Persistenter Identifier:	1580294371950_1
Titel:	Vorlesungen über die singulären Moduln und die komplexe Multiplikation der elliptischen Funktionen
Autor:	Fueter, Rudolf
Ort:	Leipzig
Datierung:	1924
Beschriftungen:	Elliptische Funktion
Signatur:	1H 90-41,1
Strukturtyp:	volume
Lizenz:	https://creativecommons.org/licenses/by-sa/4.0/
PURL:	https://digibus.ub.uni-stuttgart.de/viewer/image/1580294371950_1/1/

B. G. TEUBNERS SAMMLUNG VON
AUF DEM GEBIETE DER
MATHEMATISCHEN WISSENSCHAFTEN
MIT EINSCHLUSS IHRER ANWENDUNGEN
BAND XLI, 1

VORLESUNGEN ÜBER DIE SINGULÄREN MODULN UND DIE KOMPLEXE MULTIPLIKATION DER ELLIPTISCHEN FUNKTIONEN

VON
(Rudolf)
DR. R. FUETER
PROFESSOR AN DER UNIVERSITÄT
ZÜRICH

ERSTER TEIL

MIT 16 FIGUREN IM TEXT

VERLAG UND DRUCK VON B. G. TEUBNER · LEIPZIG · BERLIN 1924

Vorwort.

Historisches: Die komplexe Multiplikation der elliptischen Funktionen ist mit genialem Blick von *Niels Henrik Abel* erkannt worden. In seinen „Recherches sur les fonctions elliptiques", die in Crelles Journal 1827/28 erschienen sind, hat er für die lemniscatische Funktion $x = \varphi(\delta)$ die erste komplexe Multiplikationsformel aufgestellt[1]):

$$\varphi((2+i)\delta) = ix\frac{(1-2i)-x^4}{1-(1-2i)x^4}, \quad i = \sqrt{-1}, \quad x = \varphi(\delta),$$

und die Teilungsgleichungen in bezug auf den Körper $k(\sqrt{-1})$ angegeben. Allgemein erkannte er[2]), daß die elliptische Funktion nur für Zahlen eines imaginär-quadratischen Zahlkörpers komplexe Multiplikation zuläßt. Für die Multiplikatoren $\sqrt{-3}$ und $\sqrt{-5}$ führte er die Rechnung durch. Abel behauptete auch, daß die Teilungsgleichungen dadurch ausgezeichnet seien, daß die Moduln der zugehörigen elliptischen Funktionen durch Radikale auflösbar seien.[3]) Diese Entdeckung wird immer eine der schönsten sein, die Abels wunderbarem Geiste geglückt sind.

Abels Untersuchungen führten notgedrungen dazu, zuerst die elliptischen Modulfunktionen im „singulären" Falle, das heißt für quadratisch-imaginäre Werte des Periodenverhältnisses zu behandeln. Dies ist von *Leopold Kronecker* geschehen. In zwei Abhandlungen der Berliner Akademie aus den Jahren 1857 und 1862[4]) teilte er eine überraschende Fülle von den allerschönsten und merkwürdigsten Eigenschaften der singulären Moduln mit, die mit einem Schlage in die tiefsten Fragen der höheren Algebra und Zahlentheorie hineinführten. Damit war die komplexe Multiplikation in den Mittelpunkt von *Funktionentheorie, Algebra und Zahlentheorie* gerückt. Ihr Einfluß, speziell auf die Arithmetik, war gewaltig.[5])

1) *N. H. Abel:* Oeuvres complètes, nouvelles édition, t. 1, Christiania, 1881, pg. 354.

2) ibid. pg. 377 u. ff.

3) *N. H. Abel:* Solution d'un problème général concernant la transformation des fonctions elliptiques. 1828, Oeuvres complètes, a. a. O. pg. 425/26.

4) *L. Kronecker:* Über elliptische Funktionen, für welche komplexe Multiplikation stattfindet. Monatsberichte der Berl. Akad. 1857, S. 455. Berlin 1858. Über die komplexe Multiplikation der elliptischen Funktionen, Monatsberichte der Berliner Akad. 1862, S. 363. Berlin 1863.

5) *Fueter:* Die Klassenkörper der komplexen Multiplikation und ihr Einfluß auf die Entwicklung der Zahlentheorie, Jahresber. der D. Math.-Vereinig. Bd. 20. 1911, S. 1.

Leider hat Kronecker seine Untersuchungen über die zu diesen singulären Moduln gehörenden elliptischen Funktionen nicht veröffentlicht. In einer großen Reihe von Mitteilungen an die Berliner Akademie: „Zur Theorie der elliptischen Funktionen" hat er den Fall reeller Multiplikatoren behandelt. Nur vereinzelt ist er auf den singulären Fall zurückgekommen, so 1877, um aus allgemeinen Überlegungen den Satz nochmals zu beweisen, daß die Gruppe der Gleichungen der singulären Moduln Abelsch sei.[1])

Diese Lücke ist von *Heinrich Weber* ausgefüllt worden. Seine Leistung muß als sehr groß bezeichnet werden. Nicht nur hat er die Abel-Kroneckerschen Resultate über singuläre Moduln in einem Lehrbuch[2]) verarbeitet, ergänzt und systematisiert, sondern auch die Kroneckerschen Arbeiten über elliptische Funktionen zur Darstellung der komplexen Multiplikation ausgebaut.[3]) Alles Gewonnene hat er im dritten Bande seiner Algebra dargestellt.[4]) Betrachtet man das, was *vor* Weber war, mit seinem Gebäude, so muß man seine bedeutende Leistung bewundern.

Eine weitere Aufgabe, der sich ganz besondere Schwierigkeiten entgegenstellen, ist die numerische Berechnung der Gleichungen, denen die singulären Moduln genügen. Die theoretisch einfachsten Wege sind fast durchgängig praktisch nicht durchführbar. Die Überwindung dieser Schwierigkeiten brachten in erster Linie die durch ihre klassische Schönheit hervorragenden Arbeiten von *Hermite*[5]) und seiner Schule.

Die ganze Theorie der komplexen Multiplikation der elliptischen Funktionen wird gekrönt durch den Satz, *daß die singulären elliptischen Funktionswerte alle in einem quadratisch-imaginären Körper als Rationalitätsbereich Abelschen Gleichungen erzeugen (Vollständigkeitssatz).* Dieser Satz wird in diesem Buche zum ersten Male bewiesen werden. Es ist von mir[6]) bisher nur der Satz bewiesen worden, daß die singulären Moduln mit den Einheitswurzeln zusammen, alle in einem quadratisch-imaginären Körper Abelschen Gleichungen ergeben. Dabei fehlten noch gewisse Quadratwurzeln. Letztere Lücke wurde seither durch *Takagi*[7]) ausgefüllt. Die singulären elliptischen Werte ergeben jedoch direkt die

1) *L. Kronecker:* Über Abelsche Gleichungen. Sitz.-Ber. der Berl. Akad. 1877, S. 845, Berlin 1878. Einen Beweis der Irreduzibilität der Gleichung der singulären Moduln und ihrer Gruppe erbrachte auch *Pick:* Über die komplexe Multiplikation der elliptischen Funktionen, Math. Annalen, Bd. 25 (1885) u. Bd. 26 (1886).

2) *H. Weber:* Elliptische Funktionen u. algebraische Zahlen. Braunschweig 1891.

3) *H. Weber:* Über Zahlengruppen in algebraischen Körpern. Math. Ann. Bd. 48 (1897), S. 433, Bd. 49 (1897), S. 83, Bd. 50 (1898), S. 1.

4) *H. Weber:* Lehrbuch der Algebra. Bd. 3, Vieweg, Braunschweig 1908.

5) *Charles Hermite:* Sur la théorie des équations modulaires. Oeuvres, t. 2, pg. 38, Paris 1908.

6) *R. Fueter:* Abelsche Gleichungen in quadratisch-imaginären Zahlkörpern. Math. Annalen, Bd. 75 (1914), S. 177.

7) *T. Takagi:* Über eine Theorie des relativ Abelschen Zahlkörpers. Journal of the College of Science, Tokyo Imperial University. Vol. 41, Art. 9 (1920).

aus jenen Irrationalitäten zusammengesetzten Größen. Damit ist erst die wirkliche Bedeutung der komplexen Multiplikation gezeigt und das wirkliche Analogon zum Kroneckerschen Satze über Einheitswurzeln dargetan.

Der vorliegende erste Teil, der aus meinen Vorlesungen entsprungen ist, beginnt mit der independenten Darstellung der Theorie der elliptischen Modulfunktionen. Gegenüber *Hurwitz*[1]) gelang es mir, Vereinfachungen zu erzielen. Auch die anschließende Theorie der Transformationsgleichungen scheint mir durch konsequente Benutzung der gruppentheoretischen Begriffe gewonnen zu haben.[2]) Ich habe mich lange gefragt, ob meine von derjenigen der Gruppentheoretiker abweichende Darstellung zweier aufeinanderfolgenden Operationen durch $S_2 S_1$ statt $S_1 S_2$ erlaubt sei, habe sie dann doch beibehalten, da sie mir für die funktionentheoretische Anwendung die einzig Gegebene scheint.

Die Theorie der singulären Moduln ist ganz neu dargestellt, indem die quadratischen *Formen* ganz beiseite gelassen wurden, und direkt der quadratische *Körper* zugezogen wurde. Dadurch wird alles enorm vereinfacht und systematisiert. Auch in vielen Einzelheiten wird man gegenüber der *Weber*schen Darstellung neue, und wie ich hoffe, vereinfachte Methoden finden.

Die Theorie der komplexen Multiplikation gründe ich einzig auf die Weierstraßsche $\wp$-Funktion. Die Entwicklung ihrer Eigenschaften und ihrer Multiplikationsformeln geht in völliger Analogie mit derjenigen der Modulfunktionen vor sich. Aus ihr folgt auch die für die zahlentheoretischen und algebraischen Untersuchungen grundlegende Funktion $\mathfrak{T}(z)$, die von *Jacobi*[3]) herrührt, und schon von *Kronecker* und *Weber* benutzt wurde. Ihren Modul kann man mit Hilfe der *Gauß*schen Transformation überraschend einfach mit der vollständigen Invariante in Verbindung bringen.

Die komplexe Multiplikation bringt zum ersten Male die Teilung auch durch *gerade* komplexe Zahlen, sowie den Beweis des Satzes, daß die Gruppe der Teilungsgleichungen *Abel*sch sei. Der Zusammenhang mit dem quadratischen Körper scheint mir nun vollständig klargelegt zu sein. Auf die bemerkenswerte Analogie mit den Körpern der Einheitswurzeln brauche ich wohl nicht besonders hinzuweisen.

Dieser erste Teil bringt den funktionentheoretischen und algebraischen Abschnitt. Er setzt nur die Elemente der Funktionentheorie, Algebra und Zahlentheorie voraus. Was vom quadratischen Körper zu

---

1) *A. Hurwitz:* Über die Theorie der elliptischen Modulfunktionen. Math. Annalen, Bd. 58, Leipzig 1904, S. 343.

2) Siehe das umfassende Werk: *F. Klein — R. Fricke:* Vorlesungen über die Theorie der elliptischen Modulfunktionen, 2. Bd., Leipzig 1890—92.

3) *Jacobi:* „Suite des notices sur les fonctions elliptiques", Werke, Bd. 1, pg. 266 und: „De multiplicatione functionum ellipticarum per quantitatem imaginariam pro certo quodam modulorum systemate", Werke, Bd. 1, pg. 489.

wissen nötig ist, wird in einem besonderen Abschnitt dargestellt. Der zweite Teil wird die zahlentheoretische Behandlung der Körper der komplexen Multiplikation und die numerische Berechnung der Gleichungen enthalten.

Für Durchlesen der Korrekturen und mannigfaltige Anregungen habe ich Herrn Prof. Dr. *Speiser* herzlich zu danken. Besonderen Dank verdient auch Herr cand. phil. *Max Gut*, der das ganze Manuskript durchgearbeitet, und mich auf verschiedene Mängel aufmerksam gemacht hat. Auch im Lesen der Korrekturen hat er mich aufs beste unterstützt. Dem Verlage danke ich für die trotz den ungünstigen Zeiten erfolgte Drucklegung.

Zürich, im Dezember 1923.

Rudolf Fueter.

Inhaltsverzeichnis.

Vorlesungen über die singulären Moduln und die komplexe Multiplikation der elliptischen Funktionen.

I. Die elliptische Modulfunktion.

1. Die Modulgruppe und ihre Untergruppen.

Sind $\alpha, \beta, \gamma, \delta$ irgend vier Zahlen, zwischen denen die Relation:

$$\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = \alpha\delta - \beta\gamma = +1 \tag{1}$$

besteht, so läßt sich eine Operation:

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

definieren, die eine komplexe Variable z in:

$$w = \frac{\alpha z + \beta}{\gamma z + \delta}$$

überführt. Wir schreiben kurz $w = Sz$ und nennen S eine *lineare Substitution*. Eine solche ändert sich nicht, wenn jede der vier Zahlen $\alpha, \beta, \gamma, \delta$ in ihre entgegengesetzte verwandelt wird. Zwei Substitutionen heißen somit gleich, wenn jede der vier Zahlen $\alpha, \beta, \gamma, \delta$ in beiden dieselbe oder die entgegengesetzte Zahl ist. S heißt *„unimodular"*, weil der *„Modul"* $\alpha\delta - \beta\gamma$ nach (1) die Einheit ist. Alle S bilden eine *Gruppe*. Dazu ist erforderlich:

a) Es gibt die Einheitssubstitution $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, für die

$$Ez = z.$$

b) Jedes S besitzt ein inverses S^{-1}, für das:

$$S^{-1}(Sz) = z.$$

In der Tat wird für $S^{-1} = \begin{pmatrix} -\delta & \beta \\ \gamma & -\alpha \end{pmatrix}$:

$$S^{-1}(Sz) = \frac{-\delta(Sz) + \beta}{\gamma(Sz) - \alpha} = \frac{-\delta\dfrac{\alpha z + \beta}{\gamma z + \delta} + \beta}{\gamma\dfrac{\alpha z + \beta}{\gamma z + \delta} - \alpha} = \frac{-\delta(\alpha z + \beta) + \beta(\gamma z + \delta)}{\gamma(\alpha z + \beta) - \alpha(\gamma z + \delta)} = z.$$

Außerdem ist S^{-1} wieder unimodular, da:

$$\begin{vmatrix} -\delta & \beta \\ \gamma & -\alpha \end{vmatrix} = \alpha\delta - \beta\gamma = 1.$$

c) Sind zwei Substitutionen S_1 und S_2 gegeben, und übt man auf

$$w_1 = S_1 z = \frac{\alpha_1 z + \beta_1}{\gamma_1 z + \delta_1}, \quad \alpha_1\delta_1 - \beta_1\gamma_1 = 1,$$

die Substitution S_2 aus, und setzt $w_2 = S_2 w_1$:

$$w_2 = S_2 w_1 = \frac{\alpha_2 w_1 + \beta_2}{\gamma_2 w_1 + \delta_2}, \quad \alpha_2\delta_2 - \beta_2\gamma_2 = 1,$$

so muß es ein S geben, für das:

$$w_2 = Sz.$$

In der Tat ist:

$$w_2 = \frac{\alpha_2(\alpha_1 z + \beta_1) + \beta_2(\gamma_1 z + \delta_1)}{\gamma_2(\alpha_1 z + \beta_1) + \delta_2(\gamma_1 z + \delta_1)} = \frac{(\alpha_2\alpha_1 + \beta_2\gamma_1)z + (\alpha_2\beta_1 + \beta_2\delta_1)}{(\gamma_2\alpha_1 + \delta_2\gamma_1)z + (\gamma_2\beta_1 + \delta_2\delta_1)}, \text{ also:}$$

$$S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \alpha_2\alpha_1 + \beta_2\gamma_1 & \alpha_2\beta_1 + \beta_2\delta_1 \\ \gamma_2\alpha_1 + \delta_2\gamma_1 & \gamma_2\beta_1 + \delta_2\delta_1 \end{pmatrix} \tag{2}$$

und

$$\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = \begin{vmatrix} \alpha_2\alpha_1 + \beta_2\gamma_1 & \alpha_2\beta_1 + \beta_2\delta_1 \\ \gamma_2\alpha_1 + \delta_2\gamma_1 & \gamma_2\beta_1 + \delta_2\delta_1 \end{vmatrix} = \begin{vmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{vmatrix} \begin{vmatrix} \alpha_2 & \beta_2 \\ \gamma_2 & \delta_2 \end{vmatrix} = 1.$$

Man schreibt diese wichtigste Gruppeneigenschaft symbolisch:

$$S = S_2 S_1.$$

d) Bei Zusammensetzung von drei und mehr Substitutionen gilt das *assoziative* Gesetz.

Alle vier Eigenschaften bleiben erhalten, wenn man die $\alpha, \beta, \gamma, \delta$ der weiteren Bedingung unterwirft, daß sie *reelle* Zahlen sind. Diese reellen Substitutionen bilden daher ebenfalls eine Gruppe, die nach *Poincaré* die *Fuchs*sche Gruppe genannt wird.

Wir wollen noch eine weitergehende, und zwar *zahlentheoretische* Einschränkung vornehmen und festsetzen, daß die $\alpha, \beta, \gamma, \delta$ *ganze, rationale Zahlen* seien. Dies ist von allergrößter Tragweite, da damit zahlentheoretische Überlegungen in den Bereich funktionentheoretischer Untersuchungen gezogen werden.

Auch bei dieser Einschränkung bleiben die Eigenschaften a), b), c), d) erhalten; denn beim Beweise treten nur ganze, ganzzahlige rationale Funktionen der $\alpha, \beta, \gamma, \delta$ auf:

1. Satz: *Die linearen, unimodularen Substitutionen mit ganzen Koeffizienten bilden eine Gruppe.*

Dieselbe heißt die *Modulgruppe* $\mathfrak{G}$. Sie enthält unendlich viele Substitutionen, da $\alpha\delta - \beta\gamma = 1$ unendlich viele ganzzahlige Lösungen besitzt.

Nimmt man von den Substitutionen der Modulgruppe nur solche, die einer weiteren Bedingung genügen, so sagt man, sie bilden eine *Untergruppe von* $\mathfrak{G}$, wenn sie für sich allein schon die Bedingungen a), b), c), d) erfüllen. Eine solche kann endlich oder unendlich viele S enthalten; z. B. bilden:

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

eine Untergruppe, da $S \cdot S = E$,

wie (2) ergibt; es ist: $Sz = -\frac{1}{z}$, $SSz = -\frac{1}{-\frac{1}{z}} = z$.

Eine besonders wichtige Untergruppe ist die folgende: Es sei n eine beliebige, ganze, rationale, positive Zahl, > 1; dann sollen nur diejenigen $S^{(n)}$ betrachtet werden, für die:

$$\alpha \equiv \delta \equiv \pm 1, \quad \beta \equiv \gamma \equiv 0 \pmod{n}. \tag{3}$$

Die Einheitssubstitution E genügt dieser Bedingung, ebenso auch $S^{(n)-1}$, falls ihr $S^{(n)}$ genügt. Durch Zusammensetzung von $S_1^{(n)}$ und $S_2^{(n)}$, die (3) befriedigen, erhält man ein $S^{(n)}$ derselben Eigenschaft; denn ist:

$$S_1^{(n)} = \begin{pmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{pmatrix}, \quad S_2^{(n)} = \begin{pmatrix} \alpha_2 & \beta_2 \\ \gamma_2 & \delta_2 \end{pmatrix}$$

und
$$\alpha_1 \equiv \delta_1 \equiv \pm 1, \quad \alpha_2 \equiv \delta_2 \equiv \pm 1 \pmod{n},$$
$$\beta_1 \equiv \gamma_1 \equiv \beta_2 \equiv \gamma_2 \equiv 0 \pmod{n},$$

so folgt aus (2):

$$\alpha_2\alpha_1 + \beta_2\gamma_1 \equiv \gamma_2\beta_1 + \delta_2\delta_1 \equiv \pm 1 \pmod{n};$$
$$\alpha_2\beta_1 + \beta_2\delta_1 \equiv \gamma_2\alpha_1 + \delta_2\gamma_1 \equiv 0 \pmod{n};$$

alle $S^{(n)}$ bilden daher eine Untergruppe von $\mathfrak{G}$, die *Kongruenzgruppe n^{ter} Stufe* $\mathfrak{G}^{(n)}$ heißt. Sie besitzt eine wichtige Eigenschaft in bezug auf $\mathfrak{G}$; es gibt endlich viele Substitutionen von $\mathfrak{G}$,

$$s_1 = E, s_2, s_3, \ldots s_m,$$

mit der Eigenschaft, daß jedes S der Modulgruppe $\mathfrak{G}$ in der Form darstellbar ist:

$$S = s_i S^{(n)}. \qquad (i = 1, 2, \ldots m)$$

Ist μ der kleinste Wert von m, so heißt μ der *Index von* $\mathfrak{G}^{(n)}$. Die Untergruppe $\mathfrak{G}^{(n)}$ ist daher von *endlichem Index*.

Diese Tatsache ist grundlegend für das Folgende und soll daher bewiesen werden. μ ist die zu berechnende zahlentheoretische Funktion $\mu = \mu(n)$.

