hier nur die nach dem Modul $n$ genommenen Reste der Zahlen $a, b, c, \partial$ in Betracht kommen, so dass die Anzahl der Vertauschungen $S$ stets endlich ist.

1. Der Inbegriff aller Substitutionen $\begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix}$ bildet eine Gruppe, die wir mit $\mathfrak{A}$ bezeichnen, in welcher nach dem, was wir bewiesen haben, die Gruppe $\mathfrak{G}$ der Theilungsgleichung enthalten ist.

In $\mathfrak{A}$ ist als Theiler eine Gruppe $\mathfrak{B}$ enthalten, welche aus allen denjenigen Substitutionen (5)

(8)
$$T = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$$
besteht, welche der Bedingung

(9)
$$\alpha\delta - \beta\gamma \equiv 1 \pmod{n}$$
genügen.

Jede Substitution $S$ lässt sich durch Zusammensetzung von
$$\begin{pmatrix} m, & 0 \\ 0, & 1 \end{pmatrix}$$
mit einer Substitution $T$ herleiten; man hat, damit
$$S = \begin{pmatrix} m, & 0 \\ 0, & 1 \end{pmatrix} T$$
sei, $\alpha$, $\beta$, $\gamma$, $\delta$ einfach aus den Congruenzen
$$a \equiv \alpha m, \quad b \equiv \beta m, \quad c \equiv \gamma, \quad d \equiv \delta \pmod{n}$$
zu bestimmen.

Wir betrachten nun

(10)
$$x_{\mu,\mu'} = \operatorname{sn}\left(\frac{4\mu K + 4\mu' i K'}{n}\right) = \frac{\vartheta_{00}\vartheta_{11}\left(\frac{2\mu + 2\mu'\omega}{n}\right)}{\vartheta_{10}\vartheta_{01}\left(\frac{2\mu + 2\mu'\omega}{n}\right)},$$
$$\varkappa^2 = \frac{\vartheta_{10}^4}{\vartheta_{00}^4}$$
als Functionen von $\omega$, und wenden darauf eine lineare Transformation
$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$$
an, in welcher wir

(11) $\alpha \equiv 1, \quad \delta \equiv 1, \quad \beta \equiv 0, \quad \gamma \equiv 0 \pmod{8}, \quad \alpha\delta - \beta\gamma = 1$

voraussetzen. Nach §. 34 geht hierdurch
$$x_{\mu,\mu'} \quad \text{in} \quad x_{\alpha\mu + \gamma\mu',\ \beta\mu + \delta\mu'},$$
d. h. es erleiden die $x_{\mu,\mu'}$ eine Substitution, welche nach (3), (6) mit
$$T = \begin{pmatrix} \delta, & -\gamma \\ -\beta, & \alpha \end{pmatrix}$$
zu bezeichnen ist, während $\varkappa^2$ ungeändert bleibt.

Dass auf diese Weise auch umgekehrt jede der Substitutionen $T$ entsteht, folgt daraus, dass, wenn irgend eine Substitution $T$ gegeben ist, man durch Hinzufügen passender Vielfachen der (ungeraden) Zahl $n$ zu den Zahlen $\alpha$, $\beta$, $\gamma$, $\delta$ die Bedingungen (11) immer erfüllen kann.

Irgend eine rationale Gleichung zwischen den Wurzeln $x_{\mu,\,\mu'}$ geht, auch wenn beliebige constante, d. h. von $\omega$ unabhängige Zahlencoëfficienten darin vorkommen, durch (8) in eine Identität über, und man kann daher für $\omega$

$$\frac{\gamma + \delta\omega}{\alpha + \beta\omega}$$

substituiren, d. h. man kann jede Substitution $T$ auf die rationale Gleichung zwischen den $x_{\mu,\,\mu'}$ anwenden. Daraus folgt, dass die ganze Gruppe $\mathfrak{B}$ in $\mathfrak{G}$ enthalten ist (§. 56), und dies bleibt auch dann noch richtig, wenn $\mathfrak{G}$ durch die Gruppe $\mathfrak{G}'$ der Theilungsgleichung nach Adjunction beliebiger Constanten ersetzt wird.

Wenn wir nun den Rationalitätsbereich durch Adjunction von $n$ten Einheitswurzeln erweitern, so gehören zu den rationalen Gleichungen auch die Abel'schen Relationen des vorigen Paragraphen. Auf diese Relationen, etwa auf

$$\Sigma^{\nu} e^{\frac{8\nu\nu'\pi i}{n}} x_{\nu,\,\nu'} = 0$$

ist aber keine der Substitutionen

$$M = \begin{pmatrix} m, & 0 \\ 0, & 1 \end{pmatrix}$$

anwendbar; denn durch diese Substitution geht, wenn $mm' \equiv 1 \pmod{n}$ ist,

$$\Sigma^{\nu} e^{\frac{8\nu\nu'\pi i}{n}} x_{\nu,\,\nu'} \text{ in } \Sigma^{\nu} e^{\frac{8\nu m'\nu'\pi i}{n}} x_{\nu,\,\nu'}$$

über, was nach (12), §. 65 von Null verschieden ist, wenn nicht $m'$ und also auch $m \equiv 1 \pmod{n}$ ist. Daraus folgt der Satz:

2. Nach Adjunction der $n$ten Einheitswurzeln (und beliebiger anderer Constanten) ist $\mathfrak{B}$ die Galois'sche Gruppe der Theilungsgleichung. Es wird $\mathfrak{B}$ auch die Monodromiegruppe der Theilungsgleichung genannt.

3. Wir beweisen jetzt noch, dass in dem ursprünglichen Rationalitätsbereich, also ohne Adjunction der $n$ten Einheitswurzeln die Gruppe der Theilungsgleichung mit der Gruppe $\mathfrak{A}$ identisch ist.

Dabei setzen wir den aus der Kreistheilungstheorie [1]) bekannten Satz voraus, dass die primitiven $n$ten Einheitswurzeln $\varrho$ Wurzeln einer irreducibeln Gleichung

---

[1]) Man vgl. etwa Bachmann, Die Lehre von der Kreistheilung, fünfte Vorlesung.

(12) $$\Phi(\varrho) = 0$$

sind (die auch nicht durch Adjunction der unabhängigen Veränderlichen $\varkappa^2$ zum Rationalitätsbereich der rationalen Zahlen zerfallen kann).

Der Grad dieser Gleichung ist $\varphi(n)$, d. h. gleich der Anzahl derjenigen Modulo $n$ incongruenten Zahlen $m$, welche relativ prim zu $n$ sind.

Es sei nun

(13) $$F(r) = 0$$

die Galois'sche Resolvente der Theilungsgleichung im ursprünglichen Rationalitätsbereich vom Grade $\mu$ (so dass alle Wurzeln $x_{\nu,\nu'}$ rational durch $r$ darstellbar sind). Diese Gleichung muss nach Adjunction einer Wurzel von (10) zerfallen; denn wäre dies nicht, so würde jede rationale Relation

(14) $$\psi(r, \varrho) = 0$$

für alle Wurzeln von (13) befriedigt sein, und $\psi(t, \varrho)$ wäre durch $F(t)$ (für ein variables $t$) theilbar. Es würde also (14) noch bestehen bleiben, wenn $\varrho$ durch eine andere Wurzel $\varrho^m$ von (10) ersetzt wird. Dies ist aber nach §. 65 (12) nicht zutreffend, wenn man an Stelle von (14) eine der Abel'schen Relationen setzt.

Es sei nun nach Adjunction von $\varrho$

(15) $$F(r, \varrho) = 0$$

die Galois'sche Resolvente der Theilungsgleichung, vom Grade $\nu$, so dass $\nu$ nach 2. gleich dem Grade der Gruppe $\mathfrak{B}$ ist. Es ist dann $F(t)$ durch $F(t, \varrho)$ algebraisch theilbar und also wegen der Irreducibilität von (12) auch durch jede der Functionen $F(t, \varrho^m)$. Da die Functionen $F(t, \varrho^m)$ irreducibel sind, so können nur dann zwei von ihnen einen gemeinsamen Theiler haben, wenn sie ganz identisch sind. Wenn aber

$$F(t, \varrho) = F(t, \varrho^m)$$

wäre, dann würde aus jeder Gleichung der Form (14) folgen, dass $\psi(t, \varrho)$ durch $F(t, \varrho) = F(t, \varrho^m)$ theilbar wäre, und es würde folgen, dass in (14) die Vertauschung $(\varrho, \varrho^m)$ gestattet ist, was wieder bei den Abel'schen Relationen nicht zutrifft. Mithin sind die $\varphi(n)$ Functionen $F(t, \varrho^m)$ alle von einander verschieden, und $F(t)$ ist durch ihr Product theilbar. Der Grad $\mu$ von $F(t)$ ist also wenigstens $= \nu\varphi(n)$. Er kann aber auch nicht höher als $\nu\varphi(n)$ sein, da $\nu\varphi(n)$ der Grad der Gruppe $\mathfrak{A}$ ist, und die Gruppe $\mathfrak{G}$ vom Grade $\mu$ gewiss in $\mathfrak{A}$ enthalten ist. Es ergiebt sich hieraus

(16) $$\mu = \nu\,\varphi(n)$$

und zugleich die Identität von $\mathfrak{G}$ mit $\mathfrak{A}$.

Daraus folgt aber auch, dass $F(t)$ dem Product der sämmtlichen Factoren $F(t, \varrho^m)$ gleich ist, also

(17) $$F(t) = \overset{m}{\Pi} F(t, \varrho^m),$$

und da $F(t) = 0$ keine gleichen Wurzeln hat, dass zwar $F(r, \varrho)$, aber keiner von den anderen Factoren $F(r, \varrho^m)$ verschwindet. Die Gleichungen

(18) $$F(r, t) = 0, \quad \Phi(t) = 0$$

haben daher nur die eine Wurzel $t = \varrho$ mit einander gemein, und durch Aufsuchen ihres grössten gemeinschaftlichen Theilers findet man $\varrho$ rational ausgedrückt durch $r$, d. h. durch die Wurzeln der Theilungsgleichung.

Diese Ausdrücke für $\varrho$ ändern ihren Werth nicht, wenn auf $r$ eine Substitution der Gruppe $\mathfrak{B}$ angewandt wird, während (nach (12)) $\varrho$ durch eine Substitution der Gruppe $\mathfrak{A}$ in eine Potenz von $\varrho$ übergeht.

Die Abel'schen Relationen zeigen, dass durch die in $\mathfrak{A}$ enthaltene Substitution

(19) $$\begin{pmatrix} m, & 0 \\ 0, & 1 \end{pmatrix}$$

$\varrho$ in $\varrho^m$ übergeht; denn setzen wir

$$e^{\frac{8\pi i}{n}} = \varrho^{\lambda},$$

so lautet eine der Abel'schen Relationen

(20) $$\overset{\nu}{\Sigma}\, \varrho^{\lambda\nu\nu'} x_{\nu,\nu'} = 0,$$

worauf, wenn für $\varrho$ der Ausdruck durch $r$ gesetzt wird, alle Substitutionen von $\mathfrak{A}$, also auch (19), anwendbar sind. Nach §. 65, (12) bleibt aber (20) bei dieser Substitution nur richtig, wenn $\varrho$ in $\varrho^m$ übergeht.

Da $\varrho$ durch die Substitutionen in $\mathfrak{B}$ nicht geändert wird und da die Gruppe $\mathfrak{A}$ aus $\mathfrak{B}$ durch Zusammensetzung mit (19) entsteht, so folgt, dass durch irgend eine Substitution in $\mathfrak{A}$

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

$\varrho$ in $\varrho^m$ übergeht, wenn $m$ der Determinante $(a\,\partial - b\,c)$ congruent ist.

4. Wir wollen schliesslich noch die Zahl $\nu$, d. h. den Grad der Gruppe $\mathfrak{B}$ bestimmen.

$\varphi(n)$ hat, wie bekannt, den Ausdruck

$$\varphi(n) = n\,\Pi\left(1 - \frac{1}{p}\right), \tag{21}$$

wenn das Productzeichen $\Pi$ sich auf alle in $n$ aufgehenden, von einander verschiedenen Primzahlen $p$ erstreckt[1]).

Die Zahl $\nu$ ist gleich der Anzahl der incongruenten Zahlensysteme $\alpha$, $\beta$, $\gamma$, $\delta$, welche der Bedingung

$$\alpha\delta - \beta\gamma \equiv 1 \pmod{n} \tag{22}$$

genügen. Wir fragen zunächst nach der Anzahl der Paare $\alpha$, $\beta$, welche mit $n$ keinen gemeinschaftlichen Theiler haben, und bezeichnen diese mit $\chi(n)$.

Ist $n = n'n''$ und $n'$ relativ prim zu $n''$, so kann man aus jeder Combination eines zu $n'$ gehörigen Zahlenpaares $\alpha'$, $\beta'$ mit einem zu $n''$ gehörigen Zahlenpaar $\alpha''$, $\beta''$ ein zu $n$ gehöriges

$$\alpha = n''\alpha' + n'\alpha'', \qquad \beta = n''\beta' + n'\beta''$$

herleiten, und man erhält auf diese Weise alle Zahlenpaare $\alpha$, $\beta$ und jedes nur einmal. Daraus folgt:

$$\chi(n) = \chi(n')\,\chi(n''). \tag{23}$$

Es ist also noch $\chi(p^\pi)$, d. h. $\chi(n)$ für eine Primzahlpotenz $p^\pi$ zu bestimmen.

Setzen wir zunächst für $\alpha$, $\beta$ alle modulo $p^\pi$ verschiedenen Zahlen, so ist diese Anzahl $p^{2\pi}$. Hiervon sind aber diejenigen Paare wegzulassen, bei welchen $\alpha$ und $\beta$ durch $p$ theilbar sind, deren Anzahl $p^{2\pi-2}$ beträgt, so dass

$$\chi(p^\pi) = p^{2\pi} - p^{2\pi-2},$$

oder

$$\chi(n) = n^2\,\Pi\left(1 - \frac{1}{p^2}\right) \tag{24}$$

folgt.

Jedes Zahlenpaar $\alpha$, $\beta$ lässt sich durch Vermehrung um Vielfache von $n$ in ein solches verwandeln, welches unter sich relativ prim ist, und dann lässt sich $\gamma$, $\delta$ so bestimmen, dass

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

wird, darin kann $\gamma$, $\delta$ durch $\gamma + h\alpha$, $\delta + h\beta$ ersetzt werden, und indem man $h$ ein vollständiges Restsystem modulo $n$ durchlaufen lässt, erkennt man, dass zu jedem Zahlenpaar $\alpha$, $\beta$ $n$ der

---

[1]) Vgl. z. B. Dirichlet-Dedekind, Vorlesungen über Zahlentheorie, 3. Aufl., §. 11.

Bedingung (23) genügende Zahlenpaare $\gamma$, $\delta$ gehören Demnach ist die Ordnung der Gruppe $\mathfrak{B}$:

$$\nu = n^3 \Pi \left(1 - \frac{1}{p^2}\right),$$

oder, wenn wir noch die numerische Function

$$\psi(n) = n \Pi \left(1 + \frac{1}{p}\right) \tag{25}$$

einführen:

$$\nu = n \varphi(n) \psi(n) \tag{26}$$

und die Ordnung der Gruppe $\mathfrak{A}$:

$$\mu = n \varphi(n)^2 \psi(n). \tag{27}$$

## §. 67. Die irreduciblen Factoren der Theilungsgleichung.

Ist

$$\begin{aligned} \nu &= \quad \partial \mu - b \mu' \\ \nu' &= - c \mu + a \mu' \end{aligned}$$

und $a\partial - bc$ relativ prim zu $n$, so ist der grösste gemeinschaftliche Theiler von $\mu$, $\mu'$, $n$ zugleich der grösste gemeinschaftliche Theiler von $\nu$, $\nu'$, $n$. Die Wurzeln $x_{\mu,\mu'}$ der Theilungsgleichung zerfallen also nach dem grössten gemeinschaftlichen Theiler von $\mu$, $\mu'$, $n$ in Systeme, welche durch die Substitutionen der Gruppe $\mathfrak{A}$ immer nur in einander übergehen und deren jedes daher die Wurzeln einer rationalen Gleichung enthält.

Nach dem vorhergehenden Paragraphen giebt es $\varphi(n)\psi(n)$ Zahlenpaare $\mu$, $\mu'$, deren grösster gemeinschaftlicher Theiler mit $n$ gleich 1 ist, und die diesen Zahlenpaaren entsprechenden Wurzeln $x_{\mu,\mu'}$ genügen daher einer rationalen Gleichung des Grades $\varphi(n)\psi(n)$, welche wir die eigentliche Theilungsgleichung für den Divisor $n$ nennen wollen, weil nur dann, wenn $\mu$, $\mu'$, $n$ ohne gemeinsamen Theiler sind, $x_{\mu,\mu'}$ nicht zugleich Wurzel einer Theilungsgleichung für einen kleineren Divisor ist. Im Gegensatz hierzu nennen wir die Gleichung, deren Wurzeln die sämmtlichen $x_{\mu,\mu'}$ sind, die allgemeine Theilungsgleichung für den Divisor $n$.

Durch irgend eine Substitution der Gruppe $\mathfrak{A}$

$$S = \begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix}$$

geht $(1, 0)$, $(0, 1)$ in $(\partial, -c)$, $(-b, a)$ über, und wenn also $S$ nicht die identische Substitution ist, so wird gewiss wenigstens eine der beiden Wurzeln $x_{1,0}$, $x_{0,1}$ durch $S$ verändert. Daraus ergiebt sich nach der Schlussbemerkung des §. 56, dass die Galois'sche Gruppe der eigentlichen Theilungsgleichung genau dieselbe ist, wie die der allgemeinen, nur angewandt auf den Fall, dass $\mu$, $\mu'$, $n$ keinen gemeinsamen Theiler haben, nämlich, je nachdem die $n$ten Einheitswurzeln adjungirt sind oder nicht, $\mathfrak{B}$ oder $\mathfrak{A}$.

Daraus folgt noch, dass die eigentliche Theilungsgleichung irreducibel ist, selbst nach Adjunction beliebiger Constanten.

Denn sind $\gamma$, $\delta$ irgend zwei Zahlen ohne gemeinsamen Theiler mit $n$, so kann man $\alpha$, $\beta$ der Congruenz

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

gemäss bestimmen und die in $\mathfrak{B}$ enthaltene Substitution

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

auf jede rationale Gleichung zwischen den Wurzeln $x_{\mu, \mu'}$ anwenden. Wenn also $x_{1,0}$ einer rationalen Gleichung (mit beliebigen constanten Coëfficienten)

$$\Phi(x_{1,0}) = 0$$

genügt, so genügt derselben Gleichung jede andere Wurzel $x_{\delta, -\gamma}$ der eigentlichen Theilungsgleichung, woraus die Irreducibilität der letzteren folgt.

## §. 68. Zurückführung der Theilungsgleichung auf Transformationsgleichungen.

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

$$x_{\mu_1, \mu_1'} = \operatorname{sn}\left(\frac{4\mu_1 K + 4\mu_1' i K'}{n}\right) = \operatorname{sn} \Omega_1.$$

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

$(R_1)$ $$\operatorname{sn} h\,\Omega_1$$

vor, welche, wenn $h$ ein vollständiges System incongruenter zu $n$ theilerfremder Zahlen durchläuft, alle von einander verschieden sind. Das System $(R_1)$ wollen wir die erste Reihe der Wurzeln nennen.

Ist nun $\operatorname{sn} \Omega_2$ eine in $(R_1)$ nicht enthaltene Wurzel, so bilden die $\varphi(n)$ Grössen

$$(R_2) \qquad \operatorname{sn} h \Omega_2,$$

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

Nach dem Multiplicationstheorem lässt sich durch eine Wurzel jede andere Wurzel derselben Reihe rational ausdrücken in der Form:

$$(1) \qquad \operatorname{sn} h \Omega = f_h(\operatorname{sn} \Omega),$$

worin $f_h$ eine nur von dem Multiplicator $h$, nicht von der Wahl von $\Omega$ abhängige rationale Function ist.

Wenn die beiden Wurzeln $x_{\mu, \mu'}$, $x_{\nu, \nu'}$ in dieselbe Reihe gehören, so muss sich die Zahl $h$ so bestimmen lassen, dass

$$(2) \qquad h\mu \equiv \nu, \quad h\mu' \equiv \nu' \pmod{n},$$

und umgekehrt, wenn dies der Fall ist, so gehören die beiden Wurzeln in dieselbe Reihe. Aus (2) aber folgt die Congruenz

$$(3) \qquad \mu\nu' - \nu\mu' \equiv 0 \pmod{n},$$

und aus dieser lassen sich auch umgekehrt die Congruenzen (2) wieder herleiten.

Denn da $\mu$, $\mu'$, $n$ relativ prim sind, so kann man die Zahlen $\alpha$, $\beta$ so bestimmen, dass

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

und daraus folgt mittelst (3):

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

also, wenn $\alpha\nu - \beta\nu' = h$ gesetzt wird, die Congruenzen (2).

Die Congruenz (3) ist also die nothwendige und hinreichende Bedingung dafür, dass die beiden Wurzeln der eigentlichen Theilungsgleichung $x_{\mu, \mu'}$, $x_{\nu, \nu'}$ derselben Reihe angehören.

Hieraus folgt, dass die Eintheilung in Reihen gänzlich unabhängig ist von der Willkürlichkeit in der Annahme über die Wurzeln $\operatorname{sn} \Omega_1$, $\operatorname{sn} \Omega_2$ ...

Es folgt aber noch weiter daraus, dass durch die Substitutionen der Gruppe $\mathfrak{A}$ die Reihen nicht auseinander gerissen, sondern nur unter einander vertauscht werden.

Denn wendet man auf $(\mu, \mu')$ und $(\nu, \nu')$ gleichzeitig die Substitution

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

an, so bleibt die Congruenz (3) erhalten.

Sucht man unter den Substitutionen der Gruppe $\mathfrak{A}$ diejenigen Substitutionen aus, welche die Wurzeln einer Reihe nur unter einander vertauschen, so erhält man eine Gruppe, und zwar einen Theiler von $\mathfrak{A}$. Zu jeder Reihe gehört also ein solcher Theiler von $\mathfrak{A}$. Bezeichnen wir mit $R_{\mu, \mu'}$ die Reihe, welche die Wurzel $x_{\mu, \mu'}$ enthält, und mit $\mathfrak{A}_{\mu, \mu'}$ den zu dieser Reihe gehörigen Divisor von $\mathfrak{A}$, so sind nach (3) (vgl. §. 66, (3)) die Substitutionen

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

von $\mathfrak{A}_{\mu, \mu'}$ durch die Congruenz

$$(4) \qquad (\partial\mu - b\mu')\,\mu' + (c\mu - a\mu')\,\mu' \equiv 0 \pmod{n}$$

charakterisirt.

Ebenso erhält man eine Gruppe $\mathfrak{B}_{\mu, \mu'}$, wenn man die Substitutionen in $\mathfrak{B}$ aufsucht, welche die Wurzeln der Reihe $R_{\mu, \mu'}$ nur unter sich vertauschen, deren Substitutionen:

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

durch die beiden Congruenzen:

$$(5) \qquad \begin{array}{c} (\delta\mu - \beta\mu')\mu' + (\gamma\mu - \alpha\mu')\mu \equiv 0 \\ \alpha\delta - \beta\gamma \equiv 1 \end{array} \pmod{n}$$

charakterisirt sind.

Beispielsweise bestehen die Gruppen $\mathfrak{A}_{1,0}$, $\mathfrak{B}_{1,0}$ aus den Substitutionen

$$\begin{pmatrix} a, & b \\ 0, & \partial \end{pmatrix}, \quad \begin{pmatrix} \alpha, & \beta \\ 0, & \delta \end{pmatrix}, \quad \alpha\delta \equiv 1 \pmod{n}.$$

Die Gruppen $\mathfrak{A}_{\mu, \mu'}$ sind **conjugirte Divisoren** von $\mathfrak{A}$ (§. 53, 3), denn wenn $x_{1,0}$ durch $S$ in $x_{\mu, \mu'}$, also $R_{1,0}$ in $R_{\mu, \mu'}$ übergeht, so werden durch die Gruppe

$$S^{-1}\mathfrak{A}_{1,0}S$$

die Wurzeln von $R_{\mu,\,\mu'}$ nur unter sich vertauscht, und es ist also

(6) $$S^{-1}\,\mathfrak{A}_{1,\,0}\,S = \mathfrak{A}_{\mu,\,\mu'}.$$

Ebenso ist, wenn $T$ eine Substitution in $\mathfrak{B}$ ist, durch welche $x_{1,\,0}$ in $x_{\mu,\,\mu'}$ übergeht:

(7) $$T^{-1}\,\mathfrak{B}_{1,\,0}\,T = \mathfrak{B}_{\mu,\,\mu'}.$$

Der grösste gemeinschaftliche Theiler $\mathfrak{A}_0$ aller Gruppen $\mathfrak{A}_{\mu,\,\mu'}$ wird nach (4) bestimmt durch

$$b \equiv 0, \quad c \equiv 0, \quad a \equiv d \pmod{n}$$

und besteht also aus den Substitutionen:

$$\begin{pmatrix} a, & 0 \\ 0, & a \end{pmatrix},$$

worin $a$ eine beliebige, zu $n$ theilerfremde Zahl ist. $\mathfrak{A}_0$ ist identisch mit dem grössten gemeinschaftlichen Theiler dreier der Gruppen $\mathfrak{A}_{\mu,\,\mu'}$, etwa

$$\mathfrak{A}_{1,\,0}, \quad \mathfrak{A}_{0,\,1}, \quad \mathfrak{A}_{1,\,1}.$$

Ebenso ist nach (5) der grösste gemeinschaftliche Theiler $\mathfrak{B}_0$ aller $\mathfrak{B}_{\mu,\,\mu'}$ der Inbegriff der Substitutionen:

(8) $$\begin{pmatrix} \alpha, & 0 \\ 0, & \alpha \end{pmatrix}$$

mit der Bedingung:

(9) $$\alpha^2 \equiv 1 \pmod{n}.$$

Die Congruenz (9) besitzt, wenn $k$ die Anzahl der in $n$ aufgehenden, von einander verschiedenen Primzahlen ist, $2^k$ incongruente Lösungen, welches also der Grad der Gruppe $\mathfrak{B}_0$ ist[1]).

Hiernach wenden wir die Sätze des §. 57 auf die Theilungsgleichung an.

Eine rationale Function $\xi$ der Wurzeln einer Reihe, etwa der Reihe $R_{1,\,0}$, lässt sich nach (1) rational durch eine dieser Wurzeln darstellen. Wenn diese Function die Eigenschaft hat, ungeändert zu bleiben, falls diese eine Wurzel durch eine andere derselben Reihe ersetzt wird, wenn also beispielsweise $\xi$ eine symmetrische Function der Wurzeln einer Reihe ist, dann erhält $\xi$ durch Anwendung der Substitutionen von $\mathfrak{A}$ (oder auch von $\mathfrak{B}$) nur

---

[1]) Vgl. Dirichlet-Dedekind, Vorlesungen über Zahlentheorie. 3. Auflage, §. 37.

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

verschiedene Werthe

(11) $$\xi_1, \xi_2 \ldots, \xi_\nu$$

und wenn diese Werthe alle von einander verschieden sind, so gehört $\xi$ zu der Gruppe $\mathfrak{A}_{1,0}$ und alle anderen symmetrischen Functionen der Wurzeln von $R_{1,0}$ sind rational durch $\xi$ darstellbar.

In Folge von §. 57 sind die $\nu$ Grössen (11) Wurzeln einer irreducibeln rationalen Gleichung $\nu$ten Grades, welche wir eine Transformationsgleichung nennen.

Die Transformationsgleichung hat, wenn in $\xi$ nur rationale Zahlcoëfficienten vorkommen, selbst rationale Zahlcoëfficienten. Sie bleibt aber irreducibel, auch wenn $n$te Einheitswurzeln oder überhaupt irgend welche Constanten adjungirt werden, wie sich daraus ergiebt, dass durch Substitutionen der Gruppe $\mathfrak{B}$ jede Wurzel der Theilungsgleichung in jede andere, also auch jede Reihe in jede andere Reihe übergeführt werden kann.

Durch die Adjunction einer Wurzel $\xi$ der Transformationsgleichung, etwa der zur Gruppe $\mathfrak{A}_{1,0}$ gehörigen, reducirt sich die Gruppe der Theilungsgleichung auf $\mathfrak{A}_{1,0}$, die letztere Gruppe ist aber nicht mehr transitiv, sondern vertauscht die $\varphi(n)$ Wurzeln $x_{h,0}$, worin $h$ ein vollständiges System incongruenter, zu $n$ theilerfremder Zahlen durchläuft, unter einander. Die Theilungsgleichung wird also reducibel und hat einen Factor $\varphi(n)$ten Grades, dessen Wurzeln die $x_{h,0}$ sind. Der Einfluss einer Substitution der Gruppe $\mathfrak{A}_{1,0}$

$$\begin{pmatrix} a, & b \\ 0, & \partial \end{pmatrix}$$

auf $x_{h,0}$ besteht darin, dass $x_{h,0}$ in $x_{\partial h,0}$ übergeht, und die Gruppe dieser Gleichung $\varphi(n)$ten Grades besteht daher aus den Vertauschungen

$$(x_{h,0}, \; x_{\partial h,0}),$$

worin $\partial$ jede beliebige zu $n$ theilerfremde Zahl sein kann. Diese Gruppe ist eine Abel'sche und daher sind die Wurzeln $x_{h,0}$ nach Adjunction von $\xi$ algebraisch durch Wurzelziehen zu bestimmen.

Wenn wir aber nicht nur eine, sondern sämmtliche Wurzeln $\xi$ der Transformationsgleichung adjungiren, oder, was auf dasselbe hinauskommt, die drei zu $R_{1,0}$, $R_{0,1}$, $R_{1,1}$ gehörigen, so reducirt sich die Gruppe der Theilungsgleichung auf $\mathfrak{A}_0$, und wenn wir noch $n$te Einheitswurzeln adjungiren, auf $\mathfrak{B}_0$. Die Gruppe $\mathfrak{B}_0$ ist eine Abel'sche vom Grade $2^k$, welche nur solche Elemente enthält, deren Grad $= 2$ ist. In Folge dessen ist die Theilungsgleichung durch Quadratwurzeln lösbar (§. 58).

Um die Form dieser Lösung zu finden, setze man

$$n = p^\pi \, p'^{\pi'} \ldots,$$

worin $p, p' \ldots$ von einander verschiedene Primzahlen, $\pi, \pi' \ldots$ positive Exponenten sind. Man bestimme die Zahlen $c, c', \ldots$ aus den Congruenzen

$$c \equiv -1 \pmod{p^\pi}, \qquad c' \equiv -1 \pmod{p'^{\pi'}} \ldots$$
$$c \equiv +1 \pmod{np^{-\pi}}, \quad c' \equiv +1 \pmod{n\,p'^{-\pi'}} \ldots,$$

dann erhält man jede Lösung $\alpha$ der Congruenz

$$\alpha^2 \equiv 1 \pmod{n},$$

und jede nur einmal, in der Form

$$\alpha \equiv c^\varepsilon \, c'^{\varepsilon'} \ldots \pmod{n}, \tag{12}$$

wenn $\varepsilon, \varepsilon' \ldots$ die Werthe 0, 1 annehmen.

Ist nun $\Omega$ irgend einer der Werthe

$$\frac{4\mu K + 4\mu' i K'}{n},$$

also $\operatorname{sn}\Omega$ irgend eine Wurzel der eigentlichen Theilungsgleichung, so hat die auf alle $\alpha$ auszudehnende Summe

$$\Sigma\, (\pm 1)^\varepsilon (\pm 1)^{\varepsilon'} \ldots \operatorname{sn}\alpha\Omega = \psi(\Omega), \tag{13}$$

worin die $k$ Vorzeichen von $\pm 1$ beliebig gewählt werden können, die Eigenschaft, dass für jedes nach (18) bestimmte $\alpha$

$$\psi(\alpha\Omega) = (\pm 1)^\varepsilon (\pm 1)^{\varepsilon'} \ldots \psi(\Omega) \tag{14}$$

ist, und das Quadrat von $\psi(\Omega)$ bleibt durch die Substitutionen der Gruppe $\mathfrak{B}_0$ ungeändert, ist also durch $n$te Einheitswurzeln und die Wurzeln einer Transformationsgleichung rational ausdrückbar. $\psi(\Omega)$ ist also die Quadratwurzel $\sqrt{A}$ aus einem solchen Ausdruck $A$. Die Anzahl der Ausdrücke (13) beträgt aber $2^k$, und es ergiebt sich durch Addition aller so gebildeter Gleichungen

$$2^k \operatorname{sn}\Omega = \Sigma \sqrt{A}. \tag{15}$$

Es ist noch zu bemerken, dass von den Grössen $\psi$, also auch von den $A$ die Hälfte verschwindet. Denn es ist

$$-1 \equiv c\,c' \ldots \pmod{n},$$

und wenn man also in (14) $\alpha \equiv -1$ setzt, so folgt:

$$\psi(-\Omega) = (\pm 1)\,(\pm 1)\,\ldots\,\psi(\Omega);$$

andererseits ist aber

$$\psi(-\Omega) = -\,\psi(\Omega),$$

und folglich verschwindet $\psi(\Omega)$ immer dann, wenn unter den in (14) vorkommenden $k$ Grössen $\pm 1$ eine gerade Anzahl von negativen Einheiten enthalten ist.

Die Wurzeln $x_{\mu,\,\mu'}$ können also linear durch $2^{k-1}$ Quadratwurzeln ausgedrückt werden.

Wenn $n$ eine Primzahl oder eine Potenz einer Primzahl ist, so sind die Quadrate der Wurzeln der Theilungsgleichung rational durch die Wurzeln der Transformationsgleichung ausdrückbar[1]).

Ist $n$ eine zusammengesetzte Zahl, so lässt sich die Eintheilung der Wurzeln $x_{\mu,\,\mu'}$ in Reihen noch weiter treiben. Ist $p$ eine in $n$ aufgehende Primzahl, so nehme man zwei Wurzeln $x_{\mu,\,\mu'}$, $x_{\nu,\,\nu'}$ in dieselbe oder in verschiedene Reihen auf, je nachdem

$$\mu\nu' - \nu\mu' \equiv 0 \pmod{p}$$

oder nicht; gehören hiernach $x_{\nu,\,\nu'}$ und $x_{\nu_1,\,\nu_1'}$ in eine Reihe mit $x_{\mu,\,\mu'}$, so gehören sie auch unter einander in dieselbe Reihe. Die Anzahl der so gebildeten Reihen ist, wie leicht nachzuweisen, $p+1$ und man erhält auf diese Weise als erste Resolvente der Theilungsgleichung eine zum Divisor $p$ gehörige Transformationsgleichung. Wir werden später auf anderem Wege zeigen, wie die Transformationsgleichungen für zusammengesetzte Divisoren auf solche für Primzahldivisoren zurückgeführt werden können.

---

[1]) Vgl. über diesen Satz Kronecker, Monatsbericht der Berliner Akademie, 19. Juli 1875.

## Neunter Abschnitt.

# Theorie der Transformationsgleichungen.

---

## §. 69. Bildung von Transformationsgleichungen.

Nachdem nun die Theilungsgleichungen auf Transformationsgleichungen zurückgeführt sind, gehen wir an ein genaueres Studium dieser letzteren Gleichungen.

Wir setzen

$$\nu = \psi(n) = n\,\Pi\left(1 + \frac{1}{p}\right), \tag{1}$$

und bezeichnen die $\nu$ Reihen der Wurzeln der Theilungsgleichung mit $R_1, R_2 \ldots, R_\nu$.

Aus jeder dieser Reihen nehmen wir für

$$\Omega_{\mu,\,\mu'} = \frac{4\mu K + 4\mu' i K'}{n} \tag{2}$$

einen Repräsentanten $\Omega_1, \Omega_2 \ldots, \Omega_\nu$ und erhalten die $\varphi(n)$ Wurzeln einer Reihe, wenn wir in

$$\operatorname{sn} m\Omega$$

$m$ ein vollständiges System incongruenter zu $n$ theilerfremder Zahlen durchlaufen lassen.

Die einfachsten Ausdrücke, welche als Wurzeln von Transformationsgleichungen eingeführt werden können, sind die Producte

$$\overset{h}{\underset{1,\,n-1}{\Pi}}\; \Phi(\operatorname{sn} h\Omega), \tag{3}$$

wenn $\Phi$ eine beliebige rationale Function ist, und $h$ die Reihe der Zahlen $1, 2 \ldots, n-1$ durchläuft.

Jede solche Function ist rational ausdrückbar durch $\operatorname{sn}\Omega$ und bleibt offenbar ungeändert, wenn $\Omega$ durch irgend ein $m\Omega$ ersetzt wird, man hat also nur noch dafür zu sorgen, dass die

$\nu$ Werthe von (3), welche den $\nu$ Reihen entsprechen, von einander verschieden sind, um (3) zur Wurzel einer (irreducibeln) Transformationsgleichung zu machen[1]).

Wir nehmen an, die Function $\Phi(x)$ sei entweder eine gerade oder eine ungerade Function von $x$, und machen danach folgende Unterscheidung.

Ist $\Phi(x)$ eine gerade Function, so sind unter den Factoren des Productes (3) je zwei, nämlich

$$(4) \qquad \Phi(\operatorname{sn} h\,\Omega), \quad \Phi(\operatorname{sn}(n-h)\,\Omega)$$

einander gleich. Setzen wir also

$$(5) \qquad \Pi(\Omega) = \prod_{1,\,\frac{n-1}{2}}^{h} \Phi(\operatorname{sn} h\,\Omega),$$

so ist, wenn $m$ eine beliebige zu $n$ theilerfremde Zahl ist,

$$(6) \qquad \Pi(m\,\Omega) = \Pi(\Omega)$$

[weil unter den $\frac{1}{2}(n-1)$ Zahlen $hm$ nicht zwei eine durch $n$ theilbare Summe oder Differenz haben, also, vom Vorzeichen abgesehen, die $\operatorname{sn} h\,\Omega$ dieselben sind, wie die $\operatorname{sn} h\,m\,\Omega$]. Es ist also $\Pi(\Omega)$ die Wurzel einer Transformationsgleichung. Diese Classe von Transformationsgleichungen nennen wir Modulargleichungen.

Ist $\Phi(x)$ eine ungerade Function, so sind die beiden Grössen (4) entgegengesetzt und (6) ist nicht mehr allgemein richtig, sondern es ist

$$(7) \qquad \Pi(m\,\Omega) = \pm\,\Pi(\Omega).$$

Daher ist, wenigstens im Allgemeinen, nicht mehr $\Pi(\Omega)$, sondern erst $\Pi(\Omega)^2$ Wurzel einer Transformationsgleichung, welche Multiplicatorgleichung genannt wird. Um die Fälle kennen zu lernen, in welchen $\Pi(\Omega)$ selbst Wurzel einer Transformationsgleichung ist, muss das Vorzeichen in (7) bestimmt werden.

Dies gelingt auf Grund eines Satzes der Zahlentheorie, der trotz seiner Einfachheit unter die weniger bekannten gehört, der

---

[1]) Ausdrücke wie (3) sind auch dann noch Wurzeln von Transformationsgleichungen, wenn $h$ nur zu $n$ theilerfremde Werthe annimmt. Solche Transformationsgleichung hat man bisher noch wenig benutzt. Wir werden weiterhin ein Beispiel kennen lernen.

daher hier nebst einem ganz elementaren Beweis eine Stelle finden soll.

Der Satz lautet:

Sind $m$, $n$ irgend zwei theilerfremde Zahlen, letztere ungerade, bedeutet ferner $\mu$ die Anzahl derjenigen unter den Zahlen

$$m,\ 2m,\ 3m \cdots \frac{n-1}{2}\, m,$$

deren absolut kleinste Reste (mod $n$) negativ sind, so ist

$$(-1)^{\mu} = \left(\frac{m}{n}\right), \tag{8}$$

worin $\left(\frac{m}{n}\right)$ das Legendre-Jacobi'sche Symbol aus der Theorie der quadratischen Reste ist. Der Beweis ist folgender:

1. Enthält die ungerade Zahl $n$ mehrere verschiedene Primfactoren, und ist wie oben $\varphi(n)$ die Anzahl der incongruenten zu $n$ theilerfremden Zahlen, so ist

$$m^{\frac{1}{2}\varphi(n)} \equiv 1 \pmod{n}.$$

Denn ist $n = n'n''$ und $n'$, $n''$ zwei relative Primzahlen, von denen keine $= 1$ ist, so ist nach dem verallgemeinerten Fermat'schen Satze:

$$\begin{aligned} m^{\frac{1}{2}\varphi(n)} &= \left(m^{\varphi(n')}\right)^{\frac{1}{2}\varphi(n'')} \equiv 1 \pmod{n'} \\ &= \left(m^{\varphi(n'')}\right)^{\frac{1}{2}\varphi(n')} \equiv 1 \pmod{n''}, \end{aligned}$$

also auch

$$m^{\frac{1}{2}\varphi(n)} \equiv 1 \pmod{n}.$$

2. Ist $n$ eine Primzahlpotenz, $p^{\pi}$, so ist

$$m^{\frac{1}{2}\varphi(n)} \equiv \left(\frac{m}{p}\right) \pmod{n}.$$

Diese Congruenz ist richtig für $\pi = 1$, d. h. für $n = p$ (Dirichlet-Dedekind, Vorlesungen über Zahlentheorie, §. 33). Nehmen wir sie als bewiesen an für $n = p^{\pi}$, so folgt, indem man

$$m^{\frac{1}{2}\varphi(n)} = \left(\frac{m}{p}\right) + \lambda p^{\pi}$$

in die $p$te Potenz erhebt, wegen

$$\varphi(p^{\pi+1}) = p\,\varphi(p^{\pi}),$$

die Richtigkeit für $n = p^{\pi+1}$.

Es ist also

$$m^{\frac{1}{2}\varphi(n)} \equiv -1 \pmod{n}$$

nur dann, wenn $n$ eine Potenz einer Primzahl ist, von welcher $m$ quadratischer Nichtrest ist; in allen anderen Fällen ist

$$m^{\frac{1}{2}\varphi(n)} \equiv +1 \pmod{n}.$$

3. Es durchlaufe $r$ alle positiven Zahlen, welche relativ prim zu $n$ und $< \frac{1}{2} n$ sind, deren Anzahl $\frac{1}{2}\varphi(n)$ ist, und $\varrho$ sei die Anzahl derjenigen unter den Zahlen $mr$, deren absolut kleinster Rest negativ ist. Die absolut kleinsten Reste der Zahlen $mr$ stimmen bis auf das Vorzeichen mit den Zahlen $r$ überein, woraus folgt:

$$\Pi(r) \equiv (-1)^{\varrho} m^{\frac{1}{2}\varphi(n)} \Pi(r) \pmod{n},$$

$$m^{\frac{1}{2}\varphi(n)} \equiv (-1)^{\varrho} \pmod{n},$$

also $(-1)^{\varrho} = -1$, dann und nur dann, wenn $n$ eine Potenz einer Primzahl $p$ ist, für welche

$$\left(\frac{m}{p}\right) = -1.$$

4. Es durchlaufe $h$ die Reihe der Zahlen

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

und $\mu$ sei die Anzahl derjenigen unter den Zahlen $mh$, deren absolut kleinster Rest negativ ist.

Sind $1, a', a'', \ldots$ die sämmtlichen Divisoren der Zahl $n$, so zerfällt die Zahlenreihe $h$ in folgende Unterabtheilungen:

$$\begin{array}{llll}
r, & r \text{ relativ prim zu } & n, & r < \frac{n}{2} \\[1ex]
a'r', & r' \quad ,, \quad ,, & ,, \ \frac{n}{a'}, & r' < \frac{n}{2a'} \\[1ex]
a''r'', & r'' \quad ,, \quad ,, & ,, \ \frac{n}{a''}, & r'' < \frac{n}{2a''} \\
\cdots & \cdots & \cdots & \cdots
\end{array}$$

und wenn nun $\varrho, \varrho', \varrho'' \ldots$ für die Zahlenpaare

$$r, n; \quad r', \frac{n}{a'}; \quad r'', \frac{n}{a''}; \quad \ldots$$

die in 3. festgesetzte Bedeutung haben, so ist

$$(9)\qquad \begin{aligned} \mu &= \varrho + \varrho' + \varrho'' + \cdots \\ (-1)^\mu &= (-1)^\varrho (-1)^{\varrho'} (-1)^{\varrho''} \ldots \end{aligned}$$

Nun ist $(-1)^{\varrho'} = +1$, wenn $n : a'$ aus mehreren Primzahlen zusammengesetzt ist, und $= \left(\frac{m}{p}\right)$, wenn $n : a'$ eine Potenz der Primzahl $p$ ist. Es kann aber, wenn $p^\pi$ die höchste in $n$ aufgehende Potenz von $p$ ist, $n : a'$ jeden der Werthe $p, p^2 \ldots, p^\pi$ haben, so dass auf der rechten Seite von (9) der Factor $\left(\frac{m}{p}\right)$ genau $\pi$ mal vorkommt. Daraus aber ergiebt sich die zu beweisende Gleichung:

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

Dieser Satz führt nun unmittelbar zur Bestimmung des Vorzeichens in (7). Denn wenn in (5) die Function $\Phi(x)$ ungerade ist, so ändern beim Uebergang von $\Omega$ zu $m\,\Omega$ genau $\mu$ Factoren in (5) ihr Vorzeichen und wir schliessen

$$(10)\qquad \Pi(m\,\Omega) = \left(\frac{m}{n}\right) \Pi(\Omega).$$

Da es nun, ausser wenn $n$ eine Quadratzahl ist, immer Werthe von $m$ giebt, für welche $\left(\frac{m}{n}\right) = -1$ ist, so folgt der Satz:

Bei ungerader Function $\Phi$ ist $\Pi(\Omega)^2$ und nur wenn $n$ eine Quadratzahl ist, $\Pi(\Omega)$ selbst Wurzel einer Transformationsgleichung [2]).

---

[1]) Vgl. über diesen Satz: Schering und Kronecker im Monatsbericht der Berliner Akademie vom 22. Juni 1876. Schering, Acta mathematica I.

[2]) Diese Vereinfachung der Multiplicatorgleichung in dem Fall, wo $n$ ein Quadrat ist, hat Joubert entdeckt, aber auf einem von dem unserigen ganz verschiedenen Wege nachgewiesen. „Sur les équations, qui se rencontrent dans la théorie de la transformation des fonctions elliptiques. Paris 1876.

## §. 70. Besondere Transformationsgleichungen.

Es sollen nun die Wurzeln der Transformationsgleichungen durch $\vartheta$-Functionen dargestellt werden. Wir setzen zu diesem Zweck:

$$(1)\qquad \begin{aligned} &\Omega = \frac{4\mu K + 4\mu' i K'}{n}, \quad i K' = K\omega \\ &\varpi = \frac{\mu + \mu'\omega}{n}, \quad \Omega = 4 K \varpi \end{aligned}$$

und betrachten die Producte

$$\prod_{1,\frac{n-1}{2}}^{h} \vartheta_{00}(2h\varpi), \quad \prod_{1,\frac{n-1}{2}}^{h} \vartheta_{01}(2h\varpi), \quad \prod_{1,\frac{n-1}{2}}^{h} \vartheta_{10}(2h\varpi), \quad \prod_{1,\frac{n-1}{2}}^{h} \vartheta_{11}(2h\varpi).$$

Es empfiehlt sich folgende Bezeichnung:

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

so dass nach §. 34, (9) die Relation besteht:

$$(3)\qquad (-1)^{\frac{n^2-1}{8}}\, 2^{\frac{n-1}{2}}\, P_{00} P_{10} P_{01} = 1.$$

Ausserdem setzen wir noch:

$$(4)\qquad P_{11}\,\eta(\omega)^{\frac{n-1}{2}} = e^{\frac{\pi i}{6}\mu'(\mu+\mu'\omega)\frac{n^2-1}{n}} \prod_{1,\frac{n-1}{2}}^{h} \vartheta_{11}(2h\varpi).$$

Diese Grössen $P$ lassen sich durch die Wurzeln der Theilungsgleichung ausdrücken, wenn man unter Anwendung von (3) die Quotienten

$$\frac{P_{00}^2}{P_{01}P_{10}}, \quad \frac{P_{10}^2}{P_{01}P_{00}}, \quad \frac{P_{01}^2}{P_{10}P_{00}}, \quad \frac{P_{11}^3}{P_{00}P_{01}P_{10}}$$

bildet und vermittelst der Formeln des §. 37 elliptische Functionen einführt.

Man erhält so

$$
\begin{aligned}
&(-1)^{\frac{n^2-1}{8}}\, 2^{\frac{n-1}{2}}\, P_{00}^3 = \prod_{1,\frac{n-1}{2}}^{h} \frac{\operatorname{dn}^2 h\Omega}{\operatorname{cn} h\Omega}\\
(5)\qquad &(-1)^{\frac{n^2-1}{8}}\, 2^{\frac{n-1}{2}}\, P_{10}^3 = \prod_{1,\frac{n-1}{2}}^{h} \frac{\operatorname{cn}^2 h\Omega}{\operatorname{dn} h\Omega}\\
&(-1)^{\frac{n^2-1}{8}}\, 2^{\frac{n-1}{2}}\, P_{01}^3 = \prod_{1,\frac{n-1}{2}}^{h} \frac{1}{\operatorname{cn} h\Omega\, \operatorname{dn} h\Omega},
\end{aligned}
$$

$$
(6)\qquad (-1)^{\frac{n^2-1}{8}}\, P_{11}^3 = (\varkappa\varkappa')^{\frac{n-1}{2}} \prod^{h} \frac{\operatorname{sn}^3 h\Omega}{\operatorname{cn} h\Omega\, \operatorname{dn} h\Omega}.
$$

Diese Ausdrücke zeigen nun, dass $P_{00}^3$, $P_{10}^3$, $P_{01}^3$ die Wurzeln von Transformationsgleichungen (Modulargleichungen) sind. $P_{11}^6$ ist die Wurzel einer Multiplicatorgleichung, und wenn $n$ eine Quadratzahl ist, so ist auch $P_{11}^3$ die Wurzel einer Multiplicatorgleichung.

Man kann in mannigfaltiger Weise die Functionen $P$ mit einander combiniren, um neue Transformationsgleichungen zu erhalten. Wir führen folgende an:

$$
(7)\qquad
\begin{aligned}
\frac{P_{10}}{P_{00}} &= \prod_{1,\frac{n-1}{2}}^{h} \frac{\operatorname{cn} h\Omega}{\operatorname{dn} h\Omega}\\
\frac{P_{01}}{P_{00}} &= \prod_{1,\frac{n-1}{2}}^{h} \frac{1}{\operatorname{dn} h\Omega}
\end{aligned}
$$

$$
\begin{aligned}
&(-1)^{\frac{n^2-1}{8}} \frac{2^{\frac{n-1}{3}}\, P_{00}^2 P_{11}}{\sqrt{\varkappa\varkappa'}^{\,\frac{n-1}{3}}} = \prod_{1,\frac{n-1}{2}}^{h} \frac{\operatorname{sn} h\Omega\, \operatorname{dn} h\Omega}{\operatorname{cn} h\Omega}\\
(8)\qquad &(-1)^{\frac{n^2-1}{8}} \frac{2^{\frac{n-1}{3}}\, P_{10}^2 P_{11}}{\sqrt{\varkappa\varkappa'}^{\,\frac{n-1}{3}}} = \prod_{1,\frac{n-1}{2}}^{h} \frac{\operatorname{sn} h\Omega\, \operatorname{cn} h\Omega}{\operatorname{dn} h\Omega}\\
&(-1)^{\frac{n^2-1}{8}} \frac{2^{\frac{n-1}{3}}\, P_{01}^2 P_{11}}{\sqrt{\varkappa\varkappa'}^{\,\frac{n-1}{3}}} = \prod_{1,\frac{n-1}{2}}^{h} \frac{\operatorname{sn} h\Omega}{\operatorname{cn} h\Omega\, \operatorname{dn} h\Omega}.
\end{aligned}
$$

Ein wichtiges Resultat ergiebt sich aber noch durch Anwendung des Multiplicationstheorems. Wenn man in der letzten Formel II des §. 60 $v = h\Omega$ setzt und nach §. 38 die Function $\vartheta_{01}$ einführt, so findet man

$$(9)\qquad e^{4\pi i\omega h^2\mu'^2}\,\vartheta_{01}(2h\varpi)^{n^2} = \frac{\vartheta_{01}^{n^2}}{D(\mathrm{sn}^2\, h\Omega)},$$

worin, wie wir uns erinnern, $D$ eine ganze rationale Function ist, deren Coëfficienten rational aus $\varkappa^2$ und ganzen Zahlen gebildet sind.

Nehmen wir das Product aus diesen Ausdrücken, für $h = 1, 2, \dots \frac{n-1}{2}$, so folgt aus der letzten Gleichung (2) $\left(\text{weil bekanntlich } \Sigma h^2 = \frac{n(n^2-1)}{24}\right)$

$$(10)\qquad P_{01}^{n^2} = \prod_{1,\frac{n-1}{2}}^{h} \frac{1}{D(\mathrm{sn}^2\, h\Omega)}.$$

Wir schliessen hieraus, dass auch $P_{01}^{n^2}$ die Wurzel einer Transformationsgleichung ist. Dies ist nichts Neues, wenn $n$ durch 3 theilbar ist, wohl aber, wenn $n$ nicht durch 3, also $n^2-1$ durch 3 theilbar ist. Wir erhalten dann nämlich aus (10) mit Benutzung von (5), (7), (8)

$$P_{01} = 2^{\frac{(n-1)(n^2-1)}{6}} \prod_{1,\frac{n-1}{2}}^{h} \frac{(\mathrm{cn}\, h\Omega)^{\frac{n^2-1}{3}}\,(\mathrm{dn}\, h\Omega)^{\frac{n^2-1}{3}}}{D(\mathrm{sn}^2\, h\Omega)}$$

$$(11)\qquad P_{00} = 2^{\frac{(n-1)(n^2-1)}{6}} \prod_{1,\frac{n-1}{2}}^{h} \frac{(\mathrm{cn}\, h\Omega)^{\frac{n^2-1}{3}}\,(\mathrm{dn}\, h\Omega)^{\frac{n^2+2}{3}}}{D(\mathrm{sn}^2\, h\Omega)}$$

$$P_{10} = 2^{\frac{(n-1)(n^2-1)}{6}} \prod_{1,\frac{n-1}{2}}^{h} \frac{(\mathrm{cn}\, h\Omega)^{\frac{n^2+2}{3}}\,(\mathrm{dn}\, h\Omega)^{\frac{n^2-1}{3}}}{D(\mathrm{sn}^2\, h\Omega)},$$

$$(12)\qquad (-1)^{\frac{n^2-1}{8}}\, 2^{\frac{n^2(n-1)}{3}}\, P_{11}$$

$$= \sqrt{\varkappa\varkappa'}^{\,\frac{n-1}{3}} \prod_{1,\frac{n-1}{2}}^{h} \frac{\mathrm{sn}\, h\Omega\, D(\mathrm{sn}^2\, h\Omega)^2}{(\mathrm{cn}\, h\Omega)^{\frac{2n^2+1}{3}}\,(\mathrm{dn}\, h\Omega)^{\frac{2n^2+1}{3}}}.$$

Soll als Rationalitätsbereich der der rationalen Zahlen und rationalen Functionen von $\varkappa^2$ aufrecht erhalten werden, so schreibt man die letzte Gleichung besser in der Form [vgl. §. 49, (4)]:

$$(13)\quad P_{11}\,\gamma_2(\omega)^{\frac{n-1}{2}} = (-1)^{\frac{n^2-1}{8}}\,2^{-\frac{(n^2-4)(n-1)}{3}}\,(\varkappa\varkappa')^{-\frac{n-1}{2}}\,(1-\varkappa^2\varkappa'^2)^{\frac{n-1}{2}}$$

$$\prod_{1,\frac{n-1}{2}}^{h} \frac{\operatorname{sn} h\,\Omega\; D(\operatorname{sn}^2 h\,\Omega)^2}{(\operatorname{cn} h\,\Omega)^{\frac{2n^2+1}{3}}\;(\operatorname{dn} h\,\Omega)^{\frac{2n^2+1}{3}}},$$

und schliesst daraus auf den folgenden wichtigen Satz:

Wenn $n$ nicht durch 3 theilbar ist, so sind $P_{00}$, $P_{01}$, $P_{10}$, $P_{11}^2\,\gamma_2(\omega)^{n-1}$, und wenn $n$ ein Quadrat ist, auch $P_{11}\,\gamma_2(\omega)^{\frac{n-1}{2}}$ Wurzeln von Transformationsgleichungen.

## §. 71. Zweite Darstellung der Wurzeln der Transformationsgleichungen.

Wenn wir zunächst eine der Reihen ins Auge fassen, nämlich die, zu welcher die Wurzel $x_{1,0}$ gehört, also $\mu = 1$, $\mu' = 0$ setzen, so können wir auf (2), (3) des vorigen Paragraphen die Formeln (20), (21), (10), §. 29 anwenden und erhalten so, wenn wir die diesem speciellen Fall entsprechenden Functionen $P$ durch $P^0$ bezeichnen

$$(1)\quad \begin{aligned} P^0_{00} &= \frac{f(n\,\omega)}{f(\omega)^n} \\ P^0_{01} &= \frac{f_1(n\,\omega)}{f_1(\omega)^n} \\ P^0_{10} &= \left(\frac{2}{n}\right)\frac{f_2(n\,\omega)}{f_2(\omega)^n}, \end{aligned}$$

$$(2)\quad P^0_{11} = \sqrt{n}\;\frac{\eta(n\,\omega)}{\eta(\omega)}.$$

Um durch solche Formeln die sämmtlichen Wurzeln der Transformationsgleichungen darzustellen, bestimmen wir eine lineare Transformation folgendermaassen:

$$(3)\quad \begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix} \equiv \begin{pmatrix}1, 0\\ 0, 1\end{pmatrix} \pmod{16},$$

$$(4)\quad \alpha \equiv \mu, \quad \beta \equiv \mu' \pmod{n},$$

und ersetzen $\omega$ in (1), (2) durch

$$(5)\quad \omega' = \frac{\gamma + \delta\,\omega}{\alpha + \beta\,\omega};$$

auf die linke Seite lassen sich dann die Formeln (3) bis (6), §. 34 und (19), §. 33 anwenden und ergeben:

$$
(6)\quad
\begin{aligned}
P_{00} &= \frac{f(n\,\omega')}{f(\omega')},\\
P_{01} &= \frac{f_1(n\,\omega')}{f_1(\omega')^n},\\
P_{10} &= \left(\frac{2}{n}\right) \frac{f_2(n\,\omega')}{f_2(\omega')^n},\\
P_{11} &= \varepsilon^{1-n}\sqrt{n}\,\frac{\eta(n\,\omega')}{\eta(\omega')},
\end{aligned}
$$

worin $\varepsilon$ die in §. 33, (15), (18) genau definirte 24te Einheitswurzel ist.

Wir haben schon in §. 25 darauf hingewiesen, dass sich immer zwei Transformationen

$$
\begin{pmatrix}\alpha', & \beta'\\ \gamma', & \delta'\end{pmatrix},\quad \begin{pmatrix}a, & 0\\ c, & \partial\end{pmatrix},\quad a\,\partial = n,
$$

von denen die erste linear, die andere von der $n$ten Ordnung ist, so bestimmen lassen, dass

$$
(7)\qquad \begin{pmatrix}\alpha', & \beta'\\ \gamma', & \delta'\end{pmatrix}\begin{pmatrix}a, & 0\\ c, & \partial\end{pmatrix} = \begin{pmatrix}1, & 0\\ 0, & n\end{pmatrix}\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}.
$$

Schreiben wir die Relation (7) so:

$$
\begin{pmatrix}\delta', & -\beta'\\ -\gamma', & \alpha'\end{pmatrix}\begin{pmatrix}1, & 0\\ 0, & n\end{pmatrix} = \begin{pmatrix}a, & 0\\ c, & \partial\end{pmatrix}\begin{pmatrix}\delta, & -\beta\\ -\gamma, & \alpha\end{pmatrix},
$$

so leitet man daraus einfach her:

$$
(8)\qquad
\begin{aligned}
\delta' &= a\,\delta, & \gamma' &= \partial\,\gamma - c\,\delta\\
\partial\,\beta' &= \beta, & n\,\alpha' &= \partial\,\alpha - c\,\beta, \quad a\,\alpha' = \alpha - c\,\beta'.
\end{aligned}
$$

Hierdurch ist zunächst $\partial$ bestimmt als der grösste gemeinschaftliche Theiler von $\beta$ und $n$ oder [wegen (4)] von $\mu'$ und $n$. Dadurch ist, weil $a\,\partial = n$ ist, zugleich $a$ bestimmt, und $c$ muss der Congruenz

$$
(9)\qquad \partial\,\alpha - c\,\beta \equiv 0 \pmod{n}
$$

genügen, wodurch jedoch $c$ nicht absolut, sondern nur nach dem Modul $a$ bestimmt ist. Man kann also $c$ z. B. noch an die Bedingung knüpfen, dass es durch irgend eine Potenz von 2, oder wenn $a$ nicht durch 3 theilbar ist, durch irgend eine Potenz von 3 theilbar sein soll, was wir später bisweilen thun werden.

Die drei Zahlen $a$, $\partial$, $c$ können keinen gemeinsamen Theiler haben, denn ein solcher wäre [nach (8)] auch Theiler von $\alpha$ und $\beta$, was unmöglich ist. Bezeichnen wir also den grössten gemeinsamen Theiler von $a$ und $\partial$ mit $e$, so muss $c$ relativ prim zu $e$ sein.

Die Zahlen $a$, $\partial$, $c$, letztere modulo $a$, sind wegen (4) und (8) durch die beiden Zahlen $\mu$, $\mu'$ völlig bestimmt und ändern sich nicht, wenn $\mu$, $\mu'$ mit einem gemeinsamen, zu $n$ theilerfremden Factor multiplicirt, d. h. durch ein anderes Paar derselben Reihe ersetzt werden. Zerlegt man $n$ irgendwie in zwei Factoren $a$, $\partial$, so kann man für $c$ noch

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

nach dem Modul $a$ verschiedene zu $e$ theilerfremde Werthe annehmen. Jede dieser Annahmen führt zu einem Zahlenpaar $\mu$, $\mu'$ durch die Congruenzen

$$(10)\qquad \begin{aligned} \mu &\equiv \alpha = a\alpha' + c\beta' \\ \mu' &\equiv \beta = \partial\beta' \end{aligned} \qquad (\mathrm{mod}\ n),$$

worin $\beta'$ eine beliebige, zu $a$ theilerfremde Zahl bedeutet und $\alpha'$ so bestimmt wird, dass $\alpha$, $\beta$ relativ prim werden, und es ist auch leicht [nach §. 68, (3)] einzusehen, dass, so lange $a$, $\partial$, $c$ dieselben bleiben, die nach (10) bestimmten Zahlenpaare $\mu$, $\mu'$ derselben Reihe angehören.

Wir nennen die Zahlen $a$, $c$, $\partial$ (wie in §. 23) die Transformationszahlen und $n$ den Transformationsgrad.

Das Zahlensystem $a$, $c$, $\partial$ ist also vollständig charakteristisch für eine Reihe und die Anzahl der Reihen ist gleich der Anzahl dieser Zahlensysteme, woraus für die Zahl $\psi(n)$, (§. 66) folgt:

$$(11)\qquad \psi(n) = \Sigma\,\frac{a}{e}\,\varphi(e),$$

wenn die Summe auf alle Divisoren $a$ von $n$ erstreckt wird.

Es ist von Interesse, diese Relation auch direct zu beweisen, wobei die Annahme eines ungeraden $n$ wegfallen kann. Betrachten wir $\psi(n)$ jetzt als Zeichen für die Summe (11), so ergiebt sich, wenn $n'$, $n''$ relativ prim sind, zunächst

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

und es erübrigt also nur, die Summe $\psi(n)$ für den Fall zu bestimmen, dass $n = p^\pi$ eine Primzahlpotenz ist. In diesem Falle ist nun $e$ gleich dem kleineren der beiden Divisoren $a$, $\partial$, und wenn $a = \partial$ ist, $e = a$. Wenn wir also das erste und letzte Glied der Summe $\psi(n)$ absondern, so erhalten wir

$$\psi(p^\pi) = 1 + p^\pi + \sum_{1<a\leqq\sqrt{n}} \varphi(a) + \sum_{\sqrt{n}<a<n} \frac{a}{\partial}\,\varphi(\partial).$$

Es ist aber

$$\varphi(a) = a\,\frac{p-1}{p}, \qquad \varphi(\partial) = \partial\,\frac{p-1}{p},$$

also

$$\psi(p^\pi) = 1 + p^\pi + \frac{p-1}{p} \sum_{1<a<n} a$$

$$= 1 + p^\pi + (p-1)(1 + p + p^2 + \cdots p^{\pi-2}) = p^\pi\left(1 + \frac{1}{p}\right),$$

woraus sich für $\psi(n)$ der Ausdruck

$$\psi(n) = n\,\Pi\left(1 + \frac{1}{p}\right)$$

ergiebt, wie in §. 66[1]).

Nach (7) ist nun in den Formeln (6) für $n\omega'$ zu setzen:

$$\frac{\gamma' + \delta'\,\dfrac{c + \partial\omega}{a}}{\alpha' + \beta'\,\dfrac{c + \partial\omega}{a}},$$

und es lassen sich die linearen Transformationen der $f$-Functionen [§. 35, (4), (8), (11)] anwenden. Wir nehmen dabei

(12) $$c \equiv 0 \pmod{16},$$

so dass nach (3) und (8):

$$\begin{pmatrix}\alpha', & \beta' \\ \gamma', & \delta'\end{pmatrix} \equiv \begin{pmatrix} a^3, & 0 \\ 0, & a\end{pmatrix} \pmod{16}.$$

Bezeichnen wir mit $\varrho$ die dritte Einheitswurzel

(13) $$\varrho = e^{-\frac{2\pi i}{3}[\alpha'(\gamma' - \beta') - (\alpha'^2 - 1)\beta'\delta']}\; e^{\frac{2n\pi i}{3}[\alpha(\gamma - \beta) - (\alpha^2 - 1)\beta\delta]},$$

so erhalten wir

(14) $$\begin{aligned} P_{00} &= \varrho \quad \frac{f\left(\dfrac{c + \partial\omega}{a}\right)}{f(\omega)^n} \\ P_{01} &= \varrho\left(\frac{2}{a}\right)\frac{f_1\left(\dfrac{c + \partial\omega}{a}\right)}{f_1(\omega)^n} \\ P_{10} &= \varrho\left(\frac{2}{\partial}\right)\frac{f_2\left(\dfrac{c + \partial\omega}{a}\right)}{f_2(\omega)^n} \end{aligned}$$

---

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

Ist $n$ nicht durch 3 theilbar, so nehmen wir

$$c \equiv 0 \pmod{3} \tag{15}$$

an, wodurch $\varrho$ den Werth 1 erhält.

In gleicher Weise kann man die Transformation der $\eta$-Function [§. 33, (15), (18), (19)] auf (7) anwenden und erhält:

$$P_{11} = \left(\frac{\beta}{\alpha}\right)\left(\frac{\beta'}{\alpha'}\right) \varrho\, i^{\frac{a-1}{2}} \sqrt{\partial}\, \frac{\eta\left(\frac{c+\partial\omega}{a}\right)}{\eta(\omega)} \tag{16}$$

(wobei es schon genügen würde, wenn $c$ durch 8 theilbar ist). Ist $n$ durch 3 nicht theilbar und $c$ durch 3 theilbar, so ist auch hierin $\varrho = 1$ zu setzen.

Die Bestimmung des Vorzeichens in (16) hat für uns nur in dem Fall Interesse, wo $n$ ein Quadrat ist. Es ist aber [nach (8)]

$$\left(\frac{\beta}{\alpha}\right)\left(\frac{\beta'}{\alpha'}\right) = \left(\frac{\partial}{\alpha}\right)\left(\frac{\beta'}{\alpha\alpha'}\right) = \left(\frac{\partial}{\alpha}\right)\left(\frac{\beta'}{a}\right) = \left(\frac{\alpha}{\partial}\right)\left(\frac{\beta'}{a}\right)$$

(letzteres nach dem Reciprocitätsgesetz der quadratischen Reste). Wenn nun $n$ ein Quadrat ist, so sind auch $a:e$, $\partial:e$ Quadrate und es ergiebt sich:

$$\left(\frac{\alpha}{\partial}\right)\left(\frac{\beta'}{a}\right) = \left(\frac{\alpha\beta'}{e}\right) = \left(\frac{c}{e}\right),$$

also wird in diesem Fall

$$P_{11} = \varrho\, i^{\frac{a-1}{2}} \left(\frac{c}{e}\right) \sqrt{\partial}\, \frac{\eta\left(\frac{c+\partial\omega}{a}\right)}{\eta(\omega)}.$$

Die zur Charakterisirung einer Reihe aufgestellten Formeln (10) sind ein specieller Fall eines allgemeineren Systems, welches man erhält, indem man auf $\alpha'$, $\beta'$ in (10) eine lineare Transformation anwendet. Man erhält dann Folgendes:

Sind $a, b, c, \partial$ vier der Bedingung:

$$a\partial - bc = n$$

genügende ganze Zahlen ohne gemeinsamen Theiler, so erhält man die einer Reihe entsprechenden Zahlenpaare $\mu$, $\mu'$, wenn man in

$$\begin{aligned} \mu &\equiv a\alpha' + c\beta' \\ \mu' &\equiv b\alpha' + \partial\beta' \end{aligned} \pmod{n} \tag{17}$$

$\alpha'$, $\beta'$ alle und nur solche Werthe durchlaufen lässt, bei denen $\mu$, $\mu'$ ohne gemeinsamen Theiler mit $n$ sind.

Dass zwei den Gleichungen (17) entsprechende Werthpaare $\mu$, $\mu'$ wirklich derselben Reihe angehören, ergiebt sich unmittelbar aus §. 68 (3), und ebenso ist selbstverständlich, dass alle Zahlenpaare einer Reihe in dieser Form enthalten sind, da man $\alpha'$, $\beta'$ durch $h\alpha'$, $h\beta'$ ersetzen kann, wenn $h$ relativ prim zu $n$ ist. Dass man sämmtliche Reihen auf diesem Wege bekommt, zeigen die Formeln (10).

## §. 72. Die Invariantengleichung.

Unter den Transformationsgleichungen ist eine, welche ein besonderes Interesse in Anspruch nimmt, nämlich die, deren Wurzeln die $\psi(n)$ Grössen

$$j\left(\frac{c + \partial\,\omega}{a}\right) \tag{1}$$

oder nach der Bestimmung (17), §. 71 die damit identischen Grössen

$$j\left(\frac{c + \partial\,\omega}{a + b\,\omega}\right), \tag{2}$$

sind, wenn $j(\omega)$ die in §. 41 definirte Invariante ist.

Diese Gleichung heisst die Invariantengleichung.

Die Function $j(\omega)$ lässt sich nach §. 49 rational durch $f(\omega)^{24}$ darstellen, nämlich

$$j(\omega) = \frac{[f(\omega)^{24} - 16]^3}{f(\omega)^{24}}, \tag{3}$$

so dass also nach den Resultaten des vorigen Paragraphen die Grössen (1) die Wurzeln einer Gleichung sind, deren Coëfficienten rationale Functionen von $\varkappa^2$ sind.

Setzt man aber für $f(\omega)$ in (3) eine der früher gefundenen Entwickelungen, z. B. §. 21, (10):

$$f(\omega) = q^{-\frac{1}{24}} \mathop{\Pi}_{1,\infty}^{\nu} (1 + q^{2\nu - 1}),$$

so erkennt man, dass $j(\omega)$ sich in eine nach Potenzen von $q^2$ fortschreitende Reihe entwickeln lässt, welche die Form hat

$$j(\omega) = q^{-2} + a_1 + a_2 q^2 + a_3 q^4 + \cdots, \tag{4}$$

worin die $a_1, a_2, a_3 \ldots$ ganze rationale Zahlen sind, die sich successive berechnen lassen (es ergiebt sich z. B. $a_1 = 744$,

$a_2 = 196\,884$). Die Entwickelungen der Grösse (1) beginnen also mit

$$(5) \qquad e^{-\frac{2\pi i c}{a}} e^{-\frac{2\pi i \partial}{a}\omega}$$

und sind daher alle von einander verschieden, so dass die Invariantengleichung irreducibel ist.

Es giebt aber einen zweiten Weg, um zu dieser wie überhaupt zu den Transformationsgleichungen zu gelangen, den wir jetzt zunächst bei der Invariantengleichung kennen lernen wollen. Diese Ableitung stützt sich auf die Sätze des §. 49 über Modulfunctionen, und gilt auch für ein gerades $n$. Hier ist es der Satz 4, §. 49, welcher zur Anwendung kommt:

Jede Modulfunction, welche durch die beiden Transformationen

$$(6) \qquad \begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix}, \qquad (7) \qquad \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}$$

ungeändert bleibt, ist eine rationale Function von $j(\omega)$.

Wir weisen zunächst nach, dass durch Anwendung der Substitutionen (6), (7) die $\nu$ Grössen (1) unter einander vertauscht werden. Wir haben die Zusammensetzung

$$(8) \qquad \begin{pmatrix} a, & 0 \\ c, & \partial \end{pmatrix} \begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix} = \begin{pmatrix} 1, & 0 \\ \lambda, & 1 \end{pmatrix} \begin{pmatrix} a, & 0 \\ c_1, & \partial \end{pmatrix},$$

wenn

$$(9) \qquad c_1 = c + \partial - \lambda a$$

gesetzt wird, und es geht durch die Transformation (6), da $j(\omega)$ durch jede lineare Transformation ungeändert bleibt,

$$j\left(\frac{c + \partial\omega}{a}\right) \text{ in } j\left(\frac{c_1 + \partial\omega}{a}\right)$$

über.

Ferner bestimmen wir $a_2, \partial_2, c_2$, so dass

$$(10) \qquad \begin{pmatrix} a, & 0 \\ c, & \partial \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \begin{pmatrix} a_2, & 0 \\ c_2, & \partial_2 \end{pmatrix},$$

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

Dazu ist erforderlich

$$(11) \qquad \begin{aligned} \alpha a_2 + \beta c_2 &= 0 \\ \gamma a_2 + \delta c_2 &= -\partial, \end{aligned} \qquad (12) \qquad \begin{aligned} \beta \partial_2 &= a \\ \delta \partial_2 &= c. \end{aligned}$$

Es ist also $\partial_2$ bestimmt als der grösste gemeinschaftliche Theiler von $a$ und $c$, und damit zugleich, wegen $a_2 \partial_2 = n$, auch $a_2$.

Nach den beiden Gleichungen (12) kennt man jetzt $\beta$, $\delta$ als relative Primzahlen und kann $\alpha$, $\gamma$ aus der diophantischen Gleichung

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

bestimmen. Ist dies geschehen, so folgt aus den beiden Gleichungen (11)

$$(13) \qquad \begin{aligned} a_2 &= \partial\beta \\ c_2 &= -\partial\alpha, \end{aligned}$$

wodurch auch $c_2$ bestimmt ist, und es zeigt sich zugleich, dass $\partial$ der grösste gemeinschaftliche Theiler von $a_2$, $c_2$ ist. Ersetzt man $\alpha$, $\gamma$ durch eine andere Lösung $\alpha + h\beta$, $\gamma + h\delta$, so ändert sich nur $c_2$ um ein Vielfaches von $a_2$.

Durch die Transformation (7) geht also

$$j\left(\frac{c + \partial\omega}{a}\right) \text{ in } j\left(\frac{c_2 + \partial_2\omega}{a_2}\right)$$

über.

Bilden wir nun eine symmetrische Function der sämmtlichen Grössen (1), etwa für ein unbestimmtes $x$ das Product

$$\Pi\left[x - j\left(\frac{c + \partial\omega}{a}\right)\right],$$

so ändert sich diese Function nicht durch die Transformationen (6), (7) und ist also nach dem oben erwähnten Satz eine rationale Function von $j(\omega)$. Ausserdem ist sie eine ganze rationale Function $\nu$ten Grades von $x$ mit dem Anfangsglied $x^\nu$, und wir bezeichnen sie mit $F_n[x, j(\omega)]$. Die Gleichung

$$(14) \qquad F_n[x, j(\omega)] = 0$$

hat die Grössen $j\left(\frac{c + \partial\omega}{a}\right)$ zu Wurzeln und ist die Invariantengleichung, deren wichtigste Eigenschaften wir nun ableiten wollen.

1. Die Invariantengleichung ist irreducibel, wenn als Rationalitätsbereich der Inbegriff aller rationalen Functionen von $j(\omega)$ mit beliebigen Zahlencoëfficienten betrachtet wird. Denn besteht irgend eine rationale Gleichung

$$(15) \qquad \Phi\,[j(n\omega), j(\omega)] = 0,$$

so darf darauf jede beliebige lineare Transformation

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

angewandt werden, und nach §. 25, (6) lassen sich, wenn

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

eine beliebige Transformation $n$ter Ordnung ist, die linearen Transformationen

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

immer so bestimmen, dass

$$\begin{pmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{pmatrix} \begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix} = \begin{pmatrix} 1, & 0 \\ 0, & n \end{pmatrix} \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}. \tag{16}$$

Daraus folgt aber, dass die Gleichung (9) durch jede der Grössen

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

und mithin auch durch jede der Grössen (1) befriedigt ist, woraus [wegen der Verschiedenheit der Grössen (1)] die Irreducibilität von (14) folgt.

2. Die Function

$$F_n[x, j(\omega)] = \Pi\left[x - j\left(\frac{c + \partial\,\omega}{a}\right)\right] \tag{17}$$

hat für jeden endlichen Werth von $\omega$ mit positiv imaginärem Bestandtheil, also auch für jeden endlichen Werth von $j(\omega)$ einen endlichen Werth und ist sonach eine ganze rationale Function von $j(\omega)$.

Suchen wir ferner nach (3) das Anfangsglied der Entwickelung der rechten Seite von (17) nach Potenzen von $q$, so ergiebt sich

$$(-1)^\nu\, e^{-2\pi i \Sigma \frac{c}{a}}\, e^{-2\pi i \omega \Sigma \frac{\partial}{e} \varphi(e)} = C q^{-2\nu},$$

wenn $C$ eine endliche Constante ist. Es ist daher

$$j(\omega)^{-\nu}\, F_n[x, j(\omega)]$$

für ein unendliches $j(\omega)$ endlich, d. h. der Grad von $F_n[x, j(\omega)]$ in Bezug auf $j(\omega)$ ebenfalls der $\nu$te.

3. Es ist

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

und wenn wir $n\,\omega$ durch $\omega$ ersetzen:

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

Da nun $j\left(\frac{\omega}{n}\right)$ gleichfalls eine Wurzel der Invariantengleichung ist, so folgt, dass die beiden Gleichungen $\nu$ten Grades

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

eine Wurzel gemeinsam haben, und folglich, wegen der Irreducibilität der ersteren und der Gleichheit des Grades, alle. Es ist daher

$$F_n(x, y) = C F_n(y, x)$$

für unbestimmte Werthe der Variablen $x$, $y$ und ein constantes $C$. Daher auch, durch Vertauschung von $x$ mit $y$:

$$F_n(y, x) = C F_n(x, y),$$

also $C^2 = 1$ oder

$$F_n(x, y) = \pm F_n(y, x).$$

Wenn wir nun $x = y$ setzen, so folgt:

$$F_n(y, y) = \pm F_n(y, y),$$

also, wenn das untere Zeichen gilt,

$$F_n(y, y) = 0.$$

Dies ist aber nur möglich, wenn $n = 1$ ist [wo $F_1(x, y) = x - y$ wird], da sonst $F_n(x, y)$ durch $x - y$ theilbar sein müsste, was der Irreducibilität widerspricht. Daher ist immer, sobald $n > 1$ ist

(18) $$F_n(x, y) = F_n(y, x).$$

4. Es sei

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

und $n'$, $n''$ ohne gemeinsamen Theiler, und $x_1, x_2, \ldots x_{\nu''}$ seien die Wurzeln der Gleichung

(19) $$F_{n''}[x, j(\omega)] = 0.$$

Das Product

(20) $$F_{n'}(x, x_1) F_{n'}(x, x_2) \ldots F_{n'}(x, x_{\nu''}),$$

welches in Bezug auf $x$ vom Grade

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

ist, hängt als symmetrische Function der Wurzeln von (19), rational von $j(\omega)$ ab und verschwindet für

$$x = j\left(\frac{\omega}{n' n''}\right),$$

d. h. für eine Wurzel der Gleichung $F_n[x, j(\omega)] = 0$. Wegen der Irreducibilität der letzteren Gleichung, der Gleichheit des Grades und des Coëfficienten von $x^\nu$ ist also

(21) $$F_n[x, j(\omega)] = F_{n'}(x, x_1)\, F_{n'}(x, x_2) \ldots F_{n'}(x, x_{\nu''}).$$

5. Wir betrachten ferner, wenn

$$n = p^\pi$$

eine Primzahlpotenz ist, die Gleichung

(22) $$F_{p^{\pi-1}}[x, j(\omega)] = 0$$

vom Grade

$$\nu' = p^{\pi-2}(p+1)$$

und bezeichnen ihre Wurzeln mit $x_1, x_2, \ldots x_{\nu'}$.

Das Product

$$P = F_p(x, x_1)\, F_p(x, x_2) \ldots F_p(x, x_{\nu'})$$

ist in Bezug auf $x$ vom Grade $p^{\pi-2}(p+1)^2$; es hängt symmetrisch von den Wurzeln von (22), also rational von $j(\omega)$ ab und verschwindet für

$$x = j\left(\frac{\omega}{p^\pi}\right).$$

Daher ist $P$ durch $F_n[x, j(\omega)]$ theilbar.

Aber der Grad von $P$ ist höher als der von $F_n$. Nehmen wir

$$x_1 = j\left(\frac{p^{\pi-2}c + \omega}{p^{\pi-1}}\right),$$

wo $c$ jeden der Werthe $0, 1, 2 \ldots p-1$ haben kann, so verschwindet $F_p(x, x_1)$ für

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

d. h. es haben $p$ von den Factoren von $P$ einen bestimmten Factor mit $F_{p^{\pi-2}}[x, j(\omega)]$ gemein; daraus folgt, dass $P$ durch

$$\{F_{p^{\pi-1}}[x, j(\omega)]\}^p$$

theilbar ist, und mithin, wie die Vergleichung der Grade und höchsten Glieder lehrt:

(23) $$F_{p^\pi}[x, j(\omega)] = \frac{F_p(x, x_1)\, F_p(x, x_2) \ldots F_p(x, x_{\nu'})}{\{F_{p^{\pi-2}}[x, j(\omega)]\}^p}.$$

Diese Formel ist einer Ausnahme unterworfen für $\pi = 2$, weil in diesem Falle der Grad der Function auf der rechten Seite noch zu hoch ist. Für diesen Fall hat aber jeder der $p+1$ Factoren des Productes $P$ den Theiler $x - j(\omega)$ und es tritt an Stelle von (22) die Formel

(24) $$F_{p^2}[x, j(\omega)] = \frac{F_p(x, x_1)\, F_p(x, x_2) \ldots F_p(x, x_{p+1})}{[x - j(\omega)]^{p+1}}.$$

Hierdurch ist die Lösung der Invariantengleichung $F_n = 0$ auf die successive Lösung solcher Fälle zurückgeführt, in welchen $n$ eine Primzahl ist.

6. Während bei der Ableitung der Transformationsgleichungen aus den Theilungsgleichungen von Haus aus feststeht, dass die numerischen Coëfficienten in diesen Gleichungen rationale Zahlen sind, so lehrt uns die zweite Ableitung zunächst nichts über die Zahlencoëfficienten. Wir können aber nachträglich beweisen, dass diese Coëfficienten nicht nur rationale, sondern auch ganze Zahlen sind und gelangen zugleich zu einem wichtigen Satz über die Theilbarkeit dieser Coëfficienten.

Wenn wir beweisen können, dass, wenn $p$ eine Primzahl ist, die Coëfficienten in $F_p(x, y)$ ganze Zahlen sind, so folgt das Gleiche aus 4. und 5. für jedes zusammengesetzte $n$.

Nach (3) ist $j(\omega)$ in eine Reihe von der Form entwickelbar

$$(25) \qquad j(\omega) = q^{-2} \sum_{0,\infty}^{h} a_h \, q^{2h},$$

deren Coëfficienten $a_h$ ganze Zahlen sind, und zwar $a_0 = 1$.

Bilden wir hiervon, wenn $p$ eine Primzahl ist, die $p$te Potenz, und beachten den für jede ganze Zahl gültigen Fermat'schen Satz:

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

so folgt

$$(26) \qquad j(\omega)^p = q^{-2p} \sum_{0,\infty}^{h} a_h \, q^{2hp} + p \, q^{-2(p-1)} \sum_{0,\infty}^{h} b_h \, q^{2h},$$

worin $b_h$ ebenfalls ganze Zahlen sind. Andererseits ist, wenn man in (25) $\omega$ durch $p\omega$ ersetzt:

$$(27) \qquad j(p\omega) = q^{-2p} \sum_{0,\infty}^{h} a_h \, q^{2hp}$$

und daraus, wenn man

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

setzt:

$$u^p - v = p q^{-2(p-1)} \sum_{0,\infty}^{h} b_h \, q^{2h},$$

wofür wir auch schreiben können

$$(28) \qquad (u^p - v)(u - v^p) = p q^{-2(p^2+p-1)} \sum_{0,\infty}^{h} c_h \, q^{2h},$$

wenn $c_h$ ein drittes System ganzer Zahlen bedeutet.

Nun kommen in $F_p(x, y)$ die in Bezug auf $x$, $y$ höchsten Glieder $x^{p+1} + y^{p+1}$ vor, und wir setzen demnach

$$(29)\qquad F_p(x, y) = (x^p - y)(x - y^p) - \sum_{0,p}^{h,k} c_{h,k}\, x^h y^k,$$

worin $c_{h,k}$ die zu bestimmenden Coëfficienten sind, welche nach 3. der Bedingung

$$c_{h,k} = c_{k,h}$$

genügen. Um sie zu bestimmen, setzen wir in (29)

$$x = u, \quad y = v,$$

wodurch $F_p$ verschwindet, und erhalten

$$(30)\qquad (u^p - v)(v^p - u) = \sum^{h,k} c_{h,k}\, u^h v^k.$$

Hieraus folgt zunächst, dass

$$c_{p,p} = 0$$

sein muss, da nach (28) bei der Entwickelung nach Potenzen von $q$ die Potenz $q^{-2(p^2+p)}$ nicht vorkommen kann, und wir können (29) jetzt in die Form setzen

$$(31)\qquad (u^p - v)(u - v^p) = \sum_{0,p}^{h} \sum_{0,h-1}^{k} c_{h,k}(u^h v^k + u^k v^h)$$
$$+ \sum_{0,p-1}^{h} c_{h,h}\, u^h v^h.$$

Hierin sind die aus (25) und (27) sich ergebenden Entwickelungen von

$$u^h v^k + u^k v^h, \quad u^h v^h$$

nach Potenzen von $q$ einzusetzen, welche mit den Anfangsgliedern

$$q^{-2(hp+k)}, \quad q^{-2h(p+1)}$$

mit dem Coëfficienten 1 beginnen.

Auf der rechten Seite von (31) kommen nicht zwei Glieder vor, in welchen die Entwickelung mit derselben Potenz von $q$ beginnt, denn aus

$$hp + k = h'p + k'$$

folgt $k \equiv k' \pmod{p}$ und mithin, da $k$ und $k' < p$ sind, $k = k'$, $h = h'$.

Ordnet man daher die Reihen, welche die beiden Seiten von (31) darstellen, nach aufsteigenden Potenzen von $q$, und setzt dann die Coëfficienten gleich hoher Potenzen einander gleich, so erhält man eine Reihe linearer Gleichungen für die Unbekannten $c_{h,k}$, von welchen jede folgende nur eine neue Unbekannte enthält, und diese mit dem Coëfficienten 1. Die aus der linken Seite sich ergebenden bekannten Glieder dieser Gleichungen sind nach (28) lauter durch $p$ theilbare ganze Zahlen, und es ergeben sich also für die $c_{h,k}$ ebenfalls ganzzahlige, durch $p$ theilbare Zahlwerthe. Demnach haben wir

$$(31) \qquad F_p(x, y) = (x^p - y)(x - y^p) - p \sum_{0,p}^{h,k} a_{h,k}\, x^h y^k,$$

worin $a_{h,k}$ ganze Zahlen sind, welche den Bedingungen

$$a_{h,k} = a_{k,h}, \quad a_{p,p} = 0$$

genügen.

## §. 73. Die invarianten Transformationsgleichungen.

Die Invariantengleichung ist von grosser theoretischer Wichtigkeit theils wegen ihrer allgemeinen Gültigkeit (auch für gerade $n$), theils wegen der Leichtigkeit, mit welcher die linearen Transformationen auf $j(\omega)$ angewandt werden können. Die wirkliche Berechnung dieser Gleichung aber zeigt sich so complicirt, und die Zahlencoëfficienten sind so gross, dass die Berechnung bis jetzt nur in dem einfachsten Fall $p = 2$ durchgeführt ist. Dagegen kann man, indem man andere Modulfunctionen benutzt, weit einfachere Transformationsgleichungen erhalten.

Ueber das hierbei anzuwendende Princip bemerken wir Folgendes:

Wenn irgend ein System von $\nu$ Functionen von $\omega$ vorliegt, entsprechend den $\nu$ Systemen von Transformationszahlen $a, c, \partial$, die wir mit

$$(1) \qquad \Phi_{a,c,\partial}$$

bezeichnen wollen, welche ebenso wie die Functionen

$$(2) \qquad j\left(\frac{c + \partial\omega}{a}\right)$$

durch die Substitutionen

$$(3) \qquad \left(\omega, -\frac{1}{\omega}\right), \quad (\omega, \omega + 1)$$

unter einander permutirt werden, so ist (1) rational durch (2) und durch $j(\omega)$ ausdrückbar, denn die Function

$$(4) \qquad F_n[x, j(\omega)] \sum^{a,c,\partial} \frac{\Phi_{a,c,\partial}}{x - j\left(\frac{c+\partial\omega}{a}\right)} = \Psi[x, j(\omega)]$$

bleibt durch die Substitutionen (3) ungeändert, und ist daher (für ein unbestimmtes $x$) eine rationale Function von $j(\omega)$

und überdies eine ganze rationale Function von $x$, höchstens vom Grade $\nu - 1$; $F_n[x, j(\omega)]$ hat dieselbe Bedeutung, wie in (17) des vorigen Paragraphen. Aus (4) aber erhält man, indem man

$$x = j\left(\frac{c + \partial\,\omega}{a}\right)$$

setzt:

$$\Phi_{a, c, \partial} = \frac{\Psi\left[j\left(\frac{c + \partial\,\omega}{a}\right), j(\omega)\right]}{F'\left[j\left(\frac{c + \partial\,\omega}{a}\right)\right]}. \tag{5}$$

Es gehört also $\Phi_{a, c, \partial}$ dem algebraischen Körper an, der aus den rationalen Functionen von $j\left(\frac{c + \partial\,\omega}{a}\right)$ und $j(\omega)$ besteht, und wir können die Sätze des §. 55 anwenden. Aus diesen folgt, dass die $\nu$ Grössen $\Phi_{a, c, \partial}$ die Wurzeln einer Gleichung $\nu$ten Grades sind, deren Coëfficienten rational von $j(\omega)$ abhängen, welche, wenn die $\nu$ Grössen $\Phi_{a, c, \partial}$ von einander verschieden sind, irreducibel ist. Eine solche Gleichung nennen wir eine zum Transformationsgrad $n$ gehörige invariante Transformationsgleichung. Jede andere Grösse des Körpers kann durch ein solches $\Phi_{a, c, \partial}$ und durch $j(\omega)$ rational ausgedrückt werden.