Wir nennen zwei Substitutionen S_1 und S_2 von $\mathfrak{G}$ kongruent (mod. n),

$$S_1 \equiv S_2 \pmod{n},$$

falls: $\alpha_1 \equiv \pm \alpha_2$, $\beta_1 \equiv \pm \beta_2$, $\gamma_1 \equiv \pm \gamma_2$, $\delta_1 \equiv \pm \delta_2$, (mod. n).

Alle $S^{(n)}$ sind dann definiert durch:

$$S^{(n)} \equiv E = s_1 \pmod{n}, \quad E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Es sei s_2 irgendein S von $\mathfrak{G}$, $\not\equiv E \pmod{n}$; dann ist auch $s_2 S^{(n)} \not\equiv E \pmod{n}$; denn aus (2) folgt:

$$s_2 S^{(n)} \equiv s_2 E \equiv s_2 \pmod{n}.$$

Dies gilt für jedes $S^{(n)}$ von $\mathfrak{G}^{(n)}$. Sind durch $S^{(n)}$ und $s_2 S^{(n)}$ alle S von $\mathfrak{G}$ erschöpft, so ist $\mu = 2$. Andernfalls gibt es ein nicht darin enthaltenes s_3. Dann ist $s_3 \not\equiv s_2 \pmod{n}$, da sonst $s_3 s_2^{-1}$ in $\mathfrak{G}^{(n)}$ wäre. Also ist auch: $s_3 S^{(n)} \not\equiv s_2 S^{(n)} \pmod{n}$,

und alle Substitutionen $S^{(n)}$, $s_2 S^{(n)}$, $s_3 S^{(n)}$ sind voneinander verschiedene S von $\mathfrak{G}$. Sind damit alle erschöpft, so ist $\mu = 3$. Andernfalls fährt man in dieser Weise fort, durch Aufstellung von $s_4, s_5, \ldots$, wobei stets $s_i \not\equiv s_h \pmod{n}$ $(i \neq h)$ ist. Nun gibt es nur endlich viele inkongruente $s_i \pmod{n}$. Also ist der Index μ *endlich*.

Sind umgekehrt s_1 und s_2 zwei inkongruente Matrizen von $\mathfrak{G} \pmod{n}$, so finden sich unter allen $s_1 S^{(n)}$ und $s_2 S^{(n)}$ dann und nur dann zwei gleiche, wenn:

$$s_2 = s_1 S^{(n)} = \begin{pmatrix} \alpha_1 \beta_1 \\ \gamma_1 \delta_1 \end{pmatrix} \begin{pmatrix} \alpha^{(n)} \beta^{(n)} \\ \gamma^{(n)} \delta^{(n)} \end{pmatrix} = \begin{pmatrix} \alpha_1 \alpha^{(n)} + \beta_1 \gamma^{(n)} & \alpha_1 \beta^{(n)} + \beta_1 \delta^{(n)} \\ \gamma_1 \alpha^{(n)} + \delta_1 \gamma^{(n)} & \gamma_1 \beta^{(n)} + \delta_1 \delta^{(n)} \end{pmatrix}.$$

Dies ist nur möglich, wenn:

$$\begin{aligned} \alpha_2 &= \pm (\alpha_1 \alpha^{(n)} + \beta_1 \gamma^{(n)}) \equiv \pm \alpha_1 \pmod{n}, \\ \beta_2 &= \pm (\alpha_1 \beta^{(n)} + \beta_1 \delta^{(n)}) \equiv \pm \beta_1 \pmod{n}, \\ \gamma_2 &= \pm (\gamma_1 \alpha^{(n)} + \delta_1 \gamma^{(n)}) \equiv \pm \gamma_1 \pmod{n}, \\ \delta_2 &= \pm (\gamma_1 \beta^{(n)} + \delta_1 \delta^{(n)}) \equiv \pm \delta_1 \pmod{n}. \end{aligned}$$

Ist $n = 2$, so gilt für jede Zahl $r \equiv -r \pmod{n}$, also für die Matrizen:

$$s_1 \equiv s_2 \pmod{2}.$$

Ist dagegen $n \neq 2$, so gibt es, da $\alpha, \beta, \gamma, \delta$ bei geradem n niemals alle durch $\frac{1}{2}n$ teilbar sind, wegen (1), zwei inkongruente Matrizen:

$$s_1 = \begin{pmatrix} \alpha_1 \beta_1 \\ \gamma_1 \delta_1 \end{pmatrix}, \quad s_2 = \begin{pmatrix} -\alpha_1 & -\beta_1 \\ -\gamma_1 & -\delta_1 \end{pmatrix},$$

für die die Substitution dieselbe ist: $\mu(2)$ und $2\mu(n)$ $(n > 2)$ *ist die Anzahl der inkongruenten Matrizen s der Modulgruppe.*

Zerlegt man n in zwei teilerfremde Faktoren $\neq 2$, $n = n_1 n_2$, so ist:

$$2\mu(n) = 2\mu(n_1) \cdot 2\mu(n_2).$$

Denn nimmt man eine der $2\mu(n_1)$ inkongruenten $s^{(n_1)} = \begin{pmatrix} \alpha \beta \\ \gamma \delta \end{pmatrix}$, wo $\alpha\delta - \beta\gamma = 1$ ist, so darf man $\alpha, \beta, \gamma, \delta$ stets so wählen, daß:

$$s^{(n_1)} \equiv E \pmod{n_2},$$

da wegen der Teilerfremdheit von n_1 und n_2 vier Zahlen $\alpha, \beta, \gamma, \delta$ existieren, für die:

$$\begin{matrix} \alpha \equiv \delta \equiv 1 \\ \beta \equiv \gamma \equiv 0 \end{matrix} \pmod{n_2} \qquad \begin{matrix} \alpha \equiv \alpha\,, & \beta \equiv \beta \\ \gamma \equiv \gamma\,, & \delta \equiv \delta \end{matrix} \pmod{n_1}.$$

Diese Zahlen genügen der Kongruenz:

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

γ und δ haben keinen Teiler mit n gemein, und da sie nur (mod. n) bestimmt sind, kann man sie so wählen, daß auch:

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

ist. Man kann jetzt statt $s^{(n_1)}$ die Matrix $\bar{s}^{(n_1)} = \begin{pmatrix} \alpha & \bar{\beta} \\ \bar{\gamma} & \bar{\delta} \end{pmatrix}$ wählen, für die:

$$\bar{s}^{(n_1)} \equiv s^{(n_1)} \pmod{n_1},$$
$$\bar{s}^{(n_1)} \equiv E \pmod{n_2}.$$

Ebenso bildet man das System von $2\mu(n_2)$ inkongruenten Matrizen $s^{(n_2)}$, für die: $s^{(n_2)} \equiv E \pmod{n_1}$.

Die $2\mu(n_1) \cdot 2\mu(n_2)$ Matrizen $s^{(n_1)} \cdot s^{(n_2)}$ sind dann inkongruent (mod. n), also: $2\mu(n_1) \cdot 2\mu(n_2) \leqq 2\mu(n)$.

Anderseits läßt sich jedes s in der Form darstellen:

$$s \equiv s^{(n_1)} \cdot s^{(n_2)} \pmod{n},$$

weil jedes s (mod. n) einem $s^{(n_1)}$ (mod. n_1) und einem $s^{(n_2)}$ (mod. n_2) kongruent sein muß. Also ist auch:

$$2\mu(n) \leqq 2\mu(n_1) \cdot 2\mu(n_2).$$

Es ist also nur das Gleichheitszeichen möglich.

Setzt man daher $n = 2^{r_0} p_1^{r_1} \cdot p_2^{r_2} \ldots p_h^{r_h}$, wo $p_1, p_2, \ldots p_h$ voneinander verschiedene ungerade Primzahlen sind, so ist:

$$2\mu(n) = \begin{cases} 2\mu(p^{r_1}) \cdot 2\mu(p^{r_2}) \ldots 2\mu(p^{r_h}), & r_0 = 0; \\ \mu(2) \cdot 2\mu(p^{r_1}) \ldots 2\mu(p^{r_h}), & r_0 = 1; \quad (h > 0) \\ 2\mu(2^{r_0}) \cdot 2\mu(p^{r_1}) \ldots 2\mu(p^{r_h}), & r_0 > 1\,. \end{cases}$$

Es bleibt daher nur noch $\mu(p^r)$ zu berechnen. Geben wir in $s = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ α alle $(p^r - p^{r-1})$ zu p teilerfremden inkongruenten Werte (mod. p^r), β p^r zu α teilerfremde inkongruente Werte (mod. p^r), so machen das $p^r(p^r - p^{r-1})$ Zahlenpaare (α, β). Durchläuft α die p^{r-1} Vielfachen von p zwischen 0 und p^r, so kann β nur $(p^r - p^{r-1})$ teilerfremde Reste (mod. p^r) durchlaufen. Dadurch werden noch weitere $p^{r-1}(p^r - p^{r-1})$ Zahlenpaare (α, β) erhalten, zusammen:

$$p^r(p^r - p^{r-1}) + p^{r-1}(p^r - p^{r-1}) = p^{2r-2}(p^2 - 1)$$

inkongruente teilerfremde Paare (α, β). Zu diesen bestimmen wir aus $\alpha\delta - \beta\gamma = 1$, γ und δ. Aus einer Lösung γ, δ ergeben sich alle (mod. p^r) inkongruenten, indem in $\gamma + \alpha t$, $\delta + \beta t$, t ein Restsystem (mod. p^r), also p^r Zahlen durchläuft. Somit erhält man:

$$2\mu(p^r) = p^{3r-2}(p^2-1)$$

und:

$$\mu(n) = \tfrac{1}{2} \prod_{(p)} p^{3r-2}(p^2-1). \qquad (n+2)$$

Ist $r_0 = 1$, so ist $2\mu(2)$ durch $\mu(2)$ zu ersetzen, und es bleibt alles gleich. Ist $n = 2$, so muß auch $2\mu(n)$ durch $\mu(n)$ ersetzt werden, und es ist:

$$\mu(2) = 2^{3-2}(2^2-1) = 6.$$

Die sechs Substitutionen s sind z. B.:

$$s_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ s_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ s_3 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},\ s_4 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ s_5 = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix},\ s_6 = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}.$$

2. Der Diskontinuitätsbereich der Modulgruppe.

Jede Substitution S:

$$w = Sz = \frac{\alpha z + \beta}{\gamma z + \delta}, \quad \alpha\delta - \beta\gamma = 1,$$

vermittelt eine konforme Abbildung der Ebene z in sich. Denn w ist eine analytische Funktion von z, deren Differentialquotient:

$$\frac{dw}{dz} = \frac{\alpha\delta - \beta\gamma}{(\gamma z + \delta)^2} = \frac{1}{(\gamma z + \delta)^2}$$

nur im Punkt $z = \infty$ Null wird, falls $\gamma \neq 0$ ist. Setzt man in diesem Falle $z = \frac{1}{\zeta}$, so wird:

$$w = \frac{\alpha + \beta\zeta}{\gamma + \delta\zeta}, \quad \frac{dw}{d\zeta} = -\frac{1}{(\gamma + \delta\zeta)^2}, \quad \left(\frac{dw}{d\zeta}\right)_{\zeta=0} = -\frac{1}{\gamma^2}, \quad \gamma \neq 0,$$

und die Abbildung ist auch in $z = \infty$ konform. Entsprechend wird für

$$z = -\frac{\delta}{\gamma},\ \gamma \neq 0\colon\ w = \infty,\ \frac{1}{w} = 0 \text{ und } \left(\frac{d\frac{1}{w}}{dz}\right)_{z=-\frac{\delta}{\gamma}} = -\gamma^2 \neq 0.$$

Es liege S in $\mathfrak{G}$; dann geht durch $w = Sz$ die reelle Achse in sich über; wegen der Stetigkeit muß daher die obere Halbebene und entsprechend die untere Halbebene in sich oder in die andere übergehen. Setzt man $z = x + iy$, $w = u + iv$ (i die imaginäre Einheit), so ist:

$$u + iv = \frac{\alpha(x+iy) + \beta}{\gamma(x+iy) + \delta} = \frac{(\alpha(x+iy) + \beta)(\gamma(x-iy) + \delta)}{(\gamma x + \delta)^2 + \gamma^2 y^2},$$

$$v = \frac{y}{(\gamma x + \delta)^2 + \gamma^2 y^2}.$$

v und y haben gleiches Vorzeichen. *Die obere und entsprechend die untere Halbebene gehen in sich über.*

2. Satz: *Bei der Abbildung $w = Sz$ gehen Kreise und Geraden in Kreise oder Geraden über.*

Denn aus der eben gefundenen Relation folgt:

$$u = \frac{\alpha\gamma(x^2+y^2)+(\alpha\delta+\beta\gamma)x+\beta\delta}{\gamma^2(x^2+y^2)+2\gamma\delta x+\delta^2}, \quad v = \frac{y}{\gamma^2(x^2+y^2)+2\gamma\delta x+\delta^2},$$

$$u^2+v^2 = \frac{\alpha^2(x^2+y^2)+2\alpha\beta x+\beta^2}{\gamma^2(x^2+y^2)+2\gamma\delta x+\delta^2}.$$

Die rechten Seiten sind lineare Funktionen von x, y, x^2+y^2, die Nenner sind gleich. Daher geht jede Gleichung

$$A(u^2+v^2)+Bu+Cv+D=0$$

in eine Gleichung der Form über:

$$\bar{A}(x^2+y^2)+\bar{B}x+\bar{C}y+\bar{D}=0.$$

Punkte, die sich bei der Abbildung nicht verändern, heißen *Fixpunkte*. Es kann höchstens zwei Fixpunkte geben, da sie aus der Bedingungsgleichung:

$$z = \frac{\alpha z+\beta}{\gamma z+\delta}, \quad \gamma z^2+(\delta-\alpha)z-\beta=0$$

folgen. Die Diskriminante der quadratischen Gleichung ist:

$$(\alpha-\delta)^2+4\beta\gamma = (\alpha+\delta)^2-4(\alpha\delta-\beta\gamma) = (\alpha+\delta)^2-4.$$

Je nachdem sie negativ, Null oder positiv ist, sagt man, S sei *elliptisch, parabolisch* oder *hyperbolisch*.

a) Elliptischer Typus. $(\alpha+\delta)^2-4<0$. Da α, β, γ, δ ganze, rationale Zahlen sind, kann $(\alpha+\delta)^2-4$ nur -4 oder -3 sein, d. h. $(\alpha+\delta)^2=0$ oder 1 sein. Im ersteren Falle ergeben sich die beiden Fixpunkte aus:

$$z_{1,2} = \frac{\alpha \pm i}{\gamma}.$$

Ist dagegen $\alpha+\delta = (\pm 1)$, so wird:

$$z_{1,2} = \frac{\alpha-\delta\pm\sqrt{3}\,i}{2\gamma} = \frac{\alpha+(\pm 1)\frac{-1\pm\sqrt{3}\,i}{2}}{\gamma} = \frac{\alpha+(\pm 1)e^{\pm\frac{2\pi i}{3}}}{\gamma}.$$

In beiden Fällen ist $\gamma \neq 0$, da sonst $\alpha\delta=1$, $\alpha=\delta=\pm 1$ wäre. Die Fixpunkte liegen daher im endlichen, und nicht auf der reellen Achse. Zur genauen Diskussion führen wir eine Hilfs-ζ-Ebene ein:

$$\zeta = \frac{z-z_1}{z-z_2},$$

wo z_1 und z_2 die beiden Fixpunkte sind, denen jetzt die Werte $\zeta=0$ und $\zeta=\infty$ entsprechen. Dem Werte $w=Sz$ entspreche:

$$\bar{\zeta} = \frac{w-z_1}{w-z_2};$$

dann ist $\bar{\zeta} : \zeta$ eine in der ganzen Ebene endliche Größe, d. h. eine Konstante k:

$$\bar{\zeta} = k\zeta .$$

Zur Berechnung von k bedenke man, daß $\gamma \neq 0$ und für $z = \infty$, $w = \frac{\alpha}{\gamma}$ wird. Also ist wegen der quadratischen Gleichung, der z_1 und z_2 genügen,

$$\frac{\alpha - z_1\gamma}{\alpha - z_2\gamma} = k, \quad |k| = 1, \quad k = \frac{(\alpha - z_1\gamma)^2}{(\alpha - z_2\gamma)(\alpha - z_1\gamma)} = (\alpha - z_1\gamma)^2 .$$

Im Falle $\alpha = -\delta$ ist:

$$k = (\alpha - (\alpha \pm i))^2 = -1 .$$

Die doppelte Anwendung von S ergibt daher E. Man sagt, S sei vom Grade 2.

Im Falle $\alpha + \delta = (\pm 1)$, ist:

$$k = \left(\alpha - \left(\alpha + (\pm 1)\, e^{\pm \frac{2\pi i}{3}}\right)\right)^2 = e^{\mp \frac{2\pi i}{3}}, \quad k^3 = 1 .$$

k ist eine dritte Einheitswurzel, S vom Grade 3.

Das wichtigste Beispiel einer elliptischen Substitution ist $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $w = -\frac{1}{z}$, $z_{1,2} = \pm i$.

b) Parabolischer Typus. $(\alpha + \delta)^2 - 4 = 0$, $\alpha + \delta = \pm 2$. Ist $\gamma = 0$, so muß $\alpha = \delta = \pm 1$, β beliebig sein. Es wird:

$$S = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}, \quad w = z + \beta, \quad z_1 = \infty .$$

Ist $\gamma \neq 0$, so ist der einzige Fixpunkt:

$$z_1 = \frac{\alpha - \delta}{2\gamma} = \frac{\alpha \mp 1}{\gamma} ,$$

reell, rational und endlich. Setzt man in diesem Falle:

$$\zeta = \frac{1}{z - z_1}, \qquad \bar{\zeta} = \frac{1}{w - z_1} ,$$

so ist $\bar{\zeta} - \zeta$ in der ganzen Ebene endlich, d. h. eine Konstante k:

$$\bar{\zeta} = \zeta + k .$$

Zur Berechnung von k setzt man wieder $z = \infty$, $w = \frac{\alpha}{\gamma}$:

$$k = \frac{\gamma}{\alpha - \gamma z_1} = \frac{\gamma}{\alpha - (\alpha \pm 1)} = \pm\gamma, \quad \bar{\zeta} = \zeta \pm \gamma .$$

c) Hyperbolischer Typus. $(\alpha + \delta)^2 - 4 > 0$, $|\alpha + \delta| > 2$. Dann ist $\gamma \neq 0$, und z_1 und z_2 sind reelle, quadratische Zahlen. Wie im Falle a) wird:

$$\bar{\zeta} = k\zeta$$

und $k = (\alpha - z_1\gamma)^2 = \left(\alpha - \frac{\alpha - \delta + \sqrt{(\alpha+\delta)^2 - 4}}{2}\right)^2 = \left(\frac{\alpha + \delta - \sqrt{(\alpha+\delta)^2 - 4}}{2}\right)^2 .$

Die Größe $$\varepsilon = \frac{\alpha + \delta - \sqrt{(\alpha+\delta)^2 - 4}}{2}$$

ist eine Einheit des quadratischen Körpers von $\sqrt{(\alpha+\delta)^2-4}$. Denn ist ε' die konjugierte, so ist $\varepsilon \cdot \varepsilon' = 1$, und ε ist eine ganze Zahl, da es der ganzzahligen Gleichung:

$$\varepsilon^2 - (\alpha+\delta)\varepsilon + 1 = 0 \quad \text{genügt.}$$

Da $\varepsilon \neq \pm 1$ ist, so sind die Potenzen von ε alle voneinander verschieden und ergeben unendlich viele verschiedene Einheiten. Der Grad von S ist unendlich.

Wir werden uns von nun an darauf beschränken, die Abbildung in der oberen Halbebene zu betrachten. Die Verhältnisse in der unteren Halbebene sind symmetrisch zur reellen Achse und werden durch Spiegelung zu derselben erhalten. Der Untersuchung sei nicht nur ein S, sondern eine der Gruppen $\mathfrak{G}^{(n)}$ des § 1 zugrunde gelegt.

1. Definition: *Zwei Punkte z und $\bar{z}$ heißen ähnlich in bezug auf* $\mathfrak{G}$,

$$\bar{z} \sim z,$$

wenn es ein S von $\mathfrak{G}$ gibt, so daß:

$$\bar{z} = Sz.$$

Diese Definition ist sinnlos, wenn aus ihr nicht folgende Eigenschaften hervorgehen: Jeder Punkt ist sich selbst ähnlich; aus $\bar{z} \sim z$ folgt $z \sim \bar{z}$, und aus $\bar{z} \sim z$, $\bar{\bar{z}} \sim z$ folgt $\bar{\bar{z}} \sim \bar{z}$. Das erste verlangt, daß E in $\mathfrak{G}$ ist; das zweite, daß zu jedem S auch S^{-1} in $\mathfrak{G}$ liege; das dritte, daß ein S, das aus zwei S von $\mathfrak{G}$ zusammengesetzt ist, wieder in $\mathfrak{G}$ liege. Dies sind aber nichts anderes, wie die Gruppeneigenschaften a), b), c) von S. 1, die für $\mathfrak{G}$ nach Voraussetzung erfüllt sind. Die Ähnlichkeit ist die geometrische Auswertung des Gruppenbegriffes. Wir heben die eine Eigenschaft besonders hervor:

3. Satz: *Wenn zwei Punkte einem dritten ähnlich sind, so sind sie untereinander ähnlich.*

2. Definition: *Ein Bereich von Punkten mit der Eigenschaft, daß jeder Punkt der Ebene einem und nur einem Punkt desselben ähnlich ist in bezug auf die Gruppe $\mathfrak{G}$, heißt der Diskontinuitätsbereich von $\mathfrak{G}$.*

Nach der Definition kann kein Punkt des D.-B. einem seiner anderen Punkte ähnlich sein. Unsere Aufgabe wird es sein, den D.-B. für die Modulgruppe und ihre Untergruppen anzugeben.