Wenn die $\nu$ Grössen $\Phi_{a, c, \partial}$ nicht alle von einander verschieden sind, so zerfallen sie in Reihen von gleich vielen unter einander gleichen, und die aus (5) abzuleitende Gleichung $\nu$ten Grades ist eine Potenz einer irreducibeln Gleichung, die wir gelegentlich wohl auch als Transformationsgleichung bezeichnen werden [§. 55, 5].

Hiervon können wir eine Anwendung machen, welche zur Berechnung von Transformationsgleichungen von Nutzen ist.

Sind die Grössen $\Phi_{a, c, \partial}$ so gewählt, dass sie für kein endliches $\omega$ mit positiv imaginärem Bestandtheil unendlich werden, so bleiben sie für jedes endliche $j(\omega)$ endlich, woraus folgt, dass die Coëfficienten in der Function des $\nu$ten Grades

$$\Pi(x - \Phi_{a, c, \partial}) \tag{6}$$

ganze rationale Functionen von $j(\omega)$ sind, d. h. die $\Phi_{a, c, \partial}$ sind ganze algebraische Functionen von $j(\omega)$.

Richtet man die Functionen $\Phi_{a, c, \partial}$, etwa durch geeignete Bestimmung von Constanten, die darin noch verfügbar sind, so ein, dass sie auch für ein unendliches imaginäres $\omega$, d. h. für $q = 0$ endlich bleiben, so sind diese Functionen auch für ein unendliches $j(\omega)$ endlich, und die Coëfficienten in (6) sind constant. Dies ist aber nur dadurch möglich, dass die $\Phi_{a,c,\partial}$ alle einer und derselben Constanten $C$ gleich sind. Kennt man $\Phi_{a,c,\partial}$ als rationale Function einer anderen Grösse $\Psi_{a,c,\partial}$, so ist $\Phi_{a,c,\partial} = C$ entweder eine Identität oder eine Transformationsgleichung.

## §. 74. Die Transformationsgleichungen für $\gamma_2$ und $\gamma_3$.

Invariante Transformationsgleichungen erhält man zunächst aus der Betrachtung der Functionen §. 49, (4), (5):

$$\gamma_2(\omega) = \sqrt[3]{j(\omega)}, \quad \gamma_3(\omega) = \sqrt{j(\omega) - 1728}.$$

Wenn $n$ nicht durch 3 theilbar ist, so können wir die Zahlen $a$, $c$, $\partial$ so wählen, dass immer $c$ durch 3 theilbar wird.

Nun übt nach §. 49, (15) eine lineare Transformation $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$ auf die Function $\gamma_2(\omega)$ den Einfluss:

$$\gamma_2\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right) = e^{-\frac{2\pi i}{3}(\alpha\beta + \alpha\gamma + \beta\delta - \alpha\beta^2\gamma)}\gamma_2(\omega).$$

In den Zusammensetzungen (8), (10) des §. 72 wird

$$\lambda \equiv n \pmod 3$$
$$\alpha \equiv \delta \equiv 0 \pmod 3,$$

und daraus ergiebt sich, dass durch die beiden Substitutionen

$$(\omega, \omega + 1), \quad \left(\omega, -\frac{1}{\omega}\right)$$

die $\nu$ Functionen

$$(1) \qquad \gamma_2\left(\frac{c + \partial\omega}{a}\right)\gamma_2(\omega)^{-n}$$

nur unter einander vertauscht werden und also die Wurzeln einer invarianten Transformationsgleichung sind.

Ist zweitens $n$ eine ungerade Zahl, so nehme man $c$ gerade an.

Für die Function $\gamma_3(\omega)$ ist [nach §. 49, (15)]:

$$\gamma_3\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right) = (-1)^{\alpha\gamma + \beta\gamma + \beta\delta}\ \gamma_3(\omega),$$

und in den Zusammensetzungen (8), (10), §. 72 ist

$$\lambda \equiv 1, \quad \alpha \equiv \delta \equiv 0 \pmod 2.$$

Die $\nu$ Grössen

$$\gamma_3\left(\frac{c + \partial\omega}{a}\right)\gamma_3(\omega) \tag{2}$$

vertauschen sich daher unter einander und sind also die Wurzeln einer invarianten Transformationsgleichung.

Um für den einfachsten Fall $n = 2$ die erstere dieser Gleichungen zu bilden, beachte man die Relation (§. 49):

$$\gamma_2(\omega) = \frac{f(\omega)^{24} - 16}{f(\omega)^8} = \frac{f_1(\omega)^{24} + 16}{f_1(\omega)^8} = \frac{f_2(\omega)^{24} + 16}{f_2(\omega)^8}, \tag{3}$$

woraus wegen

$$f_1(2\omega)\, f_2(\omega) = \sqrt{2} \qquad [\text{§. 29, (16)}]$$

folgt

$$\begin{aligned} \gamma_2(2\omega) &= \frac{2^8 + f_2(\omega)^{24}}{f_2(\omega)^{16}} \\ \gamma_2\left(\frac{\omega}{2}\right) &= \frac{2^8 + f_1(\omega)^{24}}{f_1(\omega)^{16}} \\ \gamma_2\left(\frac{\omega + 3}{2}\right) &= \frac{2^8 - f(\omega)^{24}}{f(\omega)^{16}}. \end{aligned} \tag{4}$$

[§. 29, (13)]

Bezeichnen wir diese drei Grössen mit $x$, $x_0$, $x_1$, so ergiebt sich aus den Relationen (6), (8), §. 49:

$$\begin{aligned} x + x_0 + x_1 &= \gamma_2(\omega)^2 \\ x x_0 + x x_1 + x_0 x_1 &= 495\, \gamma_2(\omega) \\ x x_0 x_1 &= -j(\omega) + 2^4 . 3^3 . 5^3, \end{aligned}$$

so dass $x$, $x_0$, $x_1$ die Wurzeln der Gleichung sind

$$x^3 - \gamma_2(\omega)^2 x^2 + 5 . 9 . 11 . \gamma_2(\omega) x + j(\omega) - 2^4 . 3^3 . 5^3 = 0. \tag{5}$$

Die Gleichung, deren Wurzeln die Cuben der Wurzeln von (5) sind, ist die Invariantengleichung für $n = 2$, und lässt sich daraus ohne Schwierigkeit berechnen.

## §. 75. Die invarianten Multiplicatorgleichungen.

Unter den Multiplicatorgleichungen sollen hier die betrachtet werden, deren Wurzeln die verschiedenen Potenzen von $P_{11}$ sind, multiplicirt mit Potenzen von $\gamma_2(\omega)$, $\gamma_3(\omega)$, deren Coëfficienten rational von $j(\omega)$ abhängen. Diese Gleichungen nennen wir invariante Multiplicatorgleichungen [1]).

Wir betrachten die Grössen [§. 71, (16)]:

$$(1) \qquad P_{c,\partial,a} = i^{\frac{a-1}{2}} \left(\frac{c}{e}\right) \sqrt{\partial}\, \frac{\eta\left(\frac{c+\partial\omega}{a}\right)}{\eta(\omega)},$$

und den Einfluss, welchen die Transformationen

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

auf sie ausüben. Dieser Einfluss bestimmt sich nach den Formeln (8) bis (13), §. 72, wonach [weil $c_1 \equiv c \pmod{e}$]

$$P_{c,\partial,a} \text{ durch } (\omega, \omega + 1) \text{ in } e^{\frac{\pi i(\lambda-1)}{12}} P_{c_1,\partial,a}$$

$$(2) \qquad \text{durch } \left(\omega, -\frac{1}{\omega}\right)$$

$$\text{in } \sqrt{\frac{\partial}{\partial_2}}\, \frac{i^{\frac{a-a_2}{2}}}{\sqrt{-i\omega}} \left(\frac{c}{e}\right)\left(\frac{c_2}{e_2}\right) E\begin{pmatrix}\alpha, \beta & \frac{c_2+\partial_2\omega}{a_2}\\ \gamma, \delta, & \end{pmatrix} P_{c_2,\partial_2,a_2}$$

übergeht, worin $E$ die in §. 33, (15) angegebene Bedeutung hat. Es ist aber [§. 72, (11), (12)]

$$\sqrt{\partial}\sqrt{\alpha + \beta\,\frac{c_2+\partial_2\omega}{a_2}} = \sqrt{\partial_2\,\omega}$$

und mithin, wenn wir

$$E\begin{pmatrix}\alpha, \beta & \frac{c_2+\partial_2\omega}{a_2}\\ \gamma, \delta, & \end{pmatrix} = r\sqrt{-i\omega}\sqrt{\frac{\partial_2}{\partial}}$$

setzen, $r$ eine 24te Einheitswurzel, und durch die Vertauschung

---

[1]) Diese Gleichungen sind besonders eingehend von Kiepert untersucht worden, zuerst in mehreren Abhandlungen in Crelle's Journal, Bd. 87, 88, 95, am ausführlichsten in den Abhandlungen in den Mathematischen Annalen, Bd. 26, 33. Vgl. auch F. Klein, Mathematische Annalen, Bd. 14, 15.

$$\left(\omega, -\frac{1}{\omega}\right)$$

geht

$$P_{c,\delta,a} \text{ in } r\, i^{\frac{a-a_2}{2}} \left(\frac{c}{c}\right) \left(\frac{c_2}{c_2}\right) P_{c_2,\delta_2,a_2}$$

über.

Daraus ergiebt sich wie oben der Schluss:

1. Für jedes beliebige $n$ sind die Grössen

$$P^{24}_{c,\delta,a}$$

die Wurzeln einer invarianten Transformationsgleichung.

Ist $n$ durch 3 nicht theilbar, so kann man die $c$, $c_2$, $c_1$ durch 3 theilbar voraussetzen. Dann wird

$$\lambda \equiv n, \quad \alpha \equiv 0, \quad \delta \equiv 0 \pmod 3.$$

Es ist also, wie aus §. 33, (15) hervorgeht, $r$ eine achte Einheitswurzel, beachtet man daher noch

$$\gamma_2(\omega + 1) = e^{-\frac{2\pi i}{3}} \gamma_2(\omega),\; \gamma_2\left(-\frac{1}{\omega}\right) = \gamma_2(\omega), \qquad [\text{§. } 49, (14)]$$

so haben wir den Satz:

2. Ist $n$ nicht durch 3 theilbar und $c$ durch 3 theilbar, so sind die Grössen

$$P^8_{c,\delta,a}\, \gamma_2(\omega)^{n-1}$$

Wurzeln einer invarianten Transformationsgleichung.

Um die Anwendung auf den einfachsten Fall $n = 2$ zu machen, setzen wir

$$(3) \qquad x = 16\, \frac{\eta(2\omega)^8}{\eta(\omega)^8}, \quad x_0 = \frac{\eta\left(\frac{\omega}{2}\right)^8}{\eta(\omega)^8}, \quad x_1 = \frac{\eta\left(\frac{\omega+3}{2}\right)^8}{\eta(\omega)^8},$$

d. h. es sind $x$, $x_0$, $x_1$ nichts Anderes als unsere Functionen

$$f_2(\omega)^8, \quad f_1(\omega)^8, \quad -f(\omega)^8 \qquad [\text{§. } 29, (9)]$$

und diese sind, wie wir schon früher gesehen haben [§. 49, (8)], die Wurzeln der cubischen Gleichung

$$(4) \qquad x^3 - x\gamma_2(\omega) + 16 = 0.$$

Der Umstand, dass $f_2^8$, $f_1^8$, $-f^8$ selbst Wurzeln einer Transformationsgleichung für den Transformationsgrad 2 sind, erklärt die Erscheinung, dass bei Adjunction dieser Grössen, also auch bei Adjunction von $\varkappa^2$ die zu einem geraden $n$ gehörigen Transformationsgleichungen reducibel werden.

Wenn $n$ eine ungerade Zahl ist, so nehme man $c$ durch 4 theilbar an, dann ist [§. 72, (9), (11)]

$$\lambda \equiv n \pmod 4,$$

$$\alpha \equiv 0, \quad \delta \equiv 0, \quad \beta \equiv \alpha \delta_2, \quad \gamma \equiv -\delta \alpha_2 \pmod 4,$$

also ergiebt sich

$$r^6 = (-1)^{\frac{\beta - 1}{2}} = (-1)^{\frac{n-1}{2}} (-1)^{\frac{\alpha - \alpha_2}{2}}$$

und daraus folgt mit Rücksicht auf

$$\gamma_3(\omega + 1) = -\gamma_3(\omega), \quad \gamma_3\left(-\frac{1}{\omega}\right) = -\gamma_3(\omega): \quad [§. 49, (14)]$$

3. Ist $n$ ungerade, $c$ durch 4 theilbar, so sind die Grössen

$$P^6_{c, \delta, a}\, \gamma_3(\omega)^{\frac{n-1}{2}}$$

Wurzeln einer invarianten Multiplicatorgleichung. Ist $n \equiv 1 \pmod 4$, so gilt dasselbe von $P^6_{c, \delta, a}$.

Als Beispiel wählen wir $n = 3$ und setzen

$$(5) \quad \begin{aligned} x &= 27\left(\frac{\eta(3\omega)}{\eta(\omega)}\right)^6, & x_0 &= -\left(\frac{\eta\left(\frac{\omega}{3}\right)}{\eta(\omega)}\right)^6, \\ x_1 &= -\left(\frac{\eta\left(\frac{4+\omega}{3}\right)}{\eta(\omega)}\right)^6, & x_2 &= -\left(\frac{\eta\left(\frac{8+\omega}{3}\right)}{\eta(\omega)}\right)^6. \end{aligned}$$

Die Coëfficienten der Gleichung, welche diese Grössen zu Wurzeln hat, sind rationale Functionen von $\gamma_3(\omega)$, und da keine der Grössen (5) für einen endlichen Werth von $\gamma_3$ unendlich wird, so sind es ganze Functionen von $\gamma_3$. Nach 3. können wir diese Gleichung also in der Form ansetzen:

$$x^4 + A_1 \gamma_3 x^3 + A_2 x^2 + A_3 \gamma_3 x + A_4 = 0,$$

worin $A_1, A_2, A_3, A_4$ ganze rationale Functionen von $j(\omega)$ sind. Zunächst erhält man $A_4$ als das Product $x x_0 x_1 x_2$, welches für keinen Werth von $j(\omega)$ verschwinden kann und daher constant sein muss. Aus den Anfängen der Entwickelung [§. 21]

$$(6) \quad \begin{aligned} x &= 27\, q \ldots \\ x_0 &= -q^{-\frac{1}{3}} \ldots \\ x_1 &= -e^{\frac{2\pi i}{3}} q^{-\frac{1}{3}} \ldots \\ x_2 &= -e^{-\frac{2\pi i}{3}} q^{-\frac{1}{3}} \ldots \\ \gamma_3 &= q^{-1} \ldots \end{aligned}$$

findet man daher

$$A_4 = -27.$$

Es ist ferner

$$-A_1 \gamma_3 = x + x_0 + x_1 + x_2.$$

Da die rechte Seite für ein unendliches $\gamma_3$, d. h. für $q = 0$, nicht einmal in der ersten Ordnung unendlich wird, so muss $A_1$ verschwinden.

Aus

$$-A_3 \gamma_3 = x x_0 x_1 x_2 \left(\frac{1}{x} + \frac{1}{x_0} + \frac{1}{x_1} + \frac{1}{x_2}\right)$$

ergiebt sich nach (6) für $A_3$ der constante Werth 1. Um aber $A_2$ zu bestimmen, müssen wir in der Entwickelung noch um ein Glied weiter gehen. Wir setzen in

$$x_0^4 + \gamma_3 x_0 - 27 = -A_2 x_0^2$$

für $x_0$ die Entwickelung

$$x_0 = -q^{-\frac{1}{3}} + 6 q^{\frac{1}{3}} + \cdots$$

und finden $A_2 = 18$, so dass also die gesuchte Gleichung lautet:

$$x^4 + 18 x^2 + \gamma_3 x - 27 = 0. \tag{7}$$

Ist $n$ ungerade und nicht durch 3 theilbar, so nehme man $c$ durch 12 theilbar an.

Es ist alsdann

$$\lambda \equiv n, \quad \alpha \equiv 0, \quad \delta \equiv 0, \quad \beta \equiv a \partial_2, \quad \gamma \equiv -\partial a_2 \pmod{12}$$

und es wird

$$r^2 = (-1)^{\frac{\beta-1}{2}} = (-1)^{\frac{n-1}{2}} (-1)^{\frac{a-a'}{2}},$$

also der Satz

4. Ist $n$ relativ prim zu 6, $c$ durch 12 theilbar, so sind die Grössen

$$P^2_{c,\partial,a}\, \gamma_2(\omega)^{n-1}\, \gamma_3(\omega)^{\frac{n-1}{2}}$$

Wurzeln einer invarianten Multiplicatorgleichung.

Da die Functionen $P^2$ für keinen endlichen Werth von $j(\omega)$ unendlich oder Null werden, so schliessen wir, dass die Coëfficienten der Gleichung, deren Wurzeln die $P^2$ sind, ganze rationale Functionen von $\gamma_2$, $\gamma_3$ sind und dass der letzte Coëfficient eine Constante ist.

Ist $n$ eine Primzahl $p$, so sind die Wurzeln dieser Gleichung

$$x = p\left(\frac{\eta(p\omega)}{\eta(\omega)}\right)^2, \; x_h = (-1)^{\frac{p-1}{2}}\left(\frac{\eta\left(\frac{12h+\omega}{p}\right)}{\eta(\omega)}\right)^2 \; h = 0, 1, \ldots p-1$$

und die Anfangsglieder der Entwickelungen sind folgende:

$$x = pq^{\frac{p-1}{6}} \ldots, \quad x_h = (-1)^{\frac{p-1}{2}} e^{\frac{2\pi i h}{p}} q^{-\frac{p-1}{6p}} \ldots,$$

wodurch sich für den letzten Coëfficienten der Werth $(-1)^{\frac{p-1}{2}} p$ ergiebt. Daraus, dass das erste Glied in der Entwickelung von $j(\omega)$ nach Potenzen von $q$ den Coëfficienten 1 hat, schliesst man leicht, dass die numerischen Coëfficienten in diesen Gleichungen rationale ganze Zahlen sind.

Für $p = 5$ hat die fragliche Gleichung die Form:

$$x^6 + A_1 \gamma_2^2 x^5 + A_2 \gamma_2 x^4 + A_3 x^3 + A_4 \gamma_2 x + 5 = 0,$$

worin die $A_1$, $A_2$, $A_3$, $A_4$ ganze rationale Functionen von $j(\omega)$ und, wie leicht zu sehen, Constante sind.

Aus den Anfangsgliedern ergiebt sich sofort

$$A_1 = 0, \quad A_2 = 0, \quad A_4 = -1.$$

Um aber $A_3$ zu bestimmen, geht man in der Entwickelung von $x_0$ bis zum nächstfolgenden Gliede:

$$x_0 = q^{-\frac{7}{15}}\left(1 - 2q^{\frac{2}{5}} \ldots\right),$$

woraus man $A_3 = 10$ erhält; also lautet für $n = 5$ die Multiplicatorgleichung

$$(8) \qquad x^6 + 10x^3 - \gamma_2 x + 5 = 0.$$

In gleicher Weise berechnet man die Gleichungen für $p = 7$, $p = 11$, indem man die Entwickelungen von $x_0$ benutzt:

$$p = 7{:}\;\; x_0 = -q^{-\frac{1}{7}}\left(1 - 2q^{\frac{2}{7}} - q^{\frac{4}{7}} + 2q^{\frac{6}{7}} \ldots\right),$$

$$p = 11{:}\;\; x_0 = -q^{-\frac{5}{33}}\left(1 - 2q^{\frac{2}{11}} - q^{\frac{4}{11}} + 2q^{\frac{6}{11}} + q^{\frac{8}{11}} + 2q^{\frac{10}{11}} + \cdots\right),$$

während von $\gamma_2(\omega)$, $\gamma_3(\omega)$ immer nur die ersten Glieder gebraucht werden. So findet sich

$$(9) \;\; p = 7{:}\;\; x^8 + 7.2x^6 + 7.9x^4 + 7.10x^2 + \gamma_3 x - 7 = 0,$$

$$(10) \;\; p = 11{:}\;\; x^{12} - 11.90x^6 + 11.40\gamma_2 x^4 + 11.15\gamma_3 x^3 + 11.2\gamma_2^2 x^2 + \gamma_2\gamma_3 x - 11 = 0.$$

Wenn $n$ eine ungerade Quadratzahl ist, so nehmen wir $c$ durch 8 theilbar an. Es sind dann $a:e$ und $\partial:e$ ebenfalls Quadratzahlen. Es ist ferner

$$\alpha \equiv \delta \equiv 0 \pmod 8, \quad \lambda \equiv 1 \pmod 8 \tag{11}$$

$$\left.\begin{matrix} a = \beta\,\partial_2 & a_2 = \beta\,\partial & a \equiv \partial \equiv e \\ c = \delta\,\partial_2 & c_2 = -\,\alpha\,\partial & a_2 \equiv \partial_2 \equiv e_2 \end{matrix}\right\} \pmod 8. \tag{12}$$

Die Einheitswurzel $r$ in (2) erhält den Werth

$$r = \left(\frac{\alpha}{\beta}\right) i^{\frac{1-\beta}{2}}\, e^{\frac{2\pi i}{3}\,\frac{\beta(\alpha+\delta)-(\beta^2-1)\alpha\gamma}{8}}. \tag{13}$$

Es ist aber nach (12) $\beta$ sowohl durch $e$ als auch durch $e_2$ theilbar und $\beta e e_2$ ein Quadrat; also

$$\left(\frac{\alpha}{\beta}\right) = \left(\frac{\alpha}{e\,e_2}\right) = \left(\frac{\alpha}{e}\right)\left(\frac{\alpha}{e_2}\right) = \left(\frac{\delta}{e}\right)\left(\frac{\alpha}{e_2}\right) \text{ (wegen } \alpha\,\delta \equiv 1 \bmod e);$$

ferner ist nach (12)

$$\left(\frac{\delta}{e}\right) = \left(\frac{c}{e}\right)\left(\frac{\partial_2}{e}\right), \quad \left(\frac{\alpha}{e_2}\right) = \left(\frac{c_2}{e_2}\right)\left(\frac{-\,\partial}{e_2}\right),$$

und

$$\left(\frac{\partial_2}{e}\right) = \left(\frac{e_2}{e}\right), \quad \left(\frac{-\,\partial}{e_2}\right) = \left(\frac{-\,e}{e_2}\right), \quad \left(\frac{e_2}{e}\right)\left(\frac{-\,e}{e_2}\right) = (-1)^{\frac{(e+1)(e_2-1)}{4}},$$

also

$$\left(\frac{\alpha}{\beta}\right) = (-1)^{\frac{(e+1)(e_2-1)}{4}} \left(\frac{c}{e}\right)\left(\frac{c_2}{e_2}\right)$$

$$i^{\frac{1-\beta}{2}} = i^{\frac{1-e\,e_2}{2}}; \quad i^{\frac{a-a_2}{2}} = i^{\frac{e-e_2}{2}}.$$

Durch die Vertauschungen (2) geht also

$$P_{c,\partial,a} \text{ in } e^{\frac{2\pi i}{3}\,\frac{\lambda-1}{8}}\, P_{c_1,\partial,a} \text{ und in } e^{\frac{2\pi i}{3}\,\frac{\beta(\alpha+\delta)-(\beta^2-1)\alpha\gamma}{8}}\, P_{c_2,\partial_2,a_2} \tag{14}$$

über.

Ist $n$ noch durch 3 untheilbar, so nehme man $c$ durch 3 theilbar an, wodurch

$$\lambda \equiv 1, \quad \alpha \equiv \delta \equiv 0 \pmod 3)$$

werden und die in (14) vorkommenden dritten Einheitswurzeln den Werth 1 erhalten.

Hieraus ergeben sich die Sätze:

5. Ist $n$ eine ungerade Quadratzahl, $c$ durch 8 theilbar, so sind die Grössen

$$P^3_{c,\partial,a},$$

und ist $n$ eine durch 3 nicht theilbare ungerade Quadratzahl, $c$ durch 24 theilbar, so sind die Grössen

$$P_{c, \partial, a}$$

Wurzeln von invarianten Multiplicatorgleichungen.

Die ersten Beispiele sind $n = 9$, $n = 25$.

Zur Bildung dieser Gleichungen kann man auf verschiedene Arten gelangen. Wir wollen hier (nach Kiepert) den Weg gehen, dass wir nach §. 72 die Wurzeln einer zum Grade $p$ gehörenden Transformationsgleichung durch die für den Grad $p^2$ rational ausdrücken und diesen Ausdruck in die zu $p$ gehörige Transformationsgleichung einsetzen.

Nach 3. Formel (7) wird die Gleichung

$$x^4 + 18 x^2 + \gamma_3(\omega) x - 27 = 0 \tag{15}$$

von den beiden Functionen

$$-\left(\frac{\eta\left(\frac{\omega}{3}\right)}{\eta(\omega)}\right)^6, \quad 27\left(\frac{\eta(3\,\omega)}{\eta(\omega)}\right)^6 \tag{16}$$

befriedigt. Bezeichnen wir den ersten dieser Werthe mit $x$, so geht der zweite durch die Substitution $\left(\omega, \frac{\omega}{3}\right)$ in $\frac{-27}{x}$ über, und folglich wird durch $x$ auch die Gleichung

$$27^3 + 18 . 27 x^2 - \gamma_3\left(\frac{\omega}{3}\right) x^3 - x^4 = 0 \tag{17}$$

befriedigt. Setzen wir nun

$$y = \left(\frac{\eta\left(\frac{\omega}{9}\right)}{\eta(\omega)}\right)^3, \tag{18}$$

so geht $x$ durch die Substitution $\left(\omega, \frac{\omega}{3}\right)$ in $\frac{y^2}{x}$ über, so dass man auch die Gleichung erhält:

$$y^8 + 18 y^4 x^2 + \gamma_3\left(\frac{\omega}{3}\right) y^2 x^3 - 27 x^4 = 0 \tag{19}$$

und durch Elimination von $\gamma_3\left(\frac{\omega}{3}\right)$ aus (17) und (19) erhält man nach Weghebung des Factors $y^2 + 27$

$$x^4 - 18 x^2 y^2 - y^2(y^4 - 27 y^2 + 27^2) = 0. \tag{20}$$

Löst man diese quadratische Gleichung nach $x^2$ auf, so folgt:

$$x^2 = y^3 + 9 y^2 + 27 y = (y + 3)^3 - 27, \tag{21}$$

wo über das Zeichen durch Einsetzen der Anfangsglieder der Entwickelungen entschieden wird, am einfachsten wohl, da diese Gleichung (nach §. 72) auch für

$$x = 27\left(\frac{\eta(3\omega)}{\eta(\omega)}\right)^6, \quad y = 27\left(\frac{\eta(9\omega)}{\eta(\omega)}\right)^3$$

erfüllt wird, indem man

$$x = 27q + \cdots, \quad y = 27q^2 + \cdots$$

setzt.

Sondert man in (15) die erste Potenz von $x$ ab und erhebt ins Quadrat, so erhält man durch Einsetzen von (21) die gesuchte invariante Multiplicatorgleichung für den 9ten Transformationsgrad. Sie erhält eine einfachere Gestalt, wenn man

(22) $$(y + 3)^3 = t$$

setzt:

(23) $$(j(\omega) - 27.64)(t - 27) = (t^2 - 36t + 27.8)^2$$

oder

(24) $$j(\omega)(t - 27) = t(t - 24)^3.$$

Ganz ähnlich kann man beim 25. Transformationsgrad verfahren. Wenn wir

(25) $$x = \left(\frac{\eta\left(\frac{\omega}{5}\right)}{\eta(\omega)}\right)^2, \quad y = \frac{\eta\left(\frac{\omega}{25}\right)}{\eta(\omega)}$$

setzen, so haben wir zunächst nach 4. (8):

(26) $$x^6 + 10x^3 - \gamma_2(\omega)x + 5 = 0,$$

woraus, wie oben, die beiden Gleichungen

$$5^5 + 10.5^2x^3 - \gamma_2\left(\frac{\omega}{5}\right)x^5 + x^6 = 0,$$

$$y^{12} + 10y^6x^3 - \gamma_2\left(\frac{\omega}{5}\right)y^2x^5 + 5x^6 = 0,$$

und durch Elimination von $\gamma_2\left(\frac{\omega}{5}\right)$

$$x^6 - 10x^3y^2(5 + y^2) = y^2(y^8 + 5y^6 + 5^2y^4 + 5^3y^2 + 5^4).$$

Diese Gleichung nach $x^3$ aufgelöst, ergiebt:

(27) $$x^3 = y^5 + 5y^4 + 15y^3 + 25y^2 + 25y,$$

und wenn wir zur Abkürzung die rechte Seite dieser Gleichung mit $\chi(y)$ bezeichnen, nach (26)

(28) $$j(\omega)\chi(y) = (\chi(y)^2 + 10\chi(y) + 5)^3,$$

welches die gesuchte Gleichung 30ten Grades für $y$ ist.

## §. 76. Die Schlaefli'schen Modulargleichungen.

Zu einfacheren Transformationsgleichungen gelangt man, wenn man dem Rationalitätsbereich, welcher bis jetzt aus den rationalen Functionen von $j(\omega)$ bestand, die Grösse $f(\omega)^{24}$ adjungirt. Diesem Rationalitätsbereich gehören die Functionen von $\omega$ an, welche durch die beiden Substitutionen

$$(1) \qquad \left(\omega, -\frac{1}{\omega}\right), \quad (\omega, \omega + 2)$$

ungeändert bleiben (§. 49, 2). Wenn also ein System von $\nu$ Functionen $\Phi_{a,c,\partial}$ durch die Substitutionen (1) nur unter sich permutirt wird, so sind diese Functionen die Wurzeln einer Transformationsgleichung, welche rational von $f(\omega)^{24}$ abhängt. Hierzu gehören (wie wir früher schon auf anderem Wege nachgewiesen haben) für ein ungerades $n$, welches wir jetzt immer voraussetzen, gewisse Potenzen der Grössen

$$f\left(\frac{c + \partial\, \omega}{a}\right),$$

worin, wie ein- für allemal bemerkt sei, $c$ durch 16, und wenn $n$ nicht durch 3 theilbar ist, durch 48 theilbar angenommen wird.

Die etwas erweiterten Grundsätze des §. 73 führen verhältnissmässig einfach zur Berechnung dieser Gleichungen.

Eine Erweiterung ist aber nothwendig aus folgendem Grunde:

Bei den bisherigen Betrachtungen konnten wir den Schluss machen: wenn eine rationale Function von $j(\omega)$ für jedes endliche $\omega$ mit positiv imaginärem Theil endlich bleibt, so ist sie eine ganze Function von $j(\omega)$, weil zu jedem endlichen $j(\omega)$ auch ein endliches, nicht reelles $\omega$ gehört (§. 50). Bei den rationalen Functionen von $f(\omega)$ können wir aber aus der Endlichkeit für jedes endliche imaginäre $\omega$ nur schliessen, dass sie ganze Functionen von $f(\omega)$ und $1 : f(\omega)$ sind, weil nur zu jedem endlichen $f(\omega)$ mit Ausnahme von $f(\omega) = 0$ ein endliches imaginäres $\omega$ gehört.

Es entspricht aber der Substitution

$$(2) \qquad \left(\omega, \frac{\omega - 1}{\omega + 1}\right)$$

die Vertauschung

$$\left(f(\omega), \frac{\sqrt{2}}{f(\omega)}\right), \qquad [§. 29, (18)]$$

und wenn also die Functionen $\Phi_{a,c,\partial}$ so gewählt sind, dass sie auch durch die Substitution (2) nur unter einander permutirt werden, so werden die Coëfficienten der Gleichung, deren Wurzeln sie sind, rational von

$$f(\omega) + \frac{\sqrt{2}}{f(\omega)}$$

abhängen. Sie sind ganze Functionen dieser Verbindungen, wenn die $\Phi_{a,c,\partial}$ für jedes endliche, nicht reelle $\omega$ endlich bleiben, und sie sind constant, wenn alle $\Phi_{a,c,\partial}$ auch für $q = 0$, d. h. für $f(\omega) = 0$ und $f(\omega) = \infty$, endlich bleiben. In diesem Falle sind sämmtliche $\Phi_{a,c,\partial}$ einer und derselben Constanten gleich (§. 73).

Daraus ergiebt sich der Satz:

Bildet man ganze rationale Functionen $\Phi_{a,c,\partial}$ aus

$$f\left(\frac{c+\partial\,\omega}{a}\right), \quad f(\omega), \quad \frac{1}{f\left(\frac{c+\partial\,\omega}{a}\right)}, \quad \frac{1}{f(\omega)},$$

welche die Eigenschaft haben:

1. durch die Substitutionen

$$\left(\omega, -\frac{1}{\omega}\right), \quad (\omega, \omega + 2), \quad \left(\omega, \frac{\omega-1}{\omega+1}\right)$$

nur unter einander vertauscht zu werden,

2. für $q = 0$ nicht unendlich zu werden, so ist

$$\Phi_{a,c,\partial} = \text{constans}$$

eine Transformationsgleichung.

Um diese Bedingungen zu befriedigen, ist zunächst der Einfluss der Substitutionen (1) auf die Functionen $f$ zu untersuchen. Dieser ergiebt sich aus den Zusammensetzungen §. 72, (8) bis (13) und aus den Transformationsformeln für die $f$-Functionen §. 35.

Zur Abkürzung führen wir die Bezeichnung ein:

$$(3) \qquad \begin{aligned} f(\omega) &= u, & f\left(\frac{c+\partial\,\omega}{a}\right) &= v, \\ f_1(\omega) &= u_1, & \left(\frac{2}{a}\right) f_1\left(\frac{c+\partial\,\omega}{a}\right) &= v_1, \\ f_2(\omega) &= u_2, & \left(\frac{2}{\partial}\right) f_2\left(\frac{c+\partial\,\omega}{a}\right) &= v_2. \end{aligned}$$

Es ergeben sich dann folgende zusammengehörige Aenderungen, wenn in der Bezeichnung auf die Verwandlung der Zahlen $a$, $c$, $\partial$ in $a$, $c_1$, $\partial$ oder $a_2$, $c_2$, $\partial_2$, wie sie eben durch die angeführten Formeln des §. 72 charakterisirt ist, keine Rücksicht genommen wird:

$$
\tag{4}
\begin{array}{cccc}
\omega, & u, & u_1, & u_2; \\
-\dfrac{1}{\omega}, & u, & u_2, & u_1; \\
\omega + 1, & e^{-\frac{\pi i}{24}} u_1, & e^{-\frac{\pi i}{24}} u, & e^{\frac{\pi i}{12}} u_2; \\
\omega + 2, & e^{-\frac{\pi i}{12}} u, & e^{-\frac{\pi i}{12}} u_1, & e^{\frac{\pi i}{6}} u_2; \\
\hline
\omega, & v, & v_1, & v_2, \\
-\dfrac{1}{\omega}, & \varrho\, v, & \varrho\, v_2, & \varrho\, v_1, \\
\omega + 1, & \sigma\, e^{-\frac{n\pi i}{24}} v_1, & \sigma\, e^{-\frac{n\pi i}{24}} v, & \sigma\, e^{\frac{n\pi i}{12}} v_2, \\
\omega + 2, & \sigma^2 e^{-\frac{n\pi i}{12}} v, & \sigma^2 e^{-\frac{n\pi i}{12}} v_1, & \sigma^2 e^{\frac{n\pi i}{6}} v_2,
\end{array}
$$

worin

$$
\varrho = e^{-\frac{2\pi i}{3}(\alpha(\gamma - \beta) + (\alpha^2 - 1)\beta\delta)}, \qquad \sigma = \left(\frac{2}{a}\right) e^{\frac{(n - \lambda)\pi i}{24}}
$$

zwei dritte Einheitswurzeln sind, welche, falls $n$ nicht durch 3 theilbar ist, den Werth 1 haben.

Um ferner die Wirkung der Substitution (2), welche aus der Transformation zweiten Grades

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

hervorgeht, auf die Functionen $u$, $v$ zu ermitteln, müssen wir die Transformationen erster und $n$ter Ordnung

$$
\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}, \quad \begin{pmatrix} a', & 0 \\ c', & \partial' \end{pmatrix}
$$

so bestimmen, dass

$$
\tag{5}
\begin{pmatrix} a, & 0 \\ c, & \partial \end{pmatrix} \begin{pmatrix} 1, & 1 \\ -1, & 1 \end{pmatrix} = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \begin{pmatrix} 1, & 1 \\ -1, & 1 \end{pmatrix} \begin{pmatrix} a', & 0 \\ c', & \partial' \end{pmatrix}
$$

wird. Dieser Ansatz führt zu den Gleichungen

$$
\tag{6}
\begin{array}{ll}
a = a'(\alpha - \beta) + c'(\alpha + \beta), & a = \partial'(\alpha + \beta), \\
c - \partial = a'(\gamma - \delta) + c'(\gamma + \delta), & c + \partial = \partial'(\gamma + \delta).
\end{array}
$$

Hiermit ist zunächst, da $\alpha + \beta$ und $\gamma + \delta$ zufolge $\alpha\delta - \beta\gamma = 1$ relativ prim sind, $\partial'$ bestimmt als der grösste gemeinschaftliche Theiler von $a$ und $c + \partial$, und aus $n = a'\partial'$ ergiebt sich $a'$. Dann ist nach den Gleichungen (6):

$$\alpha + \beta = \frac{a}{\partial'}, \qquad \gamma + \delta = \frac{c + \partial}{\partial'},$$

und $\delta$ und $\beta$ lassen sich so bestimmen, dass

(7) $$\delta(\alpha + \beta) - \beta(\gamma + \delta) = \alpha\delta - \beta\gamma = 1.$$

Aus den Gleichungen (6) für $a$ und $c - \partial$ findet sich dann

(8) $$c' + a' = a\delta - (c - \partial)\beta.$$

$\delta$ und $\beta$ können, da $\alpha + \beta$ und $\gamma + \delta$ beide ungerade sind, nach (7) nicht beide ungerade sein; folglich fällt $c'$ nach (8) gerade aus. Ersetzt man, was nach (7) gestattet ist, $\delta$, $\beta$ durch $\delta + h(\gamma + \delta)$, $\beta + h(\alpha + \beta)$, für ein beliebiges $h$, so ändert sich $c'$ nach (8) um $2ha'$, und über $h$ kann so verfügt werden, dass $c'$ durch 16 oder 48 theilbar wird.

Es ist dann nach (6) $\alpha + \beta + \gamma - \delta$ gerade und daher die Formel (11), §. 35 anzuwenden. Darin ist nun zu berücksichtigen

$$a'(\alpha - \beta) \equiv a, \quad \partial'(\alpha + \beta) \equiv a, \quad a'(\gamma - \delta) \equiv -\partial \pmod{16},$$

woraus folgt:

$$n(\alpha - \beta)(\alpha + \beta + \gamma - \delta) \equiv a^2 - \partial'^2 \pmod{16},$$

also

$$\left(\frac{2}{\alpha - \beta}\right) e^{-\frac{3\pi i}{8}(\alpha - \beta)(\alpha + \beta + \gamma - \delta)} = \left(\frac{2}{a}\right)\left(\frac{2}{a'}\right)\left(\frac{2}{a}\right)\left(\frac{2}{\partial'}\right) = \left(\frac{2}{n}\right)$$

und

$$\varrho = e^{-\frac{2\pi i}{3}(\alpha(\gamma - \beta) - (\alpha^2 - 1)\beta\delta)}.$$

Ist $n$ nicht durch 3 theilbar, so ist

$$\begin{aligned} 2\alpha &\equiv a(a' + \partial'), & 2\delta &\equiv \partial(a' + \partial'), \\ 2\beta &\equiv a(\partial' - a'), & 2\gamma &\equiv \partial(\partial' - a') \end{aligned} \pmod{3},$$

also entweder $\alpha$ und $\delta$ oder $\beta$ und $\gamma$ durch 3 theilbar und also $\varrho = 1$.

Hieraus ergeben sich folgende zusammengehörige Vertauschungen (wobei die Aenderung von $a$, $c$, $\partial$ in $a'$, $c'$, $\partial'$ durch (6) bestimmt ist):

(9) $$\begin{array}{ccc} \omega, & u, & v \\ \dfrac{\omega - 1}{\omega + 1}, & \dfrac{\sqrt{2}}{u} & \varrho\left(\dfrac{2}{n}\right)\dfrac{\sqrt{2}}{v}. \end{array}$$

Wir wenden die Vertauschungen (4), (5), (9) auf folgende Functionen an:

$$(10)\qquad \begin{aligned} A &= \left(\frac{u}{v}\right)^r + \left(\frac{v}{u}\right)^r \\ B &= (u\,v)^s + \left(\frac{2}{n}\right)^{r+s} \frac{2^s}{(u\,v)^s}, \end{aligned}$$

worin $r$, $s$ zwei ganze Zahlen sind, welche den Bedingungen

$$(11)\qquad (n-1)\,r \equiv 0, \quad (n+1)\,s \equiv 0 \quad (\mathrm{mod}\ 12)$$

genügen, die also, wenn $n$ durch 3 theilbar ist, beide durch 3 theilbar sind.

Es ergeben sich dann folgende zusammengehörige Vertauschungen:

$$(12)\qquad \begin{array}{lll} \omega, & A, & B, \\ -\dfrac{1}{\omega}, & A, & B, \\ \omega + 2, & (-1)^{\frac{(n-1)r}{12}} A, & (-1)^{\frac{(n+1)s}{12}} B, \\ \dfrac{\omega - 1}{\omega + 1}, & \left(\dfrac{2}{n}\right)^r A, & \left(\dfrac{2}{n}\right)^r B. \end{array}$$

Bilden wir nun aus $A$, $B$ eine ganze rationale Function mit numerischen Coëfficienten

$$(13)\qquad \Phi_{a,\,c,\,\mathfrak{d}} = \Sigma\, M_{h,k}\, A^h B^k,$$

worin, falls in (12) Vorzeichenänderungen auftreten, die Exponenten $h$, $k$ so einzurichten sind, dass in allen Gliedern von (13) die gleichen Vorzeichenänderungen stattfinden, so wird das Functionensystem $\Phi_{a,\,c,\,\mathfrak{d}}$ oder wenigstens $\Phi^2_{a,\,c,\,\mathfrak{d}}$ der Forderung 1. des oben aufgestellten Satzes genügen und wir haben, um auch die Forderung 2. zu befriedigen und so eine Transformationsgleichung zu erhalten, die Coëfficienten $M_{h,k}$ so zu bestimmen, dass die sämmtlichen $\nu$ Werthe von $\Phi_{a,\,c,\,\mathfrak{d}}$ für $q = 0$ endlich bleiben. Diese Aufgabe vereinfacht sich wesentlich, wenn $n$ keinen quadratischen Theiler hat, und noch mehr, wenn $n$ eine Primzahl ist.

Hat nämlich $n$ keinen quadratischen Theiler, so kann man aus $\Phi_{a,\,0,\,\mathfrak{d}}$ die sämmtlichen Werthe $\Phi_{a,\,c,\,\mathfrak{d}}$ herleiten, durch Vermehrung von $\omega$ um gewisse ganze Zahlen; wenn also, was unsere Forderung ist, in der Entwickelung von $\Phi_{a,\,0,\,\mathfrak{d}}$ nach steigenden Potenzen von $q$ keine negativen Potenzen vorkommen, so gilt das Gleiche von sämmtlichen $\Phi_{a,\,c,\,\mathfrak{d}}$.

Ist aber $n$ eine Primzahl, so genügt der Nachweis, dass $\Phi_{1,\,0,\,n}$ keine negativen Potenzen von $q$ enthält, da das Gleiche durch Vertauschung von $\omega$ mit $\omega : n$ für $\Phi_{n,\,0,\,1}$ folgt.

Der constante Werth, welchen die Function $\Phi_{a,c,\delta}$ erhält, bestimmt sich aus einem Gliede der Entwickelung.

Bei der Ausführung dieser Rechnungen dienen die Entwickelungen für $a = n$, $c = 0$ [§. 21, (10)]:

$$
\begin{aligned}
A &= q^{-\frac{n-1}{24} r} \prod_{1,\infty}^{h} \left(\frac{1 + q^{n(2h-1)}}{1 + q^{2h-1}}\right)^r \\
&\quad + q^{\frac{n-1}{24} r} \prod_{1,\infty}^{h} \left(\frac{1 + q^{2h-1}}{1 + q^{n(2h-1)}}\right)^r \\
B &= q^{-\frac{n+1}{24} s} \prod_{1,\infty}^{h} (1 + q^{2h-1})^s \, (1 + q^{n(2h-1)})^s \\
&\quad + \left(\frac{2}{n}\right)^{r+s} q^{\frac{(n+1)}{24} s} \, 2^s \prod_{1,\infty}^{h} \frac{1}{(1 + q^{2h-1})^s \, (1 + q^{n(2h-1)})^s}.
\end{aligned}
\tag{14}
$$

Die Formeln werden nicht immer am einfachsten, wenn $r$, $s$ möglichst klein angenommen werden, sondern es erweist sich am zweckmässigsten, noch die Bedingung

$$
\frac{(n-1)r}{12} \equiv \frac{(n+1)s}{12} \pmod{2}
\tag{15}
$$

hinzuzufügen.

Wir erhalten so für die sieben ersten ungeraden Primzahlen folgende Bestimmung von $A$ und $B$:

$$
\begin{aligned}
n &= 3, & A &= \left(\frac{u}{v}\right)^6 + \left(\frac{v}{u}\right)^6, & B &= (u v)^3 - \frac{8}{(u v)^3}, \\
n &= 5, & A &= \left(\frac{u}{v}\right)^3 + \left(\frac{v}{u}\right)^3, & B &= (u v)^2 - \frac{4}{(u v)^2}, \\
n &= 7, & A &= \left(\frac{u}{v}\right)^4 + \left(\frac{v}{u}\right)^4, & B &= (u v)^3 + \frac{8}{(u v)^3}, \\
n &= 11, & A &= \left(\frac{u}{v}\right)^6 + \left(\frac{v}{u}\right)^6, & B &= u v - \frac{2}{v u}, \\
n &= 13, & A &= \frac{u}{v} + \frac{v}{u}, & B &= (u v)^6 - \frac{64}{(u v)^6}, \\
n &= 17, & A &= \left(\frac{u}{v}\right)^3 + \left(\frac{v}{u}\right)^3, & B &= (u v)^4 + \frac{16}{(u v)^4}, \\
n &= 19, & A &= \left(\frac{u}{v}\right)^2 + \left(\frac{v}{u}\right)^2, & B &= (u v)^3 - \frac{8}{(u v)^3}.
\end{aligned}
$$

Die Entwickelungen nach Potenzen von $q$ für $A$ und $B$ ergeben sich aus (14), soweit sie zur Rechnung gebraucht werden, folgendermaassen:

$$
\begin{aligned}
n &= 3, & A &= q^{-\frac{1}{2}}(1 - 5q \ldots), \\
& & B &= q^{-\frac{1}{2}}(1 - 5q \ldots), \\
n &= 5, & A &= q^{-\frac{1}{2}}(1 - 2q \ldots), \\
& & B &= q^{-\frac{1}{2}}(1 - 2q \ldots), \\
n &= 7, & A &= q^{-1}(1 - 4q \ldots), \\
& & B &= q^{-1}(1 + 11q \ldots), \\
n &= 11, & A &= q^{-\frac{5}{2}}(1 - 6q + 21q^2 \ldots), \\
& & B &= q^{-\frac{1}{2}}(1 - q + 2q^2 \ldots), \\
n &= 13, & A &= q^{-\frac{1}{2}}(1 + 2q^2 - 2q^3 \ldots), \\
& & B &= q^{-\frac{7}{2}}(1 + 6q + 15q^2 + 26q^3 \ldots), \\
n &= 17, & A &= q^{-2}(1 - 3q + 6q^2 - 13q^3 + 25q^4 - 39q^5 + 76q^6 \ldots), \\
& & B &= q^{-3}(1 + 4q + 6q^2 + 8q^3 + 17q^4 + 28q^5 + 54q^6 \ldots), \\
n &= 19, & A &= q^{-\frac{3}{2}}(1 - 2q + 3q^2 - 5q^3 + 11q^4 - 13q^5 + 24q^6 \\
& & & \qquad - 28q^7 \ldots), \\
& & B &= q^{-\frac{5}{2}}(1 + 3q + 3q^2 + 4q^3 + 9q^4 + 4q^5 + 39q^6 \\
& & & \qquad - 27q^7 \ldots),
\end{aligned}
$$

und daraus erhält man durch Elimination der negativen Potenzen die gesuchten Gleichungen zwischen $A$ und $B$:

$$
\begin{aligned}
\text{I.}\quad n &= 3, & A - B &= 0, \\
n &= 5, & A - B &= 0, \\
n &= 7, & A - B + 7 &= 0, \\
n &= 11, & A - B^5 + B^3 + 2B &= 0, \\
n &= 13, & A^7 + 6A^5 + A^3 - 20A - B &= 0, \\
n &= 17, & A^3 - B^2 + 17AB - 34A^2 + 34B + 116A & \\
& & + 440 &= 0, \\
n &= 19, & A^5 - B^3 + 19AB^2 - 95A^2B + 109A^3 & \\
& & + 128B - 128A &= 0 \text{ 1)}.
\end{aligned}
$$

---

1) Diese Gleichungen sind zuerst von Schläfli aufgestellt (Journal für Mathematik, Bd. 72).

Aus diesem System von Gleichungen leitet man ein zweites und drittes her für die Functionen $f_1$, $f_2$, indem man $\omega$ durch $\omega + 1$ und darauf $\omega$ durch $-1:\omega$ ersetzt. Diese beiden Systeme haben die gleiche Form, nur ist das eine Mal

$$u_1 = f_1(\omega), \quad v_1 = \left(\frac{2}{a}\right) f_1\left(\frac{c + \partial\omega}{a}\right),$$

das andere Mal

$$u_1 = f_2(\omega), \quad v_1 = \left(\frac{2}{\partial}\right) f_2\left(\frac{c + \partial\omega}{a}\right)$$

zu setzen. Aus den Vertauschungen (4) ergiebt sich so:

$$\text{II.} \quad n = 3, \quad A_1 = \left(\frac{u_1}{v_1}\right)^6 - \left(\frac{v_1}{u_1}\right)^6, \quad B_1 = (u_1 v_1)^3 + \frac{8}{(u_1 v_1)^3},$$
$$A_1 + B_1 = 0,$$

$$n = 5, \quad A_1 = \left(\frac{u_1}{v_1}\right)^3 - \left(\frac{v_1}{u_1}\right)^3, \quad B_1 = (u_1 v_1)^2 + \frac{4}{(u_1 v_1)^2},$$
$$A_1 + B_1 = 0,$$

$$n = 7, \quad A_1 = \left(\frac{u_1}{v_1}\right)^4 + \left(\frac{v_1}{u_1}\right)^4, \quad B_1 = (u_1 v_1)^3 + \frac{8}{(u_1 v_1)^3},$$
$$A_1 - B_1 - 7 = 0,$$

$$n = 11, \quad A_1 = \left(\frac{u_1}{v_1}\right)^6 - \left(\frac{v_1}{u_1}\right)^6, \quad B_1 = u_1 v_1 + \frac{2}{u_1 v_1},$$
$$A_1 + B_1^5 + B_1^3 - 2 B_1 = 0,$$

$$n = 13, \quad A_1 = \frac{u_1}{v_1} - \frac{v_1}{u_1}, \quad B_1 = (u_1 v_1)^6 + \frac{64}{(u_1 v_1)^6},$$
$$A_1^7 - 6 A_1^5 + A_1^3 + 20 A_1 + B_1 = 0,$$

$$n = 17, \quad A_1 = \left(\frac{u_1}{v_1}\right)^3 + \left(\frac{v_1}{u_1}\right)^3, \quad B_1 = (u_1 v_1)^4 + \frac{16}{(u_1 v_1)^4},$$
$$A_1^3 - B_1^2 - 17 A_1 B_1 - 34 A_1^2 - 34 B_1 + 116 A_1 + 440 = 0,$$

$$n = 19, \quad A_1 = \left(\frac{u_1}{v_1}\right)^2 - \left(\frac{v_1}{u_1}\right)^2, \quad B_1 = (u_1 v_1)^3 + \frac{8}{(u_1 v_1)^3},$$
$$A_1^5 + B_1^3 - 19 A_1 B_1^2 + 95 A_1^2 B_1 - 109 A_1^3 + 128 B_1 - 128 A_1 = 0.$$

## §. 77. Die Form der Schläfli'schen Modulargleichungen für einen Primzahlgrad.

Die Form, welche wir im vorigen Paragraphen für die zwischen

$$(1) \qquad u = f(\omega), \qquad v = f\left(\frac{c + \partial\,\omega}{a}\right)$$

bestehenden Relationen gefunden haben, lässt sich, wenigstens wenn der Transformationsgrad eine Primzahl $p$ ist, leicht unter ein allgemeines Gesetz bringen. Da für die Folge viel auf diese Form ankommt, gehen wir hier noch etwas genauer darauf ein.

Die Bestimmung der Zahlen $r$, $s$ nach (11) und (15) des vorigen Paragraphen hängt von dem Verhalten von $p$ gegen den Modul 24 ab, und da wir den Fall $p = 3$ ausschliessen können, so haben wir folgende Fälle:

$$(2) \qquad \begin{array}{lll}
p \equiv 1 \pmod{24} & r = 1 & s = 12 \\
p \equiv 5 & r = 3 & s = 2 \\
p \equiv 7 & r = 4 & s = 3 \\
p \equiv 11 & r = 6 & s = 1 \\
p \equiv 13 & r = 1 & s = 6 \\
p \equiv 17 & r = 3 & s = 4 \\
p \equiv 19 & r = 2 & s = 3 \\
p \equiv 23 & r = 12 & s = 1,
\end{array}$$

so dass $r + s$ stets ungerade ist und $p + 1$ durch $2r$, $p - 1$ durch $2s$ theilbar ist. Hiernach wird

$$(3) \qquad \begin{aligned}
A &= \left(\frac{u}{v}\right)^r + \left(\frac{v}{u}\right)^r, \\
B &= (u\,v)^s + \left(\frac{2}{p}\right)\frac{2^s}{(u\,v)^s}.
\end{aligned}$$

Nun wissen wir, dass die $p + 1$ Grössen $v$ die Wurzeln einer irreducibeln Transformationsgleichung

$$(4) \qquad \Phi_p(v, u) = v^{p+1} + U_1 v^p + \cdots U_{p+1} = 0$$

sind, in welcher die Coëfficienten $U_1 \ldots, U_{p+1}$ rationale Functionen von $u$ sind.

Wir schliessen sofort, dass es ganze rationale Functionen von $u$ sind. Denn erstens werden für $u = \infty$ die sämmtlichen

Wurzeln von (4) unendlich, wie man erkennt, wenn man $\omega = i\,\infty$, also $q = 0$ werden lässt. Zweitens geht nach (9) des vorigen Paragraphen durch die Vertauschung $\left(u, \frac{\sqrt{2}}{u}\right)$ die Gesammtheit der Wurzeln $v$ in

$$\left(\frac{2}{p}\right)\frac{\sqrt{2}}{v}$$

über. Hieraus folgt, dass für $u = 0$ die sämmtlichen Wurzeln $v$ in Null übergehen, also keine von ihnen unendlich wird, woraus zu schliessen ist, dass nicht nur die $U_1, U_2, \ldots U_{p+1}$ ganze Functionen von $u$ sind, sondern dass auch jede von ihnen den Factor $u$ enthalten muss.

Wir schliessen nun zunächst, genau wie bei der Invariantengleichung (§. 72, 2., 3. und 6.), dass

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

und dass

$$\Phi_p(v, u) = (v^p - u)(v - u^p) + p \sum_{1, p-1}^{h, k} c_{h,k}\, u^h v^k, \tag{6}$$

worin $c_{h,k} = c_{k,h}$ ganze Zahlen sind.

Wir wollen diese Function in der Weise darstellen

$$\Phi_p(v, u) = v^{p+1} + u^{p+1} + \sum_{1, p}^{h, k} a_{h,k}\, u^h\, v^k, \tag{7}$$

worin also $a_{h,k} = a_{k,h}$ ebenfalls ganze Zahlen sind, auf deren Theilbarkeit durch $p$ es nun weiter nicht ankommt, und es ist insbesondere $a_{p,p} = -1$. Wenn wir in der Gleichung

$$\Phi_p[f(p\,\omega), f(\omega)] = 0$$

$\omega$ durch $\omega + 2$ ersetzen, so ergiebt sich wegen der Irreducibilität auf Grund der Relation

$$f(\omega + 2) = e^{-\frac{\pi i}{12}} f(\omega),$$

dass in (7) nicht alle Glieder, sondern nur solche vorkommen, welche der Congruenz

$$h p + k \equiv p + 1 \pmod{24} \tag{8}$$

genügen.

Nun kennen wir noch eine weitere Eigenschaft der Functionen $\Phi_p(v, u)$, die sich aus der schon benutzten Vertauschung (9) des vorigen Paragraphen ergiebt, und die, wenn wir zur Abkürzung

$$\varepsilon = \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

setzen, so dargestellt werden kann

$$\Phi_p(v, u) = \left(\frac{u\,v}{\sqrt{2}}\right)^{p+1} \Phi_p\left(\frac{\varepsilon\sqrt{2}}{v}, \frac{\sqrt{2}}{u}\right). \tag{9}$$

Hieraus schliesst man auf die Relationen

$$\varepsilon^h\, 2^{\frac{h+k-p-1}{2}}\, a_{p+1-h,\; p+1-k} = a_{h,k}. \qquad a_{h,k} = a_{k,h}. \tag{10}$$

Wenn wir also diejenigen Glieder in (7) zusammenfassen, welche gleiche Coëfficienten $a_{h,k}$ haben, so können wir uns auf die Annahme beschränken, dass $h \geqq k$, $h + k \geqq p + 1$ sei, und es ergiebt sich $\Phi_p$, von den beiden Gliedern $v^{p+1}$, $u^{p+1}$ abgesehen, als ein Aggregat von Gliedern von den folgenden beiden Formen (wenn noch berücksichtigt wird, dass wegen (8) $\varepsilon^h = \varepsilon^k$ ist):

$$\begin{aligned} &v^h u^k + v^k u^h + \varepsilon^h\, 2^{\frac{h+k-p-1}{2}} \left(u^{p+1-h} v^{p+1-k} + u^{p+1-k} v^{p+1-h}\right) = \\ &\underset{h>k}{(u\,v)^{\frac{p+1}{2}}} \left[\left(\frac{v}{u}\right)^{\frac{h-k}{2}} + \left(\frac{u}{v}\right)^{\frac{h-k}{2}}\right] \left[(u\,v)^{\frac{h+k-p-1}{2}} + \frac{\varepsilon^h\, 2^{\frac{h+k-p-1}{2}}}{(u\,v)^{\frac{h+k-p-1}{2}}}\right]. \end{aligned} \tag{11}$$

$$\begin{aligned} &v^h\, u^h + \varepsilon^h\, 2^{h-\frac{p+1}{2}} (u\,v)^{p+1-h} \\ &= (u\,v)^{\frac{p+1}{2}} \left[(u\,v)^{h-\frac{p+1}{2}} + \frac{\varepsilon^h\, 2^{h-\frac{p+1}{2}}}{(u\,v)^{h-\frac{p+1}{2}}}\right]. \end{aligned} \tag{12}$$

Die Coëfficienten dieser Glieder in $\Phi_p$ sind ganze Zahlen. Nun ergiebt sich aus (8):

$$\left.\begin{aligned} (h-k) &\equiv (h-1)(p+1) \\ h+k-p-1 &\equiv -h(p-1) \end{aligned}\right\} \pmod{24},$$

und daher ist $h - k$ durch $2r$, $h + k - p - 1$ (worin $h$ auch $= k$ sein kann) durch $2s$ theilbar.

Setzen wir daher

$$\frac{h-k}{2} = r\alpha, \qquad \frac{h+k-p-1}{2} = s\beta,$$

so sind $\alpha$ und $\beta$ positive ganze Zahlen, welche an die Grenzen gebunden sind:

$$0 \overset{=}{<} \alpha < \frac{p+1}{2r}, \qquad 0 \overset{=}{<} \beta \leqq \frac{p-1}{2s}, \tag{13}$$

und überdies ergiebt die Congruenz $-h(p-1) \equiv 2s\beta \pmod{24}$, dass wenigstens in den Fällen, wo $\varepsilon = -1$ ist, $h \equiv \beta \pmod{2}$, also stets $\varepsilon^h = \varepsilon^\beta$.

Demnach wird (11)

$$(u\,v)^{\frac{p+1}{2}} \left[\left(\frac{v}{u}\right)^{r\alpha} + \left(\frac{u}{v}\right)^{r\alpha}\right] \left[(u\,v)^{s\beta} + \frac{\varepsilon^\beta\, 2^{s\beta}}{(u\,v)^{s\beta}}\right],$$

und (12)

$$(u\,v)^{\frac{p+1}{2}} \left[(u\,v)^{s\beta} + \frac{\varepsilon^\beta\, 2^{s\beta}}{(u\,v)^{s\beta}}\right].$$

Nun gelten die bekannten Formeln, wenn $x$, $\gamma$ beliebige Grössen sind und

$$x + \frac{\gamma}{x} = y$$

gesetzt wird,

$$x^2 + \frac{\gamma^2}{x^2} = y^2 - 2\gamma, \quad x^3 + \frac{\gamma^3}{x^3} = y^3 - 3\gamma y, \ldots,$$

woraus man durch den Schluss von $n$ auf $n+1$ erkennt, dass

$$x^n + \frac{\gamma^n}{x^n}$$

sich für jedes beliebige $n$ als ganze rationale Function $n$ten Grades von $y$ darstellen lässt, welche, wenn $\gamma$ eine ganze Zahl ist, ganzzahlige Coëfficienten hat, deren höchster $= 1$ ist.

Die beiden Grössen

$$\left(\frac{v}{u}\right)^{r\alpha} + \left(\frac{u}{v}\right)^{r\alpha} \quad \text{und} \quad (u\,v)^{s\beta} + \frac{\varepsilon^\beta\, 2^{s\beta}}{(u\,v)^{s\beta}}$$

können also in dieser Weise als ganze rationale Functionen von $A$ und $B$ der Grade $\alpha$ und $\beta$ dargestellt werden, und wir finden, wenn wir noch das dem Werthe $\beta = \frac{p-1}{2s}$ entsprechende Glied, das den Coëfficienten $-1$ hat, absondern und mit $c_{\alpha,\beta}$ ganzzahlige Coëfficienten bezeichnen:

$$(14) \qquad \frac{\Phi_p(u,v)}{(u\,v)^{\frac{p+1}{2}}} = A^{\frac{p+1}{2r}} - B^{\frac{p-1}{2s}} + \sum^{\alpha,\beta} c_{\alpha,\beta}\, A^\alpha B^\beta,$$

worin $\alpha$ und $\beta$ an die Grenzen

$$0 \leqq \alpha < \frac{p+1}{2r}, \quad 0 \leqq \beta < \frac{p-1}{2s}$$

gebunden sind. Dies ist die Form, welche wir im vorigen Paragraphen den Modulargleichungen bis $p = 19$ gegeben haben.

Es ist noch zu erwähnen, dass die in §. 72, 4., 5. für die Invariantengleichung bei zusammengesetztem Transformationsgrade durchgeführte Betrachtung unverändert auch für die Schlaefli'schen Modulargleichungen gilt, woraus wir schliessen können, dass alle diese Gleichungen rationale Zahlencoëfficienten haben.

## §. 78. Die irrationalen Formen der Modulargleichungen.

Den Transformationsgleichungen lassen sich durch Anwendung desselben Verfahrens weit einfachere Formen geben. Die Gleichungsformen, mit denen wir uns jetzt beschäftigen werden, enthalten die drei Functionen $f$, $f_1$, $f_2$ zugleich; da man aber nach §. 29, (11), (12) zwei dieser Functionen durch die dritte ausdrücken kann, so lassen sich zwei von ihnen eliminiren, und man kann so zu den Gleichungen des vorigen Paragraphen gelangen. Wenn man für $f_1$, $f_2$ die Ausdrücke durch $f$, oder für die drei Functionen $f, f_1\, f_2$ die Ausdrücke durch $k^2$ einsetzt, so kommen Wurzelzeichen vor, woraus der Name dieser Gleichungen sich erklärt.

Wir setzen wie oben

$$
\begin{aligned}
u &= f(\omega), & v &= f\left(\frac{c + \delta\,\omega}{a}\right),\\
u_1 &= f_1(\omega), & v_1 &= \left(\frac{2}{a}\right) f_1\left(\frac{c + \delta\,\omega}{a}\right),\\
u_2 &= f_2(\omega), & v_2 &= \left(\frac{2}{\delta}\right) f_2\left(\frac{c + \delta\,\omega}{a}\right)
\end{aligned} \tag{1}
$$

und erhalten nach (4), §. 76 folgende zusammengehörige Vertauschungen:

$$
\begin{array}{llll}
\omega, & u\,v, & u_1\,v_1, & u_2\,v_2,\\
(2)\quad -\dfrac{1}{\omega}, & \varrho\,u\,v, & \varrho\,u_2\,v_2, & \varrho\,u_1\,v_1,\\
\omega + 1, & e^{-\frac{(n+1)\pi i}{24}}\,\sigma\,u_1\,v_1 & e^{-\frac{(n+1)\pi i}{24}}\,\sigma\,u\,v, & e^{\frac{(n+1)\pi i}{12}}\,\sigma\,u_2\,v_2,
\end{array}
$$

worin $\varrho$, $\sigma$ die oben definirten dritten Einheitswurzeln sind.

Wir unterscheiden drei verschiedene Fälle nach dem Verhalten von $n$ zum Modul 8.

1. $n + 1 \equiv 0$, (mod 8).

Wir setzen

$$2A = uv + (-1)^{\frac{n+1}{8}}(u_1 v_1 + u_2 v_2)$$

$$(3) \qquad B = uvu_1v_1 + uvu_2v_2 + (-1)^{\frac{n+1}{8}} u_1v_1u_2v_2$$

$$= \frac{2}{u_1 v_1} + \frac{2}{u_2 v_2} + (-1)^{\frac{n+1}{8}} \frac{2}{uv},$$

so dass sich die zusammengehörigen Vertauschungen ergeben

$$(4) \qquad \begin{array}{ccc} \omega, & A, & B, \\ -\frac{1}{\omega}, & \varrho A, & \varrho^2 B, \\ \omega + 1, & e^{\frac{\pi i(n+1)}{12}} \sigma A, & e^{-\frac{\pi i(n+1)}{12}} \sigma^2 B. \end{array}$$

Ein Product von der Form $A^h B^k$ nimmt also durch die beiden Vertauschungen

$$\left(\omega, -\frac{1}{\omega}\right), \quad (\omega, \omega + 1)$$

die Factoren an

$$\varrho^{h-k}, \quad e^{(h-k)\frac{(n+1)\pi i}{12}} \sigma^{h-k},$$

welche $= 1$ sind, wenn $n + 1$ durch 3 theilbar ist. Wir bilden also jetzt mit numerischen Coëfficienten $M_{h,k}$ Functionen der Form

$$(5) \qquad \Phi_{a,c,\mathfrak{d}} = \Sigma\, M_{h,k} A^h B^k,$$

worin, wenn $n \equiv 0$ oder $\equiv 1 \pmod 3$ ist, $h$ und $k$ nur solche (ganzzahlige) Werthe annehmen dürfen, deren Differenzen $h - k$ bei der Theilung mit 3 denselben Rest lassen, wenn aber $n \equiv -1 \pmod 3$ dieser Beschränkung nicht unterworfen sind. Eine solche Function selbst, oder wenigstens ihre dritte Potenz genügt also einer invarianten Transformationsgleichung. Sie bleibt ausserdem für alle endlichen Werthe von $j(\omega)$ endlich und ist folglich eine ganze algebraische Function von $j(\omega)$. [Die Transformation zweiter Ordnung $\begin{pmatrix} 1, & 1 \\ -1, & 1 \end{pmatrix}$ braucht hier nicht zugezogen zu werden, da der Inbegriff der $\Phi_{a,c,\mathfrak{d}}$ schon bei der Substitution $(\omega, \omega + 1)$, nicht erst bei $(\omega, \omega + 2)$ ungeändert bleibt. Vgl. die Bemerkung am Anfang des §. 76.]

Wenn wir also die Constanten in $\Phi_{a,c,\mathfrak{d}}$ so bestimmen, dass in den Entwickelungen dieser Functionen keine negativen Potenzen von $q$ vorkommen, so müssen die sämmtlichen $\Phi_{a, c, \delta}$ einer und derselben Constanten gleich sein.

Zur Erreichung dieses Zieles genügt es auch hier, wenn $n$ keinen quadratischen Theiler hat, dass $\Phi_{a, 0, \delta}$, und wenn $n$ eine Primzahl ist, wenn $\Phi_{1, 0, n}$ für $q = 0$ endlich bleibt.

Bei diesen Rechnungen machen wir Gebrauch von den Entwickelungen:

$$\begin{aligned} u\,v &= q^{-\frac{n+1}{24}}\, \Pi(1 + q^{n(2h+1)})\,(1 + q^{2h+1}) \\ u_1\,v_1 &= q^{-\frac{n+1}{24}}\, \Pi(1 - q^{n(2h+1)})\,(1 - q^{2h+1}) \\ u_2\,v_2 &= 2\,q^{\frac{n+1}{12}}\, \Pi(1 + q^{2hn})\,(1 + q^{2h}), \end{aligned} \tag{6}$$

woraus durch Entwickelung nach Potenzen von $q$:

$$\begin{aligned} u\,v &= q^{-\frac{n+1}{24}}(1 + q + q^3 + q^4 + q^5 + q^6 + q^7 + 2\,q^8 \ldots) \\ u_1\,v_1 &= q^{-\frac{n+1}{24}}(1 - q - q^3 + q^4 - q^5 + q^6 - q^7 + 2\,q^8 \ldots) \\ u_2\,v_2 &= 2\,q^{\frac{n+1}{12}}(1 + q^2 + q^4 + 2\,q^6 + 2\,q^8 + \cdots) \end{aligned} \tag{7}$$

Die letzteren Formeln sind richtig für $n > 7$ (für $n = 3, 5, 7$ sind die Glieder von $q^3$, $q^5$, $q^7$ an zu modificiren). Für $n = 7$, $n = 23$ zeigen diese Ausdrücke, dass $A$ selbst für $q = 0$ endlich bleibt, woraus für diese Fälle die Gleichungen folgen:

$$\begin{aligned} n &= 7, & A &= 0, \\ n &= 23, & A &= 1. \end{aligned} \tag{8}$$

Durch einfache Rechnung findet man ferner noch:

$$\begin{aligned} n &= 31, & (A^2 - B)^2 - A &= 0, \\ n &= 47, & A^2 - A - B &= 2, \\ n &= 71, & A^3 - 4\,A^2 + 2\,A - B &= 1. \end{aligned} \tag{9}$$

Nicht ganz so einfach gestaltet sich die Rechnung für ein zusammengesetztes $n$. So muss man z. B. für $n = 15$ die Bedingung der Endlichkeit für $q = 0$ nicht nur für $\Phi_{1, 0, 15}$, sondern auch für $\Phi_{3, 0, 5}$ berücksichtigen. Diese beiden aber genügen. Man erhält so:

$$n = 15, \quad A^3 - A\,B + 1 = 0. \tag{10}$$

2. Ist $n \equiv 3 \pmod 8$, so sind dieselben Schlüsse zu ziehen, wenn wir setzen:

$$
\begin{aligned}
4A &= u^2 v^2 - u_1^2 v_1^2 - u_2^2 v_2^2 \\
B &= u^2 v^2 u_1^2 v_1^2 + u^2 v^2 u_2^2 v_2^2 - u_1^2 v_1^2 u_2^2 v_2^2,
\end{aligned}
\tag{11}
$$

für welche man aus (2) die zusammengehörigen Vertauschungen erhält

$$
\begin{array}{ccc}
\omega, & A, & B, \\
-\dfrac{1}{\omega}, & \varrho^2 A, & \varrho B, \\
\omega + 1, & e^{\frac{(n+1)\pi i}{6}} \sigma^2 A, & e^{-\frac{(n+1)\pi i}{6}} \sigma B,
\end{array}
\tag{12}
$$

woraus man in der gleichen Weise die Gleichungen ableitet:

$$
\begin{aligned}
n &= 3, & A &= 0, \\
n &= 11, & A &= 1, \\
n &= 19, & A^5 - 7A - B &= 0.
\end{aligned}
\tag{13}
$$

3. Ist $n \equiv 1 \pmod 4$, so kann man ebenso verfahren mit den Functionen

$$
\begin{aligned}
8A &= u^4 v^4 - u_1^4 v_1^4 - u_2^4 v_2^4 \\
B &= u^4 v^4 u_1^4 v_1^4 + u^4 v^4 u_2^4 v_2^4 - u_1^4 v_1^4 u_2^4 v_2^4,
\end{aligned}
\tag{14}
$$

für welche man die zusammengehörigen Vertauschungen erhält:

$$
\begin{array}{ccc}
\omega & A, & B, \\
-\dfrac{1}{\omega}, & \varrho A, & \varrho^2 B, \\
\omega + 1, & e^{\frac{(n+1)\pi i}{3}} \sigma A, & e^{-\frac{(n+1)\pi i}{3}} \sigma^2 B.
\end{array}
\tag{15}
$$

Nur der erste Fall $n = 5$ führt hier zu einem einfachen Resultat:

$$
n = 5, \quad A = 1. \tag{16}
$$

Für $n = 5$ lässt sich noch eine einfachere Form der Transformationsgleichung gewinnen.

Wenn wir nämlich auf die drei Functionen

$$
w = \frac{u_1^2 v_2^2 + u_2^2 v_1^2}{u v}, \quad w_1 = \frac{u_2^2 v^2 - v_2^2 u^2}{u_1 v_1}, \quad w_2 = \frac{u_1^2 v^2 - v_1^2 u}{u_2 v_2}
\tag{17}
$$

die Substitutionen $\left(\omega, -\dfrac{1}{\omega}\right)$, $(\omega, \omega + 1)$ anwenden, so ergeben sich unter der Voraussetzung $n \equiv 5 \pmod 8$ die zusammengehörigen Vertauschungen:

$$
\begin{array}{cccc}
\omega, & w, & w_1, & w_2, \\
-\dfrac{1}{\omega}, & w, & w_2, & w_1, \\
\omega + 1, & e^{-\frac{\pi i}{24}(n-5)} w_1, & e^{-\frac{\pi i}{24}(n-5)} w, & e^{\frac{\pi i}{12}(n-5)} w_2.
\end{array}
$$

Setzt man also

$$\begin{aligned} A &= w^2 + w_1^2 + w_2^2 \\ B &= w^2 w_1^2 + w^2 w_2^2 + w_1^2 w_2^2 \\ C &= w\, w_1\, w_2, \end{aligned}$$

so erhält man

$$\begin{array}{cccc} \omega, & A, & B, & C, \\ -\frac{1}{\omega}, & A, & B, & C, \\ \omega + 1, & e^{-\frac{\pi i}{12}(n-5)} A, & e^{-\frac{\pi i}{6}(n-5)} B, & C, \end{array}$$

so dass zwei dieser Functionen ebenso wie oben $A$ und $B$ benutzt werden können. Für $n = 5$ zeigt sich aber, dass in den Entwickelungen von $w, w_1, w_2$ nach Potenzen von $q$ keine negativen Potenzen vorkommen und dass also $A, B, C$ und mithin auch $w, w_1, w_2$ selbst constant sind.

Es lässt sich also die Modulargleichung für $n = 5$ in jeder der drei Formen aufstellen

$$(18) \qquad \begin{aligned} u_1^2 v_2^2 + u_2^2 v_1^2 &= 2\, u\, v \\ u_2^2 v^2 - v_2^2 u^2 &= 2\, u_1\, v_1 \\ u_1^2 v^2 - v_1^2 u^2 &= 2\, u_2\, v_2. \end{aligned}$$

Diese Gleichungen lassen sich auch aus der von Jacobi (Fund. art. 30, gesammelte Werke, Bd. 1, S. 123) gegebenen herleiten.

Wir schliessen diese Betrachtungen, indem wir in den einfachsten Fällen die Jacobi'schen Modulargleichungen aus diesen irrationalen Formen ableiten.

Wir setzen [vergl. §. 49, (3)]:

$$\frac{u_2}{u} = x = \sqrt[4]{\varkappa}, \qquad \frac{u_1}{u} = x' = \sqrt[4]{\varkappa'},$$

$$\frac{v_2}{v} = y = \sqrt[4]{\lambda}, \qquad \frac{v_1}{v} = y' = \sqrt[4]{\lambda'},$$

und eliminiren mittelst der Relationen

$$(19) \qquad \begin{aligned} x^8 + x'^8 &= 1, \quad x\,x' = \frac{\sqrt{2}}{u^3} \\ y^8 + y'^8 &= 1, \quad y\,y' = \frac{\sqrt{2}}{v^3} \end{aligned}$$

die Grössen $u$ und $v$.

Für $n = 3$ erhält man aus (13):

$$(20) \qquad x^2 y^2 + x'^2 y'^2 = 1,$$

eine Form der Modulargleichung, die von Legendre herrührt.

Daraus, indem man für $x'$, $y'$ aus (19) die Werthe setzt,

$$x^8 + y^8 = 4x^2y^2 - 6x^4y^4 + 4x^6y^6,$$

oder

$$(x^4 - y^4)^2 = 4(xy - x^3y^3)^2$$

und indem man hieraus die Wurzel zieht und das Vorzeichen durch $q = 0$ bestimmt, findet man:

$$(21) \qquad x^4 - y^4 = 2xy - 2x^3y^3, \qquad (n = 3),$$

was, abgesehen von dem dort nicht näher erklärten Vorzeichen von $\sqrt[4]{\lambda}$, mit §. 7, (12) übereinstimmt.

Für $n = 5$ folgt aus der zweiten Gleichung (18):

$$(x^2 - y^2)^3 = 4xyx'^4y'^4,$$

und daraus durch Quadriren

$$(x^2 - y^2)^6 = 16x^2y^2(1 - x^8 - y^8 + x^8y^8),$$

was leicht in die Form gebracht wird

$$(x^2 - y^2)^2 [(x^2 - y^2)^2 + 8x^2y^2]^2 = 16x^2y^2(1 - x^4y^4)^2.$$

Zieht man hieraus die Wurzel, so folgt, wie oben:

$$(22) \qquad x^6 - y^6 - 4xy(1 - x^4y^4) + 5x^2y^2(x^2 - y^2) = 0 \qquad (n = 5).$$

Für $n = 7$ erhält man, ohne Wurzelziehen, aus (8):

$$(23) \qquad xy + x'y' = 1$$

und daraus:

$$(24) \qquad x^8 + y^8 - 8xy(1 + x^6y^6) + 28x^2y^2(1 + x^4y^4)$$
$$- 56x^3y^3(1 + x^2y^2) + 70x^4y^4 = 0 \qquad (n = 7).$$

## §. 79. Zusammengesetzte Transformationsgrade.

Ist der Transformationsgrad eine zusammengesetzte Zahl, so kann man noch andere Transformationsgleichungen aufstellen, welche einfacher sind als die, welche man auf dem Wege des vorigen Paragraphen gewinnt.

Wir führen diese Betrachtungen hier nur in den einfachsten Fällen durch.

Der ungerade Transformationsgrad $n$ sei in zwei Factoren zerlegt

$$(1) \qquad n = n'n'',$$

welche zu einander relativ prim sind.

Es lassen sich dann jeder Transformation $n$ten Grades von der Form

$$(2)\qquad \begin{pmatrix} a, & 0 \\ c, & \partial \end{pmatrix}$$

je eine und nur eine Transformation der Grade $n'$, $n''$

$$(3)\qquad \begin{pmatrix} a', & 0 \\ c', & \partial' \end{pmatrix}, \quad \begin{pmatrix} a'', & 0 \\ c'', & \partial'' \end{pmatrix}$$

zuordnen, welche durch folgende Bedingungen bestimmt sind:

$$(4)\qquad \begin{array}{ll} a = a'\,a'', & \partial = \partial'\,\partial'' \\ \partial''\,c' \equiv c \pmod{a'}, & \partial'\,c'' \equiv c \pmod{a''} \end{array}$$

und umgekehrt folgt aus jedem Paar Transformationen von der Form (3) nach (4) eine und nur eine Transformation (2). Nach (4) sind nämlich zunächst $\partial'$, $\partial''$ bestimmt als die grössten gemeinschaftlichen Theiler von $\partial$ mit $n'$ und $n''$, und darauf wird $c'$ nach dem Modul $a'$, $c''$ nach dem Modul $a''$ bestimmt aus den beiden letzten Congruenzen (4).

Es kommt nun vor Allem darauf an, zu zeigen, dass die Congruenzen (4) erhalten bleiben, wenn die Transformationen (2) und (3) nach §. 72, (8) bis (12) durch die beiden linearen Transformationen

$$(\omega, \omega + 1), \quad \left(\omega, -\frac{1}{\omega}\right)$$

umgeformt werden.

Wir setzen nach den erwähnten Formeln:

$$(5)\qquad \begin{aligned} \begin{pmatrix} a, & 0 \\ c, & \partial \end{pmatrix} \begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix} &= \begin{pmatrix} 1, & 0 \\ \lambda, & 1 \end{pmatrix} \begin{pmatrix} a, & 0 \\ c_1, & \partial \end{pmatrix} \\ \begin{pmatrix} a', & 0 \\ c', & \partial' \end{pmatrix} \begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix} &= \begin{pmatrix} 1, & 0 \\ \lambda', & 1 \end{pmatrix} \begin{pmatrix} a' & 0 \\ c_1', & \partial' \end{pmatrix} \\ \begin{pmatrix} a'', & 0 \\ c'', & \partial'' \end{pmatrix} \begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix} &= \begin{pmatrix} 1, & 0 \\ \lambda'', & 1 \end{pmatrix} \begin{pmatrix} a'', & 0 \\ c_2'', & \partial'' \end{pmatrix} \end{aligned}$$

$$(6)\qquad \begin{aligned} \begin{pmatrix} a, & 0 \\ c, & \partial \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} &= \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \begin{pmatrix} a_2, & 0 \\ c_2, & \partial_2 \end{pmatrix} \\ \begin{pmatrix} a', & 0 \\ c', & \partial' \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} &= \begin{pmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{pmatrix} \begin{pmatrix} a_2', & 0 \\ c_2', & \partial_2' \end{pmatrix} \\ \begin{pmatrix} a'', & 0 \\ c'', & \partial'' \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} &= \begin{pmatrix} \alpha'', & \beta'' \\ \gamma'', & \delta'' \end{pmatrix} \begin{pmatrix} a_2'', & 0 \\ c_2'', & \partial_2'' \end{pmatrix}. \end{aligned}$$

Es folgt zunächst aus §. 72, (9):

$$c_1 \equiv c + \partial \pmod{a}, \quad c_1' \equiv c' + \partial' \pmod{a'}, \quad c_1'' \equiv c'' + \partial'' \pmod{a''},$$

woraus, nach (4)

$$\partial'' c_1' \equiv \partial'' c' + \partial \equiv c_1 \pmod{a'}$$
$$\partial' c_1'' \equiv \partial' c'' + \partial \equiv c_1 \pmod{a''}$$

in Uebereinstimmung mit den Congruenzen (4).

Für die Zusammensetzung (6) ergiebt sich nach §. 72, (12), dass $\partial_2$, $\partial_2'$, $\partial_2''$ die grössten gemeinschaftlichen Theiler von $a, c$; $a', c'$; $a'', c''$ sind; weil aber $\partial''$ relativ prim zu $a'$, und $\partial'' c' \equiv c \pmod{a'}$ ist, so ist auch $\partial_2'$ der grösste gemeinschaftliche Theiler von $a'$ und $c$ und aus den gleichen Gründen $\partial_2''$ der grösste gemeinschaftliche Theiler von $a''$ und $c$, woraus man schliesst, da $a'$, $a''$ relativ prim sind:

$$\partial_2 = \partial_2' \partial_2'', \quad a_2 = a_2' a_2''.$$

Ferner ist nach §. 72, (11), (12), (13):

$$\partial_2 = \alpha\, c - \gamma\, a, \quad c_2 = - \partial\, \alpha$$
$$\partial_2' = \alpha' c' - \gamma' a', \quad c_2' = - \partial' \alpha',$$

also nach (4):

$$\partial_2 c_2' - c_2 \partial_2' \equiv \alpha \alpha' (\partial c' - c \partial') \equiv 0 \pmod{n'},$$

folglich auch

$$\partial_2'' c_2' - c_2 \equiv 0 \pmod{a_2'},$$

in Uebereinstimmung mit (4), und ebenso folgt:

$$\partial_2' c_2'' - c_2 \equiv 0 \pmod{a_2''},$$

wodurch also der Beweis geführt ist, dass die durch (4) ausgedrückte Zusammengehörigkeit der Transformationen

$$\begin{pmatrix} a, & 0 \\ c, & \partial \end{pmatrix}, \quad \begin{pmatrix} a', & 0 \\ c', & \partial' \end{pmatrix}, \quad \begin{pmatrix} a'', & 0 \\ c'', & \partial'' \end{pmatrix}$$

durch Anwendung irgend einer linearen Transformation auf $\omega$ nicht gestört wird. Da wir hier $n$ als ungerade voraussetzen, so können wir immer $c$, $c'$ $c''$ durch 16 theilbar annehmen; wenn $n$ und folglich auch $n'$, $n''$ untheilbar sind durch 3, so können $c$, $c'$, $c''$ auch durch 3 theilbar angenommen werden. Ist aber $n$ durch 3 theilbar, so wird von den beiden Factoren $n'$, $n''$ der eine, etwa $n''$, durch 3 theilbar sein, der andere, $n'$, nicht. Es kann dann $c'$ noch durch 3 theilbar vorausgesetzt werden, nicht aber $c$ und $c''$. In diesem Falle soll die Abhängigkeit des $c''$ von $c$ noch näher bestimmt werden durch die Congruenz

$$\partial' c'' \equiv c \pmod{3\, a''}. \tag{7}$$

Eine Lösung dieser Congruenz kann man immer aus einer Lösung der Congruenz (4) $\partial' c'' \equiv c \pmod{a''}$ herleiten, indem man zu $c''$ ein Vielfaches von $a''$ hinzufügt.

Die Congruenz (7) hat dann nach §. 72, (9) bis (13) zur Folge:

$$\lambda \equiv n' \lambda'' \pmod{3} \tag{8}$$

$$\left.\begin{array}{ll} \alpha \equiv \alpha'' \partial' \partial_2', & \beta \equiv \beta'' a' \partial_2' \\ \gamma \equiv \gamma'' a' \partial_2', & \delta \equiv \delta'' \partial' \partial_2' \end{array}\right. \pmod{3}. \tag{9}$$

Es mögen nun $v', v_1', v_2'; v'', v_1'', v_2''$ dieselbe Bedeutung für die Zahlen $n', n''$ haben, welche den $v, v_1, v_2$ in §. 76 (3) für die Zahl $n$ gegeben wär, nämlich:

$$\begin{array}{ll} v' = f\left(\dfrac{c' + \partial' \omega}{a'}\right), & v'' = f\left(\dfrac{c'' + \partial'' \omega}{a''}\right), \\ v_1' = \left(\dfrac{2}{a'}\right) f_1\left(\dfrac{c' + \partial' \omega}{a'}\right), & v_1'' = \left(\dfrac{2}{a''}\right) f_1\left(\dfrac{c'' + \partial'' \omega}{a''}\right), \\ v_2' = \left(\dfrac{2}{\partial'}\right) f_2\left(\dfrac{c' + \partial' \omega}{a'}\right), & v_2'' = \left(\dfrac{2}{\partial''}\right) f_2\left(\dfrac{c'' + \partial'' \omega}{a''}\right). \end{array} \tag{10}$$

Wir wenden die Vertauschungstabelle (4), §. 76 auf diese Functionen an. Da $n'$ unter allen Umständen durch 3 untheilbar ist, so sind die cubischen Einheitswurzeln $\varrho', \sigma' = 1$ zu setzen, während in Folge der Congruenzen (8), (9):

$$\varrho'' = \varrho^{n'}, \quad \sigma'' = \sigma^{n'} \tag{11}$$

wird. Wir erhalten hiernach folgende zusammengehörige Vertauschungen:

$$\begin{array}{cccc} \omega, & v' & v_1', & v_2', \\ -\dfrac{1}{\omega}, & v' & v_2', & v_1', \\ \omega + 1, & e^{-\frac{n'\pi i}{24}} v_1', & e^{-\frac{n'\pi i}{24}} v', & e^{\frac{n'\pi i}{12}} v_2', \\ \hline \omega & v'', & v_1'', & v_2'', \\ -\dfrac{1}{\omega}, & \varrho^{n'} v'', & \varrho^{n'} v_2'', & \varrho^{n'} v_1'', \\ \omega + 1, & \sigma^{n'} e^{-\frac{n''\pi i}{24}} v_1'', & \sigma^{n'} e^{-\frac{n''\pi i}{24}} v'', & \sigma^{n'} e^{\frac{n''\pi i}{12}} v_2'', \end{array} \tag{12}$$

welche zusammen mit den Vertauschungen (4), §. 76 gelten.

Wir unterscheiden jetzt zwei Fälle.

1. Wenn

$$(n' + 1)(n'' + 1) = 8\mu \equiv 0 \pmod{8} \text{ ist,} \tag{13}$$

so setzen wir

$$(14)\qquad U = u\,v\,v'\,v'', \quad U_1 = u_1\,v_1\,v'_1\,v''_1, \quad U_2 = u_2\,v_2\,v'_2\,v''_2.$$

$$2A = U + (-1)^\mu (U_1 + U_2)$$

$$(15)\qquad B = U\,U_1 + U\,U_2 + (-1)^\mu\,U_1\,U_2$$

$$= \frac{4}{U_1} + \frac{4}{U_2} + (-1)^\mu\,\frac{4}{U}.$$

Aus (12) und §. 76, (4) erhalten wir dann folgende zusammengehörige Vertauschungen:

$$\begin{array}{llll} & \omega, & A, & B, \\ (16) & -\dfrac{1}{\omega}, & \varrho^{n'+1} A, & \varrho^{-(n'+1)} B, \\ & \omega + 1, & \sigma^{n'+1}\, e^{\frac{2\mu\pi i}{3}} A, & \sigma^{-(n'+1)}\, e^{-\frac{2\mu\pi i}{3}} B. \end{array}$$

Wir wenden nun unser Princip zur Herleitung von Modulargleichungen auf diese Functionen an und bemerken dazu noch Folgendes:

Die in (16) vorkommenden dritten Einheitswurzeln sind $= 1$, wenn entweder $n$ durch 3 untheilbar und $\mu$ durch 3 theilbar ist, oder $n''$ durch 3 theilbar ist und $n'$ den Rest 2 lässt. In diesen Fällen ist jede rationale Function von $A$ und $B$ Wurzel einer invarianten Transformationsgleichung. In den anderen Fällen kommt diese Eigenschaft dem Cubus einer solchen rationalen Function von $A$ und $B$ zu, bei welchen die Differenzen der Exponenten sämmtlicher Glieder einander nach dem Modul 3 congruent sind.

Sind diese rationalen Functionen ganze Functionen und sind ausserdem ihre sämmtlichen Werthe für $q = 0$ endlich, so müssen sie einer Constanten gleich sein und dadurch gewinnen wir Transformationsgleichungen.