Hierzu greifen wir aus $\mathfrak{G}$ irgendein S heraus und betrachten seine Potenzen S^k, $k = 0, \pm 1, \pm 2, \cdot, \cdot,$ wo $S^0 = E$ sei. Alle diese Substitutionen bilden eine Untergruppe $\mathfrak{G}(S)$ (dieselbe besitzt keinen endlichen Index). Welches ist der D.-B. von $\mathfrak{G}(S)$?

a) S sei von elliptischem Typus. Statt die Abbildung der z-Ebene betrachten wir diejenige der ζ-Ebene:

$$\zeta = \frac{z - z_1}{z - z_2} \quad \text{(S. 7)}.$$

Dann ist $\zeta = k\zeta$, $k = e^{\pi i}$ oder $e^{\pm \frac{2\pi i}{3}}$. $\mathfrak{G}(S)$ ist eine endliche Gruppe von dem Grade (Ordnung) 2 oder 3. Die Abbildung in der ζ-Ebene wird

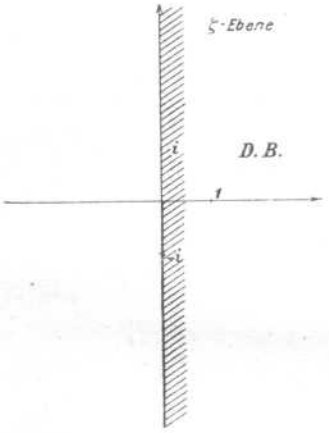

Fig. 1.

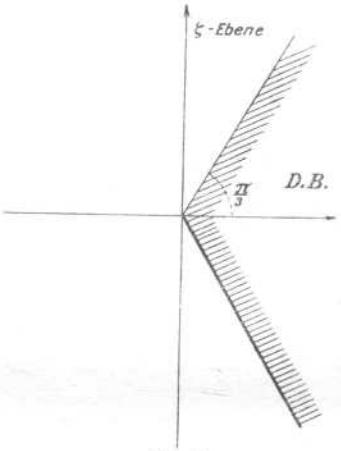

Fig. 2.

durch eine Drehung um den Winkel π oder $\pm \frac{2\pi}{3}$ erhalten. In beiden Fällen zeigen Figur 1 und 2 die D.-B. der ζ-Ebene.

Von der Begrenzung wird jeweils nur die Hälfte zum D.-B. gerechnet. Bilden wir diese D.-B. rückwärts auf die z-Ebene ab:

$$z = \frac{z_2\zeta - z_1}{\zeta - 1},$$

so entsprechen den Punkten 0, ∞ die Fixpunkte z_1 und z_2, die Grenzgeraden gehen nach Satz 2 in Kreise durch z_1 und z_2 über. Da z_1 und z_2 konjugiert imaginär sind, so liegt der Mittelpunkt auf der reellen Achse. Im Falle $k = e^{\pi i}$ wird der Bildpunkt von $\zeta = -i$:

$$z_{1,2} = \frac{\alpha \pm i}{\gamma}, \quad z = \frac{-\frac{\alpha - i}{\gamma} - \frac{\alpha + i}{\gamma}}{-i - 1} = \frac{\alpha + 1}{\gamma}.$$

Der Kreis geht durch die drei Punkte $\frac{\alpha \pm i}{\gamma}$, $\frac{\alpha + 1}{\gamma}$ und ist dadurch bestimmt. Der negativen imaginären Achse der ζ-Ebene entspricht der Halbkreis durch $\frac{\alpha - i}{\gamma}$, $\frac{\alpha + 1}{\gamma}$, $\frac{\alpha + i}{\gamma}$. Der Mittelpunkt ist $\frac{\alpha}{\gamma}$ und der Radius $\left|\frac{1}{\gamma}\right|$. Das Äußere des Kreises mit der ausgezogenen Kreishälfte ist der gesuchte D.-B. Siehe Figur 3.

Im Falle $k = e^{\pm\frac{2\pi i}{3}}$ berechnen wir den Bildpunkt von $\zeta = e^{-\frac{\pi i}{3}}$:

$$z_{1,2} = \frac{\alpha + (\pm 1)e^{\pm\frac{2\pi i}{3}}}{\gamma}, \quad z = \frac{\frac{\alpha + (\pm 1)e^{-\frac{2\pi i}{3}}}{\gamma} e^{-\frac{\pi i}{3}} - \frac{\alpha + (\pm 1)e^{+\frac{2\pi i}{3}}}{\gamma}}{e^{-\frac{\pi i}{3}} - 1} = \frac{\alpha + (\pm 1)}{\gamma}.$$

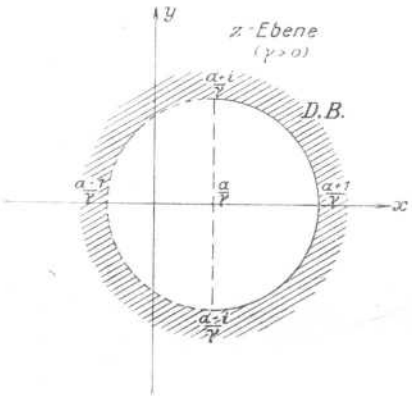

Fig. 3.

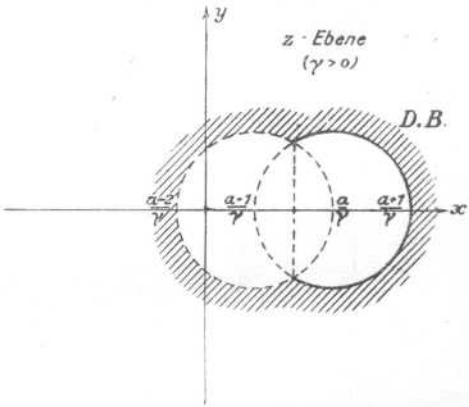

Fig. 4.

Der Mittelpunkt des Kreises ist $\frac{\alpha}{\gamma}$, der Radius $\left|\frac{1}{\gamma}\right|$. Damit ist der Bildkreis der einen Grenzgeraden gefunden. Der der anderen wird durch Berechnung des Bildpunktes von $\zeta = e^{\frac{\pi i}{3}}$ gefunden:

$$z = \frac{\frac{\alpha + (\pm 1)e^{-\frac{2\pi i}{3}}}{\gamma} e^{\frac{\pi i}{3}} - \frac{\alpha + (\pm 1)e^{+\frac{2\pi i}{3}}}{\gamma}}{e^{\frac{\pi i}{3}} - 1} = \frac{\alpha + (\mp 2)}{\gamma}.$$

Der Mittelpunkt ist $\frac{\alpha + (\mp 1)}{\gamma}$, der Radius $\left|\frac{1}{\gamma}\right|$. Siehe Figur 4. Das Äußere der beiden Kreise mit der ausgezogenen Berandung ist der gesuchte D.-B.

In beiden Fällen ist stets ein Punkt außerhalb der Kreise einem Punkt im Innern der Kreise ähnlich, niemals sind aber zwei Punkte außerhalb der Kreise einander ähnlich. Nimmt man $|\gamma| > 1$ an, so ist der Radius der Kreise $\left|\frac{1}{\gamma}\right| \leqq \frac{1}{2}$. Somit ergibt sich das Resultat: *Zwei verschiedene Punkte, deren Imaginärteile absolut* $\geqq \frac{1}{2}$ *sind, können niemals einander in bezug auf* $\mathfrak{G}(S)$ *ähnlich sein, falls* $|\gamma| > 1$.

Eine Ausnahme machen einzig die beiden Fixpunkte, indem *sie sich selbst ähnlich sind.* Sie müssen gesondert betrachtet werden.

Im Falle $\alpha + \delta = 0$ ordnen wir dem D.-B. die Substitution E, dem Innern des Kreises S zu. Entsprechend im Falle $\alpha + \delta = \pm 1$ wird dem Äußern der Kreise E, dem Innern S und S^2 zugerechnet, so daß z. B. S der Bereich ist, dessen Punkte aus dem D.-B. durch S erhalten werden. Die Fixpunkte gehören *allen* Bereichen an, werden also nur zur Hälfte bzw. nur zu einem Drittel dem entsprechenden Bereiche angerechnet.

b) S sei von parabolischem Typus. Betrachten wir wieder zuerst die ζ-Ebene, wo, für $\gamma \neq 0$:

$$\zeta = \frac{1}{z - z_1},$$

so ist $\bar{\zeta} = \zeta \pm \gamma$; für $\gamma = 0$ ist $\zeta = z$, $\bar{\zeta} = \zeta + \beta$. Die Gruppe $\mathfrak{G}(S)$ enthält unendlich viele Substitutionen. Die Abbildung geschieht durch Ver-

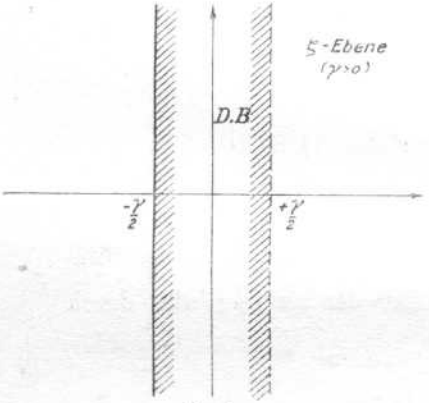

Fig. 5.

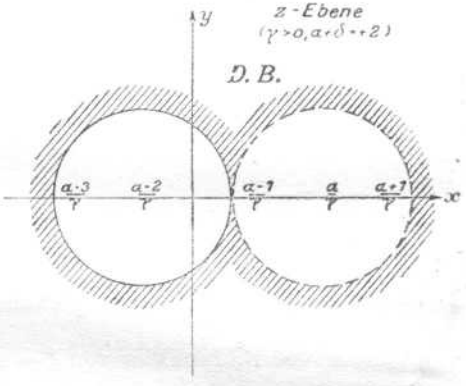

Fig. 6.

schiebung parallel zur reellen Achse um $\pm \gamma$, siehe Figur 5. Die Grenzgerade links gehöre zum D.-B.

Rückwärts ergibt sich der D.-B. der z-Ebene mittels:

$$z = z_1 + \frac{1}{\zeta} = \frac{\alpha \mp 1}{\gamma} + \frac{1}{\zeta}.$$

Nach Satz 2 entsprechen den Geraden Kreise durch den reellen Punkt $\frac{\alpha \mp 1}{\gamma}$, und den reellen Punkten $\pm \frac{1}{2}\gamma$ die reellen Punkte:

$$z = \frac{\alpha \mp 1}{\gamma} \pm \frac{2}{\gamma} = \frac{\alpha \pm 1}{\gamma}, \quad \frac{\alpha \pm 3}{\gamma}.$$

Da die Geraden auf der reellen Achse normal stehen, müssen auch die Kreise auf der reellen Achse normal stehen, also ihren Mittelpunkt auf derselben haben. Der Mittelpunkt der Kreise ist somit $z = \frac{\alpha}{\gamma}$ und $\frac{\alpha \mp 2}{\gamma}$, der Radius $\left|\frac{1}{\gamma}\right|$. Siehe Figur 6.

Das Äußere der Kreise mit der einen ausgezogenen Kreisperipherie ist der D.-B. Es gilt wie im Falle a): *Zwei verschiedene Punkte, deren Imaginärteile absolut* $\geqq \frac{1}{2}$ *sind, können niemals einander in bezug auf* $\mathfrak{G}(S)$ *ähnlich sein, falls* $|\gamma| > 1$.

Zerteilen wir die ζ-Ebene in Streifen der Breite $|\gamma|$, so ordnen wir jedem Streifen diejenige Potenz S^k zu, durch deren Anwendung seine Punkte aus dem D.-B. entstehen. Dem D.-B. selbst ist dann E zugeordnet. Entsprechend wird die z-Ebene in unendlichviele Bereiche eingeteilt, denen dieselben S^k zugeordnet werden. Der Fixpunkt gehört allen Bereichen an und spielt eine besondere Rolle.

c) S sei von hyperbolischem Typus. In (S. 7 und 8)

$$\zeta = \frac{z - z_1}{z - z_2}, \quad \bar{\zeta} = k\zeta, \quad k = (\alpha - z_1\gamma)^2,$$

ist k reell, $\neq 1$ und > 0. z_1 und z_2 sind reell. In der ζ-Ebene werden deshalb die beiden Kreise um den 0-Punkt mit den Radien $|\sqrt{k}|$ und $\left|\frac{1}{\sqrt{k}}\right|$ den D.-B. einschließen, wobei nur ein Grenzkreis mit einzubeziehen ist. Bildet man rückwärts diesen D.-B. durch:

$$z = \frac{z_2\zeta - z_1}{\zeta - 1}$$

auf die z-Ebene ab, so gehen die Kreise nach Satz 2 wieder in Kreise über, deren Mittelpunkte auf der reellen Achse liegen müssen. Als Bildpunkte von $\zeta = \pm\frac{1}{\sqrt{k}}, \pm\sqrt{k}$ berechnen sich unter Berücksichtigung der quadratischen Gleichung von z_1 und z_2:

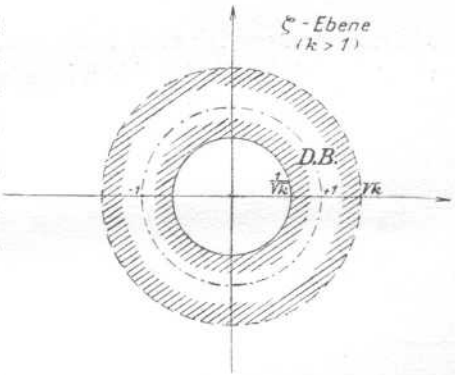

Fig. 7.

$$z = \frac{\pm z_2\frac{1}{\sqrt{k}} - z_1}{\pm\frac{1}{\sqrt{k}} - 1} = \frac{z_2 \mp z_1(\alpha - z_1\gamma)}{1 \mp (\alpha - z_1\gamma)} = \frac{-\delta \mp 1}{\gamma},$$

$$z = \frac{\pm z_2\sqrt{k} - z_1}{\pm\sqrt{k} - 1} = \frac{\pm z_2(\alpha - z_1\gamma) - z_1}{\pm(\alpha - z_1\gamma) - 1} = \frac{\alpha \pm 1}{\gamma}.$$

Die beiden Kreise liegen ganz außerhalb voneinander, ihre Mittelpunkte sind $\frac{\alpha}{\gamma}$ und $-\frac{\delta}{\gamma}$, ihre Radien $\left|\frac{1}{\gamma}\right|$. Das Äußere der beiden Kreise mit der einen ausgezogenen Kreisperipherie ist der gesuchte D.-B. Wieder gilt:

Zwei verschiedene Punkte, deren Imaginärteile absolut $\geqq \frac{1}{2}$ sind, können niemals einander in bezug auf $\mathfrak{G}(S)$ ähnlich sein, falls $|\gamma| > 1$.

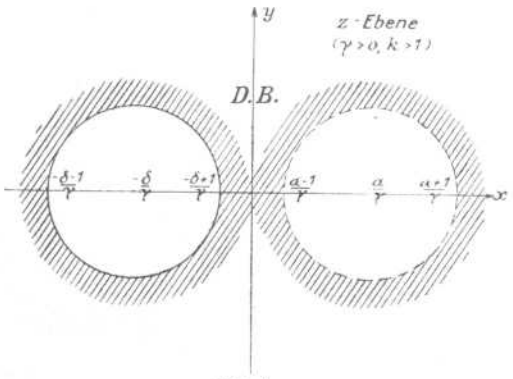

Fig. 8.

Dieses Resultat gilt daher für jedes $\mathfrak{G}(S)$. Man sieht die Richtigkeit folgenden Satzes ein:

4. Satz: *Ist S irgendeine Substitution der Modulgruppe, für die $|\gamma| > 1$ ist, so sind niemals zwei Punkte, deren Imaginärteile absolut $> \frac{1}{2}$ sind, einander bezüglich S ähnlich.*

Auch im Fall c) wird die ζ-Ebene und entsprechend die z-Ebene in unendlich viele Teilbereiche zerlegt, deren jeder eine Potenz S^k zugeteilt wird, die der Abbildung aus dem D.-B. entspricht. Die Fixpunkte z_1 und z_2 sind sich selbst auf unendlich viele Weisen ähnlich.

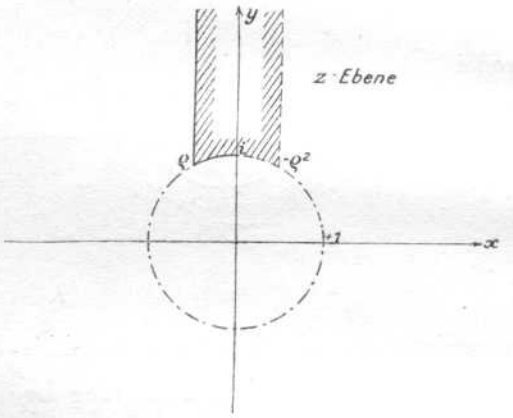

Fig. 9.

Jetzt ist es leicht, den D.-B. der Modulgruppe anzugeben. Für die obere Halbebene stellt ihn Figur 9 dar.

Er liegt außerhalb des Einheitskreises und zwischen den Geraden $z = \pm\frac{1}{2} + iy$. Seine Eckpunkte sind:

$$\varrho = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$$

und

$$-\varrho^2 = +\frac{1}{2} + i\frac{\sqrt{3}}{2} = -e^{-\frac{2\pi i}{3}}.$$

Von der Berandung gehört das Geradenstück durch ϱ und der Kreisbogen von ϱ bis i zum D.-B. Analytisch wird derselbe für $z = x + iy$ so definiert:

$$(4) \qquad \begin{aligned} -\tfrac{1}{2} \leqq x < \tfrac{1}{2}, \quad & x^2 + y^2 > 1, \\ -\tfrac{1}{2} \leqq x \leqq 0, \quad & x^2 + y^2 = 1. \end{aligned}$$

Für alle Punkte des D.-B. ist $y \geqq \frac{1}{2}\sqrt{3} > \frac{1}{2}$.

Zum Beweise zeigen wir zuerst, daß niemals zwei verschiedene Punkte des Bereiches einander ähnlich sind. Wäre dies der Fall, so gäbe es ein S, so daß:

$$w = Sz = \frac{\alpha z + \beta}{\gamma z + \delta}, \quad \alpha\delta - \beta\gamma = 1, \quad w \neq z.$$

w und z müssen beide dem oben in Figur 9 angegebenen Bereiche angehören. Da alle vier Zahlen $\alpha, \beta, \gamma, \delta$ durch ihre entgegengesetzten ersetzt werden können, darf $\gamma \geqq 0$ angenommen werden.

a) $\gamma = 0$, $\alpha = \delta = \pm 1$, $w = z \pm \beta$. Da β eine ganze Zahl ist und die Breite des Streifens 1 ist, muß dieser Fall ausgeschlossen werden.

b) $\gamma = 1$, $w = \frac{\alpha z + \beta}{z + \delta} = \alpha - \frac{1}{z + \delta}$. Liegt z nicht auf dem Einheitskreis, so liegt $z + \delta$ außerhalb desselben, $-\frac{1}{z+\delta}$ also in seinem Innern und $\alpha - \frac{1}{z+\delta}$ sicherlich nicht im angegebenen Bereich. Das gleiche folgt, wenn z auf dem Einheitskreis liegt und $\delta \neq 0$. Ist dagegen in diesem Falle $\delta = 0$, so liegt $-\frac{1}{z}$ spiegelbildlich zur imaginären Achse, w somit außerhalb oder bei $\alpha = 0$ auf dem nicht mehr zum Bereiche gehörenden Bogen desselben. Dieser Fall ist unmöglich.

c) $\gamma > 1$. Die Imaginärteile von z und w sind sicherlich $\geqq \frac{|\sqrt{3}|}{2} > \frac{1}{2}$.

Nach Satz 4 sind z und w niemals in $\mathfrak{G}(S)$ ähnlich. Damit ist in allen Fällen bewiesen, daß *niemals zwei Punkte des in Figur 9 dargestellten Bereiches einander in bezug auf eine Substitution der Modulgruppe ähnlich sind.*

Im zweiten Teil des Beweises haben wir zu zeigen, daß jeder Punkt der oberen Halbebene einem Punkt des Bereiches ähnlich ist.

a) $z = x + iy$ besitze den Imaginärteil $y > 1$.

Es sei a die nächstgelegene ganze Zahl von x, so daß $|a - x| < \frac{1}{2}$ oder, wenn x in der Mitte zwischen zwei ganzen Zahlen liegt, $a > x$. Setzt man $s = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, so ist:

$$s^{-a} z = z - a = (x - a) + iy .$$

Diese Zahl genügt den Ungleichungen (4) und liegt daher im Bereich.

b) $z = x + iy$; $0 < y \leqq \frac{1}{2}$. Hat a wieder die vorige Bedeutung und setzt man $t = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, so wird:

$$z_1 = t s^{-a} z = -\frac{1}{z - a} = -\frac{1}{(x-a) + iy} = -\frac{x - a}{(x-a)^2 + y^2} + \frac{y}{(x-a)^2 + y^2}\, i .$$

Nach Voraussetzung ist:

$$(x - a)^2 + y^2 \leqq \tfrac{1}{4} + \tfrac{1}{4} = \tfrac{1}{2},$$

also:

$$\frac{y}{(x-a)^2 + y^2} \geqq 2y .$$

Die der Zahl z ähnliche Zahl z_1 hat daher ein wenigstens doppelt so großes y. Wiederholt man das Verfahren, so erhält man nach endlich vielen Schritten ein z_n, dessen $y > \frac{1}{2}$ ist.

c) $z = x + iy$; $\frac{1}{2} < y \leqq 1$. Man darf annehmen, daß z im Innern des Einheitskreises liegt, also $-\frac{1}{2} \leqq x < \frac{1}{2}$ ist. Es ist dann:

$$z_1 = s^a t z = a - \frac{1}{z} = \left(a - \frac{x}{x^2+y^2}\right) + \frac{y}{x^2+y^2} i.$$

Man bestimme a so, daß:

$$\left| a - \frac{x}{x^2+y^2} \right| < \frac{1}{2} \quad \text{oder} \quad a - \frac{x}{x^2+y^2} = -\frac{1}{2}$$

ist. Dann wird:

$$\left| a - \frac{1}{z} \right|^2 = \left(a - \frac{x}{x^2+y^2}\right)^2 + \frac{y^2}{(x^2+y^2)^2} = \frac{a^2(x^2+y^2)+1-2ax}{x^2+y^2} = \frac{(ax-1)^2+a^2y^2}{(x^2+y^2)}.$$

Wegen $y > \frac{1}{2}$, $x < \frac{1}{2}$, $x^2 + y^2 < 1$, $(ax-1)^2 + a^2y^2 \geqq 1$ für $|a| + 1$, $(ax-1)^2 + a^2y^2 \geqq x^2 + y^2$, für $|a| = 1$, muß: $|z_1| \geqq 1$ sein. z_1 liegt daher im verlangten Bereich.

Damit ist bewiesen, daß jeder Punkt der oberen Halbebene einem Punkte des Bereiches bezüglich $\mathfrak{G}$ ähnlich ist.

d) $z = \frac{\alpha}{\gamma}$ sei ein rationaler Punkt der reellen Achse. α und γ seien ohne gemeinsamen Teiler. Man bestimme β und δ so, daß:

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

Der Punkt $\frac{\alpha}{\gamma}$ ist dem Punkt ∞ bezüglich S ähnlich.

e) Die irrationalen Punkte der reellen Achse werden durch die S von $\mathfrak{G}$ untereinander vertauscht, werden aber niemals einem Punkte des Bereiches bezüglich $\mathfrak{G}$ ähnlich. Um unserer Definition Genüge zu verschaffen, müßten wir noch eine bestimmte Menge irrationaler Zahlen zum D.-B. hinzunehmen. Man tut dies der Einfachheit wegen nicht, sondern nennt den Bereich der Figur 9 trotzdem den D.-B. der Modulgruppe $\mathfrak{G}$.

Der Beweis läßt die Tatsache erkennen, daß jedes S durch eine abwechselnde Anwendung von s und t ersetzt werden kann:

$$S = s^a t s^{a_1} t s^{a_2} \ldots s^{a_{n-1}} t s^{a_n}.$$

Da $s^a z = z + a$, $tz = -\frac{1}{z}$, so heißt dies nichts anderes, als daß:

$$w = Sz = \frac{\alpha z + \beta}{\gamma z + \delta} = a - \cfrac{1}{a_1 - \cfrac{1}{a_2 - \ddots - \cfrac{1}{a_{n-1} - \cfrac{1}{a_n + z}}}}.$$

s und t heißen *Erzeugende* der S von $\mathfrak{G}$. Man kann zeigen, daß alle a als positive Zahlen angenommen werden können; denn $s^{-1} = tstst$.

Jedes beliebige S bildet den D.-B. auf ein nach Satz 4 durch Kreisbögen begrenztes Dreieck ab. Diesem Flächenstück wird S zugeordnet, während dem ursprünglichen D.-B. E zugeteilt ist. Alle diese Dreiecke überdecken die obere Halbebene einfach und lückenlos. So entsteht die berühmte *Dedekind*sche Figur 10.

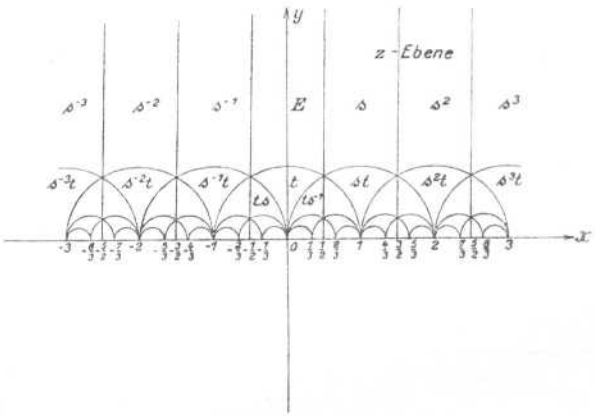

Fig. 10.

Alle und nur die Fixpunkte irgendeines S sind sich selbst in $\mathfrak{G}$ ähnlich. Es sind dies die Punkte:

$$\frac{\alpha \pm i}{\gamma}, \quad \frac{\alpha \pm e^{\frac{2\pi i}{3}}}{\gamma}, \quad \infty,$$

sowie die quadratischen Irrationalitäten $\frac{\alpha - \delta \pm \sqrt{(\alpha+\delta)^2 - 4}}{2\gamma}$. Von diesen liegen im D.-B. nur $\varrho = e^{\frac{2\pi i}{3}}$, i, ∞. Sie heißen die Eckpunkte des D.-B. Der D.-B. wird somit als ein *Viereck* aufgefaßt, das die Winkel $\frac{\pi}{3}$ oder 60^0 bei $z = \varrho$, π oder 180^0 bei $z = i$, 0 bei $z = \infty$ besitzt. Bei ϱ stoßen sechs, bei i zwei Bereiche zusammen, bei ∞ unendlich viele.

Da die Kongruenzgruppen n^{ter} Stufe $\mathfrak{G}^{(n)}$ Untergruppen von $\mathfrak{G}$ von endlichem Index sind, so erhält man deren D.-B., indem man die auf S. 3 definierten Substitutionen:

$$E = s_1, s_2, s_3, \ldots s_u$$

nimmt, und deren zugehörigen Bereiche in Figur 10 bestimmt. Die Gesamtheit bildet den D.-B. von $\mathfrak{G}^{(n)}$. In der Tat gilt für jedes beliebige S: $S = s_i S^{(n)}$ oder $S^{(n)} = s_i^{-1} S$, woraus sich sofort die Richtigkeit der Aussage ergibt.

3. Die Modulfunktion.

Wir betrachten den D.-B. der Modulgruppe $\mathfrak{G}$ und ordnen jedem seiner Randpunkte den durch $sz = z + 1$, $tz = -\frac{1}{z}$ zugeordneten Randpunkt zu. Die beiden Geradenstücke $\pm\frac{1}{2} + it$ und die beiden Kreisbogenstücke links und rechts der imaginären Achse denke man sich also zusammengeknüpft. Die so erhaltene Fläche hat das Geschlecht null. Sie kann durch eine analytische Funktion auf die schlichte Ebene abgebildet

werden. Die Abbildung ist konform an allen Stellen, die keine Eckpunkte sind. Ist $w = f(z)$ eine solche Funktion, so ist auch:

$$\frac{aw+b}{cw+d}, \quad ad - bc \neq 0 ,$$

eine solche. Daraus folgt, daß man bei der Abbildung noch *drei Punkte in drei beliebig vorgeschriebene Punkte überführen kann.* Unter allen w sind diejenigen ausgezeichnet, die dem *Schwarzschen Prinzip der Symmetrie* genügen. Teilen wir das Viereck des D.-B. durch die imaginäre Achse in zwei Dreiecke, so sind diese symmetrisch in bezug auf die imaginäre Achse (Figur 11).

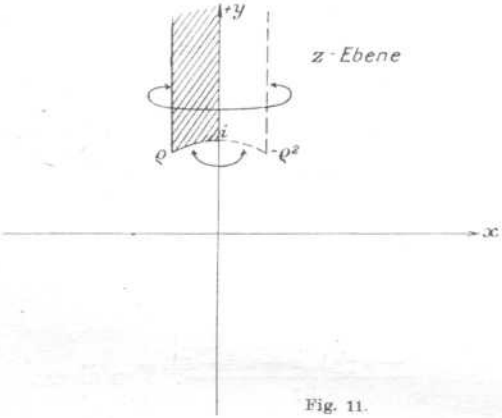

Fig. 11.

Eines der beiden Dreiecke ist schraffiert. Wir greifen die Funktion w heraus, die das schraffierte Dreieck auf die obere Halbebene abbildet. Da Randpunkte bei der Abbildung in Randpunkte übergehen, muß die Umgrenzung des Dreieckes in die reelle Achse übergehen. Die Abbildung hört in den drei Eckpunkten $z = \varrho, i, \infty$ auf, konform zu sein. Die drei Winkel $\frac{\pi}{3}, \frac{\pi}{2}, 0$ gehen in den gestreckten Winkel π über. Es ist praktisch, gerade die Bildpunkte dieser drei Eckpunkte vorzuschreiben. Sie müssen nur reell sein und in positivem Sinne die Achse durchlaufen, falls man die Eckpunkte in der Reihenfolge ϱ, i, ∞ abzählt. Dem wird genügt, wenn vorgeschrieben wird:

$$\begin{aligned} z &= \varrho, \quad & w &= 0, \\ z &= i, \quad & w &= 1, \\ z &= \infty, \quad & w &= \infty. \end{aligned}$$

Wird das Verhalten der Funktion im Unendlichen noch näher präzisiert, so ist durch diese Festsetzungen $w = f(z)$ völlig bestimmt. Wir bezeichnen diese Funktion mit $J(z)$. Ihre Eigenschaften sind:

1. *$w = J(z)$ ist eine analytische Funktion, die das schraffierte Dreieck von Figur 11 auf die obere w-Ebene abbildet.*

2. *Die Abbildung ist überall konform, mit Ausnahme der Punkte $z = \varrho, i, \infty$, denen die Punkte $w = 0, 1, \infty$ zugeordnet sind.*

3. *Gemäß dem Symmetrieprinzip ist $J(z)$ in das nicht schraffierte Dreieck analytisch fortsetzbar und bildet dieses auf die untere w-Ebene ab.*

Symmetrische Punkte bezüglich der imaginären Achse gehen in symmetrische Punkte bezüglich der reellen Achse über. Ist nämlich

$z = x + iy$ ein innerer Punkt des schraffierten Dreiecks und $J(z) = u(x, y) + v(x, y)\,i$, so setze man:

$$J(-x + iy) = u(x, y) - iv(x, y). \quad (v(0, y) = 0,\ y > 1)$$

Diese für alle Punkte des nichtschraffierten Dreiecks definierte Funktion geht stetig in die erste Funktion über, da beide für Punkte der imaginären Achse identisch sind. Ferner ist $J(-x + iy)$ wieder analytisch, da:

$$\frac{\partial u}{\partial(-x)} = \frac{\partial(-v)}{\partial y};\quad \frac{\partial u}{\partial y} = -\frac{\partial(-v)}{\partial(-x)}.$$

Da beide analytischen Funktionen längs eines Kurvenstückes übereinstimmen, ist die eine die analytische Fortsetzung der andern.

4. Für $z = \varrho$ und i muß $J(z)$ folgende Taylorentwicklung besitzen:

$$J(z) = b_1 (z - \varrho)^3 + \cdots,\ b_1 \neq 0,$$
$$J(z) = 1 + c_2 (z - i)^2 + \cdots,\ c_2 \neq 0.$$

Für $z = \infty$ werde folgende Festsetzung gemacht: Es sei $q = e^{2\pi i z}$; geht dann z auf der positiven imaginären Achse ins Unendliche, so wird:

$$\lim_{z=\infty} q = 0.$$

$J(z)$ soll als Funktion von q in $q = 0$ einen Pol 1. Ordnung haben. $J(z)$ besitzt dann um $z = \infty$ die Reihenentwicklung:

$$J(z) = \frac{a_{-1}}{q} + a_0 + \cdots,\quad a_{-1} \neq 0.$$

$J(z)$ ist jetzt völlig bestimmt.

5. $J(z)$ kann über die Grenzen des D.-B. analytisch fortgesetzt werden. Liegt z im D.-B., und ist Sz ein in bezug auf die Modulgruppe $\mathfrak{G}$ ähnlicher Punkt, so setzen wir fest:

$$J(Sz) = J(z). \tag{5}$$

Die so definierte Funktion ist die analytische Fortsetzung von $J(z)$. Denn $J(z_1)$ ist an der Stelle $z_1 = Sz$ stetig, falls z ein innerer Punkt des D.-B. ist. Aber auch auf den Randpunkten trifft dies zu, da nach unseren Festsetzungen $J(z)$ an den Randpunkten z und $sz = z + 1$ oder z und $tz = -\frac{1}{z}$ denselben Wert annimmt. $J(z)$ ist in der ganzen obern Halbebene stetig. $J(z)$ ist auch analytisch im Bereiche S, da dieser durch S^{-1} konform auf den D.-B. E und dieser durch $J(z)$ konform auf die schlichte Ebene abgebildet wird.

Alle rationalen Punkte $\frac{\alpha}{\gamma}$ der reellen Achse der z-Ebene sind $z = \infty$ ähnlich, somit $J\left(\frac{\alpha}{\gamma}\right) = \infty$. Da die rationalen Punkte überall dicht lie-

gen, so ist die reelle Achse als Ort aller Häufungspunkte dieser Pole eine *natürliche Grenze von* $J(z)$.

Es fehlt, noch den *Existenzbeweis von* $J(z)$ zu erbringen. Dieser wird geführt durch die *analytische Darstellung von* $J(z)$. Wir betrachten die Doppelreihe:

$$G_k(z) = \sum_{n,m=-\infty}^{+\infty}{}' \frac{1}{(nz+m)^{2k}},$$

wo k eine ganze positive Zahl ist, der Strich an Σ bedeutet, daß die Kombination $n=0$, $m=0$ ausgeschlossen ist und $z = x + iy$ einen positiven Imaginärteil $y > 0$ hat.

5. **Satz:** *$G_k(z)$ konvergiert in jedem ganz in der oberen Halbebene gelegenen, endlichen Bereich gleichmäßig und absolut für $k > 1$.*

Denn faßt man in $\sum_{(n,m)}{}' \frac{1}{|nz+m|^{2k}}$ alle diejenigen Glieder zusammen, für die $|n| + |m| = N$ ist, so darf man schreiben:

$$\sum_{(n,m)}{}' \frac{1}{|nz+m|^{2k}} = \sum_{N=1}^{\infty} \sum_{|n|+|m|=N} \frac{1}{|nz+m|^{2k}}.$$

Nun ist $|nz+m| > Nq$, wenn $|n| + |m| = N$ ist, und falls q der kleinste Normalabstand des Nullpunktes von den Seiten des Parallelogramms mit den Ecken $1, z, -1, -z$ ist. Daher wird:

$$\frac{1}{|nz+m|^{2k}} < \frac{1}{N^{2k} q^{2k}},$$

also, da es $4N$ Wertepaare gibt, für die $|n| + |m| = N$ ist:

$$\sum_{|n|+|m|=N} \frac{1}{|nz+m|^{2k}} < \frac{4}{q^{2k} N^{2k-1}}, \qquad \sum_{(n,m)}{}' \frac{1}{|nz+m|^{2k}} < \frac{4}{q^{2k}} \sum_{N=1}^{\infty} \frac{1}{N^{2k-1}}.$$

Da die Reihe rechts für $k > 1$ konvergiert, folgt die absolute Konvergenz für $G_k(z)$. Nimmt man für q den kleinsten Wert, der sich für ein z des Bereiches ergeben kann, so ist wegen der Annahmen immer noch $q > 0$, woraus die Gleichmäßigkeit der Konvergenz in dem betreffenden Bereiche folgt.

6. **Satz:** $G_2(\varrho) = 0$, $\varrho = e^{\frac{2\pi i}{3}}$.

Wegen $\varrho^3 = 1$, $\varrho^2 + \varrho + 1 = 0$ wird:

$$G_2(\varrho) = \sum_{n,m=-\infty}^{+\infty}{}' \frac{1}{(n\varrho+m)^4} = \sum_{n,m=-\infty}^{+\infty}{}' \frac{1}{(n\varrho+m\varrho^3)^4} = \frac{1}{\varrho^4} \sum_{n,m=-\infty}^{+\infty}{}' \frac{1}{(n+m\varrho^2)^4}$$

$$= \frac{1}{\varrho} \sum_{n,m=-\infty}^{+\infty}{}' \frac{1}{((n-m)-m\varrho)^4} = \frac{1}{\varrho} G_2(\varrho).$$

Wegen $\frac{1}{\varrho} \neq 1$ folgt der Satz.

7. Satz: $G_3(i) = 0$, $i = \sqrt{-1}$.

Wegen $i^2 = -1$ folgt:

$$G_3(i) = \sum_{n,m=-\infty}^{+\infty}{}' \frac{1}{(ni+m)^6} = \sum_{n,m=-\infty}^{+\infty}{}' \frac{1}{(ni-mi^2)^6} = \frac{1}{i^6} \sum_{n,m=-\infty}^{+\infty}{}' \frac{1}{(n-mi)^6} = -G_3(i).$$

8. Satz: *Ist* $S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ *eine Substitution der Modulgruppe* $\mathfrak{G}$, *so ist für jedes endliche* z *der oberen Halbebene:*

$$G_k(Sz) = (\gamma z + \delta)^{2k} G_k(z). \qquad (k>1)$$

Zunächst ist Sz wieder ein endlicher Punkt der oberen Halbebene. $G_k(Sz)$ ist absolut konvergent, die Reihe ist von der Summationsfolge unabhängig:

$$G_k(Sz) = (\gamma z + \delta)^{2k} \sum_{n,m=-\infty}^{+\infty}{}' \frac{1}{(n(\alpha z+\beta)+m(\gamma z+\delta))^{2k}}$$

$$= (\gamma z + \delta)^{2k} \sum_{n,m=-\infty}^{+\infty}{}' \frac{1}{((n\alpha+m\gamma)z+(n\beta+m\delta))^{2k}}.$$

Setzt man:

$$\begin{matrix} n' = n\alpha + m\gamma, \\ m' = n\beta + m\delta, \end{matrix} \quad \text{so ist:} \quad \begin{matrix} n = \delta n' - \gamma m', \\ m = -\beta n' + \alpha m', \end{matrix} \quad \text{weil } \alpha\delta - \beta\gamma = 1 \text{ ist.}$$

n', m' durchlaufen gleichzeitig mit n, m alle Kombinationen der ganzen Zahlen mit Ausnahme von 0, 0 Also steht rechts wieder $G_k(z)$.

Es ist noch notwendig, $G_k(z)$ in $z = \infty$ zu untersuchen. Dazu entwickeln wir es in eine Reihe nach $q = e^{2\pi i z}$. Da in $z = x + iy$, $y > 0$, so muß:

$$0 < |q| = e^{-2\pi y} < 1$$

sein. Wir schreiben in $G_k(z)$ folgende besondere Summation vor:

$$G_k(z) = 2\sum_{m=1}^{\infty} \frac{1}{m^{2k}} + \sum_{n=+1}^{\infty} \sum_{m=-\infty}^{+\infty} \left[\frac{1}{(nz+m)^{2k}} + \frac{1}{(nz-m)^{2k}}\right].$$

Diese Summation hat den Vorteil, auch für $k = 1$ wenigstens noch bedingt zu konvergieren. Sie definiert dann die neue Funktion $G_1(z)$. $2\pi i n z$ hat einen negativen Realteil, $n > 0$, also konvergiert das Integral:

$$\frac{1}{(nz \pm m)^{2k}} = \frac{(2\pi i)^{2k}}{(2k-1)!} \int_0^{\infty} e^{2\pi i(nz \pm m)t} t^{2k-1} dt,$$

für jedes $n > 0$. Setzt man dies oben ein und bedeutet B_k die k^{te} Bernoullische Zahl, so wird:

$$G_k(z) = \frac{(2\pi)^{2k}}{(2k)!} B_k + 2\frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sum_{m=-\infty}^{+\infty} \int_0^{\infty} e^{2\pi i n z t} t^{2k-1} \cos(2\pi m t)\, dt.$$

Wir zerlegen das Intervall des Integrales in die Summe der Intervalle $(h, h+1)$, $h = 0, 1, 2, \ldots$ und schreiben $t+h$ statt t:

$$G_k(z) = \frac{(2\pi)^{2k}}{(2k)!} B_k + 2\frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sum_{m=-\infty}^{+\infty} \int_0^1 \Big[\sum_{h=0}^{\infty} e^{2\pi i n z (t+h)} (t+h)^{2k-1}\Big] \cos(2\pi m t)\, dt.$$

Da die innerste Summe gleichmäßig konvergiert, durfte Summation und Integration vertauscht werden.