Sind $n'$, $n''$ Primzahlen, so genügt es auch hier (vgl. §. 75), wenn die negativen Potenzen von $q$ in der Entwickelung einer solchen Function nach steigenden Potenzen von $q$ in dem einen Hauptfall wegfallen, nämlich in dem, wo

$$\begin{pmatrix} a, & 0 \\ c, & \partial \end{pmatrix}, \begin{pmatrix} a', & 0 \\ c', & \partial' \end{pmatrix}, \begin{pmatrix} a'', & 0 \\ c'', & \partial'' \end{pmatrix}$$

gleich sind

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

also

$$U = f(\omega) f(n'\,\omega) f(n''\,\omega) f(n'\,n''\,\omega);$$

denn aus der Entwickelung für diesen einen Fall kann man die Entwickelungen für die übrigen Fälle herleiten, indem man $\omega$ ersetzt durch

$$\frac{\omega}{n}, \quad \frac{\omega}{n'}, \quad \frac{\omega}{n''} \tag{17}$$

und dann noch $\omega$ um ganze Zahlen vermehrt, wodurch keine negativen Potenzen von $q$ neu eingeführt werden können.

Für die Durchführung der Rechnung bedient man sich der Entwickelungen

$$\begin{aligned} U &= q^{-\frac{(n'+1)(n''+1)}{24}} \times \\ &\Pi(1+q^{2h-1})(1+q^{(2h-1)n'})(1+q^{(2h-1)n''})(1+q^{(2h-1)n}) \\ U_1 &= q^{-\frac{(n'+1)(n''+1)}{24}} \times \\ &\Pi(1-q^{2h-1})(1-q^{(2h-1)n'})(1-q^{(2h-1)n''})(1-q^{(2h-1)n}) \\ U_2 &= 4\,q^{\frac{(n'+1)(n''+1)}{12}} \times \\ &\Pi(1+q^{2h})(1+q^{2hn'})(1+q^{2hn''})(1+q^{2hn}), \end{aligned} \tag{18}$$

welche in den einzelnen Fällen die Potenzentwickelungen von $A$, $B$ liefern, woraus die negativen Potenzen von $q$ zu eliminiren sind. Man berechnet auf diese Weise sehr einfach die folgenden Gleichungen:

$$\begin{aligned} n &= 15, \quad A = 1 \\ n &= 21, \quad (A^2 - B)^2 - A = 0 \\ n &= 33, \quad A^2 - B - A = 4 \\ n &= 35, \quad A^2 - B - A = 2 \\ n &= 55, \quad A^3 - B - 4A^2 - A + 4 = 0. \end{aligned} \tag{19}$$

2. Wenn

$$(n'-1)(n''-1) = 8\mu \equiv 0 \pmod 8,$$

so setzen wir

$$\begin{aligned} A &= \frac{uv}{v'v''} + (-1)^{\mu}\left(\frac{u_1 v_1}{v_1' v_1''} + \frac{u_2 v_2}{v_2' v_2''}\right) \\ B &= \frac{v'v''}{uv} + (-1)^{\mu}\left(\frac{v_1' v_1''}{u_1 v_1} + \frac{v_2' v_2''}{u_2 v_2}\right) \end{aligned} \tag{20}$$

und erhalten nach (12) die zusammengehörigen Vertauschungen

$$\begin{array}{ccc} \omega, & A, & B, \\ -\dfrac{1}{\omega}, & \varrho^{1-n'} A, & \varrho^{n'-1} B, \\ \omega + 1, & \sigma^{1-n'} e^{\frac{2\mu\pi i}{3}} A, & \sigma^{n'-1} e^{-\frac{2\mu\pi i}{3}} B. \end{array} \tag{21}$$

Wir können daher dasselbe Verfahren anwenden wie oben, wenn wir noch die Beschränkung hinzufügen, dass nur symmetrische Functionen von $A$ und $B$, d. h. rationale Functionen von $AB$, $A+B$ benutzt werden, weil nur unter dieser Voraussetzung aus einem der Werthe einer solchen Function durch die Vertauschungen (17) alle übrigen folgen. Man berechnet leicht die folgenden Beispiele:

$$\begin{aligned} &n = 15, \quad AB + 1 = 0 \\ (22) \qquad &n = 35, \quad 2(A+B) - AB = 5 \\ &n = 39, \quad 2(A+B) - AB = 3. \end{aligned}$$

---

## Zehnter Abschnitt.

# Die Gruppe der Transformationsgleichungen und die Gleichung 5ten Grades.

### §. 80. Die Galois'sche Gruppe der Transformationsgleichungen für einen Primzahlgrad.

Ein eingehenderes algebraisches Studium der Transformationsgleichungen erfordert die Kenntniss ihrer Galois'schen Gruppe. Da wir die Transformationsgleichungen aus den Theilungsgleichungen hergeleitet haben, deren Gruppe uns bekannt ist (§. 66), so können wir die Gruppe der Transformationsgleichungen gleichfalls bilden.

Die Transformationsgleichungen ergaben sich (§. 68) dadurch, dass die Wurzeln der Theilungsgleichungen sich in Reihen eintheilen liessen, welche durch die Vertauschungen der Gruppe der Theilungsgleichung nicht aus einander gerissen, sondern nur unter einander vertauscht werden.

Jeder dieser Reihen ordnet sich eine bestimmte Wurzel einer Transformationsgleichung zu, und die Gruppe der letzteren besteht daher aus dem Inbegriff der Vertauschungen, welche durch die Gruppe der Theilungsgleichung unter den Reihen hervorgerufen werden.

Ist der Transformationsgrad $n$ eine ungerade Primzahl $p$, so gestattet diese Gruppe eine sehr elegante Darstellung, die zu weiteren Untersuchungen geeignet ist, und wir halten jetzt diese Voraussetzung fest.

Es wurde im §. 68, (3) bereits die nothwendige und hinreichende Bedingung ermittelt, dass zwei Wurzeln der Theilungsgleichung

(1) $$x_{\mu,\mu'}, \quad x_{\nu,\nu'}$$

in dieselbe Reihe $R$ gehören, nämlich die Congruenz

(2) $$\mu\nu' - \nu\mu' \equiv 0 \pmod{p}.$$

Wenn wir nun, wie es in der Zahlentheorie üblich ist (Gauss, Disquisitiones arithmeticae, art. 31), durch das Symbol

$$\frac{a}{b} \pmod{p}$$

diejenige ganze Zahl oder Zahlclasse (mod $p$) verstehen, welche, mit $b$ multiplicirt, bei der Theilung durch $p$ den Rest $a$ lässt, so können wir, vorausgesetzt, dass $\mu'$, $\nu'$ nicht durch $p$ theilbar sind, die eine Reihe definirende Congruenz (2) auch so schreiben:

(3) $$\frac{\mu}{\mu'} \equiv \frac{\nu}{\nu'} \pmod{p},$$

und wir werden also naturgemäss darauf geführt, durch den Werth des Verhältnisses

(4) $$\frac{\mu}{\mu'} \equiv z \pmod{p},$$

welches jeder der Zahlen 0, 1, . . . $p - 1$ congruent sein kann, und welches für eine ganze Reihe unveränderlich ist, diese Reihe $R$ zu bezeichnen. Es bleibt dabei zunächst die eine Reihe unbezeichnet, in welcher $\mu'$ und folglich alle $\nu'$ durch $p$ theilbar sind, aber auch diese Reihe ordnet sich der allgemeinen Bezeichnung sehr gut unter, wenn wir, falls $\mu' \equiv 0 \pmod{p}$

(5) $$\frac{\mu}{\mu'} \equiv \infty \pmod{p}$$

setzen, so dass wir also noch eine $p + 1$te Reihe $R_\infty$ erhalten. Die Gesammtheit der Reihen, deren Anzahl $p + 1$ beträgt, ist hiernach zu bezeichnen durch

(6) $$R_\infty, R_0, R_1 \ldots, R_{p-1}.$$

Entsprechend werden die zugehörigen Wurzeln einer Transformationsgleichung mit

(7) $$v_\infty, v_0, v_1 \ldots, v_{p-1}$$

zu bezeichnen sein.

Wenn wir beispielsweise die Invariantengleichung (§. 72) zu Grunde legen, so ist (nach den Bestimmungen des §. 71, (10) über die Zahlen $a$, $c$, $\partial$)

$$(8) \qquad v_\infty = j(p\omega), \quad v_z = j\left(\frac{z+\omega}{p}\right)$$

zu setzen, und ebenso, wenn irgend eine andere Transformationsgleichung gewählt wird.

Nach dieser Bezeichnungsweise sind wir im Stande, die Gruppe der Transformationsgleichung aus der der Theilungsgleichung sofort abzuleiten.

Wir setzen zunächst als Rationalitätsbereich den Inbegriff der rationalen Functionen von $\varkappa^2$ mit rationalen Zahlencoëfficienten fest.

Nach §. 66, 3. besteht in diesem Rationalitätsbereich die Gruppe der Theilungsgleichung aus allen Substitutionen, wodurch $\mu$, $\mu'$ in

$$\begin{gathered} \partial\mu - b\mu' \\ -c\mu + a\mu' \end{gathered}$$

übergeführt werden, worin $a$, $b$, $c$, $\partial$ beliebige, nach dem Modul $p$ genommene ganze Zahlen sind, deren Determinante

$$(9) \qquad \Delta = a\partial - bc$$

durch $p$ nicht theilbar ist, und die Anzahl aller dieser Substitutionen beträgt

$$(10) \qquad p(p-1)(p^2-1) \qquad [\S.\ 66,\ (27)].$$

Daraus ergiebt sich aber nach der Bezeichnungsweise (4), (5) die Gruppe der Transformationsgleichung als bestehend aus allen durch das Symbol

$$(11) \qquad \left(z, \frac{\partial z - b}{-cz + a}\right) \pmod p$$

ausgedrückten Vertauschungen.

Wir bezeichnen eine Substitution $(z, z')$, wenn

$$(12) \qquad z \equiv \frac{c + \partial z'}{a + bz'} \pmod p$$

ist, ähnlich wie früher durch

$$(13) \qquad \begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix}$$

und erhalten für die Zusammensetzung zweier solcher Substitutionen, wenn

$$z' \equiv \frac{c' + \partial' z''}{a' + b' z''} \pmod p$$

ist, die Regel

$$(14)\qquad (z, z')\,(z', z'')$$
$$\equiv \begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix} \begin{pmatrix} a', & b' \\ c', & \partial' \end{pmatrix} \equiv \begin{pmatrix} a a' + b c', & a b' + b \partial' \\ c a' + \partial c', & c b' + \partial \partial' \end{pmatrix} \pmod{p},$$

in Uebereinstimmung mit der Regel für die Zusammensetzung zweier Transformationen in §. 24. Die Substitution (11) ist hiernach zu bezeichnen mit

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

Die durch alle Substitutionen dieser Form [nach (14)] gebildete Gruppe bezeichnen wir mit $\mathfrak{L}$ (Gruppe der linearen Substitutionen).

Die Functionen (12) von $z'$ und also auch die Substitutionen (13) bleiben ungeändert, wenn die vier Zahlen $a$, $b$, $c$, $\partial$ mit einem und demselben durch $p$ nicht theilbaren Factor multiplicirt werden, und daraus ergiebt sich nach (10) die Anzahl dieser Functionen oder der Grad der Gruppe $\mathfrak{L}$

$$(15)\qquad p\,(p^2 - 1),$$

den man auch leicht durch directe Abzählung findet.

Werden in einer der Substitutionen (13) die vier Zahlen $a$, $b$, $c$, $\partial$ mit einem gemeinsamen, durch $p$ untheilbaren Factor multiplicirt, so wird die Determinante $\Delta$ mit dem Quadrat dieses Factors multiplicirt. Es bleibt daher nicht die Determinante $\Delta$, wohl aber ihr quadratischer Charakter, d. h. der Werth des Symbols

$$\left(\frac{\Delta}{p}\right)$$

durch diese Multiplication erhalten.

Setzen wir zwei der Substitutionen (13) zusammen, so multipliciren sich ihre Determinanten und hieraus folgt, dass alle diejenigen Substitutionen der Gruppe $\mathfrak{L}$, in welchen $\Delta$ quadratischer Rest von $p$ ist, eine Gruppe unter sich bilden, die wir mit $\mathfrak{L}_0$ bezeichnen wollen.

Die Gruppe $\mathfrak{L}_0$ ist ein (eigentlicher) Divisor der Gruppe $\mathfrak{L}$ vom Index 2.

Setzt man die Substitutionen von $\mathfrak{L}_0$ zusammen mit irgend einer Substitution $(z, \beta z) = \begin{pmatrix} 1, & 0 \\ 0, & \beta^{-1} \end{pmatrix}$, wo $\beta$ und also auch $\beta^{-1}$ ein quadratischer Nichtrest von $p$ ist, so erhält man die ganze Gruppe $\mathfrak{L}$.

Ist $\Delta$ quadratischer Rest von $p$, so kann man einen zu $a$, $b$, $c$, $\partial$ hinzuzufügenden gemeinsamen Factor so wählen, dass $\Delta \equiv 1 \pmod{p}$ wird, so dass wir die Gruppe $\mathfrak{L}_0$ auch darstellen können durch

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}, \quad \alpha\delta - \beta\gamma \equiv 1 \pmod{p}. \tag{16}$$

In einer dieser Substitutionen sind die Zahlen $\alpha$, $\beta$, $\gamma$, $\delta$ nach dem Modul $p$ bis auf das gemeinsame Vorzeichen bestimmt. Der Grad der Gruppe $\mathfrak{L}_0$ ist

$$\frac{1}{2} p(p^2 - 1). \tag{17}$$

Auf die Form (16) kommt man aber direct, wenn man als die Gruppe der Theilungsgleichung nicht die Gruppe $\mathfrak{A}$, sondern die Gruppe $\mathfrak{B}$ des §. 66 betrachtet, d. h. wenn man $p$te Einheitswurzeln dem Rationalitätsbereich adjungirt, woraus der Satz fliesst:

Die Gruppe $\mathfrak{L}_0$ ist die Gruppe der Transformationsgleichung, wenn $p$te Einheitswurzeln dem Rationalitätsbereich adjungirt sind.

Zur Reduction der Gruppe $\mathfrak{L}$ auf die Gruppe $\mathfrak{L}_0$ genügt aber schon die Adjunction einer zweiwerthigen Function und daher ist mit der Adjunction der $p$ten Einheitswurzeln zu viel geschehen. Um zu erkennen, welche Irrationalität nothwendig zu adjungiren ist, dienen die Sätze der §§. 66, 68.

Im §. 66, 3. haben wir gesehen, dass die $p$te Einheitswurzel $\varrho$ rational darstellbar ist durch die Wurzeln der Theilungsgleichung und dass durch eine Substitution der Gruppe $\mathfrak{A}$, deren Determinante mit $m$ congruent ist, $\varrho$ in $\varrho^m$ übergeht; ferner haben wir im §. 68 nachgewiesen, dass durch Adjunction sämmtlicher Wurzeln einer Transformationsgleichung die Gruppe der Theilungsgleichung auf die Gruppe $\mathfrak{A}_0$ reducirt wird, welche aus sämmtlichen Substitutionen der Form

$$\begin{pmatrix} a, & 0 \\ 0, & a \end{pmatrix} \tag{18}$$

besteht, wo $a$ eine beliebige, durch $p$ nicht theilbare Zahl ist. Die Determinanten der Substitutionen von $\mathfrak{A}_0$ sind also Quadrate und sind daher nach dem Modul $p$ congruent mit je einem der $\frac{p-1}{2}$ quadratischen Reste von $p$.

Die Summe

$$(19) \qquad A = \sum^{a} \varrho^{a},$$

worin für $a$ die sämmtlichen quadratischen Reste von $p$ zu setzen sind, bleibt daher ungeändert durch die Substitutionen von $\mathfrak{A}_0$ und ist in Folge dessen rational durch die Wurzeln der Transformationsgleichung ausdrückbar. Die Summe $A$ bleibt ungeändert durch die Substitutionen der Gruppe $\mathfrak{B}$ und also auch durch $\mathfrak{L}_0$, während sie durch die Substitutionen von $\mathfrak{A}$ und daher auch von $\mathfrak{L}$ zwei verschiedene Werthe erhält, nämlich, wenn $b$ die Reihe der Nichtreste durchläuft,

$$A = \sum^{a} \varrho^{a}, \qquad B = \sum^{b} \varrho^{b}.$$

$A$ ist daher eine zur Gruppe $\mathfrak{L}_0$ gehörige Function und durch ihre Adjunction wird $\mathfrak{L}$ auf $\mathfrak{L}_0$ reducirt.

Die Werthe der Summen $A$, $B$ sind aber bekannt[1]):

$$A = \frac{-1 \pm \sqrt{(-1)^{\frac{p-1}{2}} p}}{2}, \quad B = \frac{-1 \mp \sqrt{(-1)^{\frac{p-1}{2}} p}}{2}.$$

Das Vorzeichen der Wurzel hängt von der Wahl der Wurzel $\varrho$ ab und lässt sich bestimmen, kommt aber hier nicht in Betracht. Wir haben daher den Satz:

Die Gruppe der Transformationsgleichung ist $\mathfrak{L}_0$, wenn $\sqrt{(-1)^{\frac{p-1}{2}} p}$ dem Rationalitätsbereich adjungirt wird.

## §. 81. Untersuchung der Gruppe $\mathfrak{L}_0$[2]).

Die in $\mathfrak{L}_0$ enthaltenen Substitutionen

$$(1) \qquad \begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix} = \left(z, \frac{-c + az}{\partial - bz}\right),$$

in welchen

---

[1] Vgl. Gauss, Disq. arithm. art. 356, oder „Summatio serierum quarundam singularium", Werke Bd. II. Dirichlet-Dedekind, Zahlentheorie, Supplement I. Bachmann, Die Lehre von der Kreistheilung, XV. Vorlesung.

[2] Ueber die Gruppe der linearen Substitutionen $\mathfrak{L}_0$ ist zu vergleichen: Galois, Liouville's Journal, Bd. XI. Serret, Algèbre supérieure, Section IV, Chapitre IV. C. Jordan, Traité des Substitutions. Gierster, Gruppe der Modulargleichungen. Mathematische Annalen, Bd. 18.

(2) $$\Delta = a\partial - bc$$

quadratischer Rest von $p$ ist, können, wie schon oben bemerkt, auf die Form gebracht werden

(3) $$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} = \left(z, \frac{-\gamma + \alpha z}{\delta - \beta z}\right),$$

worin

(4) $$\alpha\delta - \beta\gamma \equiv 1 \pmod{p},$$

wir haben nur, wenn wir unter $\sqrt{\Delta} \pmod{p}$ eine ganze Zahl verstehen, deren Quadrat nach dem Modul $p$ congruent mit $\Delta$ ist

$$\begin{aligned} a &\equiv \alpha\sqrt{\Delta}, & b &\equiv \beta\sqrt{\Delta}\\ c &\equiv \gamma\sqrt{\Delta}, & \partial &\equiv \delta\sqrt{\Delta}\end{aligned} \pmod{p}$$

zu setzen. In der Form (3) können noch die Vorzeichen von $\alpha$, $\beta$, $\gamma$, $\delta$ gleichzeitig geändert werden.

Wir fragen nach denjenigen Elementen $z$, welche durch eine Substitution von der Form (3) ungeändert bleiben. Diese werden bestimmt durch die Congruenz

$$z \equiv \frac{\gamma + \delta z}{\alpha + \beta z} \pmod{p},$$

oder

(5) $$\beta z^2 + (\alpha - \delta)z - \gamma \equiv 0 \pmod{p},$$

eine Congruenz, die, wenn sie nicht identisch ist, höchstens zwei incongruente Wurzeln hat. Um diese zu erhalten, schreiben wir, zunächst unter der Voraussetzung, dass $\beta$ nicht durch $p$ theilbar ist, die Congruenz (5) so:

$$\left(\beta z + \frac{\alpha - \delta}{2}\right)^2 \equiv \left(\frac{\alpha - \delta}{2}\right)^2 + \beta\gamma \pmod{p},$$

oder mit Hülfe von (4):

(6) $$\left(\beta z + \frac{\alpha - \delta}{2}\right)^2 \equiv \left(\frac{\alpha + \delta}{2}\right)^2 - 1 \pmod{p}.$$

Demnach sind drei verschiedene Fälle zu unterscheiden:

I. $$\left(\frac{\alpha + \delta}{2}\right)^2 - 1 \equiv 0 \pmod{p};$$

dann hat die Congruenz (5) eine Wurzel; es giebt ein und nur ein Element $z$, welches ungeändert bleibt.

II. $\left(\frac{\alpha+\delta}{2}\right)^2 - 1$ quadratischer Rest von $p$;

die Congruenz (5) hat zwei verschiedene Wurzeln, es giebt zwei Elemente $z$, welche ungeändert bleiben.

III. $\left(\frac{\alpha+\delta}{2}\right)^2 - 1$ quadratischer Nichtrest von $p$;

die Congruenz (5) hat gar keine Wurzel und alle Elemente $z$ werden umgesetzt.

Ist $\beta \equiv 0$, so hat (5) immer die eine Wurzel $z = \infty$; ist dann $\delta \equiv \alpha$ und $\gamma$ nicht $\equiv 0 \pmod{p}$, so giebt es nur diese eine; in diesem Falle ist aber

$$\alpha\delta \equiv 1, \quad \alpha \equiv \delta, \quad \left(\frac{\alpha+\delta}{2}\right)^2 \equiv 1 \pmod{p},$$

und die Bedingung I erfüllt. Ist aber gleichzeitig $\gamma \equiv 0 \pmod{p}$, so ist die Substitution die identische.

Ist $\beta \equiv 0$, aber $\alpha - \delta$ nicht $\equiv 0 \pmod{p}$, so hat (5) noch eine zweite Wurzel; da jetzt $\alpha\delta \equiv 1 \pmod{p}$, so ist:

$$\left(\frac{\alpha+\delta}{2}\right)^2 - 1 \equiv \left(\frac{\alpha-\delta}{2}\right)^2 \pmod{p},$$

also quadratischer Rest, und die Bedingung II erfüllt. Wir fassen diese Sätze so zusammen:

Im Falle I bleibt ein Element oder alle Elemente ungeändert, im Falle II bleiben zwei Elemente ungeändert und im Falle III werden alle Elemente geändert.

Wenn wir eine und dieselbe Substitution

$$A = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \tag{7}$$

mehrmals wiederholen, so entstehen die Substitutionen

$$A, A^2, A^3 \ldots,$$

in deren Reihe einmal die identische Substitution $\begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix}$ auftreten muss. Ist $n$ die kleinste positive Zahl, für welche

$$A^n = 1$$

ist, so heisst $n$ der Grad von $A$ (§. 53, 5.).

Setzen wir für ein beliebiges $m$

$$A^m = \begin{pmatrix} \alpha_m, & \beta_m \\ \gamma_m, & \delta_m \end{pmatrix},$$

so erhalten wir zur Berechnung der Zahlen $\alpha_m, \beta_m, \gamma_m, \delta_m$ folgendes System recurrenter Formeln:

$$
(8)\qquad \begin{aligned} \alpha_{m+1} &= \alpha\alpha_m + \beta\gamma_m, & \beta_{m+1} &= \alpha\beta_m + \beta\delta_m, \\ \gamma_{m+1} &= \gamma\alpha_m + \delta\gamma_m, & \delta_{m+1} &= \gamma\beta_m + \delta\delta_m. \end{aligned}
$$

Besonders einfach lassen sich hieraus die Zahlen $\alpha_m, \beta_m, \gamma_m, \delta_m$ im Falle I berechnen.

In diesem Falle können wir, da die Vorzeichen von $\alpha$, $\beta$, $\gamma$, $\delta$ alle gleichzeitig umgekehrt werden dürfen, annehmen

$$
\alpha + \delta \equiv 2, \quad \alpha\delta - \beta\gamma \equiv 1 \pmod{p},
$$

und so erhalten wir aus (8):

$$
\left.\begin{aligned} \alpha_2 &\equiv -1 + 2\alpha, & \beta_2 &\equiv 2\beta \\ \delta_2 &\equiv -1 + 2\delta, & \gamma_2 &\equiv 2\gamma \\ \alpha_3 &\equiv -2 + 3\alpha, & \beta_3 &\equiv 3\beta \\ \delta_3 &\equiv -2 + 3\delta, & \gamma_3 &\equiv 3\gamma \end{aligned}\right\} \pmod{p},
$$

woraus durch den Schluss von $m$ auf $m + 1$ gefolgert wird

$$
(9)\qquad \begin{aligned} \alpha_m &\equiv -(m-1) + m\alpha, & \beta_m &\equiv m\beta \\ \delta_m &\equiv -(m-1) + m\delta, & \gamma_m &\equiv m\gamma \end{aligned} \pmod{p}.
$$

Hieraus ersieht man, dass die sämmtlichen $A^m$ wieder zum Falle I gehören, und dass $p$ der Grad von $A$ ist.

Die analoge Betrachtung der beiden anderen Fälle ist von Serret durchgeführt, erscheint aber für unseren Zweck entbehrlich.

Dagegen wollen wir hier noch den Satz hinzufügen, dass die ganze Gruppe $\mathfrak{L}_0$ sich zusammensetzen lässt aus den beiden folgenden speciellen Substitutionen

$$
(10)\qquad A = \begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}.
$$

Der Beweis ergiebt sich aus §. 25, wenn man beachtet, dass zu jedem der Bedingung $\alpha\delta - \beta\gamma \equiv 1 \pmod{p}$ genügenden Zahlensystem $\alpha, \beta, \gamma, \delta$, sich das Zahlensystem $\alpha', \beta', \gamma', \delta'$ so wählen lässt, dass

$$
\begin{pmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{pmatrix} \equiv \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \pmod{p} \text{ und } \alpha'\delta' - \beta'\gamma' = 1
$$

wird. Es sind also alle Substitutionen von $\mathfrak{L}_0$ unter den in §. 25 betrachteten enthalten. Wir können hier aber auch leicht die Zusammensetzung einer beliebigen Substitution in $\mathfrak{L}_0$ aus $A$

und $B$ wirklich darstellen, und so unabhängig von §. 25 den Beweis führen.

Denn wenn zunächst $c$ eine beliebige, durch $p$ nicht theilbare Zahl ist, so ergiebt sich durch wirkliche Ausrechnung leicht

$$(11)\quad A^c = \begin{pmatrix} 1, & 0 \\ c, & 1 \end{pmatrix}, \quad C = \begin{pmatrix} c, & 0 \\ 0, & c^{-1} \end{pmatrix} = A^{-c^{-1}} B A^{-c} B A^{-c^{-1}} B,$$

und sodann, wenn $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ eine beliebige Substitution in $\mathfrak{L}_0$ und $\beta$ von 0 verschieden ist:

$$(12)\quad \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} = \begin{pmatrix} 1, & 0 \\ \delta\beta^{-1}, & 1 \end{pmatrix} \begin{pmatrix} \beta, & 0 \\ 0, & \beta^{-1} \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} \begin{pmatrix} 1, & 0 \\ \alpha\beta^{-1}, & 1 \end{pmatrix},$$

und wenn $\beta = 0$ ist:

$$(13)\quad \begin{pmatrix} \alpha, & 0 \\ \gamma, & \alpha^{-1} \end{pmatrix} = \begin{pmatrix} \alpha, & 0 \\ 0, & \alpha^{-1} \end{pmatrix} \begin{pmatrix} 1, & 0 \\ \gamma\alpha, & 1 \end{pmatrix}.$$

Es ist aus diesem Satz zu schliessen, dass, wenn eine in $\mathfrak{L}_0$ enthaltene Gruppe die zwei Substitutionen $A$, $B$ enthält, sie nothwendig mit $\mathfrak{L}_0$ identisch sein muss.

## §. 82. Eigentliche Divisoren der Gruppe $\mathfrak{L}_0$.

Nach den Sätzen des §. 57 ist es, um die etwa möglichen Reductionen der Transformationsgleichung kennen zu lernen, vor Allem erforderlich, die Divisoren der Gruppe $\mathfrak{L}_0$ zu untersuchen. Wir fragen zuerst nach der Existenz eines eigentlichen Divisors $\mathfrak{K}$ von $\mathfrak{L}_0$.

Ist

$$(1)\quad S = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$$

irgend eine von der identischen Substitution verschiedene Substitution in $\mathfrak{K}$, so ist, nach dem Wesen des eigentlichen Divisors, jede Substitution

$$(2)\quad U = T S T^{-1}$$

gleichfalls in $\mathfrak{K}$ enthalten, wenn

$$(3)\quad T = \begin{pmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{pmatrix}.$$

eine beliebige Substitution in $\mathfrak{L}_0$ ist.

Wir stellen uns die Aufgabe, $T$ und $\xi$ so zu bestimmen, dass

$$U = \begin{pmatrix} 0, & 1 \\ -1, & \xi \end{pmatrix} \tag{4}$$

wird. Diese Bedingung kann auch so geschrieben werden:

$$\begin{pmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{pmatrix} \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} = \begin{pmatrix} 0, & 1 \\ -1, & \xi \end{pmatrix} \begin{pmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{pmatrix},$$

und führt zu den Congruenzen:

$$\left.\begin{array}{ll} 1. & \alpha'\alpha + \beta'\gamma \equiv \gamma' \\ 2. & \alpha'\beta + \beta'\delta \equiv \delta' \\ 3. & \gamma'\alpha + \delta'\gamma \equiv -\alpha' + \gamma'\xi \\ 4. & \gamma'\beta + \delta'\delta \equiv -\beta' + \delta'\xi \end{array}\right\} \pmod{p}, \tag{5}$$

und aus 1. und 2. folgt noch

$$\left.\begin{array}{ll} 5. & \alpha' \equiv \gamma'\delta - \delta'\gamma \\ 6. & \beta' \equiv -\gamma'\beta + \delta'\alpha \end{array}\right\} \pmod{p}. \tag{6}$$

Setzt man diese Werthe in (5) 3. und 4. ein, so folgt:

$$\left.\begin{array}{l} \gamma'(\alpha + \delta - \xi) \equiv 0 \\ \delta'(\alpha + \delta - \xi) \equiv 0 \end{array}\right\} \pmod{p},$$

woraus, da $\gamma'$, $\delta'$ nicht beide durch $p$ theilbar sein können, folgt:

$$\xi \equiv \alpha + \delta \pmod{p}; \tag{7}$$

ist $\xi$ so bestimmt, so folgen in (5) die Congruenzen 3., 4. aus 1., 2. Setzt man aber $\gamma'$, $\delta'$ aus 1., 2. in

$$\alpha'\delta' - \beta'\gamma' \equiv 1 \pmod{p} \tag{8}$$

ein, so erhält man

$$\alpha'^2\beta + \alpha'\beta'(\delta - \alpha) - \beta'^2\gamma \equiv 1 \pmod{p}. \tag{9}$$

Ist hieraus $\alpha'$, $\beta'$ bestimmt, so sind alle in (5), und also auch in (2), (4) ausgesprochenen Forderungen befriedigt.

Es handelt sich also noch darum, nachzuweisen, dass die Congruenz (9) immer lösbar ist.

Diese Möglichkeit ist evident, wenn $\beta$ oder $-\gamma$ quadratischer Rest von $p$ ist; denn dann genügt

$$\left.\begin{array}{lll} & \alpha' \equiv \sqrt{\beta^{-1}}, & \beta' \equiv 0 \\ \text{oder} & \alpha' \equiv 0, & \beta' \equiv \sqrt{-\gamma^{-1}} \end{array}\right\} \pmod{p}$$

der gestellten Forderung.

Im Weiteren ist nun zu unterscheiden, ob die Substitution $S$ zur Classe I, II, III des vorigen Paragraphen gehört.

Ist zunächst

I. $$\left(\frac{\alpha+\delta}{2}\right)^2 \equiv 1 \pmod{p},$$

so geht, wenn wir $S^m$ an Stelle von $S$ setzen, $\beta$ in $m\beta$, $\gamma$ in $m\gamma$ über, und es lässt sich $m$ immer so bestimmen, dass $m\beta$ oder $-m\gamma$ quadratischer Rest von $p$ wird.

Hierher gehört auch der Fall, dass $\beta \equiv 0$ oder $\gamma \equiv 0$ und $\alpha \equiv \delta \pmod{p}$ ist.

Ist dagegen $\beta \equiv 0$ und $\alpha - \delta$ nicht durch $p$ theilbar, so kann man in (9) $\beta'$ beliebig wählen und dann $\alpha'$ aus einer Congruenz ersten Grades bestimmen.

Ist $\beta$ nicht durch $p$ theilbar, so setze man (9) in die Form

$$(10)\quad \left[\alpha'\beta + \beta'\left(\frac{\delta-\alpha}{2}\right)\right]^2 \equiv \beta + \beta'^2\left[\left(\frac{\alpha+\delta}{2}\right)^2 - 1\right] \pmod{p},$$

und wenn nun

II. $\left(\frac{\alpha+\delta}{2}\right)^2 - 1$ quadratischer Rest von $p$ ist, so bestimme man $\beta'$ aus der Congruenz:

$$\beta'^2\left[\left(\frac{\alpha+\delta}{2}\right)^2 - 1\right] \equiv \left(\frac{\beta-1}{2}\right)^2,$$

wodurch (10) übergeht in

$$\alpha'\beta + \beta'\left(\frac{\delta-\alpha}{2}\right) \equiv \pm\frac{\beta+1}{2} \pmod{p},$$

und woraus $\alpha'$ bestimmt werden kann, welches Zeichen auch gewählt wird.

Ist

III. $\left(\frac{\alpha+\delta}{2}\right)^2 - 1$ quadratischer Nichtrest von $p$ und zugleich $\beta$ quadratischer Nichtrest, so lässt sich immer ein Nichtrest $\nu$ so bestimmen, dass $\beta + \nu$ quadratischer Rest wird; denn lässt man $\nu$ in $\beta + \nu$ die Reihe der Nichtreste durchlaufen, so können nicht lauter Nichtreste entstehen, weil unter diesen auch $\beta$ sein müsste.

Dann kann man $\beta'$ so bestimmen, dass

$$\beta'^2\left[\left(\frac{\alpha+\delta}{2}\right)^2 - 1\right] \equiv \nu \pmod{p},$$

und dann $\alpha'$ aus

$$\alpha'\beta + \beta'\left(\frac{\delta-\alpha}{2}\right) \equiv \pm\sqrt{\beta+\nu} \pmod{p}.$$

Hieraus folgt:

In einem eigentlichen Divisor $\mathfrak{K}$ der Gruppe $\mathfrak{L}_0$ muss gewiss eine Substitution $U$ von der Form

$$(11)\qquad \begin{pmatrix} 0, & 1 \\ -1, & \xi \end{pmatrix}$$

vorkommen.

Es sei zunächst $\xi$ von Null verschieden (mod $p$).

Nach dem Begriff des eigentlichen Divisors enthält $\mathfrak{K}$ auch die Substitution

$$(12)\qquad \begin{pmatrix} 0, & -1 \\ 1, & 0 \end{pmatrix}\begin{pmatrix} 0, & 1 \\ -1, & \xi \end{pmatrix}\begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} = \begin{pmatrix} \xi, & 1 \\ -1, & 0 \end{pmatrix}$$

und folglich auch

$$(13)\qquad \begin{pmatrix} 0, & 1 \\ -1, & \xi \end{pmatrix}\begin{pmatrix} \xi, & 1 \\ -1, & 0 \end{pmatrix} = \begin{pmatrix} 1, & 0 \\ 2\xi, & 1 \end{pmatrix} \equiv A^{2\xi} \text{ [§. 81, (10)]},$$

also auch $A$ und alle seine Potenzen. Daher enthält $\mathfrak{K}$ auch

$$(14)\qquad \begin{pmatrix} 1, & 0 \\ \eta, & 1 \end{pmatrix}\begin{pmatrix} 0, & 1 \\ -1, & \xi \end{pmatrix} = \begin{pmatrix} 0, & 1, \\ -1, & \xi + \eta \end{pmatrix}$$

für ein beliebiges $\eta$, d. h. die Substitution (11) für jedes beliebige $\xi$ und mithin auch

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

Demnach ist nach dem Satze des vorigen Paragraphen die Gruppe $\mathfrak{K}$ mit $\mathfrak{L}_0$ identisch.

Es bleibt noch die Möglichkeit zu erörtern, dass in (11) $\xi \equiv 0$ ist.

In diesem Falle enthält die Gruppe $\mathfrak{K}$ also die Substitution

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

und folglich auch, für ein beliebiges, durch $p$ nicht theilbares $\alpha$

$$V = \begin{pmatrix} 0, & \alpha \\ -\alpha^{-1}, & 0 \end{pmatrix}\begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}\begin{pmatrix} 0, & -\alpha \\ \alpha^{-1}, & 0 \end{pmatrix}\begin{pmatrix} 0, & -1 \\ 1, & 0 \end{pmatrix} = \begin{pmatrix} \alpha^2, & 0 \\ 0, & \alpha^{-2} \end{pmatrix}.$$

Daraus leitet man als in $\mathfrak{K}$ enthalten noch weiter ab:

$$W = \begin{pmatrix} 1, & 0 \\ -1, & 1 \end{pmatrix}\begin{pmatrix} \alpha^{-2}, & 0 \\ 0, & \alpha^2 \end{pmatrix}\begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix}\begin{pmatrix} \alpha^2, & 0 \\ 0, & \alpha^{-2} \end{pmatrix} = \begin{pmatrix} 1, & 0 \\ \alpha^4 - 1, & 1 \end{pmatrix}.$$

Wenn nun $p$ grösser ist als 5, so kann man $\alpha$ so annehmen, dass $\alpha^4 - 1$ nicht durch $p$ theilbar ist; dann enthält also $\mathfrak{K}$ auch die Substitution $A$ und ihre Potenzen und mithin ist $\mathfrak{K}$ mit $\mathfrak{L}_0$ identisch.

Ist $p = 5$, so ist $\alpha^4 - 1$ immer durch $p$ theilbar, also dieser Schluss nicht anwendbar.

In diesem Falle folgt aber aus dem Begriff des eigentlichen Divisors als in $\mathfrak{K}$ enthalten:

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

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

d. h. $A^2$ und mithin alle Potenzen von $A$, woraus wie oben zu schliessen, dass $\mathfrak{K}$ mit $\mathfrak{L}_0$ identisch ist. Wir haben also den Satz:

Ist $p > 3$, so hat die Gruppe $\mathfrak{L}_0$ keinen eigentlichen Theiler.

Im Falle $p = 3$ enthält $\mathfrak{K}$ gleichfalls

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

also auch

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

und es bilden auch in der That die vier Substitutionen

$$(16) \qquad \begin{pmatrix}1, & 0\\ 0, & 1\end{pmatrix}, \quad \begin{pmatrix}0, & 1\\ -1, & 0\end{pmatrix}, \quad \begin{pmatrix}-1, & 1\\ 1, & 1\end{pmatrix}, \quad \begin{pmatrix}1, & 1\\ 1, & -1\end{pmatrix}$$

einen eigentlichen Divisor von $\mathfrak{L}_0$ vom Index 3.

Im Falle $p = 3$ ist die Gruppe $\mathfrak{L}_0$ identisch mit der sogenannten alternirenden Gruppe der Vertauschungen von vier Elementen, d. h. mit der Gruppe derjenigen Vertauschungen, welche das Differenzenproduct der vier Elemente ungeändert lässt. Es ist dies die Gruppe einer beliebigen Gleichung vierten Grades, wenn die Quadratwurzel aus der Discriminante dem Rationalitätsbereich adjungirt wird. Der Divisor (16) dieser Gruppe vom Index 3 liefert dann die in der Algebra bekannte cubische Resolvente der biquadratischen Gleichung.

Eine zur Gruppe (16) gehörige Function der Wurzeln $v_\infty$, $v_0$, $v_1$, $v_2$ der Transformationsgleichung für den vierten Transformationsgrad ist z. B.

$$v_\infty v_0 + v_1 v_2$$

oder

$$(v_\infty - v_0)(v_1 - v_2).$$

Der Unterschied zwischen diesen beiden Functionen ist der, dass die erstere durch die Substitution der Determinante — 1

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

ungeändert bleibt, während die zweite dabei ihr Zeichen ändert. Die erstere wird daher zu einer Gleichung dritten Grades mit rationalen Coëfficienten führen, während in der cubischen Gleichung für die zweite noch $\sqrt{-3}$ auftritt (§. 80).

## §. 83. Uneigentliche Divisoren von $\mathfrak{L}_0$.

Wir fragen nun, indem wir den Fall $p = 3$ bei Seite lassen, nach den uneigentlichen Divisoren der Gruppe $\mathfrak{L}_0$, deren Index kleiner als $p + 1$ ist; von der Existenz solcher Divisoren hängt die Möglichkeit der Bildung von Resolventen der Transformationsgleichung ab, deren Grad niedriger ist als $p + 1$.

Zunächst lässt sich zeigen, dass der Index eines Divisors $\mathfrak{K}$ von $\mathfrak{L}_0$ niemals kleiner als $p$ sein kann.

Es sei

(1) $$\mathfrak{K} = S_0, S_1, \ldots S_{\nu-1}$$

irgend ein Divisor von $\mathfrak{L}_0$ vom Grade $\nu$, und, wenn es möglich ist

(2) $$T = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$$

eine Substitution $p$ten Grades, welche in $\mathfrak{L}_0$, aber nicht in $\mathfrak{K}$ vorkommt. Es kann dann auch, da $p$ Primzahl ist, keine niedrigere Potenz von $T$ als die $p$te in $\mathfrak{K}$ vorkommen. Die Reihen

(3) $$\mathfrak{K},\quad T\mathfrak{K},\quad T^2\mathfrak{K} \ldots,\quad T^{p-1}\mathfrak{K}$$

enthalten lauter von einander verschiedene Elemente $T^i S_k$, und demnach ist

$$\nu p \overline{\gtrless} p\,\frac{p^2 - 1}{2},$$

also der Index von $\mathfrak{K}$, d. h. der Quotient

$$p\,\frac{p^2 - 1}{2} : \nu$$

gleich oder grösser als $p$.

Ein Divisor $\mathfrak{K}$ von $\mathfrak{L}_0$, dessen Index kleiner als $p$ ist, muss daher sämmtliche Substitutionen $p$ten Grades enthalten, also auch (§. 81) alle Substitutionen $T$, in welchen

$$(4) \qquad \alpha + \delta \equiv 2 \pmod{p}$$

ist.

Demnach enthält eine solche Gruppe $\mathfrak{K}$ zunächst die Substitution

$$(5) \qquad A = \begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix}$$

und ihre Potenzen; ebenso die Substitutionen

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

und folglich auch

$$(6) \qquad B = \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} = \begin{pmatrix} 1, & 2 \\ 0, & 1 \end{pmatrix} \begin{pmatrix} 2, & 1 \\ -1, & 0 \end{pmatrix}.$$

Wenn aber die Substitutionen $A$, $B$ in $\mathfrak{K}$ enthalten sind, so muss $\mathfrak{K}$ nach §. 81 mit $\mathfrak{L}_0$ identisch sein. Wir haben also den Satz:

Der Index eines Divisors von $\mathfrak{L}_0$ kann nicht kleiner als $p$ sein.

Unser Problem beschränkt sich also auf die Frage nach den Divisoren von $\mathfrak{L}_0$ vom Index $p$ oder vom Grade $\frac{p^2-1}{2}$.

Es sei $\mathfrak{K}$ ein solcher Divisor und $S_0$, $S_1, \ldots S_{\nu-1}$ seien seine Elemente, so dass die Zahl $\nu$ den Werth

$$(7) \qquad \nu = \frac{p^2-1}{2}$$

hat.

Da der Grad eines jeden Elementes einer Gruppe immer ein Theiler vom Grade der Gruppe ist, so kann, da $\nu$ durch $p$ nicht theilbar ist, in $\mathfrak{K}$ kein Element vom Grade $p$ vorkommen, nehmen wir also für $T$ die Substitution vom Grade $p$:

$$(8) \qquad A = \begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix},$$

so lässt sich die Gruppe $\mathfrak{L}_0$ in die $p$ Reihen zerlegen:

$$(9) \qquad \mathfrak{L}_0 = \mathfrak{K}, \quad A\mathfrak{K}, \quad A^2\mathfrak{K} \ldots, \quad A^{p-1}\mathfrak{K}.$$

Mit $\mathfrak{K}$ sind von demselben Grade, also auch von demselben Index alle seine conjugirten Divisoren

$$T\mathfrak{K}T^{-1}.$$

Es sei nun $g$ eine primitive Wurzel der Primzahl $p$, und

$$C = \begin{pmatrix} g, & 0 \\ 0, & g^{-1} \end{pmatrix}, \tag{10}$$

eine Substitution, welche offenbar vom Grade $\frac{p-1}{2}$ ist. Diese muss, wie jede Substitution von $\mathfrak{L}_0$, in einer der Reihen (9) vorkommen; d. h. es giebt eine Substitution $S$ in $\mathfrak{K}$ und einen Exponenten $\lambda$, so dass

$$C = A^{\lambda} S, \quad S = A^{-\lambda} C. \tag{11}$$

Es lässt sich aber $\gamma$ weiter so bestimmen, dass

$$A^{\gamma-\lambda} C A^{-\gamma} = C, \tag{12}$$

man erhält dafür die Bedingung

$$\gamma (g - g^{-1}) \equiv \lambda g \pmod{p},$$

welche, da $p > 3$ ist, immer befriedigt werden kann; danach ist aber wegen (11)

$$C = A^{\gamma} S A^{-\gamma}.$$

Es kommt also $C$ in dem mit $\mathfrak{K}$ conjugirten Divisor $A^{\gamma} \mathfrak{K} A^{-\gamma}$ vor, und wir können also, indem diese Gruppe an Stelle von $\mathfrak{K}$ gesetzt wird, unbeschadet der Allgemeinheit annehmen, $\mathfrak{K}$ enthalte selbst die Substitution $C$.

Es kann nun in $\mathfrak{K}$ die Substitution

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

entweder vorkommen oder nicht vorkommen. Im ersten Fall enthält $\mathfrak{K}$ auch alle aus $B$ und $C$ zusammengesetzten Substitutionen, die sämmtlich von einer der beiden Formen sind

$$(13)\ \begin{pmatrix} g^r, & 0 \\ 0, & g^{-r} \end{pmatrix}, \qquad (14)\ \begin{pmatrix} 0, & g^{-r} \\ -g^r, & 0 \end{pmatrix}, \quad r = 0, 1, \ldots \frac{p-3}{2},$$

und deren Anzahl $p - 1$ beträgt. Im ersten Fall enthält also $\mathfrak{K}$ alle Substitutionen von der Form (13), (14), im zweiten alle Substitutionen der Form (13) und keine der Form (14).

Es sei nun

$$V = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \tag{15}$$

eine in $\mathfrak{K}$ enthaltene Substitution, die weder in der Form (13), noch in der Form (14) enthalten ist, bei der also weder $\alpha$ und $\delta$

noch $\beta$ und $\gamma$ zugleich congruent mit 0 sind. Dann sind die sämmtlichen Substitutionen der Form

$$(16)\qquad C^r V C^s = \begin{pmatrix} \alpha g^{r+s}, & \beta g^{r-s} \\ \gamma g^{-r+s}, & \delta g^{-r-s} \end{pmatrix},$$

wenn $r$, $s$ beide die Reihe der Zahlen durchlaufen

$$0, 1, 2, \ldots \frac{p-3}{2}$$

in $\mathfrak{K}$ enthalten und alle von einander verschieden. Denn sind zwei unter den Substitutionen (16) einander gleich, so muss es auch eine unter ihnen geben, welche, ohne dass $r$, $s$ verschwinden, mit $V$ identisch wird. Dies verlangt aber

$$\begin{matrix} \alpha \equiv \pm\, \alpha g^{r+s}, & \beta \equiv \pm\, \beta g^{r-s} \\ \gamma \equiv \pm\, \gamma g^{-r+s}, & \delta \equiv \pm\, \delta g^{-r-s} \end{matrix} \quad (\mathrm{mod}\ p),$$

wo in allen vier Formeln die oberen oder die unteren Zeichen gelten, also, da weder $\alpha$ und $\delta$, noch $\beta$ und $\gamma$ gleichzeitig verschwinden,

$$r + s \equiv 0, \qquad r - s \equiv 0, \qquad (\mathrm{mod}\ p-1),$$

oder $$r + s \equiv \frac{p-1}{2}, \qquad r - s \equiv \frac{p-1}{2}, \qquad (\mathrm{mod}\ p-1),$$

also in beiden Fällen

$$r \equiv 0, \quad s \equiv 0 \left(\mathrm{mod}\ \frac{p-1}{2}\right),$$ w. z. b. w.

In der Form (16) sind also $\left(\frac{p-1}{2}\right)^2$ verschiedene Substitutionen enthalten. Ist damit die Gruppe $\mathfrak{K}$ noch nicht erschöpft, so wähle man eine nicht in (13), (14), (16) enthaltene Substitution $V'$ und bilde in gleicher Weise die Reihe

$$(17)\qquad C^r V' C^s,$$

welche nur Substitutionen enthält, welche sowohl unter sich als auch von den in (13), (14), (16) enthaltenen verschieden sind, und fahre auf diese Weise fort, bis die ganze Gruppe $\mathfrak{K}$ erschöpft ist.

Bezeichnen wir die Anzahl der auf diese Weise gebildeten Reihen (16), (17) ... mit $q$, so ergiebt sich also der Grad der Gruppe $\mathfrak{K}$:

1. wenn $B$ in $\mathfrak{K}$ nicht vorkommt:

$$= \frac{p-1}{2} + q\left(\frac{p-1}{2}\right)^2;$$

2. wenn $B$ in $\mathfrak{K}$ vorkommt:

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

und diese Zahl soll also nach der Forderung unserer Aufgabe

$$= \frac{(p-1)(p+1)}{2}$$

sein. Hieraus aber ergiebt sich, dass der Fall 1. unmöglich ist, denn es müsste in diesem Falle

$$q\left(\frac{p-1}{2}\right) = p,$$

also

$$q = p, \quad p = 3$$

sein, was wir ausgeschlossen haben.

Im Falle 2. aber folgt für jedes beliebige $p$:

$$q = 2.$$

Daher muss in $\mathfrak{K}$ jedenfalls die Substitution $B$ vorkommen, und die gesuchte Gruppe ist durch (13), (14), (16), (17) erschöpft.

Wir zeigen zunächst, dass in den beiden Substitutionen $V$, $V'$ der Gruppe $\mathfrak{K}$ keine der Zahlen $\alpha, \beta, \gamma, \delta, \alpha', \beta', \gamma', \delta'$ congruent 0 sein kann.

Es kommt nämlich, wie wir schon gesehen haben, in $\mathfrak{K}$ nicht vor

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

wenn $\gamma$ von 0 verschieden ist, also auch nicht

$$\begin{pmatrix} \alpha, & 0 \\ 0, & \alpha^{-1} \end{pmatrix} \begin{pmatrix} 1, & 0 \\ \alpha\gamma, & 1 \end{pmatrix} = \begin{pmatrix} \alpha, & 0 \\ \gamma, & \alpha^{-1} \end{pmatrix},$$

wenn $\alpha$ beliebig ist; und folglich auch nicht

$$\begin{pmatrix} \alpha, & 0 \\ \gamma, & \alpha^{-1} \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} = \begin{pmatrix} 0, & \alpha \\ -\alpha^{-1}, & \gamma \end{pmatrix}$$

$$\begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} \begin{pmatrix} \alpha, & 0 \\ \gamma, & \alpha^{-1} \end{pmatrix} = \begin{pmatrix} \gamma, & \alpha^{-1} \\ -\alpha, & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0, & -1 \\ 1, & 0 \end{pmatrix} \begin{pmatrix} 0, & \alpha \\ -\alpha^{-1}, & -\gamma \end{pmatrix} = \begin{pmatrix} \alpha^{-1}, & \gamma \\ 0, & \alpha \end{pmatrix},$$

worin alle Substitutionen $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ enthalten sind, in welchen eine der vier Zahlen $\alpha, \beta, \gamma, \delta$ congruent mit 0 ist.

Die Substitutionen des Systems (16) bezeichnen wir jetzt mit

$$W = \begin{pmatrix} \alpha g^{r+s}, & \beta g^{r-s} \\ \gamma g^{-r+s}, & \delta g^{-r-s} \end{pmatrix},$$

und setzen

$$\begin{aligned} &(18) \qquad \xi \equiv \alpha g^{r+s}, \quad \varrho \equiv \alpha^{-1} \beta g^{-2s}, \\ &(19) \qquad \alpha\delta \equiv m, \quad \beta\gamma \equiv m-1, \end{aligned} \qquad \pmod{p}.$$

$m$ ändert sich nicht, wenn $V$ durch eine beliebige Substitution des Systems (16) ersetzt wird. Die Zahl $m'$ soll die entsprechende Bedeutung für das System (17) haben; $\xi$ kann in jedem dieser beiden Systeme jeden der Werthe

$$(20) \qquad 1, 2, \ldots p-1$$

annehmen, und $\varrho$ durchläuft, je nachdem $\alpha^{-1}\beta$ quadratischer Rest oder Nichtrest ist, in einem System die Reihe der Reste oder der Nichtreste. Die Aenderung des Vorzeichens von $\xi$ giebt keine neue Substitution $W$. Hiernach können wir $W$ so darstellen:

$$(21) \qquad W = \begin{pmatrix} \xi, & \xi\varrho \\ \xi^{-1}\varrho^{-1}(m-1), & \xi^{-1} m \end{pmatrix}.$$

Da nun das Quadrat von $W$

$$W^2 = \begin{pmatrix} \xi^2 + m - 1, & (\xi^2 + m)\varrho \\ \xi^{-2}\varrho^{-1}(m-1)(\xi^2+m), & [(m-1)\xi^2 + m^2]\xi^{-2} \end{pmatrix},$$

zu $\mathfrak{K}$ gehören muss, so ist es unter einem der Systeme (13), (14), (16), (17) enthalten, so dass sich folgende vier Möglichkeiten ergeben:

$$(22) \qquad \begin{aligned} &1.\ \ \xi^2 + m \equiv 0 \\ &2.\ \ \xi^2 + m - 1 \equiv 0, \quad (m-1)\xi^2 + m^2 \equiv 0 \\ &3.\ \ (\xi^2 + m - 1)\,[(m-1)\xi^2 + m^2] \equiv m\xi^2 \\ &4.\ \ (\xi^2 + m - 1)\,[(m-1)\xi^2 + m^2] \equiv m'\xi^2 \end{aligned}$$

und jeder der $p-1$ Werthe (20), für $\xi$ gesetzt, muss einem dieser vier Fälle genügen. Wenn eine der Congruenzen (22), 2. erfüllt ist, so muss die andere daraus folgen, was nur möglich ist, wenn

$$(23) \qquad 2m \equiv 1, \quad \xi^2 \equiv m \pmod{p}.$$

Nun hat eine Congruenz in Bezug auf einen Primzahlmodul höchstens so viele incongruente Wurzeln, als der Grad der Congruenz beträgt; 1. und 2. können also höchstens für je zwei, 3. und 4. höchstens für je vier Werthe von $\xi$ befriedigt sein; also giebt es im Ganzen höchstens 12 Werthe von $\xi$, welche einer der vier Congruenzen (22) genügen.

Daraus folgt:

$$p - 1 \leqq 12, \quad p \leqq 13.$$

Ist aber $p = 13$, so muss jede der Congruenzen (22) die Maximalzahl von Wurzeln haben; es muss also auch 2. für zwei Werthe von $\xi$ befriedigt sein; dann müsste nach (23) $m \equiv 7$, $\xi^2 \equiv 7 \pmod{13}$ sein, was unmöglich ist, da 7 quadratischer Nichtrest von 13 ist.

Ein Divisor von $\mathfrak{L}_0$ vom Index $p$ existirt also nicht, wenn $p > 11$ ist.

## §. 84. Divisoren von $\mathfrak{L}_0$ vom Index $p$ für $p = 5, 7, 11$.

Es bleibt die Möglichkeit übrig, dass für $p = 5, 7, 11$ Divisoren von $\mathfrak{L}_0$ vom Index $p$ existiren.

1. $p = 5$. Wir untersuchen zunächst den Fall $p = 5$. Da $m$ und $m - 1$ nicht congruent 0 sein können, so bleiben für $m$ die Annahmen

$$m \equiv 2, 3, 4 \pmod{p}.$$

Ersetzen wir aber die Substitution $W$ §. 83, (21) durch

$$WB = \begin{pmatrix} -\xi\varrho, & \xi \\ -\xi^{-1}m, & \xi^{-1}\varrho^{-1}(m-1) \end{pmatrix}, \tag{24}$$

wodurch $m$ in $1 - m$ übergeht, so kommt der Fall $m \equiv 4$ auf den Fall $m \equiv 2$ zurück.

Für $m \equiv 2$ ist aber (23), §. 83 nicht erfüllt, und von den Congruenzen (22) ist keine möglich, da $\pm 2$ Nichtreste von 5 sind und die linken Seiten von (22), 3., 4. sich für $m = 2$ auf $\xi^4 - 1$ reduciren, was für jedes von Null verschiedene $\xi$ durch 5 theilbar ist. Es bleibt also nur übrig, dass

$$m \equiv 3, \quad m' \equiv 3 \pmod{5} \tag{25}$$

und die beiden Systeme $W$, $W'$, [§. 83, (16), (17)] können sich nur dadurch von einander unterscheiden, dass $\alpha^{-1}\beta$ und also auch $\varrho$ in dem einen quadratischer Rest, in dem anderen quadratischer Nichtrest von 5 ist. Die gesuchte Gruppe besteht also, falls sie existirt, aus den 12 in den drei Formen

$$(26)\qquad \begin{pmatrix}\xi, & 0\\ 0, & \xi^{-1}\end{pmatrix},\quad \begin{pmatrix}0, & \xi\\ -\,\xi^{-1}, & 0\end{pmatrix},\quad \begin{pmatrix}\xi, & \eta\\ 2\,\eta^{-1}, & 3\,\xi^{-1}\end{pmatrix}$$

enthaltenen Substitutionen, worin

$$\xi \equiv 1,\ 2,\quad \eta \equiv \pm 1,\ \pm 2 \pmod{5}$$

zu setzen ist.

2. $p = 7,\ 11$.

Da $-1$ für $p = 7,\ 11$ unter den quadratischen Nichtresten zu finden ist, so gehört die zusammengesetzte Substitution $WB$, (24), zu den $W'$ [weil der quadratische Charakter der in (18), §. 83 mit $\varrho$ bezeichneten Grösse in $W$ und $WB$ der entgegengesetzte ist]. Daraus folgt für diese beiden Fälle:

$$(27)\qquad m + m' \equiv 1 \pmod{p}.$$

Für $p = 7$ bleiben also, da die Vertauschung von $m$ mit $m'$ nichts Neues liefert, die drei folgenden Möglichkeiten:

1. $m \equiv 2,\ m' \equiv 6$. 2. $m \equiv 3,\ m' \equiv 5$. 3. $m \equiv 4,\ m' \equiv 4$.

Im Falle 1. ist von den Congruenzen §. 83, (22), 1. und 2. unmöglich; also müsste für jedes $\xi$ eine der beiden Congruenzen 3., 4. erfüllt sein, welche hier lauten:

$$(\xi^2 + 1)(\xi^2 + 4) \equiv 2\,\xi^2,\ 6\,\xi^2 \pmod{7},$$

deren keine für $\xi \equiv 1$ erfüllt ist.

Im Falle 3. ist (22), 1. nicht erfüllbar und (22), 2. ist für $\xi^2 \equiv 4$ erfüllt; daher muss für $\xi^2 \equiv 1,\ 2$ die Congruenz (22), 3. oder 4.

$$(\xi^2 + 3)(3\,\xi^2 + 2) \equiv 4\,\xi^2 \pmod{7}$$

erfüllt sein, was wieder nicht der Fall ist. Es bleibt also für $p = 7$ allein übrig:

$$(28)\qquad m \equiv 3,\quad m' \equiv 5 \pmod{7}.$$

Für $p = 11$ ist von vornherein die Möglichkeit auszuschliessen, dass die Congruenzen (22), 2. erfüllt seien, weil in diesem Falle in Folge von (23) und (27):

$$m \equiv m'$$

sein müsste; dann wären (22), 3., 4. nicht verschieden und die Congruenzen (22) könnten zusammen höchstens acht Wurzeln haben und nicht zehn, wie es doch sein müsste.

Es müssen also die Congruenzen (22), 1., 3., 4. jede die Maximalzahl von Wurzeln haben, und es muss, damit 1. erfüllt sei, $m$, und aus gleichen Gründen $m'$ quadratischer Nichtrest von

11 sein. Dieser Bedingung und gleichzeitig der Bedingung (27) genügen aber nur die beiden Zahlen

$$m, m' \equiv 2, -1 \pmod{11}. \tag{29}$$

Die gesuchten Gruppen bestehen also in diesen beiden Fällen, falls sie existiren, aus folgenden Substitutionen:

$p = 7$

$$\begin{pmatrix} \xi, & 0 \\ 0, & \xi^{-1} \end{pmatrix}, \begin{pmatrix} 0, & \xi \\ \xi^{-1}, & 0 \end{pmatrix}, \begin{pmatrix} \xi, & \xi\varrho \\ 2\xi^{-1}\varrho^{-1}, & 3\xi^{-1} \end{pmatrix}, \begin{pmatrix} -\xi\varrho, & \xi \\ -3\xi^{-1}, & 2\xi^{-1}\varrho^{-1} \end{pmatrix} \tag{30}$$

$$\xi \equiv 1, 2, 3 \pmod{7},$$

$p = 11$

$$\begin{pmatrix} \xi, & 0 \\ 0, & \xi^{-1} \end{pmatrix}, \begin{pmatrix} 0, & \xi \\ -\xi^{-1}, & 0 \end{pmatrix}, \begin{pmatrix} \xi, & \xi\varrho \\ \xi^{-1}\varrho^{-1}, & 2\xi^{-1} \end{pmatrix}, \begin{pmatrix} -\xi\varrho, & \xi \\ -2\xi^{-1}, & \xi^{-1}\varrho^{-1} \end{pmatrix} \tag{31}$$

$$\xi \equiv 1, 2, 3, 4, 5 \pmod{11};$$

$\varrho$ durchläuft in (30) und (31) entweder die Reihe der quadratischen Reste oder die der Nichtreste, so dass man für $p = 7$ oder 11 je zwei Gruppen vom Index $p$ erhält.

Dass die in (26), (30), (31) zusammengestellten Substitutionssysteme wirklich Gruppen constituiren, lässt sich durch directe Zusammensetzung auf verschiedene Arten nachweisen. Einfacher gelangt man zu diesem Beweise aber dadurch, dass man Functionen der $v_z$, §. 80, bildet, welche durch die Substitutionen dieser Systeme ungeändert bleiben, und durch die Substitutionen von $\mathfrak{L}_0$ überhaupt nur $p$ verschiedene Werthe erhalten.

Die Systeme (26), (30), (31) lassen sich, wie aus ihrer Entstehungsweise hervorgeht, durch wiederholte Anwendung von $B, C, U, U'$ zusammensetzen, wenn $U, U'$ irgend zwei specielle Substitutionen $W, W'$ sind. Für $p = 5$ gehört $U^2$ und für $p = 7, 11$ gehört $UB$ zu den $W'$, so dass $U'$ noch weggelassen werden kann. Wählen wir $U$ irgendwie beliebig, und nehmen für die primitive Wurzel $g$ in $C$ für $p = 5, 7, 11$ bezw. $2, -2, 2$, so können wir (26) zusammensetzen aus:

$$B = \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 2, & 0 \\ 0, & 3 \end{pmatrix}, \quad U = \begin{pmatrix} 1, & 1 \\ 2, & 3 \end{pmatrix} \qquad (p = 5)$$

(30) aus:

$$B = \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 2, & 0 \\ 0, & 4 \end{pmatrix}, \quad U = \begin{pmatrix} 1, & \pm 1 \\ \pm 2, & 3 \end{pmatrix} \qquad (p = 7)$$

(31) aus:

$$B = \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 2, & 0 \\ 0, & 6 \end{pmatrix}, \quad U = \begin{pmatrix} 1, & \pm 1 \\ \pm 1, & 2 \end{pmatrix} \qquad (p = 11),$$

wo in den beiden letzten Fällen aus den doppelten Vorzeichen die oben erwähnten zwei verschiedenen Gruppen entspringen.

Wir stellen nun die diesen Substitutionen entsprechenden Vertauschungen der Indices $z$ zusammen [§. 81, (3)].

$p = 5$:

$$\begin{array}{rcccccl} z = & \infty, & 0, & 1, & 2, & 3, & 4 \\ & 0, & \infty, & 4, & 2, & 3, & 1 \quad (B) \\ & \infty, & 0, & 4, & 3, & 2, & 1 \quad (C) \\ & 4, & 1, & 2, & 0, & \infty, & 3 \quad (U) \end{array}$$

Es werden also durch $B$, $C$, $U$ die Indexpaare

$$(\infty, 0), \quad (1, 4), \quad (2, 3)$$

nicht auseinander gerissen, sondern nur unter einander vertauscht. Ueberdies werden jedesmal in zweien dieser Paare die Elemente vertauscht. Bilden wir daher eine Function wie

$$(32) \qquad V = (v_\infty - v_0)(v_1 - v_4)(v_2 - v_3),$$

so bleibt diese durch $B$, $C$, $U$ und also durch das ganze System (26) ungeändert, während sie durch wiederholte Anwendung der cyklischen Vertauschung (0, 1, 2, 3, 4), d. h. der Substitution

$$A = \begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix}$$

fünf verschiedene Werthe erhält. Aus $A$ und $B$, lässt sich aber [§. 81, (10)] die ganze Gruppe $\mathfrak{L}_0$ zusammensetzen, und $V$ erhält daher durch Anwendung von $\mathfrak{L}_0$ nicht mehr als fünf Werthe.

Die fünf Werthe von $V$ sind die Wurzeln einer Gleichung fünften Grades.

Für $p = 7$ ist

$$B = \left(z, -\frac{1}{z}\right), \quad C = (z, 4z), \quad U = \left(z, \frac{\mp 2 + z}{3 \mp z}\right).$$

Zur besseren Uebersicht stellen wir noch $B$, $C$, $U$ durch die cyklischen Vertauschungen dar, welche durch sie in den acht Werthen von $z$ hervorgerufen werden:

$$A = (0, \infty)(1, -1)(2, 3)(-2, -3),$$
$$C = (1, -3, 2)(-1, 3, -2),$$
$$U = (\infty, \mp 1, \pm 1, \pm 3)(0, \mp 3, \mp 2, \pm 2),$$

und daraus erhält man die siebenwerthige Function

$$(33) \quad V = (v_\infty - v_0)(v_{\mp 1} - v_{\mp 3})(v_{\pm 1} - v_{\mp 2})(v_{\pm 3} - v_{\pm 2}),$$

worin beide Zeichen genommen werden können.

Für $p = 11$ ist

$$B = \left(z, -\frac{1}{z}\right), \quad C = (z, 4z), \quad U = \left(z, \frac{\mp 1 + z}{2 \mp z}\right),$$

oder durch die Cyklen dargestellt:

$$B = (0, \infty)(1, -1)(2, 5)(-2, -5)(3, -4)(-3, 4),$$
$$C = (1, 4, 5, -2, 3)(-1, -4, -5, 2, -3),$$
$$U = (\infty, \mp 1, \pm 3, \mp 2, \pm 2)(0, \pm 5, \mp 5, \mp 4, \pm 1),$$

woraus die beiden 11 werthigen Functionen

$$(34) \qquad V = (v_\infty - v_0)(v_{\mp 1} - v_{\pm 5})(v_{\pm 3} - v_{\mp 5})(v_{\mp 2} - v_{\mp 4})(v_{\pm 2} - v_{\pm 1})(v_{\pm 4} - v_{\mp 3}).$$

Hierbei ist noch folgende Bemerkung von Interesse. Die Resolventen $p$ten Grades, deren Wurzeln die Grössen (32), (33), (34) sind, enthalten nach §. 80 in ihren Coëfficienten noch $\sqrt{\pm p}$.

Die Gruppe $\mathfrak{L}_0$ wird aber zur Gruppe $\mathfrak{L}$ erweitert, wenn wir eine lineare Substitution von der Form §. 80, (13) hinzufügen, in welcher $a\delta - bc$ quadratischer Nichtrest ist, also etwa:

$$\text{für } p = 5 \quad (z, 2z)$$
$$\text{für } p = 7, 11 \quad (z, -z).$$

Durch Anwendung dieser Substitution geht aber der Werth (32)

$$V = (v_\infty - v_0)(v_1 - v_4)(v_2 - v_3)$$

in den entgegengesetzten über, und daraus folgt, dass, wenn $p = 5$ ist, $V^2$ einer Gleichung 5ten Grades mit rationalen Zahlencoëfficienten genügt. Daraus schliesst man, dass in der Gleichung für $V$ die Coëfficienten der ungeraden Potenzen den Factor $\sqrt{5}$ haben, während die anderen rational sind, oder dass man für die Unbekannte $V\sqrt{5}$ eine Gleichung mit rationalen Coëfficienten erhält.

Für $p = 7, 11$ gehen die den beiden Vorzeichen in (33) oder (34) entsprechenden Ausdrücke durch die Vertauschung $(z, -z)$ in einander über. Die Resolventen 7ten oder 11ten Grades, welchen einer der beiden Ausdrücke (33) resp. (34) genügt, gehen also durch Aenderung des Vorzeichens von $\sqrt{-7}$, $\sqrt{-11}$ in einander über.

## §. 85. Verschiedene Resolventen 5ten Grades für den 5ten Transformationsgrad.

Bei der Bildung der Resolventen $p$ten Grades beschränken wir uns hier auf den Fall $p = 5$.

Diesen Resolventen kann man sehr mannigfaltige Formen geben, indem man nicht nur in der Function $V$, (32) des vorigen Paragraphen, für die Grössen $v$ die Wurzeln einer beliebigen Transformationsgleichung wählen, sondern auch $V$ durch mancherlei andere Functionen ersetzen kann, etwa durch

$$(v_\infty + v_0)(v_1 + v_4)(v_2 + v_3),$$

oder durch

$$v_\infty v_0 + v_1 v_4 + v_2 v_3.$$

Wir wollen zunächst die Transformationsgleichung §. 75, (8)

$$v^6 + 10\, v^3 - \gamma_2\, v + 5 = 0 \tag{1}$$

anwenden, worin, wenn

$$c \equiv 0 \pmod{12}, \quad z \equiv c \pmod{5}$$

ist,

$$v_\infty = 5\left(\frac{\eta(5\,\omega)}{\eta\,\omega}\right)^2, \quad v_z = \left(\frac{\eta\left(\dfrac{\omega + c}{5}\right)}{\eta(\omega)}\right)^2 \tag{2}$$

gesetzt werden muss. Nehmen wir dann

$$\begin{aligned} \sqrt{5}\, w_z &= (v_\infty - v_z)(v_{z+1} - v_{z-1})(v_{z-2} - v_{z+2}) \\ &= (v_\infty - v_c)(v_{c+12} - v_{c-12})(v_{c+24} - v_{c-24}), \\ z &= 0, 1, 2, 3, 4, \quad c = 0, \pm 12, \pm 24, \end{aligned} \tag{3}$$

so sind nach der Schlussbemerkung des vorigen Paragraphen die $w_0, w_1, w_2, w_3, w_4$ die Wurzeln einer Gleichung 5ten Grades, deren Coëfficienten rational aus $\gamma_2$ und rationalen Zahlen gebildet sind.

Beachtet man aber die Relationen [§. 49 (14)]:

$$\gamma_2(\omega + 1) = e^{-\frac{2\pi i}{3}}\, \gamma_2(\omega), \quad \gamma_2\left(-\frac{1}{\omega}\right) = \gamma_2(\omega),$$

so folgt aus der Form von (1), dass durch die Vertauschung $(\omega, \omega + 1)$ die Wurzeln $v$, abgesehen von einer Umstellung, den

Factor $e^{\frac{2\pi i}{3}}$ annehmen, während sie durch $\left(\omega, -\frac{1}{\omega}\right)$ ungeändert bleiben. Die $w_z$ vertauschen sich also nur unter einander, und ihre symmetrischen Functionen bleiben ungeändert und hängen daher rational nur von der Invariante $j(\omega)$ ab. Die Coëfficienten in der Gleichung für $w$ können überdies für kein endliches $j(\omega)$ unendlich werden und sind demnach ganze Functionen von $j(\omega)$.

Ein weiterer Aufschluss über diese Coëfficienten ergiebt sich durch die Entwickelung nach steigenden Potenzen von $q$. Die Entwickelungen der $v$ haben nach (2) die Anfänge

$$v_\infty = 5\, q^{\frac{2}{3}} \ldots, \quad v_z = e^{\frac{c}{12}\frac{2\pi i}{5}}\, q^{-\frac{2}{15}} \ldots,$$

und daraus folgt mit Benutzung der bekannten Gleichung

$$4 \sin\frac{2\pi}{5} \cdot \sin\frac{4\pi}{5} = \sqrt{5}$$

der Anfang der Entwickelung für $w_z$:

(4) $$w_z = q^{-\frac{2}{5}}\, e^{\frac{c}{2}\frac{\pi i}{5}} \ldots$$

Hieraus folgt, dass die Potenzsummen der $w_z$ bis zur vierten einschliesslich Constanten sind, da sie nicht einmal die erste Potenz von $j(\omega)$ enthalten können, und dass das Product der $w_z$ eine lineare Function von $j(\omega)$ sein muss, in welcher $j(\omega)$ den Coëfficienten 1 hat.

Die Gleichung der $w$ hat daher die Form:

(5) $$w^5 + b_1\, w^4 + b_2\, w^3 + b_3\, w^2 + b_4\, w + b_5 = j(\omega),$$

wenn die $b$ rationale Zahlen sind. Diese Coëfficienten lassen sich dadurch berechnen, dass man die Entwickelung (4) weiter fortsetzt. Wir schlagen hier einen anderen Weg ein, der streng genommen zu der im nächsten Theil behandelten complexen Multiplication gehört, bei seiner Einfachheit aber trotzdem ganz wohl hier seine Stelle finden kann.

Setzen wir $\omega = i = \sqrt{-1}$, so ist

$$\omega = -\frac{1}{\omega}$$

und in Folge dessen ist [§. 29, (11), (12), (14)]:

$$f_1(i) = f_2(i) = \sqrt[8]{2}, \quad f(i) = \sqrt[4]{2},$$

also [§. 49, (5)]:

(6) $$\gamma_3(i) = 0, \quad \gamma_2(i) = 12, \quad j(i) = 12^3.$$

Man findet aber ferner aus den Transformationsformeln für $\eta(\omega)$, [§. 29, (4), (5)]:

$$\eta(\omega + 1) = e^{\frac{\pi i}{12}}\, \eta(\omega), \quad \eta\left(-\frac{1}{\omega}\right) = \sqrt{-i\omega}\, \eta(\omega),$$

wenn man auf die Zerlegung

$$5 = (2 + i)(2 - i)$$

Rücksicht nimmt:

$$\eta\left(\frac{12 + i}{5}\right) = e^{\frac{\pi i}{6}}\, \eta\left(\frac{2 + i}{5}\right) = e^{\frac{\pi i}{6}}\, \eta\left(\frac{1}{2 - i}\right) = \sqrt{1 + 2i}\, \eta(i),$$

also

$$v_2 = 1 + 2i, \quad v_3 = 1 - 2i,$$

und man kann jetzt, da für $\gamma_2 = 12$ zwei Wurzeln der Gleichung (1) bekannt sind, für diesen besonderen Werth von $\gamma_2$ den linken Theil dieser Gleichung leicht in Factoren zerlegen:

$$v^6 + 10v^3 - 12v + 5 = (v^2 - 2v + 5)(v^2 + v - 1)^2,$$

woraus zu schliessen:

$$(7) \qquad \begin{aligned} v_\infty &= v_0 = \frac{-1 + \sqrt{5}}{2}, \\ v_1 &= v_4 = \frac{-1 - \sqrt{5}}{2}. \end{aligned}$$

($v_0$, $v_\infty$ müssen, da in ihnen $q$ reell ist, positiv sein.)

Aus (3) ergiebt sich sodann:

$$(8) \qquad \begin{aligned} w_0 = 0, \quad w_1 &= w_3 = -5 - 2i\sqrt{5}, \\ w_2 &= w_4 = -5 + 2i\sqrt{5}. \end{aligned}$$

Dies müssen die Wurzeln von (5) sein für $j = 12^3$ und daraus erhält man die gesuchte Resolvente in der Form:

$$(9) \qquad w(w^2 + 10w + 45)^2 = \gamma_3^2 = j(\omega) - 12^3.$$

Diese Gleichung lässt sich auch in die Form bringen:

$$(10) \qquad (w + 3)^3 (w^2 + 11w + 64) = j(\omega),$$

auf die man auch direct kommt, wenn man, anstatt $\omega = i$ zu setzen,

$$\omega = \frac{-1 + i\sqrt{3}}{2}$$

annimmt.

Die gefundene Resolvente vereinfacht sich noch, wenn man [nach (9)]:

$$z = \sqrt{w} = \frac{\gamma_3}{w^2 + 10w + 45}$$

setzt:

(11) $$z^5 + 10z^3 + 45z = \gamma_3,$$

oder wenn man (nach 10)

(12) $$w^2 + 11w + 64 = y^3, \quad y = \frac{\gamma_2}{w + 3}$$

setzt:

(13) $$y^5 - 40y^2 - 5\gamma_2 y - \gamma_2^2 = 0,$$

eine Gleichung, die sich auch ergiebt, wenn man von vornherein die Annahme macht:

$$2y = v_\infty v_0 + v_1 v_4 + v_2 v_3.$$

In der Gleichung (13) fehlen, wie man sieht, die dritte und die vierte Potenz der Unbekannten. Dieselbe Eigenschaft kommt auch, wie leicht nachzuweisen ist, derjenigen Gleichung zu, deren Wurzeln

(14) $$x = y(\lambda + \mu z) = \frac{(\lambda + \mu z)\gamma_2}{z^2 + 3}$$ [1])

sind, wenn $\lambda$, $\mu$ beliebige Parameter bedeuten, welche für alle fünf Werthe $x$ die gleichen sind.

Setzt man diese Gleichung in die Form

(15) $$x^5 - 5ax^3 - 5b\gamma_2 x - bc\gamma_2^2 = 0,$$

so ergeben sich nach einigen Rechnungen, mit Benutzung der besonderen Werthe, welche $x$ für $\gamma_3 = 0$ und $\gamma_3 = \infty$ annimmt, für $a$, $b$, $c$ die folgenden Ausdrücke:

(16) $$\begin{aligned} a &= 8\lambda^3 - 72\lambda\mu^2 + \gamma_3(\lambda^2\mu - \mu^3) \\ b &= \lambda^4 + 18\lambda^2\mu^2 - 27\mu^4 + \gamma_3\lambda\mu^3 \\ c &= \lambda^5 + 10\lambda^3\mu^2 + 45\lambda\mu^3 + \gamma_3\mu^5. \end{aligned}$$

---

Es soll noch eine Resolvente 5ten Grades mit Benutzung der Function $f(\omega)$ gebildet werden.

Wir setzen:

(17) $$u = f(\omega), \quad v_\infty = f(5\omega), \quad v_z = f\left(\frac{\omega + c}{5}\right)$$

---

[1]) Vgl. Kiepert, Auflösung der Gleichung 5ten Grades. Crelle's Journal, Bd. 87, S. 114.

$$c \equiv 0 \pmod{48}, \quad z \equiv c \pmod{5},$$

und haben nach §. 76 zwischen $u$ und $v$ die Gleichung 6ten Grades:

$$u^6 + v^6 - u^5 v^5 + 4uv = 0. \tag{18}$$

Wir untersuchen den Einfluss, welchen die drei Vertauschungen

$$(\omega, \omega + 2), \quad \left(\omega, -\frac{1}{\omega}\right), \quad \left(\omega, \frac{\omega - 1}{\omega + 1}\right)$$

auf die Grössen $v_z$ haben. Durch diese Vertauschungen geht $c$ über in $c_1$, $c_2$, $c'$, welche nach §. 72, (9), (11) und §. 76 (6) durch die Congruenzen

$$c_1 \equiv c + 2, \quad c_2 \equiv -\frac{1}{c}, \quad c' \equiv \frac{c-1}{c+1} \pmod{5} \tag{19}$$

bestimmt sind. Abgesehen von dieser Aenderung des Index gehen nach §. 76, (4) und (9) die $v$ über in

$$e^{-\frac{5\pi i}{12}} v, \quad v, \quad -\frac{\sqrt{2}}{v}. \tag{20}$$

Man hat also, wenn zur Abkürzung $e^{-\frac{5\pi i}{12}} = \varepsilon$ gesetzt wird, folgende zusammengehörige Vertauschungen:

$$\begin{array}{llllllll}
\omega, & u, & v_\infty, & v_0, & v_1, & v_2, & v_3, & v_4, \\
\omega + 2, & e^{-\frac{\pi i}{12}} u, & \varepsilon v_\infty, & \varepsilon v_2, & \varepsilon v_3, & \varepsilon v_4, & \varepsilon v_0, & \varepsilon v_1, \\
-\frac{1}{\omega}, & u, & v_0, & v_\infty, & v_4, & v_2, & v_3, & v_1, \\
\frac{\omega - 1}{\omega + 1}, & \frac{\sqrt{2}}{u}, & -\frac{\sqrt{2}}{v_1}, & -\frac{\sqrt{2}}{v_4}, & -\frac{\sqrt{2}}{v_0}, & -\frac{\sqrt{2}}{v_2}, & -\frac{\sqrt{2}}{v_3}, & -\frac{\sqrt{2}}{v_\infty}.
\end{array} \tag{21}$$

Wir führen nun die fünf Grössen $w_z$ durch die Gleichung ein:

$$w_z = \frac{(v_\infty - v_z)(v_{z+1} - v_{z-1})(v_{z+2} - v_{z-2})}{\sqrt{5}\, u^3,}, \tag{22}$$

also:

$$w_0 = \frac{(v_\infty - v_0)(v_1 - v_4)(v_2 - v_3)}{\sqrt{5}\, u^3},$$

$$w_1 = \frac{(v_\infty - v_1)(v_2 - v_0)(v_3 - v_4)}{\sqrt{5}\, u^3},$$

$$w_2 = \frac{(v_\infty - v_2)(v_3 - v_1)(v_4 - v_0)}{\sqrt{5}\, u^3},$$

$$w_3 = \frac{(v_\infty - v_3)(v_4 - v_2)(v_0 - v_1)}{\sqrt{5}\, u^3},$$

$$w_4 = \frac{(v_\infty - v_4)(v_0 - v_3)(v_1 - v_2)}{\sqrt{5}\, u^3},$$

so dass, wenn man in der letzten Reihe davon Gebrauch macht, dass nach (18) das Product der sechs Grössen $v_z$ den Werth $u^6$ hat, sich aus (21) folgende zusammengehörige Vertauschungen der $w$ ergeben:

$$(23)\qquad \begin{array}{cccccc} \omega, & w_0, & w_1, & w_2, & w_3, & w_4, \\ \omega + 2, & -w_2, & -w_3, & -w_4, & -w_0, & -w_1, \\ -\frac{1}{\omega}, & w_0, & w_2, & w_1, & w_4, & w_3, \\ \frac{\omega - 1}{\omega + 1}, & -w_0, & -w_3, & -w_4, & -w_2, & -w_1. \end{array}$$

Die Functionen $w$ können für keinen von 0 und $\infty$ verschiedenen Werth von $u$ unendlich werden. Nehmen wir daher die Gleichung, deren Wurzeln die fünf Grössen $w_z$ sind, in der Form an

$$w^5 + A_1 w^4 + A_2 w^3 + A_3 w^2 + A_4 w + A_5 = 0,$$

so sind $A_1^2$, $A_2$, $A_3^2$, $A_4$, $A_5^2$ nach den Grundsätzen des §. 76 ganze rationale Functionen von

$$(24)\qquad u^{24} + \frac{2^{12}}{u^{24}}.$$

Die Entwickelung von (24) nach steigenden Potenzen von $q$ fängt an mit $q^{-1}$, während der Anfang der Entwickelung von $w_z$

$$q^{-\frac{1}{10}} e^{-\frac{c\pi i}{60}}$$

ist. Die Grössen $A_1^2$, $A_2$, $A_3^3$, $A_4$ können daher nicht einmal die erste Potenz von (24) enthalten und sind also constant, während $A_5^2$ die Form hat:

$$A_5^2 = u^{24} + \frac{2^{12}}{u^{24}} + C,$$

worin $C$ eine Constante ist. Die Werthe der Constanten kann man bestimmen, wenn man die Werthe der $w_z$ für $\omega = i$ kennt. Es ist aber für $\omega = i$ [vgl. oben (6), (7)]:

$$u = f(i) = \sqrt[4]{2},$$

$$v_3 = f\left(\frac{i + 48}{5}\right) = f\left(\frac{i - 2}{5} + 10\right) = e^{-\frac{10\pi i}{24}} f\left(\frac{i - 2}{5}\right),$$

$$= e^{-\frac{10\pi i}{24}} f(i + 2) = -i\sqrt[4]{2},$$

$$v_2 = i\sqrt[4]{2}$$

und folglich nach (18):

$$v_\infty = v_0 = \sqrt[4]{2}\,\frac{1+\sqrt{5}}{2},$$

$$v_1 = v_4 = \sqrt[4]{2}\,\frac{1-\sqrt{5}}{2}.$$

Folglich wird:

$$w_0 = 0, \quad w_1 = w_2 = i\sqrt{5}, \quad w_3 = w_4 = -i\sqrt{5}.$$

Danach wird zunächst $C = -2^7$, also

$$A_5^2 = \left(u^{12} - \frac{64}{u^{12}}\right)^2,$$

und daraus durch Vergleichung der Anfänge der Entwickelung

$$A_5 = -u^{12} + \frac{64}{u^{12}},$$

und die Gleichung für $w$ bekommt die Form:

$$w(w^2+5)^2 = u^{12} - \frac{64}{u^{12}}. \tag{25}$$

Man kann ihr aber noch eine andere, sehr bemerkenswerthe Form geben.

Nach den zwischen den Functionen $f(\omega)$, $f_1(\omega)$, $f_2(\omega)$ stattfindenden Relationen [§. 29, (11), (12)] ist:

$$\frac{f(\omega)^{24}-64}{f(\omega)^{12}} = \frac{[f_1(\omega)^8 - f_2(\omega)^8]^2}{f(\omega)^4}.$$

Führen wir also für $w$ die neue Unbekannte

$$y = \sqrt{w} = \frac{f_1(\omega)^8 - f_2(\omega)^8}{f(\omega)^2(w^2+5)}, \tag{26}$$

ein, so erhalten wir die Form:

$$y^5 + 5y = \frac{f_1(\omega)^8 - f_2(\omega)^8}{f(\omega)^2}. \tag{27}$$

Es liegt nicht in unserem Plane, die umfassenden algebraischen Untersuchungen hier wiederzugeben oder weiter zu verfolgen, die durch die Transformationstheorie der elliptischen Functionen angeregt wurden und besonders für die Theorie der Gleichungen fünften Grades wichtige und schöne Resultate zu Tage gebracht haben. Wir verweisen darüber neben den grundlegenden Arbeiten von Hermite und Kronecker auf das Werk von F. Klein, „Vorlesungen über das Ikosaëder und die Auflösung der Gleichungen vom fünften Grade“, Leipzig 1884, wo der Leser neben den eigenen Untersuchungen des Verfassers auch eine eingehende historische Würdigung der hierher gehörigen Fragen findet.

Indessen wollen wir die Frage der Auflösung der Gleichung fünften Grades um so weniger ganz mit Stillschweigen übergehen, als die erforderlichen Formeln im Vorhergehenden vollständig aufgestellt sind.

Hermite reducirt die zu lösende Gleichung fünften Grades auf die sogenannte Jerrard'sche Form (die nach F. Klein's Bemerkung richtiger als die Bring'sche Form zu bezeichnen wäre), d. h. eine Gleichung, in welcher die zweite, dritte und vierte Potenz der Unbekannten nicht vorkommt. Man erreicht die Transformation der allgemeinen Gleichung fünften Grades auf diese Form durch Auflösung von Gleichungen, die den dritten Grad nicht übersteigen[1]). Diese Gleichung vergleicht Hermite mit der Resolvente fünften Grades der Jacobi'schen Modulargleichung. Man kann sich zum gleichen Zweck aber auch der Resolvente (27) bedienen.

Nach der soeben erwähnten Methode kann die allgemeine Gleichung fünften Grades auf die Form reducirt werden:

(28) $$z^5 + 5z = a,$$

und diese Gleichung wird mit (27) identisch, wenn man setzt:

$$f_1(\omega)^8 - f_2(\omega)^8 = a f^2(\omega).$$

Nimmt man hierzu die Gleichungen:

$$f_1^8 + f_2^8 = f^8, \quad f f_1 f_2 = \sqrt{2},$$

so erhält man

(29) $$f^{24} - a^2 f^{12} - 64 = 0.$$

Durch diese quadratische Gleichung ist $f^{12}$ als Function von $a$ bestimmt.

Dann sind die Wurzeln der Gleichung (28) durch die Quadratwurzeln aus den Ausdrücken (22) dargestellt. Das doppelte Vorzeichen dieser Quadratwurzeln erklärt sich daraus, dass zwei entgegengesetzte Werthe von $a$ zu derselben Gleichung (29) führen. Man kann aber auch die Wurzeln eindeutig bestimmen nach der Formel (26)

(30) $$z = \frac{a}{w^2 + 5}.$$

---

[1]) Man vgl. z. B. die einfache Darstellung bei Serret, Cours d. Alg. sup., Nr. 192.

In der oben erwähnten Arbeit von **Kiepert** wird die allgemeine Gleichung fünften Grades auf die Form (15) transformirt, wozu nur die Auflösung einer quadratischen Gleichung erforderlich ist. Sieht man darin $a$, $b$, $c$ als beliebig gegeben an, so dienen die Gleichungen (16) zur Bestimmung von $\lambda$, $\mu$, $\gamma_3$. Dies geschieht ebenfalls mit Hülfe einer quadratischen Gleichung, was allerdings nicht auf den ersten Blick zu ersehen ist. (Vgl. F. **Klein**, Vorlesungen über das Ikosaëder, S. 191 f.)

Auf die Resolventenbildung für den siebenten Transformationsgrad werden wir weiter unten zurückkommen, wenn wir über die Hülfsmittel verfügen, welche die complexe Multiplication bietet.

# III.

# ZAHLENTHEORETISCHER THEIL.

## Elfter Abschnitt.

# Complexe Multiplication.

### §. 86. Ursprung der complexen Multiplication.

Bezeichnen wir mit $\varphi(u)$ eine doppelt periodische Function mit den Perioden $\omega_1$, $\omega_2$, so besitzt, wenn $n$ eine ganze Zahl bedeutet, $\varphi(nu)$ dieselben Perioden, und hierauf beruht die Multiplication der elliptischen Functionen, die im achten Abschnitt betrachtet wurde. Es entsteht nun die Frage, ob sich nicht noch auf andere Weise ein Multiplicator $\mu$ so bestimmen lässt, dass $\varphi(\mu u)$ die Perioden $\omega_1$, $\omega_2$ besitzt, ob also eine Multiplication auch mit nicht ganzzahligem Multiplicator existirt. Dies wird dann und nur dann der Fall sein, wenn für ein System ganzer Zahlen $a$, $b$, $c$, $\partial$ die Gleichungen bestehen:

$$(1)\qquad \begin{aligned} \mu\omega_1 &= a\omega_1 + b\omega_2 \\ \mu\omega_2 &= c\omega_1 + \partial\omega_2 \end{aligned}$$

Setzen wir, um die darin enthaltene Forderung näher zu ergründen:

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

und nehmen an, dass $\omega$ einen positiven imaginären Bestandtheil habe, so folgt aus (1):

$$(2)\qquad \mu = a + b\omega$$

$$(3)\qquad \omega = \frac{c + \partial\omega}{a + b\omega}.$$

So lange $\omega$ als variabel betrachtet wird, ist diese Gleichung nur möglich, wenn $b = c = 0$, $a = \partial$ und $\mu$ also eine ganze Zahl ist.

Ist dagegen die Gleichung (3) nicht eine identische, so ist $\omega$ die Wurzel einer ganzzahligen quadratischen Gleichung:

$$b\omega^2 + (a - \partial)\omega - c = 0, \tag{4}$$

also, wenn wir

$$a\partial - bc = n$$

$$\Delta = -4bc - (a - \partial)^2 = 4n - (a + \partial)^2$$

setzen:

$$\omega = \frac{-a + \partial + \sqrt{-\Delta}}{2b}, \tag{5}$$

$$\mu = \frac{a + \partial + \sqrt{-\Delta}}{2}, \tag{6}$$

$$n = \frac{a + \partial + \sqrt{-\Delta}}{2} \cdot \frac{a + \partial - \sqrt{-\Delta}}{2}, \tag{7}$$

$$\mu^2 - (a + \partial)\mu + n = 0. \tag{8}$$

Damit $\omega$ einen positiven imaginären Theil haben kann, muss $\Delta$ und um so mehr also $n$ positiv sein, und $\mu$ ist eine complexe, ganze, algebraische Zahl. Daher erklärt sich die Bezeichnung complexe Multiplication.

Wenn nun umgekehrt $\omega$ einer quadratischen Gleichung

$$A\omega^2 + B\omega + C = 0 \tag{9}$$

genügt, worin $A, B, C$ ganze Zahlen sind, für welche

$$\Delta = 4AC - B^2 \tag{10}$$

positiv ist, so ist $\omega$ nicht reell, und in einer der beiden Wurzeln von (9), welche für $\omega$ genommen werden soll, ist der imaginäre Theil positiv.

Unbeschadet der Allgemeinheit können $A$, $B$, $C$ ohne gemeinsamen Theiler und $A$, $C$ positiv angenommen werden. Es lassen sich dann für $\omega$ unendlich viele Relationen von der Form (3) [oder (4)] aufstellen. Man hat nur, wenn $x$ eine ganze von Null verschiedene Zahl ist, zu setzen:

$$\begin{aligned} b &= Ax, \\ c &= -Cx, \\ a - \partial &= Bx. \end{aligned} \tag{11}$$

Setzt man noch

$$a + \partial = y, \tag{12}$$

so folgt:

$$\begin{aligned} 2a &= y + Bx, & b &= Ax, \\ 2\partial &= y - Bx, & c &= -Cx, \end{aligned} \tag{13}$$

woraus sich für $a\partial - bc = n$ ergiebt

$$4n = y^2 + \varDelta x^2. \tag{14}$$

Die Zahl $n$ wird also in die beiden complexen ganzzahligen Factoren

$$n = \frac{y + ix\sqrt{\varDelta}}{2} \cdot \frac{y - ix\sqrt{\varDelta}}{2} \tag{15}$$

zerlegt. Für $\omega$ und $\mu$ findet sich noch

$$\omega = \frac{-B + i\sqrt{\varDelta}}{2A} = \frac{2C}{-B - i\sqrt{\varDelta}}, \tag{16}$$

$$\mu = a + b\omega = \frac{y + ix\sqrt{\varDelta}}{2}. \tag{17}$$

Die hier eingeführten Zahlen $x$, $y$ sind nur an die eine Bedingung geknüpft, dass $y + Bx$ und folglich auch $y - Bx$ gerade Zahlen seien, damit $a$, $\partial$ nach (13) ganze Zahlen werden. Ist also $B$ gerade, so muss $y$ gerade sein, während $x$ beliebig ist; ist $B$ ungerade, so sind $x$ und $y$ beide gerade oder beide ungerade anzunehmen. Nach (10) kann man diese Unterscheidung auch so ausdrücken:

$$\begin{array}{lll} & 1) \text{ Ist } \varDelta \equiv 0 \pmod 4, & \text{so ist } y \equiv 0 \pmod 2, \\ (18) & 2) \text{ Ist } \varDelta \equiv -1 \pmod 4, & \text{so ist } y \equiv x \pmod 2, \end{array}$$

Sollen bei gegebenen $A$, $B$, $C$ die Zahlen $a$, $b$, $c$, $\partial$ ohne gemeinsamen Theiler sein, so kommen noch andere Bedingungen hinzu:

Aus (11), (12) folgt, dass jeder gemeinsame Theiler von $a$, $b$, $c$, $\partial$ auch Theiler von $x$ und $y$ ist; umgekehrt ist jeder gemeinsame Theiler von $x$ und $y$ auch Theiler von $b$, $c$, $2a$, $2\partial$. Sollen also $a$, $b$, $c$, $\partial$ ohne gemeinsamen Theiler sein, so können $x$ und $y$ keinen grösseren gemeinsamen Theiler haben als 2, und damit, wenn sie diesen haben, $a$, $b$, $c$, $\partial$ nicht alle vier gerade sind, dürfen $y$ und $Bx$ nicht beide durch 4 theilbar sein.

Es ist bei einer späteren Frage nothwendig, über $x$, $y$ so zu verfügen, dass $a\partial - bc = n$ kein Quadrat ist. Dies erreichen wir nach (14), wenn $y^2 + \varDelta x^2 = z^2$ ein Quadrat ist, und $p$ eine in $z$, aber nicht in $y$ und folglich auch nicht in $x$ aufgehende Primzahl, ferner $\lambda$ eine beliebige durch $p$ nicht theilbare Zahl, wenn wir $y + \lambda p$ an Stelle von $y$ treten lassen; denn es ist

$$(y + \lambda p)^2 + \varDelta y^2 = z^2 + 2y\lambda p + \lambda^2 p^2$$

durch $p$, aber nicht durch $p^2$ theilbar.

## §. 87. Die singulären Werthe der Invariante $j(\omega)$.

Die Frage, die zunächst unser Interesse in Anspruch nimmt, ist die nach den Werthen der Modulfunctionen von $\omega$ für die besonderen Werthe des Arguments $\omega$, die wir im vorigen Paragraphen betrachtet haben. Von diesen hängen die Moduln der elliptischen Functionen ab, welche eine complexe Multiplication zulassen, die nach Kronecker singuläre Moduln heissen. Wir werden dem entsprechend auch von den singulären Werthen der Modulfunctionen sprechen.

Die merkwürdigen Gesetze, welche diese algebraischen Zahlen beherrschen, treten am reinsten und deutlichsten zu Tage bei den singulären Werthen der Invariante $j(\omega)$; bei der numerischen Berechnung geben, wie wir sehen werden, andere Modulfunctionen einfachere Resultate.

Wenn $\omega$ der Gleichung (9), §. 86, genügt und $a$, $b$, $c$, $\partial$, $n$ wie im vorigen Paragraphen bestimmt sind, so folgt zunächst:

$$j(\omega) = j\left(\frac{c + \partial\omega}{a + b\omega}\right), \tag{1}$$

und wenn also

$$F_n(u, v) = 0 \tag{2}$$

die zum Transformationsgrad $n$ gehörige Invariantengleichung ist (§. 72), so ist (2) befriedigt, wenn $a$, $b$, $c$, $\partial$ ohne gemeinsamen Theiler sind und

$$u = j(\omega), \quad v = j\left(\frac{c + \partial\omega}{a + b\omega}\right) = u \tag{3}$$

gesetzt wird. Danach gelangen wir zu dem ersten Hauptsatz dieser Theorie:

1. Der singuläre Werth

$$u = j(\omega)$$

ist, wenn $a$, $b$, $c$, $\partial$ ohne gemeinsamen Theiler sind, eine Wurzel der algebraischen Gleichung

$$F_n(u, u) = 0. \tag{4}$$

Ist umgekehrt $u$ eine Wurzel der Gleichung (4), so ist, wenn $\omega$ aus der Gleichung $j(\omega) = u$ bestimmt wird, einer von den der Gleichung (2) genügenden Werthen von $v$ gleichfalls gleich $u$. Nach §. 72 sind aber die Wurzeln von (2) in der Form

$$v = j\left(\frac{c + \partial\omega}{a}\right), \quad a\partial = n$$

enthalten, und es besteht also eine Gleichung:

$$j(\omega) = j\left(\frac{c + \partial\omega}{a}\right),$$

welche nach §. 47 eine Gleichung

$$\frac{c + \partial\omega}{a} = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}, \quad \alpha\delta - \beta\gamma = 1$$

zur Folge hat.

Diese ist aber gleichbedeutend mit einer Gleichung der Form

$$\omega = \frac{c + \partial\omega}{a + b\omega}, \quad a\partial - bc = n,$$

woraus eine Gleichung von der Form (9), §. 86

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

folgt, und $u$ ist daher ein singulärer Werth der Invariante $j(\omega)$.

Es ist zunächst der Grad der Gleichung (4) zu ermitteln.

Nach §. 72, (17) ist für ein unbestimmtes $x$

$$F_n[x, j(\omega)] = \Pi\left[x - j\left(\frac{c + \partial\omega}{a}\right)\right]$$

und folglich

$$F_n[j(\omega), j(\omega)] = \Pi\left[j(\omega) - j\left(\frac{c + \partial\omega}{a}\right)\right]. \tag{5}$$

$a$, $c$, $\partial$ haben hier die Bedeutung wie im §. 72, so dass $a$, $\partial$ alle der Bedingung $a\partial = n$ genügenden Paare positiver ganzer Zahlen und $c$ ein Restsystem nach dem Modul $a$ durchläuft, mit Ausschluss solcher Werthe, die zu dem grössten gemeinschaftlichen Theiler $e$ von $a$ und $\partial$ nicht relativ prim sind, so dass die Anzahl der Werthe von $c$, die zu einer Zerlegung von $n$ in die beiden Factoren $a$, $\partial$ gehören,

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

ist.

Bezeichnen wir den Grad von (4), d. h. die höchste Potenz von $j(\omega)$, welche auf der linken Seite von (5) vorkommt, mit $N$ und mit $C_0$ den Coëfficienten dieser höchsten Potenz, so beginnt die Entwickelung der linken Seite von (5) nach steigenden Potenzen von $q$ mit dem Gliede

$$C_0 q^{-2N},$$

und wenn wir also die Factoren der rechten Seite von (5) in gleicher Weise entwickeln, so können wir sowohl $C_0$ als $N$ bestimmen.

Für einen Factor der rechten Seite von (5)

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

haben wir folgende Anfänge der Entwickelung

$$\begin{array}{lll} 1. & -q^{-\frac{2\mathfrak{d}}{a}} e^{-\frac{2\pi i c}{a}} & \mathfrak{d} > a, \\ 2. & q^{-2} & \mathfrak{d} < a, \\ 3. & q^{-2}\left(1 - e^{-\frac{2\pi i c}{a}}\right) & \mathfrak{d} = a. \end{array}$$

Nehmen wir zunächst an, $n$ sei kein Quadrat, so kommt der Fall 3. nicht vor und es ist

$$N = \sum_{\mathfrak{d} > a} \frac{\mathfrak{d}}{e}\, \varphi(e) + \sum_{\mathfrak{d} < a} \frac{a}{e}\, \varphi(e)$$

oder was dasselbe ist

$$N = 2 \sum_{\mathfrak{d} > a} \frac{\mathfrak{d}}{e}\, \varphi(e). \tag{6}$$

$C_0$ ist jedenfalls eine $n$te Einheitswurzel und da es zugleich eine rationale Zahl ist, so muss es $= \pm 1$ sein.

Ist sodann $n$ ein Quadrat, so kommen $\varphi(\sqrt{n})$ Factoren 3. vor und es ergiebt sich:

$$N = 2 \sum_{\mathfrak{d} > a} \frac{\mathfrak{d}}{e}\, \varphi(e) + \varphi(\sqrt{n}). \tag{7}$$

$C_0$ ist hier zwar auch von Null verschieden, aber nicht gleich $\pm 1$. Den Werth von $C_0$ brauchen wir in diesem Falle nicht näher zu bestimmen. (Er ist, wie aus der Kreistheilungstheorie folgt, immer ein Theiler von $\sqrt{n}$).

Da wir nun nach der Schlussbemerkung des vorigen Paragraphen, wie auch die Gleichung (9), §. 86 beschaffen sein mag, immer annehmen können, dass $n$ kein Quadrat sei, so genügt $u$ einer algebraischen Gleichung mit ganzzahligen Coëfficienten, worin die höchste Potenz der Unbekannten den Coëfficienten 1 hat, und daraus folgt der zweite Satz.

2. Die singulären Werthe $j(\omega)$ sind **ganze** algebraische Zahlen.

## §. 88. Die Classeninvarianten.

Einer quadratischen Gleichung

(1) $$A\omega^2 + B\omega + C,$$

in welcher, wie oben, $A$, $B$, $C$ ohne gemeinschaftlichen Theiler, $A$, $C$ und $\Delta = 4AC - B^2$ positiv sind, 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, nämlich, wenn wir nach der Bezeichnung von Gauss die Form

$$ax^2 + 2bxy + cy^2$$

mit $(a, b, c)$ bezeichnen, die Form

(2) $$\psi = \left(A, \frac{1}{2}B, C\right) \quad \text{oder} \quad = (2A, B, 2C).$$

Die Determinante dieser Form ist negativ und hat in den beiden Fällen den Werth

(3) $$-m = -\frac{1}{4}\Delta \quad \text{oder} \quad = -\Delta.$$

Umgekehrt wird aus jeder quadratischen Form (2) eine Gleichung (1) abgeleitet. Wir sprechen demgemäss auch von quadratischen Gleichungen erster und zweiter Art[1]).

Die quadratische Gleichung (1) geht durch die lineare Substitution

(4) $$\omega = \frac{\gamma + \delta\omega'}{\alpha + \beta\omega'}, \quad \alpha\delta - \beta\gamma = 1$$

in eine Gleichung derselben Form

(5) $$A'\omega'^2 + B'\omega' + C' = 0$$

über, worin

$$A' = A\delta^2 + B\delta\beta + C\beta^2,$$
$$B' = 2A\delta\gamma + B(\alpha\delta + \beta\gamma) + 2C\alpha\beta,$$
$$C' = A\gamma^2 + B\gamma\alpha + C\alpha^2,$$

und folglich

$$4A'C' - B'^2 = 4AC - B^2 = \Delta.$$

Die der Gleichung (5) entsprechende quadratische Form

$$\psi' = \left(A', \frac{1}{2}B', C'\right) \text{ oder } (2A', B', 2C')$$

---

[1]) Bezüglich der Voraussetzungen aus der Zahlentheorie, die hier und in der Folge zu machen sind, verweisen wir nächst Gauss, „Disquisitiones arithmeticae“, besonders auf Dirichlet-Dedekind, „Vorlesungen über Zahlentheorie“. 3. Auflage. Braunschweig 1879.

ist mit der Form $\psi$ äquivalent und man erhält alle mit (2) äquivalenten Formen auf diese Weise.

Nennen wir also kurzweg $\omega$ die Wurzel der Form $\psi$ [es ist darunter diejenige Wurzel der quadratischen Gleichung (1) zu verstehen, deren imaginärer Theil positiv ist] und nennen wir ferner zwei Zahlen $\omega$, $\omega'$, die in der Beziehung (4) zu einander stehen, äquivalente Zahlen, so haben wir den Satz, dass quadratische Formen dann und nur dann äquivalent sind, wenn ihre Wurzeln äquivalente Zahlen sind.

Nach der fundamentalen Eigenschaft der Function $j(\omega)$ (§. 47) sind zwei Werthe, $j(\omega)$, $j(\omega')$, dann und nur dann einander gleich, wenn $\omega$ und $\omega'$ äquivalente Zahlen sind.

Es gehört hiernach einer der singulären Werthe von $j(\omega)$ nicht nur zu einer bestimmten quadratischen Form mit negativer Determinante, sondern zu einer Formenclasse und unterscheidet diese Classe von allen anderen Formenclassen derselben Determinante.

Wir bezeichnen daher diesen singulären Werth $j(\omega)$ als Invariante der durch $\psi$ repräsentirten Formenclasse oder kurz als **Classeninvariante.**

Wir werden später den Begriff als Classeninvariante noch etwas weiter fassen, bleiben aber fürs Erste bei dieser Definition stehen.

Aus dem, was in §. 87 bewiesen ist, ergiebt sich, dass die Classeninvariante $j(\omega)$ unendlich vielen Gleichungen

$$F_n(u, u) = 0 \tag{6}$$

genügt, und wir haben auch die Werthe von $n$ bereits bestimmt, welche in (6) zulässig sind. Wir geben dem Kriterium für $n$, welches in der Gleichung (14), §. 86 liegt, eine etwas andere Gestalt, indem wir Formen erster und zweiter Art unterscheiden.

Ist $j(\omega)$ Invariante einer Classe erster Art von der Determinante $-m$, so ist in der eben angeführten Formel $\varDelta = 4m$ zu setzen und wir ersetzen noch $y$ durch $2y$.

1. Eine zur Determinante $-m$ gehörige Classeninvariante $j(\omega)$ der ersten Art genügt also der Gleichung (6) dann und nur dann, wenn $n$ durch die Form $x^2 + my^2$ eigentlich darstellbar ist (d. h. so, dass $x$ und $y$ keinen gemeinschaftlichen Theiler haben).

2. Eine zur Determinante $-m$ gehörige Classeninvariante $j(\omega)$ der zweiten Art genügt der Gleichung

(6) dann und nur dann, wenn durch die Form $x^2 + my^2$ entweder $n$ oder $4n$ eigentlich darstellbar ist.

Wir suchen nun aus $F_n(u, u)$ einfachere Factoren abzuscheiden. Indem wir unter $u$ eine Variable verstehen, bezeichnen wir das Polynom

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

wenn sich das Product über alle Invarianten primitiver Classen erster oder zweiter Art der Determinante $-m$ erstreckt, mit

$$H_m(u) \quad \text{oder} \quad H'_m(u),$$

wobei $H'_m(u)$ natürlich nur für solche Werthe von $m$ existirt, die $\equiv -1 \pmod 4$ sind, weil es nur für solche Determinanten Classen zweiter Art giebt.

$H_m(u)$, $H'_m(u)$ sind dann ganze rationale Functionen von $u$, deren Grade $h$, $h'$ gleich den Classenzahlen der quadratischen Formen erster und zweiter Art der Determinante $-m$ sind. Die höchste Potenz der Variablen hat in beiden Functionen den Coëfficienten 1 und die Wurzeln von $H_m = 0$, $H'_m = 0$ sind die Invarianten der einzelnen zur Determinante $-m$ gehörigen Formenclassen.

Wir beweisen nun den Satz, dass die Functionen $H_m$, $H'_m$ rationale Coëfficienten haben.

Ist dies bewiesen, so folgt von selbst, dass die Coëfficienten ganze rationale Zahlen sind.

Da nämlich diese Coëfficienten durch Multiplication und Addition aus den Classeninvarianten zusammengesetzt sind, so folgt zunächst, dass sie ganze algebraische Zahlen sind. Ist aber eine ganze algebraische Zahl zugleich rational, so ist sie eine ganze rationale Zahl (§. 59).

Zum Beweise wenden wir die vollständige Induction an. Wir nehmen den Satz als bewiesen an für $H_n$, so lange $n < m$, und für $H'_n$, so lange $n < 4m - 1$, und beweisen daraus die Richtigkeit für $H_m$ und $H'_{4m-1}$. Können wir dann noch die Richtigkeit für $H_1$ und $H'_3$ nachweisen, so ist der Beweis allgemein geführt.

Wir wollen die Gleichung

$$F_m(u, u) = 0 \tag{7}$$

betrachten. Nach 1. ist sie erfüllt für die zur Determinante $-m$ gehörigen Classeninvarianten erster Art und ausserdem nur noch für solche Classeninvarianten erster Art, die zu absolut kleineren Determinanten gehören; denn

$$m = x^2 + ny^2$$

ist befriedigt für $n = m$, $x = 0$, $y = \pm 1$ und ausserdem nur noch für solche Werthe von $n$, die kleiner als $m$ sind.

Es ist ferner (7) erfüllt für die zur Determinante $-(4m-1)$ gehörigen Classeninvarianten zweiter Art und ausserdem wieder nur für solche Classeninvarianten zweiter Art, die zu absolut kleineren Determinanten gehören; denn

$$4m = x^2 + ny^2$$

ist befriedigt für $n = (4m-1)$, $x = \pm 1$, $y = \pm 1$ und sonst nur noch für solche Werthe von $n$, die kleiner als $4m-1$ sind.

Hieraus folgt, dass die Function $F_m(u, u)$ theilbar ist durch $H_m(u)$, $H'_{4m-1}(u)$ und dass alle anderen Factoren von $F_m(u, u)$ zugleich in solchen Functionen $H_n(u)$, $H'_n(u)$ enthalten sind, in welchen $n < m$ oder $< 4m-1$ ist, deren Coëfficienten nach Voraussetzung ebenso wie die von $F_m$ rational sind.

Befreit man also $F_m$ von mehrfachen Factoren und ferner von allen gemeinschaftlichen Factoren mit solchen $H_n$, $H'_n$, für welche $n < m$ oder $< 4m-1$ ist, was durch rationale Operationen geschieht, so bleibt das Product

$$H_m(u)\, H'_{4m-1}(u) \tag{8}$$

übrig, welches sonach auch rationale Coëfficienten hat.

Wir betrachten ferner die Gleichung:

$$F_{4m-1}(u, u) = 0. \tag{9}$$

Sie ist erfüllt für die Wurzeln von $H'_{4m-1}(u) = 0$, weil

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

durch $y = 0$ und $x = \pm 1$ befriedigt ist. Dagegen ist (9) für die Wurzeln von $H_m(u)$ nicht erfüllt, da die Gleichung

$$4m-1 = y^2 + mx^2$$

nicht lösbar ist [denn es müsste $x^2 < 4$, also $x = \pm 1$ sein, dann würde aber folgen $y^2 \equiv -1 \pmod 3$, was unmöglich ist].

Es ist also $F_{4m-1}(u, u)$ durch $H'_{4m-1}(u)$ theilbar, dagegen relativ prim zu $H_m(u)$. Indem man also den grössten gemeinsamen Theiler von $F_{4m-1}$ und $H_m\, H'_{4m-1}$ sucht, erhält man $H'_{4m-1}$ und daraus auch $H_m$ rational.

Es bleibt also nur noch zu beweisen übrig, dass $H_1$ und $H'_3$ rationale Coëfficienten haben.

Wählen wir als Repräsentanten der zur Determinante $-1$ und $-3$ gehörigen Formenclassen erster und zweiter Art

$$(1, 0, 1), \quad (2, 1, 2),$$

so haben wir für $\omega$ im ersten Falle

$$\omega = -\frac{1}{\omega}, \quad \omega = i,$$

und im zweiten

$$\omega = -1 - \frac{1}{\omega}, \quad \omega = e^{\frac{2\pi i}{3}}.$$

Nach §. 49, (14) haben wir aber

$$\gamma_3\left(-\frac{1}{\omega}\right) = -\gamma_3(\omega),$$

$$\gamma_2(\omega) = e^{-\frac{2\pi i}{3}}\gamma_2\left(-1-\frac{1}{\omega}\right),$$

und daher

$$\gamma_3(i) = 0, \quad \gamma_2\left(e^{\frac{2\pi i}{3}}\right) = 0.$$

Daraus folgt nach der Definition von $\gamma_2$, $\gamma_3$ [§. 49, (4)]

$$j(i) = 27.64, \quad j\left(e^{\frac{2\pi i}{3}}\right) = 0,$$

mithin

(10) $$H_1 = u - 27.64, \quad H'_3 = u$$

und w. z. b. w., dass $H_1(u)$ und $H'_3(u)$ rationale Coëfficienten haben.

Hiermit ist die Existenz von ganzzahligen Gleichungen $H_m = 0$, $H'_m = 0$ vom Grade der Classenzahlen $h$, $h'$ nachgewiesen, deren Wurzeln die Classeninvarianten sind.

Wir bezeichnen diese Gleichungen als Classengleichungen.

Jede Classeninvariante $j(\omega)$ giebt Anlass zu einem algebraischen Zahlkörper $\mathfrak{K}[j(\omega)]$ (vergl. §. 55, 3. 4.), welches der Inbegriff aller rationalen Functionen von $j(\omega)$ mit rationalen Zahlcoëfficienten ist. Den Grad dieses Körpers zu bestimmen, wird weiter unten eine unserer Hauptaufgaben sein.

Aus jeder Zahl $\alpha$ dieses Körpers entstehen $h$ oder $h'$ conjugirte Zahlen, wenn man $j(\omega)$ durch die verschiedenen Wurzeln der betreffenden Classengleichung ersetzt. Sind diese Werthe von $\alpha$ alle von einander verschieden, so ist $\alpha$ eine primitive Zahl des Körpers und $j(\omega)$ kann auch rational durch $\alpha$ ausgedrückt werden. Der Körper $\mathfrak{K}[j(\omega)]$ ist identisch mit $\mathfrak{K}(\alpha)$. Die $h$ oder $h'$ Werthe einer solchen Zahl $\alpha$, die den verschiedenen Formenclassen entsprechen, sind dann gleichfalls die Wurzeln einer rationalen Gleichung.

Wir erweitern die Bedeutung des Wortes Classeninvariante dahin, dass jede primitive Zahl des Körpers $\mathfrak{K}[j(\omega)]$ jetzt als Classeninvariante bezeichnet werden soll, und ebenso soll unter einer Classengleichung die rationale Gleichung verstanden werden, deren Wurzeln die verschiedenen Werthe einer Classeninvariante sind; wir unterscheiden Classeninvarianten und Classengleichungen erster und zweiter Art, je nachdem die entsprechenden Formenclassen erster oder zweiter Art sind[1].

## §. 89. Beziehungen zwischen den Classeninvarianten erster und zweiter Art.

Ist $m \equiv -1 \pmod 4$, so haben wir zur Determinante $-m$ gehörige Formenclassen erster und zweiter Art und demnach auch eine Classengleichung der ersten und der zweiten Art

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

von den Graden der Classenzahlen $h$, $h'$.

Ist $u = j(\omega)$ eine Wurzel der ersteren, so ist, wenn $A, B, C$ ganze Zahlen ohne gemeinsamen Theiler sind,

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

Da die Gleichung (3) primitiv und von der ersten Art sein soll, so können nicht $A$ und $C$ beide gerade sein. Ist $A$ ungerade, so kann man auch $B$ ungerade voraussetzen, da man eventuell, indem man $\omega + 1$ an Stelle von $\omega$ treten lässt, $B$ durch $B + A$ ersetzen kann; dann aber muss $C$ durch 4 theilbar sein.

Wir betrachten nun die cubische Invariantengleichung

$$(4) \qquad F_2(v, u) = 0,$$

deren Wurzeln, wenn $u = j(\omega)$ ist,

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

sind (§. 72). Wird

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

gesetzt, so ergeben sich aus (3) für $\omega'$ die folgenden drei quadratischen Gleichungen:

---

[1] Die sämmtlichen zu einer Formenclasse negativer Determinanten gehörigen Invarianten erster oder zweiter Art bilden, was Kronecker eine Gattung algebraischer Zahlen nennt.

$$\omega' = 2\omega, \quad A\omega'^2 + 4B\omega' + 4C = 0, \quad \text{Det.} = -4m,$$

$$(6) \quad \omega' = \frac{\omega}{2}, \quad A\omega'^2 + B\omega' + \frac{C}{4} = 0, \quad \text{Det.} = -m, \text{ zweite Art,}$$

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

$$\text{Det.} = -4m.$$

Von den drei Werthen (5) genügt also nur der eine, nämlich $j\left(\frac{\omega}{2}\right)$ zugleich der Gleichung (2) und (4). Der grösste gemeinschaftliche Theiler der beiden Gleichungen

$$H'_m(v) = 0, \quad F_2(v, u) = 0$$

ist also $v - j\left(\frac{\omega}{2}\right)$ und wir erhalten das Resultat:

Die Classeninvarianten zweiter Art sind rational durch die der ersten Art ausdrückbar.

Ersetzt man in dem so gewonnenen rationalen Ausdruck

$$(7) \qquad j(\omega') = R(u)$$

$u$ durch die verschiedenen Wurzeln der Gleichung (1), so bekommt man die sämmtlichen Wurzeln von (2). Denn ist $v = j(\omega')$ eine beliebige Classeninvariante zweiter Art, so genügt $\omega'$ der Gleichung

$$(8) \qquad A\omega'^2 + B\omega' + C = 0, \quad B^2 - 4AC = -m$$

mit ungeradem $B$.

Nun kann man nach einem bekannten Satz aus der Theorie der quadratischen Formen, von dem wir oft Gebrauch machen werden, in jeder Formenclasse vom Theiler $\sigma$ einen Repräsentanten $(A, B, C)$ so wählen, dass $A:\sigma$ relativ prim zu einer beliebig angenommenen Zahl wird, also durch irgend welche Primzahlen nicht theilbar ist.

Ferner erhält man durch die Substitution

$$x = x' + \lambda y', \quad y = y'$$

für ein beliebiges $\lambda$ aus $(A, B, C)$ eine Schaar äquivalenter Formen $(A, B + \lambda A, C + 2\lambda B + \lambda^2 A)$, die von Dedekind parallele Formen genannt worden sind. Wählt man $A$ so, dass $A:\sigma$ relativ prim zu $\sigma$ wird, so kann man $\lambda$ so bestimmen, dass $B + \lambda A$ bei der Theilung durch einen beliebigen zu $A:\sigma$ theilerfremden Modul einen beliebig gegebenen Rest lässt; d. h. man kann den Repräsentanten einer Classe so auswählen, dass der mittlere Coëfficient einer beliebig gegebenen Zahl congruent wird in Bezug auf einen gleichfalls beliebig gegebenen Modul[1]).

Hiernach können wir voraussetzen, dass in (8) $A$ ungerade ist. Setzen wir also $\omega = 2\,\omega'$, so ergiebt sich aus (8) die Gleichung

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

welche primitiv von der ersten Art und von der Determinante $-m$ ist. Es ist also nach dem Obigen $j(\omega')$ eine rationale Function von $j(\omega)$.

Es ist noch zu entscheiden, ob und wie oft aus verschiedenen Werthen von $j(\omega)$ ein und derselbe Werth von $j(\omega')$ abgeleitet werden kann.

Dazu bemerken wir, dass, wenn zwei verschiedene Wurzeln der Gleichung (1), in (7) für $u$ gesetzt, denselben Werth $j(\omega') = v$ hervorrufen, beide Werthe von $u$ der cubischen Gleichung (4) genügen müssen, aus welcher (7) abgeleitet ist. Es können daher höchstens je drei der Werthe von $u$ zu dem gleichen $v$ führen.

Nun sind aber, wenn $v = j(\omega')$ ist, die drei Wurzeln von (4)

$$(9) \qquad u = j(2\,\omega'),\quad j\left(\frac{\omega'}{2}\right),\quad j\left(\frac{\omega'+1}{2}\right)$$

und es handelt sich nur noch um die Frage, welche von diesen drei Werthen Wurzeln von (1) sind.

Wir erhalten aber aus (8) die folgenden drei quadratischen Gleichungen der Determinante $-m$ von der ersten Art:

$$(10) \qquad \begin{aligned} \omega &= 2\,\omega', & A\omega^2 + 2\,B\omega + 4\,C &= 0, \\ \omega &= \frac{\omega'}{2}, & 4\,A\omega^2 + 2\,B\omega + \phantom{4\,}C &= 0, \\ \omega &= \frac{\omega'+1}{2}, & 4\,A\omega^2 + 2\,(B - 2\,A)\omega + (A - B + C) &= 0. \end{aligned}$$

1. Ist nun

$$m \equiv -1 \pmod{8},$$

so ist nach unserer Voraussetzung, dass $A$, $B$ ungerade sind, $C$ eine gerade Zahl; von den drei quadratischen Gleichungen (10) ist nur die erste primitiv, und es führt also auch nur diese zu einer Wurzel der Gleichung (1).

Es gehört zu jeder Classeninvariante zweiter Art nur eine Classeninvariante erster Art, so dass auch die Classeninvarianten erster Art durch die der zweiten Art rational ausdrückbar sind.

---

[1]) Vgl. **Dirichlet-Dedekind**, Vorlesungen über Zahlentheorie, §. 56, §. 93.

Der Körper $\mathfrak{K}[j(\omega)]$ ist mit $\mathfrak{K}[j(\omega')]$ identisch. Es folgt in diesem Falle noch, dass die Classenzahlen $h$, $h'$ einander gleich sind, wie auch aus der Zahlentheorie bekannt ist.

2. Ist
$$m \equiv 3 \pmod{8},$$
so ist $A$ ungerade und die Gleichungen (10) sind alle drei primitiv. Wenn daher die drei Grössen (9) von einander verschieden sind, so gehören zu jeder Classeninvariante zweiter Art drei Classeninvarianten erster Art, also:
$$h = 3h'.$$

Der Körper $\mathfrak{K}[j(\omega')]$ ist ein Theiler des Körpers $\mathfrak{K}[j(\omega)]$.

3. Wir haben also schliesslich noch zu entscheiden, ob unter den drei Grössen (9) einander gleiche vorkommen können, oder mit anderen Worten, ob unter den drei Zahlen
$$2\omega', \quad \frac{\omega'}{2}, \quad \frac{\omega'+1}{2} \tag{11}$$
einander äquivalente enthalten sind.

Nehmen wir die beiden ersten derselben äquivalent an, also
$$2\omega' = \frac{2\gamma + \delta\omega'}{2\alpha + \beta\omega'} \qquad \alpha\delta - \beta\gamma = 1,$$
so folgt aus (8), wenn $x$, $y$ ganze Zahlen sind
$$2\gamma = Cx, \qquad \delta - 4\alpha = Bx,$$
$$-2\beta = Ax, \qquad \delta + 4\alpha = y,$$
$$y^2 + mx^2 = 16,$$
worin, da $A$ ungerade, $x$ und folglich auch $y$ gerade ist.

Die letzte Gleichung ist aber nur möglich für $m = 3$; und in diesem Falle sind in der That die drei Grössen (11) äquivalent. Man übersieht dies am besten, wenn man für den Repräsentanten (8) die Gleichung
$$\omega'^2 + \omega' + 1 = 0$$
wählt, aus der man erhält
$$2\omega' = \frac{1 + 2\dfrac{\omega'}{2}}{-\dfrac{\omega'}{2}} = \frac{-1}{\dfrac{\omega'+1}{2}}.$$

Hier ist also wieder
$$h = h',$$
und da, wie wir oben gesehen haben (§. 88), in diesem Falle $j(\omega') = 0$ ist, so muss $j(\omega)$ eine rationale Zahl sein, die sich aus der Gleichung (5), §. 74 ergiebt:
$$j(\omega) = j(\sqrt{-3}) = 2^4 . 3^3 . 5^3.$$

## §. 90. Beziehungen zwischen Classeninvarianten, deren Determinanten in quadratischem Verhältniss stehen.

Wenn zwei negative Determinanten quadratischer Formen sich nur durch einen quadratischen Factor von einander unterscheiden, so bestehen zwischen ihren Classeninvarianten algebraische Beziehungen, welche eine Verallgemeinerung der im vorigen Paragraphen betrachteten Relationen sind, und die wir nun aufzusuchen haben.

Es sei $p$ eine beliebige Primzahl (auch $p = 2$ nicht ausgeschlossen) und

(1) $$m' = p^2 m.$$

Ferner seien

(2) $$H_m(u) = 0,$$ (3) $$H_{m'}(v) = 0$$

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

(4) $$A'\omega'^2 + 2B'\omega' + C' = 0, \quad A'C' - B'^2 = m'$$

die primitive quadratische Gleichung, welcher $\omega'$ genügt. $A'$ möge, was erlaubt ist, durch $p$ untheilbar vorausgesetzt sein.

Wir betrachten nun die Invariantengleichung

(5) $$F_p(u, v) = 0,$$

deren Wurzeln sind:

(6) $$u = j(p\omega'), \quad j\left(\frac{\omega' + c}{p}\right), \quad c = 0, 1, 2, \ldots p - 1.$$

Das Argument dieser Functionen

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

genügt einer aus (4) abzuleitenden quadratischen Gleichung, nämlich

(7) $$\omega = p\omega', \quad A'\omega^2 + 2B'p\omega + C'p^2 = 0,$$
$$\omega = \frac{\omega' + c}{p},$$

$$A'p^2\omega^2 + 2(B' - A'c)p\omega + A'c^2 - 2B'c + C' = 0,$$

deren Determinanten $-p^2 m'$ sind, und die alle primitiv sind, mit Ausnahme derer, in welchen $A'c^2 - 2B'c + C'$ durch $p$ theilbar ist. Nun ist

$$A'(A'c^2 - 2B'c + C') = (A'c - B')^2 + m',$$

also $A'c^2 - 2B'c + C'$ dann und nur dann durch $p$ theilbar, wenn

$$A'c - B' \equiv 0 \pmod{p}. \tag{8}$$

Dadurch ist ein bestimmter Werth von $c$ gegeben, für welchen $A'c^2 - 2B'c + C'$ nicht nur durch $p$, sondern durch $p^2$ theilbar ist. Aus (7) erhalten wir daraus eine und nur eine zur Determinante $-m$ gehörige Gleichung:

$$A'\omega^2 + 2\frac{B' - A'a}{p}\omega + \frac{A'c^2 - 2B'c + C'}{p^2} = 0. \tag{9}$$

Es haben also die Gleichungen (2) und (5) eine und nur eine Wurzel $u$ mit einander gemein und diese lässt sich rational durch $v$ ausdrücken:

$$u = R(v). \tag{10}$$

Wir haben zweitens nachzuweisen, dass man hieraus alle Wurzeln der Gleichung (2) erhält, wenn man für $v$ alle Wurzeln von (3) setzt, und daran schliesst sich noch die Frage, wie oft jeder Werth von $u$ durch (10) erzeugt wird. Sei also $u = j(\omega)$ eine beliebige Wurzel der Gleichung (2) und

$$A\omega^2 + 2B\omega + C = 0, \quad AC - B^2 = m, \tag{11}$$

worin $A$ wieder durch $p$ untheilbar vorausgesetzt wird. Setzen wir $\omega' = p\omega$, so genügt $\omega'$ der Gleichung

$$A\omega'^2 + 2Bp\omega' + Cp^2 = 0, \tag{12}$$

welche primitiv ist und zur Determinante $-m' = -p^2 m$ gehört. Es ist also $v = j(\omega')$ eine Wurzel von (3), welche der Gleichung (5) genügt, und aus der man daher durch (10) $u = j(\omega)$ erhält. Also können alle Wurzeln von (3) durch die Gleichung (10) dargestellt werden.

Um aber die zweite Frage zu beantworten, wie viele Werthe von $v$ zu demselben Werthe von $u$ führen, bemerken wir, dass die verschiedenen Werthe von $v$, welche dies leisten, Wurzeln der Gleichung (5) und (3) sein müssen, also in einer der Formen

$$j(p\omega), \quad j\left(\frac{\omega + c}{p}\right) \tag{13}$$

enthalten sind. Nun haben wir aus (11):

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

deren Determinante $-m'$ ist. Unter den Grössen (13) werden aber nur diejenigen der Gleichung (3) genügen, für welche die entsprechende Gleichung (14) primitiv ist.

Die erste der Gleichungen (14) ist nach unserer Voraussetzung stets primitiv; von den übrigen sind nur die nicht primitiv, für welche

$$Ac^2 - 2Bc + C$$

oder

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

durch $p$ theilbar ist. Hier hat man nun vier Fälle zu unterscheiden.

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

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

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

$$(Ac - B)^2 \equiv -m \pmod{p}.$$

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

d) Für $p = 2$ hat, da $A$ ungerade ist, die Congruenz

$$(Ac - B)^2 \equiv -m \pmod{p}$$

immer eine und nur eine Wurzel, und folglich ist für $p = 2$ immer eine unter den Gleichungen (14) imprimitiv.

Nehmen wir also vorläufig an, was wir gleich genauer untersuchen werden, es seien unter den $p + 1$ Grössen

$$p\omega, \quad \frac{\omega + c}{p} \tag{15}$$

keine zwei äquivalente, so gehören zu jedem Werthe von $u$ in dem Falle a), d) $p$ Werthe $v$, im Falle b) $p - 1$ Werthe $v$, im Falle c) $p + 1$ Werthe $v$, und wenn wir die Grade von (2) und (3) mit $h$ und $h'$ bezeichnen, so ergeben sich (in Uebereinstimmung mit bekannten Formeln der Zahlentheorie) folgende Beziehungen:

$$\begin{aligned} h' &= ph, && \text{falls } m \equiv 0 \pmod{p} \text{ oder } p = 2, \\ h' &= (p-1)h, && \text{,,} \quad \left(\frac{-m}{p}\right) = +1, \\ h' &= (p+1)h, && \text{,,} \quad \left(\frac{-m}{p}\right) = -1. \end{aligned} \tag{16}$$

Es handelt sich also noch um die Frage, ob unter den Grössen (15) nach Ausschluss der wegen a), b), d) wegfallenden, noch äquivalente vorkommen können, oder ob die Invariantengleichung (5) für $u = j(\omega)$ gleiche Wurzeln haben kann. Diese Frage behandeln wir ihrer principiellen Wichtigkeit wegen in einem besonderen Paragraphen.

## §. 91. Die Factoren der Discriminante der Invariantengleichung.

Wir stellen uns jetzt die Frage allgemein, wann eine Invariantengleichung

$$(1) \qquad F_p(u, v) = 0,$$

worin $p$ eine Primzahl ist, für $u = j(\omega)$ zwei oder mehrere gleiche Wurzeln hat, oder wann unter den $p + 1$ Grössen

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

zwei oder mehrere einander gleiche vorkommen. Dies findet dann und nur dann statt, wenn unter den $p + 1$ Grössen

$$(3) \qquad p\omega, \quad \frac{\omega + c}{p}$$

zwei äquivalente vorkommen. Es muss also jedenfalls $\omega$ einer ganzzahligen quadratischen Gleichung mit negativer Discriminante genügen, die wir in der Form annehmen:

$$(4) \qquad A\omega^2 + B\omega + C = 0, \quad 4AC - B^2 = \Delta > 0,$$

worin $A$, $B$, $C$ ohne gemeinsamen Theiler sind.

Ersetzen wir $\omega$ durch eine äquivalente Zahl, also (4) durch eine äquivalente Gleichung, so werden die Grössen (2) nur unter einander vertauscht. Die Frage nach der Anzahl der gleichen Wurzeln von (1) wird also davon nicht berührt, und wir können daher in Uebereinstimmung mit dem vorigen Paragraphen annehmen, dass $A$ durch $p$ nicht theilbar sei. Ist nun zunächst $p\omega$ äquivalent mit $\frac{\omega + c}{p}$, so ist:

$$(5) \qquad \frac{\omega + c}{p} = \frac{\gamma + \delta p\omega}{\alpha + \beta p\omega}, \quad \alpha\delta - \beta\gamma = 1.$$

Schreiben wir diese Gleichung so:

$$(6) \qquad \beta p\omega^2 + (\alpha + \beta cp - \delta p^2)\omega + c\alpha - \gamma p = 0,$$

so folgt durch Vergleichung mit (4) (da $A$ durch $p$ untheilbar sein sollte), dass $\alpha$ durch $p$ theilbar, also $= p\alpha'$ sein muss, und dass eine ganze Zahl $x$ existirt, welche den Bedingungen genügt:

$$(7)\qquad \beta = Ax, \quad \alpha' + \beta c - \delta p = Bx, \quad c\alpha' - \gamma = Cx.$$

Setzen wir noch

$$(8)\qquad \alpha' - \beta c + \delta p = y,$$

so folgt

$$(9)\qquad \begin{aligned} 2\alpha' &= Bx + y \\ 2(\beta c - \delta p) &= Bx - y \end{aligned}$$

und aus

$$(10)\qquad p\alpha'\delta - \beta\gamma = 1$$

folgt sodann

$$(11)\qquad y^2 + \varDelta x^2 = 4.$$

Der Werth $x = 0$ ist auszuschliessen, weil sonst $\beta = 0$ sein müsste, was der Gleichung (10) widerspricht, und wir können unbeschadet der Allgemeinheit $x$ positiv annehmen. Da überdies $\varDelta$ nach dem Modul 4 entweder $\equiv 0$ oder $\equiv 3$ sein muss, so bleiben zur Erfüllung von (11) nur folgende zwei Möglichkeiten übrig:

1. $\varDelta = 3, \quad x = 1, \quad y = \pm 1.$

Nach (9) ist $B$ ungerade, also die Gleichung (4) von der zweiten Art und der Determinante $-3$. Da es für diese Determinante nur eine Formenclasse zweiter Art giebt, so können wir $A = 1$, $B = 1$, $C = 1$ annehmen, d. h. für $\omega$ die imaginäre dritte Einheitswurzel $e^{\frac{2\pi i}{3}}$ setzen, und erhalten unter den Grössen (3) drei äquivalente, indem wir $y = +1$, und $= -1$ annehmen:

$$(12)\qquad p\omega, \quad \frac{\omega}{p}, \quad \frac{\omega+1}{p},$$

wie auch aus den Gleichungen

$$\frac{\omega}{p} = \frac{-1}{p + p\omega}, \quad \frac{\omega+1}{p} = \frac{-1}{p\omega}$$

erkannt wird, welche die Aequivalenz der drei Grössen (12) evident machen.

2. $\varDelta = 4, \quad x = 1, \quad y = 0.$

Die Gleichung (4) ist von der ersten Art mit der Determinante $-1$, wir können $B = 0$, $A = C = 1$, d. h. $\omega = i$ annehmen und finden die zwei äquivalenten Werthe:

$$p\omega, \quad \frac{\omega}{p},$$

wie auch aus der Gleichung

$$p\omega = \frac{-p}{\omega}$$

folgt.

Es seien ferner zwei der Werthe (3)

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

äquivalent, so dass eine Gleichung besteht

$$(13) \qquad \frac{\omega + c}{p} = \frac{\gamma p + \delta(\omega + c')}{\alpha p + \beta(\omega + c')}, \quad \alpha\delta - \beta\gamma = 1,$$

oder

$$(14) \qquad \begin{gathered} \beta\omega^2 + (\beta c' + \beta c + \alpha p - \delta p)\omega + \\ \beta c c' + \alpha c p - \delta c' p - \gamma p^2 = 0, \end{gathered}$$

woraus durch Vergleichung mit (4)

$$(15) \qquad \begin{aligned} \beta &= Ax, \\ \beta c' + \beta c + \alpha p - \delta p &= Bx, \\ \beta c c' + \alpha c p - \delta c' p - \gamma p^2 &= Cx, \end{aligned}$$

und wenn man wieder

$$(16) \qquad \beta c' - \beta c + \alpha p + \delta p = y$$

setzt:

$$(17) \qquad \begin{aligned} 2(\beta c' + \alpha p) &= Bx + y, \\ 2(\beta c - \delta p) &= Bx - y. \end{aligned}$$

Daraus

$$(18) \qquad y^2 + \Delta x^2 = 4p^2.$$

Aus (15) ergeben sich die Congruenzen

$$(19) \qquad \beta c c' \equiv Cx, \quad \beta(c + c') \equiv Bx, \quad \beta \equiv Ax \pmod{p},$$

und man hat nun folgende Fälle zu unterscheiden:

3. Ist $x$ nicht durch $p$ theilbar, so folgt aus (19):

$$(20) \quad Acc' \equiv C, \quad A(c + c') \equiv B, \quad A^2(c - c')^2 \equiv -\Delta \pmod{p}.$$

Die letzte Congruenz ist aber nur dann möglich, wenn entweder $\Delta$ durch $p$ theilbar ist, dann aber ist $c = c'$ und die beiden äquivalenten Zahlen sind identisch, oder wenn $-\Delta$ quadratischer Rest von $p$ ist; dann ist $c$ von $c'$ verschieden, und $c$ und $c'$ sind die beiden Wurzeln der Congruenz:

$$(21) \qquad (2Ac - B)^2 \equiv -\Delta \pmod{p}.$$

$\Delta$ muss in der Form enthalten sein

(22) $$\varDelta = \frac{4p^2 - y^2}{x^2},$$

und aus (15) und (16) findet man die Werthe von $\alpha$, $\beta$, $\gamma$, $\delta$.

Ist aber $x$ durch $p$ theilbar, so ist auch $y$ durch $p$ theilbar; die Gleichung (16) ist wieder nur möglich, wenn $\varDelta = 3$ oder $\varDelta = 4$ ist, und wir erhalten die beiden Fälle

4. $\varDelta = 3$, $x = p$, $y = \pm p$.

Man kann wieder, wie oben bei 1., $A = B = C = 1$ annehmen und erhält zu jedem $c$ gehörig, mit Ausnahme von $c = 0$, $c = 1$, die schon durch 1. erledigt sind, aus (15), (16) zwei Werthe von $c'$, die mit $c'$ und $c''$ bezeichnet sein mögen:

(23) $$c' \equiv \frac{1}{1 - c}, \quad c'' \equiv \frac{1 - c}{-c} \pmod{p}.$$

Diese drei Werthe von $c$ sind von einander verschieden, ausser wenn

(24) $$(2c - 1)^2 \equiv -3 \pmod{p},$$

wo alle drei einander gleich werden.

Dies ist für $\varDelta = 3$ dieselbe Congruenz wie (21) des Falles 3.

5. $\varDelta = 4$, $x = p$, $y = 0$.

Wir machen die Annahme $A = C = 1$, $B = 0$ und erhalten für jedes $c$, mit Ausnahme von $c = 0$, einen zugehörigen Werth von $c'$ aus

$$c c' \equiv -1 \pmod{p}.$$

Die beiden Werthe $c, c'$ fallen nur dann in einen zusammen, wenn

$$c^2 \equiv -1 \pmod{p},$$

was wiederum für diesen Fall unter (21) des Falles 3. gehört.

Wir fassen das hiermit Bewiesene folgendermaassen zusammen.

Die Invariantengleichung (1)

$$F_p(v, u) = 0,$$

deren Wurzeln wir wie früher mit

$$v_\infty, v_0, v_1, \ldots v_{p-1}$$

bezeichnen, hat gleiche Wurzeln unter folgenden Voraussetzungen:

I. Wenn in $u = j(\omega)$ für $\omega$ die Wurzel der Gleichung (4)

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

gesetzt wird, in welcher $-\varDelta = B^2 - 4AC$ negativ, durch $p$ nicht theilbar, quadratischer Rest von $p$ und zugleich in der Form

$$\varDelta = \frac{4p^2 - y^2}{x^2}$$

darstellbar ist (also sicherlich $\varDelta < 4p^2$). Dann ist $v_c = v_{c'}$, wenn $c$ und $c'$ die beiden Wurzeln der Congruenz (21)

$$(2Ac - B)^2 \equiv - \varDelta \pmod{p}$$

sind (Fall 3).

II. Wenn $u = j\left(e^{\frac{2\pi i}{3}}\right) = 0$ (§. 88) gesetzt wird, so werden für $p = 2$ alle drei Wurzeln einander gleich (Fall 1), für $p = 3$ wird $v_\infty = v_0 = v_1$, während $v_2$ davon verschieden ist (Fälle 1, 4). Ist $-3$ quadratischer Nichtrest von $p$, so ist $p \equiv -1 \pmod{3}$ und von den Wurzeln von (1) werden je drei einander gleich (Fälle 1, 4). Ist endlich $-3$ quadratischer Rest von $p$, also $p \equiv 1 \pmod{3}$, so kann immer $4p^2 = y^2 + 3x^2$ gesetzt werden (vgl. Dirichlet-Dedekind, §. 70). Es sind also die zwei der Congruenz $(2c - 1)^2 \equiv -3 \pmod{p}$ entsprechenden Wurzeln $v_c, v_{c'}$ einander gleich, während die übrigen $p - 1$ Wurzeln zu je dreien einander gleich werden (Fälle 3, 4).

III. Wenn $u = j(i) = 27.64$ gesetzt wird, so werden für $p = 2$ die beiden Wurzeln $v_\infty$, $v_0$ einander gleich, $v_1$ davon verschieden (Fälle 2, 5), für alle anderen Werthe von $p$ werden die $p + 1$ Wurzeln paarweise einander gleich (Fälle 3, 5).

Kehren wir nun zurück zu den Formeln (16) des vorigen Paragraphen, so sehen wir aus den jetzt gewonnenen Resultaten, dass diese Formeln nur in dem Falle $m = 1$ einer Correctur bedürfen, und dass in diesem Falle die rechten Seiten durch 2 zu theilen sind. Wollen wir die Formeln (16) allgemein gültig erhalten, so müssen wir die auch sonst oft zweckmässige Uebereinkunft treffen, dass unter der Classenzahl $h$ für die Determinante $-1$ nicht die Einheit, sondern $\frac{1}{2}$ verstanden werden soll.

## Zwölfter Abschnitt.

# Berechnung der Classeninvarianten.

### §. 92. Die Classeninvariante $\gamma_2$.

Wir haben schon oben bemerkt, dass ausser der Function $j(\omega)$ noch andere Modulfunctionen zur Bildung von Classeninvarianten sich eignen, und oft zu einfacheren Resultaten Anlass geben. Unter diesen tritt uns zunächst die Function $\gamma_2(\omega)$ entgegen, welche durch $\sqrt[3]{j(\omega)}$ definirt ist.

Wir haben im §. 74 gesehen, dass zwischen den Functionen

$$u = \gamma_2(\omega), \quad v = \gamma_2\left(\frac{c + \partial\omega}{a}\right), \tag{1}$$

falls $a\partial = n$ durch 3 nicht theilbar ist, und $c$ durch 3 theilbar angenommen ist, eine Transformationsgleichung

$$\Phi_n(u, v) = 0 \tag{2}$$

besteht. Die Function $\Phi_n$ hängt aber nur von den beiden Argumenten $vu^{-n}$, $u^3$ ab und in $\Phi_n(u, u) = 0$ kommt also, wenn $n \equiv 1 \pmod 3$ ist, nur $u^3$, d. h. $j(\omega)$ vor; in diesem Falle kann daher diese Gleichung kein anderes Resultat ergeben, als die Invariantengleichung. Anders ist es aber in dem Falle

$$n \equiv -1 \pmod 3, \tag{3}$$

den wir jetzt voraussetzen wollen.

Wenn einer der Werthe $v = u$ werden soll, so muss eine Relation bestehen

$$\frac{\gamma + \delta\omega}{\alpha + \beta\omega} = \frac{c + \partial\omega}{a}, \quad \alpha\delta - \beta\gamma = 1, \tag{4}$$

und zugleich muss [§. 49, (15)]

$$\alpha\beta + \alpha\gamma + \beta\delta - \alpha\beta^2\gamma \equiv 0 \pmod 3 \tag{5}$$

sein. Es muss also jedenfalls $\omega$ Wurzel einer quadratischen Gleichung

$$(6)\qquad A\omega^2 + B\omega + C = 0, \quad \varDelta = 4AC - B^2$$

sein.

Besteht umgekehrt eine solche Gleichung, so folgt durch Vergleichung mit (4) in der früher angewandten Art, wenn $x$, $y$ ganze Zahlen sind:

$$(7)\qquad \begin{aligned} \partial\beta &= Ax, \\ c\alpha - a\gamma &= Cx, \\ c\beta + \partial\alpha - a\delta &= Bx, \\ c\beta - \partial\alpha - a\delta &= y, \end{aligned}$$

woraus

$$(8)\qquad \begin{aligned} 2\,\partial\alpha &= Bx - y, \\ 2(c\beta - a\delta) &= Bx + y, \\ 4n &= y^2 + \varDelta x^2. \end{aligned}$$

Setzen wir $A$ relativ prim zu $3n$ voraus (§. 89), so muss $\partial = 1$, $a = n$ angenommen werden; denn nach (7) muss unter dieser Voraussetzung $x$ durch $\partial$ theilbar sein und folglich auch $c\alpha - a\gamma$ und $c\beta - a\delta$, woraus folgt, dass auch $a$, $c$ durch $\partial$ theilbar sein müssten, während doch $a$, $c$, $\partial$ keinen gemeinsamen Theiler haben. Also ist

$$(9)\qquad \begin{aligned} 2\alpha &= Bx - y, & \beta &= Ax, \\ 2n\gamma &= c(Bx - y) - 2Cx, & 2n\delta &= 2cAx - Bx - y. \end{aligned}$$

Die Zahlen $x$, $y$ sind hier ausser den in §. 86, (18) angegebenen Beschränkungen wegen (3) noch der unterworfen, dass $y^2 + \varDelta x^2 \equiv -1 \pmod 3$ werde. Dadurch ist ausgeschlossen, dass $\varDelta$ durch 3 theilbar sei. $x$ muss von Null verschieden sein, und wir können es, ohne die Allgemeinheit zu beschränken, positiv annehmen, was in der Folge geschehen soll. (Eine gleichzeitige Vorzeichenänderung von $x$ und $y$ bewirkt nur eine Vorzeichenänderung von $\alpha$, $\beta$, $\gamma$, $\delta$, die ohne Belang ist.)

Ist $\varDelta \equiv 1 \pmod 3$, so müssen $x$ und $y$ durch 3 untheilbar sein; ist $\varDelta \equiv -1 \pmod 3$, so ist $y$ durch 3 theilbar, $x$ nicht theilbar. Im Uebrigen können die Zahlen $x$, $y$ beliebig angenommen werden. Es ist dann $c$ bestimmt aus den beiden (mit einander verträglichen) Congruenzen:

$$\left.\begin{aligned} cAx &\equiv \frac{Bx + y}{2} \\ c\,\frac{Bx - y}{2} &\equiv Cx \end{aligned}\right\} \pmod n$$

und kann, da $n$ immer durch 3 untheilbar ist, noch der Bedingung

$$c \equiv 0 \pmod 3$$

unterworfen werden.

Da $\beta$ durch 3 nicht theilbar ist, so reducirt sich die Congruenz (5) auf:

$$\alpha + \delta \equiv 0 \pmod 3,$$

oder nach (9) auf

$$B \equiv 0 \pmod 3. \tag{10}$$

Ersetzen wir in (6) $\omega$ durch $\omega \pm 1$, so geht $B$ über in $B \pm 2A$ und von den drei Zahlen $B$, $B + 2A$, $B - 2A$ ist eine und nur eine durch 3 theilbar. Wir nehmen also an, es sei $B$ selbst durch 3 theilbar, dann folgt, dass von den drei Werthen

$$\gamma_2(\omega), \quad \gamma_2(\omega + 1) = e^{-\frac{2\pi i}{3}} \gamma_2(\omega), \quad \gamma_2(\omega - 1) = e^{\frac{2\pi i}{3}} \gamma_2(\omega) \tag{11}$$

nur der erste der Gleichung

$$\Phi_n(u, u) = 0 \tag{12}$$

genügt. Die Gleichung (12) und

$$u^3 - j(\omega) = 0 \tag{13}$$

haben daher nur eine gemeinsame Wurzel, welche also rational durch $j(\omega)$ ausdrückbar ist. Damit ist bewiesen:

$\gamma_2(\omega)$ ist eine Classeninvariante, wenn $\omega$ die Wurzel einer quadratischen Form von negativer Determinante ist, deren Determinante und erster Coëfficient durch 3 nicht theilbar sind, während der mittlere Coëfficient durch 3 theilbar ist.

Wenden wir dies Ergebniss auf den Fall $n = 2$ an, so erhalten wir zunächst aus der Gleichung (5), §. 74:

$$\Phi_2(u, u) = u^4 - 2u^3 - 495u^2 + 2^4 . 3^3 . 5^3 = 0. \tag{14}$$

Die Gleichung

$$y^2 + \Delta x^2 = 8$$

ist, da $\Delta \equiv 0$ oder $\equiv -1 \pmod 4$ sein muss, nur für drei Werthe von $\Delta$ lösbar, nämlich

$$\begin{aligned} \Delta &= 8, \quad x = 1, \quad y = 0, \\ \Delta &= 7, \quad x = 1, \quad y = \pm 1, \\ \Delta &= 4, \quad x = 1, \quad y = \pm 2. \end{aligned} \tag{15}$$

Diesen drei Werthen von $\Delta$ entsprechend kann man für die Gleichung (6) die folgenden wählen:

$$\begin{array}{ll} \varDelta = 8, & \omega^2 + 2 = 0 \\ \varDelta = 7, & \omega^2 + 3\omega + 4 = 0 \text{ (zweite Art)}, \\ \varDelta = 4, & \omega^2 + 1 = 0 \end{array}$$

oder

$$\varDelta = 8, \quad \omega = \sqrt{-2},$$
$$\varDelta = 7, \quad \omega = \frac{-3 + \sqrt{-7}}{2},$$
$$\varDelta = 4, \quad \omega = i.$$

Der Werth $\gamma_2(i)$ ist aber (nach §. 88) bekannt, nämlich $= 12$, und daher muss die linke Seite von (14) durch $u - 12$ theilbar sein. Da dieser Factor bekannt ist, findet man leicht die übrigen:

$$u^4 - 2u^3 - 495u^2 + 2^4 . 3^3 . 5^3 = (u - 12)(u - 20)(u + 15)^2.$$

Da $\gamma_2(\omega)$ ebenso wie $j(\omega)$ für ein rein imaginäres $\omega$ einen positiven Werth hat, so muss der Factor $u - 20$ dem Werthe $\varDelta = 8$ entsprechen, und wir erhalten:

(16) $$\gamma_2(i) = 12,$$

(17) $$\gamma_2(\sqrt{-2}) = 20,$$

(18) $$\gamma_2\left(\frac{-3 + \sqrt{-7}}{2}\right) = -15.$$

Es existiren fünf negative Determinanten $-m$:

(19) $$-11, \quad -19, \quad -43, \quad -67, \quad -163$$ [1]),

zu welchen es nur eine Formenclasse zweiter Art und drei Formenclassen erster Art giebt. Für diese ist also nach unserem Satze:

$$\gamma_2\left(\frac{-3 + \sqrt{-m}}{2}\right)$$

eine ganze rationale Zahl $Z$.

Um diese rationalen Zahlen zu finden, wollen wir Grenzen aufsuchen, zwischen denen sie liegen müssen, die um weniger als eine Einheit von einander verschieden sind.

---

[1]) Dass nicht mehr Determinanten dieser Art existiren, kann bis jetzt nur daraus geschlossen werden, dass, so weit man die Berechnung der Classenzahlen fortgesetzt hat, weitere Zahlen dieser Art nicht gefunden sind [vgl. die Tafel der Classenzahlen von Gauss (Werke, Bd. II, S. 450)].

Nach §. 49, (5), (8) ist:

$$\gamma_2(\omega) = f(\omega)^{16} - \frac{16}{f(\omega)^8} = f_1(\omega)^{16} + \frac{16}{f_1(\omega)^8}$$

$$= f_2(\omega)^{16} + \frac{16}{f_2(\omega)^8},$$

ferner nach §. 29, (19):

$$f_2\left(\frac{-3+\omega}{2}\right) f(\omega) = e^{-\frac{\pi i}{8}} \sqrt{2},$$

also

$$-\gamma_2\left(\frac{-3+\omega}{2}\right) = f(\omega)^8 - \frac{256}{f(\omega)^{16}}.$$

Setzt man also:

(20) $$q = e^{-\pi\sqrt{m}},$$

so erhält man:

$$Z = -\gamma_2\left(\frac{-3+i\sqrt{m}}{2}\right)$$

$$= q^{-\frac{1}{3}} \prod_{1,\infty}^{\nu} (1+q^{2\nu-1})^8 - \frac{256\, q^{\frac{2}{3}}}{\prod\limits_{1,\infty}^{\nu} (1+q^{2\nu-1})^{16}}.$$

Wir machen nun Gebrauch von der für jedes echt gebrochene positive $x$ gültigen Grenzbestimmung:

$$1 + x < e^x < \frac{1}{1-x}, \quad e^{-x} > 1 - x,$$

und erhalten:

$$1 < \Pi\,(1+q^{2\nu-1}) < e^{\frac{q}{1-q^2}},$$

woraus

$$q^{-\frac{1}{3}} - 256\, q^{\frac{2}{3}} < Z < q^{-\frac{1}{3}}\, e^{\frac{8q}{1-q^2}} - 256\, q^{\frac{2}{3}}\, e^{-\frac{16q}{1-q^2}},$$

und indem man die obere Grenze noch vergrössert, kann man dafür auch setzen:

$$Z < q^{-\frac{1}{3}} - 256\, q^{\frac{2}{3}} + \frac{8\, q^{\frac{2}{3}}}{1-8\,q-q^2} + \frac{2^{12}\, q^{\frac{5}{3}}}{1-q^2},$$

für $m = 11$ ist $q$ ungefähr $= 2^{-15}$, woraus man ersieht, dass der Unterschied beider Grenzen:

$$\frac{8\, q^{\frac{2}{3}}}{1-8\,q-q^2} + \frac{2^{12}\, q^{\frac{5}{3}}}{1-q^2}$$

bereits für $m = 11$ und noch mehr also für die grösseren Werthe von $m$ sehr klein ist. $Z$ ist also die zunächst über

$$q^{-\frac{1}{3}} - 256\, q^{\frac{2}{3}}$$

gelegene ganze Zahl, und dieser Werth, für die grösseren $m$ schon $q^{-\frac{1}{3}}$, kommen einer ganzen Zahl ausserordentlich nahe. Daraus berechnet man sehr leicht diese Zahlen[1]):

$$-\gamma_2\left(\frac{-3+\sqrt{-11}}{2}\right) = 32,$$

$$-\gamma_2\left(\frac{-3+\sqrt{-19}}{2}\right) = 96 = 32.3,$$

$$-\gamma_2\left(\frac{-3+\sqrt{-43}}{2}\right) = 960 = 64.15,$$

$$-\gamma_2\left(\frac{-3+\sqrt{-67}}{2}\right) = 5280 = 32.3.5.11,$$

$$-\gamma_2\left(\frac{-3+\sqrt{-163}}{2}\right) = 640\,320 = 64.3.5.23.29.$$

Bei diesen Zahlen ist die Zerlegbarkeit in verhältnissmässig kleine Primzahlen bemerkenswerth.

## §. 93. Die Classeninvarianten $f(\omega)^{24}$.

Die Wurzeln der cubischen Gleichung

$$(u - 16)^3 - u j(\omega) = 0 \tag{1}$$

sind, wie wir früher allgemein gesehen haben (§. 49),

$$u = f(\omega)^{24}, \quad -f_1(\omega)^{24}, \quad -f_2(\omega)^{24},$$

oder

$$f(\omega)^{24}, \quad f(\omega+1)^{24}, \quad f\left(1-\frac{1}{\omega}\right)^{24}. \tag{2}$$

Es sei nun $j(\omega)$ eine Classenvariante erster Art und

$$A\omega^2 + 2B\omega + C = 0, \quad AC - B^2 = m, \tag{3}$$

worin $A$, $2B$, $C$ keinen gemeinschaftlichen Theiler haben. Setzen wir

$$\omega' = \omega + 1, \quad \omega'' = 1 - \frac{1}{\omega},$$

---

[1]) Man thut gut, sich bei diesen und vielen der später beschriebenen Rechnungen ein- für allemal den Briggischen Logarithmus

$$\log(\pi \log e) = 0{,}1349341840$$

zu bemerken, bei dem man übrigens meist mit 7 Decimalen ausreicht.

so ist

$$(4)\qquad \begin{aligned} A\omega'^2 + 2(B - A)\omega' + (A - 2B + C) = 0,\\ A + 2B + C - 2(B + C)\omega'' + C\omega''^2 = 0. \end{aligned}$$

Die drei Argumente von (2) sind also die Wurzeln von äquivalenten quadratischen Formen. Da $A$ und $C$ nicht beide gerade sein können, so ergiebt sich, dass von den drei Formen (3), (4) eine und nur eine die Eigenschaft hat, dass die beiden äusseren Coëfficienten ungerade sind.

Wenn es nun gelingt, eine ganzzahlige Gleichung aufzustellen, welcher von den drei Wurzeln (2) nur die eine genügt, so folgt daraus, dass diese eine Wurzel rational durch $j(\omega)$ ausdrückbar und also eine Classeninvariante ist.

Es besteht zwischen den Functionen

$$(5)\qquad u = f(\omega)^{24},\quad v = f\left(\frac{c + \partial\,\omega}{a}\right)^{24} [c \equiv 0 \pmod{2}]$$

für einen ungeraden Transformationsgrad $n$ (§§. 76, 77) eine Transformationsgleichung

$$\Phi_n(u, v) = 0,$$

und die Gleichung

$$(6)\qquad \Phi_n(u, u) = 0$$

ist also nach §. 47 nur dann befriedigt, wenn für eine der Grössen (5):

$$(7)\qquad \frac{c + \partial\,\omega}{a} = \frac{\gamma + \delta\,\omega}{\alpha + \beta\,\omega},$$

worin

$$(8)\qquad \begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} \equiv \begin{pmatrix}1, & 0\\ 0, & 1\end{pmatrix} \pmod{2},$$

oder

$$(9)\qquad \begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} \equiv \begin{pmatrix}0, & 1\\ -1, & 0\end{pmatrix} \pmod{2}$$

eine zur ersten oder zur zweiten Classe (§. 31) gehörige lineare Transformation ist.

Die Vergleichung von (7) mit (3) führt aber, wie oben, zu den Bedingungen:

$$(10)\qquad \begin{gathered} \beta\,\partial = A x,\\ \alpha c - \gamma a = C x,\\ \beta c - \delta a + \alpha\,\partial = 2 B x,\\ \beta c - \delta a - \alpha\,\partial = 2 y,\\ \beta c - \delta a = B x + y,\quad \alpha\,\partial = B x - y,\\ n = y^2 + m x^2. \end{gathered}$$

Nehmen wir $A$ und $n$ ohne gemeinsamen Theiler an, so muss $\partial = 1$, $a = n$ sein, und aus (10) wird $\alpha$, $\beta$, $\gamma$, $\delta$, $c$ ebenso bestimmt, wie im vorigen Paragraphen, so dass $c$ eine gerade Zahl wird.

Es ergiebt sich:

$$(11) \qquad \begin{aligned} \alpha &= Bx - y, & n\gamma &= -Cx + c(Bx - y), \\ \beta &= Ax, & n\delta &= -Bx - y + Acx. \end{aligned}$$

Wir erreichen am einfachsten unser Ziel, wenn wir, je nachdem $m$ gerade oder ungerade ist,

$$(12) \qquad n = m + 1, \quad n = m$$

setzen.

Sehen wir von dem singulären Fall $m = 1$ vorläufig ab, so folgt aus der Annahme (12) nach (10) in den beiden Fällen eines geraden und eines ungeraden $m$:

$$\begin{aligned} m &\equiv 0 \pmod 2, & x &= 1, & y &= \pm 1, \\ m &\equiv 1 \pmod 2, & x &= 1, & y &= 0. \end{aligned}$$

Aus (11) folgt dann für ein gerades $m$:

$$\left.\begin{aligned} \alpha &\equiv B + 1, & \beta &\equiv A \\ \gamma &\equiv C, & \delta &\equiv B + 1 \end{aligned}\right. \pmod 2,$$

für ein ungerades $m$:

$$\left.\begin{aligned} \alpha &\equiv B, & \beta &\equiv A \\ \gamma &\equiv C, & \delta &\equiv B \end{aligned}\right. \pmod 2.$$

Da $A$, $C$ nicht beide gerade sein können, so kann hiernach die Transformation $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$ nur dann einer der beiden Bedingungen (8), (9) genügen, und zwar nur der zweiten, wenn $A$ und $C$ beide ungerade sind.

Hieraus folgt also, dass unter dieser Voraussetzung $f(\omega)^{24}$ eine Classeninvariante ist.

Die Annahme, dass $A$ relativ prim zu $n$, d. h. zu $m + 1$ oder zu $m$ sei, kann nachträglich als unwesentlich aufgegeben werden.

Denn wenden wir auf $\omega$ eine lineare Transformation $(S)$ an, so geht die Gleichung (3) in eine äquivalente Gleichung über, in welcher die äusseren Coëfficienten dann und nur dann beide ungerade sind, wenn $(S)$ zur ersten oder zweiten Classe gehört, also wenn $f(\omega)^{24}$ durch $(S)$ ungeändert bleibt. Man kann dann noch $(S)$ so bestimmen, dass der erste Coëfficient in der umgeformten Gleichung (3) zu einer beliebigen Zahl, also auch zu $n$ relativ prim wird.

Auf den Fall $m = 1$ ist dies Verfahren nicht anwendbar, weil $\Phi_n(u, u)$ für $n = 1$ (aber auch nur für diesen Werth) identisch verschwindet, für $m = 1$ haben wir aber bereits früher gefunden (§. 85):

$$f(i)^{24} = 64,$$

so dass also auch in diesem Falle der ausgesprochene Satz gilt.

Wenn $m$ ungerade ist, so ist bei ungeradem $A$, $C$ der mittlere Coëfficient $B$ gerade; dagegen ist bei geradem $m$ unter der gleichen Voraussetzung $B$ ungerade. Durch die Substitution $\omega + 1$ für $\omega$ erreichen wir aber auch im Fall eines geraden $m$, dass $B$ gerade, dann aber auch $C$ gerade wird, durch die Vertauschung $(\omega, \omega + 1)$ geht aber $f(\omega)^{24}$ in $-f_1(\omega)^{24}$ über, so dass wir also unserem Satz auch den folgenden Ausdruck geben können:

Ist $\omega$ die Wurzel der quadratischen Gleichung:

$$A\omega^2 + 2B\omega + C = 0, \quad AC - B^2 = m,$$

worin $A$ ungerade, $B$ gerade ist, so ist, je nachdem $m$ ungerade oder gerade ist, $f(\omega)^{24}$ oder $f_1(\omega)^{24}$ Classeninvariante.

Da $A$ und $C$ nicht beide gerade sein können, so sind nur drei Fälle möglich, von denen durch die Vertauschungen

$$(\omega, \omega + 1), \quad \left(\omega, -\frac{1}{\omega}\right)$$

der zweite auf den ersten und der dritte auf den zweiten zurückgeführt wird. Wir haben also in diesen Fällen:

$$(13) \quad \begin{array}{lll} A \equiv 1, & C \equiv 1 \pmod 2, & \text{Classeninvariante } f(\omega)^{24} \\ A \equiv 1, & C \equiv 0 \quad \text{„} & \text{„} \quad f_1(\omega)^{24} \\ A \equiv 0, & C \equiv 1 \quad \text{„} & \text{„} \quad f_2(\omega)^{24}. \end{array}$$

Insbesondere ist also, wenn wir die Hauptform der Determinante $-m$, $(1, 0, m)$ zu Grunde legen, $f(\sqrt{-m})^{24}$ bei ungeradem und $f_1(\sqrt{-m})^{24}$ bei geradem $m$ eine Classeninvariante. Diese beiden Zahlen haben einen reellen positiven Werth, und sollen in den weiter unten folgenden Rechnungen vorzugsweise berücksichtigt werden.

Aus der Gleichung (1) schliessen wir (§. 59), da $j(\omega)$ eine ganze algebraische Zahl ist, dass auch $f(\omega)^{24}$ eine ganze algebraische Zahl sein muss, und die Form der Gleichung (1) zeigt, dass die Norm dieser Zahl eine Potenz von 2 ist.

Wir können aus dem Bewiesenen noch einen auf das Modulquadrat $\varkappa^2$ bezüglichen Schluss ziehen.

Es ist nach §. 49 und §. 29:

$$\varkappa^2 \varkappa'^2 = \frac{16}{f(\omega)^{24}}, \quad \varkappa^2 = \frac{f_2(\omega)^8}{f(\omega)^8} = \frac{16}{f(\omega)^8 f_1(2\omega)^8}. \tag{14}$$

Wenn also $\omega$ einer quadratischen Gleichung (3) mit ungeraden äusseren Coëfficienten und der Determinante $-m$ genügt, so sind $\varkappa^2 \varkappa'^2$ und $\varkappa^6$ rational ausdrückbar durch Classeninvarianten, aber nicht durch die zur Determinante $-m$, sondern die zur Determinante $-4m$ gehörigen (§. 90). Die identische Gleichung

$$\frac{\varkappa^2 \varkappa'^2 + \varkappa^4 \varkappa'^4 + 2\varkappa^6}{1 + \varkappa^6} = \varkappa^2 \tag{15}$$

zeigt, dass dasselbe auch von dem Modulquadrat $\varkappa^2$ gilt. Und dass $\varkappa^2$ selbst Classeninvariante der Determinante $-4m$ ist, ergiebt sich aus folgenden beiden Darstellungen:

$$j(2\omega) = \frac{(f_1(2\omega)^{24} + 16)^3}{f_1(2\omega)^{24}} = \frac{(256 + f_2(\omega)^{24})^3}{f_2(\omega)^{48}} = \frac{16(16\varkappa'^2 + \varkappa^4)^3}{\varkappa^8 \varkappa'^2},$$

$$j\left(\frac{\omega}{2}\right) = \frac{16(16\varkappa^2 + \varkappa'^4)^3}{\varkappa^2 \varkappa'^8},$$

welche zeigen, dass die zur Determinante $-4m$ gehörigen Classeninvarianten sämmtlich rational durch $\varkappa^2$ darstellbar sind.

Da $\varkappa^2$ durch jede lineare Substitution in eine rationale (lineare) Function von $\varkappa^2$ übergeht, so kann $\omega$ durch jede äquivalente Zahl ersetzt werden. Wir haben also den Satz:

> Wenn $\omega$ die Wurzel einer ganzzahligen quadratischen Gleichung erster Art der Determinante $-m$ ist, so ist $\varkappa^2(\omega)$ Classeninvariante für die Determinante $-4m$.

Wie $\varkappa^2(\omega)$ auch dann als Classeninvariante aufgefasst werden kann, wenn $\omega$ Wurzel einer Gleichung zweiter Art ist, wird weiter unten gezeigt werden.

## §. 94. Die Potenzen von $f(\omega)$ als Classeninvarianten.

Nach der Definition von $\gamma_2(\omega)$ ist:

(1) $$f(\omega)^8 = \frac{f(\omega)^{24} - 16}{\gamma_2(\omega)}.$$

Ist $\omega$ die Wurzel einer Gleichung:

(2) $$A\omega^2 + 2B\omega + C = 0, \quad AC - B^2 = m,$$

deren Determinante $-m$ durch 3 nicht theilbar ist, so können wir, wenn nöthig, durch Uebergang zu einer äquivalenten Gleichung, $A$, $C$ als ungerade, $A$ durch 3 untheilbar und $B$ durch 3 theilbar voraussetzen. Dann aber sind nach den beiden vorigen Paragraphen $f(\omega)^{24}$ und $\gamma_2(\omega)$ Classeninvarianten, und wir erhalten aus (1) den Satz:

I. Ist $\omega$ Wurzel einer quadratischen Form erster Art mit negativer, durch 3 nicht theilbarer Determinante, deren beide äussere Coëfficienten ungerade, deren mittlerer Coëfficient durch 3 theilbar ist, so ist

$$f(\omega)^8$$

eine Classeninvariante.

Um die Frage zu untersuchen, ob auch noch niedrigere Potenzen von $f(\omega)$ Classeninvarianten sein können, machen wir Gebrauch von der Formel:

(3) $$f(\omega + 2r)^6 = i^{-r} f(\omega)^6,$$

worin $r$ eine ganze Zahl ist; die Werthe

$$\omega_r = \omega + 2r$$

sind die Wurzeln von äquivalenten quadratischen Gleichungen

$$A\omega_r^2 + 2B_r\omega_r + C_r = 0,$$

worin

(4) $$B_r = B - 2Ar,$$

und hierin lässt sich $r$ nach dem Modul 4 so bestimmen, dass bei ungeradem $m$:

(5) $$B_r \equiv 0, 2, 4, 6 \pmod 8$$

und bei geradem $m$:

(6) $$B_r \equiv 1, 3, 5, 7 \pmod 8).$$

Wenn es nun gelingt, eine Gleichung mit rationalen Coëfficienten aufzufinden, welcher von den vier Werthen (3) entweder nur der eine, der dem Werthe $r = 0$ oder zwei, die den Werthen $r = 0, 2$ entsprechen, genügen, so folgt, dass $f(\omega)^6$ oder $f(\omega)^{12}$ Classeninvarianten sind.

Ist ausserdem $m$ durch 3 untheilbar, so kann man die $B_r$ alle durch 3 theilbar voraussetzen, und es folgt dann durch Combination mit dem Satz I, dass auch

$$f(\omega)^8 f(\omega)^{-6} = f(\omega)^2 \quad \text{oder} \quad f(\omega)^{12} f(\omega)^{-8} = f(\omega)^4$$

unter den Classeninvarianten enthalten sind.

Nachdem so unser nächstes Ziel bezeichnet ist, machen wir von dem Ergebniss des §. 76 Gebrauch, dass zwischen

$$v = f\left(\frac{c + \partial\,\omega}{a}\right)^3, \quad u = f(\omega)^3$$

eine Modulargleichung:

$$\Phi_n(u, v) = 0 \tag{7}$$

besteht, wenn

$$a\,\partial = n, \quad c \equiv 0 \pmod{16}$$

ist. Die hieraus abgeleitete Gleichung

$$\Phi_n(u, u) = 0 \tag{8}$$

ist dann und nur dann befriedigt, wenn

$$\frac{c + \partial\,\omega}{a} = \frac{\gamma + \delta\,\omega}{\alpha + \beta\,\omega}, \tag{9}$$

worin $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ eine lineare Transformation der ersten oder zweiten Classe ist, welche [nach §. 35, (11)] der Bedingung genügt:

$$\left(\frac{2}{\alpha - \beta}\right) e^{-\frac{\pi i}{8}(\alpha - \beta)(\alpha + \beta + \gamma - \delta)} = 1,$$

oder der damit gleichbedeutenden

$$\alpha\gamma + \beta\delta + 2\alpha^2 - 2\alpha\beta - 2\alpha\delta \equiv 0 \pmod{16}. \tag{10}$$

Aus (9) folgt aber, wenn $\omega$ der Gleichung (2) genügt, wie wir im vorigen Paragraphen gesehen haben,

$$n = y^2 + m x^2,$$

$$\begin{aligned} \alpha &= Bx - y, & n\gamma &= -\,Cx + c(Bx - y), \\ \beta &= Ax, & n\delta &= -\,Bx - y + Acx. \end{aligned} \tag{11}$$

Nehmen wir zunächst $m$ ungerade an, so können wir $n = m$, also $x = 1$, $y = 0$ setzen, und da $c$ durch 16 theilbar ist, folgt:

$$\alpha = B, \quad \beta = A, \quad \gamma \equiv -m\,C, \quad \delta \equiv -m\,B \pmod{8},$$

also ergiebt (10):

$$B\left(m\,\frac{A+C}{2} - (m+1)B + A\right) \equiv 0 \pmod{8}. \tag{12}$$

Wenn nun $m \equiv 3 \pmod{4}$, so ist $A + C \equiv 0 \pmod{4}$ und der in (12) in der Klammer stehende Ausdruck ungerade, daher ist (12) nur unter der Voraussetzung befriedigt, dass

$$B \equiv 0 \pmod{8}.$$

Wir wollen, um Wiederholungen zu vermeiden, bei den im Folgenden auszusprechenden Theoremen ein- für allemal voraussetzen, dass $\omega$ die Wurzel einer solchen Gleichung (3) der Determinante $-m$ sei, in der $A$ ungerade, $B$ durch 8 theilbar sei. Damit ist also das Theorem bewiesen:

II. Ist $m \equiv 3 \pmod{4}$, so ist $f(\omega)^6$ Classeninvariante.

Ist ferner $m \equiv 5 \pmod{8}$, so reducirt sich die Congruenz (12) auf:

$$B\left(\frac{5\,C - A}{2} + 2\,B\right) \equiv 0 \pmod{8}$$

und diese Bedingung ist erfüllt, wenn $B$ durch 4 theilbar ist, dagegen nicht erfüllt, wenn $B$ nur durch 2, nicht durch 4 theilbar ist. Daraus folgt:

III. Ist $m \equiv 5 \pmod{8}$, so ist $f(\omega)^{12}$ Classeninvariante.

Ist $m \equiv 1 \pmod{8}$, so lässt sich aus der Congruenz (12) nichts schliessen. Dies stimmt mit dem Umstande überein, dass in diesem Falle $\Phi_m(u, u)$ nur von $u^8$ abhängig ist. Um auch hier zu ähnlichen Resultaten zu gelangen, wenden wir die Transformation zweiter Ordnung an. Wir nehmen in (7):

$$n \equiv 1 \pmod{8} \tag{13}$$

und setzen:

$$u\,v = \pm \sqrt{2}^3,$$

d. h.:

$$f\left(\frac{c + \partial\,\omega}{a}\right)^3 f(\omega)^3 = \pm \sqrt{2}^3,$$

oder [§. 29, (18)]:

$$f\left(\frac{c + \partial\,\omega}{a}\right)^3 = \pm f\left(\frac{\omega - 1}{\omega + 1}\right)^3. \tag{14}$$

Die Gleichung (7) geht dadurch über in eine Gleichung:

$$\Phi_n\left(u, \frac{\pm\sqrt{2}^3}{u}\right) = 0, \tag{15}$$

oder genauer gesagt, je nach der Wahl des Vorzeichens in zwei Gleichungen, welche ausser dem Product

$$\sqrt{2}\, f(\omega)^2,$$

nur rationale Zahlcoëfficienten enthalten. Letzteres ersieht man daraus, dass in der Gleichung (7) nur solche Producte $u^h v^k$ vorkommen, in welchen $h + k$ gerade ist (vgl. den Anfang von §. 77).

Die Relation (14) fordert nun, dass $\omega$ einer Gleichung

$$\frac{c + \partial\omega}{a} = \frac{\gamma(\omega+1) + \delta(\omega-1)}{\alpha(\omega+1) + \beta(\omega-1)} \tag{16}$$

genüge, in welcher $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ eine zur ersten oder zweiten Classe gehörige lineare Transformation ist. Damit aber eine der beiden Gleichungen (15) wirklich erfüllt sei, ist nach §. 35, (11) noch erforderlich:

$$(\alpha-\beta)(\alpha+\beta+\gamma-\delta) \equiv 0 \pmod{8}. \tag{17}$$

Nun folgt aber, wenn $\omega$ Wurzel der quadratischen Gleichung (2) ist, aus (16) wie oben:

$$\begin{aligned}\partial(\alpha+\beta) &= Ax,\\ \partial(\alpha-\beta) &= Bx + y,\\ c(\alpha-\beta) - a(\gamma-\delta) &= Cx,\\ c(\alpha+\beta) - a(\gamma+\delta) &= Bx - y,\\ 2n &= y^2 + mx^2.\end{aligned} \tag{18}$$

Ist nun, wie vorausgesetzt war,

$$m \equiv 1 \pmod{8},$$

so setzen wir:

$$n = \frac{m+1}{2} \quad \text{oder} \quad \frac{m+9}{2},$$

je nachdem $m \equiv 1$ oder $\equiv 9 \pmod{16}$ ist, so dass auch $n \equiv 1 \pmod{8}$ wird, dann ist $x = 1$, $y = \pm 1$ oder $= \pm 3$ zu setzen, und wenn wir $A$ relativ prim zu $n$ voraussetzen, so wird $\partial = 1$, $a = n$ und aus (18) folgt:

$$\begin{aligned}\alpha + \beta &= A, & n(\gamma-\delta) &= -C + c(B+y),\\ \alpha - \beta &= B + y, & n(\gamma+\delta) &= -B + y + cA.\end{aligned}$$

Hiernach ergiebt die Bedingung (17), da $B + y$ ungerade, $c \equiv 0 \pmod{16}$ ist:

$$A \equiv C \pmod{8},$$

welche nur erfüllt ist, wenn $B \equiv 0 \pmod{4}$ ist. Um aber zu entscheiden, welche der beiden Gleichungen (15) erfüllt ist, kommt es nach §. 35, (11) darauf an, ob

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

oder, was dasselbe ist

$$(B + y)^2 - 1 + (B + y)(A - n\,C)$$

durch 16 oder nur durch 8 theilbar ist. Vermehrt man aber in diesem Ausdruck $B$ um ein ungerades Vielfache von 4, so verändert er sich um ein ungerades Vielfache von 8, woraus zu schliessen, dass, je nachdem $B \equiv 0$ oder $\equiv 4 \pmod{8}$, die eine oder die andere der beiden Gleichungen (15) befriedigt ist.

Damit ist bewiesen:

IV. Ist $m \equiv 1 \pmod{8}$, so ist $\sqrt{2} f(\omega)^6$ Classeninvariante.

In den Fällen, wo $m \equiv 3 \pmod{4}$ ist, können wir noch einen Schritt weiter gehen. Wir haben in §. 76 neben den Schlaefli'schen Modulargleichungen auch die Gleichungen

$$\Phi_n(u_1, v_1) = 0 \tag{19}$$

kennen gelernt, die zwischen

$$u_1 = f_1(\omega)^3, \quad v_1 = \left(\frac{2}{a}\right) f_1\left(\frac{c + \partial\,\omega}{a}\right)^3 \tag{20}$$

bestehen, und aus §. 76 (4) ergiebt sich, dass, wenn $n \equiv 7 \pmod{8}$ vorausgesetzt wird, $\Phi_n(u_1, v_1)$ rational durch

$$u_1 v_1, \quad u_1^8 + v_1^8$$

dargestellt werden kann. Wenn wir also in (19)

$$v_1 = f_1\left(\frac{c + \partial\,\omega}{a}\right)^3 = \pm f_2(\omega)^3, \quad u_1 = f_1(\omega)^3 \tag{21}$$

setzen, so wird

$$u_1 v_1 = \frac{\pm\sqrt{2}^3}{f(\omega)^3},$$

und $u_1^8 + v_1^8$ kann rational durch $f(\omega)^{24}$ ausgedrückt werden (§. 29), d. h. es geht

$$\Phi_n(u_1, v_1) = 0$$

in eine oder, nach der Wahl des Vorzeichens, zwei rationale Gleichungen für

$$\xi = \sqrt{2} f(\omega)^3$$

über, die wir mit

$$F(\pm \xi) = 0 \tag{22}$$

bezeichnen wollen.

Die Gleichung (18) hat aber wieder eine Gleichung der Form (21) zur Folge, so dass in beiden die Vorzeichen übereinstimmen, und die Gleichung (21) fordert nach §. 35, (7):

$$\frac{c + \partial \omega}{a} = \frac{\gamma + \delta \omega}{\alpha + \beta \omega}, \quad \delta \equiv 0 \pmod{2}, \tag{23}$$

$$\gamma^2 - 1 + \gamma(2\alpha - \delta) \equiv 0, 8 \pmod{16},$$

und zwar gilt, je nachdem die eine oder die andere Congruenz stattfindet, in (21) und (22) das eine oder das andere Vorzeichen.

Nehmen wir $m = n$, also $m \equiv -1 \pmod{8}$, so ergiebt sich ganz wie oben:

$$\beta = A, \quad n\gamma = -C + cB,$$
$$\alpha = B, \quad n\delta = -B + cA,$$

also aus (23):

$$C^2 - CB - 1 \equiv 0, 8 \pmod{16},$$

woraus zunächst folgt, dass $B$ jedenfalls durch 8 theilbar sein muss; vermehren wir aber $B$ um ein ungerades Vielfache von 8, so geht die eine dieser Congruenzen in die andere über, und in Folge dessen geht in (21) das eine in das andere Vorzeichen über. Für ein bestimmtes $\omega$ besteht also nur die eine der beiden Gleichungen (22) und es folgt:

V. Ist $m \equiv 7 \pmod{8}$, so ist $\sqrt{2} f(\omega)^3$ Classeninvariante.

Wenn wir einer durch alle bekannten Beispiele bestätigten Induction vertrauen dürfen, so besteht noch das folgende Theorem:

VI. Ist $m \equiv 3 \pmod{8}$, so ist $f(\omega)^3$ Classeninvariante.

Indessen fehlt hierfür noch der allgemeine Beweis.

Ist $m \equiv 2 \pmod{4}$, so wenden wir dasselbe Verfahren an, wie oben im Falle $m \equiv 1 \pmod{8}$.

Wir setzen:

$$2n = m + y^2 \tag{24}$$

und nehmen $y = 0$ oder $= \pm 2$, so dass $n \equiv 1 \pmod{4}$ wird.