Nach *Fourier* gilt für jede in $(0, 1)$ stetige und differentiierbare Funktion $f(t)$:

$$\sum_{m=-\infty}^{+\infty} \int_0^1 f(t) \cos(2\pi m t)\, dt = \frac{f(0) + f(1)}{2}.$$

Setzt man: $$f(t) = \sum_{h=0}^{\infty} e^{2\pi i n z (t+h)} (t+h)^{2k-1},$$

so wird, da $f(t)$ für $h = 0$, $t = 0$ verschwindet:

$$G_k(z) = \frac{(2\pi)^{2k}}{(2k)!} B_k + 2\frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sum_{h=1}^{\infty} h^{2k-1} q^{nh}.$$

Die innere Reihe konvergiert wegen $|q| < 1$ absolut. Wir dürfen die Summationsreihenfolge vertauschen und finden:

$$G_k(z) = \frac{(2\pi)^{2k}}{(2k)!} B_k + 2\frac{(-1)^k (2\pi)^{2k}}{(2k-1)!} \sum_{h=1}^{\infty} h^{2k-1} \frac{q^h}{1-q^h}. \qquad (k = 1, 2, 3 \ldots)$$

Der *Fourier*sche Lehrsatz hat *eine* Summation auszuführen gestattet. Wegen $B_1 = \frac{1}{6}$, $B_2 = \frac{1}{30}$, $B_3 = \frac{1}{42}$ wird:

$$(6) \qquad \begin{cases} G_1(z) = \dfrac{\pi^2}{3} - 8\pi^2 \displaystyle\sum_{h=1}^{\infty} h \frac{q^h}{1-q^h}, \\ G_2(z) = (2\pi)^4 \Big[\dfrac{1}{720} + \dfrac{1}{3} \displaystyle\sum_{h=1}^{\infty} h^3 \frac{q^h}{1-q^h}\Big], \\ G_3(z) = (2\pi)^6 \Big[\dfrac{1}{42 \cdot 720} - \dfrac{1}{60} \displaystyle\sum_{h=1}^{\infty} h^5 \frac{q^h}{1-q^h}\Big]. \end{cases}$$

$G_1(z)$ läßt sich auch so schreiben:

$$(7) \qquad G_1(z) = -4\pi i \frac{d \ln \eta(z)}{dz},$$

wo $$\eta(z) = q^{\frac{1}{24}} \prod_{h=1}^{\infty} (1-q^h).$$

Wir müssen noch für die Funktion $G_1(z)$ die dem 8. Satze entsprechende Eigenschaft herleiten. Nach dem Resultat von S. 16 genügt es,

die Änderung von $G_1(z)$ und $\eta(z)$ bei Anwendung von s und t zu bestimmen. Aus (6) und (7) erkennt man sofort, daß:

$$G_1(sz) = G_1(z), \quad \eta(sz)^{24} = \eta(z)^{24}, \quad s = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Nach Definition ist:

$$\frac{1}{z^2} G_1\left(-\frac{1}{z}\right) = 2\sum_{m=1}^{\infty} \frac{1}{(mz)^2} + \sum_{n=1}^{\infty} \sum_{m=-\infty}^{+\infty} \left[\frac{1}{(mz+n)^2} + \frac{1}{(mz-n)^2}\right]$$

$$= 2\sum_{n=1}^{\infty} \frac{1}{n^2} + \sum_{n=-\infty}^{+\infty} \sum_{m=1}^{\infty} \left[\frac{1}{(mz+n)^2} + \frac{1}{(mz-n)^2}\right].$$

Wir führen jetzt wieder, wie auf S. 21, für die eckige Klammer das bestimmte Integral ein, zerlegen sein Intervall in die Summe der Intervalle $(h, h+1)$, $h = 0, 1, 2, \ldots$ und schreiben $t + h$ statt t. Dann ergibt sich, da man die Summation über m ausführen kann:

$$\frac{1}{z^2} G_1\left(-\frac{1}{z}\right) = \frac{\pi^2}{3} + 2(2\pi i)^2 \sum_{n=-\infty}^{+\infty} \int_0^1 \left[\sum_{h=0}^{\infty} \frac{e^{2\pi i z(t+h)}(t+h)}{1 - e^{2\pi i z(t+h)}}\right] \cos(2\pi n t)\, dt.$$

Der *Fourier*sche Lehrsatz wird jetzt auf:

$$f(t) = \sum_{h=0}^{\infty} \frac{e^{2\pi i z(t+h)}(t+h)}{1 - e^{2\pi i z(t+h)}}$$

angewandt. Diese Funktion wird nicht null, für $h = 0$, $t = 0$. Somit wird in Abweichung des frühern Falles:

$$\frac{1}{z^2} G_1\left(-\frac{1}{z}\right) = \frac{\pi^2}{3} + 2(2\pi i)^2 \left[\tfrac{1}{2} \lim_{t=0} \frac{e^{2\pi i z t} t}{1 - e^{2\pi i z t}} + \sum_{h=1}^{\infty} \frac{e^{2\pi i z h} h}{1 - e^{2\pi i z h}}\right]$$

$$= \frac{\pi^2}{3} + 2(2\pi i)^2 \left[-\frac{1}{4\pi i z} + \sum_{h=1}^{\infty} h \frac{q^h}{1 - q^h}\right]$$

oder nach (6): $$\frac{1}{z^2} G_1\left(-\frac{1}{z}\right) = -\frac{2\pi i}{z} + G_1(z).$$

Für $\eta(z)$ lautet die Formel so:

$$4\pi i \frac{d \lg \eta\left(-\frac{1}{z}\right)}{dz} = \frac{2\pi i}{z} + 4\pi i \frac{d \lg \eta(z)}{dz},$$

woraus durch Integration:

$$\eta\left(-\frac{1}{z}\right) = c\sqrt{z}\,\eta(z).$$

Die Integrationskonstante bestimmt sich für $z = i$, da $\eta(i) \neq 0$:

$$(8)\qquad \begin{cases} \eta\left(-\frac{1}{z}\right) = \sqrt{-iz}\,\eta(z) \\ \eta^{24}\left(-\frac{1}{z}\right) = z^{12}\,\eta^{24}(z) \\ \eta^{24}(z) = q\prod_{h=1}^{\infty}(1-q^h)^{24}. \end{cases}$$

Durch sukzessive Anwendung von (8) und $\eta(z)^{24} = \eta(sz)^{24}$ folgt:

$$\eta^{24}(Sz) = (cz+d)^{12}\,\eta(z)^{24}, \quad S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

wo c und d von z unabhängige Zahlen sind. Ist $\gamma = 0$, so ist $c = 0$, $d = 1$. Ist $\gamma \neq 0$, so setze man statt z: $S^{-1}z$, wo $S^{-1} = \begin{pmatrix} -\delta & \beta \\ \gamma & -\alpha \end{pmatrix}$ ist. Dann wird:

$$\eta^{24}(z) = (cS^{-1}z+d)^{12}\eta^{24}(S^{-1}z) = \left(\frac{(-c\delta+d\gamma)z+(c\beta-\alpha d)}{\gamma z-\alpha}\right)^{12}\eta^{24}(S^{-1}z).$$

$$\eta^{24}(S^{-1}z) = (c_1 z + d_1)^{12}\eta^{24}(z).$$

Wegen $\gamma \neq 0$ ist auch $c \neq 0$ und $c_1 \neq 0$; denn sonst wäre $\eta(Sz)^{24}$ für $\lim z = \infty$, $q = 0$ in q nur von 1^{ter} Ordnung null, was unmöglich ist. Somit folgt, daß $-c\delta + d\gamma = 0$ oder $d = \frac{\delta}{\gamma}c$, und

$$\eta^{24}(Sz) = \bar{c}\,(\gamma z+\delta)^{12}\eta^{24}(z).$$

$\bar{c}$ ist von S unabhängig, da es sich nicht ändert, falls man auf z eine der Substitutionen s oder t ausübt. Somit ist $\bar{c} = 1$, wegen des Falles $\gamma = 0$, $\delta = 1$, und es gilt:

$$(9)\qquad \eta^{24}(Sz) = \eta^{24}\left(\frac{\alpha z+\beta}{\gamma z+\delta}\right) = (\gamma z+\delta)^{12}\,\eta^{24}(z),$$

und wegen (7) für $G_1(z)$:

$$G_1(Sz) = -2\pi i\gamma(\gamma z+\delta) + (\gamma z+\delta)^2 G_1(z).$$

Es ist leicht, aus $G_k(z)$ Funktionen zu bilden, die bei den S der Gruppe $\mathfrak{G}$ ungeändert bleiben. Eine solche Funktion ist z. B. wegen Satz 8:

$$\frac{G_2^{\,3}}{G_3^{\,2}}.$$

Tritt unter denselben auch $J(z)$ auf? Wegen Eigenschaft 2 S. 18 ist $J(\varrho) = 0$, $J(i) = 1$; ferner besitzt $J(z)$ für $z = \infty$ einen Pol 1^{ter} Ordnung in q. Nun folgt aus (6):

$$\lim_{q=0} G_2(z) = (2\pi)^4\frac{1}{720}, \quad \lim_{q=0} G_3(z) = (2\pi)^6\frac{1}{720\cdot 42}.$$

Somit folgt für die Verbindung $G_2^{\,3} - \frac{49}{20}G_3^{\,2}$:

$$\lim_{q=0}\frac{1}{q}\left(G_2^{\,3} - \frac{49}{20}G_3^{\,2}\right) = (2\pi)^{12}\left(\frac{1}{720^2} + \frac{2\cdot 49}{42\cdot 720\cdot 60\cdot 20}\right) = \frac{12}{720^2\cdot 5}(2\pi)^{12}.$$

Die Funktion $$\bar{J}(z) = \frac{G_2^3}{G_2^3 - \frac{49}{20} G_3^2}$$

hat deshalb für $z = \infty$ oder $q = 0$ einen Pol 1. Ordnung:

$$\lim_{q=0} q\bar{J}(z) = \frac{1}{\frac{720^3}{12} \cdot \frac{1}{720^2 \cdot 5}} = \frac{1}{2^6 \cdot 3^3}, \quad \bar{J}(z) = \frac{1}{2^6 \cdot 3^3 \cdot q} + \cdots.$$

Ferner ist, falls $G_2(i) \neq 0$, $G_3(\varrho) \neq 0$ ist,

$$\bar{J}(\varrho) = 0, \quad \bar{J}(i) = 1$$

und entsprechend (5): $$\bar{J}(Sz) = \bar{J}(z).$$

Da außerdem q auf der imaginären Achse reell wird, so ist $\bar{J}(z)$ für reinimaginäre z reell, genügt also dem Schwarzschen Symmetrieprinzip; allein wir wissen noch nicht, ob die Abbildung eine schlichte ist.

4. Funktionentheoretische Sätze über Modulfunktionen.

Die Funktion $J(z)$, die wir im § 3 kennen gelernt haben, blieb bei jeder Substitution der Modulgruppe ungeändert und war in der ganzen oberen Halbebene regulär, mit Ausnahme von $z = \infty$, wo sie als Funktion von $q = e^{2\pi i z}$ einen Pol 1. Ordnung hatte. Eine Funktion von diesen Eigenschaften heißt eine Modulfunktion. Wir definieren allgemein:

3. **Definition:** *Die analytische Funktion $f(z)$ heißt eine Modulfunktion, wenn sie nicht konstant, in jedem Punkt der oberen Halbebene definiert ist, und*

1. *bei jeder Substitution der Modulgruppe oder einer ihrer Untergruppen von endlichem Index unverändert bleibt:*

$$f\left(\frac{\alpha z + \beta}{\gamma z + \delta}\right) = f(z);$$

2. *in jedem endlichen Punkt regulär ist, oder höchstens einen Pol besitzt;*

3. *im Punkt $z = \infty$ als Funktion von $q = e^{2\pi i z}$ keine wesentliche Singularität besitzt.*

Die unter 1. genannte Gruppe heißt die Gruppe der Modulfunktion.

Wir setzen demgemäß fest, daß unter $\lim z = \infty$ stets $\lim q = 0$ zu verstehen ist, und daß $f(z)$ einen Wert für $z = \infty$ von derjenigen Ordnung annimmt, die sie als Funktion von q besitzt.

Wie wir gesehen haben, gehören die Eckpunkte eines D.-B. verschiedenen Bereichen an. Z. B. gehört $z = \varrho$ für $J(z)$ drei verschiedenen Bereichen an. Gehört $z = z_1$ n verschiedenen Bereichen an, und nimmt

eine Modulfunktion ihren Wert für $z = z_1$ von r^{ter} Ordnung an, so setzen wir fest, daß sie den Wert im D.-B. nur von $\frac{r^{\text{ter}}}{n}$ Ordnung annehmen soll. Z. B. $J(z)$, das für $z = \varrho$ den Wert 0 nach Eigenschaft 4, S. 19 von 3. Ordnung annimmt, nimmt ihn im D.-B. nur von $\frac{3^{\text{ter}}}{3} = 1$. Ordnung an.

Auf Grund dieser Festsetzungen gilt der

9. Satz: *Eine Modulfunktion nimmt jeden Wert im D.-B. ihrer Gruppe gleich oft an.*

Wir führen den Beweis für den Fall, daß die Gruppe die Modulgruppe selbst ist. Ihr D.-B. ist durch Figur 9 gegeben.

Ist G irgendein geschlossener, endlicher, doppelpunktsfreier Weg, auf dem $f(z)$ nirgends null oder unendlich wird, so ist nach *Cauchy* für positiv durchlaufenes G:

$$\frac{1}{2\pi i}\int_{(G)} \frac{f'(z)}{f(z)}\,dz = \text{Anzahl der Nullstellen} - \text{Anzahl der Pole in } G.$$

Nehmen wir zunächst an, $f(z)$ werde auf dem Rande des D.-B. (auch für $z = \infty$) nirgends null oder unendlich. Wäre dies nicht erfüllt, so bestimme man zwei endliche, voneinander verschiedene Zahlen c_1 und c_2, die von $f(z)$ auf dem Rande nirgends angenommen werden, und lege der Betrachtung

$$\frac{f(z) - c_1}{f(z) - c_2}, \quad c_1 \neq c_2,$$

statt $f(z)$ zugrunde. Diese Funktion genügt der obigen Annahme. Ist der Satz für sie bewiesen, so ist er es auch für $f(z)$ wegen der konformen Abbildung einer Ebene in sich selbst durch eine lineare Substitution (§ 2, S. 6).

Wir schließen den D.-B. nach oben durch die Strecke $x + Ni$, $-\frac{1}{2} \leqq x \leqq +\frac{1}{2}$ ab, wo N eine beliebige positive Zahl ist, nur so groß, daß oberhalb und auf der Strecke keine Null- oder Unendlichkeitspunkte mehr liegen. G sei jetzt die Umgrenzung dieses abgeschnittenen D.-B., und es ist:

$$\frac{1}{2\pi i}\int_{(G)} \frac{f'(z)}{f(z)}\,dz = \frac{1}{2\pi i}\left[\int_{\varrho}^{i} + \int_{i}^{-\varrho^2} + \int_{-\varrho^2}^{\frac{1}{2}+Ni} + \int_{\frac{1}{2}+Ni}^{-\frac{1}{2}+Ni} + \int_{-\frac{1}{2}+Ni}^{\varrho}\right].$$

Im 2. Integral macht man die Substitution $z_1 = -\frac{1}{z}$, der Kreisbogen $(i, -\varrho^2)$ geht dann in den Kreisbogen (i, ϱ) über. Da nach Annahme $f\left(-\frac{1}{z}\right) = f(z)$, so ist

$$\int_{\varrho}^{i} + \int_{i}^{-\varrho^2} = 0.$$

Im dritten Integral setzt man $z_1 = z - 1$, $z = z_1 + 1$, wodurch die Strecke $(-\varrho^2, \frac{1}{2} + Ni)$ in die Strecke $(\varrho, -\frac{1}{2} + Ni)$ übergeht. Wegen $f(z+1) = f(z)$ folgt:

$$\int_{-\varrho^2}^{\frac{1}{2}+Ni} + \int_{-\frac{1}{2}+Ni}^{\varrho} = 0.$$

Im vierten Integral setzen wir $q = e^{2\pi i z}$. q durchläuft negativ den Kreis K mit dem Radius $e^{-2\pi N}$ um $q = 0$, wenn z die Punkte der Strecke durchläuft. Nach Annahme hat $f(z)$ weder einen Pol noch eine Nullstelle für $q = 0$. Also hat $f(z)$ wegen der Wahl von N im Innern und auf dem Rande von K keine Null- und Unendlichkeitsstellen, und es ist:

$$\int_{-\frac{1}{2}+Ni}^{+\frac{1}{2}+Ni} = \int_{(K)} = 0.$$

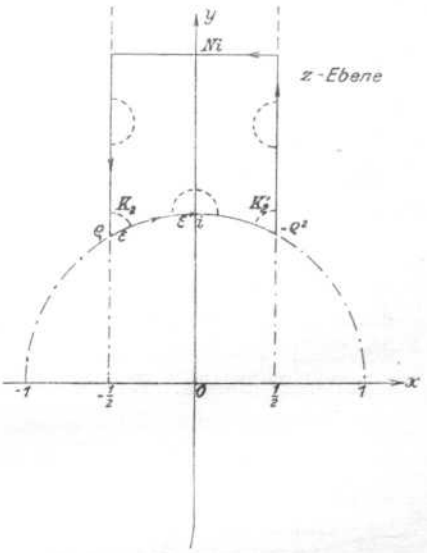

Fig. 12.

Daraus folgt, daß die Anzahl der Null- und Unendlichkeitsstellen im D.-B. gleich groß ist.

Ist c irgendein Wert, den $f(z)$ auf dem Rande nirgends annimmt, so darf man statt $f(z)$ auch $f(z) - c$ nehmen; somit wird auch der Wert c gleich oft, wie der Wert ∞ angenommen.

Ist dagegen c der Wert, den $f(z)$ für $z = \infty$, $q = 0$ annimmt, so sei:

$$f(z) = c + c_r q^r + \cdots, \quad c_r \neq 0, \quad r > 0.$$

$$\frac{f'(z)}{f(z)-c} \cdot \frac{dz}{dq} = \frac{r}{q} + \cdots, \quad \frac{1}{2\pi i} \int_{\frac{1}{2}+Ni}^{-\frac{1}{2}+Ni} \frac{f'(z)}{f(z)-c}\, dz = -\frac{r}{2\pi i} \int_{(K)} \frac{dq}{q} = -r,$$

und für $f(z) - c$ gilt im abgeschnittenen D.-B.:

Anzahl der Nullstellen in G — Anzahl der Pole in $G = -r$.

Nach unseren Festsetzungen nimmt $f(z)$ für $z = \infty$, $q = 0$, den Wert c von r^{ter} Ordnung an. Somit besitzt $f(z)$ den Wert c ebensooft, wie es unendlich wird.

Ist c der Wert, den $f(z)$ für $z = \varrho$ annimmt, so schneiden wir den Punkt $z = \varrho$ durch einen kleinen Kreisbogen um $z = \varrho$ ab (Fig. 12), dessen Radius ε beliebig klein ist. Ebenso den Punkt $z = -\varrho^2$. Dann kommen zu den schon berechneten Integralen noch die folgenden hinzu:

$$f(z) = c + c_r(z-\varrho)^r + \cdots, \quad c_r \neq 0, \quad r > 0.$$

$$\frac{f'(z)}{f(z)-c} = \frac{r}{z-\varrho} + \cdots$$

$$\frac{1}{2\pi i}\left[\int_{(K_\varepsilon)} + \int_{(K_\varepsilon')}\right] = \frac{1}{2\pi i}\int_{(K_\varepsilon)} \frac{r\,dz}{z-\varrho} + \frac{1}{2\pi i}\int_{(K_\varepsilon')} \frac{r\,dz}{z+\varrho^2} = -\frac{r}{\pi}\int_0^{\frac{\pi}{3}} d\varphi = -\frac{r}{3},$$

und es ist im abgeschnittenen D.-B. wie vorhin:

Anzahl der Nullstellen in G − Anzahl der Unendlichkeitsstellen in G

$$= -\frac{r}{3}.$$

Da $f(z)$ den Wert c von der $\frac{r}{3}$ten Ordnung annimmt, ist auch jetzt der Satz bewiesen. Genau so wird die Behauptung erwiesen, falls c an der Stelle $z = i$ angenommen wird. Man schlägt den Halbkreis um $z = i$ mit dem Radius ε. Wird schließlich c an einer anderen Stelle des Randes angenommen, so wird um diesen und den um eins vergrößerten der Halbkreis geschlagen, die Summe der beiden Integrale gibt in diesem Falle $2\pi i$ mal der Ordnung, mit der der betreffende Wert angenommen wird.

Damit ist bewiesen, daß jeder Wert ebensooft angenommen wird, wie die Funktion unendlich wird. Diese Zahl heißt die *Ordnung der Modulfunktion*. Es gilt folgendes

Korollar zu Satz 9: *Eine Funktion, die alle Eigenschaften einer Modulfunktion hat, einen Wert aber nirgends im D.-B. annimmt, ist eine Konstante.*

Wir machen folgende Anwendung von Satz 9:

$$f(z) = \frac{G_2^{\,3}(z) - \frac{49}{20}G_3^{\,2}(z)}{\eta^{24}(z)}$$

ist eine in der ganzen oberen Halbebene definierte analytische Funktion, die nach Satz 8 und Formel (9) bei jedem S der Modulgruppe unverändert bleibt, im endlichen überall regulär ist, da der Zähler nach Satz 5 überall regulär ist und der Nenner wegen

$$\eta^{24}(z) = q\prod_{h=1}^{\infty}(1-q^h)^{24}$$

nur für $q = 0$ oder reelle z null wird. Für $q = 0$, $z = \infty$ haben Zähler und Nenner eine Nullstelle 1. Ordnung in q, der Quotient ist somit ebenfalls regulär. $f(z)$ ist daher eine Modulfunktion, die nirgends unendlich wird, was unmöglich ist. $f(z)$ muß daher eine Konstante sein. Der Wert derselben ergibt sich aus den Formeln am Ende des § 3 für $q = 0$:

$$\frac{G_2^{\,3}(z) - \frac{49}{20}G_3^{\,2}(z)}{\eta^{24}(z)} = \lim_{q=0}\frac{\frac{1}{q}\left(G_2^{\,3} - \frac{49}{20}G_3^{\,2}\right)}{\frac{1}{q}\eta^{24}(z)} = \frac{12}{720^2 \cdot 5}(2\pi)^{12}.$$

Somit ist:

$$G_2^3(z) - \tfrac{49}{20} G_3^2(z) = \frac{12(2\pi)^{12}}{720^2 \cdot 5}\, q \prod_{h=1}^{\infty} (1-q^h)^{24}. \tag{10}$$

Die linke Seite wird deshalb für keinen endlichen Wert z der oberen Halbebene null. $G_2(z)$ und $G_3(z)$ werden niemals gleichzeitig null, und die auf S. 25 gemachte Annahme ist erwiesen.

$$\bar{J}(z) = \frac{G_2^3(z)}{G_2^3(z) - \frac{49}{20} G_3^2(z)}$$

hat somit für $q = 0$ einen Pol erster Ordnung und wird für keinen endlichen Wert von z der oberen Halbebene ∞. Da sie also den Wert ∞ nur einmal annimmt, kann sie nach Satz 9 auch jeden andern Wert nur einmal annehmen, d. h. es ist:

$$\bar{J}(z) = J(z),$$

da ja auch nach S. 25:

$$\bar{J}(\varrho) = 0, \quad \bar{J}(i) = 1, \quad \lim_{q=0} q\bar{J}(z) = \frac{1}{2^6 3^3}$$

erfüllt ist. Damit ist die *Existenz* der zu $\mathfrak{G}$ gehörigen Modulfunktion erbracht.

10. Satz: *Die Modulfunktion der Modulgruppe* $\mathfrak{G}$:

$$J(z) = \frac{G_2^3(z)}{G_2^3(z) - \frac{49}{20} G_3^2(z)}, \quad \text{wo } J(\varrho) = 0, \quad J(i) = 1, \quad \lim_{q=0} qJ(z) = \frac{1}{2^6 3^3},$$

vermittelt eine in allen Punkten des D.-B. mit Ausnahme der Eckpunkte ϱ, i, ∞ *konforme Abbildung des D.-B. auf die schlichte Ebene. Sie nimmt im D.-B. jeden Wert ein- und nur einmal an,* $\frac{dJ(z)}{dz}$ *ist nur in den drei Eckpunkten* ϱ, i, ∞ *gleich null oder unendlich.*

Ein neues Prinzip erlaubt in hervorragender Weise neue Modulfunktionen aus $J(z)$ zu bilden. Zunächst ist das Produkt aus einer Modulfunktion und einer beliebigen komplexen Konstanten wieder eine Modulfunktion. Ferner ist Summe, Produkt und Quotient von zwei Modulfunktionen wieder eine Modulfunktion; denn sie erfüllen alle Bedingungen der Definition 3. Man nennt die Menge aller Größen, die aus einer endlichen Zahl von Größen durch diese elementaren Operationen erhalten wird, den *Körper* dieser Größen.

11. Satz: *Alle Funktionen des aus* $J(z)$ *und den komplexen Zahlen gebildeten Funktionenkörpers sind Modulfunktionen der Gruppe* $\mathfrak{G}$.

Jede solche Funktion hat die Gestalt:

$$R(J(z)) \equiv \frac{c_0 J(z)^n + c_1 J(z)^{n-1} + \cdots + c_{n-1} J(z) + c_n}{J(z)^m + d_1 J(z)^{m-1} + \cdots + d_{m-1} J(z) + d_m},$$

wo die c und d beliebige, endliche, komplexe Zahlen sind. Es gilt nun aber auch die Umkehrung von Satz 11:

12. Satz: *Jede Modulfunktion der Modulgruppe $\mathfrak{G}$ gehört dem Funktionskörper von $J(z)$ an, d. h. ist in der Form $R(J(z))$ darstellbar.*

Zum Beweise nehmen wir an, $f(z)$ sei eine beliebige Modulfunktion n^{ter} Ordnung der Gruppe $\mathfrak{G}$. $f(z)$ nehme den Wert null im D.-B. an den Stellen $\nu_1, \nu_2, \ldots \nu_n$, den Wert ∞ an den Stellen $\mu_1, \mu_2, \ldots \mu_n$ an. Dabei ist jede Stelle so oft geschrieben, als ihre Ordnung angibt. Wir bilden:

$$\varphi(z) = \prod_{s=1}^{n} \frac{J(z) - J(\nu_s)}{J(z) - J(\mu_s)},$$

wobei im Zähler oder Nenner jedesmal für $(J(z) - J(\infty))$ eins zu setzen ist. $\varphi(z)$ ist eine Modulfunktion n^{ter} Ordnung; denn sie gehört dem Funktionskörper von $J(z)$ an, und Zähler oder Nenner ist sicherlich vom Grade n, wird also an n Stellen Null. Sind die ν oder μ keine Eckpunkte, so wird ja jeder Faktor von erster Ordnung Null. Sind dagegen z. B. r unter den $\mu = \infty$, so sind alle ν endlich. Nach Voraussetzung ist der Grad des Nenners um r kleiner als der Grad des Zählers, $\varphi(z)$ wird von r^{ter} Ordnung unendlich für $q = 0$. Sind unter den μ oder ν die Zahlen ϱ oder i, so wird allerdings der entsprechende Faktor von 3. oder 2. Ordnung Null, aber nach unsern Festsetzungen ist dann auch die Ordnung von $\varphi(z)$ an diesen Stellen durch 3 oder 2 zu dividieren. Somit haben $f(z)$ und $\varphi(z)$ genau dieselben Nullstellen und Pole mit denselben Ordnungen. Daher ist $f(z) : \varphi(z)$ nirgends null oder unendlich, also eine Konstante:

$$f(z) = c\varphi(z), \quad c \neq 0,$$

womit der Satz bewiesen ist.

Wir entnehmen aus dem Beweise, daß die Ordnung einer Modulfunktion $R(J(z))$ immer gleich dem Exponenten der höchsten Potenz von $J(z)$ in $R(J(z))$ ist.

13. Satz: *Ist $f_1(z)$ eine Modulfunktion n^{ter}, $f_2(z)$ eine solche m^{ter} Ordnung, so besteht zwischen ihnen eine algebraische Gleichung:*

$$\Phi(f_1(z), f_2(z)) = 0,$$

deren Koeffizienten komplexe Zahlen und deren Grad in $f_1(z)$ m, in $f_2(z)$ n ist.

Denn es ist: $f_1(z) = R_1(J(z)), \quad f_2(z) = R_2(J(z)),$

wo R_1 in $J(z)$ vom n^{ten}, R_2 in $J(z)$ vom m^{ten} Grade ist. Die Resultante beider Beziehungen ergibt die gesuchte Gleichung.

$\mathfrak{G}$ ist die *Modulgruppe 1. Stufe* (s. S. 3). Entsprechend heißt $J(z)$ eine *Modulfunktion 1. Stufe* und $R(J(z))$ der *Modulkörper 1. Stufe*. Jede Funktion:

$$\frac{c_1 J(z) + c_2}{c_3 J(z) + c_4}, \quad c_1 c_4 - c_2 c_3 \neq 0,$$

wo c_1, c_2, c_3, c_4 komplexe Zahlen sind, bildet ebenfalls den D.-B. auf die schlichte Ebene ab. Für alle diese Funktionen ist der D.-B. zugleich *Fundamentalbereich*. Entsprechend kann man für die Modulgruppe $\mathfrak{G}^{(n)}$ n^{ter} Stufe die *Modulfunktionen* n^{ter} *Stufe* bilden. Man hat dann den D.-B. von $\mathfrak{G}^{(n)}$ zugrunde zu legen.

Für das Folgende ist es wichtig, an Stelle von z homogene Koordinaten einzuführen: $z = \omega_2 : \omega_1$, wo ω_1 und ω_2 an die Bedingung gebunden sind, daß ihr Quotient einen *positiven* Imaginärteil hat. Statt $G_2(z)$ und $G_3(z)$ führt man dann ein:

$$g_2(\omega_1, \omega_2) = 60 \sum_{n,m=-\infty}^{+\infty}{}' \frac{1}{(n\omega_2 + m\omega_1)^4},$$

$$g_3(\omega_1, \omega_2) = 140 \sum_{n,m=-\infty}^{\infty}{}' \frac{1}{(n\omega_2 + m\omega_1)^6}, \tag{11}$$

$$G(\omega_1, \omega_2) = \tfrac{1}{16}(g_2^3 - 27 g_3^2).$$

Unter der Operation S, $S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ versteht man dann das Vertauschen von ω_1, ω_2 durch:

$$\omega_2' = \alpha\omega_2 + \beta\omega_1,$$

$$\omega_1' = \gamma\omega_2 + \delta\omega_1.$$

g_2, g_3, G sind unendliche Formen von ω_1 und ω_2 der Dimensionen $-4, -6, -12$. Sie bleiben bei Anwendung von S ungeändert. Es wird:

$$G_2(z) = \frac{\omega_1^4}{60} g_2(\omega_1, \omega_2); \quad G_3(z) = \frac{\omega_1^6}{140} g_3(\omega_1, \omega_2);$$

$$G_2^3(z) - \tfrac{49}{20} G_3^2(z) = \frac{\omega_1^{12}}{60^3}(g_2^3 - 27 g_3^2) = \frac{\omega_1^{12}}{2^3 \cdot 3^3 \cdot 5^3} G(\omega_1, \omega_2); \tag{12}$$

$$J(z) = \frac{g_2^3(\omega_1, \omega_2)}{16\, G(\omega_1, \omega_2)}.$$

Es ist praktisch, statt $J(z)$ eine Modulfunktion einzuführen, deren Residuum in bezug auf q eins ist:

$$j(\omega_1, \omega_2) = 2^6 \cdot 3^3 J(z) = \frac{4 \cdot 27 g_2^3(\omega_1, \omega_2)}{G(\omega_1, \omega_2)} = \frac{1}{q} + \sum_{h=0}^{\infty} c_h q^h. \tag{13}$$

$j(\omega_1, \omega_2)$ heißt die *vollständige Invariante*. Sie genügt den Bedingungen:

$$j(1, \varrho) = 0, \quad j(1, i) = 2^6 \cdot 3^3, \quad j(\omega_1, \omega_2) = \frac{1}{q} + \sum_{h=0}^{\infty} c_h q^h. \tag{14}$$

Da $j(\omega_1, \omega_2)$ homogen in ω_1 und ω_2 ist, werden wir auch häufig $j(z)$ schreiben. Für $G(\omega_1, \omega_2)$ gilt nach (12) und (10):

$$G(\omega_1, \omega_2) = \frac{(2\pi)^{12}}{\omega_1{}^{12} \cdot 2^4} q \prod_{h=1}^{\infty} (1 - q^h)^{24}.$$

14. **Satz:** *Die Zahlen c der Reihenentwicklung:*

$$j(z) = \frac{1}{q} + \sum_{h=0}^{\infty} c_h q^h$$

sind ganze, rationale Zahlen.

Denn es ist nach (6), (10) und (12):

$$j(z) = \frac{\left[1 + 240 \sum_{h=1}^{\infty} h^3 \frac{q^h}{1 - q^h}\right]^3}{q \prod_{h=1}^{\infty} (1 - q^h)^{24}}.$$

II. Die Transformationsgleichungen.

1. Die Transformationsgruppen n^{ter} Ordnung.

Über die Kongruenzgruppe n^{ter} Stufe $\mathfrak{G}^{(n)}$, die durch $S^{(n)}$ gegeben ist,

wo $$S^{(n)} = \begin{pmatrix} \alpha^{(n)} & \beta^{(n)} \\ \gamma^{(n)} & \delta^{(n)} \end{pmatrix} \equiv E \pmod{n},$$

müssen wir noch weitere Eigenschaften herleiten.

15. Satz: *Die Kongruenzgruppe n^{ter} Stufe ist eine invariante Untergruppe (Normalteiler) der Modulgruppe $\mathfrak{G}$.*

Eine Untergruppe ist invariant, wenn für jedes S von $\mathfrak{G}$ und jedes $S^{(n)}$ von $\mathfrak{G}^{(n)}$: $$S^{-1} S^{(n)} S$$

wieder der Untergruppe angehört. Ist:

$$S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \quad S^{-1} = \begin{pmatrix} -\delta & \beta \\ \gamma & -\alpha \end{pmatrix},$$

so folgt aus (2), S. 2:

$$S^{-1} S^{(n)} S =$$

$$= \begin{pmatrix} -\alpha\delta\,\alpha^{(n)} - \gamma\delta\,\beta^{(n)} + \alpha\beta\,\gamma^{(n)} + \beta\gamma\,\delta^{(n)} & -\beta\delta\,\alpha^{(n)} - \delta^2\,\beta^{(n)} + \beta^2\,\gamma^{(n)} + \beta\delta\,\delta^{(n)} \\ \alpha\gamma\,\alpha^{(n)} + \gamma^2\,\beta^{(n)} - \alpha^2\,\gamma^{(n)} - \alpha\gamma\,\delta^{(n)} & \beta\gamma\,\alpha^{(n)} + \gamma\delta\,\beta^{(n)} - \alpha\beta\,\gamma^{(n)} - \alpha\delta\,\delta^{(n)} \end{pmatrix}$$

$$\equiv \begin{pmatrix} -\alpha\delta + \beta\gamma & 0 \\ 0 & -\alpha\delta + \beta\gamma \end{pmatrix} \equiv E \pmod{n}.$$

Die im 1. Kap., S. 3, aufgestellten $s_1, s_2, s_3, \ldots s_\mu$ bilden (mod. n) die Faktorgruppe $\mathfrak{G}/\mathfrak{G}^{(n)}$.[1])

Es seien a, b, c, d vier ganze, rationale Zahlen *ohne gemeinsamen Teiler*, für die: $$ad - bc = n$$

größer als Null sei. $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ heißt dann eine *Substitution n^{ter} Ordnung*. Zwei T heißen wieder einander gleich, wenn die a, b, c, d ihren entsprechenden alle gleich, oder alle entgegengesetzt gleich sind. Hätten a, b, c, d einen gemeinsamen Teiler, so muß man sie durch denselben kürzen, und die Ordnung n ist durch das Quadrat desselben zu reduzieren. T gehört für $n > 1$ niemals der Modulgruppe an.

1) Siehe über die gruppentheoretischen Begriffe: Speiser, Theorie der Gruppen von endlicher Ordnung. Berlin 1923. S. 14ff.

Die inverse Substitution von T ist:

$$T^{-1} = \begin{pmatrix} -d & b \\ c & -a \end{pmatrix}, \quad T^{-1}T = \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E.$$

Wir transformieren alle $S^{(n)}$ von $\mathfrak{G}^{(n)}$ mit T, bilden also:

$$T^{-1}S^{(n)}T = \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

wo A, B, C, D teilerfremd vorausgesetzt werden.

16. Satz: *Die Substitutionen $T^{-1}S^{(n)}T$ sind Substitutionen der Modulgruppe $\mathfrak{G}$.*

Denn es ist:

$$T^{-1}S^{(n)}T = \begin{pmatrix} \overline{A} & \overline{B} \\ \overline{C} & \overline{D} \end{pmatrix}, \quad \text{wo:} \quad \begin{aligned} \overline{A} &= ad\alpha^{(n)} + cd\beta^{(n)} - ab\gamma^{(n)} - bc\delta^{(n)} \\ \overline{B} &= bd\alpha^{(n)} + d^2\beta^{(n)} - b^2\gamma^{(n)} - bd\delta^{(n)} \\ \overline{C} &= -ac\alpha^{(n)} - c^2\beta^{(n)} + a^2\gamma^{(n)} + ac\delta^{(n)} \\ \overline{D} &= -bc\alpha^{(n)} - cd\beta^{(n)} + ab\gamma^{(n)} + ad\delta^{(n)} \end{aligned}$$

Da $S^{(n)} \equiv E (\text{mod. } n)$, $ad - bc = n$ ist, so wird:

$$\overline{A} \equiv \overline{B} \equiv \overline{C} \equiv \overline{D} \equiv 0 \pmod{n}.$$

Also:

$$T^{-1}S^{(n)}T = \begin{pmatrix} \frac{A}{n} & \frac{B}{n} \\ \frac{\overline{C}}{n} & \frac{\overline{D}}{n} \end{pmatrix}, \quad \begin{vmatrix} \frac{\overline{A}}{n} & \frac{\overline{C}}{n} \\ \frac{\overline{B}}{n} & \frac{\overline{D}}{n} \end{vmatrix} = \frac{1}{n^2} \begin{vmatrix} -d & b \\ c & -a \end{vmatrix} \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} \begin{vmatrix} a & b \\ c & d \end{vmatrix} = 1.$$

Die ganzen Zahlen $\frac{\overline{A}}{n}, \frac{\overline{B}}{n}, \frac{\overline{C}}{n}, \frac{\overline{D}}{n}$ sind ohne gemeinsamen Teiler.

17. Satz: *Die Substitutionen $T^{-1}S^{(n)}T$ bilden eine Untergruppe der Modulgruppe, falls T eine feste Substitution n^{ter} Ordnung ist und $S^{(n)}$ alle Substitutionen der Kongruenzgruppe n^{ter} Stufe $\mathfrak{G}^{(n)}$ durchläuft.*

Denn E liegt in $\mathfrak{G}^{(n)}$, $T^{-1}S^{(n)}T$ ist die Inverse von $T^{-1}S^{(n)-1}T$, und

$$T^{-1}S_2^{(n)}T \cdot T^{-1}S_1^{(n)}T = T^{-1}S_2^{(n)}S_1^{(n)}T.$$

Diese Gruppe heißt *die zu T gehörige Transformationsgruppe n^{ter} Ordnung* $\mathfrak{T}_n(T)$. Es fragt sich, ob zu verschiedenen T auch verschiedene $\mathfrak{T}_n(T)$ gehören oder nicht?

Ist S eine beliebige Substitution der Modulgruppe, so sind auch ST und TS Substitutionen n^{ter} Ordnung. Denn die Determinante von ST oder TS ist das Produkt der Determinanten von S und T, also $1 \cdot n$.

Ferner sind in: $$ST = \begin{pmatrix} \alpha a + \beta c & \alpha b + \beta d \\ \gamma a + \delta c & \gamma b + \delta d \end{pmatrix}$$

die vier Größen ganz und teilerfremd.

18. Satz: *Jede Substitution ST erzeugt die gleiche Transformationsgruppe $\mathfrak{T}_n(T)$, wie T.*

Denn es ist:

$$(ST)^{-1} = T^{-1}S^{-1}, \quad (ST)^{-1}S^{(n)}(ST) = T^{-1}S^{-1}S^{(n)}ST.$$

Nach Satz 15 ist $S^{-1}S^{(n)}S$ wieder in $\mathfrak{G}^{(n)}$. Umgekehrt ist:

$$T^{-1}S^{(n)}T = T^{-1}S^{-1} \cdot SS^{(n)}S^{-1} \cdot ST = (ST)^{-1}SS^{(n)}S^{-1}(ST).$$

Satz 18 erlaubt zu zeigen, daß es nur eine endliche Anzahl von Transformationsgruppen n^{ter} Ordnung gibt.