Wenn wir dann in der Gleichung (19):

$$(25) \qquad v_1 = f_2\left(\frac{\omega}{2}\right)^3 = \frac{\sqrt{2}^3}{f_1(\omega)^3}, \quad u_1 = f_1(\omega)^3$$

setzen, so ergiebt sich eine Gleichung, welche nur $\sqrt{2} f_1(\omega)^6$ und rationale Coëfficienten enthält. (19) ist aber nur dann erfüllt [§. 35, (7)], wenn

$$(26) \qquad \frac{c + \partial\omega}{a} = \frac{2\gamma + \delta\omega}{2\alpha + \beta\omega}, \quad \delta \equiv 0 \pmod{2}$$

und ausserdem

$$(27) \qquad \gamma^2 - 1 + \gamma(2\alpha - \delta) \equiv 0 \pmod{16};$$

aus (26) und (24) folgt:

$$\left.\begin{array}{ll} 2\alpha = B + y, & 2n\gamma \equiv -C \\ \beta = A, & 2n\delta \equiv -(B - y) \end{array}\right\} \pmod{16}$$

und daraus schliesst man wie oben:

VII. Ist $m \equiv 2 \pmod 4$, so ist $\sqrt{2} f_1(\omega)^6$ Classeninvariante.

Wiederum weisen sämmtliche Beispiele darauf hin, dass, wenn $m \equiv 4 \pmod 8$ ist, $\sqrt{2} f_1(\omega)^4$ Classeninvariante ist. Aber auch hierfür fehlt noch der Beweis. Wenn $m$ durch 8 theilbar ist, tritt eine Reduction nicht ein.

Die Classeninvarianten $f(\omega)$ eignen sich ganz besonders zur numerischen Berechnung, weil sie unter allen die denkbar einfachsten Resultate liefern. Wir geben daher zunächst eine grössere Reihe von Beispielen, die sich auf Grund unserer bisherigen Entwickelungen leicht ableiten lassen, und die zugleich die Methoden kennen lehren, deren man sich auch zu weiter fortgesetzten Rechnungen dieser Art bedienen kann.

Es wird bei diesen Berechnungen häufig die Aufgabe gestellt, reducible, ganze rationale Functionen in Factoren zu zerlegen. Eine solche Zerlegung ist, wenn sie gefunden ist, natürlich sofort zu verificiren; aber auch das Auffinden der Factoren gelingt leicht, wenigstens soweit die Rechnungen bis jetzt fortgesetzt sind, da man häufig in den späteren Fällen früher gefundene Resultate benutzen kann und überdies die allgemeine Form der Factoren kennt. Beispiele werden dies erläutern.

## §. 95. Die ersten Fälle der Berechnung von $f(\sqrt{-m})$.

Setzen wir in der cubischen Gleichung

(1) $$u^3 - \gamma_2(\omega) u - 16 = 0,$$

deren Wurzeln nach §. 49

$$f(\omega)^8, \quad -f_1(\omega)^8, \quad -f_2(\omega)^8$$

sind $\omega = i$, also [§. 92, (16)], $\gamma_2 = 12$, so folgt:

$$u^3 - 12u - 16 = 0,$$

eine Gleichung, welche die einzige positive Wurzel $u = 4$ hat, so dass wir in Uebereinstimmung mit §. 85 und §. 93 erhalten:

(2) $$f(i) = \sqrt[4]{2};$$

setzen wir $\omega = \sqrt{-2}$, also $\gamma_2 = 20$ (§. 92, (17)], so erhalten wir aus (1) die Gleichung:

$$u^3 - 20u - 16 = 0$$

mit der einzigen rationalen Wurzel $-4$. Da aber nach den Sätzen der beiden vorhergehenden Paragraphen $f_1(\sqrt{-2})^8$ rational sein muss, so ist:

(3) $$f_1(\sqrt{-2}) = \sqrt[4]{2}.$$

Wir setzen ferner $\omega = e^{\frac{2\pi i}{3}}$, also $\gamma_2(\omega) = 0$ (§. 88) und erhalten aus (1):

$$u^3 = 16.$$

Dieser Gleichung genügt [§. 29, (19)]:

$$u = -f_2\left(\frac{-1+\sqrt{-3}}{2}\right)^8 = \frac{16\, e^{\frac{2\pi i}{3}}}{f(\sqrt{-3})^8},$$

woraus der reelle positive Werth:

(4) $$f(\sqrt{-3}) = \sqrt[3]{2}.$$

Um die übrigen Resultate des §. 92 anwenden zu können, setzen wir

$$m = 7, \quad 11, \quad 19, \quad 43, \quad 67, \quad 163,$$

und benutzen die aus §. 29, (19) folgende Formel:

$$f(\omega) f_2\left(\frac{-3+\omega}{2}\right) = e^{-\frac{\pi i}{8}} \sqrt{2}.$$

Demnach ist, wenn wir

$$f(\sqrt{-m}) = x$$

setzen, $x$ nach (1) die reelle positive Wurzel der Gleichung

$$x^{24} + \gamma_2\left(\frac{-3+\sqrt{-m}}{2}\right) x^{16} - 2^8 = 0. \tag{5}$$

Für $m = 7$ erhalten wir nach §. 92, (18)

$$f(\sqrt{-7}) = \sqrt{2}, \tag{6}$$

während in den anderen Fällen, nach Einsetzen der Werthe für $\gamma_2$, sich die Gleichung (5) erst in zwei Factoren 12ten, diese wieder in zwei Factoren 6ten und schliesslich diese in zwei 3ten Grades spaltet. Die so erhaltenen Gleichungen sind cubische Gleichungen für $x^8$, $x^4$, $x^2$, $x$, von denen wir jedesmal nur die beibehalten, welche eine reelle positive Wurzel hat, welcher schliesslich $f(\sqrt{-m})$ selbst genügt.

Um die erste Zerlegung zu finden, setzen wir die Gleichung (5) in die Form:

$$(x^{12} - a x^4)^2 - (b x^8 + c)^2 = 0$$

und haben die ganzen Zahlen $a$, $b$, $c$ aus den Gleichungen:

$$2a + b^2 = -\gamma_2, \quad 2bc = a^2, \quad c^2 = 2^8$$

zu bestimmen, also $c = \pm 16$; die Gleichung 12ten Grades mit positiver Wurzel lautet also:

$$x^{12} - b x^8 - a x^4 - 16 = 0.$$

Die Zahlen $a$, $b$ bestimmen sich aus den obigen Gleichungen leicht, und so findet man schliesslich die gesuchten cubischen Gleichungen. Man erhält z. B. für $m = 11$ successive

$$x^{12} - 8x^8 + 16x^4 - 16 = 0,$$
$$x^6 - 4x^2 - 4 = 0,$$
$$x^3 - 2x^2 + 2x - 2 = 0.$$

In den fünf Fällen des §. 92 findet man folgende Gleichungen:

$$x = f(\sqrt{-11}), \quad x^3 - 2x^2 + 2x - 2 = 0, \tag{7}$$
$$x = f(\sqrt{-19}), \quad x^3 - 2x - 2 = 0, \tag{8}$$
$$x = f(\sqrt{-43}), \quad x^3 - 2x^2 - 2 = 0, \tag{9}$$
$$x = f(\sqrt{-67}), \quad x^3 - 2x^2 - 2x - 2 = 0, \tag{10}$$
$$x = f(\sqrt{-163}), \quad x^3 - 6x^2 + 4x - 2 = 0. \tag{11}$$

## §. 96. Anwendung der Transformation zweiter Ordnung zur Berechnung von Classeninvarianten.

Die Transformation zweiter Ordnung lässt sich, wenn nöthig in mehrmaliger Wiederholung, auf alle solche Determinanten $-m$ anwenden, für welche $y^2 + m x^2$ eine Potenz von 2 ist, also z. B. auf $m = 7, 15, 23, 31$.

Diese Rechnungen sind aber beschwerlich und wir werden einfachere Wege finden, um in diesen Fällen zum Ziele zu kommen. Bessere Dienste leistet die Transformation zweiter Ordnung, um aus einer bekannten Classeninvariante eine neue zu finden, die zu einer Determinante gehört, welche das Vierfache der ersteren ist.

Dazu führen folgende Formeln:

Nach §. 29 ist:

$$f_1(\omega)^8 + f_2(\omega)^8 = f(\omega)^8,$$

$$f_1(\omega)^8 f_2(\omega)^8 = \frac{16}{f(\omega)^8},$$

woraus

$$f_1(\omega)^8 - f_2(\omega)^8 = \frac{\sqrt{f(\omega)^{24} - 64}}{f(\omega)^4}.$$

Das Vorzeichen der Wurzel wechselt nur für $f(\omega)^{24} = 64$, also für $\omega = i$, und ist, so lange $-i\omega$ reell und grösser als 1 ist, positiv zu nehmen, da die linke Seite für ein verschwindendes $q$ positiv unendlich wird. Es ergiebt sich daraus:

$$2 f_2(\omega)^8 = \frac{f(\omega)^{12} - \sqrt{f(\omega)^{24} - 64}}{f(\omega)^4},$$

oder

$$f_2(\omega)^8 f(\omega)^4 \left[f(\omega)^{12} + \sqrt{f(\omega)^{24} - 64}\right] = 32,$$

und auf dieselbe Weise:

$$f_2(\omega)^8 f_1(\omega)^4 \left[f_1(\omega)^{12} + \sqrt{f_1(\omega)^{24} + 64}\right] = 32.$$

Ferner ist nach §. 29, (16):

$$f_1(2\omega) f_2(\omega) = \sqrt{2},$$

woraus

$$(1) \qquad \begin{aligned} 2 f_1(2\omega)^8 &= f(\omega)^4 \left[f(\omega)^{12} + \sqrt{f(\omega)^{24} - 64}\right], \\ &= f_1(\omega)^4 \left[f_1(\omega)^{12} + \sqrt{f_1(\omega)^{24} + 64}\right]. \end{aligned}$$

Diese Formeln können dazu dienen, wenn $f(\omega)$ oder $f_1(\omega)$ bekannt ist, $f_1(2\omega)$ zu berechnen, also $f_1(\sqrt{-4m})$ aus $f(\sqrt{-m})$

oder $f_1(\sqrt{-m})$. Auf diese Weise findet man sehr leicht, wenn man aus den Formeln des vorigen Paragraphen $f(i)$, $f_1(\sqrt{-2})$, $f(\sqrt{-3})$, $f(\sqrt{-7})$ entnimmt:

(2) $f_1(\sqrt{-4})^8 = 8$,

(3) $f_1(\sqrt{-16})^8 = 8\sqrt{2}(1+\sqrt{2})^2$,

(4) $f_1(\sqrt{-8})^8 = 8(1+\sqrt{2})$,

(5) $f_1(\sqrt{-32})^8 = 32(1+\sqrt{2})^2 + 8\sqrt{2}\sqrt{8(1+\sqrt{2})^4+(1+\sqrt{2})}$.

Setzen wir:

$$f_1(\sqrt{-32})^8 = 8x,$$

so ist $x$ Wurzel der biquadratischen Classengleichung:

$$(x^2 - 24x - 2)^2 - 8(8x+1)^2 = 0, \tag{6}$$

welche durch Adjunction von $\sqrt{2}$ in zwei quadratische Gleichungen

$$x^2 - 8(1 \pm \sqrt{2})^2 x - 2(1 \pm \sqrt{2}) = 0$$

zerfällt. Ferner finden wir so:

$$f_1(\sqrt{-12})^4 = 2\sqrt[6]{2}(1+\sqrt{3}), \tag{7}$$

$$f_1(\sqrt{-28})^4 = 2\sqrt{2}(3+\sqrt{7}). \tag{8}$$

Auf andere Fälle werden wir diese Methode später noch anwenden.

## §. 97. Berechnung von Classeninvarianten aus den Schlaefli'schen Modulargleichungen.

I. Wenn wir in einer der Gleichungen zwischen $u = f(\omega)$ und $v = f(n\omega)$ oder zwischen $u = f_1(\omega)$, $v = f_1(n\omega)$ (§. 76), für $u$ einen der bekannten Werthe von $f(\sqrt{-m})$ oder $f_1(\sqrt{-m})$ einsetzen, so erhalten wir eine Gleichung, welcher $f(\sqrt{-n^2m})$ oder $f_1(\sqrt{-n^2m})$ genügt.

Diese Gleichung enthält unter Umständen noch fremde Factoren, die man aufzusuchen und zu beseitigen hat.

Ist $n$ eine Primzahl, so erhalten wir nach §. 90 vollständigen Aufschluss über diese überflüssigen Factoren. Geht $n$ in $m$ auf, so ist in der betreffenden Gleichung ein zur Determinante $-m$ gehöriger Linearfactor abzusondern, ist $-m$ quadratischer Nichtrest von $n$, so sind überflüssige Factoren überhaupt nicht vorhanden, ist $-m$ quadratischer Rest von $n$, so ist ein zur Determinante $-m$ gehöriger quadratischer Factor abzusondern, und wenn $m = 1$ ist, so ist die nach Absonderung der fremden Factoren übrig bleibende Gleichung ein Quadrat.

Als Beispiele für diese Fälle nehmen wir:

1. $m = 3$, $n = 3$, Absonderung eines Linearfactors.
2. $m = 2$, $n = 5$, kein fremder Factor.
3. $m = 2$, $n = 3$, Absonderung eines quadratischen Factors.
4. $m = 1$, $n = 3$, Quadrat.
5. $m = 1$, $n = 5$, Quadrat nach Absonderung eines quadratischen Factors.
6. $m = 1$, $n = 7$, Quadrat.

Im Falle 1. hat man in der auf den Transformationsgrad $n = 3$ bezüglichen Formel des §. 76 zu setzen:

$$u^3 = 2, \quad v^3 = f(\sqrt{-27})^3 = 2x,$$

also

$$A = x^2 + \frac{1}{x^2}, \quad B = 4x - \frac{2}{x},$$

und folglich:

$$x^4 - 4x^3 + 2x + 1 = (x-1)(x^3 - 3x^2 - 3x - 1) = 0,$$

so dass man für $m = 27$ erhält:

$$(1) \qquad f(\sqrt{-27})^3 = 2x, \quad x^3 - 3x^2 - 3x - 1 = 0.$$

Im Falle 2. setzen wir im System II des §. 76 ($n = 5$):

$$u_1 = f_1(\sqrt{-2}) = \sqrt[4]{2}, \quad v_1 = f_1(\sqrt{-50}) = \sqrt[4]{2}\,x,$$

$$A_1 = \frac{1}{x^3} - x^3, \qquad B_1 = 2\left(x^2 + \frac{1}{x^2}\right),$$

so dass man (ohne fremden Theiler) die Gleichung 6ten Grades:

$$(2) \qquad \frac{1}{x^3} - x^3 + 2\left(x^2 + \frac{1}{x^2}\right) = 0, \quad f_1(\sqrt{-50}) = \sqrt[4]{2}\,x$$

erhält, die sich für

$$y = \frac{1}{x} - x,$$

auf den dritten Grad reducirt:

$$(3) \qquad y^3 + 2y^2 - 3y + 4 = 0.$$

Im Falle 3. setzen wir im System II des §. 76 ($n = 3$):

$$u_1 = \sqrt[4]{2}, \quad v_1^3 = f_1(\sqrt{-18})^3 = \sqrt[4]{2}\,x,$$

$$A_1 = \frac{2}{x^2} - \frac{x^2}{2}, \quad B_1 = 2x + \frac{4}{x},$$

$$x^4 - 4x^3 - 8x - 4 = (x^2 + 2)(x^2 - 4x - 2),$$

also

$$x^2 - 4x - 2 = 0, \quad f_1(\sqrt{-18})^3 = \sqrt[4]{2}\,x. \tag{4}$$

Die Auflösung von (4) ergiebt:

$$x = 2 + \sqrt{6}. \tag{5}$$

Im Falle 4. ist:

$$u = f(i) = \sqrt[4]{2}, \quad v^3 = f(\sqrt{-9})^3 = \sqrt[4]{2}\,x,$$

$$A = \frac{x^2}{2} + \frac{2}{x^2}, \quad B = 2x - \frac{4}{x},$$

$$x^4 - 4x^3 + 8x + 4 = (x^2 - 2x - 2)^2 = 0,$$

also

$$x^2 - 2x - 2 = 0, \quad f(\sqrt{-9})^3 = \sqrt[4]{2}\,x, \tag{6}$$

$$x = 1 + \sqrt{3}. \tag{7}$$

Im Falle 5.:

$$u = f(i) = \sqrt{2}, \quad v = f(\sqrt{-25}) = \sqrt[4]{2}\,x,$$

$$A = x^3 + \frac{1}{x^3}, \quad B = 2\left(x^2 - \frac{1}{x^2}\right),$$

$$x^3 + \frac{1}{x^3} - 2\left(x^2 - \frac{1}{x^2}\right) = \left(x + \frac{1}{x}\right)\left(x - \frac{1}{x} - 1\right)^2 = 0.$$

$$x - \frac{1}{x} - 1 = 0, \quad f(\sqrt{-25}) = \sqrt[4]{2}\,x, \tag{8}$$

$$x = \frac{1 + \sqrt{5}}{2}. \tag{9}$$

Endlich setzen wir für $n = 7$:

$$u = \sqrt[4]{2}, \quad v = f(\sqrt{-49}) = \frac{x}{\sqrt[4]{2}}$$

und finden

$$\begin{aligned} 0 &= (x^8 - 4x^7 + 28x^4 - 32x + 16) \\ &= (x^4 - 2x^3 - 2x^2 - 4x + 4)^2, \end{aligned}$$

woraus leicht durch Auflösung einer quadratischen Gleichung:

$$x + \frac{2}{x} = 1 + \sqrt{7}, \quad x = \sqrt[4]{2}\, f(\sqrt{-49}) \tag{10}$$

Auf dieselbe Weise sind die in der unten folgenden Tabelle aufgeführten Classeninvarianten für

$$m = 75,\quad 36,\quad 100,\quad 63,\quad 175$$

berechnet, und diese Rechnungen lassen sich auch noch weiter fortsetzen.

II. Aus den Schlaefli'schen Modulargleichungen lässt sich noch auf verschiedene andere Arten für die Berechnung von Classeninvarianten Nutzen ziehen.

Setzen wir

$$\omega = -\frac{m}{\omega},\quad \omega = \sqrt{-m},$$

so wird

$$f(\omega) = f\left(\frac{\omega}{m}\right) = f(\sqrt{-m}); \tag{11}$$

wenn also in der Modulargleichung für den Transformationsgrad $m$

$$u = v$$

gesetzt wird, so ergiebt sich eine Gleichung, unter deren Wurzeln $u = f(\sqrt{-m})$ vorkommt. In dem Systeme I. des §. 76 ist dann immer $A = 2$ zu setzen und es ergeben sich die Formeln:

$$m = 3,\quad B = u^6 - \frac{8}{u^6} = 2,$$

$$m = 5,\quad B = u^4 - \frac{4}{u^4} = 2,$$

$$m = 7,\quad B = u^6 + \frac{8}{u^6} = 9,$$

$$m = 11,\quad B = u^2 - \frac{2}{u^2},\quad B^5 - B^3 - 2B = 2,$$

$$m = 13,\quad B = u^{12} - \frac{64}{u^{12}} = 9 \,.\, 2^5,$$

$$m = 17,\quad B = u^8 + \frac{16}{u^8},\quad B^2 - 68B - 544 = 0,$$

$$m = 19,\quad B = u^6 - \frac{8}{u^6},\quad B^3 - 38B^2 + 252B - 648 = 0.$$

Die Fälle $m = 3, 7, 11, 19$ ergeben keine neuen Resultate, können aber zur Verificirung der früher gefundenen verwandt werden; aus $m = 5, 13$ erhalten wir direct durch Auflösung einer quadratischen Gleichung:

(12) $$f(\sqrt{-5})^4 = 1 + \sqrt{5},$$

(13) $$f(\sqrt{-13})^4 = 3 + \sqrt{13}.$$

Für $m = 17$ ist die Classenzahl 4, also die oben angegebene Gleichung, welche in Bezug auf $u^8$ vom 4ten Grade ist, die Classengleichung. Löst man sie in Bezug auf $B$ auf, so erhält man:

$$u^8 + \frac{16}{u^8} = 34 + 10\sqrt{17},$$

$$u^4 + \frac{4}{u^4} = 5 + \sqrt{17},$$

$$\left(u^2 + \frac{2}{u^2}\right)^2 = \frac{(1 + \sqrt{17})^2}{2}.$$

Wenn man also

$$\sqrt{2}\,x = f(\sqrt{-17})^2$$

setzt, so erhält man für $x$ die quadratische Gleichung:

(14) $$x + \frac{1}{x} = \frac{1 + \sqrt{17}}{2}.$$

III. Wir setzen für $\omega$ die Wurzel der quadratischen Gleichung:

$$2\,\omega^2 + 2\,r\,\omega + n = 0,$$

worin $n$ eine ungerade ganze Zahl bedeutet und $r$ eine ganze Zahl, deren Quadrat kleiner als $2\,n$ ist, also:

(15) $$2\,\omega + 2\,r = -\frac{n}{\omega},$$

(16) $$\omega = \frac{-r + \sqrt{-m}}{2}, \quad m = 2\,n - r^2.$$

Es ist dann nach §. 29:

(17) $$f_2(\omega) f_1(2\,\omega + 2\,r) = e^{-\frac{r\pi i}{12}}\sqrt{2},$$

und nach (15), (16):

(18) $$f_2(\omega) f_2\left(\frac{\omega}{n}\right) = e^{-\frac{r\pi i}{12}}\sqrt{2},$$

(19) $$f_2(\omega) = \frac{e^{-\frac{r\pi i}{12}}\sqrt{2}}{f_1(r + \sqrt{-m})},$$

setzen wir also, je nachdem $r$ und folglich auch $m$ gerade oder ungerade ist,

(20) $$x = f_1(\sqrt{-m}), \quad x = f(\sqrt{-m}),$$

so wird

$$(21) \qquad f_2(\omega) = \frac{e^{-\frac{r\pi i}{24}}\sqrt{2}}{x}, \quad f_2\left(\frac{\omega}{n}\right) = e^{-\frac{r\pi i}{24}}x,$$

und diese Werthe hat man für $u_1$, $v_1$ in das System II, §. 76 zu substituiren, um eine Gleichung für $x$ zu erhalten.

Indem man für $r$ die verschiedenen zulässigen Werthe setzt, bekommt man aus (16):

$n = 3$, $m = 6, 5, 2$,
$n = 5$, $m = 10, 9, 6, 1$,
$n = 7$, $m = 14, 13, 10, 5$,
$n = 11$, $m = 22, 21, 18, 13, 6$,
$n = 13$, $m = 26, 25, 22, 17, 10, 1$,
$n = 17$, $m = 34, 33, 30, 25, 18, 9$,
$n = 19$, $m = 38, 37, 34, 29, 22, 13, 2$.

Als einfaches Beispiel wählen wir $n = 7$, und erhalten:

$$\frac{x^8}{4} + \frac{4}{x^8} = 7 + 4\sqrt{2}\cos\frac{r\pi}{4}.$$

Daraus ergiebt sich für $r = 0$:

$$(22) \qquad \frac{x^2}{\sqrt{2}} + \frac{\sqrt{2}}{x^2} = 1 + \sqrt{2}, \quad x = f_1(\sqrt{-14}),$$

für $r = 1$ das bereits bekannte

$$(23) \qquad f(\sqrt{-13})^4 = 3 + \sqrt{13},$$

für $r = 2$:

$$(24) \qquad f_1(\sqrt{-10})^2 = \frac{1+\sqrt{5}}{\sqrt{2}}.$$

Als zweites Beispiel nehmen wir noch $n = 13$, und erhalten:

$$(25) \qquad A_1 = \frac{\sqrt{2}}{x^2} - \frac{x^2}{\sqrt{2}}, \quad B_1 = 16\cos\frac{r\pi}{2};$$

für $r = 0, 4$ also $m = 26, 10$ ergiebt sich hieraus $B_1 = 16$, und folglich nach §. 76:

$$A_1^7 - 6A_1^5 + A_1^3 + 20A_1 + 16 = 0,$$

während für $r = 2$, also $m = 22$ in dieser Gleichung $A_1$ in $-A_1$ zu verwandeln ist.

Man findet aber leicht die Zerlegung:

$$\begin{aligned} &A_1^7 - 6A_1^5 + A_1^3 + 20A_1 + 16 \\ &= (A_1 + 1)^2 (A_1 - 2)^2 (A_1^3 + 2A_1^2 + A_1 + 4). \end{aligned} \tag{26}$$

Ist $-i\omega > \sqrt{2}$, so ist auch $f_1^2(\omega) > \sqrt{2}$, denn $f_1(\omega)^2$ geht, während $-i\omega$ von $\sqrt{2}$ bis $\infty$ geht, ebenfalls, und zwar stets wachsend[1]), von $\sqrt{2}$ bis $\infty$, und folglich ist $A_1$ negativ für $r = 0, 2, 4$.

Der erste Factor $A_1 + 1$ verschwindet, wie aus dem schon bekannten Resultat (24) hervorgeht, für $r = 4$; daher verschwindet der dritte Factor $A_1^3 + 2A_1^2 + A_1 + 4$ für $r = 0$, während $A_1 + 2$ für $r = 2$ verschwindet.

Wir erhalten also nach (25):

$$f_1(\sqrt{-10})^2 = \sqrt{2}\,y, \quad y - \frac{1}{y} = 1, \tag{27}$$

$$f_1(\sqrt{-22})^2 = \sqrt{2}\,y, \quad y - \frac{1}{y} = 2, \tag{28}$$

$$f_1(\sqrt{-26})^2 = \sqrt{2}\,y, \; y^6 - 2y^5 - 2y^4 + 2y^2 - 2y - 1 = 0. \tag{29}$$

IV. Als Beispiel für eine andere Art der Verwendung der Schlaefli'schen Modulargleichungen, welche zu den Classeninvarianten der sonst schwer zugänglichen Determinante $-41$ führt, möge das Folgende dienen.

Wir setzen:

$$2n\omega^2 + 2r\omega + n = 0, \tag{30}$$

$$\omega = \frac{-r + \sqrt{-m}}{2n}, \quad m = 2n^2 - r^2. \tag{31}$$

Es kann hierin $r$ jede Zahl bedeuten, die $m$ positiv macht, die aber mit $n$ keinen Theiler gemeinschaftlich hat [weil sonst (30) imprimitiv ist]. Es wird also nach §. 29:

$$\begin{gathered} f_2\left(\frac{\omega}{n}\right) = f_1[2(n\omega + r)] = \frac{e^{-\frac{r\pi i}{12}}\sqrt{2}}{f_2(n\omega)}, \\ f_1[2(n\omega + r)] = f_1(r + \sqrt{-m}) = e^{-\frac{r\pi i}{24}}\,x, \end{gathered} \tag{32}$$

---

[1]) Aus §. 49, (11) folgt nämlich durch die Substitution $\left(\omega,\ 1 - \frac{1}{\omega}\right)$:

$$d f_1(\omega)^8 = -\frac{\pi i}{3}\vartheta_{10}^{h}\,[f(\omega)^8 + f_1(\omega)^8]\,d\omega.$$

also

$$f_2\left(\frac{\omega}{n}\right) = e^{-\frac{r\pi i}{24}}\, x,$$

$$f_2(n\,\omega) = \frac{e^{-\frac{r\pi i}{24}}\sqrt{2}}{x},$$

wenn, je nachdem $r$ gerade oder ungerade ist,

$$(33) \qquad x = f_1(\sqrt{-m}) \quad \text{oder} \quad = f(\sqrt{-m})$$

gesetzt wird. Nehmen wir also in der zu $n$ gehörigen Modulargleichung II, §. 76:

$$u_1 = f_2(\omega),$$

$$v_1 = \left(\frac{2}{n}\right) f_2(n\,\omega) = \left(\frac{2}{n}\right) \frac{e^{-\frac{r\pi i}{24}}\sqrt{2}}{x}$$

oder

$$v_1 = f_2\left(\frac{\omega}{n}\right) = e^{-\frac{r\pi i}{24}}\, x,$$

so ergeben sich zwei Gleichungen, aus welchen man durch Elimination von $u_1$ eine Gleichung für $x$ herleitet.

Um für $n = 5$ diese Rechnung durchzuführen, setzen wir:

$$(34) \qquad \begin{aligned} x f_2(\omega) &= \sqrt{2}\, e^{-\frac{5r\pi i}{24}}\, \xi, \\ \frac{x}{f_2(\omega)} &= e^{\frac{5r\pi i}{24}}\, \eta, \end{aligned}$$

woraus man, entsprechend den beiden Annahmen für $v_1$, für ein ungerades $r$ die Gleichungen erhält:

$$(35) \qquad \begin{aligned} \xi^3 + \frac{1}{\xi^3} + 2\left(\eta^2 - \frac{1}{\eta^2}\right) &= 0, \\ \eta^3 + \frac{1}{\eta^3} + 2\left(\xi^2 - \frac{1}{\xi^2}\right) &= 0. \end{aligned}$$

Diese Gleichungen gelten für $r = 1, 3, 7$, welche zu den Werthen $m = 49, 41, 1$ gehören.

Subtrahirt man die beiden Gleichungen (35), so kann man den Factor $\xi - \eta$ abwerfen, welcher nur für $m = 1$ verschwinden kann:

$$[(\xi + \eta)^2 - \xi\,\eta]\left(1 - \frac{1}{\xi^3\,\eta^3}\right) - 2\,(\xi + \eta)\left(1 + \frac{1}{\xi^2\,\eta^2}\right) = 0,$$

und wenn man die beiden Gleichungen (35) addirt:

$$[(\xi + \eta)^3 - 3\,\xi\,\eta\,(\xi + n)]\left(1 + \frac{1}{\xi^3\,\eta^3}\right)$$
$$+ 2\,[(\xi + \eta)^2 - 2\,\xi\,\eta]\left(1 - \frac{1}{\xi^2\,\eta^2}\right) = 0.$$

Es ist aber nach (34):

$$\sqrt{2}\,\xi\,\eta = x^2,$$

und man erhält also eine Gleichung für $x^2$, wenn man $(\xi + \eta)$ eliminirt. Diese Gleichung wird nach dem gewöhnlichen Eliminationsverfahren, wenn man

$$z = \frac{x^2}{\sqrt{2}} + \frac{\sqrt{2}}{x^2}$$

setzt, in der Form

$$(36)\quad z^6 - 9\,z^5 + 20\,z^4 + 6\,z^3 - 19\,z^2 - 17\,z - 6 = 0$$

gefunden. Hierin ist nun noch der auf die Determinante $-49$ bezügliche Factor enthalten. Für diesen ist aber [nach Formel (10)]:

$$z = 2 + \sqrt{7}.$$

Es muss also die linke Seite von (36) durch

$$z^2 - 4\,z - 3$$

theilbar sein und die Ausführung der Division ergiebt den für die Determinante $-41$ gültigen Factor:

$$(37)\quad \begin{gathered} z^4 - 5\,z^3 + 3\,z^2 + 3\,z + 2 = 0, \\ z = \frac{f(\sqrt{-41})}{\sqrt{2}} + \frac{\sqrt{2}}{f(\sqrt{-41})}. \end{gathered}$$

## §. 98. Berechnung von Classeninvarianten aus den irrationalen Formen der Modulargleichungen.

In ausserordentlich einfacher Weise führen vielfach die irrationalen Formen der Modulargleichungen zur Aufstellung von Classengleichungen.

1. Im §. 78 haben wir gesehen, dass, falls $m \equiv -1 \pmod 8$ ist, zwischen den beiden Functionen

$$2\,A = f(\omega)f(m\,\omega) + (-1)^{\frac{m+1}{8}}\,[f_1(\omega)f_1(m\,\omega) + f_2(\omega)f_2(m\,\omega)],$$

$$B = \frac{2}{f_1(\omega)f_1(m\,\omega)} + \frac{2}{f_2(\omega)f_2(m\,\omega)} + \frac{(-1)^{\frac{m+1}{8}}\,2}{f(\omega)f(m\,\omega)}$$

eine algebraische Gleichung besteht, und diese Gleichungen sind dort für $m = 7, 23, 31, 47, 71$ aufgestellt.

Setzen wir darin:

$$\omega = \frac{-1}{\sqrt{-m}}, \quad m\omega = \sqrt{-m}, \quad f(\sqrt{-m}) = \sqrt{2}\,x,$$

so wird nach §. 29:

$$A = x^2 + \frac{(-1)^{\frac{m+1}{8}}}{x}, \quad B = 4x + \frac{(-1)^{\frac{m+1}{8}}}{x^2}.$$

Daraus ergiebt sich z. B. für $m = 23$, wo $A = 1$ ist, die Gleichung:

(1) $$f(\sqrt{-23}) = \sqrt{2}\,x, \quad x^3 - x - 1 = 0$$

und für $m = 31$:

$$x^9 - 4x^6 + 3x^3 - 1 = 0.$$

Dies ist zunächst eine cubische Gleichung für $x^3$; man spaltet daraus aber leicht die cubische Gleichung für $x$ selbst ab:

(2) $$f(\sqrt{-31}) = \sqrt{2}\,x, \quad x^3 - x^2 - 1 = 0.$$

Aehnlich ergeben sich die Gleichungen:

(3) $$f(\sqrt{-47}) = \sqrt{2}\,x,$$
$$x^5 - x^3 - 2x^2 - 2x - 1 = 0,$$

(4) $$f(\sqrt{-71}) = \sqrt{2}\,x,$$
$$x^7 - 2x^6 - x^5 + x^4 + x^3 + x^2 - x - 1 = 0.$$

Im letzten Falle, $m = 71$, ist von der unmittelbar erhaltenen Gleichung 9ten Grades der der Aufgabe fremde Factor $(x + 1)^2$ abgesondert.

2. Um zu einer weiteren Berechnungsart zu gelangen, wenden wir die Transformation zweiter Ordnung an. Wir haben zunächst allgemein [für ein veränderliches $\omega$, §. 29, (17)]:

$$f(2\omega)^8 + f_2(2\omega)^8 = 2\,\frac{f(\omega)^8 + f_1(\omega)^8}{f_2(\omega)^4},$$

$$f(2\omega)^8 - f_2(2\omega)^8 = \frac{16}{f_2(\omega)^8},$$

woraus

$$f(2\omega)^8 = \frac{f(\omega)^8 + f_1(\omega)^8}{f_2(\omega)^4} + \frac{8}{f_2(\omega)^8},$$

$$f_2(2\omega)^8 = \frac{f(\omega)^8 + f_1(\omega)^8}{f_2(\omega)^4} - \frac{8}{f_2(\omega)^8},$$

daraus

$$f(\omega)^8 f(2\omega)^8 + f_1(\omega)^8 f_2(2\omega)^8 = 8 + \frac{[f(\omega)^8 + f_1(\omega)^8]^2}{f_2(\omega)^4},$$

was sich nach §. 29 leicht in die Form bringen lässt

$$[f(\omega)^4 f(2\omega)^4 + f_1(\omega)^4 f_2(2\omega)^4]^2 = 16 + f_2(\omega)^{12} + \frac{64}{f_2(\omega)^{12}},$$

und hieraus kann die Wurzel gezogen werden:

$$(5) \qquad f(\omega)^4 f(2\omega)^4 + f_1(\omega)^4 f_2(2\omega)^4 = f_2(\omega)^6 + \frac{8}{f_2(\omega)^6}.$$

Es genüge nun $\omega$ der quadratischen Gleichung:

$$(6) \qquad 2\omega^2 + 2r\omega + n = 0$$

mit ungeradem $n$, also:

$$(7) \qquad \omega = \frac{-r + \sqrt{-m}}{2}, \quad m = 2n - r^2.$$

Wenn dann

$$(8) \qquad \sqrt{2}\,x = f(\sqrt{-m})^2, \quad \text{oder} \quad = f_1(\sqrt{-m})^2$$

gesetzt wird, je nachdem $r$ ungerade oder gerade ist, so wird

$$(9) \qquad f_2(\omega)^2 = e^{-\frac{r\pi i}{12}} \frac{\sqrt{2}}{x}.$$

Ferner folgt aus

$$2\omega = -\frac{n}{\omega} - 2r$$

nach den Formeln des §. 29:

$$f(2\omega) = f\left(\frac{\omega}{n}\right) e^{\frac{r\pi i}{12}}$$

$$(10) \qquad f_1(2\omega) = f_2\left(\frac{\omega}{n}\right) e^{\frac{r\pi i}{12}}$$

$$f_2(2\omega) = f_1\left(\frac{\omega}{n}\right) e^{-\frac{r\pi i}{6}},$$

so dass die Gleichung (5) ergiebt:

$$(11) \qquad f(\omega)^4 f\left(\frac{\omega}{n}\right)^4 + (-1)^r f_1(\omega)^4 f_1\left(\frac{\omega}{n}\right)^4$$

$$= e^{-\frac{r\pi i}{12}} \sqrt{8} \left(x^3 + \frac{e^{-\frac{r\pi i}{2}}}{x^3}\right).$$

Aus (10) folgt noch weiter:

$$(12) \qquad f_2(\omega) f_2\left(\frac{\omega}{n}\right) = \sqrt{2}\, e^{-\frac{r\pi i}{12}},$$

$$(13) \qquad f(\omega) f\left(\frac{\omega}{n}\right) f_1(\omega) f_1\left(\frac{\omega}{n}\right) = \sqrt{2}\, e^{\frac{r\pi i}{12}}.$$

Wenn wir $n = 23$ und $r = 0$ annehmen, so giebt die Gleichung §. 78, (8) mit Benutzung von (12):

$$(14) \qquad f(\omega) f\left(\frac{\omega}{n}\right) - f_1(\omega) f_1\left(\frac{\omega}{n}\right) = 2 + \sqrt{2},$$

woraus durch zweimaliges Quadriren mit Benutzung von (11) und (13) folgt:

$$x^3 + \frac{1}{x^3} = 36 + 26\sqrt{2};$$

hieraus leitet man die einfachere Gleichung ab:

$$(15) \qquad x + \frac{1}{x} = 3 + \sqrt{2}, \quad \sqrt{2}\, x = f_1^2(\sqrt{-46}).$$

3. Wir machen endlich noch eine Anwendung der Transformationsgleichungen des §. 79 für einen zusammengesetzten Transformationsgrad auf die Determinante — 39.

Setzen wir

$$u = f(\sqrt{-39}), \quad v = f\left(\sqrt{\frac{-13}{3}}\right), \quad \frac{u^2 + v^2}{u\,v} = z,$$

so ist in der auf $n = 39$ bezüglichen Gleichung (22), §. 79 zu setzen:

$$A = \frac{u^2}{v^2} - 2\frac{v}{u}, \quad B = \frac{v^2}{u^2} - 2\frac{u}{v}$$

und die erwähnte Gleichung giebt:

$$z^3 + z^2 - 5z - 6 = 0,$$

woraus nach Abwerfung des Factors $z + 2$ die folgende hervorgeht:

$$(16) \qquad z^2 - z - 3 = 0, \quad z = \frac{1 + \sqrt{13}}{2}.$$

Zwischen $u$ und $v$ besteht aber andererseits eine Transformationsgleichung dritter Ordnung (§. 76):

$$\frac{u^6 v^6 - 8}{u^3 v^3} = \frac{u^{12} + v^{12}}{u^6 v^6} = z^6 - 6z^4 + 9z^2 - 2,$$

was sich mit Hülfe von (16) auf die Form $z^4 - 2 = \frac{27 + 7\sqrt{13}}{2}$ bringen lässt.

Daraus erhält man

$$u^3 v^3 = 4(3 + \sqrt{13}),$$
$$u^6 + v^6 = 4(17 + 5\sqrt{13}),$$
$$u^3 - v^3 = \sqrt{2}(3 + \sqrt{13}),$$

so dass, wenn $u^3 = \sqrt{8}\,x$ gesetzt wird, für $x$ die quadratische Gleichung folgt:

$$(17)\qquad x^2 - \frac{3+\sqrt{13}}{2}(x+1) = 0, \quad f(\sqrt{-39})^3 = \sqrt{8}\,x.$$

Wir wollen unsere Resultate jetzt noch anwenden auf zwei Probleme, welche in die allgemeine Transformationstheorie des neunten Abschnittes gehören.

## §. 99. Die Schlaefli'sche Modulargleichung für den 23ten Transformationsgrad.

Jede Classengleichung tritt als Divisor in einer grossen Zahl von Transformationsgleichungen auf und kann daher, wenn sie auf andere Weise bekannt ist, zur Berechnung von Transformationsgleichungen benutzt werden. Wir nehmen als Beispiel den 23ten Transformationsgrad.

Nach §. 76 besteht, wenn

$$(1)\qquad u = f(\omega), \quad v = f(23\,\omega), \quad f\left(\frac{c+\omega}{23}\right), \quad c \equiv 0 \pmod{48}$$

eine Gleichung zwischen

$$(2)\qquad \begin{aligned} A &= \left(\frac{u}{v}\right)^{12} + \left(\frac{v}{u}\right)^{12} \\ B &= u\,v + \frac{2}{u\,v}, \end{aligned}$$

und es ist schon in §. 77 gezeigt, dass diese Gleichung die Form hat:

$$(3)\qquad A = B^{11} + m_1 B^{10} + \cdots + m_{10} B + m_{11},$$

worin die Coëfficienten $m_1, m_2 \ldots, m_{11}$ rationale Zahlen sind. Statt nun diese rationalen Zahlencoëfficienten wie dort aus den Entwickelungen von $u$ und $v$ nach Potenzen von $q$ zu berechnen, suchen wir die Wurzeln der Gleichung (3) für $u = v$ aus der complexen Multiplication zu bestimmen.

Durch Multiplication mit $u^{12} v^{12}$ geht die Gleichung (3) in eine Form über, welche $u$, $v$ nicht im Nenner enthält, die wir für den Augenblick mit

$$(4)\qquad F(u, v) = 0$$

bezeichnen, so dass für ein unbestimmtes $x$ und $\omega$:

$$(5)\qquad F[f(\omega), x] = [x - f(23\,\omega)]\, \Pi \left[x - f\left(\frac{c+\omega}{23}\right)\right].$$

Wir untersuchen nun, für welche Werthe von $\omega$ die Function:

(6)
$$F(u,u) = F[f(\omega), f(\omega)]$$
$$= [f(\omega) - f(23\,\omega)]\,\Pi\left[f(\omega) - f\left(\frac{c+\omega}{23}\right)\right]$$

verschwindet. Es verschwindet zunächst offenbar der Factor:

$$f(\omega) - f\left(\frac{\omega}{23}\right)$$

für

$$u = f\,(\sqrt{-23}) = f\left(\frac{\sqrt{-23}}{23}\right).$$

Verstehen wir ferner unter $r$ eine der Zahlen $\pm 2$ oder $\pm 4$, und dem entsprechend unter

$$m = 23 - r^2,$$

entweder 19 oder 7, so verschwinden von den Factoren von (6) für $\omega = \sqrt{-m}$ je zwei, nämlich:

$$f(\omega) - f\left(\frac{24\,r + \omega}{23}\right),$$

denn es ist

$$f\left(\frac{24\,r + \sqrt{-m}}{23}\right) = e^{\frac{r\pi i}{24}} f\left(\frac{r + \sqrt{-m}}{23}\right)$$
$$= e^{\frac{r\pi i}{24}} f\left(\frac{1}{r - \sqrt{-m}}\right) = f(\sqrt{-m}).$$

Wir fügen noch hinzu, dass

$$\frac{f(\omega) - f\left(\frac{24\,r + \omega}{23}\right)}{f(\omega) - f(\sqrt{-m})}$$

für $\omega = \sqrt{-m}$ einer endlichen Grenze zustrebt, wie man durch Differentiation nach $\omega$ erkennt (§. 49), und daraus folgt, dass $F(u,u)$ durch $\left[u - f(\sqrt{-m})\right]^2$ theilbar ist.

Wenn man $u = v$ setzt, so wird

$$A = 2, \quad B = u^2 + \frac{2}{u^2},$$

und wenn $u = f(\sqrt{-m})$, $m = 7,\ 19,\ 23$ gesetzt wird, so erhält man aus §. 95, (6), (8), §. 98, (1) durch Elimination von $u$ die Gleichungen für $B$:

$$m = 7,\quad B - 3 = 0,$$
$$m = 19,\quad B^3 - 6B^2 + 10B - 6 = 0,$$
$$m = 23,\quad B^3 - 5B^2 + 4B - 1 = 0.$$

Die beiden letzten cubischen Gleichungen sind, da sie keine rationale Wurzel haben, irreducibel, und daraus ergiebt sich ohne Rechnung die gesuchte Modulargleichung (3):

$$(7)\quad A - 2 = (B-3)^2(B^3 - 6B^2 + 10B - 6)^2(B^3 - 5B^2 + 4B - 1).$$

## §. 100. Die Resolventen 7ten und 11ten Grades für den 7ten und 11ten Transformationsgrad.

Wir haben in §. 84 gesehen, dass für den 7ten und 11ten Transformationsgrad Resolventen der Grade 7 und 11 existiren. Auch bei der Bildung dieser Gleichungen kann die Theorie der complexen Multiplication nützliche Dienste leisten.

Wir betrachten, wenn $n = 7$ oder $= 11$ ist, die Transformationsgleichung

$$F_n(u, v) = 0,$$

deren Wurzeln, wenn $u = f(\omega)$ gesetzt wird,

$$(1)\qquad v_\infty = f(n\omega),\quad v_c = f\left(\frac{\omega + c}{n}\right)$$

sind, wobei $c$ als Index von $v$ nach dem Modul $n$ genommen werden kann, während es unter dem Zeichen $f$ durch 48 theilbar vorausgesetzt werden muss.

Diese Gleichungen sind nach §. 76:

$$(2)\quad n = 7,\quad v^8 - u^7v^7 + 7u^4v^4 - 8uv + u^8 = 0,$$

$$(3)\quad n = 11,\quad v^{12} - u^{11}v^{11} + 11u^9v^9 - 44u^7v^7 + 88u^5v^5 - 88u^3v^3 + 32uv + u^{12} = 0.$$

Wir haben in §. 76 den Einfluss der drei Vertauschungen

$$(4)\qquad \begin{aligned}(c') &= (\omega, \omega + 2),\\ (c'') &= \left(\omega, \frac{-1}{\omega}\right),\\ (c''') &= \left(\omega, \frac{\omega - 1}{\omega + 1}\right),\end{aligned}$$

durch welche $u$ übergeht in

$$e^{-\frac{\pi i}{12}}u,\quad u,\quad \frac{\sqrt{2}}{u},$$

auf die Wurzeln der Gleichungen (2) und (3) untersucht. Dieser Einfluss ergiebt sich aus den Zusammensetzungen:

$$(5) \qquad \begin{pmatrix} n, & 0 \\ c, & 1 \end{pmatrix} \begin{pmatrix} 1, & 0 \\ 2, & 1 \end{pmatrix} = \begin{pmatrix} n, & 0 \\ c', & 1 \end{pmatrix},$$

$$(6) \qquad c' \equiv c + 2 \pmod{n},$$

$$(7) \qquad \begin{pmatrix} n, & 0 \\ c, & 1 \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} = \begin{pmatrix} -c'', & n \\ -\dfrac{c c'' + 1}{n}, & c \end{pmatrix} \begin{pmatrix} n, & 0 \\ c'', & 1 \end{pmatrix},$$

$$(8) \qquad c c'' \equiv -1 \pmod{n},$$

$$(9) \qquad \begin{pmatrix} n, & 0 \\ c, & 1 \end{pmatrix} \begin{pmatrix} 1, & 1 \\ -1, & 1 \end{pmatrix} = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \begin{pmatrix} 1, & 1 \\ -1, & 1 \end{pmatrix} \begin{pmatrix} n, & 0 \\ c''', & 1 \end{pmatrix},$$

$$(10) \qquad c''' \equiv \frac{c-1}{c+1} \pmod{n},$$

$$\alpha - \beta = 1 - c''', \quad \gamma + \delta = c + 1,$$
$$\alpha + \beta = n, \quad n(\gamma - \delta) = (c-1) - c'''(c+1),$$

und nach §. 29 und §. 35, (11) geht also durch die Substitutionen $(c')$, $(c'')$, $(c''')$, mit Rücksicht auf

$$2 \equiv 2n^2 \pmod{48},$$

die Wurzel $v_c$ über in:

$$(11) \qquad e^{-\frac{\pi i n}{12}} v_{c'}, \quad v_{c''}, \quad \left(\frac{2}{n}\right) \frac{\sqrt{2}}{v_{c'''}},$$

und dies gilt auch für $c = \infty$. Die Vertauschungen der Indices, die sich so ergeben, sind:

$$(12) \qquad n = 7, \quad \begin{array}{rcl} c & = & \infty, 0, 1, 2, 3, 4, 5, 6, \\ c' & = & \infty, 2, 3, 4, 5, 6, 0, 1, \\ c'' & = & 0, \infty, 6, 3, 2, 5, 4, 1, \\ c''' & = & 1, 6, 0, 5, 4, 2, 3, \infty. \end{array}$$

$$(13) \qquad n = 11, \quad \begin{array}{rcl} c & = & \infty, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \\ c' & = & \infty, 2, 3, 4, 5, 6, 7, 8, 9, 10, 0, 1, \\ c'' & = & 0, \infty, 10, 5, 7, 8, 2, 9, 3, 4, 6, 1, \\ c''' & = & 1, 10, 0, 4, 6, 5, 8, 7, 9, 2, 3, \infty. \end{array}$$

Als Wurzeln der Resolventen 7ten und 11ten Grades können wir nach §. 84 je eine der beiden folgenden Functionen betrachten:

$$(14) \qquad n = 7,$$

$$w_\nu = \frac{(v_\infty - v_\nu)(v_{\nu+1} - v_{\nu+3})(v_{\nu+2} - v_{\nu+6})(v_{\nu+4} - v_{\nu+5})}{i\sqrt{7}\,u^4},$$

$$w'_\nu = \frac{(v_\infty - v_\nu)(v_{\nu+1} - v_{\nu+5})(v_{\nu+2} - v_{\nu+3})(v_{\nu+4} - v_{\nu+6})}{-i\sqrt{7}\,u^4},$$

$$(15) \qquad n = 11, \quad w_\nu =$$

$$\frac{(v_\infty - v_\nu)(v_{\nu+1} - v_{\nu+2})(v_{\nu+3} - v_{\nu+6})(v_{\nu+4} - v_{\nu+8})(v_{\nu+5} - v_{\nu+10})(v_{\nu+9} - v_{\nu+7})}{i\sqrt{11}\,u^6},$$

$$w'_\nu =$$

$$\frac{(v_\infty - v_\nu)(v_{\nu+1} - v_{\nu+6})(v_{\nu+3} - v_{\nu+7})(v_{\nu+4} - v_{\nu+2})(v_{\nu+5} - v_{\nu+8})(v_{\nu+9} - v_{\nu+10})}{-i\sqrt{11}\,u^6},$$

worin $\sqrt{7}$ und $\sqrt{11}$ positiv genommen sein sollen.

Es tritt nun zunächst der folgende bemerkenswerthe Unterschied zwischen beiden Fällen hervor.

Durch die beiden Vertauschungen $(c')$, $(c'')$ werden im Falle $n = 7$ die $w_\nu$ nur unter einander vertauscht, und zwar in folgender Weise:

$$\begin{array}{lccccccc}
 & w_0, & w_1, & w_2, & w_3, & w_4, & w_5, & w_6, \\
(c') & w_2, & w_3, & w_4, & w_5, & w_6, & w_0, & w_1, \\
(c'') & w_0, & w_2, & w_1, & w_6, & w_4, & w_5, & w_3,
\end{array}$$

während [nach (13)] im Falle $n = 11$ durch die Vertauschung $(c')$ die Grössen $w$ gleichzeitig ihr Vorzeichen ändern, so dass folgende Vertauschungen eintreten:

$$\begin{array}{lccccccccccc}
 & w_0, & w_1, & w_2, & w_3, & w_4, & w_5, & w_6, & w_7, & w_8, & w_9, & w_{10} \\
(c') & -w_2, & -w_3, & -w_4, & -w_5, & -w_6, & -w_7, & -w_8, & -w_9, & -w_{10}, & -w_0, & -w_1, \\
(c'') & w_0, & w_9, & w_6, & w_3, & w_5, & w_4, & w_2, & w_8, & w_7, & w_1, & w_{10},
\end{array}$$

und ebenso verhält es sich mit $w'$.

Daraus folgt nun (§. 49), dass die $w_\nu$ Wurzeln einer Gleichung 7ten oder 11ten Grades:

$$(16) \qquad w^n + A_1 w^{n-1} + A_2 w^{n-2} + \cdots + A_n = 0$$

sind, dass darin aber im Falle $n = 7$ sämmtliche $A_i$ rational von $f(\omega)^{24}$ abhängen, dagegen im Falle $n = 11$ die $A_i$ mit geradem Index ebenfalls rational von $f(\omega)^{24}$ abhängen, während die mit ungeradem Index das Product von $f(\omega)^{12}$ mit einer rationalen Function von $f(\omega)^{24}$ sind. Die Zahlcoëfficienten enthalten ausser rationalen Zahlen nur noch die Irrationalität

$i\sqrt{7}$ bezw. $i\sqrt{11}$, und demnach wollen wir diese Gleichung bezeichnen durch

$$(17)\qquad \begin{aligned} &\Phi\left[w, f(\omega)^{24}, \quad i\sqrt{7}\right] = 0,\\ &\Phi\left[w, f(\omega)^{12}, \quad i\sqrt{11}\right] = 0. \end{aligned}$$

Aendern wir gleichzeitig die Vorzeichen von $i$ und $w$, so ergiebt sich, wie wir in §. 84 gesehen haben, eine Gleichung, deren Wurzeln die Grössen $w'$ sind.

Auch bei der Anwendung der Substitution $(c''')$ zeigt sich für die beiden Fälle ein Unterschied.

Es ergiebt sich nämlich aus (13), mit Rücksicht darauf, dass nach (2) das Product sämmtlicher $v_\nu$ den Werth $u^8$ hat, dass im Falle $n = 7$ durch die Substitution $(c''')$ die $w_\nu$ nur unter einander vertauscht werden, und zwar in folgender Weise:

$$\begin{pmatrix} w_0, & w_1, & w_2, & w_3, & w_4, & w_5, & w_6 \\ w_5, & w_3, & w_6, & w_2, & w_4, & w_0, & w_1 \end{pmatrix}$$

und daraus folgt, dass in diesem Falle die Coëfficienten $A_\nu$ alle ungeändert bleiben, durch die Vertauschung:

$$\left(f(\omega)^{24}, \frac{2^{12}}{f(\omega)^{24}}\right).$$

Ueberdies kommen im Nenner dieser Coëfficienten nur Potenzen von $f(\omega)^{24}$ vor (§. 76), und die Potenzen von $f(\omega)^{24}$ steigen bis zu derselben Höhe wie die von $f(\omega)^{-24}$.

Im Falle $n = 11$ gehen durch die Vertauschung $(c''')$ die Grössen $w_\nu$ in die Grössen $w'_\nu$ über, und zwar in folgender Reihenfolge:

$$\begin{pmatrix} w_0, & w_1, & w_2, & w_3, & w_4, & w_5, & w_6, & w_7, & w_8, & w_9, & w_{10} \\ w'_8, & w'_2, & w'_7, & w'_0, & w'_9, & w'_5, & w'_6, & w'_4, & w'_3, & w'_{10}, & w'_1 \end{pmatrix}.$$

Nach (17) können wir diese Eigenschaft durch die in Bezug auf $w$ identische Gleichung ausdrücken:

$$-\Phi\left[-w, f(\omega)^{12}, -i\sqrt{11}\right] = \Phi\left(w, \frac{2^6}{f(\omega)^{12}}, i\sqrt{11}\right),$$

und daraus ergeben sich die folgenden Eigenschaften der Coëfficienten $A_\nu$:

$A_\nu$ bleibt ungeändert durch die gleichzeitige Vertauschung:

$$\left(f(\omega)^{12}, \frac{64}{f(\omega)^{12}}\right), \qquad \left(i\sqrt{11}, -i\sqrt{11}\right),$$

und enthält bei geradem $\nu$ nur die geraden, bei ungeradem $\nu$ nur die ungeraden Potenzen von $f(\omega)^{12}$.

Auch hier treten nur Potenzen von $f(\omega)$ im Nenner auf, und die Potenzen von $f(\omega)$ steigen bis zur selben Höhe wie die von $f(\omega)^{-1}$.

Um über die Grade der Functionen $A_\nu$ ins Klare zu kommen, betrachten wir die Anfänge der Entwickelungen nach steigenden Potenzen von $q = e^{\pi i \omega}$.

Es beginnt die Entwickelung von $f(\omega)$ mit $q^{-\frac{1}{24}}$, die von $v_\infty$ mit $q^{-\frac{n}{24}}$, von $v_c$ mit $q^{-\frac{1}{24n}} e^{-\frac{2\pi i c}{48}\frac{1}{n}}$, worin aber in der letzten Exponentialgrösse, wenn wir $c$ auf seinen kleinsten Rest (mod $n$) reduciren, auch $\frac{1}{48}$ nach dem Modul $n$ zu nehmen, also für $n = 7, 11$:

$$\frac{1}{48} \equiv -1 \pmod{7},$$

$$\frac{1}{48} \equiv 3 \pmod{11}$$

zu setzen ist. Wenn wir also hiernach

$$\varrho = e^{\frac{2\pi i}{7}} \quad \text{oder} \quad = e^{-\frac{6\pi i}{11}}$$

setzen, so erhalten wir aus (14), (15) als Anfänge der Entwickelung

für $n = 7$:

$$i\sqrt{7}\, w_\nu = q^{-\frac{1}{7}} \varrho^{3\nu} (\varrho - \varrho^3)(\varrho^2 - \varrho^6)(\varrho^4 - \varrho^5) + \cdots,$$

für $n = 11$:

$$i\sqrt{11}\, w_\nu = q^{-\frac{5}{22}} \varrho^{5\nu} (\varrho - \varrho^2)(\varrho^3 - \varrho^6)(\varrho^4 - \varrho^8)(\varrho^5 - \varrho^{10})(\varrho^9 - \varrho^7) + \cdots$$

Es ist aber für $n = 7$:

$$(\varrho - \varrho^3)(\varrho^2 - \varrho^6)(\varrho^4 - \varrho^5) = -\varrho - \varrho^2 - \varrho^4 + \varrho^3 + \varrho^5 + \varrho^6,$$

und für $n = 11$:

$$(\varrho - \varrho^2)(\varrho^3 - \varrho^6)(\varrho^4 - \varrho^8)(\varrho^5 - \varrho^{10})(\varrho^9 - \varrho^7) =$$
$$-\varrho - \varrho^3 - \varrho^4 - \varrho^5 - \varrho^9 + \varrho^2 + \varrho^6 + \varrho^8 + \varrho^7 + \varrho^{10}.$$

Da 1, 2, 4 die quadratischen Reste von 7; 1, 3, 4, 5, 9 die quadratischen Reste von 11 sind, so können diese beiden Summen nach einer aus der Kreistheilungstheorie bekannten Formel (vgl.

Dirichlet-Dedekind, §. 115) bestimmt werden, und ergeben in den beiden Fällen:

$$i\sqrt{7} \quad \text{und} \quad -i\sqrt{11},$$

so dass

$$(18) \qquad \begin{aligned} w_\nu &= \phantom{-}q^{-\frac{1}{7}}\varrho^{3\nu} + \cdots, \quad n = 7, \\ w_\nu &= -q^{-\frac{5}{22}}\varrho^{5\nu} + \cdots, \quad n = 11. \end{aligned}$$

Hierdurch lässt sich eine obere Grenze ableiten, bis zu welcher in $A_\nu$ die Potenzen von $f(\omega)$ höchstens ansteigen können, wenn man noch beachtet, dass die $A_\nu$ als ganze rationale (und symmetrische) Functionen der $w_\nu$ darstellbar sind.

Für $n = 7$ ergiebt sich so, da alle Exponenten von $f(\omega)$ durch 24 theilbar sein müssen, dass $A_1, A_2, A_3, A_4, A_5, A_6$ Constanten sind, während $A_7$ nur die erste Potenz von $f(\omega)^{24}$, und zwar mit dem Coëfficienten $-1$ [nach (18)], enthält.

Für $n = 11$ muss, wenn $f(\omega)^{12\lambda}$ die höchste in $A_\nu$ vorkommende Potenz von $f(\omega)$ ist,

$$\lambda \overline{\lessgtr} \frac{5\nu}{11}$$

sein, und überdies muss $\lambda$ mit $\nu$ zugleich gerade oder ungerade sein. Daher sind $A_2$, $A_4$ constant, $A_6$, $A_8$ enthalten die höchste Potenz $f(\omega)^{24}$, $A_{10}$ enthält auch $f(\omega)^{48}$. Da die $A$ mit ungeradem Index nur ungerade Potenzen von $f(\omega)^{12}$ enthalten, so ist $A_1 = 0$, $A_3$, $A_5$ enthalten $f(\omega)^{12}$, $A_7$, $A_9$ enthalten bis $f(\omega)^{36}$, in $A_{11}$ steigt $f(\omega)$ bis zur 60ten Potenz an.

Für den Fall $n = 7$ wollen wir nun die Constanten vollständig mit Hülfe der complexen Multiplication bestimmen, und zwar genügt dazu die Betrachtung der Werthe der $w_\nu$ für $\omega = i$.

Für $\omega = i$ wird

$$u = f(i) = \sqrt[4]{2},$$

und wenn wir diesen Werth in die Gleichung (2) einführen, und

$$\sqrt[4]{2}\, v = x$$

setzen, so ergiebt sich:

$$(19) \qquad x^8 - 4x^7 + 28x^4 - 32x + 16 = 0.$$

Die linke Seite dieser Gleichung ist das Quadrat des Ausdruckes:

$$(20) \qquad x^4 - 2x^3 - 2x^2 - 4x + 4,$$

so dass also die Werthe von $v$ für $\omega = i$ paarweise einander gleich werden. Nach §. 91, 5. muss, wenn $v_c = v_{c'}$ ist, $c\,c' \equiv -1$ (mod 7) sein, so dass also:

$$(21) \qquad v_\infty = v_0, \quad v_1 = v_6, \quad v_2 = v_3, \quad v_4 = v_5.$$

Der Ausdruck (20) lässt sich in die beiden quadratischen Factoren:

$$x^2 - (1 + \sqrt{7})\, x + 2, \quad x^2 - (1 - \sqrt{7})\, x + 2$$

zerlegen, so dass die acht Werthe von $x$ paarweise je einer der vier Grössen

$$(22) \qquad \frac{1 + \sqrt{7}}{2} \pm \frac{\sqrt[4]{7}}{\sqrt{2}}, \quad \frac{1 - \sqrt{7}}{2} \pm i \frac{\sqrt[4]{7}}{\sqrt{2}}$$

gleich werden, und es handelt sich noch darum, diese vier Werthe den einzelnen $v_\nu$ zuzuordnen. Dazu bemerken wir, dass $v_\infty$, $v_0$ für $\omega = i$ reell sind, und dass ebenso $v_1$, $v_6$ reell sein müssen, weil sie gleichzeitig einander gleich und conjugirt imaginär sind.

Aus $v_0$ entsteht $v_\nu$ dadurch, dass man $q$ mit einer gewissen Einheitswurzel multiplicirt; da aber die Entwickelung von $v_0$ nach Potenzen von $q$ nur positive Coëfficienten enthält [vgl. §. 21, (10)], so folgt, dass $v_0$ grösser sein muss als $v_1$, und mithin ist

$$(23) \qquad \begin{aligned} \sqrt[4]{2}\, v_\infty &= \sqrt[4]{2}\, v_0 = \frac{1 + \sqrt{7}}{2} + \frac{\sqrt[4]{7}}{\sqrt{2}} \\ \sqrt[4]{2}\, v_1 &= \sqrt[4]{2}\, v_6 = \frac{1 + \sqrt{7}}{2} - \frac{\sqrt[4]{7}}{\sqrt{2}}. \end{aligned}$$

Für die beiden anderen Wurzelpaare ergiebt sich:

$$(24) \qquad \begin{aligned} \sqrt[4]{2}\, v_2 &= \sqrt{2}\, v_3 = \frac{1 - \sqrt{7}}{2} + i \frac{\sqrt[4]{7}}{\sqrt{2}} \\ \sqrt[4]{2}\, v_4 &= \sqrt{2}\, v_5 = \frac{1 - \sqrt{7}}{2} - i \frac{\sqrt[4]{7}}{\sqrt{2}}. \end{aligned}$$

Dass in diesen Ausdrücken das Vorzeichen von $i$ richtig gewählt ist, schliesst man auf folgende Weise:

Aus (23) ist zu ersehen, dass für $\omega = i$, also für $u = \sqrt{2}$, die Wurzel $w_0$ verschwindet, und dass also für diesen Werth $A_7$ verschwinden muss. Nach den oben nachgewiesenen Eigenschaften ist hierdurch $A_7$ vollständig bestimmt, nämlich:

$$(25) \qquad A_7 = -\left(u^{12} - \frac{64}{u^{12}}\right)^2,$$

woraus folgt, dass für keinen anderen Werth von $u^{24}$ als 64 zwei der Werthe $v_\nu$ einander gleich werden. Es tritt diese Gleichheit also nur für $\omega = i$ und gewisse mit $i$ äquivalente Werthe von $\omega$ ein und daher nicht für einen anderen rein imaginären Werth von $\omega$.

Der Anfang der Entwickelung nach steigenden Potenzen von $q$ ergiebt nun:

$$(26)\qquad v_2 - v_5 = f\left(\frac{\omega - 2\,.\,48}{7}\right) - f\left(\frac{\omega + 2\,.\,48}{7}\right)$$
$$= 2\,i\,q^{-\frac{1}{7\,.\,24}} \sin\frac{4\pi}{7} + \cdots,$$

so dass für einen hinlänglich grossen reellen Werth von $-i\omega$ die linke Seite von (26) positiv imaginär ist. Wenn nun $-i\omega$ auf reellem Wege von $\infty$ bis 1 geht, so geht, wie wir oben gesehen haben, $v_2 - v_5$ nicht durch Null, so dass auch für $\omega = i$ die Differenz $v_2 - v_5$ positiv imaginär sein muss, wie in (24) angenommen ist.

Wenn man also die Werthe (23), (24) in (14) einsetzt, so ergiebt sich für $\omega = i$:

$$w_0 = 0, \quad w_5 = 0$$
$$(27)\qquad w_1 = w_2 = w_3 = w_6 = \frac{7 + i\sqrt{7}}{2}$$
$$w_4 = -\frac{i\sqrt{7}\,(1 + i\sqrt{7})^2}{4}.$$

Danach kann für den Fall $n = 7$ die Resolvente vollständig gebildet werden. Sie lautet:

$$(28)\qquad w^2\left(w - \frac{7 + i\sqrt{7}}{2}\right)^4 \left(w + \frac{i\sqrt{7}\,(1 + i\sqrt{7})^2}{4}\right)$$
$$= \left(u^{12} - \frac{64}{u^{12}}\right)^2,$$

und nimmt eine einfachere Gestalt an, wenn man

$$w + \frac{i\sqrt{7}\,(1 + i\sqrt{7})^2}{4} = z^2$$

setzt:

$$(29)\quad z\left(z^2 - \frac{i\sqrt{7}\,(1 + i\sqrt{7})^2}{4}\right)(z + i\sqrt{7})^2 = u^{12} - \frac{64}{u^{12}}.$$

Für den Fall $n = 11$ ist die entsprechende Rechnung noch nicht durchgeführt. Verhältnissmässig einfach erhält man, wenn man mit Benutzung der Betrachtungsweise des §. 91 die Werthe von $\omega$ aufsucht, für welche eine der Grössen $w_\nu$ verschwindet:

$$\omega = i, \quad \omega = \sqrt{-7}, \quad \omega = \frac{1+\sqrt{-7}}{1-\sqrt{-7}},$$

$$u = \sqrt[4]{2}, \quad u = \sqrt{2}, \quad u = 1,$$

und daraus

$$A_{11} = \left(u^{12} - \frac{2^6}{u^{12}}\right)^3 \left(u^{12} - \frac{2^{12}}{u^{12}}\right) \left(u^{12} - \frac{1}{u^{12}}\right).$$

---

## Dreizehnter Abschnitt.

# Die Multiplicatorgleichung in der complexen Multiplication und die Zerfällung der Classengleichung in Factoren.

---

### §. 101. Die Classenzahlrelation.

Wir haben schon im §. 88 gesehen, dass die Function $F_n(u, u)$ immer theilbar ist durch gewisse der Functionen $H_m(u)$, $H'_m(u)$, und haben darauf den Beweis gegründet, dass diese Functionen $H$ rationale Coëfficienten haben. Es soll nun genauer bestimmt werden, wie die Function $F_n(u, u)$ in Factoren $H_m$, $H'_m$ zerlegt werden kann, wodurch sich ein neuer Beweis jenes Satzes über die Coëfficienten der Functionen $H$ ergeben wird.

Da für ein variables $\omega$

$$(1) \qquad F_n[j(\omega), j(\omega)] = \Pi\left[j(\omega) - j\left(\frac{c + \partial\omega}{a}\right)\right]$$

ist, so wird $F_n(u, u)$ für $u = j(\omega)$ dann und nur dann verschwinden, wenn

$$(2) \qquad \frac{c + \partial\omega}{a} = \frac{\gamma + \delta\omega}{\alpha + \beta\omega},$$

worin $a\partial = n$ und $a$, $\partial$, $c$ ganze Zahlen ohne gemeinsamen Theiler, $\alpha$, $\beta$, $\gamma$, $\delta$ ebenfalls ganze Zahlen sind, die der Bedingung

$$(3) \qquad \alpha\delta - \beta\gamma = 1$$

genügen. Für $\omega$ erhalten wir hieraus eine quadratische Gleichung

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

worin $A$, $B$, $C$ ohne gemeinsamen Theiler sind und

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

negativ ist. Da $\omega$ bei der Beurtheilung der Frage nach dem Verschwinden von $F[j(\omega), j(\omega)]$ durch eine äquivalente Zahl ersetzt werden kann, so dürfen wir immer voraussetzen, dass $A$ relativ prim zu $2\varDelta$ und zu $n$ ist.

Je nachdem $B$ gerade oder ungerade ist, gehört (4) zu der ersten oder zweiten Art. Um beide Fälle zu umfassen, wollen wir unter $\sigma$ für ein gerades $B$ die Zahl 1, für ein ungerades $B$ die Zahl 2 verstehen und setzen

$$\sigma^2 \varDelta = 4m,$$

so dass $-m$ die Determinante der quadratischen Form ist

$$\left(\sigma A,\ \frac{\sigma B}{2},\ \sigma C\right).$$

Bezeichnen wir mit $x$ einen unbestimmten ganzzahligen Factor, so ergiebt die Vergleichung von (2) mit (4)

$$\begin{aligned} \partial\beta &= Ax, \\ c\alpha - a\gamma &= Cx, \\ \partial\alpha - a\delta + c\beta &= Bx. \end{aligned} \tag{5}$$

Wir führen noch die Zahl $y$ ein vermittelst der Gleichung

$$\partial\alpha + a\delta - c\beta = \frac{2y}{\sigma}, \tag{6}$$

und erhalten aus (5) und (6)

$$\begin{aligned} \partial\alpha &= \frac{Bx}{2} + \frac{y}{\sigma} \\ a\delta - c\beta &= -\frac{Bx}{2} + \frac{y}{\sigma}, \end{aligned} \tag{7}$$

woraus wegen $a\partial = n$ folgt

$$\sigma^2 n = mx^2 + y^2. \tag{8}$$

Den Gleichungen (5), (7) geben wir mittelst (3) die Gestalt

$$\begin{aligned} c &= \quad Cx\delta - \left(\frac{Bx}{2} - \frac{y}{\sigma}\right)\gamma \\ a &= \quad Cx\beta - \left(\frac{Bx}{2} - \frac{y}{\sigma}\right)\alpha \\ \partial &= -Ax\gamma + \left(\frac{Bx}{2} + \frac{y}{\sigma}\right)\delta, \end{aligned} \tag{9}$$

woraus sich für $x$, $y$ die Bedingungen ergeben:

$x$, $y$ müssen so gewählt sein, dass

$$x,\ \frac{Bx}{2} + \frac{y}{\sigma} \tag{10}$$

ganze Zahlen ohne gemeinsamen Theiler sind.

Denn jeder gemeinsame Theiler dieser beiden Zahlen wäre wegen $\frac{Bx}{2} - \frac{y}{\sigma} = Bx - \left(\frac{Bx}{2} + \frac{y}{\sigma}\right)$ auch Theiler von $\frac{Bx}{2} - \frac{y}{\sigma}$, und mithin auch von $a$, $c$, $\partial$.

Mit der Bedingung (10) ist gleichbedeutend die, dass

$$x \text{ und } \frac{Bx}{2} - \frac{y}{\sigma} \text{ oder } x \text{ und } \frac{B^2x^2}{4} - \frac{y^2}{\sigma^2}$$

ganze Zahlen ohne gemeinsamen Theiler sind.

Ist $\sigma = 1$, so fordert diese Bedingung (10) weiter nichts, als dass $x$ und $y$ relativ prim sind; ist dagegen $\sigma = 2$, so kann ihr auch die Form gegeben werden, dass

$$(11) \qquad x \text{ und } \frac{x^2 - y^2}{4}$$

relativ prim sein sollen, wodurch sie von $B$ unabhängig wird.

Setzen wir (8) in die Form

$$n = ACx^2 - \left(\frac{Bx}{2} - \frac{y}{\sigma}\right)\left(\frac{Bx}{2} + \frac{y}{\sigma}\right),$$

so zeigt sich, dass $x$ mit $n$ keinen gemeinsamen Theiler haben kann, und da das Gleiche von $A$ vorausgesetzt ist, so folgt aus der ersten Gleichung (5), dass $\partial = 1$ und $a = n$ sein muss.

Ist $x$, $y$ den Bedingungen (8), (10) gemäss bestimmt, so folgt

$$(12) \qquad \alpha = \frac{Bx}{2} + \frac{y}{\sigma}, \quad \beta = Ax$$

und aus unseren Voraussetzungen ergiebt sich, dass diese beiden Zahlen ohne gemeinsamen Theiler sind. Von den Gleichungen (9) wird die zweite mit (8), die dritte mit (3) identisch.

Bestimmt man daher $\gamma$, $\delta$ aus (3), so folgt $c$ aus der ersten Gleichung (9).

Es ist aber $c$ nur bis auf ein Vielfaches von $n$ bestimmt, da $\gamma$, $\delta$ durch $\gamma + \lambda\alpha$, $\delta + \lambda\beta$ ersetzt werden können.

Damit sind dann alle in der Gleichung (2) enthaltenen Forderungen erfüllt.

Hierdurch ist nachgewiesen, dass durch ein Zahlenpaar $x$, $y$, welches die Bedingungen (8), (10) befriedigt, einer unter den Factoren von (1) und zwar von der Form

$$j(\omega) - j\left(\frac{c + \omega}{n}\right)$$

eindeutig bestimmt ist, welcher, wenn $\omega$ der Gleichung (4) genügt, verschwindet.

Es handelt sich zweitens darum, ob auch umgekehrt durch den Werth von $c$ (mod $n$) das Zahlenpaar $x$, $y$ bestimmt ist oder ob verschiedene Werthpaare $x$, $y$ zu demselben Werthe (oder zu modulo $n$ congruenten Werthen) von $c$ führen können.

Dazu bemerken wir zunächst, dass eine gemeinsame Vorzeichenänderung der sechs Zahlen $\alpha$, $\beta$, $\gamma$, $\delta$, $x$, $y$ in allen unseren Formeln und also auch in der Bestimmung von $c$ nichts ändert. Um diese Zweideutigkeit auszuschliessen, können wir, da $x$, wenn $n > 1$ ist, von Null verschieden ist, festsetzen:

(13) $x$ soll positiv sein.

Sodann folgt aus (5) und (6), dass durch $\alpha$, $\beta$, $\gamma$, $\delta$ und $c$ die Zahlen $x$, $y$ vollständig bestimmt sind. Es würden also nur dann mehrere Werthepaare $x$, $y$ zu demselben oder zu congruenten Werthen von $c$ führen können, wenn die Gleichung (2) für dasselbe $c$ und für wenigstens zwei Systeme $\alpha$, $\beta$, $\gamma$, $\delta$; $\alpha'$, $\beta'$, $\gamma'$, $\delta'$ befriedigt wäre, worin $\alpha : \beta$ von $\alpha' : \beta'$ verschieden ist. Dies aber ist nur möglich, wenn eine Gleichung von der Form

$$(14) \qquad \omega = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}$$

besteht, worin $\beta$ von Null verschieden ist.

Behandelt man aber die Gleichung (14) als einen speciellen Fall von (2), so folgt für diesen Fall

$$\sigma^2 = m x^2 + y^2,$$

was nur möglich ist für $x = 0$, $y = \pm \sigma$, was aber in (14) zu $\beta = 0$ führt, und ausserdem noch in folgenden beiden Fällen:

$$(15) \qquad \sigma = 1, \quad m = 1, \quad x = 1, \quad y = 0,$$

$$(16) \qquad \sigma = 2, \quad m = 3, \quad x = 1, \quad y = \pm 1.$$

In diesen beiden Ausnahmefällen führen also je zwei oder je drei Werthepaare $x$, $y$ zu demselben Werthe von $c$ (mod $n$).

Hiermit ist bewiesen, dass von den Factoren des Products (1), wenn $\omega$ die Wurzel der Gleichung (4) ist, im Allgemeinen so viele verschwinden, als die Anzahl der Lösungen von (8) [unter der Beschränkung (11), (13)] beträgt, in den Fällen (15), (16) die Hälfte oder das Drittel dieser Zahl. Diese Zahl der Lösungen von (8) wollen wir mit $k$ bezeichnen.

Nach den Formeln (4), (5), (7) ist

$$\alpha + \beta\omega = \frac{y + x\sqrt{-m}}{\sigma}$$

und daraus ergiebt sich mit Benutzung der Relation (2) die in der Folge noch sehr wichtige Formel

$$\frac{\eta\left(\frac{c+\omega}{n}\right)}{\eta(\omega)} = \varepsilon\sqrt{\frac{x + y\sqrt{-m}}{\sigma}}, \tag{17}$$

worin $\varepsilon$ eine nach §. 33, (15) zu bestimmende 24te Einheitswurzel ist. Hieraus schliessen wir leicht durch Differentiation nach der Variablen $\tau$ auf Grund von §. 49, (13), dass für $\tau = \omega$ der Quotient

$$\frac{j(\tau) - j\left(\frac{c+\tau}{n}\right)}{j(\tau) - j(\omega)}$$

einen endlichen von Null verschiedenen Grenzwerth hat. Daraus geht hervor, dass die Function $F_n(u, u)$ durch die $k$te [oder in den Fällen (15), (16) $\frac{1}{2}\,k$te oder $\frac{1}{3}\,k$te] Potenz von $u - j(\omega)$ und durch keine höhere Potenz theilbar ist.

Die Zahl $k$ hängt aber nur von der Determinante $-m$, nicht von der besonderen Gleichung (4) ab, und es folgt also, dass $F_n(u, u)$ durch $H_m^k$ oder für $\sigma = 2$ durch $H_m'^k$ und in den Ausnahmefällen (15), (16) durch $H_{m,}^{\frac{1}{2}k}\, H_m'^{\frac{1}{3}k}$ theilbar ist, und dass der Quotient mit $H_m(u)$, $H'_m(u)$ keinen Theiler gemein hat.

Hieraus entnehmen wir zunächst einen zweiten Beweis dafür, dass die Functionen $H_m(u)$, $H'_m(u)$ rationale Coëfficienten haben. Denn die Gleichung (8) hat für $m = n$ und $\sigma = 1$ nur die eine Lösung $x = 1$, $y = 0$ und für $\sigma = 2$ im Allgemeinen nur die eine Lösung $x = 2$, $y = 0$, und wenn $3m$ ein Quadrat ist, die drei Lösungen $x = 2$, $y = \pm\sqrt{3m}$, während für alle anderen Werthe von $m$ die Lösungen paarweise vorhanden sind $(x, \pm y)$.

Wenn wir daher alle in gerader Ordnung eingehenden Factoren aus $F_m(u, u)$ absondern, was auf rationalem Wege geschieht, so bleibt $H_m(u)$ oder $H_m(u)\, H'_m(u)$ übrig, was hiernach auch rationale Coëfficienten hat.

Wenn es Formenclassen zweiter Art giebt, so ist $m \equiv -1$ (mod 4). Setzen wir also in diesem Falle in (8) $n = \frac{m+1}{4}$, so erhalten wir

$$\sigma^2(m+1) = 4(x^2m + y^2);$$

diese Gleichung hat keine Lösung für $\sigma = 1$, wohl aber für $\sigma = 2$ die Lösungen $x = 1$, $y = \pm 1$, so dass man $H'_m$ als den grössten gemeinschaftlichen Theiler von

$$H_m\, H'_m \text{ und } F_{\frac{m+1}{4}}(u, u)$$

auf rationalem Wege findet, wodurch dann auch $H_m$ gefunden ist.

Wenn man den im §. 87 bestimmten Grad der Function $F_n(u, u)$ gleich setzt der Summe der Grade der Factoren, in welche wir diese Function zerlegt haben, so erhalten wir eine Beziehung zwischen den Classenzahlen quadratischer Formen verschiedener negativer Determinanten. Hat nämlich $k$ die oben festgesetzte Bedeutung und ist $h$ der zugehörige Grad von $H_m$ oder $H'_m$, d. h. also die Classenzahl eigentlich oder uneigentlich primitiver Formen der Determinante $-m$, mit der Beschränkung, dass, wenn $\sigma = 1$, $m = 1$ ist, $h = 1/2$ und wenn $\sigma = 2$, $m = 3$ ist, $h = 1/3$ sein soll, so ist

$$\Sigma k h = N, \tag{18}$$

worin $N$ durch §. 87, (6), (7) bestimmt ist.

Diese Classenzahlrelation erhält eine einfachere Gestalt, wenn man mit $n$ zugleich alle diejenigen Werthe $n'$ ins Auge fasst, welche aus $n$ durch Fortheben eines quadratischen Factors entstehen, und die entsprechenden Gleichungen (18) addirt, wobei nur, falls $n$ ein Quadrat ist, der Werth $n' = 1$ auszuschliessen ist, weil $F_1(u, u)$ identisch verschwindet.

Es sei also $\delta^2$ irgend ein von $n$ selbst verschiedener quadratischer Factor von $n$ und

$$n = n'\delta^2.$$

Zerlegen wir $n'$ in zwei Factoren $n' = a'\partial'$ und bezeichnen mit $e'$ den grössten gemeinschaftlichen Factor von $\partial'$, $a'$, so ist die Summe der rechten Seiten der Gleichungen (17)

$$\Sigma N' = 2\sum^{\delta}\sum_{\partial' > a'}^{\partial'} \frac{\partial'}{e'}\,\varphi(e') + \sum^{n'}\varphi\left(\sqrt{n'}\right),$$

worin $\delta^2$ alle quadratischen Factoren von $n$ (mit Ausnahme von $n$)

durchläuft, und die Summe $\Sigma\varphi(\sqrt{n'})$ nur dann vorkommt, wenn $n$ ein Quadrat ist.

Setzen wir nun

$$\partial'\delta = \partial, \quad a'\delta = a, \quad e'\delta = e,$$

so ist $a\partial = n$, und $e$ ist der grösste gemeinschaftliche Theiler von $a$ und $\partial$; zugleich hat $\partial' > a'$ zur Folge, dass $\partial > a$ ist.

Umgekehrt erhält man aus jeder Zerlegung $a\partial$ von $n$ und jedem Theiler $e'$ von $e$ eine Zerlegung $a'\partial'$ von $n'$, wobei $\delta = e:e'$ wird. Demnach ist

$$\Sigma N' = 2\sum_{\partial > a}^{\partial} \frac{\partial}{e}\, \Sigma\varphi(e') + \sum^{n'}\varphi(\sqrt{n'}).$$

Hierin machen wir nun Gebrauch von der aus der Zahlentheorie bekannten Relation (Dirichlet-Dedekind, §. 13):

$$\Sigma\; \varphi(\partial) = n,$$

wenn die Summe der linken Seite sich auf alle Divisoren $\partial$ von $n$ bezieht. Nehmen wir zunächst an, dass $n$ kein Quadrat sei, so folgt hiernach, wegen $\Sigma\varphi(e') = e$

$$\Sigma N' = 2 \sum_{\partial > \sqrt{n}} \partial, \tag{19}$$

wenn dagegen $n$ ein Quadrat ist, so durchläuft $e'$ noch immer die sämmtlichen Divisoren von $e$, $\sqrt{n'}$ aber die sämmtlichen Divisoren von $\sqrt{n}$, mit Ausnahme von 1; danach ergiebt sich für diesen Fall

$$\Sigma N' = 2 \sum_{\partial > \sqrt{n}} \partial + \sqrt{n} - 1, \tag{20}$$

wo in beiden Formeln $\partial$ die sämmtlichen Divisoren von $n$ zu durchlaufen hat, die grösser als $\sqrt{n}$ sind.

Um nun den Ausdruck von $\Sigma N'$ durch die Classenzahlen zu finden, betrachten wir das System sämmtlicher [auch nicht der Bedingung (11) genügenden] Lösungen der Gleichung

$$\sigma^2 n = x^2 m + y^2, \tag{21}$$

in denen $x$ positiv ist. Wir setzen

$$x = \delta x', \quad y = \delta y' \tag{22}$$

und bestimmen den Factor $\delta$ so, dass $x'$, $y'$ die absolut grössten der Bedingung (11) genügenden Zahlen werden. Dann muss $\delta^2$ ein Theiler von $n$ sein. Dies ist zunächst klar, wenn $\sigma = 1$ ist; ist aber $\sigma = 2$, so ist $\delta^2$ jedenfalls Theiler von $4n$. Es muss aber

$$\frac{4n}{\delta^2} = m x'^2 + y'^2$$

noch durch 4 theilbar sein, denn wenn von den Zahlen $x'$, $y'$ die eine gerade, die andere ungerade ist, so genügt $2x'$, $2y'$ der Bedingung (11), gegen die in (22) liegende Voraussetzung.

Setzen wir also

$$n = \delta^2 n',$$

so folgt

(23) $$\sigma^2 n' = x'^2 m + y'^2,$$

und aus einer Lösung von (23) leiten wir auch immer eine Lösung von (21) her.

Um bei der Bildung der Summe (18) nicht genöthigt zu sein, den Fall $n' = 1$ auszuschliessen, bemerken wir, dass, wenn $n' = 1$ ist, die Gleichung (23) nur besteht für

$$\sigma = 1,\quad m = 1,\quad x' = 1,\quad y' = 0,\quad k = 1,\ h = \frac{1}{2},$$

$$\sigma = 2,\quad m = 3,\quad x' = 1,\quad y' = \pm 1,\ k = 2,\ h = \frac{1}{3},$$

so dass für diesen Fall

$$\Sigma k h = \frac{7}{6}$$

wird.

Wenn wir also unter dieser Voraussetzung die sämmtlichen Gleichungen (18) summiren, so behält die linke Seite ihre Form bei, wenn wir jetzt übereinkommen, unter $k$ die Anzahl sämmtlicher Lösungen der Gleichung (22) mit positivem $x$ zu verstehen, während die Summe der rechten Seiten, je nachdem $n$ ein Quadrat ist oder nicht,

$$2\Sigma\partial + \sqrt{n} + \frac{1}{6}\ \text{oder}\ 2\Sigma\partial$$

ergiebt, wenn $\partial$ die Divisoren von $n$, die grösser sind als $\sqrt{n}$, durchläuft.

Nach dieser Bestimmung besteht also der aus der Summation von (18) hervorgehende Ausdruck

$$\Sigma k h,$$

wenn wir der Deutlichkeit halber $h$ mit $h(m)$ bezeichnen, aus allen Gliedern der Form

$$h\left(\frac{\sigma^2 n - y^2}{x^2}\right),$$

worin $y$ alle positiven und negativen Zahlwerthe durchläuft, für welche $\sigma^2 n - y^2$ positiv ist, während $x$ jeden der quadratischen Factoren von $\sigma^2 n - y^2$ bedeuten kann und $\sigma$ sowohl $= 1$ als $= 2$ zu setzen ist. Nun ist aber die Zahl der primitiven Classen der Determinante $-m$ gleich der Zahl der nicht primitiven Classen der Determinante $-mx^2$ vom Theiler $\sigma x$, und wenn wir also die Summe

$$\overset{x}{\Sigma} h\left(\frac{\sigma^2 n - y^2}{x^2}\right)$$

bei feststehenden $n$ und $y$ über alle quadratischen Factoren von $\sigma^2 n - y^2$ nehmen, so erhalten wir für $\sigma = 1$ die Gesammtanzahl aller primitiven und imprimitiven Classen erster Art der Determinante $-(n - y^2)$, für $\sigma = 2$ und ein gerades $y$ und folglich auch ein gerades $x$ die Gesammtzahl der primitiven und imprimitiven Classen zweiter Art der Determinante $-\left(n - \frac{y^2}{4}\right)$ und für ein ungerades $y$ die Gesammtzahl aller Formen zweiter Art der Determinante $-(4n - y^2)$.

Fassen wir also Alles zusammen und bezeichnen mit $K(m)$ die Gesammtzahl aller Classen der Determinante $-m$, mit $K'(m)$ die Gesammtzahl aller aus Classen zweiter Art der Determinante $-m$ derivirten Classen mit der Einschränkung, dass eine durch die Form $(x, 0, x)$ repräsentirte Classe nur mit $^1/_2$ und eine durch die Form $(2x, x, 2x)$ repräsentirte Classe nur mit $^1/_3$ in Rechnung gesetzt werden soll, so ergiebt sich die für jedes beliebige $n$ gültige Classenzahlrelation

$$\begin{aligned} K(n) + 2K(n-1) + 2K(n-4) + \cdots \\ + 2K'(4n-1) + 2K'(4n-9) + \cdots &= 2\Sigma\partial \end{aligned}$$

oder

$$= 2\Sigma\partial + \sqrt{n} + \frac{1}{6},$$

wo $\Sigma\partial$ die Summe der Divisoren von $n$ bedeutet, die grösser als $\sqrt{n}$ sind, und der zweite Ausdruck gilt, wenn $n$ ein Quadrat ist[1].

---

[1] Die Classenzahlrelationen, von denen die hier abgeleitete nur der einfachste Fall ist, sind von Kronecker entdeckt (Crelle's Journal, Bd. 57, vgl. auch Gierster, Mathematische Annalen, Bd. 21, 22, Hurwitz, ebend., Bd. 25).

## §. 102. Die Classeninvariante $\gamma_3(\omega)$.

Wir betrachten nun die Function

$$\gamma_3(\omega) = \sqrt{j(\omega) - 12^3},$$

deren Quadrat für die singulären Werthe von $\omega$ jedenfalls zu den Classeninvarianten gehört.

Im §. 75, 3. hat sich gezeigt, dass, falls

$$n \equiv 3 \pmod 4$$

(1)
$$M = (-1)^{\frac{a-1}{2}} \partial^3 \left( \frac{\eta\left(\frac{c + \partial\omega}{a}\right)}{\eta(\omega)} \right)^6 \gamma_3(\omega)$$

für ein variables $\omega$ und ein durch 4 theilbares $c$ eine ganze algebraische Function des Körpers

$$j\left(\frac{c + \partial\omega}{a}\right), \quad j(\omega)$$

ist. Lassen wir darin $\omega$, wie im vorigen Paragraphen, in eine Wurzel der quadratischen Gleichung

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

übergehen, so wird $j(\omega)$ eine Classeninvariante; von den $\nu$ Grössen

(3)
$$j\left(\frac{c + \partial\omega}{a}\right)$$

wird eine oder mehrere gleich $j(\omega)$ und die entsprechenden Werthe $M$ sind nach §. 59, 6. algebraisch durch $j(\omega)$ ausdrückbar.

Wir betrachten drei Fälle

1. $$n = m \equiv 3 \pmod 4.$$

Die Gleichung

$$\sigma^2 m = x^2 m + y^2$$

hat, wenn $x$ immer positiv vorausgesetzt wird, nur die eine Lösung

$$x = \sigma, \quad y = 0$$

(ausser wenn $m$ das Dreifache eines Quadrates und $\sigma = 2$ ist, ein Fall, den wir unter Nr. 2 betrachten).