Zunächst wählen wir T so, daß $c = 0$ ist. Denn andernfalls können wir γ, δ ganz und teilerfremd so wählen, daß:

$$\gamma a + \delta c = 0$$

ist. Nun bestimmen wir α, β als ganze Zahlen so, daß $\alpha\delta - \beta\gamma = 1$, und setzen $S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. Dann hat ST die gewünschte Eigenschaft $c = 0$. In

$$T = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

darf man $d > 0$, $a > 0$ voraussetzen. a und d sind Teiler von n, also *gibt es nur so viele Möglichkeiten für a, d, als n Teiler besitzt.* Wenden wir auf T die Substitution $\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$ an, wo u eine beliebige ganze Zahl ist, so ist

$$T_1 = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} T = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & b + ud \\ 0 & d \end{pmatrix}.$$

T_1 erzeugt die gleiche Transformationsgruppe wie T. u kann so bestimmt werden, daß $0 \leqq b + ud < d$. Sind in T_1 a und d als Teiler von n gewählt, so bleiben für den letzten Koeffizienten b nur noch die Zahlen $0, 1, 2, \ldots, d-1$ übrig.

19. Satz: *Es gibt nur endlich viele Transformationsgruppen n^{ter} Ordnung. Jede Substitution n^{ter} Ordnung läßt sich in der Form ST darstellen, wo T eine bestimmte unter endlich vielen Substitutionen n^{ter} Ordnung und S eine Substitution der Modulgruppe ist.*

Wir bezeichnen die genaue Zahl der Transformationsgruppen mit $\psi(n)$.

20. Satz: *Sind $T_1 = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}$, $T_2 = \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}$ zwei Substitutionen n^{ter} Ordnung, die den Bedingungen genügen:*

$$a_1 d_1 = n, \; a_2 d_2 = n, \; d_1 > 0, \; d_2 > 0, \; 0 \leqq b_1 < d_1, \; 0 \leqq b_2 < d_2,$$

so folgt aus $T_2 = ST_1$, S eine Substitution der Modulgruppe, auch: $T_1 = T_2$.

Denn für $S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ folgt:

$$\begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} = \begin{pmatrix} \alpha a_1 & \alpha b_1 + \beta d_1 \\ \gamma a_1 & \gamma b_1 + \delta d_1 \end{pmatrix},$$

woraus $\gamma a_1 = 0$, $\gamma = 0$, $\alpha = \delta = +1$. Also $a_1 = a_2$, $d_1 = d_2$ und

$b_2 = b_1 + \beta d_1$. Dies ist nur mit den Annahmen vereinbar, wenn $\beta = 0$, $b_1 = b_2$, $T_1 = T_2$ ist.

21. Satz: *Genügen T_1 und T_2 den Bedingungen von Satz 20, so gibt es zwei Substitutionen der Modulgruppe S_1 und S_2, so daß*

$$S_1 T_1 = T_2 S_2.$$

Wir beweisen den Satz für $T_1 = \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}$; denn dann folgt für beliebige T_2 und T_3: $T_1 = S_1^{-1} T_2 S_2 = \bar{S}_1^{-1} T_3 S_3$ oder $\bar{S}_1 S_1^{-1} T_2 = T_3 S_3 S_2^{-1}$. Für $T_1 = \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}$ ist, wenn $S_1 = \begin{pmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{pmatrix}$, $S_2 = \begin{pmatrix} \alpha_2 & \beta_2 \\ \gamma_2 & \delta_2 \end{pmatrix}$ gesetzt wird:

$$\begin{pmatrix} \alpha_1 n & \beta_1 \\ \gamma_1 n & \delta_1 \end{pmatrix} = \begin{pmatrix} \alpha_2 a_2 + \gamma_2 b_2 & \beta_2 a_2 + \delta_2 b_2 \\ \gamma_2 d_2 & \delta_2 d_2 \end{pmatrix},$$

oder (die beiden Möglichkeiten des Vorzeichens können hier wegfallen):

$$\alpha_1 n = \alpha_2 a_2 + \gamma_2 b_2, \quad \beta_1 = \alpha_2 \beta_2 + b_2 \delta_2,$$

$$\gamma_1 n = \gamma_2 d_2, \qquad \delta_1 = d_2 \delta_2,$$

woraus: $$\gamma_2 = a_2 \gamma_1, \quad \alpha_2 = \alpha_1 d_2 - \gamma_1 b_2.$$

Ist t der größte gemeinsame Teiler von a_2 und b_2, so bestimme man β_2, δ_2 so, daß

$$t = a_2 \beta_2 + b_2 \delta_2,$$

und δ_2 zu t teilerfremd sei. Wir setzen:

$$\beta_1 = t, \quad \delta_1 = d_2 \delta_2.$$

Dann ist δ_1 zu t teilerfremd, da t in a_2 und b_2 aufgeht, also zu d_2 teilerfremd sein muß, gemäß der Annahme, daß a_2, b_2, d_2 ohne gemeinsamen Teiler sind. Zu β_1 und δ_1 können wir deshalb α_1, γ_1 so bestimmen, daß

$$\alpha_1 \delta_1 - \beta_1 \gamma_1 = 1$$

ist. Setzt man noch:

$$\alpha_2 = \alpha_1 d_2 - \gamma_1 b_2, \quad \gamma_2 = a_2 \gamma_1,$$

so sind die vier obigen Gleichungen erfüllt, und es ist:

$$\alpha_2 \delta_2 - \beta_2 \gamma_2 = (\alpha_1 d_2 - \gamma_1 b_2) \frac{a_2 \delta_1}{n} - \frac{\beta_1 d_2 - b_2 \delta_1}{n} a_2 \gamma_1$$

$$= \frac{1}{n} (\alpha_1 \delta_1 n - \gamma_1 \delta_1 a_2 b_2 - \beta_1 \gamma_1 n + \gamma_1 \delta_1 a_2 b_2) = \alpha_1 \delta_1 - \beta_1 \delta_1 = 1.$$

22. Satz: *Die Transformationsgruppen sind konjugierte Untergruppen der Modulgruppe.*

In der Tat ist: $S_2^{-1} \mathfrak{T}_n(T_2) S_2 = \mathfrak{T}_n(S_1 T_1) = \mathfrak{T}_n(T_1)$,

weil $$S_2^{-1}(T_2^{-1} S^{(n)} T_2) S_2 = (T_2 S_2)^{-1} S^{(n)} (T_2 S_2) = (S_1 T_1)^{-1} S^{(n)} (S_1 T_1)$$

$$= T_1^{-1} (S_1^{-1} S^{(n)} S_1) T_1.$$

23. **Satz:** *Die Anzahl $\psi(n)$ der Transformationsgruppen n^{ter} Ordnung ist gleich der Anzahl der verschiedenen Substitutionen n^{ter} Ordnung* $T = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, *für die* $ad = n, \quad d > 0, \quad 0 \leqq b < d.$

Im anderen Falle muß es nämlich zwei Substitutionen T_1 und T_2 geben, so daß für jedes $S_1^{(n)}$ von $\mathfrak{G}^{(n)}$ ein $S_2^{(n)}$ existiert, für das

$$T_1^{-1} S_1^{(n)} T_1 = T_2^{-1} S_2^{(n)} T_2.$$

Als T_2 dürfen wir $T_2 = \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}$ wählen; denn nach Satz 21 gibt es zwei Modulsubstitutionen S_1 und S_2, so daß

$$T_2 S_2 = S_1 \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}$$

ist, und es wird

$$S_2^{-1} T_2^{-1} S_2^{(n)} T_2 S_2 = (T_2 S_2)^{-1} S_2^{(n)} (T_2 S_2) = \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}^{-1} (S_1^{-1} S_2^{(n)} S_1) \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}.$$

Statt T_1 ist daher nur $\overline{T}_1$ in $T_1 S_2 = \overline{S}_2 \overline{T}_1$ zu nehmen. Es sei somit

$$T_1 = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, \quad T_2 = \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}, \quad \text{wo} \quad ad = n, \quad 0 \leqq b < d, \quad d > 0.$$

Die obige Gleichung lautet ausgeschrieben

$$\begin{pmatrix} -\alpha_1^{(n)} + ab\dfrac{\gamma_1^{(n)}}{n} & -bd\dfrac{\alpha_1^{(n)} - \delta_1^{(n)}}{n} - d^2\dfrac{\beta_1^{(n)}}{n} + b^2\dfrac{\gamma_1^{(n)}}{n} \\ -a^2\dfrac{\gamma_1^{(n)}}{n} & -ab\dfrac{\gamma_1^{(n)}}{n} - \delta_1^{(n)} \end{pmatrix} = \begin{pmatrix} \alpha_2^{(n)} & \dfrac{\beta_2^{(n)}}{n} \\ n\gamma_2^{(n)} & \delta_2^{(n)} \end{pmatrix}.$$

Setzt man z. B. $S_1^{(n)} = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}$, so folgt:

$$-a^2 = n\gamma_2^{(n)}, \quad \text{oder} \quad a^2 \equiv 0 \pmod{n^2}, \quad a \equiv 0 \pmod{n}.$$

Dann ist $d = 1$, d. h. $b = 0$, $T_1 = T_2$.

24. **Satz:** *Die Anzahl $\psi(n)$ der Transformationsgruppen ist*

$$\psi(n) = n \prod_{(p)} \left(1 + \frac{1}{p}\right),$$

wo das Produkt über alle voneinander verschiedenen Primzahlen p von n zu erstrecken ist.

Nach Satz 23 haben wir nur zu entscheiden, wie viele $T = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ es gibt, für die $ad = n$, $d > 0$, $0 \leqq b < d$, und a, b, d keinen gemeinsamen Teiler haben. Ist $\varphi(t)$ die *Euler*sche Funktion, die angibt, wie viele zu t teilerfremde Zahlen zwischen 0 und t liegen, so ist die Anzahl der möglichen b, falls a, d fest gewählt sind und den größten gemeinsamen Teiler t haben,

$$\varphi(t) \cdot \frac{d}{t} \quad \text{und} \quad \psi(n) = \sum_{(d)} \varphi(t) \frac{d}{t},$$

summiert über alle Teiler d von n, mit Einschluß von $d = 1$ und $d = n$.

Sind n_1 und n_2 zwei teilerfremde ganze Zahlen, so ist wegen der bekannten Eigenschaft von $\varphi(t)$:

$$\psi(n_1)\psi(n_2) = \sum_{(d_1,d_2)} \varphi(t_1)\varphi(t_2)\frac{d_1 d_2}{t_1 t_2} = \sum_{(d_1,d_2)} \varphi(t_1 t_2)\frac{d_1 d_2}{t_1 t_2}.$$

Denn t_1 und t_2 sind teilerfremd, da es n_1 und n_2 sind. Die Summe rechts durchläuft alle möglichen Teilerkombinationen d_1, d_2, das Produkt $d_1 d_2$ alle Teiler von $n_1 n_2$. Die Summe rechts ist daher $\psi(n_1 n_2)$:

$$\psi(n_1)\psi(n_2) = \psi(n_1 n_2).$$

Somit muß $\psi(n)$ nur für die Primzahlpotenz p^r berechnet werden. Die Teiler sind hier $1, p, p^2, \ldots p^{r-1}, p^r$. Für $d = p^h$ ist $a = p^{r-h}$, also $t = p^{r-h}$ oder $= p^h$, je nachdem $h > \frac{r}{2}$ oder $\leqq \frac{r}{2}$ ist. Daraus folgt:

$$\psi(p^r) = \sum_{h=0}^{\left[\frac{r}{2}\right]} \varphi(p^h) + \sum_{h=\left[\frac{r}{2}\right]+1}^{r} \varphi(p^{r-h})p^{2h-r}$$

$$= 1 + \sum_{h=1}^{\left[\frac{r}{2}\right]} (p^h - p^{h-1}) + \sum_{h=\left[\frac{r}{2}\right]+1}^{r-1} (p^h - p^{h-1}) + p^r$$

$$= p^{r-1} + p^r = p^r\left(1 + \frac{1}{p}\right),$$

und der Satz ist bewiesen.

25. Satz: *Jede Transformationsgruppe n^{ter} Ordnung ist eine Untergruppe der Modulgruppe $\mathfrak{G}$ vom Index $\mu(n)$.* $(n > 2)$

Konjugierte Untergruppen haben denselben Index. Wir brauchen denselben somit nur für $\mathfrak{T}_n(T)$ zu berechnen, wo $T = \left(\begin{smallmatrix} n & 0 \\ 0 & 1 \end{smallmatrix}\right)$ ist. Die Substitutionen dieser Gruppe haben die Gestalt:

$$T^{-1}S^{(n)}T = \begin{pmatrix} \alpha^{(n)} & \frac{\beta^{(n)}}{n} \\ n\gamma^{(n)} & \delta^{(n)} \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \text{ wo bei geeigneter Wahl der Vorzeichen}$$

$$\alpha \equiv \delta \equiv 1 \,(\text{mod. } n), \quad \gamma \equiv 0 \,(\text{mod. } n^2).$$

Nach der Formel § 1, S. 6, ist

$$\mu(n^2) = \frac{n^6}{2}\prod_{(p)}\left(1 - \frac{1}{p^2}\right). \quad (n > 2)$$

Alle Substitutionen der Kongruenzgruppe $n^{2\,ter}$ Ordnung liegen in $\mathfrak{T}_n(T)$. Umgekehrt sind nur diejenigen Substitutionen von $\mathfrak{T}_n(T)$ in $\mathfrak{G}^{(n^2)}$, für die auch β durch n^2 teilbar ist. Von den $\mu(n^2)$ Nebengruppen,

in die sich $\mathfrak{G}$ mittels $\mathfrak{G}^{(n^2)}$ zerlegen läßt, gehören alle diejenigen zu $\mathfrak{T}_n(T)$, für die $\alpha \equiv \delta \equiv 1 \pmod{n}$, $\gamma \equiv 0 \pmod{n^2}$, β aber einen beliebigen Rest $(\text{mod. } n^2)$ läßt. Da $\alpha\delta \equiv 1 (\text{mod. } n^2)$, so ist α oder $\delta (\text{mod. } n^2)$ bestimmt. α und δ können noch n verschiedene Werte $(\text{mod. } n^2)$ annehmen. β kann $n^2 (\text{mod. } n^2)$ verschiedene Werte annehmen. Das macht zusammen $n \cdot n^2 = n^3$ verschiedene Kombinationen $(\text{mod. } n^2)$. Somit bleiben

$$\frac{\mu(n^2)}{n^3} = \frac{n^2}{2} \prod_{(p)} \left(1 - \frac{1}{p^2}\right) = \frac{1}{2} \prod_{(p)} p^{3r-2}(p^2 - 1) = \mu(n) \qquad (n > 2)$$

Systeme von Nebengruppen übrig, die die Anordnungen der S von $\mathfrak{G}$ bezüglich $\mathfrak{T}_n(T)$, d. h. dessen Index geben.

2. Modulfunktionen n^{ter} Stufe.

Es seien $T_\nu = \begin{pmatrix} a_\nu & b_\nu \\ 0 & d_\nu \end{pmatrix}$, $a_\nu d_\nu = n$, $d_\nu > 0$, $0 \leqq b_\nu < d_\nu$, a_ν, b_ν, d_ν ohne gemeinsamen Teiler, $\nu = 1, 2, \ldots \psi(n)$, die $\psi(n)$ Substitutionen, die die $\psi(n)$ Transformationsgruppen festlegen. Wir definieren die $\psi(n)$ Funktionen

$$\tau_\nu = j(T_\nu z) = j\left(\frac{a_\nu z + b_\nu}{d_\nu}\right), \quad \nu = 1, 2, \cdots, \psi(n).$$

$j(z)$ ist die in Kap. 1, § 4 definierte vollständige Invariante. Wenn wir irgendeine der $\psi(n)$ Funktionen herausgreifen, so lassen wir den Index weg.

26. Satz: $\tau = j(Tz)$ *bleibt ungeändert, wenn auf* z *eine Substitution der Transformationsgruppe* $\mathfrak{T}_n(T)$ *ausgeübt wird.*

Denn ist $T^{-1}S^{(n)}T$ irgendein Element von $\mathfrak{T}_n(T)$, so ist wegen $j(Sz) = j(z)$: $\quad j(T(T^{-1}S^{(n)}Tz)) = j(S^{(n)}Tz) = j(Tz)$.

27. Satz: *Jede der* $\psi(n)$ *Funktionen* $\tau_\nu = j(T_\nu z)$ *ist eine Modulfunktion* n^{ter} *Stufe, d. h. bleibt ungeändert bei jedem* $S^{(n)}$ *von* $\mathfrak{G}^{(n)}$.

Denn $\quad j(T_\nu S^{(n)} z) = j(T_\nu S^{(n)} T_\nu^{-1} T_\nu z) = j(S T_\nu z) = j(T_\nu z)$,

da nach Satz 16 S eine Substitution der Modulgruppe ist.

28. Satz: *Durch die Substitutionen* S *von* $\mathfrak{G}$ *werden die Funktionen* $\tau_\nu = j(T_\nu z)$ *untereinander vertauscht.*

Denn da $T_\nu S$ wieder eine Substitution n^{ter} Ordnung ist, so muß nach den Sätzen 19 und 23

$$T_\nu S = \bar{S}\, T_\mu,$$

wo μ eine bestimmte der Zahlen $1, 2, \ldots, \psi(n)$ ist. Also ist:

$$j(T_\nu Sz) = j(\bar{S}\, T_\mu z) = j(T_\mu z).$$

Niemals wird man für zwei verschiedene ν dasselbe μ erhalten. Denn da $j(z)$ im D.-B. jeden Wert nur einmal annimmt, so folgt aus:

$$j(T_{\nu_1} Sz) = j(T_{\nu_2} Sz):$$
$$T_{\nu_1} Sz = \bar{S}\, T_{\nu_2} Sz \quad \text{oder} \quad T_{\nu_1} = \bar{S}\, T_{\nu_2},$$

was nach Satz 20 $T_{\nu_1} = T_{\nu_2}$ zur Folge hat. Daraus ergibt sich noch der

29. Satz: *Die Funktionswerte* $j(T_\nu z) = \tau_\nu$, $\nu = 1, 2, \ldots, \psi(n)$ *sind in der oberen Halbebene nicht identisch gleich.*

Umgekehrt gilt der

30. Satz: *Es gibt stets ein* S, *das ein bestimmtes* τ_ν *in ein bestimmtes* τ_μ *überführt.*

Denn nach Satz 21 gibt es zwei S: S_1 und S_2, so daß

$$S_1 T_\mu = T_\nu S_2.$$

Also wird

$$j(T_\nu S_2 z) = j(S_1 T_\mu z) = j(T_\mu z) = \tau_\mu.$$

Außer den eben definierten Modulfunktionen werden wir noch andere Modulfunktionen n^{ter} Stufe notwendig haben. Wir setzen nach (11) und (12), S. 31

$$G(z) = G(1, z) = \tfrac{1}{16}(g_2^3 - 27 g_3^2) = 2^2 \cdot 3^3 \cdot 5^3 (G_2^3(z) - \tfrac{49}{20} G_3^2(z)).$$

Dann ist nach Satz 8:

$$G(Sz) = (\gamma z + \delta)^{12} G(z), \quad S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

31. Satz: *Die Funktionen*

$$\eta_\nu = \frac{a_\nu^{12} G(T_\nu z)}{G(z)}, \quad \nu = 1, 2, \ldots, \psi(n),$$

sind Modulfunktionen n^{ter} *Stufe.*

Ist $S^{(n)} = \begin{pmatrix} \alpha^{(n)} & \beta^{(n)} \\ \gamma^{(n)} & \delta^{(n)} \end{pmatrix}$, $T = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, so folgt:

$$\frac{a^{12} G(T S^{(n)} z)}{G(S^{(n)} z)} = \frac{a^{12} G(T S^{(n)} T^{-1} T z)}{(\gamma^{(n)} z + \delta^{(n)})^{12} G(z)}.$$

$T S^{(n)} T^{-1}$ gehört $\mathfrak{T}_n(T^{-1})$ an:

$$T S^{(n)} T^{-1} = \begin{pmatrix} \alpha^{(n)} + d b \dfrac{\gamma^{(n)}}{n} & \dfrac{1}{n}(-a b \alpha^{(n)} + a^2 \beta^{(n)} - b^2 \gamma^{(n)} + b a \delta^{(n)}) \\ d^2 \dfrac{\gamma^{(n)}}{n} & -d b \dfrac{\gamma^{(n)}}{n} + \delta^{(n)} \end{pmatrix}.$$

Also:

$$\begin{aligned} G(T S^{(n)} T^{-1} T z) &= \left(d^2 \frac{\gamma^{(n)}}{n} T z - d b \frac{\gamma^{(n)}}{n} + \delta^{(n)}\right)^{12} G(T z) \\ &= \left(d^2 \frac{\gamma^{(n)}}{n} \frac{a z + b}{d} - d b \frac{\gamma^{(n)}}{n} + \delta^{(n)}\right)^{12} G(T z) \\ &= (\gamma^{(n)} z + \delta^{(n)})^{12} G(T z) \end{aligned}$$

und

$$\frac{a^{12} G(T S^{(n)} z)}{G(S^{(n)} z)} = \frac{a^{12} G(T z)}{G(z)}.$$

32. Satz: *Die Funktionen* η_ν *werden für keinen endlichen Punkt der oberen Halbebene null oder unendlich.*

Dies folgt aus (10), S. 29.