Daher wird nur eine der Grössen (3) gleich $j(\omega)$, und der entsprechende Werth $M$ ist also nach §. 59, 6. rational durch $j(\omega)$ ausdrückbar.

Für diese eine Lösung ist aber nach §. 101, (5), (7), (12)

$$\alpha = \frac{\sigma B}{2},\quad \beta = \sigma A,\quad (-1)^{\frac{a-1}{2}} = -1,$$

$$a = m,\quad \partial = 1,$$

$$\gamma \equiv \sigma C,\quad \alpha + \delta \equiv \sigma B \pmod 4,$$

$$\alpha + \beta\omega = \sqrt{-m},$$

also ergiebt sich, da $A$ ungerade vorausgesetzt ist, nach §. 33, (15)

$$M = (-1)^{\frac{A+B+1}{2}} \sqrt{m}^3\, \gamma_3(\omega),\qquad \sigma = 1, \tag{4}$$

$$M = (-1)^{\frac{B+1}{2}+A+C} \sqrt{-m}^3\, \gamma_3(\omega),\quad \sigma = 2. \tag{5}$$

2. $\qquad n = m = 3m_1^2 \equiv 3 \pmod 4,\quad \sigma = 2.$

Die Gleichung

$$4m = x^2 m + y^2$$

hat drei Lösungen

$$x = 2,\quad y = 0,$$
$$x = 1,\quad y = \pm 3m_1.$$

Für die erste dieser Annahmen gilt die Formel (5); für die beiden anderen ist

$$\alpha = \frac{B \pm 3m_1}{2},\quad \beta = A,$$

$$\gamma \equiv C,\quad \alpha + \delta \equiv B \pmod 4,$$

$$\alpha + \beta\omega = \frac{\pm 3m_1 + \sqrt{-m}}{2}.$$

Die drei entsprechenden Werthe von $M$ sind also

$$(6)\qquad \begin{aligned} &(-1)^{\frac{B+1}{2}+A+C}\sqrt{-m}^3\,\gamma_3(\omega),\\ &(-1)^{\frac{B-1}{2}}\left(\frac{\pm 3m_1 + \sqrt{-m}}{2}\right)^3 \gamma_3(\omega), \end{aligned}$$

und dies sind nach §. 59, 6. die Wurzeln einer cubischen Gleichung, deren Coëfficienten rationale Functionen von $j(\omega)$ sind.

Da $\gamma_3(\omega)^2$ selbst eine rationale Function von $j(\omega)$ ist, so folgt, indem man die Summe oder das Product der Wurzeln (6) betrachtet ebenso wie in 2., dass $\gamma_3(\omega)\sqrt{\pm m}$ eine Classeninvariante ist, wenn das obere Zeichen bei den Formen erster Art, das untere bei den Formen zweiter Art gilt.

3. Es sei $\qquad m \equiv 2 \pmod 4,\quad \sigma = 1.$

Wir machen die Annahme

$$n = m + 1 \equiv 3 \pmod{4}.$$

Die Gleichung

$$m + 1 = x^2 m + y^2$$

hat (immer bei positivem $x$) nur die beiden Lösungen $x = 1$, $y = \pm 1$. Es werden also zwei und nur zwei der Grössen (3) gleich $j(\omega)$; es ist

$$\alpha = \frac{B}{2} \pm 1, \quad \beta = A$$

$$\alpha + \delta \equiv B \pmod{4}$$

$$\alpha + \beta\omega = \pm 1 + i\sqrt{m},$$

und die beiden entsprechenden Werthe von $M$ werden

$$(-1)^{\frac{A+B+1}{2}} (\mp i + \sqrt{m})^3 \gamma_3(\omega),$$

und diese sind wieder (§. 59) die Wurzeln einer quadratischen Gleichung, deren Coëfficienten rational von $j(\omega)$ abhängen. Aus der Summe der beiden Werthe folgt auch hier, dass $\sqrt{m}\,\gamma_3(\omega)$ eine Classeninvariante ist. Damit ist also bewiesen:

Ist $m \equiv 2$ oder $\equiv 3 \pmod{4}$, so ist

$$\sqrt{\pm m}\;\gamma_3(\omega)$$

eine Classeninvariante, wenn das obere Zeichen bei Formen erster Art, das untere bei Formen zweiter Art gilt.

Hieraus lässt sich ein Schluss ziehen über die Berechnung der singulären Moduln $\varkappa^2$.

Es ist nämlich nach §. 49, (4)

$$\gamma_3(\omega) = \frac{8(2 + \varkappa^2\varkappa'^2)(\varkappa'^2 - \varkappa^2)}{\varkappa^2\varkappa'^2}.$$

Betrachten wir zunächst die Formen erster Art, und wählen den Repräsentanten

$$A\omega^2 + 2B\omega + C = 0 \tag{7}$$

so, dass $A$, $C$ ungerade sind, so ist $\varkappa^2\varkappa'^2$ nach §. 93 eine Classeninvariante.

Es lässt sich also $\varkappa^2$ und $\varkappa'^2$ rational ausdrücken durch eine Classeninvariante und durch $\sqrt{m}$ [$m \equiv 2, 3 \pmod{4}$].

Um den entsprechenden Schluss für die Formen zweiter Art zu ziehen, setzen wir

$$\omega = \frac{\omega' - 1}{\omega' + 1}$$

und erhalten aus (7):

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

welches eine zur Determinante $-m$ gehörige Gleichung zweiter Art ist [da $m \equiv 3$, folglich $B$ gerade und $A + C \equiv 0 \pmod 4$].

Es ist aber

$$f(\omega) f(\omega') = \sqrt{2}.$$

Wenn also jetzt $\varkappa^2\varkappa'^2$ den zu $\omega'$ gehörigen Werth dieser Grösse bedeutet, so ist

$$f(\omega')^{24}\varkappa^2\varkappa'^2 = 16, \quad 2^8\varkappa^2\varkappa'^2 = f(\omega)^{24},$$

woraus sich für die zu Formen zweiter Art gehörigen singulären Werthe von $\varkappa^2$ ergiebt, dass $\varkappa^2$ rational durch $\sqrt{-m}$ und eine Classeninvariante erster Art ausdrückbar ist.

Als bemerkenswerthe Beispiele wählen wir die Fälle des §. 92:

$$\gamma_3\left(\frac{-1 + \sqrt{-3}}{2}\right) = 24\sqrt{-3},$$

$$\gamma_3\left(\frac{-1 + \sqrt{-7}}{2}\right) = 27\sqrt{-7},$$

$$\gamma_3\left(\frac{-1 + \sqrt{-11}}{2}\right) = 7.\ 8\sqrt{-11},$$

$$\gamma_3\left(\frac{-1 + \sqrt{-19}}{2}\right) = 8.\ 27\sqrt{-19},$$

$$\gamma_3\left(\frac{-1 + \sqrt{-43}}{2}\right) = 8.\ 7.\ 81\sqrt{-43},$$

$$\gamma_3\left(\frac{-1 + \sqrt{-67}}{2}\right) = 7.\ 8.\ 9.\ 31\sqrt{-67},$$

$$\gamma_3\left(\frac{-1 + \sqrt{-163}}{2}\right) = 8.\ 27.\ 7.\ 11.\ 19.\ 127\sqrt{-163}.$$

Auch hier ist die Zerlegbarkeit der rationalen Factoren in verhältnissmässig kleine Primzahlen auffällig. Für die Formen erster Art geben wir gleichfalls einige Beispiele, berechnen aber nicht $\gamma_3(\omega)$ selbst, sondern $f_1(\omega)^8 - f_2(\omega)^8$, was einfacher ist, und woraus $\gamma_3(\omega)$ leicht abgeleitet werden kann (§. 49, 5.).

Wir haben im §. 95 gefunden

$$f_1(\sqrt{-2})^4 = 2, \quad f(\sqrt{-3})^3 = 2, \quad f(\sqrt{-7})^2 = 2.$$

Darauf wenden wir die Formeln an (§. 96)

$$f_1^8 - f_2^8 = \frac{\sqrt{f^{24} - 64}}{f^4},$$

$$f^8 + f_2^8 = \frac{\sqrt{f_1^{24} + 64}}{f_1^4}$$

und finden

$$f(\sqrt{-2})^8 + f_2(\sqrt{-2})^8 = 4\sqrt{2},$$

$$f_1(\sqrt{-3})^8 - f_2(\sqrt{-3})^8 = \frac{4\sqrt{3}}{\sqrt[3]{2}},$$

$$f_1(\sqrt{-7})^8 - f_2(\sqrt{-7})^8 = 6\sqrt{7}.$$

Hieraus erhält man $\varkappa^2$ und $\varkappa'^2$ aus den Formeln [§. 49, (3)]

$$\varkappa^2 = \frac{f_2(\omega)^8}{f(\omega)^8}, \quad \varkappa'^2 = \frac{f_1(\omega)^8}{f(\omega)^8},$$

also

$$\omega = \sqrt{-2}, \quad \varkappa^2 = (\sqrt{2} - 1)^2,$$

$$\omega = \sqrt{-3}, \quad \varkappa^2 = \frac{2 - \sqrt{3}}{4} = \frac{(1 - \sqrt{3})^2}{8},$$

$$\omega = \sqrt{-7}, \quad \varkappa^2 = \frac{8 - 3\sqrt{7}}{16} = \frac{(3 - \sqrt{7})^2}{32}.$$

## §. 103. Zerlegung der Classengleichung durch Adjunction von $\sqrt{m}$.

Ist $n \equiv 1 \pmod 4$, so ist

$$(1) \qquad M = (-1)^{\frac{a-1}{2}} \partial^3 \left( \frac{\eta\left(\frac{c + \partial\omega}{a}\right)}{\eta(\omega)} \right)^6$$

selbst eine ganze algebraische Function des Körpers

$$j\left(\frac{c + \partial\omega}{a}\right), \quad j(\omega)$$

und wir können darauf die Betrachtung des §. 101 anwenden.

Es sei jetzt

$$m \equiv 0 \quad \text{oder} \quad \equiv 1 \pmod 4,$$

also $\sigma = 1$, und wir setzen entsprechend

$$n = m + 1, \quad n = m.$$

Dann finden wir, wie im vorigen Paragraphen, aus den Formeln (7), (9), (12) des §. 101 und (15), §. 33

(2) $$m \equiv 1 \pmod 4, \quad M = (-1)^{\frac{A-1}{2}} \sqrt{m^3}.$$

(3) $$m \equiv 0 \pmod 4, \quad M = (-1)^{\frac{A+1}{2}} (\sqrt{m} \pm i)^3.$$

Im Falle (2) ist $M$ selbst, im Falle (3) die Summe der beiden Werthe von $M$ rational durch die Classeninvariante $j(\omega)$ ausdrückbar, und je nachdem $A \equiv 1$ oder $\equiv 3 \pmod 4$ ist, hat $M$ das eine oder das andere Zeichen.

Hierin ist der erste Specialfall eines sehr merkwürdigen allgemeinen Theorems enthalten.

Wenn $m$ keine Quadratzahl ist, so lässt sich nach dem Bewiesenen, wenn $u = j(\omega)$ ist, eine Gleichung von der Form

(4) $$\Phi(u) \pm \sqrt{m}\, \Psi(u) = 0,$$

aufstellen, worin $\Phi(u)$ und $\Psi(u)$ rationale Coëfficienten haben, $\Phi(u)$ nicht verschwindet, und das obere oder untere Zeichen gilt, je nachdem $A \equiv 1$ oder $\equiv 3 \pmod 4$ ist. Die Gleichung (4) muss mit der Classengleichung $H_m(u) = 0$ zugleich bestehen, und daraus folgt, indem man den grössten gemeinschaftlichen Theiler von $\Phi(u) \pm \sqrt{m}\, \Psi(u)$ mit $H_m(u)$ aufsucht, dass durch Adjunction von $\sqrt{m}$ die Function $H_m(u)$ in zwei Factoren vom Grade $^1/_2 h$ zerfällt:

(3) $$H_m(u) = [\varphi(u) + \sqrt{m}\, \psi(u)][\varphi(u) - \sqrt{m}\, \psi(u)].$$

Dies stimmt mit einem bekannten zahlentheoretischen Satze überein und beweist ihn sogar, dass nämlich, wenn $m \equiv 0, 1 \pmod 4$, durch eine zur Determinante $-m$ gehörige Formenclasse entweder nur solche ungerade Zahlen $A$ dargestellt werden können, welche $\equiv 1$, oder nur solche, welche $\equiv 3 \pmod 4$ sind, und dass es gleich viel Formenclassen der einen und der anderen Art giebt, oder nach der Sprache der Zahlentheorie, dass die Formenclassen der Determinante $-m$ in zwei Geschlechter zerfallen nach dem Werthe des Charakters

$$(-1)^{\frac{A-1}{2}}$$

(vgl. Dirichlet-Dedekind, Supplement IV).

In dem oben ausgenommenen Falle, dass $m$ ein Quadrat ist, giebt es nur solche Formenclassen, für welche $(-1)^{\frac{A-1}{2}} = +1$ ist.

Dieser Satz ergänzt in schöner Weise den des vorigen Paragraphen und liefert einen Beweis eines Ausspruchs von Kronecker (Monatsberichte der Berliner Akademie, 26. Juni 1862), wonach die singulären Moduln $\varkappa^2$ einer Gleichung genügen, deren Grad gleich ist der Classenzahl, die ausser rationalen Zahlen nur $\sqrt{m}$ in den Coëfficienten enthält. Man hat den eben bewiesenen Satz nur anzuwenden auf die Classeninvariante $\varkappa^2 \varkappa'^2$, und dann $\varkappa^2 - \varkappa^4$ für $\varkappa^2 \varkappa'^2$ in eine der Theilgleichungen einzusetzen 1). Eine Ausnahme bilden allerdings diejenigen Formen, deren Determinante ein negatives Quadrat ist und (nach dem vorigen Paragraphen) die Formen zweiter Art, welche die Adjunction von $\sqrt{-m}$ verlangen.

## §. 104. Quadratische Transformationsgrade.

Die soeben bewiesene Zerlegung der Classengleichung ist nur ein specieller Fall eines allgemeinen von **Kronecker** entdeckten Theorems, nach welchem sich die Classengleichung noch weiter in Factoren zerlegen lässt, zu dessen Beweis wir durch die Annahme gelangen, dass der in §. 101 eingeführte Transformationsgrad $n$ eine ungerade Quadratzahl sei.

Unter dieser Voraussetzung ist, wenn $c$ durch 8 theilbar angenommen wird, nach §. 75, 5.

$$(1) \qquad M = i^{3\frac{a-1}{2}} \left(\frac{c}{e}\right) \sqrt{\partial^3}\, \frac{\eta\left(\frac{c+\partial\omega}{a}\right)^3}{\eta(\omega)^3}$$ 2)

für ein variables $\omega$ Wurzel einer Transformationsgleichung, und zwar eine ganze Function des Körpers

$$j\left(\frac{c+\partial\omega}{a}\right), \quad j(\omega).$$

Lassen wir nun $\omega$ in den besonderen Werth des §. 101 übergehen, so erhalten wir nach §. 59, (6) zwischen $M$ und $u = j(\omega)$ eine rationale Gleichung

$$(2) \qquad \Phi(M, u) = 0,$$

---

1) Nach dem, was weiter unten (§. 106) bewiesen werden wird, kann derselbe Zweck erreicht werden durch Adjunction der Quadratwurzel aus irgend einem nicht quadratischen Theiler von $m$, und dies gilt auch, wenn $m$ ein Quadrat ist.

2) Ist $n$ nicht durch 3 theilbar, so kann auch die dritte Wurzel aus $M$ zu denselben Schlüssen verwandt werden. Um aber keine neue Unterscheidung machen zu müssen, legen wir unseren theoretischen Betrachtungen den Cubus zu Grunde.

deren Grad in Bezug auf $M$ gleich ist der Anzahl der Werthe von

$$v = j\left(\frac{c + \partial\omega}{a}\right),$$

welche gleich $u$ werden, d. h. gleich der Anzahl der verschiedenen Lösungen von

$$\sigma^2 n = m x^2 + y^2 \tag{3}$$

mit positivem $x$, welche der Bedingung (10), §. 101 genügen.

Diese Werthe von $M$ sind aber nach §. 33, (15) zu bestimmen. Es ergiebt sich mit Beibehaltung der Bezeichnung des §. 101:

$$\alpha = \frac{Bx}{2} + \frac{y}{\sigma}, \quad \beta = Ax,$$

$$\text{(4)}\quad x \equiv 0 \pmod{2}, \quad M = \left(\frac{\beta}{\alpha}\right) i^{3\frac{\alpha-1}{2}} e^{\frac{\pi i}{4}\alpha(\gamma-\beta)} \sqrt{\alpha + \beta\omega}^{\,3},$$

$$\text{(5)}\quad x \equiv 1 \pmod{2}, \quad M = \left(\frac{\alpha}{\beta}\right) i^{3\frac{1-\beta}{2}} e^{\frac{\pi i}{4}\beta(\alpha+\delta)} \sqrt{-i(\alpha + \beta\omega)}^{\,3},$$

wobei jedoch zu bemerken ist, dass im ersten Falle $\alpha$, im zweiten $\beta$ als positiv vorausgesetzt, also nöthigenfalls die Vorzeichen von $\alpha$, $\beta$, $\gamma$, $\delta$ alle gleichzeitig umzukehren sind.

Die Quadratwurzeln

$$\text{(6)}\quad \begin{aligned} \sqrt{\alpha + \beta\omega} &= \sqrt{\frac{y + x\sqrt{-m}}{\sigma}}, \\ \sqrt{-i(\alpha + \beta\omega)} &= \sqrt{-i\,\frac{y + x\sqrt{-m}}{\sigma}} \end{aligned}$$

haben positiven reellen Bestandtheil. Diese Werthe von $M$ genügen also der Gleichung (2). Kommen unter ihnen gleiche vor, so kann der Grad der Gleichung (2) durch Absonderung mehrfacher Wurzeln vermindert werden.

Da die Gleichung (2) zur Zerlegung der Classengleichung nach den Vorzeichen von $M$ angewandt werden soll, so ist es von Wichtigkeit, zu entscheiden, ob unter den zu demselben $\omega$ gehörigen Werthen von $M$ [(4) oder (5)] solche vorkommen, welche sich nur durch das Vorzeichen unterscheiden.

Wir untersuchen, wann zwei verschiedene von den Werthen (4), (5), etwa $M$, $M'$, dieselbe 8te Potenz haben. Ist

$$M^8 = M'^8, \tag{7}$$

so muss, wenn $\varrho$ eine zwölfte Einheitswurzel und $x, y$; $x', y'$ zwei verschiedene Lösungen der Gleichung (3) sind

$$(8) \qquad y' + ix'\sqrt{m} = \varrho\,(y + ix\sqrt{m})$$

sein, woraus, indem man rechts und links mit $y - ix\sqrt{m}$ multiplicirt,

$$(9) \qquad yy' + mxx' + i\sqrt{m}\,(yx' - xy') = \varrho\,\sigma^2 n.$$

Dies ist unmöglich für

$$\varrho = \pm 1, \quad \varrho = \frac{\pm i \pm \sqrt{3}}{2},$$

denn nach der ersten Annahme wäre $x'$, $y'$ von $x$, $y$ nicht verschieden, nach der zweiten wäre in (9) der reelle Theil links rational, rechts irrational.

Es bleiben also zur Erfüllung der Gleichungen (7) oder (8) zwei Möglichkeiten übrig.

1. $$\varrho = \pm i;$$

$$(10) \qquad x'\sqrt{m} = \pm y, \quad y' = \mp x\sqrt{m},$$

worin das Vorzeichen so zu wählen ist, dass $x$ und $x'$ positiv werden. Es folgt hieraus, dass $m$ ein Quadrat (mithin $\sigma = 1$), dass $y$ durch $\sqrt{m}$ und daher $n$ durch $m$ theilbar sein muss.

Wenn andererseits unter der Voraussetzung, dass $m$ ein Quadrat und $n$ durch $m$ theilbar sei, $x$, $y$ eine Lösung von (3) ist, so ergiebt sich mittelst der Gleichungen (10) eine zweite Lösung $x'$, $y'$, aus welcher auf demselben Wege wieder $x$, $y$ hergeleitet wird.

2. $$\varrho = \pm \frac{-1 + i\sqrt{3}}{2};$$

$$y' = \pm \frac{-y - x\sqrt{3m}}{2},$$

$$x'\sqrt{m} = \pm \frac{y\sqrt{3} - x\sqrt{m}}{2},$$

$$2\,(yx' - xy')\sqrt{m} = \pm \sqrt{3}\,\sigma^2 n,$$

worin das Vorzeichen von $\sqrt{3}$ beliebig genommen werden kann und dann $\pm$ so bestimmt werden muss, dass $x'$ positiv wird. Man leitet also aus einem Paar $x$, $y$ zwei Paare $x'$, $y'$ ab.

Es folgt hieraus, dass $\sigma = 2$, ferner, dass $3m$ ein Quadrat, $y$, $y'$ durch $\sqrt{\frac{m}{3}}$ und folglich $n$ durch $\frac{m}{3}$ theilbar sein muss.

Wenn also von diesen beiden Ausnahmefällen keiner eintritt, so können wir schliessen, dass von den vier Gleichungen

$$\Phi(M, u) = 0,\quad \Phi(-M, u) = 0,\quad \Phi(iM, u) = 0,\quad \Phi(-iM, u) = 0$$
nicht zwei zugleich erfüllt sein können, dass sie also in Bezug auf $u$ keinen gemeinsamen Theiler haben. In den Ausnahmefällen wird derselbe Schluss erst dann zu ziehen sein, wenn nachgewiesen ist, dass die zwei oder drei Werthe von $M$, welche die gleiche 8te Potenz haben, selbst einander gleich sind[1]).

## §. 105. Die Geschlechter der quadratischen Formen.

Ist $m$ eine beliebige positive ganze Zahl und $A$ eine zu $2m$ theilerfremde positive Zahl, von welcher $-m$ quadratischer Rest ist, so giebt es primitive Formen erster oder zweiter ($\sigma$ter) Art der Determinante $-m$, deren erster Coëfficient $\sigma A$ ist:

$$\left(\sigma A,\ \frac{\sigma}{2} B,\ \sigma C\right)$$

Umgekehrt folgt auch aus

$$4m = \sigma^2(4AC - B^2),$$

dass $-m$ quadratischer Rest von $A$ sein muss. Ist $S^2$ die grösste in $m$ aufgehende Quadratzahl und

$$m = S^2 m_0 \text{ entweder } = S^2 P \quad \text{oder} \quad = 2S^2 P,$$

worin $P$ ungerade ist, so haben wir nach dem Reciprocitätsgesetz der quadratischen Reste (vgl. Dirchlet-Dedekind, §. 52):

$$\begin{aligned}
(1)\qquad 1 = \left(\frac{-m}{A}\right) = \left(\frac{-m_0}{A}\right) &= \left(\frac{A}{P}\right), & m_0 &\equiv 3 \pmod 4,\\
&= \left(\frac{-1}{A}\right)\left(\frac{A}{P}\right), & m_0 &\equiv 1 \pmod 4,\\
&= \left(\frac{2}{A}\right)\left(\frac{A}{P}\right), & m_0 &\equiv 6 \pmod 8,\\
&= \left(\frac{-2}{A}\right)\left(\frac{A}{P}\right), & m_0 &\equiv 2 \pmod 8.
\end{aligned}$$

Es sollen hier die Sätze zusammengestellt werden, auf Grund deren Gauss[2]) die verschiedenen Classen quadratischer Formen

---

[1]) In des Verfassers oben erwähnter Arbeit „Zur Theorie der elliptischen Functionen“, §. 21, Acta Mathem., Bd. 6, hat sich bei der Discussion des ersten dieser Ausnahmefälle ein Irrthum eingeschlichen, der nach dem Folgenden zu berichtigen ist.

[2]) Gauss, Disq. ar. art. 228 ff.

einer Determinante in Geschlechter eingetheilt hat, die der Leser im vierten Supplement von Dirichlet-Dedekind, Vorlesungen über Zahlentheorie, findet, bemerken aber gleich, dass wir diese Sätze nicht vorauszusetzen brauchen, dass sie nur der leichteren Uebersicht wegen hier vorangestellt werden; wir werden aus der Theorie der elliptischen Functionen neue Beweise für diese Sätze herleiten.

Wir behalten die Bedeutung von $m$ und $A$ bei und verstehen unter $m''$ irgend einen ungeraden, durch kein Quadrat theilbaren Divisor von $m$; dann haben die Symbole

$$(2) \quad \begin{array}{ll} \left(\frac{A}{m''}\right), & m \equiv 3 \pmod 4, \\ \left(\frac{A}{m''}\right), \left(\frac{-1}{A}\right), & m \equiv 1 \pmod 4, \\ \left(\frac{A}{m''}\right), \left(\frac{2}{A}\right), & m \equiv 6 \pmod 8, \\ \left(\frac{A}{m''}\right), \left(\frac{-2}{A}\right), & m \equiv 2 \pmod 8, \\ \left(\frac{A}{m''}\right), \left(\frac{-1}{A}\right), & m \equiv 4 \pmod 8, \\ \left(\frac{A}{m''}\right), \left(\frac{-1}{A}\right), \left(\frac{2}{A}\right), & m \equiv 0 \pmod 8) \end{array}$$

einen von der besonderen Wahl von $A$ unabhängigen, nur von der Formenclasse, durch welche $A$ darstellbar ist, abhängigen Werth. Die Grössen (2) heissen die Charaktere der betreffenden Formenclasse. Beschränkt man $m''$ auf die in $m$ aufgehenden, von einander verschiedenen ungeraden Primzahlen, so erhält man das System der von einander unabhängigen Charaktere, deren Anzahl gewöhnlich mit $\lambda$ bezeichnet wird.

Jeder der Charaktere kann den Werth $\pm 1$ haben, aber nach der Formel (1) sind nicht alle Vorzeichencombinationen möglich, sondern ein (zusammengesetzter) Charakter muss den Werth $+1$ haben.

Gauss vereinigt alle diejenigen Formenclassen in ein Geschlecht, welche in sämmtlichen Charakteren übereinstimmen, so dass die Anzahl der möglichen Geschlechter $2^{\lambda-1}$ ist. Ein Hauptsatz dieser Theorie ist der, dass jedes dieser Geschlechter existirt und eine gleich grosse Anzahl von Formenclassen enthält. Wir werden in der Folge für diesen Satz einen Beweis finden, indem wir zugleich zeigen, dass die Classengleichung sich unter Adjunction gewisser Quadratwurzeln in ebenso viele Factoren zerlegen lässt, als Geschlechter vorhanden sind, und dass jede dieser Theilgleichungen durch die Classeninvarianten eines Geschlechtes befriedigt wird.

Dasjenige Geschlecht, dessen Charaktere sämmtlich $= +1$ sind, heisst das Hauptgeschlecht.

Entgegengesetzte Classen gehören demselben Geschlechte an.

Wir fügen noch eine Bemerkung in Bezug auf die Formen zweiter Art hinzu.

Wir haben im §. 89 gesehen, wie man aus einer Form zweiter Art, je nachdem $m \equiv -1$ oder $\equiv 3 \pmod 8$ ist, eine oder drei primitive Formen erster Art derselben Determinante herleitet, und dass man so alle Formenclassen erster Art aus denen der zweiten Art erhält.

Ist $(2A, B, 2C)$ die Form zweiter Art, so sind nach §. 89, (10) die daraus abgeleiteten Formen erster Art:

$$(A,\ B,\ 4\,C),\quad \text{wenn } m \equiv -1 \pmod 8,$$

und

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

wenn $m \equiv 3 \pmod 8$.

Die beiden letzten Formen sind aber bezw. äquivalent mit

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

und hieraus schliesst man, dass die auf diese Weise aus einander abgeleiteten Formen dieselben Charaktere haben, also in das nämliche Geschlecht gehören. Dies ist evident, wenn $m \equiv -1 \pmod 8$. Ist aber $m \equiv 5 \pmod 8$, also $C$ ungerade, so ersieht man das Gleiche aus

$$4\,A\,C - B^2 = 4\,A\,(A - B + C) - (B - 2\,A)^2 = m$$

$$\left(\frac{A}{m''}\right) = \left(\frac{C}{m''}\right) = \left(\frac{A - B + C}{m''}\right).$$

## §. 106. Zerfällung der Classengleichung.

Wir betrachten zunächst allein die Formen und Classeninvarianten erster Art, wobei wir den Vortheil haben, dass der Ausnahmefall (2), §. 104 nicht vorkommen kann. Die entsprechenden Resultate für die Formen zweiter Art können nachträglich mit wenig Worten aus denen für die erste Art hergeleitet werden.

Es genüge also $\omega$ der Gleichung:

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

worin $B$ eine gerade Zahl ist.

Um einen quadratischen Transformationsgrad $n$ zu erhalten, befriedigen wir die Gleichung §. 104, (3)

$$n = y^2 + mx^2$$

in folgender Weise:

Wir zerlegen irgend ein beliebig gegebenes $m$ in zwei Factoren

$$m = m'm'',$$

wobei nur vorausgesetzt sein soll, dass $m''$ ungerade und durch kein Quadrat theilbar sei. Wir setzen dann

$$(1) \qquad x = 4, \quad y = 4m' - m''$$

$$(2) \qquad n = (4m' + m'')^2,$$

$$(3) \qquad \alpha + \beta\omega = \left(2\sqrt{m'} + i\sqrt{m''}\right)^2 \quad [\text{§. } 104, (6)].$$

Die Berechnung von $M$ nach der Formel §. 104, (4) ist einfach auszuführen auf Grund von

$$\alpha = 2B + 4m' - m''$$

$$\alpha m'' = 4AC - (B - m'')^2 \qquad [\text{§. } 101, (5), (12)]$$

$$\beta = 4A, \quad \gamma \equiv 4C \pmod{8}$$

$$\left(\frac{\beta}{\alpha}\right)\left(\frac{A}{m''}\right) = \left(\frac{A}{\alpha m''}\right) = 1, \quad i^{\frac{\alpha-1}{2}} = (-1)^C\, i^{-\frac{m''+1}{2}}$$

und ergiebt nach §. 104, (4):

$$(4) \qquad M = -\left(\frac{A}{m''}\right)\left(2\, i^{-\frac{m''+1}{2}}\sqrt{m'} + i^{-\frac{m''-1}{2}}\sqrt{m''}\right)^3.$$

Der Ausnahmefall 1. des §. 104 tritt nur dann ein, wenn $m$ eine ungerade Quadratzahl und $m'' = m' = \sqrt{m}$, und $\sqrt{m}$ keinen quadratischen Theiler, also $m$ jeden Primfactor zweimal und nur zweimal enthält. Denn es müsste ja $m$ ein Quadrat und daher zunächst, da $m''$ keinen quadratischen Theiler enthält, $m'$ durch $m''$ theilbar sein, etwa $m' = h^2 m''$. Andererseits müsste $n = (4m' + m'')^2 = m''^2(4h^2 + 1)^2$ durch $m$, also $(4h^2 + 1)^2$ durch $h^2$, woraus $h = 1$ folgt.

In diesem Falle wendet man einfacher die Transformation $m$ten Grades an, indem man

$$x = 1, \quad y = 0, \quad -i(\alpha + \beta\omega) = \sqrt{m} = m''$$

setzt.

Es ist hier [§. 105, (1)]:

$$A \equiv 1 \pmod{4},$$

ferner [§. 101, (6), (12)]

$$\alpha = {}^1/_2 B, \quad \beta = A, \quad \alpha + \delta \equiv 0 \pmod{8},$$

$$B m'' = (m'' + {}^1/_2 B)^2 - A C,$$

folglich

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{m''}{A}\right) = \left(\frac{{}^1/_2 B m''}{A}\right) = (-1)^{\frac{A-1}{4}}$$

und danach ergiebt die Formel (5), §. 104:

$$M = \left(\frac{A}{m''}\right)\sqrt{m''}^3. \tag{5}$$

Diese Formeln [(4), (5)] enthalten die Beweise für die im vorigen Paragraphen erwähnten Sätze über die Eintheilung der Classen quadratischer Formen in Geschlechter und geben zugleich das Mittel, durch Adjunction von Quadratwurzeln die Classengleichung in Factoren zu zerlegen, welche den Geschlechtern der Formenclassen entsprechen.

Um dies darzulegen, schicken wir folgende Bemerkungen voraus.

Die Classeninvarianten für zwei entgegengesetzte Formen sind, wie aus der Darstellung durch $q$ unmittelbar zu ersehen, conjugirt imaginär, und daraus folgt, dass die Classeninvarianten ambiger Classen, d. h. solcher Classen, die mit ihren entgegengesetzten identisch sind, reelle Werthe haben. Die in (4) und (5) bestimmten Zahlen $M$ genügen also für $u = j(\omega)$ einer Gleichung

$$\Phi(M, u) = 0, \tag{6}$$

welche wir uns auf ihren grössten gemeinschaftlichen Theiler mit der Classengleichung $H_m(u) = 0$ reducirt und so geschrieben denken, dass die höchste Potenz von $u$ den Coëfficienten 1 hat. Die Gleichung (6) besteht dann für keinen Werth von $u$ mit der Gleichung $\Phi(-M, u) = 0$ zugleich. Andererseits erfüllt jede zur Determinante $-m$ gehörige Classeninvariante $u$ (erster Art), wenn wir

$$-\mu = \left(2 i^{-\frac{m''+1}{2}}\sqrt{m'} + i^{-\frac{m''-1}{2}}\sqrt{m''}\right)^3 \tag{7}$$

oder im Falle (5)

$$\mu = \sqrt{m''}^3 \tag{8}$$

setzen, eine und nur eine der beiden Gleichungen

$$(9) \qquad \Phi(\mu, u) = 0, \quad \Phi(-\mu, u) = 0,$$

und zwar die erste oder die zweite, je nachdem

$$\left(\frac{A}{m''}\right) = +1 \quad \text{oder} \quad = -1.$$

Es folgt hieraus, dass dies Vorzeichen nicht von der besonderen Wahl von $A$, sondern nur von der betreffenden Formenclasse abhängig ist; daher wird dies Vorzeichen ein Charakter der Formenclasse genannt. Da hiernach entgegengesetzte Formen denselben Charakter haben, so folgt, dass die Gleichungen (9) reelle Coëfficienten haben müssen, und dass also, wenn wir mit $\mu'$ den zu $\mu$ conjugirten Werth bezeichnen:

$$(10) \; \Phi(\mu, u) = {}^1\!/_2 [\Phi(\mu, u) + \Phi(\mu', u)] = \psi(\sqrt{m''}, u),\ m'' \equiv 1 \pmod 4$$
$$= \psi(\sqrt{m'}, u),\ m'' \equiv 3 \pmod 4)\,^{1)},$$

worin $\psi$ ausser $\sqrt{m''}$ oder $\sqrt{m'}$ nur rationale Coëfficienten enthält.

Nun ändert $M$ sein Vorzeichen durch die gleichzeitigen Vertauschungen

$$(11) \quad \begin{array}{lll} (i, -i), & (\sqrt{m''}, -\sqrt{m''}), & m'' \equiv 1 \pmod 4 \\ (i, -i), & (\sqrt{m'}, -\sqrt{m'}), & m'' \equiv 3 \pmod 4). \end{array}$$

$H_m(u)$ ist theilbar durch $\Phi(M, u)$ und da $H_m(u)$ rationale Coëfficienten hat, so kann man in $\Phi(M, u)$ die Vorzeichenänderungen (11) vornehmen, wenn nicht $m'' = 1$ oder $m'' \equiv 3 \pmod 4$ und zugleich $\sqrt{m'}$ rational, also $m'$ ein Quadrat ist.

Abgesehen von diesen letzten Fällen folgt also, da $\Phi(M, u)$, $\Phi(-M, u)$ keinen gemeinsamen Theiler haben

$$(12) \qquad H_m(u) = \Phi(M, u)\, \Phi(-M, u),$$

d. h. es giebt ebenso viele Classen, in welchen der Charakter $\left(\frac{A}{m''}\right) = +1$ ist, wie solche, in denen er $= -1$ ist.

Nach diesem Vorzeichen zerfallen die Classen der Determinante $-m$ in zwei Geschlechter, deren jedes gleich viele Formenclassen enthält, und die Classengleichung zerfällt nach Adjunction von $\sqrt{m''}$ oder $\sqrt{m'}$ [je nachdem $m'' \equiv 1$, oder $\equiv 3 \pmod 4$ ist] in zwei Factoren.

---

1) Unter der Voraussetzung von (5) werden die beiden Fälle (10) identisch.

Ist $m'$ ein Quadrat (also die grösste in $m$ enthaltene Quadratzahl) und $m'' \equiv 3 \pmod 4$, so ist $\Phi(M, u)$ rational und $H_m(u)$ lässt sich nicht auf diese Weise zerlegen. In diesem Falle ist nach §. 105, (1) für alle Formenclassen:

$$\left(\frac{A}{m''}\right) = +1.$$

Hat man eine der hier betrachteten Zerlegungen bereits ausgeführt, und wählt an Stelle von $m''$ einen anderen, denselben Bedingungen genügenden Theiler $m'''$ von $m$, so kann man in der vorigen Betrachtung die Gleichung $H_m(u) = 0$ durch eine dem $m''$ entsprechende Theilgleichung ersetzen und ganz dieselben Schlüsse ziehen, wodurch also eine weitergehende Zerfällung von $H_m(u)$ bewirkt wird.

Wir wollen die Anwendung auf die einzelnen Fälle etwas genauer betrachten.

Ist $m \equiv 3 \pmod 4$, so sind alle Charaktere in der Form

$$\left(\frac{A}{m''}\right)$$

enthalten, und die Formel (4) reicht hin, um alle Geschlechter von einander zu trennen. Die Gleichung (10) zeigt aber, dass in den Theilgleichungen nur die Quadratwurzeln aus solchen Zahlen vorkommen, welche von der Form $4n + 1$ sind. Bezeichnen wir also mit $p, p', p'' \dots$ die Primfactoren von $m$ von der Form $4n + 1$, mit $q, q', q'' \dots$ die Primfactoren von $m$ von der Form $4n + 3$, so kommen in den Theilgleichungen nur die folgenden Quadratwurzeln vor:

$$\sqrt{p},\ \sqrt{p'},\ \sqrt{p''} \dots \sqrt{qq'},\ \sqrt{qq''} \dots,$$

wenn also nur ein $q$ in $m$ enthalten ist, so kommt $\sqrt{q}$ in den Theilgleichungen nicht vor.

Ist ferner

$$m \equiv 1 \pmod 4, \quad m \equiv 6, 2 \pmod 8, \quad m \equiv 4 \pmod{16},$$

so können nach der Formel (1), §. 105 beziehungsweise die Charaktere

$$\left(\frac{-1}{A}\right),\ \left(\frac{2}{A}\right),\ \left(\frac{-2}{A}\right),\ \left(\frac{-1}{A}\right)$$

durch die Charaktere von der Form

$$\left(\frac{A}{m''}\right)$$

ausgedrückt werden, und es reicht also auch in diesen Fällen die Formel (4) hin, um alle Geschlechter von einander zu trennen.

Die Formeln (7), (10) lehren, dass in diesen Fällen zur vollständigen Trennung der Geschlechter folgende Adjunctionen nöthig sind:

$$m \equiv 1 \pmod 4,\quad \sqrt{p},\ \sqrt{p'},\ \sqrt{p''} \ldots\quad \sqrt{q},\ \sqrt{q'},\ \sqrt{q''} \ldots$$
$$m \equiv 6 \pmod 8,\quad \sqrt{2},\ \sqrt{p},\ \sqrt{p'},\ \sqrt{p''} \ldots\quad \sqrt{qq'},\ \sqrt{qq''} \ldots$$
$$m \equiv 2 \pmod 8,\quad \sqrt{p},\ \sqrt{p'},\ \sqrt{p''} \ldots\quad \sqrt{2q},\ \sqrt{2q'},\ \sqrt{2q''} \ldots$$
$$m \equiv 4 \pmod{16},\quad \sqrt{p},\ \sqrt{p'},\ \sqrt{p''} \ldots\quad \sqrt{q},\ \sqrt{q'},\ \sqrt{q''} \ldots$$

In den noch übrigen Fällen, nämlich $m \equiv 12 \pmod{16}$ und $m \equiv 0 \pmod 8$ ist die vorstehende Zerlegung zwar auch noch anwendbar, in den so gewonnenen Theilgleichungen sind aber immer noch je zwei oder je vier Geschlechter vereinigt, entsprechend den Charakteren

$$\left(\frac{-1}{A}\right),\ \left(\frac{2}{A}\right).$$

Wir leiten also noch eine zweite Transformationsformel wie (4) her, indem wir die Gleichung (3), §. 104 folgendermaassen befriedigen:

$$m = m'm'' \equiv 0 \pmod 4,$$
$$x = 2,\quad y = m' - m'',\quad n = (m' + m'')^2,$$
$$\sqrt{\alpha + \beta\omega} = \sqrt{m'} + i\sqrt{m''},$$

worin wieder $m''$ ungerade und durch kein Quadrat theilbar angenommen ist, aber auch $= 1$ sein kann, und aus §. 104, (4) erhält man [1]):

---

[1]) Es ist

$$\alpha = B + m' - m'',\quad \beta = 2A,\quad \gamma \equiv -2C \pmod 8$$
$$\alpha m'' = AC - \left(\frac{1}{2}B - m''\right)^2.$$

Nehmen wir der Einfachheit halber $B \equiv 0$, also auch $C \equiv 0 \pmod 4$, so ist $\alpha \equiv C - m'' \pmod 8$ und folglich

$$i^{3\frac{\alpha-1}{2}}\, e^{\frac{\pi i}{4}\alpha(\gamma-\beta)} = (-1)^{\frac{1}{4}C}\,(-1)^{\frac{A+1}{2}}\, i^{3\frac{m''-1}{2}},$$
$$\left(\frac{\beta}{\alpha}\right) = \left(\frac{2}{m''}\right)\left(\frac{A}{m''}\right)\left(\frac{2}{\alpha m''}\right)\left(\frac{A}{\alpha m''}\right).$$
$$\left(\frac{A}{\alpha m''}\right) = 1,\quad \left(\frac{2}{\alpha m''}\right) = (-1)^{\frac{1}{4}C},$$

woraus unsere Formel folgt.

$$(13)\quad M = -\left(\frac{2}{m''}\right)\left(\frac{A}{m''}\right)\left(\frac{-1}{A}\right)\left(i^{\frac{m''-1}{2}}\sqrt{m'} + i^{\frac{m''+1}{2}}\sqrt{m''}\right)^3.$$

Diese Formel ergänzt die vorige für den Fall $m \equiv 12 \pmod{16}$, und zeigt, dass auch in diesem Falle die vollständige Zerfällung der Classengleichung durch Adjunction von

$$\sqrt{p},\ \sqrt{p'},\ \sqrt{p''} \ldots \quad \sqrt{q},\ \sqrt{q'},\ \sqrt{q''} \ldots$$

geschieht.

Ist nun $m$ durch eine noch höhere als die zweite Potenz von 2 theilbar, so kann man, wenn diese Potenz eine ungerade ist, nach §. 105, (1) alle Charaktere auf solche von der Form

$$\left(\frac{A}{m''}\right),\ \left(\frac{-1}{A}\right)\left(\frac{A}{m''}\right)$$

zurückführen und die Gleichungen (4) und (13) genügen zur vollständigen Zerfällung der Classengleichung unter Adjunction der Quadratwurzeln aus sämmtlichen in $m$ aufgehenden Primzahlen.

Ist aber der Exponent der höchsten in $m$ aufgehenden Potenz von 2 eine gerade Zahl, so genügt auch (13) noch nicht zur vollständigen Zerlegung der Classengleichung. Wir leiten daher, unter der Voraussetzung, dass $m$ durch 8 theilbar sei, noch eine dritte Formel her.

Wir setzen

$$m = m'm'',$$

$$x = 1,\quad y = \frac{1}{4}m' - m'',\quad n = \left(\frac{1}{4}m' + m''\right)^2.$$

$$\sqrt{-i(\alpha + \beta\omega)} = e^{-\frac{\pi i}{4}}\left(\frac{1}{2}\sqrt{m'} + i\sqrt{m''}\right),$$

worin wieder $m''$ ungerade und durch kein Quadrat theilbar ist. Hier folgt aus §. 104, (5):

$$(14)\quad M = (-1)^{\frac{m}{8}} e^{\frac{\pi i}{4}Am''}\left(\frac{A}{m''}\right)\left(i^{-\frac{m''+1}{2}}\frac{1}{2}\sqrt{m'} + i^{-\frac{m''-1}{2}}\sqrt{m''}\right)^3.$$

Nachdem die Zerlegung nach den Charakteren $\left(\frac{A}{m''}\right)$ durch die Formeln (4) und (13) erledigt ist, handelt es sich nur noch um die Zerlegung nach den Charakteren

$$\left(\frac{-1}{A}\right),\ \left(\frac{2}{A}\right),$$

d. h. nach dem Verhalten von $A$ gegen den Modul 8. Es genügt daher, in der Formel (14) $m'' = 1$ zu setzen, wodurch man folgende vier Werthe von $M$ erhält:

$$
(15) \quad
\begin{aligned}
M &= (-1)^{\frac{m}{8}} \frac{1+i}{\sqrt{2}} \left(1 - i\frac{1}{2}\sqrt{m}\right)^3, & A &\equiv 1 \pmod 8,\\
M &= (-1)^{\frac{m}{8}} \frac{-1+i}{\sqrt{2}} \left(1 - i\frac{1}{2}\sqrt{m}\right)^3 = M', & A &\equiv 3 \pmod 8,\\
M &= (-1)^{\frac{m}{8}} \frac{-1-i}{\sqrt{2}} \left(1 - i\frac{1}{2}\sqrt{m}\right)^3 = M'', & A &\equiv 5 \pmod 8,\\
M &= (-1)^{\frac{m}{8}} \frac{1-i}{\sqrt{2}} \left(1 - i\frac{1}{2}\sqrt{m}\right)^3 = M''', & A &\equiv 7 \pmod 8).
\end{aligned}
$$

Die vier Werthe von $M$ gehen aus dem ersten hervor durch die Vertauschungen:

$$
(16) \quad
\begin{array}{llll}
M, & \sqrt{2}, & i, & \sqrt{m},\\
M', & -\sqrt{2}, & -i, & -\sqrt{m},\\
M'', & -\sqrt{2}, & i, & \sqrt{m},\\
M''', & \sqrt{2}, & -i, & -\sqrt{m}.
\end{array}
$$

Ist nun $\Phi(M, u) = 0$ in demselben Sinne wie oben die zwischen $u$ und $M$ bestehende Gleichung, so sind die vier Functionen

$$\Phi(M, u), \quad \Phi(-M, u), \quad \Phi(iM, u), \quad \Phi(-iM, u)$$

ohne gemeinsamen Theiler, und wenn $\Phi(M, u)$ in $H_m(u)$ enthalten ist, so sind auch die drei anderen Functionen $\Phi(-M, u)$, $\Phi(iM, u)$, $\Phi(-iM, u)$ in $H_m(u)$ enthalten, da die Vorzeichen der Irrationalitäten (16) beliebig geändert werden können. Es ist daher

$$H_m(u) = \Phi(M, u)\,\Phi(-M, u)\,\Phi(iM, u)\,\Phi(-iM, u)$$

und es kommt also jeder der vier Fälle

$$A \equiv 1, \quad A \equiv 3, \quad A \equiv 5, \quad A \equiv 7 \pmod 8$$

in gleich vielen Formenclassen der Determinante $-m$ vor.

Eine Ausnahme tritt nur dann ein, wenn $m$ ein Quadrat oder das Doppelte eines Quadrates ist, weil im ersten Falle $\sqrt{m}$ rational und daher nur die Vertauschung $(M, M'')$ gestattet ist, im zweiten Falle $\sqrt{2}$ und $\sqrt{m}$ gleichzeitig ihr Zeichen ändern, also nur die Vertauschung $(M, M')$ zulässig ist.

Im ersten Falle kommen nach §. 105, (1) nur die beiden Congruenzen

$$A \equiv 1, \quad A \equiv 5 \pmod 8,$$

im zweiten Falle nur die beiden Congruenzen

$$A \equiv 1, \quad A \equiv 3 \pmod 8$$

vor, und zwar wieder in gleich viel Formenclassen. Die vollständige Zerlegung der Classengleichung nach den Geschlechtern erfordert, wenn $m$ durch 8 theilbar ist, immer die Adjunction der Wurzeln aus sämmtlichen in $m$ aufgehenden Primzahlen.

Was nun die Formen zweiter Art betrifft, so ergiebt sich die gleiche Möglichkeit der Zerlegung der Classengleichung nach den Geschlechtern unmittelbar aus §. 89. Denn das Product

$$\Pi[x - j(\omega)],$$

ausgedehnt über die sämmtlichen, einem Geschlecht angehörigen Classeninvarianten zweiter Art, lässt sich darstellen als symmetrische Function der Classeninvarianten erster Art, durch welche die der zweiten Art rational ausdrückbar sind, und diese bilden ein Geschlecht von Classeninvarianten erster Art.

## §. 107. Beispiele.

Zur wirklichen Ausrechnung der Zerfällung der Classengleichung sind die Formeln des vorigen Paragraphen nur in beschränktem Maasse anwendbar wegen des zu hohen Grades der Transformationsgleichungen. Wir werden nachher in einem Falle eine wenigstens nahe verwandte Methode zur Anwendung bringen. Ist die Classengleichung bekannt, so lässt sich meist leichter die Zerlegung direct finden, indem man einen Ansatz von bekannter Form mit unbestimmten Coëfficienten macht; so findet man aus den Formeln §. 97, (2), (29), (37) die folgenden Theilgleichungen, worin das positive Zeichen der Quadratwurzel dem Hauptgeschlecht entspricht:

$$m = 50, \qquad f_1(\sqrt{-50}) = \sqrt[4]{2}\, x,$$

$$x^3 - x^2 = \frac{1 + \sqrt{5}}{2}(x + 1),$$

$$m = 26, \qquad f_1(\sqrt{-26})^2 = \sqrt{2}\, x,$$

$$x^3 - x^2 = \frac{3 + \sqrt{13}}{2}(x + 1),$$

$$m = 41, \qquad z = \frac{f_1(\sqrt{-41})^2}{\sqrt{2}} + \frac{\sqrt{2}}{f_1(\sqrt{-41})^2},$$

$$z^2 - \frac{5 + \sqrt{41}}{2} z + \frac{7 + \sqrt{41}}{2} = 0.$$

Um aber eine Anwendung unserer allgemeinen Methode zu geben, nehmen wir $m \equiv 3 \pmod 8$ an und setzen eine Form zweiter Art voraus. Wir befriedigen die Gleichung

$$4\,n = m x^2 + y^2$$

[§. 104, (3)], indem wir setzen

$$m = m' m'',$$

$$x = 1, \quad y = \frac{m' - m''}{2}, \quad 4\,n = \left(\frac{m' + m''}{2}\right)^2,$$

wobei $n$ ungerade ausfällt. Es wird ferner

$$\alpha + \beta \omega = \left(\frac{\sqrt{m'} + i\sqrt{m''}}{2}\right)^2.$$

Setzen wir unter der Voraussetzung, dass $n$ durch 3 nicht theilbar ist

$$(1) \qquad M = \left(\frac{c}{e}\right) i^{\frac{a-1}{2}} \sqrt{\partial}\, \frac{\eta\left(\frac{c + \partial\omega}{a}\right)}{\eta(\omega)},$$

so lässt sich $M$ mit Anwendung von §. 101 und §. 33, (15) bestimmen und man findet, wenn $m''$ denjenigen der beiden Factoren $m'$, $m''$ bedeutet, welcher modulo 4 mit 1 congruent ist

$$(2)\ M = -\left(\frac{A}{m''}\right)(-1)^{\frac{m' - m'' - 2}{8}}\, e^{-\frac{\pi i}{3} A (m' - m'')}\, \frac{\sqrt{m''} - i\sqrt{m'}}{2}.$$

Um hiervon eine Anwendung zu machen, setzen wir $n = 25$, also

$$20 = m' + m'',$$

und folglich

$$\begin{aligned}
m'' &= 1, & m' &= 19, & m &= 19,\\
m'' &= 17, & m' &= 3, & m &= 51,\\
m'' &= 13, & m' &= 7, & m &= 91,\\
m'' &= 9, & m' &= 11, & m &= 99.
\end{aligned}$$

Legen wir die Form zweiter Art

$$\left(2, \frac{m' - m''}{2}, 2\,n\right)$$

zu Grunde, so ist $A = 1$ zu setzen, und (2) ergiebt:

$$
\begin{aligned}
m &= 19, & M &= -\frac{1 - i\sqrt{19}}{2},\\
m &= 51, & M &= e^{-\frac{\pi i}{3}}\,\frac{\sqrt{17} - i\sqrt{3}}{2},\\
m &= 91, & M &= \frac{\sqrt{13} - i\sqrt{7}}{2},\\
m &= 99, & M &= e^{\frac{\pi i}{3}}\,\frac{3 - i\sqrt{11}}{2}.
\end{aligned}
\tag{3}
$$

Nun genügt nach §. 75, (27), (28) $M$ einer Transformationsgleichung (invarianten Multiplicatorgleichung), die, wenn

$$
\begin{aligned}
\chi &= M^5 + 5\,M^4 + 15\,M^3 + 25\,M^2 + 25\,M\\
&= M^3\left[\left(M + \frac{5}{M}\right)^2 + 5\left(M + \frac{5}{M}\right) + 5\right]
\end{aligned}
$$

gesetzt wird, die Gestalt erhält:

$$
j(\omega) = \gamma_2(\omega)^3 = \frac{(\chi^2 + 10\,\chi + 5)^3}{\chi}.
\tag{4}
$$

Für $m = 19$ erhält man hieraus den schon oben (§. 92) gefundenen Werth

$$
\gamma_2\left(\frac{-3 + \sqrt{-19}}{2}\right) = 96,
$$

und für die drei übrigen Werthe von $m$ erhält man

$$
\begin{aligned}
& j\left(\frac{-7 + \sqrt{-51}}{2}\right) = -\,2^{14}\,.\,27\,(6263 + 1519\sqrt{17}),\\
& \gamma_2\left(\frac{-3 + \sqrt{-91}}{2}\right) = -\,48\,(227 + 63\sqrt{13}),\\
& j\left(\frac{-1 + \sqrt{-99}}{2}\right) = -\,2^{12}\,(4\,591\,804\,316 + 799\,330\,532\sqrt{33}).
\end{aligned}
\tag{5}
$$

Hieraus kann man zu cubischen Gleichungen für

$$
f(\sqrt{-51})^{24},\quad f(\sqrt{-91})^{8},\quad f(\sqrt{-99})^{24}
$$

gelangen, indem man von den Formeln Gebrauch macht (§. 29, §. 49):

$$
f_2\left(\frac{-r + \sqrt{-m}}{2}\right) = \frac{\sqrt{2}\,e^{-\frac{r\pi i}{24}}}{f(\sqrt{-m})},
$$

$$
\gamma_2\left(\frac{-r + \sqrt{-m}}{2}\right)e^{-\frac{r\pi i}{3}} = \frac{f(\sqrt{-m})^{24} - 16^2}{f(\sqrt{-m})^{16}},
$$

worin $r = 7, 3, 1$; $m = 51, 91, 99$ zu setzen ist. Setzt man also für $r = 3$:

$$f(\sqrt{-m}) = x,$$

so erhält man

$$x^{24} + \gamma_2(\omega)\, x^{16} - 16^2 = 0, \tag{6}$$

und für $r = 7, 1$:

$$f(\sqrt{-m})^3 = 2\,x,$$

für diese beiden Fälle

$$x^{24} - \left[3 - 2^{-8}\, j(\omega)\right] x^{16} + 3\,x^8 - 1 = 0, \tag{7}$$

wo für $\gamma_2(\omega)$ und $j(\omega)$ die Werthe (5) einzusetzen sind. Diese Gleichungen lassen sich noch zerlegen, und man erhält für $x$ selbst viel einfachere Gleichungen:

$$\begin{aligned} f(\sqrt{-51})^3 &= 2\,x, & x^3 - 4\,x^2 - x - 1 &= \sqrt{17}\,x^2,\\ f(\sqrt{-91}) &= x, & x^3 - 2\,x^2 - x - 2 &= \sqrt{13}\,x,\\ f(\sqrt{-99})^3 &= 2\,x, & x^3 - 13\,x^2 - 4\,x - 1 &= \sqrt{33}\,(2\,x^2 + x). \end{aligned} \tag{8}$$

Die Darstellung der Classeninvarianten zweiter Art $j(\omega)$ durch eine einzige Quadratwurzel ist immer dann möglich, wenn zwei Geschlechter und in jedem Geschlecht eine Classe zweiter Art und drei Classen erster Art vorhanden sind. Diese Werthe von $m$ finden sich in der Gauss'schen Tafel der Classenzahlen (Werke, Bd. II, S. 450 ff.) unter der Bezeichnung II, 3, von denen diejenigen auszuwählen sind, welche $\equiv 3 \pmod 8$ sind. Ihre Anzahl ist aller Wahrscheinlichkeit nach endlich, wie die erwähnte Tafel aufweist; es sind die Zahlen:

$$\begin{aligned} m = 35,\ &51,\ 75,\ 91,\ 99,\ 115,\ 123,\\ &147,\ 187,\ 235,\ 267,\ 403,\ 427. \end{aligned}$$

## Vierzehnter Abschnitt.

# Galois'sche Gruppe der Classengleichung.

---

### §. 108. Composition der quadratischen Formen.

Wir geben hier eine Uebersicht über die Theorie der Composition der quadratischen Formen, die für unsere folgenden Untersuchungen eine wichtige Rolle spielt, bezüglich deren näherer Begründung auf das Supplement $X$ von Dirichlet-Dedekind, Zahlentheorie verwiesen sei.

1. Sind

$$\psi = (A, B, C), \quad \psi' = (A', B', C') \tag{1}$$

zwei quadratische Formen von gleicher negativer Determinante $-m$, in welchen die drei Zahlen

$$A, A', B + B' \tag{2}$$

keinen gemeinsamen Theiler haben, so lässt sich eine nach dem Modul $AA'$ bestimmte Zahl $B''$ finden, welche den Bedingungen genügt:

$$B'' \equiv B \pmod{A}, \quad B'' \equiv B' \pmod{A'}, \quad B''^2 \equiv -m \pmod{AA'} \tag{3}$$

oder

$$B'' = B + \lambda A = B' + \lambda' A', \quad B''^2 = -m + C'' A A', \tag{4}$$

worin $\lambda$, $\lambda'$, $C''$ ganze Zahlen sind.

Demnach giebt es eine durch $\psi$, $\psi'$ bestimmte dritte Form derselben Determinante $-m$

$$\psi'' = (AA', B'', C''),$$

welche die aus (1) und (2) componirte Form genannt wird.

Wir setzen in symbolischer Bedeutung:

$$\psi'' = \psi\psi'. \tag{5}$$

Setzen wir voraus, dass die Formen $\psi$, $\psi'$ primitiv seien, so verlangen die Bedingungen (2), dass entweder beide von der ersten Art oder eine von der ersten, die andere von der zweiten Art, nicht aber beide von der zweiten Art seien.

2. Bedeuten $\omega$, $\omega'$, $\omega''$ die Wurzeln von $\psi = 0$, $\psi' = 0$, $\psi'' = 0$, also

$$\omega = \frac{-B + \sqrt{-m}}{A}, \; \omega' = \frac{-B' + \sqrt{-m}}{A'}, \; \omega'' = \frac{-B'' + \sqrt{-m}}{AA'},$$

so bestehen zwischen diesen die Relationen:

$$\omega'' = \frac{-\lambda + \omega}{A'} = \frac{-\lambda' + \omega'}{A}. \tag{6}$$

3. Ersetzt man $\psi$, $\psi'$ durch zwei äquivalente Formen, so geht auch $\psi''$ in eine äquivalente Form über. Damit ist die Composition der Formenclassen definirt.

Sind $k$, $k'$ die Classen, welche durch die Formen $\psi$, $\psi'$ repräsentirt sind, so heisst die durch $\psi''$ repräsentirte Classe $k''$ aus $k$, $k'$ zusammengesetzt oder componirt, und man schreibt symbolisch:

$$k'' = kk'. \tag{7}$$

Die wiederholte Composition einer Classe erster Art mit sich selbst wird durch die Potenzen $k^2$, $k^3$, ... bezeichnet. Wir betrachten zunächst die Composition der primitiven Classen erster Art. Aus je zweien dieser Classen lässt sich durch Composition eine bestimmte dritte herleiten und es gelten dabei die folgenden Gesetze.

Sind $k$, $k'$, $k''$ drei Classen, so ist:

$$(kk')k'' = k(k'k'') = kk'k''. \tag{8}$$

Ist

$$kk' = kk'',$$

so folgt:

$$k' = k''.$$

Endlich:

$$kk' = k'k.$$

Hiernach bilden die primitiven Classen erster Art der Determinante $-m$, da ihre Anzahl endlich ist, eine Abel'sche Gruppe (§. 54).

Das Einheitselement dieser Gruppe ist die Hauptclasse, d. h. diejenige Classe, welche durch die Hauptform

$$(1, 0, m)$$

repräsentirt ist, denn durch Composition mit dieser Hauptform ändert sich eine andere Form nicht.

Die Composition einer Classe mit ihrer entgegengesetzten führt zur Hauptclasse, wie man aus der Composition der beiden entgegengesetzten Formen $(A, B, C)$, $(C, B, A)$ erkennt; daher sind zwei entgegengesetzte Classen durch

$$k, \quad k^{-1}$$

zu bezeichnen; wenn also eine Classe ambig ist, so ist $k^2 = 1$, d. h. gleich der Hauptclasse, und umgekehrt, wenn $k^2 = 1$ ist, so ist $k$ ambig. Für jede Classe $k$ giebt es eine gewisse niedrigste positive Potenz $k^\varepsilon$, welche $= 1$ ist. Wir sagen, $k$ gehört zum Exponenten $\varepsilon$, und das System

$$1, k, k^2, \ldots k^{\varepsilon - 1}$$

heisst die Periode von $k$.

4. Es sei $(A, B, C)$ eine beliebige primitive Form erster Art der Determinante

$$-m = B^2 - AC \tag{9}$$

und $A$ relativ prim zu $2m$. Es ist dann, wie aus (9) hervorgeht, $-m$ quadratischer Rest von jeder in $A$ aufgehenden Primzahl $p$, also:

$$\left(\frac{-m}{p}\right) = +1. \tag{10}$$

Ist

$$A = pA',$$

so ist nach unserer Voraussetzung $B$ durch $p$ nicht theilbar (da sonst auch $m$ durch $p$ theilbar wäre), und die Form $(A, B, C)$ ist zusammengesetzt aus

$$(p, B, CA'), \quad (A', B, Cp).$$

Wiederholen wir diesen Schluss, so erkennen wir, dass jede quadratische Form $(A, B, C)$, welche ein Repräsentant einer beliebigen primitiven Classe erster Art sein kann, sich componiren lässt aus solchen Formen, deren erster Coëfficient eine Primzahl ist.

Setzen wir, indem wir $A$ in seine Primfactoren zerlegen:

$$A = pp'p'' \ldots,$$

so ist nach der Bezeichnungsweise (5):

$$(A, B, C) = \left(p, B, \frac{AC}{p}\right)\left(p', B, \frac{AC}{p'}\right)\left(p'', B, \frac{AC}{p''}\right) \cdots \tag{11}$$

5. Ist $p$ eine beliebige in $2m$ nicht aufgehende Primzahl und

$$\left(\frac{-m}{p}\right) = +1,$$

so hat für jeden beliebigen positiven Exponenten $\pi$ die Congruenz

$$(12) \qquad b^2 \equiv -m \pmod{p^\pi}$$

zwei nach dem Modul $p^\pi$ incongruente (durch $p$ nicht theilbare) Wurzeln, und es existiren daher, wenn $\nu \overline{\gtrless} \pi$ ist, zwei Formen der Determinante $-m$ (oder genauer gesagt, da $\pm b$ um ein Vielfaches von $p^\pi$ vermehrt werden kann, zwei Schaaren äquivalenter Formen)

$$(p^\nu, \pm b, cp^{\pi-\nu}),$$

deren erster Coëfficient $p^\nu$ ist. Diese Formen repräsentiren zwei entgegengesetzte Classen, oder, wenn sie ambig sind, nur eine. Diese Classen lassen sich leicht mit sich selbst componiren. Ist nämlich

$$(p, b, cp^{\pi-1}) = \psi_1$$

der Repräsentant einer dieser Classen, die wir mit $l$ bezeichnen wollen, so ist, so lange $\nu \overline{\gtrless} \pi$ ist

$$(p^\nu, b, cp^{\pi-\nu}) = \psi_\nu$$

der Repräsentant von $l^\nu$. Daraus geht hervor, dass, wenn $l$ zum Exponenten $\varepsilon$ gehört, $p^\varepsilon$ die niedrigste Potenz von $p$ ist, welche durch die Hauptform $(1, 0, m)$ darstellbar ist, die also einer Gleichung

$$p^\varepsilon = y^2 + mx^2$$

genügt. Diese Zahl $\varepsilon$ wird der Index der Primzahl $p$ genannt.

6. Es sei jetzt $k$ eine beliebige primitive Classe der Determinante $-m$ erster oder zweiter Art, während, wenn $\pi$ ein beliebiger fester, aber hinlänglich gross gewählter Exponent ist, $l$ und $b$ die vorige Bedeutung haben. Wir wählen den Repräsentanten von $k$

$$\chi = (A, B, C),$$

so dass $A$ durch $p$ untheilbar und

$$B \equiv b \pmod{p^\pi}$$

ist (§. 89). Dann ist $B^2 + m = AC$ sowohl durch $A$ als durch $p^\pi$ theilbar, und wenn wir

$$B^2 + m = AC'p^\pi, \quad C = C'p^\pi$$

setzen, so ergiebt sich nach 1. ein Repräsentant der zusammengesetzten Classe $kl^\nu$

$$\chi_\nu = \chi\psi_\nu = (Ap^\nu, B, C'p^{\pi-\nu}).$$

Bezeichnen wir die Wurzel der Form $\chi$ mit $\omega$, die der Form $\chi_\nu$ mit $\omega_\nu$, so ist

$$\omega_\nu = \frac{\omega}{p^\nu}$$

und $\omega_\varepsilon$ ist eine mit $\omega$ äquivalente Zahl. Hierin kann $\nu$ jede Zahl bedeuten, die nicht grösser als $\pi$ ist.

7. Die Charaktere einer zusammengesetzten Classe erhält man, indem man die Charaktere der einzelnen Componenten multiplicirt. Daher ergeben zwei Classen des Hauptgeschlechtes durch Composition immer wieder eine Classe des Hauptgeschlechtes und es folgt, dass die Classen des Hauptgeschlechtes eine in der Gruppe aller Classen enthaltene Abel'sche Gruppe bilden.

Durch Composition der Classen des Hauptgeschlechtes mit irgend einer anderen Classe erhält man die Classen des Geschlechtes, dem die letztere Classe angehört.

8. Durch Composition der sämmtlichen Formenclassen erster Art der Determinante $-m$ mit einer Classe zweiter Art erhält man sämmtliche Classen zweiter Art, und zwar jede einmal oder dreimal, je nachdem $m \equiv 7$ oder $\equiv 3 \pmod 8$ ist. Diese Zusammensetzung ist, wenn auch unausgesprochen, bereits benutzt in §. 89.

Ist nämlich

$$(2A,\ B,\ 2C)$$

irgend eine primitive Form zweiter Art mit ungeradem $A$ der Determinante

$$-m = B^2 - 4AC,$$

also $B$ ungerade, so wird diese Form abgeleitet durch Composition der beiden Formen

$$(A,\ B,\ 4C),\quad \left(2,\ 1,\ \frac{m+1}{2}\right),$$

von denen die erste von der ersten Art, die zweite von der zweiten Art ist.

Durchläuft $(2A, B, 2C)$ eine Reihe nicht äquivalenter Formen, so sind auch die entsprechenden Formen $(A, B, 4C)$ nicht äquivalent.

Ist also $m \equiv 7 \pmod 8$, so durchlaufen die beiden Formen

$$(2A,\ B,\ 2C) \quad \text{und} \quad (A,\ B,\ 4C)$$

gleichzeitig ein vollständiges Repräsentantensystem der Classen der zweiten und der ersten Art.

Ist aber $m \equiv 3 \pmod 8$, so durchläuft (von dem Falle $m = 3$ abgesehen) $(A, B, 4C)$ nur das Repräsentantensystem des dritten Theiles der Classen erster Art; um die sämmtlichen Classen erster Art zu erhalten, muss man $(A, B, 4C)$ noch componiren mit den Formenclassen

$$\left(4, \pm 1, \frac{m+1}{4}\right),$$

wodurch man erhält

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

und für die letzte Form kann auch die äquivalente Form

$$(A-B+C, C-A, A+B+C)$$

gesetzt werden.

Wenn also unter der Voraussetzung $m \equiv 3 \pmod 8$

$$(2A, B, 2C)$$

ein vollständiges Repräsentantensystem von Formenclassen zweiter Art durchläuft, so durchlaufen (von $m = 3$ abgesehen)

$$(A, B, 4C)$$
$$(4A, B, C)$$
$$(A-B+C, C-A, A+B+C)$$

zusammengenommen ein vollständiges Repräsentantensystem der Classen erster Art[1]).

Ist $m \equiv 7 \pmod 8$, so sind die Formen

$$\left(4, \pm 1, \frac{m+1}{4}\right)$$

von der zweiten Art. Die Resultate der Composition von $(A, B, 4C)$ mit diesen, nämlich

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

sind gleichfalls von der zweiten Art und durchlaufen gleichzeitig mit $(2A, B, 2C)$ je ein vollständiges Repräsentantensystem von Classen zweiter Art.

---

[1]) Vgl. Dirichlet-Dedekind, Zahlentheorie, §§. 150, 151.

## §. 109. Relationen zwischen den Classeninvarianten derselben Determinante. Auflösbarkeit der Classengleichung.

Es ist für das Folgende eine Bezeichnung wünschenswerth, welche die Abhängigkeit der Classeninvariante von der Formenclasse einfacher auszudrücken gestattet. Es sei, wenn $k$ eine beliebige primitive Classe erster oder zweiter Art der Determinante $-m$ bedeutet, mit $(k)$ die zugehörige Classeninvariante bezeichnet, so dass, wenn $k$ durch eine Form

$$\chi = (A, B, C)$$

repräsentirt wird

$$(k) = j\left(\frac{-B + \sqrt{-m}}{A}\right) \tag{1}$$

sei. Wenn eine oder mehrere der $(k)$ unter einem Functionszeichen auftreten, so werden wir die Klammern auch weglassen, also z. B. $f(k, k' \ldots)$ statt $f[(k), (k') \ldots]$ schreiben.

Ist $p$ eine beliebige in $2m$ nicht aufgehende Primzahl, von welcher $-m$ quadratischer Rest ist vom Index $\varepsilon$, so bestimmen wir, indem wir $\pi$ mindestens $= \varepsilon$ annehmen, nach §. 108, 5. die beiden Formen

$$\psi = (p, \pm b, cp^{\pi - 1}),$$

welche zu den beiden entgegengesetzten Classen $l^{\pm 1}$ gehören, durch die Congruenz

$$b^2 \equiv -m \pmod{p^\pi},$$

und um $\chi$ mit $\psi$ zu componiren, können wir, wenn $A$ durch $p$ untheilbar vorausgesetzt wird, $b$ noch an die weitere Congruenz binden

$$\pm b \equiv B \pmod{A}.$$

Setzen wir daher $\pm b = B + \lambda A$, so ist $\lambda$ aus der quadratischen Congruenz

$$(B + \lambda A)^2 \equiv -m \pmod{p} \tag{2}$$

zu bestimmen, und die componirte Form ist

$$\chi\psi = (Ap, B + \lambda A, C'),$$

so dass, wenn $\lambda, \lambda'$ die beiden Wurzeln der Congruenz (2), $\omega$ die Wurzel der Form $\chi$ ist

$$\frac{-\lambda + \omega}{p}, \quad \frac{-\lambda' + \omega}{p}$$

die Wurzeln der beiden Formen $\chi \psi_{\pm 1}$ sind. Danach erhalten wir die beiden Classeninvarianten:

$$(3) \qquad (k\,l) = j\left(\frac{-\lambda + \omega}{p}\right), \quad (k\,l^{-1}) = j\left(\frac{-\lambda' + \omega}{p}\right).$$

Dies sind, für $v$ gesetzt, Wurzeln der Invariantengleichung

$$(4) \qquad F_p(u, v) = 0,$$

wenn

$$u = (k) = j(\omega)$$

gesetzt wird. Nun sind aber $(k\,l)$, $(k\,l^{-1})$ zugleich Wurzeln der zur Determinante $-m$ gehörigen Classengleichung

$$(5) \qquad H_m(v) = 0,$$

(erster oder zweiter Art, je nachdem $\chi$ von der ersten oder zweiten Art ist).

Es ist noch zu entscheiden, ob die Gleichungen (4) und (5) noch andere gemeinschaftliche Wurzeln haben können. Die Wurzeln der Gleichung (4) sind

$$v = j(\omega') = j(p\,\omega), \quad j\left(\frac{-t + \omega}{p}\right), \quad t = 0, 1, 2 \ldots p - 1,$$

und diese werden zugleich der Classengleichung (5) dann und nur dann genügen, wenn $\omega'$ einer primitiven ganzzahligen quadratischen Gleichung

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

von der Determinante $-m$, derselben Art wie $\chi$, genügt. Da $\omega$ der Gleichung

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

genügt, so ergiebt sich für $\omega' = p\,\omega$ die Gleichung

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

welche, da $A$ durch $p$ nicht theilbar ist, primitiv und von der Determinante $-m\,p^2$ ist, und für

$$\omega' = \frac{-t + \omega}{p}$$

die Gleichung

$$p\,A\,\omega'^2 + 2\,(A\,t + B)\,\omega' + \frac{A\,t^2 + 2\,B\,t + C}{p} = 0,$$

welche nur dann zur Determinante $-m$ gehört, wenn die Congruenz

$$At^2 + 2Bt + C \equiv 0 \pmod{p},$$

oder was dasselbe ist

$$(B + At)^2 \equiv -m \pmod{p}$$

befriedigt wird.

Dies ist aber dieselbe Congruenz wie (2) und daraus folgt, dass die beiden Classeninvarianten (4) die einzigen gemeinsamen Wurzeln der Gleichungen (4) und (5) sind. Diese beiden Wurzeln werden überdies einander gleich, wenn die Classe $l$ ambig ist.

Daraus folgt:

1. Der grösste gemeinschaftliche Theiler von (4), (5) ist, wenn die Classe $l$ nicht ambig ist, in Bezug auf $v$ quadratisch und hängt rational von $u$ ab.

Ist $u = (k)$, so sind die beiden Wurzeln der so erhaltenen quadratischen Gleichung

$$v = (lk), \quad (l^{-1}k).$$

Ist die Classe $l$ ambig, also $l$ und $l^{-1}$ identisch, so ist der grösste gemeinschaftliche Theiler von (4) und (5) linear, und $(lk)$ kann rational durch $(k)$ ausgedrückt werden.

Wir können dem hiermit bewiesenen Satze auch den Ausdruck geben: es ist

$$(6) \qquad (lk) + (l^{-1}k) = f_l(k),$$

wenn $f_l(k)$ eine rationale Function von $(k)$ bedeutet, deren Coëfficienten nur von der Classe $l$, nicht von der Classe $k$ abhängige rationale Zahlen sind.

2. Wir betrachten nun die Reihe der Classeninvarianten

$$(7) \qquad \ldots (l^{-1}k), (k), (lk), (l^2k), (l^3k), \ldots$$

die beliebig nach vorwärts und nach rückwärts fortgesetzt werden kann. In dieser Reihe ist, wenn $l$ zum Exponenten $\varepsilon$ gehört, $(l^\nu k)$ mit $(l^{\nu+\varepsilon}k)$ identisch, während alle zwischenliegenden Glieder davon und unter einander verschieden sind. Ist $l$ ambig, so enthält die Reihe (7) nur zwei verschiedene Glieder, von denen jedes durch das andere rational ausdrückbar ist. Anderenfalls schliessen wir nach (6), dass jedes Glied der Reihe (7) rational ausdrückbar ist durch die beiden vorhergehenden (oder auch durch die beiden folgenden) in der Form

$$(8) \qquad (l^{\nu+1}k) = -(l^{\nu-1}k) + f_l(l^\nu k).$$

Durch eine wiederholte Anwendung dieser Formel gelangt man zu dem Satze, dass jedes Glied der Reihe (7) rational ausgedrückt werden kann durch irgend zwei auf einander folgende Glieder derselben Reihe.

3. Ist, wie wir jetzt voraussetzen wollen, die Classe $l$ nicht ambig, so sind die beiden Classeninvarianten $(lk)$, $(l^{-1}k)$ von einander verschieden und daher

$$v = (lk) = j\left(\frac{-\lambda + \omega}{p}\right)$$

eine einfache Wurzel der Transformationsgleichung $F_p(u, v) = 0$. Setzen wir also

$$M = \left(\frac{\eta\left(\frac{-\lambda + \omega}{p}\right)}{\eta(\omega)}\right)^2, \tag{9}$$

so folgt nach §. 75 und §. 59, 6., dass $M^\tau$ bei geeigneter Bestimmung des Exponenten $\tau$ rational durch

$$j(\omega) \quad \text{und} \quad j\left(\frac{-\lambda + \omega}{p}\right),$$

also rational durch $(k)$ und $(lk)$ ausdrückbar ist, und aus §. 75, 4. ergiebt sich, dass $M$ eine ganze algebraische Zahl ist. Setzen wir voraus, was erlaubt ist, dass $\lambda$ bezüglich der Divisoren 2 und 3 den Bedingungen des §. 75 genügt, so sind die kleinsten Werthe von $\tau$

$$\begin{array}{ll} p \equiv 1 \pmod 4 & \tau = 1 \\ p \equiv 3 \pmod 4 & \tau = 2 \\ p = 3 & \tau = 6. \end{array}$$

Diesen Satz wenden wir an auf je zwei auf einander folgende Glieder der Reihe (7) und erhalten, wenn wir mit $\omega_1, \omega_2, \ldots \omega_\varepsilon$ die Wurzeln der Formen

$$\psi\chi, \psi^2\chi, \ldots \psi^\varepsilon\chi$$

bezeichnen, und wenn $\varphi$ eine durch die Classe $l$ vollständig bestimmte rationale Function bedeutet:

$$\begin{aligned} M^\tau &= \left(\frac{\eta(\omega_1)}{\eta(\omega)}\right)^{2\tau} = \varphi(k, lk), \\ M_1^\tau &= \left(\frac{\eta(\omega_2)}{\eta(\omega_1)}\right)^{2\tau} = \varphi(lk, l^2k), \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ M_{\varepsilon-1}^\tau &= \left(\frac{\eta(\omega_\varepsilon)}{\eta(\omega_{\varepsilon-1})}\right)^{2\tau} = \varphi(l^{\varepsilon-1}k, k). \end{aligned} \tag{10}$$

Durch Multiplication aller dieser Gleichungen folgt:

$$(11)\qquad \left(\frac{\eta(\omega_\varepsilon)}{\eta(\omega)}\right)^{2\tau} = \varphi(k, lk)\,\varphi(lk, l^2 k)\ldots\varphi(l^{\varepsilon-1}k, k).$$

Nach 2. kann aber die rechte Seite dieser Gleichung als rationale Function $\Phi(k, lk)$ von $(k)$ und $(lk)$ (mit rationalen Zahlcoëfficienten) dargestellt werden.

Andererseits ist, da $l$ zum Exponenten $\varepsilon$ gehört, $l^\varepsilon$ mit der Hauptform, also $l^\varepsilon k$ mit $k$ und $\omega_\varepsilon$ mit $\omega$ äquivalent, also besteht eine Gleichung

$$(12)\qquad \omega_\varepsilon = \frac{\gamma + \delta\omega}{\alpha + \beta\omega},\quad \alpha\delta - \beta\gamma = 1,$$

und es ist $\eta(\omega_\varepsilon):\eta(\omega)$ nach §. 33 zu bestimmen. Setzen wir, um dies auszuführen, wie in §. 108, 6.,

$$B \equiv b \pmod{p^\pi}$$

voraus, so wird

$$\omega = p^\varepsilon\,\omega_\varepsilon,$$

und (12) ergiebt durch Vergleichung mit

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

wenn $\sigma = 1$ oder $= 2$ ist, je nachdem die letztere Gleichung von der ersten oder zweiten Art ist:

$$(13)\qquad \begin{gathered} \sigma\beta = Ax,\quad -\sigma\gamma p^\varepsilon = Cx, \\ \sigma(\alpha - p^\varepsilon\delta) = 2Bx,\quad \sigma(\alpha + p^\varepsilon\delta) = 2y, \end{gathered}$$

woraus

$$(14)\qquad \sigma^2 p^\varepsilon = y^2 + mx^2,$$

$$(15)\qquad \sigma(\alpha + \beta\omega) = y + x\sqrt{-m}.$$

Aus (13) folgt

$$(16)\qquad y \equiv bx \pmod{p^\varepsilon},$$

wodurch das Vorzeichen von $y$ aus dem von $x$ bestimmt ist, und woraus sich zugleich ergiebt, dass, wenn $b$ durch $-b$, also $l$ durch $l^{-1}$ ersetzt wird, $x$ oder $y$ das Zeichen ändert.

Aus (10) ergiebt sich also nach §. 33, wenn $\varrho$ eine 12te Einheitswurzel bedeutet

$$(17)\qquad M M_1 M_2 \ldots M_{\varepsilon-1} = \varrho\,\frac{y + x\sqrt{-m}}{\sigma}.$$

Um aber unnöthige Unterscheidungen zu vermeiden, setzen wir in den Formeln (10) und (11) $\tau = 6$ und erhalten

$$\left(\frac{\eta\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right)}{\eta(\omega)}\right)^{12} = (-1)^x\left(\frac{y + x\sqrt{-m}}{\sigma}\right)^6,$$

also nach (11) eine Gleichung von der Form:

$$(18) \qquad (y + x\sqrt{-m})^6 = \Phi(k, lk).$$

Wenn wir $b$ durch $-b$, also $l$ durch $l^{-1}$ ersetzen, so muss $\sqrt{-m}$ in $-\sqrt{-m}$ übergehen und man erhält

$$(19) \qquad (y - x\sqrt{-m})^6 = \Phi(k, l^{-1}k).$$

Die Gleichung (18) ist also nicht erfüllt, wenn $(lk)$ durch $(l^{-1}k)$ ersetzt wird, es sei denn, dass $(y + x\sqrt{-m})^6$ rational wäre, dass also

$$3y^4 - 10x^2y^2m + 3m^2x^4 = (3y^2 - mx^2)(y^2 - 3mx^2) = 0$$

wäre, was aber, da der Fall $m = 3$ hier nicht in Betracht kommt (weil in diesem Falle gar keine nicht ambige Classe existirt), unmöglich ist.

Die quadratische Gleichung, deren beide Wurzeln $(lk)$, $(l^{-1}k)$ sind, hat also mit (18) nur eine Wurzel gemein, und daraus ergiebt sich der wichtige Satz:

> Nach Adjunction von $\sqrt{-m}$ ist $(lk)$ rational ausdrückbar durch $(k)$ in der Form
>
> $$(20) \qquad (lk) = f_l(k, \sqrt{-m}),$$
>
> wo $f_l$ eine rationale Function ist, deren Form durch die Classe $l$ allein bestimmt ist.

Die Aenderung des Zeichens von $\sqrt{-m}$ hat den Erfolg, dass $(lk)$ in $(l^{-1}k)$ übergeht, also

$$f_l(k, \sqrt{-m}) = f_{l^{-1}}(k, -\sqrt{-m}).$$

Ist $l$ ambig, so gilt nach 1. dieselbe Formel, nur dass $\sqrt{-m}$ in $f_l$ dann nicht vorkommt.

Ist $l'$ eine zweite Classe von derselben Beschaffenheit wie $l$, so kann man die Formel (20) auf $l'k$ anwenden und erhält:

$$(ll'k) = f_l(l'k, \sqrt{-m}),$$

welches mit Anwendung von

$$(l'k) = f_{l'}(k, \sqrt{-m})$$

in eine Gleichung der Form

$$(ll'k) = f_{ll'}(k, \sqrt{-m})$$

übergeht. Da man auf der linken Seite $l$ mit $l'$ vertauschen kann, so folgt

$$f_{ll'}(k, \sqrt{-m}) = f_{l'l}(k, \sqrt{-m}),$$

so dass $f_{ll'}$ nur von der zusammengesetzten Classe $ll'$ abhängt. Ebenso lässt sich ableiten

$$(ll'l''k) = f_{l\,l'\,l''}(k, \sqrt{-m})$$

u. s. f., so dass, da nach §. 108, 4. jede beliebige Classe $s$ der Determinante $-m$ und der ersten Art aus solchen Classen $l$ zusammensetzbar ist, die Formel (20) nebst den daraus gezogenen Folgerungen nicht mehr an die über $l$ gemachte besondere Voraussetzung gebunden ist.

Wir haben also, wenn $s$, $k$ zwei beliebige Classen der Determinante $-m$ bedeuten, deren erste von der ersten Art ist, die Formeln:

$$(sk) = f_s(k, \sqrt{-m}), \tag{21}$$

$$(s^{-1}k) = f_s(k, -\sqrt{-m}). \tag{22}$$

Setzen wir in der Formel (22) $sk$ an Stelle von $k$, so folgt

$$(k) = f_s(sk, -\sqrt{-m}) \tag{23}$$

oder, indem man $sk = k'$ setzt und $f$ für $f_s$ schreibt, nach (21)

$$\begin{aligned}(k') &= f(k, \sqrt{-m}),\\ (k) &= f(k', -\sqrt{-m}),\end{aligned} \tag{24}$$

worin nun $k$, $k'$ irgend zwei Classen der Determinante $-m$ derselben Art sein können.

Hiernach sind wir im Stande, die Galois'sche Gruppe der Classengleichung, oder zunächst wenigstens eine Gruppe von Permutationen zu bestimmen, welche die Gruppe der Classengleichung als Theiler enthält.

Nehmen wir zuvörderst an, es sei dem Rationalitätsbereich der rationalen Zahlen die $\sqrt{-m}$ adjungirt, und wenn $(k), (k'), (k'') \ldots$ die sämmtlichen Classeninvarianten erster oder zweiter Art der Determinante $-m$ bedeuten,

$$R(k, k', k'' \ldots)$$

irgend eine rationale Function dieser Grössen. Nach unserem Satze lässt sich diese Function rational ausdrücken durch eine der Grössen $(k)$, also etwa:

$$R(k, k', k'', \ldots) = R'(k).$$

Bedeutet ferner $(s)$ eine beliebige der Classeninvarianten erster Art und hat die Function $R$ die Eigenschaft, durch die sämmtlichen $h$ Permutationen

$$\begin{pmatrix} k, & k', & k'' \ldots \\ sk, & sk', & sk'' \ldots \end{pmatrix},$$

deren Gesammtheit wir mit $\mathfrak{S}$ bezeichnen wollen, ungeändert zu bleiben, so ist $R'(k) = R'(sk)$, und daher rational ausdrückbar.

Die Galois'sche Gruppe der Classengleichung nach Adjunction von $\sqrt{-m}$ ist also in dem System $\mathfrak{S}$ enthalten, und da $\mathfrak{S}$ eine Abel'sche Gruppe ist, so ist die Classengleichung eine Abel'sche und daher durch Wurzelzeichen auflösbar.

Es ist hierbei zu beachten, dass, wenn $k, k', k'' \ldots$ die Classen zweiter Art sind, für $s$ gleichwohl die Classen erster Art zu setzen sind. Ist dann $m \equiv 3 \pmod 8$, so giebt es drei unter den $s$, welche die Reihe der $k, k', k'' \ldots$ ungeändert lassen, und der Grad der Gruppe $\mathfrak{S}$ reducirt sich auf den dritten Theil der Anzahl der primitiven Classen erster Art.

Nehmen wir an, die Function $R$ habe reelle (rationale) Coëfficienten, so wird gleichwohl ihr rationaler Ausdruck die Form $a + b\sqrt{-m}$ haben, worin $a, b$ rationale Zahlen sind. Der imaginäre Theil wird dann und nur dann wegfallen, wenn $R$ auch durch die Vertauschung sämmtlicher Classen $k, k', k'' \ldots$ mit ihren entgegengesetzten ungeändert bleibt. Daraus folgt, dass ohne Adjunction von $\sqrt{-m}$ die Galois'sche Gruppe der Classengleichung enthalten ist in dem System von $2h$ Permutationen, welches man erhält, wenn man in $\mathfrak{S}$ jede Classe in ihre entgegengesetzte verwandelt. Nur in dem besonderen Falle, in dem alle Classen ambig sind, (der nur für eine endliche Anzahl von Determinanten stattfindet, siehe den nächsten Abschnitt) ist dies letztere System mit $\mathfrak{S}$ identisch, und die Classengleichung ist ohne Adjunction von $\sqrt{-m}$ eine Abel'sche.

Der algebraische Körper, der aus den rationalen Functionen einer Classeninvariante gebildet ist, ist daher, von dem zuletzt erwähnten Ausnahmefall abgesehen, kein Normalkörper, sondern ist von seinen conjugirten Körpern verschieden. Dagegen erhält man einen Normalkörper, wenn man die Quadratwurzel $\sqrt{-m}$ dem Körper der Classeninvariante adjungirt.

## §. 110. Irreducibilität.

Indem wir uns zur Untersuchung der Irreducibilität der Classengleichung wenden, wird es nöthig, die allgemeine Theorie der algebraischen Zahlen in etwas weiterem Umfange vorauszusetzen, insbesondere die Zerlegung der Zahlen eines algebraischen Körpers in die dem Körper angehörigen Primfactoren.

Wir folgen hier der Theorie und Bezeichnungsweise von Dedekind und verweisen auf das XI. Supplement in der 3. Auflage von Dirichlet-Dedekind, Vorlesungen über Zahlentheorie [1]). Wenn wir im Folgenden zur Erleichterung für den Leser auf einzelne Paragraphen dieses Werkes verweisen, so soll dies durch den Buchstaben $D$ angedeutet sein.

Wir betrachten jetzt den algebraischen Zahlkörper, welcher die gemeinschaftliche Norm aller zu einer bestimmten Determinante $-m$ gehörigen Körper der Classeninvarianten erster oder zweiter Art [2]) ist, und der, wie wir im vorigen Paragraphen gesehen haben, aus den rationalen Functionen einer Classeninvariante und $\sqrt{-m}$ besteht. Er kann daher, wenn $(k), (k'), (k'')\ldots$ die sämmtlichen Classeninvarianten sind, nach §. 58, durch $\mathfrak{K}(k, k', k''\ldots)$ oder durch $\mathfrak{K}(k, \sqrt{-m})$ bezeichnet werden. Wir wollen ihn den Classenkörper der Determinante $-m$ nennen und kurz mit $\mathfrak{K}$ bezeichnen, während der quadratische Körper $\mathfrak{K}(\sqrt{-m})$ mit $\Omega$ bezeichnet sei.

Ist $m = m_1^2 m_0$, und $m_1^2$ die grösste in $m$ aufgehende Quadratzahl, so sind die ganzen Zahlen des Körpers $\Omega$ in einer der beiden Formen

$$x + y\sqrt{-m_0}, \quad \frac{x + y\sqrt{-m_0}}{2}$$

enthalten, wenn $x$, $y$ ganze rationale Zahlen sind. Ist also $\alpha$ eine ganze Zahl in $\Omega$, so kann man eine ganze rationale Zahl $c$, deren Primfactoren alle in $2m$ enthalten sind, und die ganzen rationalen Zahlen $x$, $y$ so bestimmen, dass

$$c\alpha = x + y\sqrt{-m} \tag{1}$$

wird.

---

[1]) Die Theorie von Kronecker, die, so verschieden sie in der Form ist, sachlich mit der von Dedekind übereinstimmt, findet sich ausführlich dargestellt in der Schrift: „Grundzüge einer arithmetischen Theorie der algebraischen Grössen". Festschrift zu Kummer's fünfzigjährigem Doctorjubiläum, Berlin 1882. Beide Theorien knüpfen an Kummer's classische Arbeiten über die Kreistheilungszahlen an.

[2]) Der Körper der Classeninvarianten erster Art enthält den der zweiten Art immer als Theiler. Das Umgekehrte findet nur statt, wenn $m \equiv -1 \pmod 8$ ist (§. 89).

Es kommt zunächst darauf an, die Zerlegung der rationalen Primzahlen in ihre Primideale zu finden (D. §§. 168, 171, 173).

Wir haben hierbei dreierlei Primzahlen zu unterscheiden:

1. Solche, welche in $2m$ und in der Discriminante der Classengleichung $H_m(u) = 0$ aufgehen. Diese Primzahlen sind in endlicher Anzahl vorhanden und müssen bis jetzt ganz von der Untersuchung ausgeschlossen werden. Ihre Theorie zu finden, ist eine wichtige Aufgabe, die zur Zeit noch nicht allgemein gelöst werden kann.

2. Primzahlen, von welchen $-m$ quadratischer Nichtrest ist, die wir mit $q$ bezeichnen, für die also:

$$\left(\frac{-m}{q}\right) = -1.$$

3. Primzahlen, von welchen $-m$ quadratischer Rest ist, die mit $p$ bezeichnet werden sollen, für die also:

$$\left(\frac{-m}{p}\right) = +1.$$

Die Primzahlen der zweiten und dritten Art bezeichnen wir auch ohne Unterschied durch $r$ und schicken nun die folgenden Bemerkungen voraus.

1. Es sei $(k)$ irgend eine der $h$ Classeninvarianten und

$$(2) \qquad \Phi(k) = (k)^\nu + \alpha_1 (k)^{\nu-1} + \alpha_2 (k)^{\nu-2} \dots + \alpha_\nu = 0$$

die Gleichung niedrigsten Grades, welcher $(k)$ genügt, deren Coëfficienten in $\Omega$ enthalten sind, und ganze Zahlen dieses Körpers sein müssen. Es ist dann, wenn $t$ eine Variable bedeutet, $\Phi(t)$ ein Divisor von $H_m(t)$ 1), und folglich ist auch die Discriminante von $\Phi(t)$ ein Theiler der Discriminante von $H_m(t)$. Eine beliebige ganze Zahl $\zeta$ des Körpers $\mathfrak{K}$ kann nach §. 59, 5. in der Form dargestellt werden

$$\zeta = \frac{\varphi(k)}{\Phi'(k)},$$

wo $\varphi(k)$ eine ganze rationale Function von $(k)$ ist, deren Coëfficienten ganze Zahlen des Körpers $\Omega$ sind. Daraus folgt, dass $\zeta$ durch eine Gleichung der Form dargestellt werden kann

$$(3) \quad b\,\zeta = \beta_0 + \beta_1 (k) + \beta_2 (k)^2 + \cdots \beta_{\nu-1} (k)^{\nu-1} = f(k, \sqrt{-m}),$$

worin $b$ eine ganze Zahl bedeutet, in welcher nur solche Primzahlen aufgehen, die in der Discriminante von $\Phi$ enthalten sind.

---

1) $H_m = 0$ kann hier die Classengleichung erster oder zweiter Art sein.

$b$ ist also gewiss durch keine der Primzahlen $r$ theilbar. Die $\beta_0, \beta_1 \ldots \beta_{\nu-1}$ sind ganze Zahlen des Körpers $\Omega$.

Ersetzen wir $(k)$ in (3) durch eine andere Wurzel der Gleichung (2), so geht $\zeta$ in einen conjugirten Werth über, der ebenfalls eine ganze Zahl ist.

Die durch (3) dargestellte Function $\zeta$ kann nur dann durch eine Primzahl $r$ theilbar sein, wenn die sämmtlichen $\beta_0, \beta_1 \ldots \beta_{\nu-1}$ durch $r$ theilbar sind. Denn sonst wäre $\zeta : r$ ebenfalls in der Form (3) darstellbar und es würde sich eine Gleichung von niedrigerem als dem $\nu$ten Grade für $(k)$ ergeben.

2. Nach dem Fermat'schen Satze ist für jede beliebige Primzahl $r$, wenn $a$ eine ganze rationale Zahl bedeutet:

$$a^r \equiv a \pmod{r}. \tag{4}$$

Ferner ist, wie aus der Zahlentheorie bekannt:

$$(-m)^{\frac{r-1}{2}} \equiv \left(\frac{-m}{r}\right) \pmod{r},$$

oder

$$\sqrt{-m}^{\,r} \equiv \left(\frac{-m}{r}\right) \sqrt{-m} \pmod{r}. \tag{5}$$

Bezeichnet daher $\alpha$ wie oben eine ganze Zahl des Körpers $\Omega$ und $\alpha'$ die conjugirt imaginäre Zahl, so ist nach (1)

$$c\alpha = x + y\sqrt{-m}, \quad c\alpha' = x - y\sqrt{-m},$$

worin $c$ durch keine der Primzahlen $r$ theilbar ist, und mit Anwendung des binomischen und des Fermat'schen Satzes erhält man:

$$\alpha^p \equiv \alpha \pmod{p}, \quad \alpha^q \equiv \alpha' \pmod{q}. \tag{6}$$

Daraus folgt nun, wenn $f(k, \sqrt{-m})$ irgend eine Function von der Form (3) ist, mit Anwendung des polynomischen Lehrsatzes

$$\begin{aligned} f(k, \sqrt{-m})^p &\equiv f(k^p, \sqrt{-m}) \pmod{p}, \\ f(k, \sqrt{-m})^q &\equiv f(k^q, -\sqrt{-m}) \pmod{q}, \end{aligned} \tag{7}$$

worin $k^p$, $k^q$ für $(k)^p$, $(k)^q$ stehen, also die Bedeutung von wirklichen Potenzen haben.

3. Wenn $\mathfrak{r}$ ein in $r$ aufgehendes Primideal in $\mathfrak{K}$ ist, so ist die Norm von $\mathfrak{r}$ eine Potenz von $r$:

$$N(\mathfrak{r}) = r^{\varrho}. \tag{8}$$

Der Exponent $\varrho$ wird der Grad des Primideals $\mathfrak{r}$ genannt. Für jede beliebige ganze Zahl $\zeta$ des Körpers $\mathfrak{K}$ ist

$$(9) \qquad \zeta^{N(\mathfrak{r})} \equiv \zeta \pmod{\mathfrak{r}},$$

und wenn umgekehrt $r^\varrho$ die niedrigste Potenz von $r$ ist, bei welcher die Congruenz

$$(10) \qquad \zeta^{r^\varrho} \equiv \zeta \pmod{\mathfrak{r}}$$

durch jede Zahl $\zeta$ befriedigt wird, so ist $\varrho$ der Grad des Ideals $r$; denn $N(\mathfrak{r})$ ist die Anzahl der überhaupt existirenden, nach dem Modul $\mathfrak{r}$ incongruenten Zahlen $\zeta$, und wenn daher $r^\varrho < N(\mathfrak{r})$ wäre, so hätte die Congruenz (10) mehr Wurzeln als ihr Grad beträgt, was bei einem Modul, der ein Primideal ist, unmöglich ist (D. §§. 171, 174).

Es ist unsere Aufgabe, die Grade der Primideale zu ermitteln, welche in einer beliebigen Primzahl $r$ enthalten sind.

4. Wir beweisen zunächst, dass keine der Primzahlen $r$ durch das Quadrat eines Primideals theilbar ist. Nehmen wir an, es sei $r$ durch $\mathfrak{r}^2$ theilbar, also, wenn $\mathfrak{o}$ das System aller ganzen Zahlen in $\mathfrak{K}$ bedeutet (D. §. 167)

$$\mathfrak{o}\, r = \mathfrak{r}^2 \mathfrak{a},$$

worin $\mathfrak{a}$ irgend ein Ideal, $\mathfrak{r}$ ein Primideal ist, so kann man eine ganze Function $\zeta$ in $\mathfrak{K}$ (eine Zahl in $\mathfrak{o}$) wählen, welche durch $\mathfrak{r}\mathfrak{a}$, aber nicht durch $r$ theilbar ist. Das Quadrat dieser Function $\zeta$, und also auch ihre $r$te Potenz, ist aber durch $r$ theilbar. Setzen wir nach (3)

$$b\zeta = f(k, \sqrt{-m}),$$

so sind die Coëfficienten $\beta$ von $f$ nicht alle durch $r$ theilbar. Durch Erheben in die $r$te Potenz ergiebt sich aber mittelst (5):

$$(11) \qquad f(k^r, \pm\sqrt{-m}) \equiv 0 \pmod{r},$$

wo das obere oder untere Zeichen gilt, je nachdem $r$ zu den $p$ oder den $q$ gehört. Die Congruenz (11) bleibt aber bestehen, wenn $(k)$ durch irgend eine der Wurzeln $(k_1), (k_2), \ldots (k_\nu)$ der Gleichung (2) ersetzt wird, und daraus folgt leicht, indem man die so entstandenen $\nu$ Gleichungen (11) wie ein System linearer Gleichungen für die $\beta$ behandelt, dass das Quadrat der Determinante

$$K_r = \begin{vmatrix} 1, (k_1)^r \ldots (k_1)^{r(\nu-1)} \\ 1, (k_2)^r \ldots (k_2)^{r(\nu-1)} \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ 1, (k_\nu)^r \ldots (k_\nu)^{r(\nu-1)} \end{vmatrix},$$

welches eine ganze Zahl in $\Omega$ ist, durch $r$ theilbar sein muss.

Die Determinante $K_r$ ist nach 2. mit der $r$ten Potenz der Determinante

$$K = \begin{vmatrix} 1, (k_1), \dots (k_1)^{r-1} \\ 1, (k_2), \dots (k_2)^{r-1} \\ \dots\dots\dots \\ 1, (k_r), \dots (k_r)^{r-1} \end{vmatrix}$$

nach dem Modul $r$ congruent, und daher ist $K^2$ gleichfalls durch $r$ theilbar. $K^2$ ist aber, vom Vorzeichen abgesehen, mit der Discriminante von $\Phi$ identisch, und daher müsste diese Discriminante und folglich auch die Discriminante von $H_m$ durch $r$ theilbar sein, gegen die Voraussetzung. Also ist $\mathfrak{o}\, r$ ein Product aus lauter verschiedenen Primidealen, oder selbst ein Primideal.

5. Bedeuten $(k), (k'), \dots (k^{(h-1)})$ die sämmtlichen Wurzeln der Gleichung

$$H_m(u) \doteq 0,$$

so ist für ein variables $t$

$$H_m(t) = [t-(k)]\,[t-(k')] \dots [t-(k^{(h-1)})],$$

und diese Function hat ganze rationale Coëfficienten. Es ist also nach 2.:

$$[H_m(t)]^r \equiv H_m(t^r) \pmod{r},$$

also, wenn wir $t = (k)$ setzen:

$$[(k)^r-(k)]\,[(k)^r-(k')] \dots [(k)^r-(k^{(h-1)})] \equiv 0 \pmod{r}.$$

Bedeutet also $\mathfrak{r}$ ein in $r$ aufgehendes Primideal, so muss wenigstens einer der Factoren der linken Seite durch $\mathfrak{r}$ theilbar sein, und daraus folgt eine Congruenz

$$(k)^r \equiv (k') \pmod{\mathfrak{r}}, \tag{12}$$

worin $(k')$ irgend eine der Classeninvarianten ist, die auch mit $(k)$ identisch sein kann.

6. Wir betrachten jetzt zunächst irgend eine Primzahl $q$ und bezeichnen mit $\mathfrak{q}$ ein in $q$ aufgehendes Primideal. $\mathfrak{q}$ kann nicht vom ersten Grade sein, denn sonst müsste, wenn $q$ eine beliebige ganze Zahl in $\mathfrak{K}$ ist, $\xi^q \equiv \xi \pmod{\mathfrak{q}}$ sein, während doch schon $\sqrt{-m}^q$ nicht congruent mit $\sqrt{-m}$, sondern mit $-\sqrt{-m}$ ist.

Es sei nun nach (12):

$$(k)^q \equiv (k') \pmod{\mathfrak{q}}. \tag{13}$$

Ist $(k')$ von $(k)$ verschieden, so können wir nach §. 109, (24) setzen

$$(k') = f(k, \sqrt{-m}), \quad (k) = f(k', -\sqrt{-m}),$$

also nach (7) und (13)

$$(k')^q \equiv f(k^q, -\sqrt{-m}) \equiv f(k', -\sqrt{-m}) \equiv (k) \pmod{\mathfrak{q}}$$

oder

$$(14) \qquad (k)^{qq} \equiv (k) \pmod{\mathfrak{q}}.$$

Diese Congruenz ist also erfüllt, mag $(k')$ von $(k)$ verschieden sein oder nicht.

Daraus ergiebt sich aber aus der Darstellung (3) mittelst der Formel (7), dass für jede Zahl $\zeta$ in $\mathfrak{o}$ die Congruenz

$$(15) \qquad \zeta^{qq} \equiv \zeta \pmod{\mathfrak{q}}$$

erfüllt ist, also nach 3. der Satz:

Jede Primzahl $q$ ist im Körper $\mathfrak{K}$ in lauter von einander verschiedene Primideale zweiten Grades zerlegbar.

7. Anders verhalten sich die Primzahlen $p$ der dritten Art. Für eine solche giebt es, wie wir in §. 108 gesehen haben, eine oder zwei entgegengesetzte Classen $l$, die durch Formen mit dem ersten Coëfficienten $p$ repräsentirt werden können, und wenn $(k)$ eine beliebige Classeninvariante ist, so ist nach §. 109 die Invariantengleichung für den Transformationsgrad $p$

$$(16) \qquad F_p(u, v) = 0$$

befriedigt für

$$u = (k), \quad v = (lk) \quad \text{und} \quad v = (l^{-1}k).$$

Nach dem, was am Schlusse des §. 72 bewiesen ist [Formel (31)], folgt aber hieraus die Congruenz

$$(17) \qquad [(k)^p - (lk)]\,[(lk)^p - (k)] \equiv 0 \pmod{p}.$$

Wenn nun $\mathfrak{p}$ ein in $p$ aufgehendes Primideal ist, so muss einer der beiden Factoren auf der linken Seite von (17) durch $\mathfrak{p}$ theilbar sein. Welche der beiden hiernach möglichen Annahmen wir weiter verfolgen, ist gleichgültig, da die eine in die andere übergeht, wenn $k$ mit $l^{-1}k$ und $l$ mit $l^{-1}$ vertauscht wird. Sei also

$$(18) \qquad (k)^p \equiv (lk) \pmod{\mathfrak{p}}.$$

Wenn die Congruenz (18) für irgend einen der conjugirten Werthe $(k)$ befriedigt ist, so gilt sie auch für jeden anderen. Denn es ist nach §. 109 (24):

$$(k') = f(k, \sqrt{-m}), \quad (lk') = f(lk, \sqrt{-m}),$$

also

$$(k')^p \equiv f(k^p, \sqrt{-m}) \equiv f(lk, \sqrt{-m}) \equiv (lk') \pmod{\mathfrak{p}}.$$

Es folgt also aus (18), wenn man $k$ durch $l^{-1}k$ ersetzt:

$$(19) \qquad (l^{-1}k)^p \equiv (k) \pmod{\mathfrak{p}},$$

d. h. je nachdem für $l$ die eine oder die andere der beiden zu $p$ gehörigen Classen $l$ gesetzt wird, ist der eine oder der andere Factor von (17) durch $\mathfrak{p}$ theilbar.

Durch wiederholte Anwendung von (18) ergiebt sich für jeden beliebigen positiven Exponenten $\pi$

$$(20) \qquad (k)^{p^\pi} \equiv (l^\pi k) \pmod{\mathfrak{p}}$$

(Schluss von $\pi$ auf $\pi + 1$).

Wenn nun $l$ zum Exponenten $\varepsilon$ gehört, oder $\varepsilon$ der Index von $p$ ist (§. 108, 5), so ist nach (20):

$$(21) \qquad (k)^{p^\varepsilon} \equiv (k) \pmod{\mathfrak{p}}$$

und $p^\varepsilon$ ist die niedrigste Potenz von $p$, welche dieser Bedingung genügt. Denn wenn noch eine niedrigere Potenz von $p$ die Congruenz (21) erfüllt, so folgt aus (20), dass zwei verschiedene Classeninvarianten $(k)$, $(k')$ nach dem Modul $\mathfrak{p}$ congruent sind. Es wäre also ihre Differenz $(k) - (k')$ durch $\mathfrak{p}$ und mithin die Discriminante von $H_m$ durch $p$ theilbar, gegen die Voraussetzung.

Daraus ergiebt sich nun wieder nach (7), dass die Congruenz

$$\zeta^{p^\varepsilon} \equiv \zeta \pmod{\mathfrak{p}}$$

für jede ganze Zahl $\zeta$ in $\mathfrak{K}$ erfüllt ist und daraus also der Satz:

Eine Primzahl $p$ zerfällt im Körper $\mathfrak{K}$ in lauter von einander verschiedene Primideale, deren Grad gleich dem Index von $p$ ist.

8. Wir wollen noch beweisen, dass es unter den verschiedenen in $p$ aufgehenden Primidealen $\mathfrak{p}$ immer eins giebt, für welches von den beiden aus (17) folgenden Congruenzen die Congruenz (18) besteht.

Dazu bemerken wir: Wenn wir die sämmtlichen Zahlen des Körpers $\mathfrak{K}$ in die conjugirt imaginären verwandeln, indem wir $\sqrt{-m}$ mit $-\sqrt{-m}$ und jede Classeninvariante $(k)$ mit der entgegengesetzten $(k^{-1})$ vertauschen, so gehen die sämmtlichen Zahlen eines Ideals $\mathfrak{a}$ in die Zahlen eines conjugirt imaginären Ideals $\mathfrak{a}'$ über, welches auch mit $\mathfrak{a}$ identisch sein kann. Dies folgt unmittelbar aus der Definition des Ideals (D. §. 168); ebenso leicht ergiebt sich auch, dass die Norm des Ideals $\mathfrak{a}$ gleich ist der Norm des Ideals $\mathfrak{a}'$, und dass, wenn $\mathfrak{a}$ ein Primideal ist, auch $\mathfrak{a}'$ ein Primideal sein muss.

Ist nun die Congruenz (18) nicht erfüllt, so muss nach (17)

$$(lk)^p \equiv (k) \pmod{\mathfrak{p}}$$

sein, und auch diese Congruenz bleibt bestehen, wenn $k$ durch eine andere Classe $k'$ ersetzt wird. Setzen wir also $l^{-1}k^{-1}$ an Stelle von $k$, so folgt:

$$(k^{-1})^p \equiv (l^{-1}k^{-1}) \pmod{\mathfrak{p}}.$$

Da also $(k^{-1})^p - (l^{-1}k^{-1})$ eine Zahl in $\mathfrak{p}$ ist, so ist $(k)^p - (lk)$ in dem zu $\mathfrak{p}$ conjugirten Ideal $\mathfrak{p}'$ enthalten, und es ist

$$(k)^p \equiv (lk) \pmod{\mathfrak{p}'},$$

was aus (18) durch Vertauschung von $\mathfrak{p}$ mit $\mathfrak{p}'$ hervorgeht.

Aus diesen Sätzen ist die Irreducibilität der Classengleichung (auch nach Adjunction von $\sqrt{-m}$) eine einfache Folge.

Sind $k$, $k'$ zwei beliebige Classen der Determinante $-m$, so können wir nach §. 108, 4. $k'$ in der Weise zusammensetzen

$$k' = k l l' l'' \ldots,$$

dass durch die Classen $l, l', l'' \ldots$ die Primzahlen $p, p', p'' \ldots$ darstellbar sind. Nach dem, was soeben bewiesen ist, können wir also die Primtheiler $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}''$ dieser Primzahlen so wählen, dass

$$(23)\qquad \begin{aligned} (k)^p &\equiv (kl) && \pmod{\mathfrak{p}} \\ (kl)^{p'} &\equiv (kll') && \pmod{\mathfrak{p}'} \\ (kll')^{p''} &\equiv (kll'l'') && \pmod{\mathfrak{p}''} \\ &\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

Nehmen wir jetzt an, es zerfalle die Classengleichung, es sei also für ein variables $t$

$$H_m(t) = H_1(t)\, H_2(t),$$

so können wir, da $k$, $k'$ beliebige Classen waren, $(k)$ unter den Wurzeln von $H_1(t)$, $(k')$ unter denen von $H_2(t)$ wählen. In der Kette (23) gehört also das Anfangsglied $(k)$ zu den Wurzeln $(k_1)$ von $H_1(t)$ und das Endglied $(k')$ zu den Wurzeln $(k_2)$ von $H_2(t)$. Da mindestens an einer Stelle der Kette (23) der Uebergang von den Wurzeln des einen Factors zu denen des anderen stattfinden muss, so giebt es ein Paar von Wurzeln $(k_1)$, $(k_2)$, welches für irgend eine Primzahl $p$ und ein darin aufgehendes Primideal $\mathfrak{p}$ der Congruenz

$$(k_1)^p \equiv (k_2) \pmod{\mathfrak{p}}$$

genügt. Da nun $H_1(k_1) = 0$ ist, so folgt durch den oft angewandten Schluss

$$H_1(k_1)^p \equiv H_1(k_1^p) \equiv H_1(k_2) \equiv 0 \pmod{\mathfrak{p}}.$$

Da nun

$$H_1(k_2) = \overset{k_1}{\Pi}[(k_2) - (k_1)]$$

ist, so muss eine der Differenzen $(k_2) - (k_1)$ durch $\mathfrak{p}$ theilbar sein, was nicht möglich ist, da $p$ nicht in der Discriminante von $H$ aufgeht.

Damit ist die Irreducibilität der Classengleichung bewiesen; der Grad des Körpers $\mathfrak{K}$ ist gleich dem Doppelten der Classenzahl $h$ festgestellt, und die im vorigen Paragraphen gefundene Gruppe $\mathfrak{S}$ ist als die wahre Gruppe der Classengleichung erkannt.

9. Eine interessante Folgerung ziehen wir noch aus diesen Resultaten. Es sei $p$ eine Primzahl der dritten Art vom Index $\varepsilon$ und

(24) $$p^\varepsilon = \mu\mu',$$

wenn zur Abkürzung

(25) $$\mu = \frac{x + y\sqrt{-m}}{2}, \quad \mu' = \frac{x - y\sqrt{-m}}{2}$$

gesetzt wird. Wir wissen nun, dass $p$ in lauter verschiedene Primideale vom Grade $\varepsilon$ zerfällt. $\mu$ und $\mu'$ haben, da $x$, $y$ theilerfremd sind, keinen gemeinsamen Primfactor. Jedem Primideal $\mathfrak{p}$, welches in $\mu$ aufgeht, entspricht ein davon verschiedenes (conjugirtes) Primideal $\mathfrak{p}'$, welches aus $\mathfrak{p}$ dadurch entsteht, dass man für alle Zahlen von $\mathfrak{p}$ die conjugirt imaginären Zahlen setzt. Es ist also $\mu$ nicht nur durch $\mathfrak{p}$, sondern durch $\mathfrak{p}^\varepsilon$ theilbar.

Wir kehren nun zurück zu den Zahlen $M$ [§. 109, (9), (17)], welche der Bedingung

(26) $$MM_1 \ldots M_{\varepsilon-1} = \varrho\mu$$

genügen. Nach §. 75, 4. ist $M$ die Wurzel einer Transformationsgleichung, welcher dort die Form gegeben war

(27) $$M\varphi(M, \gamma_2, \gamma_3) = p,$$

worin $\varphi$ eine ganze rationale Function mit ganzzahligen Coëfficienten, also in unserem Falle eine ganze algebraische Zahl bedeutet. Daraus folgt aber, dass $M$ (und ebenso $M_1, M_2 \ldots M_{\varepsilon-1}$) nicht durch eine höhere als die erste Potenz von $\mathfrak{p}$ theilbar sein kann, während doch $\mu$ durch $\mathfrak{p}^\varepsilon$ theilbar ist. Wir schliessen also aus (26), dass jede der Zahlen $M$, $M_1$, … $M_{\varepsilon-1}$ durch die erste Potenz von $\mathfrak{p}$ theilbar sein muss, dass mithin alle diese Zahlen associirt sind (d. h. sich nur durch Einheitsfactoren von einander unterscheiden). Bezeichnet also $\varrho$ irgend eine algebraische Einheit, so ist

$$\frac{x + y\sqrt{-m}}{2} = \varrho M^{\varepsilon},$$

also ist $\mu$ wirklich als $\varepsilon$te Potenz einer im Körper $\mathfrak{K}$ existirenden Zahl dargestellt.

## §. 111. Ueber die Primideale des Körpers $\mathfrak{K}$.

Wir haben im vorigen Paragraphen die Zerlegung der Primzahlen der zweiten und dritten Art in ihre Primideale zum Beweise der Irreducibilität benutzt. Es ist nur ein Punkt in dem Beweise, wo von der speciellen Form der Classengleichung $H = 0$, d. h. von der Annahme, dass gerade die Classeninvariante $j(\omega)$ zu Grunde gelegt ist, Gebrauch gemacht wird; nämlich in 7., bei Bestimmung des Grades von $\mathfrak{p}$. Aber auch, wenn statt $j(\omega)$ die Classeninvariante $f(\omega)$ oder eine Potenz dieser Function genommen wird, bleibt wegen §. 77, (6) der Beweis derselbe. Wählt man eine andere Classeninvariante, so werden in der Discriminante der Classengleichung einige Primfactoren wegfallen, andere auftreten und es ist sehr wahrscheinlich, dass der Satz 7. für alle Primzahlen $p$ gilt, die in der Discriminante irgend einer Classengleichung nicht aufgehen. Der allgemeine Beweis aber, ebenso wie die Zerlegung der Primzahlen der ersten Art überhaupt macht zur Zeit noch Schwierigkeiten, und wir beschränken uns auf die Herleitung eines darauf bezüglichen allgemeinen Satzes und auf die Betrachtung einiger Beispiele. Der allgemeine Satz lautet so:

Keine Primzahl vom Index 1, d. h. keine durch die Hauptform

$$p = y^2 + mx^2$$

darstellbare Primzahl geht in der Discriminante der Classengleichung auf.

Ist nämlich $p$ durch die Hauptform darstellbar, so ist $F_p(u, u)$ nach §. 101 durch das Quadrat von $H_m(u)$ theilbar (für ein variables $u$), also [nach §. 72, (31)]

$$H_m(u)^2\,\varphi(u) = F_p(u, u) = (u^p - u)^2 + p\,\psi(u),$$

worin $\varphi(u)$, $\psi(u)$ ganze rationale Functionen von $u$ mit ganzzahligen Coëfficienten sind. Durch zweimalige Differentiation nach $u$ folgt hieraus, wenn $\Phi(u)$, $\Psi(u)$ neue ganze rationale Functionen von $u$ sind:

$$H'_m(u)\, H'_m(u)\, \varphi(u) = -1 + p\,\Phi(u) + H_m(u)\, \Psi(u).$$

Also wenn $H_m(u) = 0$ ist, d. h. wenn $u$ eine Classeninvariante wird:

$$H'_m(u)\, H'_m(u)\, \varphi(u) \equiv -1 \pmod{p},$$

woraus hervorgeht, dass kein in $p$ aufgehendes Primideal in $H'_m(u)$, also $p$ nicht in der Discriminante von $H_m(u)$ aufgeht.

Wir wenden uns nun zur Betrachtung einiger Beispiele.

1. Classeninvarianten erster Art der Determinante $-11$.

Im §. 95, (7) haben wir für $x = f(\sqrt{-11})$ die Classengleichung aufgestellt:

$$(1) \qquad x^3 - 2x^2 + 2x - 2 = 0,$$

deren Discriminante

$$\Delta = -4 . 11$$

sich ergiebt. Es folgt also daraus, dass ausser 2 und 11 keine Primzahl durch das Quadrat eines Primideals theilbar ist, und wir beschränken uns auf die Betrachtung dieser beiden Primzahlen.

Ist $\mathfrak{z}$ ein in 2 aufgehendes Primideal, so ist nach (1):

$$x \equiv 0 \pmod{\mathfrak{z}},$$

und da $N(x) = 4$ ist, so ist $N(\mathfrak{z}) = 2$ oder $= 4$. Wäre $N(\mathfrak{z}) = 2$, wäre also $\mathfrak{z}$ ein Primideal ersten Grades, so wären alle Zahlen des Körpers 𝔎 entweder $\equiv 0$ oder $\equiv 1 \pmod{\mathfrak{z}}$. Dass das nicht der Fall ist, lehrt die Betrachtung der zu 𝔎 gehörigen Zahl

$$\alpha = \frac{1 + \sqrt{-11}}{2},$$

da

$$N(\alpha) = 27, \quad N(\alpha - 1) = 27,$$

also $\alpha$ weder $\equiv 0$ noch $\equiv 1 \pmod{\mathfrak{z}}$. Es ist daher $\mathfrak{z}$ ein Primideal zweiten Grades und $N(x) = N(\mathfrak{z})$, also $\mathfrak{o}x$ mit $\mathfrak{z}$ identisch. Die drei Wurzeln $x_0$, $x_1$, $x_2$ von (1) sind associirte Zahlen (d. h. sie unterscheiden sich nur durch Einheitsfactoren von einander) und es ist

$$2 = x_0\, x_1\, x_2,$$

also ist 2 der Cubus eines Primideals zweiten Grades.

Die Primzahl 11 ist zunächst associirt mit dem Quadrat der zu $\mathfrak{K}$ gehörigen Zahl $\sqrt{-11}$ und wir haben also nur die letztere zu zerlegen.

Sind, wie oben, $x_0, x_1, x_2$ die drei Wurzeln von (1), so haben wir

$$\sqrt{-11} = \frac{x_1 - x_2}{x_0} \; \frac{x_2 - x_0}{x_1} \; \frac{x_0 - x_1}{x_2}$$

und wenn wir

$$y_0 = \frac{x_1 - x_2}{x_0}, \quad y_1 = \frac{x_2 - x_0}{x_1}, \quad y_2 = \frac{x_0 - x_1}{x_2}$$

setzen, so sind $y_0, y_1, y_2$ die Wurzeln der Gleichung

$$(2) \qquad y^3 + \sqrt{-11}\, y^2 - 5y - \sqrt{-11} = 0,$$

deren Discriminante $-16$ ist. Es ist also

$$\sqrt{-11} = y_0 y_1 y_2,$$

und jeder Primtheiler von $y_0$ oder $y_1$ oder $y_2$ ist in $\sqrt{-11}$ enthalten. Aus der Gleichung

$$y_1 y_2 + y_2 y_0 + y_0 y_1 = -5$$

folgt, dass keine zwei der Grössen $y_0, y_1, y_2$ einen gemeinsamen Theiler haben, und folglich enthält $\sqrt{-11}$ mindestens drei von einander verschiedene Primideale. Die Betrachtung der Norm zeigt aber auch, dass es nicht mehr als drei Primideale enthalten kann, und dass diese vom ersten Grade sein müssen.

Die Gleichung (2), die zur Definition des Körpers $\mathfrak{K}$ dienen kann, hat die Discriminante $-16$. Eine noch einfachere Gleichung mit der Discriminante $-4$ erhält man für

$$z_0 = \frac{x_1}{x_2}, \quad z_1 = \frac{x_2}{x_0}, \quad z_2 = \frac{x_0}{x_1},$$

$$(3) \qquad z^3 + \frac{1 - \sqrt{-11}}{2} z^2 - \frac{1 + \sqrt{-11}}{2} z - 1 = 0.$$

2. Classeninvarianten der Determinante $-23$, $-31$.

Für die beiden Determinanten $-m = -23, -31$ haben wir im §. 98 die Classengleichungen erhalten

$$(4) \qquad m = 23, \quad x^3 - x - 1 = 0, \quad \text{Discr. } -23,$$

$$(5) \qquad m = 31, \quad x^3 - x^2 - 1 = 0, \quad \text{Discr. } -31,$$

wenn $f(\sqrt{-m}) = \sqrt{2}\, x$ gesetzt war.

Die Zahl 2 muss, da die Normen von

$$\alpha = \frac{r + \sqrt{-m}}{2}, \quad \alpha' = \frac{r - \sqrt{-m}}{2},$$

wenn $r$ eine ungerade Zahl ist, durch 2 theilbar sind, während $\alpha + \alpha' = r$ ist und also $\alpha$, $\alpha'$ und 2 relativ prim sind, mindestens zwei von einander verschiedene Primideale $\mathfrak{z}$, $\mathfrak{z}'$ enthalten, deren Grade höchstens $= 3$ sein können, da, wenn für $m = 23$ $r = 1$, für $m = 31$ $r = 3$ gesetzt wird, $N(\alpha)$ und $N(\alpha')$ nur durch $2^3$ theilbar sind. Nun kann aber der Grad von $\mathfrak{z}$ nicht $= 1$ sein, da sonst jede Zahl des Körpers $\mathfrak{K}$ einer rationalen Zahl modulo $\mathfrak{z}$ congruent wäre, was nach den Gleichungen (4), (5) für $x$ selbst nicht der Fall ist. Die Zahl $\alpha$ kann also nur durch ein Primideal dritten Grades theilbar sein und es zerfällt also 2 in zwei conjugirte Primideale dritten Grades.

Die Zerlegung von $\sqrt{-m}$ kann ebenso wie oben nach der Formel

$$\sqrt{-m} = (x_1 - x_2)(x_2 - x_0)(x_0 - x_1)$$

geschehen. Man erkennt leicht, dass die drei Factoren $x_1 - x_2$, $x_2 - x_0$, $x_0 - x_1$ relativ prim sind, und dass es also drei Primfactoren ersten Grades von $\sqrt{-m}$ sind.

Hier lassen sich Gleichungen aufstellen mit der Discriminante 1. Um diese zu erhalten, führen wir die neuen Unbekannten $y_0, y_1, y_2$ ein durch die Gleichungen:

$$m = 23,\quad \begin{aligned} y_1 - y_2 &= x_0, \\ y_2 - y_0 &= x_1, \\ y_0 - y_1 &= x_2, \end{aligned} \qquad m = 31,\quad \begin{aligned} y_1 - y_2 &= \frac{1}{x_0}, \\ y_2 - y_0 &= \frac{1}{x_1}, \\ y_0 - y_1 &= \frac{1}{x_2}. \end{aligned}$$

Da die Summe der drei Grössen rechts verschwindet, so ist diese Annahme gestattet, und wir können noch über die Summe der $y$ beliebig verfügen. Wir wollen setzen

$$y_0 + y_1 + y_2 = \sqrt{-m}$$

und erhalten die Gleichungen

$$(6)\qquad m = 23,\quad y^3 - \sqrt{-23}\, y^2 - 8y + \sqrt{-23} = 0,$$

$$(7)\qquad m = 31,\quad y^3 - \sqrt{-31}\, y^2 - 10y + \sqrt{-31} = 0,$$

deren Discriminanten in der That $= 1$ sind.

Ausser $-23$ und $-31$ giebt es keine dreiclassigen negativen Determinanten, die modulo 8 mit 1 congruent sind.

3. Classeninvarianten der Determinante $-63$.

Wir wollen noch eine Determinante mit quadratischem Factor betrachten und wählen dazu $m = 63$, für welche man nach der Methode §. 97, I sehr leicht die Classengleichung vierten Grades erhält

$$x^4 - 8x^3 + x + 1 = 0, \tag{8}$$

wenn

$$\sqrt{8}\, x = [f(\sqrt{-63})]^3$$

gesetzt ist. Die Discriminante dieser biquadratischen Gleichung findet sich leicht

$$= -27 . 63^2,$$

und von Interesse ist die Zerlegung der Primzahlen 2, 3, 7.

Was die Primzahl 2 betrifft, so schliesst man, wie in dem vorigen Falle, dass mindestens zwei conjugirte Ideale $\mathfrak{z}, \mathfrak{z}'$ in 2 aufgehen müssen; da, wie die Gleichung (8) zeigt, $x$ mit keiner der vier Zahlen

$$0,\ 1,\ \frac{1+\sqrt{-63}}{2},\ \frac{1-\sqrt{-63}}{2}$$

nach dem Modul $\mathfrak{z}$ congruent ist, so kann in 2 kein Primideal ersten oder zweiten Grades aufgehen, und es folgt, dass 2 das Product zweier von einander verschiedener Primideale vierten Grades ist.

Um die Zerlegung von 3 zu finden, substituiren wir in (8):

$$x = -\frac{1}{1+y},$$

wodurch sich für $y$ ergiebt:

$$y^4 + 3y^3 + 3y^2 + 9y + 9 = 0,$$

oder wenn wir

$$y^2 = 3(z+1)$$

einführen:

$$z^4 + 3z^3 - 6z - 3 = 0. \tag{9}$$

Nach (9) ist 3 mindestens durch die vierte Potenz eines Primideals $\mathfrak{p}$ theilbar; dies Primideal kann nicht vom ersten Grade sein, da es in $\mathfrak{K}$ Zahlen giebt, z. B. $\sqrt{-7}$, die nicht mit einer rationalen Zahl congruent sind nach dem Modul $\mathfrak{p}$, und daraus folgt:

3 ist die vierte Potenz eines Primideals zweiten Grades, und zwar des Hauptideals $\mathfrak{o}z$. Die Zahl $z$ ist eine Primzahl im Körper $\mathfrak{K}$.

Es handelt sich noch um die Zerlegung von $\sqrt{-7}$.

Da die Congruenz

$$x^4 - 8x^3 + x + 1 \equiv 0 \pmod{7}$$

keine rationale Lösung hat, so kann in $\sqrt{-7}$ kein Primideal ersten Grades aufgehen, und da $N(\sqrt{-7}) = 7^4$ ist, so bleiben die beiden Möglichkeiten, dass $\sqrt{-7}$ selbst eine Primzahl (Primideal vierten Grades) ist, oder dass $\sqrt{-7}$ in zwei Primideale zweiten Grades zerlegt wird. Es ist noch zu entscheiden, welcher dieser beiden Fälle eintritt, und ob im letzteren beide Primideale gleich oder verschieden sind.

Nach §. 106 lässt sich durch Adjunction von $\sqrt{21}$ die Classengleichung in zwei Factoren zerfällen und man findet in der That leicht:

$$\sqrt{7}(x^2 - x + 1) = \pm\sqrt{3}(x^2 + 3x - 1). \tag{10}$$

Für das obere Zeichen erhält man reelle Wurzeln $x_1$, $x_2$, für das untere conjugirt imaginäre $x'_1$, $x'_2$. Es ist aber nach (10):

$$x^2 + 3x - 1 \equiv 0 \pmod{\sqrt{-7}},$$

und daraus:

$$(x_1 - x_2)^2 \equiv (x'_1 - x'_2)^2 \equiv -1 \pmod{\sqrt{-7}}, \tag{11}$$

$x_1 - x_2$ und $x'_1 - x'_2$ sind also relativ prim zu $\sqrt{-7}$. Danach ist (wegen des Werthes der Discriminante):

$$(x_1 - x'_1)(x_1 - x'_2)(x_2 - x'_1)(x_2 - x'_2) \equiv 0 \pmod{7}.$$

Ist nun $(x_1 - x'_1)$ durch ein in 7 aufgehendes Primideal $\mathfrak{p}$ theilbar, so ist $(x_1 - x'_2)$ durch das conjugirte Ideal $\mathfrak{p}'$ theilbar, und da $(x_1 - x'_1)$ und $(x_1 - x'_2)$ wegen (11) mit $\sqrt{-7}$ keinen Theiler gemein haben können, so ist $\mathfrak{p}$ von $\mathfrak{p}'$ verschieden, also:

$\sqrt{-7}$ ist im Körper $\mathfrak{K}$ in zwei verschiedene Primideale zweiten Grades zerlegbar.

Wenn es gestattet ist, nach diesen Beispielen einen Schluss zu wagen, so würde folgen, dass in dem Körper $\mathfrak{K}$ nur diejenigen Primzahlen durch das Quadrat eines Primideals theilbar seien, welche in der Zahl $m$ aufgehen, und bei den Körpern der Classeninvarianten erster Art für ein $m \equiv 3 \pmod{8}$ die Primzahl 2. Ueberdies würde eine Primzahl, die nur einfach in $m$ enthalten ist, durch keine höhere als die zweite Potenz eines Primideals theilbar sein. Dahin deutet auch ein Ausspruch von Kronecker (Monatsberichte der Berliner Akademie, 26. Juni 1862, S. 368).

---

## Fünfzehnter Abschnitt.

## Die Normen der Classeninvarianten $f(\omega)$.

### §. 112. Convergenz einer unendlichen Reihe.

Kronecker hat zuerst einen höchst merkwürdigen directen Zusammenhang zwischen den quadratischen Formen und den Classeninvarianten aufgedeckt[1]), den wir zunächst ableiten und in seinen mannigfachen Anwendungen kennen lernen wollen. Wir schicken einen Satz über unendliche Reihen mit positiven Gliedern voraus.

Wir setzen von einer unendlichen Reihe $S$ voraus, dass ihre Glieder alle positiv und kleiner als eine gewisse endliche Zahl $\mu_0$ seien, ferner, dass nur eine endliche Anzahl ihrer Glieder grösser als ein beliebig gegebenes positives $\mu$ sei. Es bedeute $F(\mu)$ die Anzahl derjenigen Glieder von $S$, welche grösser als $\mu$ sind. Diese Function $F(\mu)$ ist, da sie nur ganzzahliger Werthe fähig ist, unstetig, verschwindet für $\mu = \mu_0$, wächst mit abnehmendem $\mu$ und wird unendlich für $\mu = 0$ (wenigstens wenn $S$ wirklich unendlich viele Glieder enthält).

Wir betrachten zunächst die Summe $S_n$ derjenigen Glieder von $S$, welche grösser als irgend eine Grösse $n$ sind, und schalten zwischen $\mu_0$ und $n$ die beliebigen Werthe $\mu_1, \mu_2 \ldots, \mu_{\nu-1}$ ein, so dass

$$\mu_0 > \mu_1 > \mu_2 \ldots > \mu_{\nu-1} > \mu_\nu = n.$$

Die Anzahl der zwischen $\mu_{h-1}$ und $\mu_h$ (mit Einschluss der oberen und Ausschluss der unteren Grenze) liegenden Glieder von $S$ ist dann $F(\mu_h) - F(\mu_{h-1})$ und daher ist:

---

[1]) Sitzungsberichte der Berliner Akademie, 22. Januar 1863, dann in denselben Sitzungsberichten aus den Jahren 1883, 1886, 1889.

$$\mu_1 [F(\mu_1) - F(\mu_0)] + \mu_2 [F(\mu_2) - F(\mu_1)]$$
$$+ \cdots \mu_\nu [F(\mu_\nu) - F(\mu_{\nu-1})] < S_n,$$
$$S_n \leqq \mu_0 [F(\mu_1) - F(\mu_0)] + \mu_1 [F(\mu_2) - F(\mu_1)]$$
$$+ \cdots \mu_{\nu-1} [F(\mu_\nu) - F(\mu_{\nu-1})].$$

Auf beiden Seiten dieser Ungleichheit werden die Glieder nur anders angeordnet, wenn wir setzen:

$$- \mu_1 F(\mu_0) + (\mu_1 - \mu_2) F(\mu_1)$$
$$+ \cdots (\mu_{\nu-1} - \mu_\nu) F(\mu_{\nu-1}) + \mu_\nu F(\mu_\nu) < S_n,$$
$$S_n \leqq - \mu_0 F(\mu_0) + (\mu_0 - \mu_1) F(\mu_1)$$
$$+ \cdots (\mu_{\nu-2} - \mu_{\nu-1}) F(\mu_{\nu-1}) + \mu_{\nu-1} F(\mu_\nu).$$

Da nun $F(\mu_0) = 0$ ist, so folgt, indem man die Differenzen $\mu_h - \mu_{h-1}$ verschwindend klein werden lässt:

$$S_n = n F(n) + \int_n^{\mu_0} F(\mu) \, d\mu.$$

Wenn $n$ gegen Null convergirt, so wird nach einem bekannten Satz der Integralrechnung das Integral nur dann convergiren können, wenn

$$\operatorname*{Lim}_{n=0} \, n F(n) = 0,$$

und es ist die Summe der Reihe $S$ zurückgeführt auf das Integral:

(1) $$S = \int_0^{\mu_0} F(\mu) \, d\mu.$$

Die Convergenz von $S$ hängt also ab von der Convergenz dieses Integrals.

Wir wenden dies an auf die folgende unendliche Reihe.

Es sei

(2) $$\psi(x, y) = A x^2 + 2 B x y + C y^2,$$

eine positive quadratische Form mit negativer Determinante:

$$- m = B^2 - A C,$$

und es werde gesetzt:

(3) $$S = \sum^{x, y} \frac{1}{\psi(x, y)^s},$$

worin $x$, $y$ alle positiven und negativen ganzzahligen Werthe mit alleiniger Ausnahme von $x = 0$, $y = 0$ durchlaufen, und $s$ einen beliebigen Exponenten bedeutet ($A$, $B$, $C$ brauchen hier zunächst noch nicht ganzzahlig zu sein).

Setzen wir

$$C\psi = m x^2 + (Bx + Cy)^2,$$

so folgt:

$$x^2 < \frac{C\psi}{m},$$

und ebenso:

$$y^2 < \frac{A\psi}{m}.$$

Ist also

$$\psi^s < \frac{1}{\mu},$$

so folgt:

$$x^2 < \frac{C}{m\mu^{\frac{1}{s}}}, \quad y^2 < \frac{A}{m\mu^{\frac{1}{s}}}.$$

Die Anzahlen der Werthe, welche $x$, $y$ annehmen können, sind daher bezw. kleiner als

$$2\mu^{-\frac{1}{2s}}\left(\sqrt{\frac{C}{m}} + \mu^{\frac{1}{2s}}\right), \quad 2\mu^{-\frac{1}{2s}}\left(\sqrt{\frac{A}{m}} + \mu^{\frac{1}{2s}}\right),$$

und da $F(\mu)$ die Anzahl der Paare $x$, $y$ ist

$$F(\mu) < 4\mu^{-\frac{1}{s}}\left(\sqrt{\frac{C}{m}} + \mu^{\frac{1}{2s}}\right)\left(\sqrt{\frac{A}{m}} + \mu^{\frac{1}{2s}}\right).$$

Das Integral (1) und mithin auch die Reihe (3) sind daher nach einem bekannten Satz aus der Theorie der bestimmten Integrale[1]) convergent, so lange $s$ positiv und grösser als 1 ist. Es handelt sich um das Verhalten von $S$ bei Annäherung von $s$ an den Grenzwerth 1.

## §. 113. Die Kronecker'sche Grenzformel.

Wir ordnen die Glieder der Reihe

$$S = \sum^{x,y} \frac{1}{\psi(x, y)^s}$$

---

[1]) Man findet diesen, sowie die nachher zu benutzenden Sätze über $\Gamma$-Functionen und Fourier'sche Reihen in jedem ausführlicheren Lehrbuche der Integralrechnung. Vgl. z. B. „Vorlesungen über bestimmte Integrale“ nach Dirichlet von G. F. Meyer, Leipzig 1871, oder: Serret, Differential- und Integralrechnung, deutsch von Harnack, 1885.

zunächst in der Weise an, dass wir die dem verschwindenden $y$ entsprechenden Glieder absondern und von den übrigen je zwei, welche entgegengesetzten Werthen von $x$ und $y$ entsprechen, zusammenfassen.

So erhalten wir:

$$(1) \qquad S = M_s + N_s,$$

wenn zur Abkürzung

$$(2) \qquad M_s = 2 \sum_{1,\infty}^{y} \sum_{-\infty,\infty}^{x} \frac{1}{(Ax^2 + 2Bxy + Cy^2)^s},$$

$$(3) \qquad N_s = 2 \sum_{1,\infty}^{x} \frac{1}{(Ax^2)^s}$$

gesetzt ist. Der Werth $N$, welchen $N_s$ für $s = 1$ erhält, lässt sich, da die Reihe für $s = 1$ unbedingt convergent bleibt, direct bestimmen und ergiebt:

$$(4) \qquad N = \frac{2}{A} \sum_{1,\infty}^{x} \frac{1}{x^2} = \frac{\pi^2}{3A}.$$

Um das Verhalten von $M_s$ für $s = 1$ zu ermitteln, zerlegen wir die Function $\psi(x, y) = Ax^2 + 2Bxy + Cy^2$ in zwei conjugirt imaginäre lineare Factoren:

$$Ax^2 + 2Bxy + Cy^2 = A(x + \omega_1 y)(x - \omega_2 y),$$

wenn

$$(5) \qquad \omega_1 = \frac{B + i\sqrt{m}}{A}, \quad \omega_2 = \frac{-B + i\sqrt{m}}{A}$$

so erklärt werden, dass $\sqrt{m}$ positiv ist.

Hierdurch wird

$$(6) \qquad M_s = \frac{2}{A^s} \sum_{1,\infty}^{y} \sum_{-\infty,\infty}^{x} \frac{1}{(x + \omega_1 y)^s (x - \omega_2 y)^s}.$$

Nun ist nach einem bekannten Satz aus der Theorie der $\Gamma$-Functionen, wenn $k$ eine beliebige Grösse mit positiv imaginärem Bestandtheil bedeutet:

$$\frac{1}{(-ik)^s} = \frac{(2\pi)^s}{\Gamma(s)} \int_0^\infty e^{2\pi i k \xi} \xi^{s-1} \, d\xi,$$

worin die Potenz $(-ik)^s$ dadurch eindeutig erklärt ist, dass, wenn $-ik = \varrho e^{i\Theta}$ gesetzt, $\varrho$ positiv und der Winkel $\Theta$ zwischen $-\frac{\pi}{2}$ und $+\frac{\pi}{2}$ angenommen wird, $(-ik)^s = \varrho^s e^{i\Theta s}$ zu setzen ist.

Ersetzt man hierin $ik$ durch die conjugirt imaginäre Grösse $-ik'$, indem man zugleich einen neuen Integrationsbuchstaben $\eta$ wählt, und multiplicirt beide Gleichungen, so folgt:

$$(7)\qquad \frac{1}{(kk')^s} = \frac{(2\pi)^{2s}}{\Gamma(s)\,\Gamma(s)} \int_0^\infty d\xi \int_0^\infty d\eta\, e^{2\pi i(k\xi - k'\eta)}\,(\xi\eta)^{s-1}.$$

Hierin setzen wir für $k$, $k'$ die beiden conjugirten Factoren $x + \omega_1 y$, $x - \omega_2 y$ von $\psi$ und führen den Integralausdruck (7) in (6) ein.

Dadurch erhalten wir:

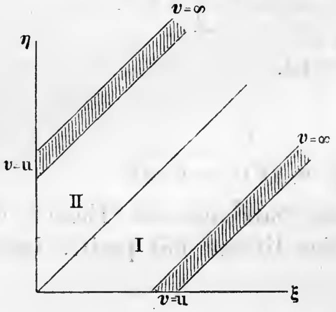
$$(8)\quad M_s = \frac{(2\pi)^{2s}}{A^s\,\Gamma(s)\,\Gamma(s)} \sum^{x,y} 2 \int_0^\infty\!\!\int_0^\infty e^{2\pi i[x(\xi-\eta)+y(\omega_1\xi+\omega_2\eta)]}\,(\xi\eta)^{s-1}\,d\xi\,d\eta.$$

Wir fassen nun das Product der beiden Integrale auf der rechten Seite dieses Ausdruckes, welches wir zur Abkürzung durch

$$(9)\qquad W = 2\int_0^\infty\!\!\int_0^\infty e^{2\pi i[x(\xi-\eta)+y(\omega_1\xi+\omega_2\eta)]}\,(\xi\eta)^{s-1}\,d\xi\,d\eta$$

bezeichnen, als Doppelintegral auf, welches, wenn $\xi$, $\eta$ als rechtwinklige Coordinaten in der Ebene gedeutet werden, sich über den positiven Quadranten des Coordinatensystems erstreckt.

Fig. 4.



Um das Doppelintegral umzuformen, theilen wir den Integrationsbereich durch eine den Winkel halbirende Gerade in die beiden Theile I, II (s. die Fig. 4), und substituiren im ersten Theil

$$\xi - \eta = u,\quad \xi + \eta = v,$$

im zweiten Theil:

$$\xi - \eta = -u,\quad \xi + \eta = v.$$

Wenn man dann, wie die Figur andeutet, zuerst bei constantem $u$ in Bezug auf $v$ integrirt, so erhält man:

$$W = \int_0^\infty e^{2\pi i x u}\,du \int_u^\infty e^{\pi i y[u(\omega_1-\omega_2)+v(\omega_1+\omega_2)]} \left(\frac{v^2-u^2}{4}\right)^{s-1} dv,$$

$$+ \int_0^\infty e^{-2\pi i x u}\,du \int_u^\infty e^{\pi i y[-u(\omega_1-\omega_2)+v(\omega_1+\omega_2)]} \left(\frac{v^2-u^2}{4}\right)^{s-1} dv,$$

oder, wenn wir zur Abkürzung

$$(10)\qquad \varphi_{\pm}(u) = \int_u^\infty e^{\pi i y[v(\omega_1+\omega_2) \pm u(\omega_1-\omega_2)]} \left(\frac{v^2-u^2}{4}\right)^{s-1} dv$$

setzen,

$$(11)\qquad W = \int_0^\infty e^{2\pi i x u}\, \varphi_+(u)\, du + \int_0^\infty e^{-2\pi i x u}\, \varphi_-(u)\, du.$$

Diese nach $u$ genommenen Integrale zerlegen wir in lauter solche Bestandtheile, deren Grenzen die Reihe der ganzen Zahlen sind, wir setzen also, da $x$ eine ganze Zahl ist:

$$(12)\qquad \begin{aligned} \int_0^\infty e^{\pm 2\pi i x u}\, \varphi_\pm(u)\, du &= \sum_{0,\infty}^{\nu} \int_\nu^{\nu+1} e^{\pm 2\pi i x u}\, \varphi_\pm(u)\, du, \\ &= \sum_{0,\infty}^{\nu} \int_0^1 e^{\pm 2\pi i x u}\, \varphi_\pm(u+\nu)\, du, \\ &= \int_0^1 e^{\pm 2\pi i x u} f(u)\, du, \end{aligned}$$

wenn wiederum

$$(13)\qquad f(u) = \sum_{0,\infty}^{\nu} \varphi_\pm(u+\nu)$$

gesetzt ist.

Wenn wir nun zunächst die Summation in Bezug auf $x$ ausführen, so können wir von der Grundformel aus der Theorie der Fourier'schen Reihen Gebrauch machen:

$$(14)\qquad \begin{aligned} \sum_{-\infty,\infty}^{x} \int_0^1 e^{\pm 2\pi i x u} f(u)\, du &= \frac{1}{2}[f(0) + f(1)] \\ &= \frac{1}{2}\varphi_\pm(0) + \sum_{1,\infty}^{\nu} \varphi_\pm(\nu), \end{aligned}$$

und erhalten also, da nach (10)

$$(15)\qquad \varphi_+(0) = \varphi_-(0) = \varphi(0) = \int_0^\infty e^{\pi i y v(\omega_1+\omega_2)} \left(\frac{v}{2}\right)^{2s-2} dv$$

ist, aus (11), (12) und (14):

$$(16)\qquad \sum_{-\infty,\infty}^{x} W = \varphi(0) + \sum_{1,\infty}^{\nu} [\varphi_+(\nu) + \varphi_-(\nu)].$$

Führen wir dies in (8) ein, so zerfällt $M_s$ in zwei Theile

$$(17)\qquad M_s = P_s + Q_s,$$

wenn

$$(18)\qquad P_s = \frac{(2\pi)^{2s}}{A^s\, \Gamma(s)\, \Gamma(s)} \sum_{1,\infty}^{y} \varphi(0),$$

$$(19) \qquad Q_s = \frac{(2\pi)^{2s}}{A^s\,\Gamma(s)\,\Gamma(s)} \sum_{1,\infty}^{y} \sum_{1,\infty}^{\nu} [\varphi_+(\nu) + \varphi_-(\nu)]$$

gesetzt wird.

Nach (15) ist, wenn wir für $v$ eine neue Integrationsvariable $t$ durch die Gleichung

$$\pi i v(\omega_1 + \omega_2) = -\frac{2\pi v\sqrt{m}}{A} = -t$$

einführen, und die Summation nach $y$ ausführen:

$$\sum_{1,\infty}^{y} \varphi(0) = \frac{2A^{2s-1}}{(4\pi\sqrt{m})^{2s-1}} \int_0^\infty \frac{t^{2s-2}\,dt}{e^t - 1},$$

also:

$$(20) \qquad P_s = \frac{(2\pi)^{2s} A^{s-1}}{(4\pi\sqrt{m})^{2s-1}\,\Gamma(s)^2}\, 2\int_0^\infty \frac{t^{2s-2}\,dt}{e^t - 1}.$$

Hieraus lässt sich der Grenzwerth $P$ leicht bestimmen. Es ist nämlich das Integral

$$(21) \qquad \int_0^\infty t^{2s-2} e^{-t} \left(\frac{1}{1-e^{-t}} - \frac{1}{t}\right) dt,$$

da der in der Klammer stehende Ausdruck für $t = 0$ und $t = \infty$ einen endlichen Werth behält, bis $s = 1$ stetig, und hat daher den Grenzwerth:

$$\int_0^\infty e^{-t} \left(\frac{1}{1-e^{-t}} - \frac{1}{t}\right) dt = -\Gamma'(1) = 0{,}5772\ldots$$

Zerlegt man also das Integral (21) in seine beiden Bestandtheile und setzt:

$$\int_0^\infty t^{2s-3} e^{-t}\, dt = \Gamma(2s-2) = \frac{\Gamma(2s-1)}{2(s-1)},$$

so folgt:

$$\lim_{s=1} \left( \int_0^\infty \frac{t^{2s-2}\,dt}{e^t - 1} - \frac{\Gamma(2s-1)}{2(s-1)} \right) = -\Gamma'(1),$$

und wenn man also die Entwickelung nach Potenzen von $s-1$:

$$\Gamma(2s-1) = 1 + 2\Gamma'(1)(s-1) + \cdots$$

einsetzt

$$(22) \qquad \lim_{s=1} \left\{ 2\int_0^\infty \frac{t^{2s-2}\,dt}{e^t - 1} - \frac{1}{s-1} \right\} = 0.$$

Man erhält ferner durch Entwickelung nach Potenzen von $s - 1$:

$$(23) \qquad \frac{(2\pi)^{2s} A^{s-1}}{(4\pi\sqrt{m})^{2s-1}\Gamma(s)^2}$$

$$= \frac{\pi}{\sqrt{m}}\left[1 + (s-1)\left(\log\frac{A}{4m} - 2\Gamma'(1)\right) + \cdots\right]$$

so dass nach (20):

$$(24) \qquad P_s = \frac{(2\pi)^{2s} A^{s-1}}{(4\pi\sqrt{m})^{2s-1}\Gamma(s)^2}\left(2\int_0^\infty \frac{t^{2s-2}\,dt}{e^t - 1} - \frac{1}{s-1}\right)$$

$$+ \frac{\pi}{\sqrt{m}(s-1)} + \frac{\pi}{\sqrt{m}}\left(\log\frac{A}{4m} - 2\Gamma'(1)\right) + \cdots,$$

worin die noch folgenden Glieder mit $s = 1$ verschwinden. Daraus folgt:

$$(25) \qquad \operatorname{Lim}\left(P_s - \frac{\pi}{\sqrt{m}(s-1)}\right) = \frac{\pi}{\sqrt{m}}\left(\log\frac{A}{4m} - 2\Gamma'(1)\right).$$

Es bleibt noch der Bestandtheil $Q_s$ zu untersuchen übrig, der für $s = 1$ einen endlichen Grenzwerth $Q$ erhält, den wir ohne Weiteres durch Einsetzen des Werthes $s = 1$ bestimmen können.

Es lässt sich nämlich in (10), so lange $u$ und $y$ grösser als Null sind, nach Einsetzen des Werthes $s = 1$ die Integration ausführen und ergiebt mit Rücksicht auf den Werth $2i\sqrt{m}$ von $A(\omega_1 - \omega_2)$:

$$\varphi_\pm(\nu) = \frac{A}{2\pi\sqrt{m}\,y}\, e^{2\pi i y \nu \omega},$$

worin $\omega = \omega_1$ oder $= \omega_2$ zu setzen ist, je nachdem das obere oder untere Zeichen in $\varphi_\pm(\nu)$ genommen wird. Durch Ausführung der Summation nach $y$ folgt hieraus:

$$\sum_{1,\infty}^{\nu}\sum_{1,\infty}^{y} \varphi_\pm(\nu) = -\frac{A}{2\pi\sqrt{m}}\sum_{1,\infty}^{\nu}\log(1 - e^{2\pi i \nu \omega}),$$

und die Summe nach $\nu$ lässt sich auf die Function $\eta(\omega)$ zurückführen, da nach §. 21, (7):

$$\eta(\omega) = e^{\frac{\pi i \omega}{12}} \prod_{1,\infty}^{\nu}(1 - e^{2\pi i \nu \omega})$$

ist. Danach wird, immer für $s = 1$,

$$\sum_{1,\infty}^{\nu}\sum_{1,\infty}^{y} \varphi_\pm(\nu) = -\frac{A}{2\pi\sqrt{m}}\left(\log\eta(\omega) - \frac{\pi i \omega}{12}\right).$$

Führen wir dies Resultat in (19) ein, nachdem wir dort $s = 1$ gesetzt haben, so ergiebt sich der Grenzwerth von $Q_s$:

$$(26) \qquad Q = -\frac{2\pi}{\sqrt{m}} \log \eta(\omega_1)\eta(\omega_2) - \frac{\pi^2}{3A}.$$

Hiernach erhalten wir aus (4), (25), (26) die folgende Grenzformel, deren Ableitung das Ziel dieser Betrachtung war:

$$(27) \qquad \operatorname*{Lim}_{s=1} \sum^{x,y} \frac{1}{(Ax^2 + 2Bxy + Cy^2)^s} - \frac{\pi}{(s-1)\sqrt{m}}$$
$$= -\frac{2\pi\Gamma'(1)}{\sqrt{m}} + \frac{\pi}{\sqrt{m}} \log \frac{A}{4m} - \frac{2\pi}{\sqrt{m}} \log \eta(\omega_1)\eta(\omega_2).$$

Eine einfachere Gleichung leiten wir hieraus für die Function

$$f(\omega) = e^{-\frac{\pi i}{24}} \frac{\eta\left(\frac{\omega+1}{2}\right)}{\eta(\omega)}$$

ab. Ersetzen wir nämlich in (27) $\omega_1$, $\omega_2$ durch

$$\omega_1' = \frac{\omega_1 + 1}{2}, \quad \omega_2' = \frac{\omega_2 - 1}{2},$$

also die Form

$$(28) \qquad \psi = (A, B, C)$$

durch die Form derselben Determinante:

$$(29) \qquad \psi' = \left(2A, B - A, \frac{A - 2B + C}{2}\right),$$

und subtrahiren die beiden so erhaltenen Ausdrücke (27), so folgt:

$$(30) \qquad \operatorname*{Lim}_{s=1} \left(\sum^{x,y} \frac{1}{\psi^s} - \sum^{x,y} \frac{1}{\psi'^s}\right) = \frac{2\pi}{\sqrt{m}} \log \frac{f(\omega_1) f(\omega_2)}{\sqrt{2}}.$$

Aus (27) ergiebt sich noch:

$$\operatorname{Lim} (s-1) \sum^{x,y} \frac{1}{\psi^s} = \frac{\pi}{\sqrt{m}},$$

also nur abhängig von der Determinante $-m$, nicht von der besonderen Form $\psi$. Verstehen wir also jetzt unter $A$, $B$, $C$ ganze Zahlen und lassen $\psi$ ein vollständiges Repräsentantensystem der zur Determinante $-m$ gehörigen Formenclassen durchlaufen, so folgt:

$$(31) \qquad \operatorname*{Lim}_{s=1} (s-1) \sum^{\psi} \sum^{x,y} \frac{1}{\psi^s} = \frac{\pi h}{\sqrt{m}},$$

wenn $h$ die zur Determinante $-m$ gehörige Classenzahl ist. Dabei kann man nach Belieben die Formen erster und zweiter Art zusammenfassen oder trennen.

Setzen wir den Coëfficienten $A$ ungerade und $B \equiv m+1 \pmod{2}$ voraus, so entsteht $\psi'$ durch Composition von $\psi$ mit $\psi_0$, also:

$$\psi' = \psi\,\psi_0, \tag{32}$$

wenn

$$\psi_0 = \left(2, 1, \frac{m+1}{2}\right) \quad \text{oder} \quad = \left(2, 0, \frac{m}{2}\right), \tag{33}$$

je nachdem $m$ ungerade oder gerade ist.

Wenn $m \equiv 1$ oder $\equiv 2 \pmod{4}$ ist, so ist $\psi_0$ primitiv von der ersten Art, und $\psi'$ durchläuft gleichzeitig mit $\psi$ ein vollständiges Repräsentantensystem der Determinante $-m$.

Wenn dagegen $m \equiv 3 \pmod{4}$ ist, so ist $\psi'$ von der zweiten Art und durchläuft ein oder drei Repräsentantensysteme von Formen zweiter Art, je nachdem $m \equiv 7$ oder $\equiv 3 \pmod{8}$ ist.

Bei der Bildung von $\omega_1$, $\omega_2$ ist die über $A$, $B$ gemachte Voraussetzung nicht bindend, da die in (27) und (30) vorkommenden Summen ungeändert bleiben, wenn $\psi$ durch eine äquivalente Form ersetzt wird. Wenn $\psi$ ein vollständiges Repräsentantensystem der Determinante $-m$ durchläuft, so durchlaufen $\omega_1$ und $\omega_2$ dieselbe Werthreihe, die wir als ein zur Determinante $-m$ gehöriges vollständiges Wurzelsystem bezeichnen wollen.

Ist $m \equiv 1$ oder $\equiv 2 \pmod{4}$, so ergiebt sich hiernach durch Summation der Formel (30):

$$\Pi \frac{f(\omega)}{\sqrt{2}} = 1, \tag{34}$$

wenn das Product $\Pi$ sich auf ein solches vollständiges Wurzelsystem bezieht. Dies Product auch für die anderen Fälle zu bestimmen, wird unser nächstes Ziel sein.

## §. 114. Die Normen der Classeninvarianten $f(\omega)$.

Wir lassen $\omega$ ein vollständiges Wurzelsystem von zur Determinante $-m$ gehörigen Classen erster Art durchlaufen, und setzen voraus, dass in der Form $(A, B, C)$, deren Wurzel $\omega$ ist, $A$, $C$ ungerade, $A$ relativ prim zu $m$ sei; dann sind nach §. 93 die 24ten Potenzen von $f(\omega)$ Classeninvarianten und ihre Norm ist eine Potenz von 2.

In einer ambigen Classe giebt es stets einen Repräsentanten von einer der beiden Formen:

$$(A,\ 0,\ C),\quad (A,\ B,\ A),$$

worin $A$ ungerade vorausgesetzt werden kann[1]. Im ersten Falle ist $\omega$ rein imaginär und folglich [§. 21, (10)]:

$$f(\omega),\ f_1(\omega),\ f_2(\omega)$$

reell und positiv; im zweiten Falle sind $\omega$ und $1:\omega$ conjugirt imaginär, folglich:

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

reell und

$$f_1(\omega) = f_2\left(-\frac{1}{\omega}\right),\quad f_2(\omega) = f_1\left(-\frac{1}{\omega}\right)$$

conjugirt imaginär, und nach der Formel $f(\omega) f_1(\omega) f_2(\omega) = \sqrt{2}$ ist auch hier $f(\omega)$ positiv.

Wir können also den Repräsentanten $(A,\ B,\ C)$ immer so gewählt annehmen, dass $A$ und $C$ ungerade sind und dass $f(\omega)$ für eine ambige Classe reell und positiv wird; repräsentiren wir ferner zwei entgegengesetzte Classen durch $(A,\ \pm B,\ C)$, so sind die entsprechenden Werthe von $f(\omega)$ conjugirt imaginär, ihr Product daher positiv, und es folgt also nach diesen Bestimmungen, dass das Product

$$\Pi f(\omega)$$

einen positiven reellen Werth hat, der eine Potenz von 2 ist. Wir setzen, indem wir mit $h$ die Anzahl der primitiven Classen erster Art bezeichnen, diese Potenz $= 2^{h\tau}$, so dass

$$\Pi \frac{f(\omega)}{2^{\tau}} = 1. \tag{1}$$

Es wird unsere Aufgabe sein, diesen Exponenten $\tau$ zu bestimmen. Wir schicken aber noch folgende Bemerkung voraus, die dieser Aufgabe ein erhöhtes Interesse verleiht.

In Folge der Gleichung [§. 49, (8)]:

$$f(\omega)^{24} - \gamma_2(\omega) f(\omega)^8 - 16 = 0 \tag{2}$$

---

[1] Vgl. Dirichlet-Dedekind, §. 58, §. 66. Die Form $\left(A, \frac{1}{2} A, C\right)$ bei geradem $A$ und ungeradem $C$ ist äquivalent mit $\left(C, -\frac{1}{2} A, A\right)$ und äquivalent mit $\left(C, C - \frac{1}{2} A, C\right)$.

ist, wenn $\omega$ die Wurzel einer zur Classe $k$ gehörigen Form der Determinante $-m$ ist, $f(\omega)$ eine ganze algebraische Zahl, und da $f(\omega)^8$ in (2) auch durch $-f_1(\omega)^8$, $-f_2(\omega)^8$ ersetzt werden kann, so sind auch $f_1(\omega)$, $f_2(\omega)$ ganze algebraische Zahlen. Mithin ist es auch

$$\frac{\sqrt{2}}{f(\omega)} = f_1(\omega) f_2(\omega).$$

Ist $p$ eine ungerade Primzahl, von welcher $-m$ quadratischer Rest ist, und $p$ durch die Formen der Classe $l$ (der Determinante $-m$) darstellbar, so ist bei passender Bestimmung von $c$ nach §. 108:

$$\frac{c+\omega}{p}$$

die Wurzel einer zur componirten Classe $lk$ gehörigen Form, und es kann (wenn nicht gerade $p = 3$ ist), $c$ durch 48 theilbar angenommen werden. Setzen wir also:

$$u = f(\omega), \quad v = f\left(\frac{c+\omega}{p}\right),$$

so ist sowohl $uv$ als $2:uv$ eine ganze algebraische Zahl.

Wenn wir daher nach §. 77

$$B = (uv)^s + \left(\frac{2}{p}\right) \frac{2^s}{(uv)^s},$$

$$A = \left(\frac{u}{v}\right)^r + \left(\frac{v}{u}\right)^r$$

setzen (wo jetzt $A$, $B$ natürlich nicht zu verwechseln sind mit den Coëfficienten der quadratischen Form), so ist $B$ eine ganze algebraische Zahl, und nach §. 77, (14) ist $A$ die Wurzel einer algebraischen Gleichung, deren Coëfficienten ganze algebraische Zahlen sind. Es ist also $A$ ebenfalls eine ganze algebraische Zahl (§. 59, 3).

Da aber die beiden Quotienten $u^r : v^r$ und $v^r : u^r$ die Wurzeln der quadratischen Gleichung

$$x^2 - Ax + 1 = 0$$

sind, so folgt, dass

$$\frac{u}{v} \text{ und } \frac{v}{u}$$

ganze Zahlen, und da sie zu einander reciprok sind, Einheiten sind.

Zwei ganze algebraische Zahlen, von denen sich die eine von der anderen nur durch einen Factor unterscheidet, der eine Einheit ist, heissen associirte Zahlen, und es sind also $u$ und $v$ associirte Zahlen.

Da man nun nach §. 108, 4. durch wiederholte Compositionen mit Classen $l$ (durch welche Primzahlen darstellbar sind) von jeder Classe $k$ zu jeder anderen Classe $k'$ derselben Determinante gelangen kann, und da zwei mit einer dritten associirten Zahl unter einander associirt sind, so haben wir den Satz:

Setzt man für $\omega$ die $h$ Wurzeln der Formen erster Art eines Systems von Repräsentanten der Determinante $-m$, so sind die $h$ Zahlen $f(\omega)$ unter einander associirt; und daraus nach (1) unmittelbar den merkwürdigen Satz, der sich leicht an allen Beispielen bestätigen lässt:

$f(\omega) : 2^\tau$ ist eine ganze Zahl und zwar eine Einheit.

1. Die Bestimmung der Exponenten $\tau$ ist durch elementare Hülfsmittel möglich, wenn $m \equiv 1$ oder $\equiv 2 \pmod 4$ oder $m \equiv 3 \pmod 8$.

Machen wir in der Gleichung mit ungeraden äusseren Coëfficienten

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

mit der Determinante $B^2 - AC = -m$ die Substitution

$$\omega = \frac{\omega' - 1}{\omega' + 1}, \quad \omega' = -\frac{\omega + 1}{\omega - 1},$$

so erhalten wir die Gleichung

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

welche gleichfalls die Determinante $-m$ hat und worin, wenn $m \equiv 1$ oder $\equiv 2 \pmod 4$ ist, die beiden äusseren Coëfficienten ungerade sind; denn es ist:

für $m \equiv 1 \pmod 4$, $B \equiv 0 \pmod 2$, $A + C \equiv 2 \pmod 4$,

für $m \equiv 2 \pmod 4$, $B \equiv 1 \pmod 2$, $A + C \equiv 0 \pmod 4$.

Daraus folgt, dass

$$f(\omega) \text{ und } f\left(\frac{\omega - 1}{\omega + 1}\right),$$

von 24sten Einheitswurzeln abgesehen, dieselbe Werthreihe durchläuft, also:

$$\Pi\, f(\omega) f\left(\frac{\omega - 1}{\omega + 1}\right) = 2^{2h\tau},$$

andererseits ist aber [§. 29, (18)]:

$$f(\omega) f\left(\frac{\omega - 1}{\omega + 1}\right) = \sqrt{2},$$

woraus sich ergiebt:

$$(3) \qquad \tau = \frac{1}{4}, \quad m \equiv 1, 2 \pmod 4,$$

in Uebereinstimmung mit dem Resultat des vorigen Paragraphen [§. 113, (34)].

2. Ist sodann $m \equiv 3 \pmod 8$, so lassen sich, wie wir im §. 89 gesehen haben, die Functionen $f(\omega)$ zu je dreien zusammenstellen, die aus einer und derselben Form zweiter Art hergeleitet sind. Die Formeln §. 89, (10) zeigen, dass, wenn $\omega'$ die Wurzel einer Form zweiter Art ist, diese drei Werthe folgende sind [vgl. §. 93, (13) und §. 29]:

$$f_1(2\omega') = \frac{\sqrt{2}}{f_2(\omega')},$$

$$f_2\left(\frac{\omega'}{2}\right) = \frac{\sqrt{2}}{f_1(\omega')},$$

$$f_2\left(\frac{\omega' + 1}{2}\right) = \frac{\sqrt{2}}{f(\omega')},$$

deren Product $= 2$ ist. Hiernach ist:

$$\Pi f(\omega) = 2^{\frac{1}{3} h},$$

also

$$(4) \qquad \tau = \frac{1}{3}, \quad m \equiv 3 \pmod 8.$$

3. Für den Fall $m \equiv 7 \pmod 8$ können wir den Werth von $\tau$ auf diesem einfachen Wege nicht bestimmen. Es ist dazu die im vorigen Paragraphen abgeleitete Grenzformel erforderlich. Zunächst behandeln wir die beiden Fälle $m \equiv 3 \pmod 4$ gleichmässig und setzen, wenn $\psi$ und $\psi'$ je eine zur Determinante $-m$ gehörige Form erster und zweiter Art bedeutet:

$$S = \sum^{x,y} \frac{1}{\psi^s}, \quad S' = \sum^{x,y} \frac{2^s}{\psi'^s},$$

worin $x$, $y$ alle ganzzahligen positiven und negativen Werthe mit Ausnahme von 0, 0 durchlaufen. Die Summe $S'$ zerlegen wir in vier Partialsummen $S'_{00}$, $S'_{01}$, $S'_{10}$, $S'_{11}$, so dass $x$, $y$ in $S'_{00}$ nur geradzahlige, in $S'_{11}$ nur ungeradzahlige Werthe durchlaufen, während in $S'_{10}$ $x$ die ungeraden, $y$ die geraden Zahlen durchläuft, und umgekehrt in $S'_{01}$. Wir können dann setzen:

(5) $$S' + 2\,S'_{00} = (S'_{01} + S'_{00}) + (S'_{10} + S'_{00}) + (S'_{11} + S'_{00}).$$

Ersetzen wir nun:

$$\begin{array}{llllll}
\text{in} & S'_{00} & x,\,y & \text{durch} & 2\,x, & 2\,y, \\
\text{„} & S'_{01} + S'_{00} & x,\,y & \text{„} & 2\,x, & y, \\
\text{„} & S'_{10} + S'_{00} & x,\,y & \text{„} & x, & 2\,y, \\
\text{„} & S'_{00} + S'_{11} & x,\,y & \text{„} & x - y, & x + y,
\end{array}$$

so sind die neuen $x$, $y$ keiner Beschränkung mehr unterworfen, und es ergiebt sich, wenn wir

(6) $$\begin{aligned}
\psi' &= (2\,A,\, B,\, 2\,C) = 2\,(A\,x^2 + B\,x\,y + C\,y^2), \\
\psi_1 &= (4\,A,\, B,\, C), \\
\psi_2 &= (A,\, B,\, 4\,C), \\
\psi_3 &= (A + B + C,\; C - A,\; A - B + C)
\end{aligned}$$

setzen:

(7) $$\begin{aligned}
4^s\,S'_{00} &= S' \\
S'_{01} + S'_{00} &= \sum^{x,y} \psi_1^{-s}, \\
S'_{10} + S'_{00} &= \sum^{x,y} \psi_2^{-s}, \\
S'_{00} + S'_{11} &= \sum^{x,y} \psi_3^{-s}.
\end{aligned}$$

Setzen wir $A$ als ungerade voraus, und lassen $\psi'$ ein vollständiges Repräsentantensystem von Classen zweiter Art durchlaufen, so durchlaufen, falls $m \equiv 3 \pmod 8$ ist, $\psi_1$, $\psi_2$, $\psi_3$ zusammen ein vollständiges Repräsentantensystem von Classen erster Art. Ist dagegen $m \equiv 7 \pmod 8$, so durchläuft $\psi_2$ ein vollständiges Repräsentantensystem der Classen erster Art, $\psi_1$ und $\psi_3$ je ein vollständiges Repräsentantensystem der Classen zweiter Art [§. 108, 8.].

Daraus aber folgt nach (5):

(8) $$\begin{aligned}
\left(1 + \frac{2}{4^s}\right) \sum^{\psi'} S' &= \sum^{\psi} S, \quad m \equiv 3 \pmod 8, \\
\left(1 + \frac{2}{4^s} - \frac{2}{2^s}\right) \sum^{\psi'} S' &= \sum^{\psi} S, \quad m \equiv 7 \pmod 8.
\end{aligned}$$

Die Summation der Formel (30) des vorigen Paragraphen über ein vollständiges Repräsentantensystem $\psi$ ergiebt nun:

$$\operatorname*{Lim}_{s=1} \left( \sum^{\psi} S - \frac{\varepsilon}{2^s} \sum^{\psi'} S' \right) = \frac{4\,\pi}{\sqrt{m}}\, log\, \Pi \frac{f(\omega)}{\sqrt[4]{2}},$$

worin $\varepsilon = 3$ oder $1$ ist, je nachdem $m \equiv 3$ oder $\equiv 7 \pmod 8$, und daraus auf Grund von (8):

$$\text{(9)}\quad \begin{aligned} &\operatorname*{Lim}_{s=1}(4^s + 2 - 3.2^s)\overset{\psi}{\Sigma} S = \frac{24\pi}{\sqrt{m}}\, log\, \Pi\, \frac{f(\omega)}{\sqrt[4]{2}}, \quad m \equiv 3 \pmod 8, \\ &\operatorname*{Lim}_{s=1}(4^s + 2 - 3.2^s)\overset{\psi}{\Sigma} S = \frac{8\pi}{\sqrt{m}}\, log\, \Pi\, \frac{f(\omega)}{\sqrt[4]{2}}, \quad m \equiv 7 \pmod 8. \end{aligned}$$

Es ist aber [§. 113, (31)]:

$$\operatorname{Lim}(s-1)\overset{\psi}{\Sigma} S = \frac{\pi h}{\sqrt{m}}, \quad \operatorname{Lim}\frac{4^s + 2 - 3.2^s}{s-1} = 2\, log\, 2,$$

also:

$$\text{(10)}\quad \begin{aligned} &log\, \Pi\, \frac{f(\omega)}{\sqrt[3]{2}} = 0, \quad m \equiv 3 \pmod 8, \\ &log\, \Pi\, \frac{f(\omega)}{\sqrt{2}} = 0, \quad m \equiv 7 \pmod 8. \end{aligned}$$

Die erste dieser Formeln giebt das bereits auf andere Weise abgeleitete Resultat; die zweite giebt das neue:

$$\text{(11)}\qquad \tau = \frac{1}{2}, \quad m \equiv 7 \pmod 8.$$

4. Es bleibt noch übrig die Bestimmung von $\tau$ in dem Falle, wo $m$ durch eine höhere Potenz von 2 theilbar ist. Um auch noch diese Bestimmung auszuführen, sei

$$\text{(12)}\qquad m = 4m',$$

und es durchlaufen $\omega'$ und $\omega$ ein zu den Determinanten $-m'$ und $-m$ gehöriges vollständiges Wurzelsystem.

Nach §. 90 gehören aber die beiden Werthe

$$2\omega' \quad \text{und} \quad \frac{\omega'}{2}$$

zur Determinante $-m$ und sind die Wurzeln der Formen

$$\text{(13)}\qquad (A,\ 2B,\ 4C), \quad (4A,\ 2B,\ C),$$

wenn $\omega'$ die Wurzel der Form $(A,\ B,\ C)$ ist, worin $A$ und $C$ ungerade angenommen sind (§. 93). Da in den beiden Formen (13) der letzte und der erste Coëfficient gerade sind, so ist für $f(\omega)$ zu setzen:

$$f_1(2\omega'), \quad f_2\left(\frac{\omega'}{2}\right)$$

und da (§. 29):

$$f_1(2\omega') = \frac{\sqrt{2}}{f_2(\omega')},$$

$$f_2\left(\frac{\omega'}{2}\right) = \frac{\sqrt{2}}{f_1(\omega')},$$

$$f_1(\omega')f_2(\omega')f(\omega') = \sqrt{2},$$

so folgt, wenn $h'$ die zur Determinante $-m'$ gehörige Classenzahl ist:

$$\Pi f(\omega) = \Pi f_1(2\omega')f_2\left(\frac{\omega'}{2}\right) = \frac{2^h}{\Pi f_1(\omega')f_2(\omega')} = \sqrt{2}^{h'}\,\Pi f(\omega').$$

Es ist aber die Classenzahl für die Determinante $-m$ (§. 90):

$$h = 2h',$$

so dass sich ergiebt, wenn

$$\Pi f(\omega') = 2^{h'\tau'}, \quad \Pi f(\omega) = 2^{h\tau}$$

gesetzt ist:

$$\tau = \frac{\tau'}{2} + \frac{1}{4}, \tag{14}$$

eine Formel, die auch noch für $m' = 1$ gilt, wo $h' = h$ und die beiden Werthe $2\omega'$ und $\omega' : 2$ äquivalent sind.

Durch wiederholte Anwendung dieser Formel ergiebt sich, wenn

$$m = 4^\lambda m'$$

ist, für ein beliebiges positives $\lambda$:

$$\tau = \frac{\tau'}{2^\lambda} + \frac{1}{2} - \frac{1}{2^{\lambda+1}}.$$

Fassen wir das hiermit Bewiesene zusammen, so können wir sagen, dass folgende Grössen **algebraische Einheiten** sind:

$$\frac{f(\omega)}{\sqrt[4]{2}}, \quad m \equiv 1, 2 \pmod 4,$$

$$\frac{f(\omega)}{\sqrt[3]{2}}, \quad m \equiv 3, \quad \pmod 8,$$

$$\frac{f(\omega)}{\sqrt{2}}, \quad m \equiv 7, \quad \pmod 8,$$

$$\frac{f(\omega)}{2^{\frac{1}{2} - \frac{1}{2^{\lambda+2}}}}, \quad m = 4^\lambda m', \quad m' \equiv 1, 2 \pmod 4,$$

$$\frac{f(\omega)}{2^{\frac{1}{2} - \frac{1}{3.2^{\lambda+1}}}}, \quad m = 4^\lambda m', \quad m' \equiv 3 \pmod 8,$$

$$\frac{f(\omega)}{\sqrt{2}}, \quad m = 4^\lambda m', \quad m' \equiv 7 \pmod 8.$$

## §. 115. Partialnormen von $f(\omega)$.

Wir machen von der Grenzformel des §. 113 noch eine Anwendung auf die Bestimmung des Productes:

$$\Pi f(\omega),$$

welches sich nur über die Wurzeln $\omega$ der Formenclassen eines Geschlechtes erstreckt. Wir beschränken uns dabei aber auf die Annahme, dass $m$ keinen quadratischen Theiler habe, und dass $m \equiv 1$ oder $\equiv 2 \pmod 4$ sei.

Wir bezeichnen mit $C_\psi$ einen der Charaktere der durch $\psi$ repräsentirten Formenclasse und bilden nach §. 113, (30) die Gleichung:

$$(1) \qquad \lim_{s=1} \sum^{\psi} C_\psi \left( \sum^{x,y} \frac{1}{\psi^s} - \sum^{x,y} \frac{1}{\psi'^s} \right) = \frac{4\pi}{\sqrt{m}} \sum^{\psi} C_\psi \log \frac{f(\omega)}{\sqrt[4]{2}},$$

worin sich die Summen auf sämmtliche Formenclassen der Determinante $-m$ erstrecken, und auf der rechten Seite davon Gebrauch gemacht ist, dass entgegengesetzte Classen dieselben Charaktere haben.

Ist der erste Coëfficient $A$ von $\psi$ relativ prim zu $2m$, so kann man (§. 105) immer einen ungeraden Divisor $m''$ von $m$ so bestimmen, dass

$$C_\psi = \left(\frac{A}{m''}\right),$$

und da $\psi'$ aus $\psi$ und $\psi_0$ [§. 113, (32), (33)] zusammengesetzt ist:

$$C_{\psi'} = \left(\frac{2}{m''}\right)\left(\frac{A}{m''}\right) = \left(\frac{2}{m''}\right) C_\psi.$$

Danach ergiebt die Formel (1):

$$(2) \qquad \begin{aligned} \left(\frac{2}{m''}\right) = +1 &: \frac{2\pi}{\sqrt{m}} \sum^{\psi} C_\psi \log \frac{f(\omega)}{\sqrt[4]{2}} = 0, \\ \left(\frac{2}{m''}\right) = -1 &: \frac{2\pi}{\sqrt{m}} \sum^{\psi} C_\psi \log \frac{f(\omega)}{\sqrt[4]{2}} = \lim_{s=1} \sum^{\psi} \left(\frac{A}{m''}\right) \sum^{x,y} \frac{1}{\psi^s}, \end{aligned}$$

und es kommt darauf an, unter der Voraussetzung, dass $m'' \equiv 3$ oder $\equiv 5 \pmod 8$ ist, den Grenzwerth rechts zu bestimmen.

Dazu müssen wir die Summen zunächst so umformen, dass $\psi$ nur noch solche Werthe annimmt, die zu $2m$ theilerfremd sind. Um diesen Zweck zu erreichen, verstehen wir unter $r$ eine in $2m$ aufgehende Primzahl, und nehmen, da wir $\psi = (A, B, C)$ durch jede äquivalente Form ersetzen dürfen, $A$ durch $r$ nicht theilbar, dagegen $B \equiv m \pmod{r}$ und folglich $C$ durch $r$, aber nicht durch $r^2$ theilbar an. $\psi(x, y)$ ist also dann und nur dann durch $r$ theilbar, wenn $x$ durch $r$ theilbar ist. Deuten wir durch $\Sigma^{(r)} \psi^{-s}$ an, dass $\psi$ alle und nur solche Werthe annimmt, welche durch $r$ nicht theilbar sind, so ergiebt sich hieraus:

$$\Sigma \frac{1}{\psi^s} = \Sigma^{(r)} \frac{1}{\psi^s} + \frac{1}{r^s} \Sigma \frac{1}{\psi'^s}, \tag{3}$$

wenn

$$\psi' = A r x^2 + 2 B x y + \frac{C}{r} y^2. \tag{4}$$

Es ist also $\psi'$ ebenfalls von der Determinante $-m$ und entsteht durch Composition von $\psi$ mit

$$\left(r,\ 0,\ \frac{m}{r}\right) \tag{5}$$

oder, wenn $r = 2$ und $m$ ungerade ist, mit

$$\left(2,\ 1,\ \frac{m+1}{2}\right) \tag{6}$$

und durchläuft daher gleichzeitig mit $\psi$ ein vollständiges Repräsentantensystem der Determinante $-m$.

Bezeichnen wir daher mit $\varepsilon$ den Charakter $C_\psi$ für die Form (5) oder (6), also, $m = m' m''$ gesetzt,

$$\varepsilon = \left(\frac{r}{m''}\right) = \left(\frac{\pm m''}{r}\right), \text{ wenn } r \text{ in } m' \text{ aufgeht,}$$

$$\varepsilon = \left(\frac{r}{m'' r^{-1}}\right) \left(\frac{m' m'' r^{-1}}{r}\right) = \left(\frac{\mp m'}{r}\right),$$

(7) wenn $r$ in $m''$ aufgeht, und das obere oder das untere Zeichen gilt, je nachdem $m'' \equiv 5$ oder $\equiv 3 \pmod{8}$ (nach dem Reciprocitätsgesetz der quadratischen Reste),

$\varepsilon = -1$, wenn $r = 2$,

so ergiebt sich aus (3):

$$\sum^{\psi} C_\psi \Sigma \frac{1}{\psi^s} = \sum^{\psi} C_\psi \Sigma^{(r)} \frac{1}{\psi^s} + \frac{\varepsilon}{r^s} \sum^{\psi} C_\psi \Sigma \frac{1}{\psi^s},$$

da die Gesammtheit der $\psi'$ mit der der $\psi$ übereinstimmt. Es wird daher:

$$\sum^{\psi} C_\psi \Sigma \frac{1}{\psi^s} = \frac{\sum^{\psi} C_\psi \Sigma^{(r)} \psi^{-s}}{1 - \varepsilon r^{-s}}. \tag{8}$$

Dieselbe Betrachtung ist auch anwendbar, wenn in $\Sigma\,\psi^{-s}$ bereits die Theilbarkeit von $\psi$ durch einige Primzahlen ausgeschlossen ist, und wenn man daher das in (8) ausgedrückte Verfahren nach und nach auf alle in $2\,m$ aufgehenden Primzahlen anwendet und durch $\Sigma^{(0)}\,\psi^{-s}$ andeutet, dass $\psi$ nur solche Werthe annehmen soll, die relativ prim zu $2\,m$ sind, so folgt:

$$(9)\qquad \overset{r}{\Pi}\,(1 - \varepsilon\, r^{-s})\,\overset{\psi}{\Sigma}\, C_\psi\, \Sigma\,\frac{1}{\psi^s} = \Sigma\, C_\psi\, \Sigma^{(0)}\,\frac{1}{\psi^s}.$$

Nach einer Formel von Dirichlet, die wir hier nur anführen[1], ist aber:

$$(10)\qquad \Sigma\, C_\psi\, \Sigma^{(0)}\,\frac{1}{\psi^s} = 2\,\overset{n}{\Sigma}\left(\frac{n}{m''}\right)\frac{1}{n^s}\,\overset{n}{\Sigma}\left(\frac{-m}{n}\right)\left(\frac{n}{m''}\right)\frac{1}{n^s},$$

worin $n$ die Reihe der positiven Zahlen durchläuft, die relativ prim zu $2\,m$ sind.

Die beiden Summen auf der rechten Seite dieser Gleichung lassen sich auf Grund des Reciprocitätsgesetzes der quadratischen Reste in folgende Form setzen, worin wie vorhin die oberen Zeichen gelten, wenn $m'' \equiv 5 \pmod 8$, die unteren, wenn $m'' \equiv 3 \pmod 8$:

$$(11)\qquad \Sigma\left(\frac{\pm\, m''}{n}\right)\frac{1}{n^s},\qquad \Sigma\left(\frac{\mp\, m'}{n}\right)\frac{1}{n^s}.$$

In diesen beiden Summen durchläuft $n$ die Reihe der positiven Zahlen, welche relativ prim zu $2\,m$ sind. Wir wollen nun mit $r'$, $r''$ die ungeraden Primzahlen bezeichnen, welche in $m'$, $m''$ aufgehen, und in der ersten und zweiten der beiden Summen (11) noch diejenigen Glieder beifügen, in welchen $n$ resp. durch $r'$ oder $r''$ theilbar ist. Bezeichnen wir die so verstandenen Summen durch $\Sigma^{(0)}$, so erhalten wir auf ähnlichem Wege, wie wir die Formel (8) gewonnen haben:

$$(12)\qquad \begin{aligned} \Sigma\left(\frac{\pm\, m''}{n}\right)\frac{1}{n^s} &= \overset{r'}{\Pi}\left[1 - \left(\frac{\pm\, m''}{r'}\right)\frac{1}{r'^s}\right]\Sigma^{(0)}\left(\frac{\pm\, m''}{n}\right)\frac{1}{n^s},\\ \Sigma\left(\frac{\mp\, m'}{n}\right)\frac{1}{n^s} &= \overset{r''}{\Pi}\left[1 - \left(\frac{\mp\, m'}{r''}\right)\frac{1}{r''^s}\right)\Sigma^{(0)}\left(\frac{\mp\, m'}{n}\right)\frac{1}{n^s}, \end{aligned}$$

also nach (9) und (10):

$$(13)\qquad \left(1 + \frac{1}{2^s}\right)\Sigma\, C_\psi\, \Sigma\,\frac{1}{\psi^s} = 2\,\Sigma^{(0)}\left(\frac{\pm\, m''}{n}\right)\frac{1}{n^s}\,\Sigma^{(0)}\left(\frac{\mp\, m'}{n}\right)\frac{1}{n^s},$$

---

[1] Dirichlet-Dedekind, Zahlentheorie, §. 125, S. 325.

und in der ersten und zweiten Summe der rechten Seite durchläuft $n$ die Reihe der positiven Zahlen, die relativ prim zu $2m''$, $2m'$ sind.

Die Grenzwerthe dieser Summen für $s = 1$ lassen sich aber finden durch die Dirichlet'schen Formeln für die Classenzahlen [1]. Danach ist, wenn wir mit $K(-D)$ die Anzahl der Classen der Determinante $D$ bezeichnen, mit der Bestimmung, dass $K(1) = \frac{1}{2}$ sei:

$$\begin{aligned} \operatorname*{Lim}_{s=1} \Sigma^{(0)}\left(\frac{\pm m''}{n}\right)\frac{1}{n^s} &= \frac{K(-m'')}{2\sqrt{m''}}\, log\left(T + U\sqrt{m''}\right) & m'' &\equiv 5 \pmod{8}, \\ &= \frac{\pi K(m'')}{2\sqrt{m''}} & m'' &\equiv 3 \pmod{8}, \\ \operatorname*{Lim}_{s=1} \Sigma^{(0)}\left(\frac{\mp m'}{n}\right)\frac{1}{n^s} &= \frac{\pi K(m')}{2\sqrt{m'}} & m'' &\equiv 5 \pmod{8}, \\ &= \frac{K(-m')}{2\sqrt{m'}}\, log\left(T + U\sqrt{m'}\right) & m'' &\equiv 3 \pmod{8}, \end{aligned}$$

worin $T$, $U$ die kleinsten positiven Lösungen der Pell'schen Gleichung

$$T^2 - m''U^2 = 1 \quad \text{oder} \quad T^2 - m'U^2 = 1$$

bedeuten. Hiernach erhält man aus (2):

$$\begin{aligned} (14)\quad 6\overset{w}{\Sigma}\left(\frac{A}{m''}\right) log\frac{f(\omega)}{\sqrt[4]{2}} &= 0, & m'' &\equiv \pm 1 \\ &= K(m')\,K(-m'')\, log\left(T + U\sqrt{m''}\right), & m'' &\equiv 5 \pmod{8} \\ &= K(-m')\,K(m'')\, log\left(T + U\sqrt{m'}\right), & m'' &\equiv 3. \end{aligned}$$

Wenn man diese Formeln für alle ungeraden Factoren $m''$ von $m$, d. h. für alle Charaktere bildet, und die erhaltenen Resultate addirt, so erhält man, da die Summe aller Charaktere für ein und dieselbe Form immer dann verschwindet, wenn die Form nicht dem Hauptgeschlecht angehört, auf der linken Seite

$$6\, g\, log \frac{f(\omega)}{\sqrt[4]{2}}\,\frac{f(\omega')}{\sqrt[4]{2}} \cdots$$

wenn $g$ die Anzahl der Geschlechter, also eine Potenz von 2, deren Exponent gleich der Anzahl der in $m$ aufgehenden unge-

---

[1] Dirichlet-Dedekind, §§. 96, 99.

raden Primzahlen, und $\omega, \omega', \ldots$ die Wurzeln der Formen des Hauptgeschlechtes sind.

Um das Product der Classeninvarianten für ein anderes als das Hauptgeschlecht zu bilden, hat man die Formel (14) vor der Summation mit $\left(\frac{A_0}{m''}\right)$ zu multipliciren, wenn $A_0$ eine beliebige, zu $2m$ theilerfremde und durch eine Form des betreffenden Geschlechtes darstellbare Zahl bedeutet, oder man hat in denjenigen der Formeln (14) das Zeichen der Quadratwurzel, $\sqrt{m''}$, $\sqrt{m'}$ zu ändern, für welche $\left(\frac{A_0}{m''}\right) = -1$ ist.

Die Anwendung der Formel (14) verlangt die Kenntniss der Classenzahlen positiver und negativer Determinanten und der Zahlen $T$, $U$. Die Classenzahlen sind in weitem Umfange von Gauss berechnet und aus seinem Nachlass im zweiten Bande der Werke, Ste 450 bis 476 veröffentlicht. Für die Lösungen $T$, $U$ der Pell'schen Gleichung enthält Legendre's „Theorie des nombres" eine Tabelle.

Es existiren 63 negative Determinanten von der Eigenschaft, dass in jedem Geschlecht nur eine Classe enthalten ist; dass es nicht mehr giebt, selbst dass die Zahl nur eine endliche ist, kann freilich bis jetzt nur durch Induction geschlossen, nicht bewiesen werden [1]). Die Mehrzahl dieser Determinanten ist $\equiv -1, -2$ (mod 4) und ohne quadratischen Theiler oder $\equiv 8$ (mod 16).

Für die ersteren lassen sich die Classeninvarianten nach der Formel (14) vollständig berechnen, und eine ähnliche Formel, auf deren Bildung wir hier nicht eingehen wollen, führt auch für die durch 8 theilbaren Determinanten zum Ziel.

Für die vereinzelten Determinanten dieser Art, die hierher nicht passen, lassen sich die Classeninvarianten $f(\omega)$ nach einer der anderen Methoden berechnen [2]).

Um an einem einfachen, leicht zu übersehenden Beispiele die Rechnung durchzuführen, wählen wir $m = 105 = 3.\ 5.\ 7.$ Wenn wir die Werthe von $m''$, die $\equiv \pm 1$ (mod 8) sind, weglassen, da diese in der Summe der Formeln (14) keinen Beitrag geben, so haben wir:

---

[1]) Euler, Nouv. Mém. de l'Ac. de Berlin 1876, p. 338. Gauss, Disq. ar. art. 303.

[2]) Vgl. des Verfassers Abhandlung: „Zur complexen Multiplication elliptischer Functionen". Mathematische Annalen, Bd. 23.

$$m'' = 3,\quad 5,\quad 21,\quad 35,$$
$$m' = 35,\quad 21,\quad 5,\quad 3$$

zu setzen und erhalten, da $g = 8$ ist:

$$\begin{aligned}48\, log \frac{f(\sqrt{-105})}{\sqrt[4]{2}} &= K(21)\, K(-5)\ \ log\, (T + U\sqrt{5}),\\ &+ K(5)\ \ K(-21)\, log\, (T + U\sqrt{21}),\\ &+ K(3)\ \ K(-35)\, log\, (T + U\sqrt{35}),\\ &+ K(35)\, K(-3)\ \ log\, (T + U\sqrt{3}).\end{aligned}$$

Es ist aber

$$K(+5) = 2,\quad K(+21) = 4,\quad K(+35) = 6,\quad K(+3) = 1,$$
$$K(-5) = 1,\quad K(-21) = 2,\quad K(-35) = 4,\quad K(-3) = 2,$$

wie man aus den Gauss'schen Tafeln oder hier auch leicht durch directe Abzählung findet.

Ferner ist nach den Legendre'schen Tafeln:

$$\begin{aligned}T + U\sqrt{5} &= (2 + \sqrt{5})^2,\\ T + U\sqrt{21} &= 55 + 12\sqrt{21} = (3\sqrt{3} + 2\sqrt{7})^2 = \left(\frac{\sqrt{3}+\sqrt{7}}{2}\right)^6,\\ T + U\sqrt{35} &= 6 + \sqrt{35} \quad = \frac{1}{2}(\sqrt{5}+\sqrt{7})^2,\\ T + U\sqrt{3} &= 2 + \sqrt{3} \quad = \frac{1}{2}(1+\sqrt{3})^2,\end{aligned}$$

also

$$\left(\frac{f(\sqrt{-105})}{\sqrt[4]{2}}\right)^{12} = (2+\sqrt{5})^2\, (3\sqrt{3}+2\sqrt{7})^2\, (6+\sqrt{35})\, (2+\sqrt{3})^3.$$

## §. 116. Berechnung einiger weiterer Classeninvarianten.

Nächst denjenigen Determinanten, bei welchen in jedem Geschlecht nur eine Formenclasse vorkommt, die wir im vorhergehenden Paragraphen betrachtet haben, geben die einfachsten Resultate die, welche in jedem Geschlecht zwei Formenclassen enthalten, und unter diesen wieder die, bei welchen nur zwei Geschlechter vorkommen. Die Classeninvarianten für diese Determinanten $-m$ sind die Wurzeln quadratischer Gleichungen, deren Coëfficienten nur eine Quadratwurzel enthalten. Wir betrachten hier diejenigen unter diesen Werthen von $m$, welche $\equiv 1$ oder

$\equiv 2 \pmod 4$ sind, die nach der Gauss'schen Tafel die folgenden sind:

$$m = 14,\ 34,\ 46,\ 82,\ 142 \equiv \pm 2 \pmod{16},$$
$$m = 17,\ 49,\ 73,\ 97,\ 193 \equiv 1 \pmod 8.$$

Die Formenclassen des Hauptgeschlechts können in diesen Fällen repräsentirt werden für ein gerades $m$ durch

$$(1) \qquad (1,\ 0,\ m),\quad \left(2,\ 0,\ \frac{m}{2}\right),$$

für ein ungerades $m$ durch

$$(2) \qquad (1,\ 0,\ m),\quad \left(2,\ 1,\ \frac{m+1}{2}\right),$$

von denen die letztere äquivalent ist mit

$$(3) \qquad \left(\frac{m+1}{2},\ \frac{m-1}{2},\ \frac{m+1}{2}\right).$$

Für die Formen (1) sind nach §. 94, VII. die Classeninvarianten

$$\frac{f_1(\sqrt{-m})^2}{\sqrt{2}} \quad \text{und} \quad \frac{1}{\sqrt{2}} f_2\left(\frac{\sqrt{-m}}{2}\right)^2 = \frac{\sqrt{2}}{f_1(\sqrt{-m})^2} \quad (\S.\ 29)$$

und für die Formen (2), (3) (§. 94, IV.)

$$\frac{f(\sqrt{-m})^2}{\sqrt{2}} \quad \text{und} \quad \frac{1}{\sqrt{2}} f\left(\frac{1+\sqrt{-m}}{1-\sqrt{-m}}\right)^2 = \frac{\sqrt{2}}{f(\sqrt{-m})^2},$$

und nach §. 114 sind dies ganze algebraische Zahlen.

Setzen wir also, entsprechend den beiden Fällen:

$$(4) \qquad \sqrt{2}\, x = f_1(\sqrt{-m})^2,\quad f(\sqrt{-m})^2,$$

so ist

$$x + \frac{1}{x}$$

eine ganze algebraische Zahl, welche nur eine Quadratwurzel enthält, und aus §. 106 erhalten wir Aufschluss, welche Quadratwurzel darin vorkommt.

Es ist $\sqrt{2}$, wenn $m \equiv 6 \pmod 8$ ist, also für $m = 14,\ 46,\ 142$, $\sqrt{\frac{m}{2}}$, wenn $m \equiv 2 \pmod 8$ ist, also für $m = 34,\ 82$, ferner $\sqrt{m}$ im Fall eines ungeraden $m$ (mit Ausnahme von $m = 49$, wo $\sqrt{7}$ an die Stelle tritt).

Setzen wir also

$$x + \frac{1}{x} = a + b\sqrt{p}, \tag{5}$$

so sind $a$, $b$ rationale Zahlen, welche höchstens den Nenner 2 haben. Es müssen aber auch $a$ und $b$ positiv sein. Denn ändern wir in (5) das Vorzeichen von $\sqrt{p}$, so entsteht eine andere quadratische Gleichung, deren Wurzeln die zum zweiten Geschlecht gehörigen Classeninvarianten sind, und die daher conjugirt imaginär sind, während die Wurzeln von (5) reell sind. Daraus ergiebt sich die Grössenbestimmung:

$$(a + b\sqrt{p})^2 > 4 > (a - b\sqrt{p})^2,$$

also müssen $a$ und $b$ gleiches Zeichen haben. Da aber $x$ nach (4) positiv ist, so müssen $a$ und $b$ beide positiv sein.

Um $a$ und $b$ wirklich zu finden, braucht man nur den Ausdruck auf der linken Seite von (5) nach (4) auf wenige Decimalen zu berechnen, wobei es weitaus hinreichend ist,

$$f(\sqrt{-m}) = f_1(\sqrt{-m}) = e^{\frac{\pi\sqrt{m}}{24}}$$

zu setzen, und die so gefundenen Decimalen mit den Decimalen von $\sqrt{p}$ zu vergleichen, um alsbald $b$ und sodann $a$ zu erhalten. Die Rechnung ist überaus einfach und giebt folgende Resultate:

$$m = 14, \quad x + \frac{1}{x} = 1 + \sqrt{2},$$

$$m = 17, \quad x + \frac{1}{x} = \frac{1 + \sqrt{17}}{2},$$

$$m = 34, \quad x + \frac{1}{x} = \frac{3 + \sqrt{17}}{2},$$

$$m = 46, \quad x + \frac{1}{x} = 3 + \sqrt{2},$$

$$m = 49, \quad x + \frac{1}{x} = 2 + \sqrt{7},$$

$$m = 73, \quad x + \frac{1}{x} = \frac{5 + \sqrt{73}}{2},$$

$$m = 82, \quad x + \frac{1}{x} = \frac{15 + \sqrt{41}}{2},$$

$$m = 97, \quad x + \frac{1}{x} = \frac{9 + \sqrt{97}}{2},$$

$$m = 142, \quad x + \frac{1}{x} = 9 + 5\sqrt{2},$$

$$m = 193, \quad x + \frac{1}{x} = 13 + \sqrt{193}\ ^{1)}.$$

---

1) In meiner Abhandlung „Zur Theorie der complexen Multiplication elliptischer Functionen“. Mathematische Annalen, Bd. 33, S. 390 ist die letzte Formel nach einer brieflichen Mittheilung von Greenhill unrichtig angegeben.

## Sechszehnter Abschnitt.

# Theilung der elliptischen Functionen mit singulären Moduln.

### §. 117. Die complexe Multiplication der elliptischen Functionen.

Wir kehren zu unserem Ausgangspunkte im §. 86 zurück, um zu untersuchen, in welcher Weise sich die complexe Multiplication der elliptischen Functionen gestaltet, wenn der Modul dieser Functionen einen der singulären Werthe erhält.

Wenn $\omega$, wie im §. 86, einer ganzzahligen quadratischen Gleichung mit negativer Discriminante genügt:

$$A\omega^2 + B\omega + C = 0, \tag{1}$$

worin $A$ positiv, $A$, $B$, $C$ ohne gemeinsame Theiler, und

$$-\varDelta = B^2 - 4AC = -m \quad \text{oder} \quad -4m \tag{2}$$

gesetzt ist, je nachdem $B$ ungerade oder gerade ist, so nehmen wir zwei beliebige ganze Zahlen $x$, $y$, welche nur an die Bedingung (18), §. 86, d. h. daran gebunden sind, dass

$$\mu = \frac{y - ix\sqrt{\varDelta}}{2}, \quad \mu' = \frac{y + ix\sqrt{\varDelta}}{2} \tag{3}$$

ganze algebraische Zahlen sind, und setzen

$$Ax = b, \quad Bx = a - \partial, \quad Cx = -c, \quad y = a + \partial, \tag{4}$$

$$a\partial - bc = n, \quad y^2 + \varDelta x^2 = 4n, \tag{5}$$

$$a + b\omega = \mu', \quad \mu\mu' = n.$$

Dadurch nimmt die Gleichung (1) die Gestalt an:

$$\omega(a + b\omega) = c + \partial\omega, \tag{6}$$

und wenn wir, um dies auf die elliptischen Functionen anzuwenden,

$$\omega = \frac{iK'}{K}$$

setzen, so folgt:

$$\begin{aligned} aK + biK' &= \mu' K, \\ cK + \partial iK' &= \mu' iK', \end{aligned} \tag{7}$$

und durch Auflösung:

$$\begin{aligned} \mu K &= \partial K - biK', \\ \mu iK' &= -cK + aiK'. \end{aligned} \tag{8}$$

Hiernach können wir [§. 39, (21), (22)] gerade Functionen der Variablen $v$ bilden, welche die Perioden $2K$ und $2iK'$ besitzen, nämlich:

$$\begin{array}{lll} 1. & \dfrac{\operatorname{sn} \mu v}{\mu \operatorname{sn} v}, & \partial \equiv 1, \quad c \equiv 0 \pmod{2}, \\[2ex] 2. & \dfrac{\operatorname{sn} \mu v \operatorname{cn} v}{\mu \operatorname{sn} v}, & \partial \equiv 0, \quad c \equiv 1 \pmod{2}, \\[2ex] 3. & \dfrac{\operatorname{sn} \mu v \operatorname{dn} v}{\mu \operatorname{sn} v}, & \partial \equiv 1, \quad c \equiv 1 \pmod{2}, \\[2ex] 4. & \dfrac{\operatorname{sn} \mu v \operatorname{cn} v \operatorname{dn} v}{\mu \operatorname{sn} v}, & \partial \equiv 0, \quad c \equiv 0 \pmod{2}, \end{array} \tag{9}$$

wenn wir dem Modul $\varkappa$ den der Gleichung (1) entsprechenden, nach §. 37, (3) berechneten singulären Werth beilegen.

In ähnlicher Weise lassen sich die Functionen $\operatorname{cn} \mu v$, $\operatorname{dn} \mu v$ verwenden.

Die Functionen (9) lassen sich nach §. 39 rational durch $\operatorname{sn}^2 v$ ausdrücken. Setzen wir also zur Abkürzung $s = \operatorname{sn} v$ und bezeichnen mit $A(s^2)$, $D(s^2)$ ganze rationale Functionen von $s^2$, so erhalten wir in den vier Fällen (9):

$$\begin{aligned} \operatorname{sn} \mu v &= \frac{\mu \operatorname{sn} v\, A(s^2)}{D(s^2)}, & \partial \equiv 1, \quad c \equiv 0 \pmod{2}, \\ &= \frac{\mu \operatorname{sn} v\, A(s^2)}{\operatorname{cn} v\, D(s^2)}, & \partial \equiv 0, \quad c \equiv 1 \pmod{2}, \\ &= \frac{\mu \operatorname{sn} v\, A(s^2)}{\operatorname{dn} v\, D(s^2)}, & \partial \equiv 1, \quad c \equiv 1 \pmod{2}, \\ &= \frac{\mu \operatorname{sn} v\, A(s^2)}{\operatorname{cn} v \operatorname{dn} v\, D(s^2)}, & \partial \equiv 0, \quad c \equiv 0 \pmod{2}. \end{aligned} \tag{10}$$

Die Functionen $A(s^2)$, $D(s^2)$ können, wenn mit $A_1$, $A_2$ . . ., $D_1$, $D_2$ . . . von $v$ unabhängige Coëfficienten bezeichnet werden, in der Weise geschrieben werden:

$$(11) \qquad \begin{aligned} A(s^2) &= 1 + A_1 s^2 + A_2 s^4 + \cdots \\ D(s^2) &= 1 + D_1 s^2 + D_2 s^4 + \cdots \end{aligned}$$

Da $\varkappa^2$ eine algebraische Zahl ist, so sind die Coëfficienten der Functionen $A(s^2)$, $D(s^2)$, die sich aus den Wurzeln der Theilungsgleichung (§. 64) zusammensetzen lassen, sicher algebraische Zahlen. Denkt man sich nun in (10) die Brüche fürs Erste dahin erweitert, dass $D(s^2)$ rationale Coëfficienten erhält, was dadurch geschieht, dass man im Zähler und Nenner mit dem Product aller zu $D(s^2)$ conjugirten Ausdrücke multiplicirt, so kann man die Coëfficienten von $A(s^2)$ durch Entwickelung nach Potenzen von $v$ bestimmen. Wenn man nämlich den betreffenden Ausdruck

$$\frac{\operatorname{sn}\mu v\, D(s^2)}{\mu \operatorname{sn} v}, \quad \frac{\operatorname{sn}\mu v \operatorname{cn} v\, D(s^2)}{\mu \operatorname{sn} v}, \quad \frac{\operatorname{sn}\mu v \operatorname{dn} v\, D(s^2)}{\mu \operatorname{sn} v},$$

$$\frac{\operatorname{sn}\mu v \operatorname{cn} v \operatorname{dn} v\, D(s^2)}{\mu \operatorname{sn} v}$$

nach dem Taylor'schen Lehrsatz entwickelt, so erhält man eine nach Potenzen von $v^2$ fortschreitende Reihe, deren Coëfficienten ganze rationale Functionen von $\varkappa^2$ sind, und die ausserdem nur rationale Zahlen und $\sqrt{-m}$ enthalten.

Wenn wir nun die rechte Seite $A(s^2)$ in gleicher Weise nach Potenzen von $v^2$ entwickeln, so tritt $A_\nu$ zuerst in dem Coëfficienten von $v^{2\nu}$, und zwar mit dem Factor 1 behaftet, auf, so dass also die Coëfficienten $A_\nu$ auf diese Weise alle rational berechnet werden können, und sie gehören alle zu dem Rationalitätsbereiche:

$$\mathfrak{R}\left(\varkappa^2, \sqrt{-m}\right).$$

Nach §. 93 und §. 102 ist dieser Rationalitätsbereich der Classenkörper der Determinante $-4m$ oder $-m$, je nachdem die Gleichung (1) zur ersten oder zweiten Art gehört, oder, wie wir nach (2) auch sagen können, der Classenkörper der Determinante $-\Delta$.

Wenn man also nachträglich wieder Zähler und Nenner von (10) von gemeinsamen Factoren befreit, so bekommt man einen Nenner $D$, dessen Coëfficienten gleichfalls dem Rationalitätsbereich $\mathfrak{R}\left(\varkappa^2, \sqrt{-m}\right)$ angehören.

Auf dieselbe Weise können wir schliessen, dass die Functionen:

$$\begin{array}{ll}
\dfrac{\mathrm{cn}\,\mu v}{\mathrm{cn}\, v}, & \partial + b \equiv 1, \quad a + c \equiv 1 \pmod{2}, \\[2ex]
\dfrac{\mathrm{cn}\,\mu v}{\mathrm{dn}\, v}, & \partial + b \equiv 0, \quad a + c \equiv 1 \pmod{2}, \\[2ex]
\dfrac{\mathrm{cn}\,\mu v}{\mathrm{cn}\, v\,\mathrm{dn}\, v}, & \partial + b \equiv 1, \quad a + c \equiv 0 \pmod{2}, \\[2ex]
\mathrm{cn}\,\mu v, & \partial + b \equiv 0, \quad a + c \equiv 0 \pmod{2},
\end{array} \tag{12}$$

$$\begin{array}{ll}
\dfrac{\mathrm{dn}\,\mu v}{\mathrm{dn}\, v}, & b \equiv 0, \quad a \equiv 1 \pmod{2}, \\[2ex]
\dfrac{\mathrm{dn}\,\mu v}{\mathrm{cn}\, v}, & b \equiv 1, \quad a \equiv 1 \pmod{2}, \\[2ex]
\dfrac{\mathrm{dn}\,\mu v}{\mathrm{cn}\, v\,\mathrm{dn}\, v}, & b \equiv 1, \quad a \equiv 0 \pmod{2}, \\[2ex]
\mathrm{dn}\,\mu v, & b \equiv 0, \quad a \equiv 0 \pmod{2}
\end{array} \tag{13}$$

rationale Functionen von $\mathrm{sn}^2 v$ sind, deren Coëfficienten dem Rationalitätsbereich $\mathfrak{R}\left(\varkappa^2, \sqrt{-m}\right)$ angehören.

Wir nehmen jetzt in der Gleichung (10) Zähler und Nenner ohne gemeinsamen Theiler an, und wollen unter dieser Voraussetzung die Grade von $A(s^2)$ und $D(s^2)$ bestimmen.

Dazu führt die Bestimmung der Anzahl der Werthe von $\mathrm{sn}\, v$, für welche $\mathrm{sn}\,\mu v$ verschwindet, oder die Anzahl der nach dem Modul $(2K, 2iK')$ incongruenten Werthe der Form:

$$\Omega = \frac{\xi\, 2K + \xi'\, 2iK'}{\mu}. \tag{14}$$

Diese Frage gehört in die Theorie der Moduln und lässt sich nach den allgemeinen Sätzen von Dedekind (Zahlentheorie, §. 165) sofort beantworten. Ohne diese allgemeine Theorie vorauszusetzen, können wir unsere specielle Frage leicht in folgender Weise erledigen.

Wir bezeichnen mit $e$ den grössten gemeinschaftlichen Theiler der beiden Zahlen $a$, $b$ und setzen:

$$a = a'e, \quad b = b'e, \quad n = n'e.$$

Setzen wir in (14):

$$\begin{aligned}
\xi &= 0, 1, \ldots n' - 1, \\
\xi' &= 0, 1, \ldots e - 1,
\end{aligned} \tag{15}$$

so erhalten wir $n$ Werthe, worunter nur der eine, $\xi = 0$, $\xi' = 0$, nach dem Modul $(2K, 2iK')$ mit Null congruent ist, denn aus

$$\frac{\xi\, 2K + \xi'\, 2iK'}{\mu} \equiv 0 \text{ mod } (2K, 2iK')$$

folgt nach (8), wenn $h$, $h'$ ganze Zahlen sind:

$$\begin{aligned} \xi &= h\partial - h'c, \\ \xi' &= -hb + h'a, \end{aligned}$$

also $\xi' \equiv 0 \pmod{e}$ und daher $\xi' = 0$, und wenn $\lambda$ wieder eine ganze Zahl ist, $h' = \lambda b'$, $h = \lambda a'$, also $\xi = \lambda n'$ und folglich $\xi = 0$.

Es ist ferner zu beweisen, dass jeder Werth von der Form (14), etwa:

$$\frac{\xi_0\, 2K + \xi'_0\, 2iK'}{\mu}$$

einem und nur einem der vermittelst (15) erhaltenen $n$ Werthe congruent ist, woraus dann folgt, dass diese $n$ Werthe incongruent sind. Dazu haben wir zu zeigen, dass, was auch die ganzen Zahlen $\xi_0$, $\xi'_0$ sein mögen, man die ganzen Zahlen $h$, $h'$ und die aus (15) entnommenen $\xi$, $\xi'$ stets und nur auf eine einzige Weise so bestimmen kann, dass

$$(16) \qquad \begin{aligned} \xi &= \xi_0 + h\partial - h'c, \\ \xi' &= \xi'_0 - hb + h'a. \end{aligned}$$

Es seien $\alpha$, $\beta$ irgend zwei der Bedingung

$$a'\beta - b'\alpha = 1$$

genügende ganze Zahlen; setzt man dann

$$\lambda = -b'h + a'h', \quad \nu = \beta h - \alpha h',$$

also umgekehrt:

$$h = \lambda\alpha + \nu a', \quad h' = \lambda\beta + \nu b',$$

so entspricht jedem Paar ganzer Zahlen $h$, $h'$ ein Paar ganzer Zahlen $\lambda$, $\nu$ und umgekehrt, und (16) geht über in

$$\begin{aligned} \xi &= \xi_0 + \lambda(\partial\alpha - c\beta) + \nu n', \\ \xi' &= \xi'_0 + \lambda e. \end{aligned}$$

Man kann daher — und nur auf eine einzige Weise — erst $\lambda$, dann $\nu$ so bestimmen, dass $\xi'$, $\xi$ in den Reihen (15) enthalten sind, w. z. b. w.

Damit ist also bewiesen, dass in der Form (14) $n$ und nicht mehr nach dem Modul $(2K, 2iK')$ incongruente Zahlen enthalten sind.

Die $n$ Werthe (14) zerfallen mit Ausschluss des Werthes 0 in Paare von entgegengesetzten [d. h. solchen, deren Summe nach dem Modul $(2K, 2iK')$ mit 0 congruent ist]; es fragt sich, ob ausser dem Werthe 0 noch andere einander entgegengesetzte zugleich congruent sind. Dies ist nur dann möglich, wenn

$$(17) \qquad \Omega = \frac{\xi\, 2K + \xi'\, 2iK'}{\mu}$$

$$\equiv K, \quad iK', \quad K + iK' \quad \mathrm{mod}\ (2K, 2iK'),$$

d. h. nach (8), wenn die Gleichungen bestehen:

$$2\xi = h\partial - h'c,$$
$$2\xi' = -hb + h'a,$$

worin wenigstens eine der Zahlen $h$, $h'$ ungerade ist; dann muss aber entweder $\partial$ und $b$, oder $c$ und $a$, oder $\partial + c$ und $b + a$ gerade sein, was nur unter der Voraussetzung eines geraden $n$ möglich ist; zugleich ist nur unter einer der Voraussetzungen (17) $\mathrm{cn}\,\Omega = 0$, $\mathrm{sn}\,\Omega = \infty$, $\mathrm{dn}\,\Omega = 0$.

Wenn wir also von nun an die Voraussetzung machen, dass $n$ ungerade sei, so zerfallen die $n - 1$ endlichen Werthe $\mathrm{sn}^2\,\Omega$, die nach Ausschluss des Werthes 0 übrig bleiben, in Paare einander gleicher, aber von allen übrigen verschiedener Werthe und für den Grad der Function $A(s^2)$ in (10) ergiebt sich $\frac{n-1}{2}$.

Die Function $A(s^2)$ ist weder durch $\mathrm{cn}^2 v = 1 - s^2$, noch durch $\mathrm{dn}^2 v = 1 - \varkappa^2 s^2$ theilbar, da sonst $\mathrm{sn}\,\mu K$ oder $\mathrm{sn}\,\mu(K + iK')$ verschwinden, also für einen Ausdruck $\Omega$ von der Form (17) $\mathrm{cn}\,\Omega$ oder $\mathrm{dn}\,\Omega$ verschwinden müsste.

Setzen wir $v = iK'$, also $\mathrm{sn}\,v = \infty$, so wird $\mathrm{sn}\,\mu v$ im Falle (9), 1. unendlich, und $\mathrm{sn}\,\mu v : \mathrm{sn}\,v$ bleibt endlich, im Falle (9), 2., 3. bleibt $\mathrm{sn}\,\mu v$ endlich [(9), 4. ist durch die Annahme des ungeraden $n$ ausgeschlossen].

Daraus folgt, dass die Function $D(s^2)$ ebenfalls vom Grade $\frac{n-1}{2}$ ist.

## §. 118. Theilung durch eine Primzahl, von welcher $-\varDelta$ quadratischer Rest ist.

Wir wenden uns zur Theilung der Perioden der elliptischen Functionen mit singulärem Modul, setzen dabei aber den Divisor als eine ungerade Primzahl voraus.

Wenn wir auf $\omega$ eine lineare Transformation der ersten Classe $\begin{pmatrix}1, & 0\\ 0, & 1\end{pmatrix}$ (§. 31) anwenden, so ändert sich $\varkappa^2$ nicht, und $K, K'$ gehen in gewisse lineare Verbindungen ihrer selbst über; die quadratische Gleichung (1), §. 117 geht in eine äquivalente Gleichung über. Wir beschränken daher die Allgemeinheit nicht, wenn wir annehmen, der Coëfficient $A$ sei durch beliebig gegebene ungerade Primzahlen nicht theilbar.

Es sei nun $p$ eine ungerade Primzahl, von welcher $-\varDelta$ quadratischer Rest ist (ohne den Fall auszuschliessen, dass $p$ in $\varDelta$ aufgeht), so hat die Congruenz:

$$\beta^2 + \varDelta \equiv 0 \pmod{p} \tag{1}$$

zwei Lösungen, oder wenn $p$ in $\varDelta$ aufgeht, nur eine [nämlich $\beta \equiv 0 \pmod{p}$].

Nehmen wir in den Formeln (4), (5) des vorigen Paragraphen $x$, $y$ so an, dass

$$y \equiv \beta x \pmod{p} \tag{2}$$

und nehmen $x$ durch $p$ untheilbar an, so wird $n$ durch $p$ theilbar, und wir behalten noch Freiheit genug, um $n$ ungerade zu machen.

Nehmen wir $A$ durch $p$ untheilbar an, so ist auch $b$ und folglich auch $e$ [§. 117, (4), (15)] untheilbar durch $p$, und wir haben:

$$2a \equiv (B + \beta)x, \quad b \equiv Ax \pmod{p}. \tag{3}$$

Wir bezeichnen jetzt der Deutlichkeit halber die Function $A(s^2)$ des vorigen Paragraphen durch $A_\mu(s^2)$, so dass $A_\mu$ durch Vertauschung von $\beta$ mit $-\beta$ in $A_{\mu'}$ übergeht. Die Wurzeln der Gleichung für $s$:

$$A_\mu(s^2) = 0 \tag{4}$$

sind die Grössen

$$\operatorname{sn} \Omega_{\xi, \xi'} = \operatorname{sn} \frac{4K\xi + 4iK'\xi'}{\mu}, \tag{5}$$

wo $\xi, \xi'$ die Reihe der Zahlen (15), §. 117, mit Ausschluss von 0, 0 durchläuft.

(Die Ersetzung von $\xi, \xi'$ durch $2\xi$, $2\xi'$, die hier vorgenommen ist, ist bei ungeradem $n$ offenbar gestattet.)

Wir wollen nun untersuchen, welche Wurzeln die Gleichung (4) mit der Theilungsgleichung für den Divisor $p$ (§. 64):

$$A_p(s^2) = 0 \tag{6}$$

gemein hat, welche letztere in der Form enthalten sind:

$$x_{\nu\nu'} = \operatorname{sn} \frac{4K\nu + 4iK'\nu'}{p}. \tag{7}$$

Die Grössen $\Omega_{\xi,\xi'}$ können in die Form gesetzt werden [§. 117, (7)]:

$$\frac{4K\xi + 4iK'\xi'}{\mu} = \frac{(4K\xi + 4iK'\xi')\mu'}{n} \tag{8}$$
$$= \frac{4K(a\xi + c\xi') + 4iK'(b\xi + \partial\xi')}{n},$$

und wenn wir also

$$n = pn_1$$

setzen, so wird $\operatorname{sn}\Omega_{\xi,\xi'}$ unter den $x_{\nu,\nu'}$ dann und nur dann enthalten sein, wenn

$$\begin{aligned} a\xi + c\xi' &\equiv n_1\nu \\ b\xi + \partial\xi' &\equiv n_1\nu' \end{aligned} \pmod{n}. \tag{9}$$

Hieraus folgt durch Multiplication mit $p$ nach dem im vorigen Paragraphen Bewiesenen, dass

$$p\xi \equiv 0 \pmod{n'}, \quad p\xi' \equiv 0 \pmod{e},$$

und da $e$ nach der Voraussetzung über $A$ nicht durch $p$ theilbar ist, so folgt $\xi' = 0$. Da nun also $n'$ durch $p$ theilbar ist, so setzen wir $n' = pn'_1$, $n_1 = en'_1$ und erhalten, wenn $\lambda$ eine ganze Zahl bedeutet, $\xi = \lambda n'_1$, also, nach (9) $\lambda a \equiv e\nu$, $\lambda b \equiv e\nu'$ (mod $p$), oder, wenn wir $\lambda e^{-1} \equiv h$ (mod $p$) setzen:

$$\nu \equiv ha, \quad \nu' \equiv hb \pmod{p},$$

oder, nach (3), indem man $hx$ durch $2h$ ersetzt, was erlaubt ist, da $p$ ungerade und $x$ nicht durch $p$ theilbar ist:

$$\nu \equiv h(B + \beta), \quad \nu' \equiv 2hA \pmod{p}. \tag{10}$$

Nimmt man $h$ nach dem Modul $p$ beliebig, von 0 verschieden, an, so erhält man umgekehrt eine Bestimmung von $\xi$ nach dem Modul $n'$. Daraus folgt, dass es die einer Reihe angehörigen unter den Wurzeln der Gleichung (6) sind, die zugleich der Gleichung (4) genügen (§. 68). Wenn $\varDelta$ und also $\beta$ durch $p$ theilbar ist, so giebt es nur eine solche Reihe, sonst zwei.

Da man den grössten gemeinschaftlichen Theiler von (4) und (5) auf rationalem Wege finden kann, so folgt der Satz:

Ist $\varkappa$ ein singulärer Modul und $p$ eine ungerade Primzahl, welche entweder in $\varDelta$ aufgeht oder für welche $\left(\frac{-\varDelta}{p}\right) = +1$ ist, so lassen sich von der Theilungsgleichung $A_p(s^2) = 0$ ein oder zwei rationale Factoren vom Grade $p-1$ abspalten, deren Wurzeln sind:

$$(11) \quad x_h = \operatorname{sn}\left(4h\,\frac{(B+\beta)K+2AiK'}{p}\right),\ h = 1, 2, \ldots p-1.$$

Diese rationalen Factoren wollen wir mit $X_p$ oder, wenn es zwei sind, mit $X_p$, $X'_p$ bezeichnen.

$X'_p$ geht aus $X_p$ hervor durch die Vertauschung von $\mu$ mit $\mu'$, d. h. von $\sqrt{-m}$ mit $-\sqrt{-m}$.

Setzen wir zur Abkürzung:

$$\Omega_0 = \frac{4(B+\beta)K+8AiK'}{p},$$

und verstehen unter $g$ eine primitive Wurzel der Primzahl $p$, so lassen sich die Wurzeln einer dieser Theilgleichungen $X_p = 0$ in der Weise anordnen:

$$(12) \quad x_0 = \operatorname{sn}\Omega_0,\quad x_1 = \operatorname{sn}(g\,\Omega_0),\quad x_2 = \operatorname{sn}(g^2\,\Omega_0)\ldots,$$
$$x_{p-2} = \operatorname{sn}(g^{p-2}\,\Omega_0),$$

und nach dem (gewöhnlichen) Multiplicationstheorem kann $x_\lambda$ rational durch $x_{\lambda-1}$ ausgedrückt werden:

$$x_\lambda = f(x_{\lambda-1}).$$

Die Gleichung $X_p = 0$ ist also eine Abel'sche (§. 58). Ihre Gruppe ist die Gruppe der cyklischen Vertauschungen

$$(x_0, x_1, x_2, \ldots x_{p-2})$$

(oder für jetzt wenigstens in dieser Gruppe enthalten, vgl. unten §. 120), und die Gleichung kann nach derselben Methode aufgelöst werden, wie die Kreistheilungsgleichung. Sie ist also beispielsweise durch Quadratwurzeln lösbar, wenn $p - 1$ eine Potenz von 2 ist[1]).

Wenn $p$ nicht in $\varDelta$ aufgeht, so kann man durch die Lösungen der beiden Gleichungen $X_p = 0$, $X'_p = 0$ die sämmtlichen Lösungen der Theilungsgleichung für den Divisor $p$ rational ausdrücken. Denn setzen wir:

$$\varOmega_0 = \frac{4(B+\beta)K + 8AiK'}{p}, \quad \varOmega'_0 = \frac{4(B-\beta)K + 8AiK'}{p},$$

so kann man, wenn $\beta$ nicht durch $p$ theilbar ist, in der Form:

$$(13) \qquad \operatorname{sn}(\nu\varOmega_0 + \nu'\varOmega'_0)$$

alle Wurzeln $x_{\nu,\nu'}$ ausdrücken, und da man nach §. 64 die Functionen $\operatorname{cn}\nu\varOmega_0$, $\operatorname{dn}\nu\varOmega_0$ rational durch $\operatorname{sn}\nu\varOmega_0$ darstellen kann, so folgt nach dem Additionstheorem, dass die sämmtlichen Wurzeln (13) rational durch $\operatorname{sn}\varOmega_0$, $\operatorname{sn}\varOmega'_0$ ausdrückbar sind. Es ist also für diesen Fall das Theilungsproblem vollständig auf zwei reguläre Abel'sche Gleichungen zurückgeführt.

## §. 119. Theilung durch eine Primzahl, von welcher $-\varDelta$ quadratischer Nichtrest ist.

Es sei $q$ eine ungerade Primzahl, für welche

$$\left(\frac{-\varDelta}{q}\right) = -1,$$

und wir setzen wieder $\varDelta$ durch $q$ untheilbar voraus. Es seien dann

$$(1) \qquad x_{\nu\nu'} = \operatorname{sn}\frac{4\nu K + 4\nu' iK'}{q} = \operatorname{sn}\varOmega_{\nu\nu'}$$

die Wurzeln der Theilungsgleichung.

Wir wählen einen beliebigen complexen Multiplicator $\mu$ und erhalten:

$$x_{ll'} = \operatorname{sn}\mu\frac{4\nu K + 4\nu' iK'}{q} = \operatorname{sn}\mu\varOmega_{\nu\nu'},$$

wenn [nach §. 117, (8), (4)]:

$$\begin{aligned} l &\equiv \partial\nu - c\nu' \\ l' &\equiv -b\nu + a\nu' \end{aligned} \pmod{q},$$

oder

---

[1]) Gauss, Disquisitiones arithmeticae, sectio VII. Eine ausführliche Darstellung der Kreistheilungslehre, auch der späteren Untersuchungen, findet man in Bachmann, „Die Lehre von der Kreistheilung“, Leipzig 1872.

$$(2)\qquad \begin{aligned} 2\,l &\equiv -(B\nu - 2\,C\nu')x + y\nu \\ 2\,l' &\equiv -(2\,A\nu - B\nu')x + y\nu' \end{aligned} \quad (\text{mod } q).$$

Aus (2) können wir, da $\nu$, $\nu'$ nicht beide durch $q$ theilbar sind, bei beliebig gegebenem $l$, $l'$, $\nu$, $\nu'$ die Zahlen $x$, $y$ (nach dem Modul $q$) bestimmen, da die Determinante der rechten Seite

$$(3)\qquad 2(A\nu^2 - B\nu\nu' + C\nu'^2) = \frac{(2\,A\nu - B\nu')^2 + \varDelta\nu'^2}{2\,A}$$

durch $q$ nicht theilbar sein kann.

Hieraus folgt nach §. 117, (10), dass jede Wurzel der Theilungsgleichung rational durch jede andere ausdrückbar ist.

Wir setzen zur Abkürzung:

$$x_{\nu\nu'} = \operatorname{sn}\Omega_0 = x_0,$$

und betrachten nun zwei Wurzeln $x_{ll'}$, die wir mit

$$x_1 = \operatorname{sn}\mu_1\,\Omega_0, \quad x_2 = \operatorname{sn}\mu_2\,\Omega_0$$

bezeichnen. Nach dem soeben Bewiesenen ist, wenn $f_1$, $f_2$ rationale Functionen bedeuten:

$$x_1 = f_1(x_0), \quad x_2 = f_2(x_0).$$

Ersetzen wir in der ersten dieser Functionen $x_0$ durch $x_2$, in der anderen $x_0$ durch $x_1$, so erhalten wir eine vierte Wurzel $x_3$:

$$(4)\qquad x_3 = f_1 f_2(x_0) = f_2 f_1(x_0) = \operatorname{sn}\mu_1\,\mu_2\,\Omega_0.$$

Dies ist aber nach §. 58 das Kennzeichen dafür, dass die Gleichung, deren Wurzeln $x_0$, $x_1$, $x_2$, ... sind, eine Abel'sche Gruppe hat, also algebraisch lösbar ist.

Diese Schlussweise ist unverändert anwendbar auch auf die Fälle, die im vorigen Paragraphen betrachtet sind, auf die Gleichung $A'_p = 0$, welche man erhält, wenn man von der Theilungsgleichung für den Divisor $p$, $A_p = 0$, den Factor $X_p$ oder $X_p\,X'_p$ absondert. Dadurch sind eben diejenigen Werthe von $\nu$, $\nu'$ ausgeschlossen, für welche der Ausdruck (3) durch $p$ theilbar wird.

Es kann dann zwar vorkommen, dass die Wurzel $x_3$ (4) zu den abgesonderten Factoren gehört; dadurch aber wird die Gültigkeit unseres Schlusses nicht beeinträchtigt.

Es ist also die Theilungsgleichung unter der Voraussetzung eines singulären Moduls unter allen Umständen algebraisch auflösbar.

## §. 120. Irreducibilität der Theilungsgleichung.

Wir wenden uns noch zur Betrachtung der verborgeneren Eigenschaften der Gleichung

(1) $$X_p = 0$$

(§. 118), deren Wurzeln die $p-1$ Grössen

(2) $$x_h = \operatorname{sn} h\Omega, \qquad h = 1, 2, \ldots p-1$$

sind, wenn

(3) $$\Omega = \frac{4(B+\beta)K + 8AiK'}{p}$$

und $\beta$ eine Wurzel der Congruenz

(4) $$\beta^2 \equiv -\Delta \pmod{p},$$

und wollen insbesondere die Irreducibilität dieser Gleichung untersuchen, wodurch nach dem Früheren zugleich ihre Galois'sche Gruppe in völliger Uebereinstimmung mit der Gruppe der Kreistheilungsgleichung dargethan wird.

Wir haben in §. 93 und §. 102 gezeigt, dass das Modulquadrat $\varkappa^2$, nöthigenfalls unter Adjunction von $\sqrt{-m}$, rational ausdrückbar ist durch die Classeninvariante der Determinante $-\Delta$, und aus der zur Gauss'schen Transformation gehörigen Formel [§. 39, (26)]

$$\varkappa^2\left(\frac{\omega}{2}\right) = \frac{4\varkappa(\omega)}{[1+\varkappa(\omega)]^2}$$

folgt, dass der Modul $\varkappa$ selbst ebenfalls rational ausdrückbar ist, wenn wir die Classeninvarianten der Determinante $-4\Delta$ adjungiren.

Wir wissen ferner (§. 93), dass $f(\omega)$, $f_1(\omega)$, $f_2(\omega)$ ganze algebraische Zahlen sind, deren reciproke Werthe durch Multiplication mit geeigneten Potenzen von 2 gleichfalls in ganze Zahlen verwandelt werden können. Aus den Gleichungen [§. 49, (3)]

$$\varkappa^2 = \frac{f_2(\omega)^8}{f(\omega)^8}, \quad \varkappa'^2 = \frac{f_1(\omega)^8}{f(\omega)^8}$$

folgt sodann, dass auch $\varkappa^2$ und $1:\varkappa^2$, $\varkappa'^2$, $1:\varkappa'^2$ durch Multiplication mit Potenzen von 2 in ganze algebraische Zahlen verwandelt werden können.

Achten wir nun auf das, was in §. 60 über die Form der Theilungsgleichung

$$A_n(x^2) = 0$$

allgemein bewiesen ist, nämlich dass der Coëfficient der höchsten Potenz von $x$ eine Potenz von $\varkappa$ ist, und dass die übrigen Coëfficienten ganze rationale Functionen von $\varkappa^2$ mit ganzen rationalen Zahlencoëfficienten sind, so folgt, dass für einen singulären Modul alle Functionen

$$(5) \qquad \operatorname{sn} \frac{2hK + 2h'iK'}{n}$$

für beliebige ganzzahlige $h$, $h'$, $n$ algebraische Zahlen sind, welche durch Multiplication mit Potenzen von 2 in ganze Zahlen verwandelt werden.

Um nun den Zusammenhang unter den Wurzeln (2) unserer Theilungsgleichung zu ergründen, wenden wir die complexe Multiplication (§. 117) an.

Wir nehmen zwei beliebige ganze Zahlen $\xi$, $\eta$, von denen die erste gerade, die zweite ungerade ist. Dann ist

$$(6) \qquad \eta^2 + \varDelta\,\xi^2 = n$$

eine ungerade Zahl, und zwar $n \equiv 1$ (mod 4). Nun ersetzen wir in den Formeln (4), (5), §. 117 $x$, $y$ durch $2\,\xi$, $2\,\eta$, und erhalten:

$$(7) \qquad \begin{array}{ll} a = \eta + B\xi, & b = 2\,\xi A, \\ c = -\,2\,\xi C, & \partial = \eta - B\xi. \end{array}$$

$$(8) \qquad \mu = \eta - i\xi\sqrt{\varDelta}, \qquad n = \mu\mu'.$$

Wir bezeichnen jetzt, wie in früheren Abschnitten, die drei Functionen $\operatorname{sn} v$, $\operatorname{cn} v$, $\operatorname{dn} v$ mit $x$, $y$, $z$, so dass, da $a$, $\partial$ ungerade, $b$, $c$ gerade sind,

$$\frac{\operatorname{sn}\mu v}{\operatorname{sn} v}, \quad \frac{\operatorname{cn}\mu v}{\operatorname{cn} v}, \quad \frac{\operatorname{dn}\mu v}{\operatorname{dn} v}$$

rationale Functionen von $x^2$ sind [§. 117, (10), (12), (13)].

Setzen wir

$$(9) \qquad P(x) = x \overset{\xi,\xi'}{\Pi} \left( x - \operatorname{sn} \frac{\xi\,2K + \xi'\,2iK'}{\mu} \right),$$

worin das Product $\Pi$ sich auf die Werthe (15), §. 117 (ausgenommen $\xi = \xi' = 0$) erstreckt, so ist $P(x)$ (von einem constanten Factor abgesehen) der Zähler des Ausdruckes für $\operatorname{sn}\mu v$. Wir setzen daher

$$\operatorname{sn}\mu v = \frac{P(x)}{Q(x)}$$

und bestimmen $Q(x)$ dadurch, dass wir $v$ in $v + iK'$, also $\mu v$ in

$\mu v - cK + aiK'$, also $x$, $\operatorname{sn}\mu v$ in $1 : \varkappa x$, $1 : \varkappa \operatorname{sn} \mu v$ verwandeln (§. 39); dadurch ergiebt sich, wenn $\lambda$ einen unbestimmten constanten Coëfficienten bedeutet:

$$Q(x) = \lambda x^n P\left(\frac{1}{\varkappa x}\right),$$

$$\varkappa P(x) = \lambda x^n Q\left(\frac{1}{\varkappa x}\right),$$

und indem man $x$ abermals in $1 : \varkappa x$ verwandelt, folgt

$$\lambda = \pm \varkappa^{\frac{n+1}{2}},$$

also

$$\operatorname{sn}\mu v = \pm \frac{P(x)}{\varkappa^{\frac{n+1}{2}} x^n P\left(\frac{1}{\varkappa x}\right)}. \tag{10}$$

Ersetzen wir in dieser Formel $v$ durch $v + K$, $\mu v$ durch $\mu v + \partial K - biK'$, so gehen $x$ über in $y : z$ und $\operatorname{sn}\mu v$ in $\pm \frac{\operatorname{cn}\mu v}{\operatorname{dn}\mu v}$. Wir erhalten also:

$$\frac{\operatorname{cn}\mu v}{\operatorname{dn}\mu v} = \pm \frac{z^n P\left(\frac{y}{z}\right)}{\varkappa^{\frac{n+1}{2}} y^n P\left(\frac{z}{\varkappa y}\right)}.$$

Daraus folgt nun, wenn wieder $\lambda$ einen constanten Coëfficienten bedeutet, da $\operatorname{cn}\mu v$, $\operatorname{dn}\mu v$ denselben Nenner $Q(x)$ haben wie $\operatorname{sn}\mu v$:

$$\operatorname{cn}\mu v = \pm \lambda \frac{z^n P\left(\frac{y}{z}\right)}{\varkappa^{\frac{n+1}{2}} x^n P\left(\frac{1}{\varkappa x}\right)},$$

$$\operatorname{dn}\mu v = \lambda \frac{y^n P\left(\frac{z}{\varkappa y}\right)}{x^n P\left(\frac{1}{\varkappa x}\right)},$$

und wenn man in der letzten Formel abermals $v$ durch $v + K$, also $x$, $y$, $z$, $\operatorname{dn}\mu v$ durch $y : z$, $-\varkappa' x : z$, $\varkappa' : z$, $\varkappa' : \operatorname{dn}\mu v$ ersetzt, so folgt:

$$\lambda = \pm \frac{1}{\varkappa'^{\frac{n-1}{2}}}$$

also:

$$\text{(11)} \qquad \operatorname{cn} \mu v = \pm \frac{z^n P\left(\frac{y}{z}\right)}{\varkappa^{\frac{n+1}{2}} \varkappa'^{\frac{n-1}{2}} x^n P\left(\frac{1}{\varkappa x}\right)},$$

$$\text{(12)} \qquad \operatorname{dn} \mu v = \pm \frac{y^n P\left(\frac{z}{\varkappa y}\right)}{\varkappa'^{\frac{n-1}{2}} x^n P\left(\frac{1}{\varkappa x}\right)}.$$

Da nun die in $P(x)$ vorkommenden Zahlen

$$\operatorname{sn} \frac{\xi 2K + \xi' 2iK'}{\mu}$$

durch §. 117, (7) auf die Form (5) gebracht werden, so schliessen wir zunächst aus (10), (11), (12):

Die Coëfficienten im Zähler und Nenner in den Ausdrücken für $\operatorname{sn} \mu v$, $\operatorname{cn} \mu v$, $\operatorname{dn} \mu v$ sind algebraische Zahlen des Rationalitätsbereiches $\mathfrak{R}(\varkappa^2, \sqrt{-\Delta})$, welche durch Multiplication mit Potenzen von 2 in ganze Zahlen verwandelt werden.

Um die Beschaffenheit dieser Coëfficienten noch weiter zu ergründen, nehmen wir jetzt an, $n$ sei eine Primzahl, und setzen [nach (10)]:

$$\begin{aligned}
\operatorname{sn} \mu v &= \frac{\mu x + \mu a_3 x^3 + \mu a_5 x^5 + \cdots \pm \varkappa^{\frac{n-1}{2}} x^n}{1 + \mu \partial_2 x^2 + \mu \partial_4 x^4 + \cdots \mu \partial_{n-1} x^{n-1}} = \frac{A(x)}{D(x)}, \\
\text{(13)} \quad \operatorname{cn} \mu v &= \frac{1 + b_2 x^2 + b_4 x^4 + \cdots b_{n-1} x^{n-1}}{1 + \mu \partial_2 x^2 + \mu \partial_4 x^4 + \cdots \mu \partial_{n-1} x^{n-1}} \operatorname{cn} v = \frac{B(x)}{D(x)} \operatorname{cn} v, \\
\operatorname{dn} \mu v &= \frac{1 + c_2 x^2 + c_4 x^4 + \cdots c_{n-1} x^{n-1}}{1 + \mu \partial_2 x^2 + \mu \partial_4 x^4 + \cdots \mu \partial_{n-1} x^{n-1}} \operatorname{dn} v = \frac{C(x)}{D(x)} \operatorname{dn} v,
\end{aligned}$$

$$\text{(14)} \qquad a_{n-\nu} = \pm \partial_\nu \varkappa^{\frac{n-2\nu-1}{2}},$$

worin nach dem, was oben bewiesen ist, $\mu a_\nu$, $\mu \partial_\nu$, $b_\nu$, $c_\nu$ durch Multiplication mit Potenzen von 2 in ganze Zahlen verwandelt werden. Es ist zu beweisen, dass diese Eigenschaft auch den Zahlen $a_\nu$, $\partial_\nu$ selbst zukommt. Hierbei ist aber die Voraussetzung wesentlich, dass $n$ eine Primzahl sei. Wenn dies für die $a_\nu$ bewiesen ist, so folgt es nach (14) auch für die $\partial_\nu$.

Wenn wir die erste Gleichung (13) nach $v$ differentiiren und die beiden letzten Gleichungen (13) zu Rathe ziehen, so folgt, wenn die Ableitungen von $A(x)$, $D(x)$ nach $x$ mit $A'(x)$, $D'(x)$ bezeichnet werden:

$$\mu B(x)\, C(x) = A'(x)\, D(x) - D'(x)\, A(x),$$

oder wenn

$$A'(x) = \mu A_1(x) = \mu \Big[1 + 3\, a_3 x^2 + 5\, a_5 x^4 + \cdots \mu' \varkappa^{\frac{n-1}{2}} x^{n-1}\Big]$$

$$D'(x) = \mu D_1(x) = \mu [2\, \partial_2 x + 4\, \partial_4 x^3 + \cdots (n-1)\, \partial_{n-1} x^{n-1}]$$

gesetzt wird:

$$B(x)\, C(x) = A_1(x)\, D(x) - D_1(x)\, A(x). \tag{15}$$

Vergleichen wir rechts und links die Coëfficienten von $x^2$, $x^4$, ... $x^{\nu-1}$, so folgt

$$\begin{gathered} 3\, a_3 - \mu \partial_2 = b_2 + c_2 \\ 5\, a_5 + a_3 \mu \partial_2 - 3\, \mu \partial_4 = b_4 + b_2 c_2 + c_4 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \nu a_\nu + (\nu - 4)\, a_{\nu-2} \mu \partial_2 + (\nu - 8)\, a_{\nu-4} \mu \partial_4 + \cdots \\ = c_{\nu-1} + c_{\nu-3} \partial_2 + \cdots, \end{gathered} \tag{16}$$

woraus also zu schliessen, dass $3\, a_3$, $5\, a_5$, ... $\nu a_\nu$ durch Multiplication mit Potenzen von 2 in ganze Zahlen verwandelt werden. Dieselbe Eigenschaft hat aber $\mu a_\nu$ und folglich auch $n a_\nu$. Wenn nun $n$ eine Primzahl ist, so ist, so lange $\nu < n$ ist, $\nu$ zu $n$ relativ prim, und man kann die rationalen ganzen Zahlen $\alpha$, $\beta$ so bestimmen, dass $\nu \alpha + n \beta = 1$, also

$$\alpha \nu a_\nu + \beta n a_\nu = a_\nu,$$

woraus also die Richtigkeit unserer Behauptung folgt, dass die $a_\nu$ und folglich auch die $\partial_\nu$ durch Multiplication mit Potenzen von 2 in ganze Zahlen verwandelt werden.

Wir setzen nun

$$v = \Omega = \frac{4(B + \beta) K + 8\, A i K'}{p}, \tag{17}$$

so dass $\operatorname{sn} v$ in die Wurzel $x_1$ der Gleichung (1) übergeht. Es wird dann nach (7) und §. 117, (8):

$$\begin{aligned} \mu \Omega &= \frac{4}{p} \{[(B + \beta)\, \partial - 2\, A c]\, K - [(B + \beta)\, b - 2\, A a]\, i K'\} \\ &= \frac{4}{p} \{[(B + \beta)(\eta - B \xi) + 4\, A C \xi]\, K + 2\, A (\eta - \beta \xi)\, i K'\}, \end{aligned}$$

oder, indem man für $4\, A\, C = B^2 + \varDelta$ den nach dem Modul $p$ congruenten Werth $B^2 - \beta^2$ einsetzt:

$$\operatorname{sn} \mu v = \operatorname{sn} \mu \Omega = \operatorname{sn} (\eta - \beta \xi)\, \Omega, \tag{18}$$

also gleichfalls eine Wurzel der Gleichung (1), und dies wird jede beliebige dieser Wurzeln sein können, wenn für ein gegebenes, durch $p$ nicht theilbares $h$ man $\xi$, $\eta$ so bestimmen kann, dass

(19) $$\eta - \beta\xi \equiv h \pmod{p},$$

während zugleich $n = \eta^2 + \Delta\xi^2$ eine Primzahl [$\equiv 1 \pmod{4}$] ist. Dass dies möglich ist, geht aus einem Satze von Dirichlet hervor, auf dessen Beweis wir hier nicht eingehen können, für welchen vor Kurzem ein Beweis gegeben ist von A. Meyer im Bd. 103 des Journals für Mathematik, und der so lautet:

Jede eigentlich primitive Form, deren Determinante kein Quadrat ist, stellt unendlich viele Primzahlen dar, welche zugleich in einer gegebenen, mit den Charakteren des Geschlechtes jener quadratischen Form verträglichen primitiven Linearform enthalten sind.

Aus diesem Satze folgt, dass durch die quadratische Form

$$\eta^2 + 4\Delta p^2\xi_1^2$$

unendlich viele Primzahlen $n$ darstellbar sind, welche nach dem Modul $p$ mit einer beliebig gegebenen Quadratzahl $h^2$ congruent sind, und wenn man daher $\xi = 2p\xi_1$ setzt, so wird bei passender Vorzeichenbestimmung $\eta$ und mithin auch $\eta - \beta\xi$, wie es (19) verlangt, mit $h$ congruent. Wir können also als bewiesen annehmen, dass durch (18) jede Wurzel der Gleichung (1) dargestellt werden kann.

Wir betrachten nun als Rationalitätsbereich den Körper

$$\mathfrak{K} = \mathfrak{K}(\sqrt{-\Delta}, \varkappa),$$

der aus den rationalen Functionen von $\varkappa$ und $\sqrt{-\Delta}$ besteht, der jedenfalls in dem Classenkörper der Determinante $-4\Delta$ enthalten ist. (Wir können dem Körper $\mathfrak{K}$ auch beliebige Classeninvarianten adjungiren, deren Determinanten zu $-\Delta$ im quadratischen Verhältniss stehen.)

Wenn nun $\mathfrak{n}$ irgend ein in der rationalen Primzahl $n$ aufgehendes Primideal dieses Körpers $\mathfrak{K}$ bedeutet, so ist, da $n$ durch die Hauptform der Determinante $-4\Delta$ (oder auch jeder zu $-\Delta$ im quadratischen Verhältniss stehenden Determinante) darstellbar ist, der Index von $n$ gleich 1, also [§. 110, (7)] für jede ganze Zahl $\xi$ des Körpers $\mathfrak{K}$

(20) $$\xi^n \equiv \xi \pmod{\mathfrak{n}},$$

also auch, da wir hier und in der Folge Zahlen, welche durch Multiplication mit Potenzen von 2 in ganze Zahlen verwandelt werden, genau so wie ganze Zahlen behandeln können, und da $\varkappa$ nicht durch $\mathfrak{n}$ theilbar ist:

$$(21) \qquad \varkappa^{n-1} \equiv 1 \pmod{\mathfrak{n}}.$$

Wir adjungiren nunmehr dem Körper $\mathfrak{K}$ eine Wurzel $x$ (mithin auch alle Wurzeln) der Gleichung $X_p = 0$, wodurch ein Körper

$$\mathfrak{K}_1 = \mathfrak{K}\left(\sqrt{-\varDelta}, \varkappa, x\right)$$

entsteht, und bezeichnen mit $\mathfrak{n}_1$ ein in $\mathfrak{n}$ aufgehendes Primideal dieses Körpers.

Aus der ersten Gleichung (13) folgt nun:

$$\operatorname{sn} \mu \Omega \equiv \pm \varkappa^{\frac{n-1}{2}} \operatorname{sn} \Omega^n \pmod{\mathfrak{n}_1},$$

oder [nach (18), (19), (21)]:

$$(22) \qquad x_h^2 \equiv x_1^{2n} \pmod{\mathfrak{n}_1},$$

worin $x_h$ jede Wurzel der Gleichung $X_p = 0$ sein kann.

Die Function $X_p$ hängt nur von $x^2$ ab, ist in Bezug auf $x^2$ vom Grade $\frac{p-1}{2}$ und hat $\frac{p-1}{2}$ von einander verschiedene Wurzeln. Sei

$$(23) \qquad F(x^2) = 0$$

die Gleichung niedrigsten Grades in $x^2$, deren Coëfficienten dem Rationalitätsbereich $\mathfrak{K}$ angehören, welche durch die Wurzel $x = x_1$ befriedigt wird. Erhebt man nun (23) in die $n$te Potenz, so folgt wegen (20), (22)

$$(24) \qquad F(x_h^2) \equiv 0 \pmod{\mathfrak{n}_1}$$

und folglich muss $x_h^2$ mit irgend einer der Wurzeln von (23) nach dem Modul $\mathfrak{n}_1$ congruent sein. Da man aber $n$ immer so wählen kann, dass $\mathfrak{n}$ nicht in der Discriminante von $X_p$ aufgeht, so folgt, dass $x_h^2$ unter den Wurzeln von (23) enthalten sein muss, also $F(x^2)$ mit $X_p$ identisch (man vgl. über dies Beweisverfahren §. 110).

$X_p$ lässt sich also im Körper $\mathfrak{K}$ nicht in Factoren zerlegen, welche rational von $x^2$ abhängen.

Es könnte noch die Frage sein, ob $X_p$ in zwei rationale Factoren vom Grade $\frac{p-1}{2}$ zerlegbar ist, welche auch ungerade Potenzen von $x$ enthalten; zwei solche Factoren müssen, wenn sie existiren, durch Vertauschung von $x$ mit $-x$ in einander übergehen, und es muss also das Product der Wurzeln

$$P = \overset{h}{\Pi} \operatorname{sn} h \Omega$$

in dem Körper $\mathfrak{K}$ ein Quadrat sein.

Für dies Product findet man aber nach §. 70, 71 den Ausdruck:

$$(25) \qquad P = \frac{f_1(\omega)^{2p} f(\omega)^{4p-4}}{2^{p-1} f_1\left(\frac{\lambda+\omega}{p}\right)^2} \left[\frac{\eta\left(\frac{\lambda+\omega}{p}\right)}{\eta(\omega)}\right]^2,$$

worin $\lambda$ durch die Congruenzen [§. 71, (10)]

$$(B+\beta) \equiv 2A\lambda \pmod{p}, \quad \lambda \equiv 0 \pmod{4}$$

bestimmt ist.

Der erste Factor dieses Ausdrucks von $P$

$$\frac{f_1(\omega)^{2p} f(\omega)^{4p-4}}{2^{p-1} f_1\left(\frac{\lambda+\omega}{p}\right)^2}$$

wird durch Multiplication mit einer Potenz von 2 in eine ganze Zahl verwandelt, und dasselbe gilt von seinem reciproken Werthe.

Der zweite Factor

$$M = \left[\frac{\eta\left(\frac{\lambda+\omega}{p}\right)}{\eta(\omega)}\right]^2$$

ist (§. 109) eine ganze algebraische Zahl, und wenn wir voraussetzen, dass $p$ zu den in §. 110 als Primzahlen dritter Art bezeichneten gehört, so ist, wie dort nachgewiesen, $M$ immer wenigstens durch ein in $p$ aufgehendes Primideal, aber nicht durch dessen Quadrat theilbar. In diesem Falle kann also $P$ kein Quadrat sein und die Zerlegung von $X_p$ in zwei rationale Factoren ist unmöglich.

Ob eine solche Zerlegung von $X_p$ möglich ist, wenn $p$ zu den Primzahlen der ersten Art gehört, also insbesondere, wenn etwa $p$ oder eine höhere Potenz von $p$ in $\Delta$ aufgeht, müssen wir dahingestellt sein lassen.

# Anhang.

---

## Verzeichniss von Classeninvarianten.

$$f(\sqrt{-1}) = \sqrt[4]{2}, \qquad m = 1$$

$$f_1(\sqrt{-2}) = \sqrt[4]{2}, \qquad m = 2$$

$$f(\sqrt{-3}) = \sqrt[3]{2}, \qquad m = 3$$

$$f_1(\sqrt{-4}) = \sqrt[8]{8}, \qquad m = 4$$

$$f(\sqrt{-5})^4 = 1 + \sqrt{5}, \qquad m = 5$$

$$f_1(\sqrt{-6})^6 = 4 + 2\sqrt{2}, \qquad m = 6$$

$$f(\sqrt{-7}) = \sqrt{2}, \qquad m = 7$$

$$f_1(\sqrt{-8})^8 = 8 + 8\sqrt{2}, \qquad m = 8$$

$$f(\sqrt{-9})^3 = \sqrt[4]{2}\,(1 + \sqrt{3}), \qquad m = 9$$

$$\sqrt{2}\, f_1(\sqrt{-10})^2 = 1 + \sqrt{5}, \qquad m = 10$$

$$f(\sqrt{-11}) = x, \quad x^3 - 2x^2 + 2x - 2 = 0, \qquad m = 11$$

$$f_1(\sqrt{-12})^4 = 2\sqrt[6]{2}\,(1 + \sqrt{3}), \qquad m = 12$$

$$f(\sqrt{-13})^4 = 3 + \sqrt{13}, \qquad m = 13$$

$$f_1(\sqrt{-14})^2 = \sqrt{2}\,x, \; x + \frac{1}{x} = 1 + \sqrt{2}, \qquad m = 14$$

$$f(\sqrt{-15})^3 = \sqrt{2}\,(1 + \sqrt{5}), \qquad m = 15$$

$$f_1(\sqrt{-16})^4 = 2\sqrt[4]{8}\,(1 + \sqrt{2}), \qquad m = 16$$

$$f(\sqrt{-17})^2 = \sqrt{2}\,x, \quad x + \frac{1}{x} = \frac{1 + \sqrt{17}}{2}, \qquad m = 17$$

$$f_1(\sqrt{-18})^3 = \sqrt[4]{2}\,(2 + \sqrt{6}), \qquad m = 18$$

$$f(\sqrt{-19}) = x, \quad x^3 - 2x - 2 = 0, \qquad m = 19$$

$$f_1(\sqrt{-20})^4 = \sqrt{8}\,x, \quad x^2 = \frac{1+\sqrt{5}}{2}(2x+1), \qquad m = 20$$

$$2f(\sqrt{-21})^{12} = (\sqrt{3}+\sqrt{7})^3(3+\sqrt{7})^2, \qquad m = 21$$

$$f_1(\sqrt{-22})^2 = \sqrt{2}(1+\sqrt{2}), \qquad m = 22$$

$$f(\sqrt{-23}) = \sqrt{2}\,x, \quad x^3 - x - 1 = 0, \qquad m = 23$$

$$f_1(\sqrt{-24})^{24} = 2^9(1+\sqrt{2})^2(2+\sqrt{3})^3(\sqrt{2}+\sqrt{3})^3, \qquad m = 24$$

$$\sqrt[4]{8}\,f(\sqrt{-25}) = 1+\sqrt{5}, \qquad m = 25$$

$$f_1(\sqrt{-26})^2 = \sqrt{2}\,x, \quad x^3 - x^2 = \frac{3+\sqrt{13}}{2}(x+1), \qquad m = 26$$

$$f(\sqrt{-27})^3 = 2x, \quad x^3 - 3x^2 - 3x - 1 = 0, \qquad m = 27$$

$$f_1(\sqrt{-28})^4 = 2\sqrt{2}(3+\sqrt{7}), \qquad m = 28$$

$$f(\sqrt{-29})^4 = 2x, \qquad m = 29$$

$$2x^3 - 9x^2 - 8x - 5 = \sqrt{29}(x+1)^2,$$

$$f_1(\sqrt{-30})^6 = 2\sqrt{2}(3+\sqrt{10})(2+\sqrt{5}), \qquad m = 30$$

$$f(\sqrt{-31}) = \sqrt{2}\,x, \quad x^3 - x^2 - 1 = 0, \qquad m = 31$$

$$f_1(\sqrt{-32})^8 = 8x, \qquad m = 32$$

$$x^2 - 8(1+\sqrt{2})^2 x - 2(1+\sqrt{2}) = 0,$$

$$\sqrt{2}\,f(\sqrt{-33})^6 = (3+\sqrt{11})(1+\sqrt{3})^3, \qquad m = 33$$

$$f_1(\sqrt{-34})^2 = \sqrt{2}\,x, \quad x + \frac{1}{x} = \frac{3+\sqrt{17}}{2}, \qquad m = 34$$

$$f(\sqrt{-35}) = x, \quad x^3 - 2 = (1+\sqrt{5})(x^2 - x), \qquad m = 35$$

$$f_1(\sqrt{-36})^3 = \sqrt[8]{8}\,x, \quad x^2 - 4x - 2 = 2\sqrt{3}(x+1), \qquad m = 36$$

$$f(\sqrt{-37})^4 = 2(6+\sqrt{37}), \qquad m = 37$$

$$f_1(\sqrt{-38})^2 = \sqrt{2}\,x, \qquad m = 38$$

$$x^3 - 2x^2 - (2x+1)(1+\sqrt{2}) = 0,$$

$$f(\sqrt{-39})^3 = \sqrt{8}\,x, \quad x^2 = \frac{3+\sqrt{13}}{2}(x+1), \qquad m = 39$$

$$f_1(\sqrt{-40})^8 = 2(1+\sqrt{5})^2(1+\sqrt{2})^2(3+\sqrt{10}), \qquad m = 40$$

$$f(\sqrt{-41}) = \sqrt{2}\,x, \qquad m = 41$$

$$\left(x+\frac{1}{x}\right)^2 - \frac{5+\sqrt{41}}{2}\left(x+\frac{1}{x}\right) + \frac{7+\sqrt{41}}{2} = 0,$$

$$\sqrt{8}\,f_1(\sqrt{-42})^6 = (2\sqrt{2}+\sqrt{7})(3+\sqrt{7})^3, \qquad m = 42$$

$$f(\sqrt{-43}) = x, \quad x^3 - 2x^2 - 2 = 0, \qquad m = 43$$

$$f_1(\sqrt{-44})^4 = \sqrt{8}\,x, \qquad m = 44$$

$$(x^3 - 6x^2 + 8x - 3) - \sqrt{11}\,(2x^2 - 2x + 1) = 0,$$

$$f(\sqrt{-45})^{12} = 2(2+\sqrt{5})^3(\sqrt{3}+\sqrt{5})^4, \qquad m = 45$$

$$f_1(\sqrt{-46})^2 = \sqrt{2}\,x, \quad x + \frac{1}{x} = 3 + \sqrt{2}, \qquad m = 46$$

$$f(\sqrt{-47}) = \sqrt{2}\,x, \qquad m = 47$$

$$x^5 - x^3 - 2x^2 - 2x - 1 = 0,$$

$$f_1(\sqrt{-48})^8 = 8\sqrt[6]{2} \qquad m = 48$$

$$(1+\sqrt{3})(\sqrt{2}+\sqrt{3})^2(1+\sqrt{2})^2,$$

$$f(\sqrt{-49})^2 = \sqrt{2}\,x, \quad x + \frac{1}{x} = 2 + \sqrt{7}, \qquad m = 49$$

$$f_1(\sqrt{-50}) = \sqrt[4]{2}\,x, \quad x^3 - x^2 = \frac{1+\sqrt{5}}{2}(x+1), \qquad m = 50$$

$$f(\sqrt{-51})^3 = 2x, \quad x^3 - 4x^2 - x - 1 = \sqrt{17}\,x^2, \qquad m = 51$$

$$f_1(\sqrt{-52})^4 = \sqrt{8}\,x, \qquad m = 52$$

$$x^2 - 2(4+\sqrt{13})\,x - \frac{3+\sqrt{13}}{2} = 0,$$

---

$$f(\sqrt{-55}) = \sqrt{2}\,x, \quad x^2 - x = \frac{1+\sqrt{5}}{2}, \qquad m = 55$$

$$\sqrt{2}\,f(\sqrt{-57})^6 = (1+\sqrt{3})^3(13+3\sqrt{19}), \qquad m = 57$$

$$\sqrt{2}\,f_1(\sqrt{-58})^2 = 5 + \sqrt{29}, \qquad m = 58$$

$$f_1(\sqrt{-60})^{12} = \qquad m = 60$$

$$\sqrt{2}^5(1+\sqrt{5})^2(2+\sqrt{3})^3(\sqrt{3}+\sqrt{5})^3,$$

$$f(\sqrt{-63})^3 = \sqrt{8}\,x, \qquad m = 63$$

$$\sqrt{7}\,(x^2 - x + 1) = \sqrt{3}\,(x^2 + 3x - 1),$$

$$f(\sqrt{-67}) = x, \quad x^3 - 2x^2 - 2x - 2 = 0, \qquad m = 67$$

$$\sqrt{8}\,f_1(\sqrt{-70})^2 = (1+\sqrt{5})^{[illegible]}(1+\sqrt{2}), \qquad m = 70$$

$$f(\sqrt{-71}) = \sqrt{2}\,x, \qquad m = 71$$

$$x^7 - 2x^6 - x^5 + x^4 + x^3 + x^2 - x - 1 = 0,$$

$$f_1(\sqrt{-72})^{24} = 2^6(2+\sqrt{6})^4(1+\sqrt{2})^9(2+\sqrt{3})^6, \qquad m = 72$$

$$f(\sqrt{-73})^2 = \sqrt{2}\,x, \qquad m = 73$$

$$x + \frac{1}{x} = \frac{5+\sqrt{73}}{2},$$

$$\sqrt[3]{2}\,f(\sqrt{-75}) = x, \qquad m = 75$$

$$x^3 - 2x^2 - 2x - 4 = 4\sqrt{5}\,x,$$

$$\sqrt{8}\,f_1(\sqrt{-78})^6 = (3+\sqrt{13})^3(5+\sqrt{26}), \qquad m = 78$$

$$f_1(\sqrt{-82})^2 = \sqrt{2}\,x, \quad x + \frac{1}{x} = \frac{15+\sqrt{41}}{2}, \qquad m = 82$$

$$16\,f(\sqrt{-85})^4 = (1+\sqrt{5})^4(9+\sqrt{85}), \qquad m = 85$$

$$f_1(\sqrt{-88})^8 = 4(1+\sqrt{2})^2(3+\sqrt{11})^2(7\sqrt{2}+3\sqrt{11}), \qquad m = 88$$

$$f(\sqrt{-91}) = x, \quad x^3 - 2x^2 - x - 2 = \sqrt{13}\,x, \qquad m = 91$$

$$2\,f(\sqrt{-93})^{12} = (3\sqrt{3}+\sqrt{31})^3(39+7\sqrt{31})^2, \qquad m = 93$$

$$f(\sqrt{-97})^2 = \sqrt{2}\,x, \quad x + \frac{1}{x} = \frac{9+\sqrt{97}}{2}, \qquad m = 97$$

$$f(\sqrt{-99})^3 = 2x, \qquad m = 99$$

$$x^3 - 13x^2 - 4x - 1 = \sqrt{33}(2x^2 + x),$$

$$\sqrt[8]{2}\,f_1(\sqrt{-100}) = x, \qquad m = 100$$

$$x^2 - x - 1 = \sqrt{5}(x+1),$$

$$f_1(\sqrt{-102})^6 = \sqrt{2}^3(1+\sqrt{2})^3(3\sqrt{2}+\sqrt{17})^2, \qquad m = 102$$

$$\sqrt{2}^{13} f(\sqrt{-105})^6 =$$

$$(1+\sqrt{5})^3(1+\sqrt{3})^3(\sqrt{3}+\sqrt{7})^3(\sqrt{5}+\sqrt{7}), \qquad m = 105$$

$$f_1(\sqrt{-112})^8 = \qquad m = 112$$

$$\sqrt{2}^7(1+\sqrt{2})^4(2\sqrt{2}+\sqrt{7})^2(3+\sqrt{7}),$$

$$8\,f_1(\sqrt{-120})^{24} = (1+\sqrt{3})^6(1+\sqrt{5})^6(\sqrt{2}+\sqrt{3})^6 \qquad m = 120$$

$$(\sqrt{3}+\sqrt{5})^6(\sqrt{5}+\sqrt{6})^3(3+\sqrt{10})^2,$$

$$\sqrt{2}^7 f_1(\sqrt{-130})^2 = (1+\sqrt{5})^3(3+\sqrt{13}), \qquad m = 130$$

$$2\,f(\sqrt{-133})^4 = (3+\sqrt{7})^2(5\sqrt{7}+3\sqrt{19}), \qquad m = 133$$

$$f_1(\sqrt{-142})^2 = \sqrt{2}\,x, \quad x + \frac{1}{x} = 9 + 5\sqrt{2}, \qquad m = 142$$

$$f\left(\sqrt{-163}\right) = x, \quad x^3 - 6x^2 + 4x - 2 = 0, \qquad m = 163$$

$$2^9 f\left(\sqrt{-165}\right)^{12} = (1+\sqrt{5})^6 (\sqrt{3}+\sqrt{5})^6 \qquad m = 165$$

$$(3\sqrt{5}+2\sqrt{11})^2 (\sqrt{11}+\sqrt{15})^3$$

$$2^6 f_1\left(\sqrt{-168}\right)^{24} = (1+\sqrt{3})^{12} (1+\sqrt{2})^6, \qquad m = 168$$

$$(3+\sqrt{7})^6 (\sqrt{3}+\sqrt{7})^6 (\sqrt{6}+\sqrt{7})^3 (\sqrt{7}+\sqrt{8})^2,$$

$$f\left(\sqrt{-175}\right) = \sqrt{2}\,x, \qquad m = 175$$

$$2x^3 - 4x^2 + x - 3 = \sqrt{5}(2x^2 - x + 1),$$

$$\sqrt{2}^7 f\left(\sqrt{-177}\right)^6 = (23+3\sqrt{59})(1+\sqrt{3})^9, \qquad m = 177$$

$$\sqrt{2}^5 f_1\left(\sqrt{-190}\right)^2 = (1+\sqrt{5})^3 (3+\sqrt{10}), \qquad m = 190$$

$$f\left(\sqrt{-193}\right)^2 = \sqrt{2}\,x, \quad x + \frac{1}{x} = 13 + \sqrt{193}, \qquad m = 193$$

$$\sqrt{2}^9 f_1\left(\sqrt{-210}\right)^6 = \qquad m = 210$$

$$(1+\sqrt{5})^3 (\sqrt{2}+\sqrt{3})^3 (\sqrt{3}+\sqrt{7})^3 (5\sqrt{5}+\sqrt{14}),$$

$$f_1\left(\sqrt{-232}\right)^8 = \qquad m = 232$$

$$2(1+\sqrt{2})^6 (5+\sqrt{29})^2 (99+13\sqrt{58}),$$

$$f_1\left(\sqrt{-240}\right)^{24} = \sqrt{2}^{17} (1+\sqrt{5})^2 (2+\sqrt{3})^3 \qquad m = 240$$

$$(\sqrt{3}+\sqrt{5})^3 (1+\sqrt{2})^6 (3+\sqrt{10})^6$$

$$(\sqrt{2}+\sqrt{3})^6 (\sqrt{5}+\sqrt{6})^6,$$

$$2 f\left(\sqrt{-253}\right)^4 = (5+\sqrt{23})^2 (13\sqrt{11}+9\sqrt{23}), \qquad m = 253$$

$$\sqrt{2}^{13} f\left(\sqrt{-273}\right)^6 = \qquad m = 273$$

$$(3+\sqrt{13})^3 (1+\sqrt{3})^3 (\sqrt{3}+\sqrt{7})^3 (11\sqrt{13}+15\sqrt{7}),$$

$$8 f_1\left(\sqrt{-280}\right)^8 = (1+\sqrt{5})^4 (1+\sqrt{2})^2 (3+\sqrt{7})^2 \qquad m = 280$$

$$(\sqrt{5}+\sqrt{7})^2 (\sqrt{7}+\sqrt{8})^2 (5\sqrt{5}+3\sqrt{14}),$$

$$2^6 f_1\left(\sqrt{-312}\right)^{24} = (1+\sqrt{3})^{18} (3+\sqrt{13})^6 (\sqrt{2}+\sqrt{3})^6 \qquad m = 312$$

$$(2\sqrt{3}+\sqrt{13})^6 (3\sqrt{3}+\sqrt{26})^3 (5+\sqrt{26})^2,$$

$$\sqrt{2}^{15} f_1\left(\sqrt{-330}\right)^6 = (1+\sqrt{5})^6 \qquad m = 330$$

$$(\sqrt{5}+\sqrt{6})^3 (\sqrt{11}+\sqrt{15})^3 (\sqrt{10}+\sqrt{11}),$$

$$\sqrt{2}^{19} f\left(\sqrt{-345}\right)^6 = (1+\sqrt{5})^6 \qquad m = 345$$

$$(1+\sqrt{3})^3 (3\sqrt{3}+\sqrt{23})^3 (15\sqrt{5}+7\sqrt{23}),$$

$$2^{16} f\left(\sqrt{-357}\right)^6 = \qquad m = 357$$

$$(\sqrt{3}+\sqrt{7})^{12} (3+\sqrt{7})^6 (\sqrt{17}+\sqrt{21})^3 (11+\sqrt{119})^2,$$

$$\sqrt{2}^7\, f(\sqrt{-385})^2 = \qquad m = 385$$

$$(1+\sqrt{5})^2\,(3+\sqrt{11})\,(\sqrt{5}+\sqrt{7})\,(\sqrt{7}+\sqrt{11}),$$

$$f_1(\sqrt{-408})^{24} = (1+\sqrt{3})^{12}\,(\sqrt{2}+\sqrt{3})^{12}\,(1+\sqrt{2})^6 \qquad m = 408$$

$$(7+\sqrt{51})^6\,(3\sqrt{2}+\sqrt{17})^4\,(5\sqrt{2}+\sqrt{51})^3,$$

$$\sqrt{2}^9 f_1(\sqrt{-462})^6 = (\sqrt{3}+\sqrt{7})^3 \qquad m = 462$$

$$(\sqrt{6}+\sqrt{7})^3\,(\sqrt{7}+\sqrt{11})^3\,(22\sqrt{22}+39\sqrt{7}),$$

$$2^5 f_1(\sqrt{-520})^8 = (1+\sqrt{5})^6\,(1+\sqrt{2})^4\,(3+\sqrt{13})^2 \qquad m = 520$$

$$(3+\sqrt{10})^2\,(5+\sqrt{26})\,(57+5\sqrt{130}),$$

$$2 f_1(\sqrt{-760})^8 = (1+\sqrt{5})^6\,(3+\sqrt{10})^2 \qquad m = 760$$

$$(13+3\sqrt{19})^2\,(3\sqrt{2}+\sqrt{19})^2\,(2\sqrt{5}+\sqrt{19})^2$$

$$(51\sqrt{10}+37\sqrt{19}),$$

$$2^{12} f_1(\sqrt{-840}) = (\sqrt{3}+\sqrt{5})^{12}\,(1+\sqrt{2})^6 \qquad m = 840$$

$$(1+\sqrt{3})^6\,(1+\sqrt{5})^6\,(3+\sqrt{7})^6\,(3+\sqrt{10})^6$$

$$(\sqrt{2}+\sqrt{3})^6\,(\sqrt{5}+\sqrt{7})^6\,(\sqrt{6}+\sqrt{7})^6$$

$$(\sqrt{14}+\sqrt{15})^3\,(3\sqrt{3}+2\sqrt{7})^2\,(5\sqrt{5}+3\sqrt{14})^2,$$

$$2^{24} f_1(\sqrt{-1320})^{24} = (1+\sqrt{3})^{18}\,(1+\sqrt{5})^{12}\,(1+\sqrt{2})^6 \qquad m = 1320$$

$$(3+\sqrt{10})^6\,(3+\sqrt{11})^6\,(\sqrt{3}+\sqrt{5})^6\,(\sqrt{5}+\sqrt{6})^6$$

$$(\sqrt{11}+\sqrt{15})^6\,(3\sqrt{5}+2\sqrt{11})^6\,(4\sqrt{2}+\sqrt{33})^6$$

$$(3\sqrt{6}+\sqrt{55})^3\,(\sqrt{10}+\sqrt{11})^2,$$

$$2^{31} f(\sqrt{-1365})^{12} = (\sqrt{3}+\sqrt{7})^{12}\,(1+\sqrt{5})^6\,(3+\sqrt{7})^6 \qquad m = 1365$$

$$(3+\sqrt{13})^6\,(\sqrt{3}+\sqrt{5})^6\,(2\sqrt{3}+\sqrt{13})^6$$

$$(\sqrt{35}+\sqrt{39})^3\,(3\sqrt{7}+\sqrt{65})^2,$$

$$2^{21} f_1(\sqrt{-1848})^{24} = (1+\sqrt{3})^{12}\,(\sqrt{2}+\sqrt{3})^{12} \qquad m = 1848$$

$$(3+\sqrt{7})^{12}\,(3+\sqrt{11})^6\,(\sqrt{3}+\sqrt{7})^6\,(\sqrt{6}+\sqrt{7})^6$$

$$(\sqrt{7}+\sqrt{11})^6\,(2\sqrt{2}+\sqrt{7})^6\,(7\sqrt{2}+3\sqrt{11})^6$$

$$(5\sqrt{3}+\sqrt{77})^6\,(\sqrt{21}+\sqrt{22})^3\,(22\sqrt{22}+39\sqrt{7})^2.$$

Verlag von Friedrich Vieweg & Sohn in Braunschweig.

---

## Lehrbuch
der
## Differential-Gleichungen
von **Dr. Andrew Russell Forsyth,**
Professor am Trinity College zu Cambridge.
Mit einem Anhange: Die Resultate der im Lehrbuche angeführten Uebungsaufgaben enthaltend,
herausgegeben von **H. Maser.**
**Autorisirte Uebersetzung.** gr. 8. geh. Preis 14 ℳ.

---

## Anfangsgründe der geometrischen Disciplinen
für Gymnasien, Real- und Gewerbeschulen, sowie auch zum Selbstunterrichte bearbeitet von
**Dr. Joh. Müller,**
weil. Professor zu Freiburg im Breisgau.
**In drei Theilen.** gr. 8. geh.

Erster Theil: **Elemente der ebenen Geometrie und Stereometrie.** Vierte verbesserte und vermehrte Auflage bearbeitet von Dr. Hubert Müller, Professor, Oberlehrer am Kaiserlichen Lyceum in Metz. Mit 155 Holzstichen, einer Tafel mit 4 Maassstäben und 4 Transporteuren. Preis 1 ℳ. 60 ₰

Zweiter Theil: **Elemente der ebenen und sphärischen Trigonometrie.** Dritte verbesserte und vermehrte Auflage bearbeitet von Dr. Hubert Müller. Mit 25 Holzstichen und einer Tafel mit Netzen. Preis 1 ℳ. 20 ₰

Dritter Theil: **Elemente der analytischen Geometrie in der Ebene und im Raum.** Zweite verbesserte und vermehrte Auflage bearbeitet von Dr. Hubert Müller. Mit 93 Holzstichen. Preis 1 ℳ. 60 ₰

---

## Die Praxis
der
## Methode der kleinsten Quadrate
für die Bedürfnisse der Anfänger bearbeitet von
**W. von Freeden.**

Erster Theil: Elementare Darstellung der Methode nebst Sammlung vollständig berechneter physikalischer, meteorologischer, geodätischer und astronomischer Aufgaben, welche auf lineare und transcendente Gleichungen führen. gr. 8. geh. Preis 3 ℳ.

---

(925)