Wie ändert sich η_ν, wenn wir eine beliebige Substitution S ausführen? Es sei wieder nach Satz 19:

$$T_\nu S = S_1 T_\mu,\ T_\nu = \begin{pmatrix} a_\nu & b_\nu \\ 0 & d_\nu \end{pmatrix},\ T_\mu = \begin{pmatrix} a_\mu & b_\mu \\ 0 & d_\mu \end{pmatrix},\ S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},\ S_1 = \begin{pmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{pmatrix};$$

$$a_\nu d_\nu = n,\ a_\mu d_\mu = n,\ \alpha\delta - \beta\gamma = 1,\ \alpha_1\delta_1 - \beta_1\gamma_1 = 1.$$

Dann ergibt sich aus $S_1 = T_\nu S T_\mu^{-1}$:

$$\alpha_1 = \frac{1}{n}(a_\nu\alpha + b_\nu\gamma)d_\mu, \quad \beta_1 = \frac{1}{n}(-(a_\nu\alpha + b_\nu\gamma)b_\mu + (a_\nu\beta + b_\nu\delta)a_\mu),$$

$$\gamma_1 = \frac{1}{n}d_\nu\gamma d_\mu, \qquad \delta_1 = \frac{1}{n}d_\nu(-\gamma b_\mu + \delta a_\mu),$$

wo alle Zahlen ganz sein müssen. Somit ist:

$$G(T_\nu S z) = G(S_1 T_\mu z) = (\gamma_1 T_\mu z + \delta_1)^{12} G(T_\mu z),$$

$$\gamma_1 T_\mu z + \delta_1 = \frac{1}{n}\left[d_\nu\gamma d_\mu \frac{a_\mu z + b_\mu}{d_\mu} + d_\nu(-\gamma b_\mu + \delta a_\mu)\right]$$

$$= \frac{a_\mu d_\nu}{n}(\gamma z + \delta) = \frac{a_\mu}{a_\nu}(\gamma z + \delta), \qquad \text{und:}$$

$$\eta_\nu(Sz) = \frac{a_\nu^{12} G(T_\nu S z)}{G(Sz)} = \frac{a_\nu^{12} a_\mu^{12}(\gamma z + \delta)^{12} G(T_\mu z)}{a_\nu^{12}(\gamma z + \delta)^{12} G(z)} = \frac{a_\mu^{12} G(T_\mu z)}{G(z)} = \eta_\mu.$$

Diese Beziehung gibt den Grund an, warum man bei der Definition von η_ν den Faktor a_ν^{12} hat hinzufügen müssen. Zugleich folgt der

33. Satz: *Ist S eine Substitution von $\mathfrak{G}$, für die*

$$T_\nu S = S_1 T_\mu,$$

so geht η_ν bei Anwendung von S in η_μ, τ_ν in τ_μ über.

3. Die Transformationsgleichungen.

Die Bezeichnungen des letzten Paragraphen sollen weiter bestehen bleiben.

34. Satz: *Die symmetrischen Funktionen von $\tau_1, \tau_2, \ldots \tau_{\psi(n)}$ sind Funktionen des Funktionenkörpers von $j(z)$.*

Denn sie bleiben nach Satz 28 bei Ausübung jedes S unverändert, sind in der ganzen oberen Halbebene regulär und besitzen als Funktionen von q höchstens Pole. Letzteres sieht man so ein: In $\tau_\nu = j\left(\frac{a_\nu z + b_\nu}{d_\nu}\right)$ tritt q in der Gestalt: $e^{2\pi i\frac{a_\nu z + b_\nu}{d_\nu}} = cq^{\frac{a_\nu}{d_\nu}} = cq^{\frac{a_\nu^2}{n}}$

auf, die Reihenentwicklung der symmetrischen Funktion beginnt somit so:

$$= dq^{\frac{r}{n}} + \cdots,$$

wo r eine bestimmte ganze Zahl ist. Da die Reihe bei Vertauschung von z mit $z + 1$ ungeändert bleibt, so muß aber r ein Vielfaches von n sein.

Da diese drei Punkte für die symmetrische Funktion erfüllt sind, so muß sie eine Modulfunktion sein, also nach Satz 12 dem Funktionskörper $j(z)$ angehören.

35. Satz: *Die elementarsymmetrischen Funktionen der* $\tau_1, \tau_2, \ldots \tau_{\psi(n)}$ *sind ganze, rationale Funktionen von* $j(z)$.

Denn sie sind an jedem endlichen Punkt der obern Halbebene regulär, werden nur für $q = 0$, $z = \infty$ unendlich. Wären sie eine gebrochene Funktion von $j(z)$, so müßten sie aber an wenigstens einem endlichen Punkt unendlich werden.

36. Satz: *Das Produkt* $\tau_1 \cdot \tau_2 \cdot \ldots \tau_{\psi(n)}$ *ist eine ganze, rationale Funktion vom* $\psi(n)^{ten}$ *Grade in* $j(z)$, *alle übrigen elementarsymmetrischen Funktionen sind von niederem Grade in* $j(z)$.

Denn nach dem vorigen ist die niederste Potenz von q in der Reihenentwicklung von $\tau_1 \cdot \tau_2 \cdot \ldots \tau_{\psi(n)}$ nach Potenzen von q:

$$q^{-\sum_{\nu=1}^{\psi(n)} \frac{a_\nu}{d_\nu}}.$$

Ist t der größte, gemeinsame Teiler von a_ν und d_ν, so tritt d_ν in der Summe des Exponenten $\varphi(t)\,\frac{d_\nu}{t}$ mal auf (siehe den Beweis von Satz 24 S. 37). Also ist:

$$\sum_{\nu=1}^{\psi(n)} \frac{a_\nu}{d_\nu} = \sum_{(a)} \frac{a}{d}\,\frac{d}{t}\,\varphi(t) = \sum_{(a)} \frac{a}{t}\,\varphi(t) = \psi(n).$$

$q^{-\psi(n)}$ ist somit die niederste Potenz von q im Produkt der τ. $j(z)^{\psi(n)}$ beginnt nach Satz 14 mit $q^{-\psi(n)}$. $j(z)^{\psi(n)}$ tritt daher sicher in $\tau_1 \cdot \tau_2 \cdot \ldots \tau_{\psi(n)}$ auf, und keine höhere Potenz von $j(z)$ kann in ihm auftreten. Auf dieselbe Weise sieht man, daß in den anderen elementarsymmetrischen Funktionen keine niedern Potenzen von q auftreten können.

Bilden wir: $$\Phi_n(t, j(z)) \equiv \prod_{\nu=1}^{\psi(n)} (t - \tau_\nu),$$

so ist Φ_n eine ganze, rationale Funktion von t vom Grade $\psi(n)$, deren Koeffizienten ganze, rationale Funktionen von $j(z)$ von höchstens $\psi(n)^{tem}$ Grade sind.

Die Gleichung: $$\Phi_n(t, j(z)) = 0$$

heißt die Transformationsgleichung n^{ter} *Ordnung (oder Modulargleichung* n^{ter} *Stufe).* Sie besitzt die Wurzeln $\tau_1, \tau_2, \ldots \tau_{\psi(n)}$.

37. Satz: *Die Transformationsgleichung* $\Phi_n(t, j(z)) = 0$ *ist im Funktionskörper von* $j(z)$ *irreduzibel.*

Wäre nämlich $$\Phi_n(t, j(z)) \equiv \Phi_n'(t, j(z))\,\Phi_n''(t, j(z)),$$

so müßte Φ_n'' eine Wurzel τ_μ besitzen, die nicht Wurzel von Φ_n' wäre,

da nach Satz 29 alle τ voneinander verschieden sind. Nun ändern sich aber die Koeffizienten von Φ_n' bei Vornahme einer Substitution S nicht:

$$\Phi_n'(t, j(Sz)) \equiv \Phi_n'(t, j(z)).$$

Wählen wir nach Satz 30 S so, daß $S\tau_\nu = \tau_\mu$, wo τ_ν irgendeine Wurzel von Φ_n' ist, so wird:

$$\Phi_n'(t, j(z)) = S\Phi_n'(t, j(z)) = S(t - \tau_\nu) \cdots = (t - S\tau_\nu) \cdots = (t - \tau_\mu) \cdots,$$

d. h. τ_μ ist auch Wurzel von Φ_n' gegen Annahme.

38. Satz: $\Phi_n(t, j(z))$ *ist symmetrisch in* t *und* $j(z)$:

$$\Phi_n(t, j(z)) \equiv \Phi_n(j(z), t).$$

Denn zu $T = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}$ gehört die Wurzel $\tau = j\left(\frac{z}{n}\right)$. Also ist identisch:

$$\Phi_n\left(j\left(\frac{z}{n}\right), j(z)\right) \equiv 0.$$

Setzt man nz an Stelle von z, so wird:

$$\Phi_n(j(z), j(nz)) \equiv 0.$$

Anderseits ist $j(nz)$ eine Wurzel τ, die zu $T = \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}$ gehört. Somit ist auch: $$\Phi_n(j(nz), j(z)) \equiv 0.$$

$\Phi_n(j(z), t)$ und $\Phi_n(t, j(z))$ haben die Wurzel $j(nz)$ gemein, und da $\Phi_n(t, j(z))$ irreduzibel im Funktionskörper von $j(z)$ ist, so muß:

$$\Phi_n(j(z), t) \equiv f(t)\, \Phi_n(t, j(z)),$$

wo $f(t)$ rationale Koeffizienten in $j(z)$ hat. Nach Satz 36 ist der Grad von $\Phi_n(j(z), t)$ höchstens $\psi(n)$, also muß der Grad für beide derselbe sein und $f(t)$ ist eine Konstante C. Durch Vertauschung von t und $j(z)$ wird:

$$\Phi_n(j(z), t) \equiv C\Phi_n(t, j(z)),$$
$$\Phi_n(t, j(z)) \equiv C\Phi_n(j(z), t),$$
$$C^2 = 1, \quad C = \pm 1.$$

Wäre $C = -1$, so hätte $\Phi_n(t, j(z))$ die Wurzel $t = j(z)$, Φ_n wäre durch $t - j(z)$ teilbar, was gegen die Irreduzibilität wäre. Somit ist $C = 1$ und der Satz bewiesen.

Der Einfachheit halber wollen wir von nun an $j(z)$ mit τ abkürzen:

$$\Phi_n(t, \tau) \equiv \Phi_n(\tau, t),$$

und Φ_n zunächst für $n = p$ berechnen, wo p eine Primzahl ist. Φ_p hat die Wurzeln

$$t = j(pz), \; j\left(\frac{z}{p}\right), \; j\left(\frac{z+1}{p}\right), \cdots j\left(\frac{z+p-1}{p}\right).$$

Nach Satz 14 sind die c in $j(z) = \frac{1}{q} + \sum_{h=0}^{\infty} c_h q^h$

ganze, rationale Zahlen. Das q von $j(pz)$ ist q^p; also wird:

$$j(pz) = \frac{1}{q^p} + \sum_{h=0}^{\infty} c_h q^{ph},$$

und es ist:

$$j(z)^p - j(pz) = \frac{1}{q^p} + \sum_{h=0}^{\infty} c_h^p q^{ph} + p \sum_{h=0}^{\infty} \bar{c}_h q^{h-p+1} - \frac{1}{q^p} - \sum_{h=0}^{\infty} c_h q^{ph}$$

$$= \sum_{h=0}^{\infty} (c_h^p - c_h) q^{ph} + p q^{1-p} \sum_{h=0}^{\infty} \bar{c}_h q^h,$$

wo auch die $\bar{c}$ ganze, rationale Zahlen sind. Nach dem Satze von *Fermat* ist

$$c_h^p - c_h \equiv 0 \pmod{p}.$$

Somit wird: $$j(z)^p - j(pz) = p q^{1-p} \sum_{h=0}^{\infty} \bar{\bar{c}}_h q^h,$$

wo auch die $\bar{\bar{c}}$ ganze, rationale Zahlen sind. Ebenso wird:

$$j(pz)^p - j(z) = \frac{1}{q^{p^2}} + \cdots,$$

wo nur die niederste Potenz von q angegeben ist. Somit wird:

$$[j(pz)^p - j(z)][j(z)^p - j(pz)] = p\, q^{1-p-p^2} \sum_{h=0}^{\infty} c_h^* q^h,$$

wo die c^* ganze rationale Zahlen sind.

Nach Definition ist $\Phi_p(t, \tau)$ vom Grade $p+1$ und symmetrisch in t und τ. Man darf deshalb den Ansatz machen:

$$\Phi_p(t, \tau) \equiv t^{p+1} + \tau^{p+1} + \cdots = -(t^p - \tau)(\tau^p - t) + \sum_{k=0}^{p} a_{k,k}\, t^k \tau^k$$

$$+ \sum_{k=1}^{p} \sum_{h=0}^{k-1} a_{k,h} (t^h \cdot \tau^k + t^k \cdot \tau^h).$$

Für $t = j(pz)$, $\tau = j(z)$ wird diese Gleichung identisch null. Wir setzen deshalb in ihr die obige Reihenentwicklung ein:

$$- p q^{1-p-p^2} \sum_{h=0}^{\infty} c_h^* q^h + \sum_{k=0}^{p} a_{k,k} \left(\frac{1}{q^{pk}} + \cdots\right)\left(\frac{1}{q^k} + \cdots\right)$$

$$+ \sum_{k=1}^{p} \sum_{h=0}^{k-1} a_{k,h} \left(\frac{1}{q^{ph+k}} + \cdots + \frac{1}{q^{pk+h}} + \cdots\right) \equiv 0,$$

und wissen, daß jeder Koeffizient einer Potenz von q null sein muß. Die niederste Potenz von q tritt nur einmal mit dem Koeffizienten $a_{p,p}$ auf; somit ist:

$$a_{p,p} = 0.$$

Der Koeffizient von q^{1-p-p^2} ist $(-pc_0^* + a_{p,p-1})$, daher:

$$a_{p,p-1} = pc_0^*,$$

und $a_{p,p-1}$ ist eine ganze, rationale, durch p teilbare Zahl. In jedem weiteren Koeffizient tritt eine weitere Unbekannte a mit 1 multipliziert hinzu. Diese läßt sich als ganze, homogene, lineare Form der schon berechneten a und pc^* darstellen, ist also selbst eine ganze, rationale, durch p teilbare Zahl.

39. **Satz:** *$\Phi_p(t, \tau)$ läßt sich in der Form darstellen:*

$$\Phi_p(t, \tau) \equiv -(t^p - \tau)(\tau^p - t) + p\sum A_{k,h} t^k \tau^h,\ 0 \leqq h \leqq k \leqq p,$$

wo in der Summe die Koeffizienten A ganze, rationale Zahlen sind und $A_{p,p} = 0$.

Bilden wir:
$$\Phi^* \equiv \prod_{h=1}^{p+1} \Phi_p(t, \tau_h),$$

so hat Φ^* ganze rationale Koeffizienten. Eine seiner Wurzeln ist $j\left(\frac{z}{p^2}\right)$; denn $\Phi_p\left(t, j\left(\frac{z}{p}\right)\right)$ hat die Wurzel $j\left(\frac{z}{p^2}\right)$. Wegen der Irreduzibilität von Φ_{p^2}, dessen eine Wurzel ebenfalls $j\left(\frac{z}{p^2}\right)$ ist, muß Φ^* durch Φ_{p^2} teilbar sein. Anderseits besitzt jedes $\Phi_p(t, \tau_h)$ wegen der Symmetrieeigenschaft die Wurzel $t = j(z)$, Φ^* ist somit auch durch $(t - j(z))^{p+1}$ teilbar, während Φ_{p^2} sicherlich diese Wurzel nicht besitzt; daher muß:

$$\Phi^*(t, \tau) \equiv f(t)\, \Phi_{p^2}(t, \tau)(t - \tau)^{p+1}$$

sein, wo $f(t)$ eine ganze rationale Funktion ist. Da der Grad der linken und rechten Seite gleich groß, nämlich gleich $(p+1)^2 = p+1+p(p+1)$ ist, wird $f(t)$ eine Konstante, die sich beim Vergleich der Koeffizienten der obersten Potenzen von t als eins ergibt. Somit gilt:

40. **Satz:** *Die Funktion*

$$\Phi_{p^2}(t, \tau) \equiv \frac{\Phi^*(t, \tau)}{(t - \tau)^{p+1}}$$

ist eine ganze rationale Funktion von t und τ, deren Koeffizienten ganze rationale Zahlen sind, und in der der Koeffizient der obersten Potenz von t oder τ eins ist.

Wir wollen jetzt durch den Schluß von $r-1$ auf r beweisen, daß auch $\Phi_{p^r}(t, \tau)$, $r > 2$, ganze rationale Zahlkoeffizienten besitzt. Die Gleichung:

$$\Phi_{p^{r-1}}(t, \tau) = 0$$

hat die $\psi(p^{r-1}) = p^{r-2}(p+1)$ Wurzeln $\tau_1, \tau_2, \ldots \tau_{\psi(p^{r-1})}$, und wir bilden:

$$\Phi^*(t, \tau) \equiv \prod_{h=1}^{\psi(p^{r-1})} \Phi_p(t, \tau_h).$$

Wir nehmen die Behauptung als für $\Phi_{p^{r-1}}$ schon bewiesen an. Dann hat Φ^* lauter ganze rationale Koeffizienten, da sie symmetrische Funktionen der τ_h mit ganzen rationalen Koeffizienten sind. Eine der Wurzeln ist $\tau = j\left(\frac{z}{p^{r-1}}\right)$; es besitzt deshalb:

$$\Phi_p(t, \tau) = 0, \quad \tau = j\left(\frac{z}{p^{r-1}}\right)$$

die Wurzel $t = j\left(\frac{z}{p^r}\right)$, wie man sofort sieht, wenn man in den Wurzeln von Φ_p an Stelle von z: $\frac{z}{p^{r-1}}$ setzt. Somit hat Φ^* die Wurzel $t = j\left(\frac{z}{p^r}\right)$ mit Φ_{p^r} gemein, ist also wegen der Irreduzibilität von Φ_{p^r} durch letztere Funktion teilbar: $\Phi^*(t, \tau) \equiv \Phi_{p^r}(t, \tau)\,\overline{\Phi}(t, \tau)$.

Der Grad von $\overline{\Phi}$ ist:

$$(p+1)\psi(p^{r-1}) - \psi(p^r) = p^{r-1} + p^{r-2} = p\psi(p^{r-2}).$$

Setzt man in $\Phi_p(j(pz), j(z)) \equiv 0$

statt z: $\frac{z + cp^{r-2}}{p^{r-1}}$, $c = 0, 1, 2, \ldots p-1$, so wird wegen $j\left(\frac{z+cp^{r-2}}{p^{r-2}}\right) = j\left(\frac{z}{p^{r-2}} + c\right) = j\left(\frac{z}{p^{r-2}}\right)$:

$$\Phi_p\left(j\left(\frac{z}{p^{r-2}}\right), \quad j\left(\frac{z+cp^{r-2}}{p^{r-1}}\right)\right) \equiv 0, \; c = 0, 1, 2, \ldots p-1.$$

Jeder der p Faktoren von Φ^*: $\Phi_p\left(t, j\left(\frac{z+cp^{r-2}}{p^{r-1}}\right)\right)$ hat daher mit $\Phi_{p^{r-2}}(t, \tau)$ die Wurzel $t = j\left(\frac{z}{p^{r-2}}\right)$ gemein, Φ^* ist durch $\left(t - j\left(\frac{z}{p^{r-2}}\right)\right)^p$ teilbar und daher wegen der Irreduzibilität von $\Phi_{p^{r-2}}$ durch $\Phi^p_{p^{r-2}}$. Da Φ_{p^r} und $\Phi_{p^{r-2}}$ keine Wurzeln gemein haben, so ist auch $\overline{\Phi}$ durch $\Phi^p_{p^{r-2}}$ teilbar, und da beide denselben Grad haben, sind sie bis auf einen konstanten Faktor gleich. Dieser Faktor ist eins, da die obersten Potenzen den Koeffizienten eins haben. Daraus folgt:

$$\overline{\Phi}(t, \tau) \equiv \Phi^p_{p^{r-2}}(t, \tau); \quad \Phi^*(t, \tau) \equiv \Phi_{p^r}(t, \tau)\,\Phi^p_{p^{r-2}}(t, \tau).$$

Da Φ^* und $\Phi_{p^{r-2}}$ nach Voraussetzung ganze rationale Koeffizienten haben, folgt dasselbe für Φ_{p^r}.

41. Satz: *Die Funktion:*

$$\Phi_{p^r}(t, \tau) \equiv \frac{\prod_{h=1}^{\psi(p^{r-1})} \Phi_p(t, \tau_h)}{\Phi^p_{p^{r-2}}(t, \tau)} \qquad (r > 2)$$

ist eine ganze rationale Funktion von t und τ, deren Koeffizienten ganze rationale Zahlen sind, und deren oberste Potenzen in t oder τ den Koeffizienten eins besitzen.

Ist schließlich n eine beliebige Zahl, so zerlegen wir sie in zwei teilerfremde Faktoren n_1 und n_2. Nach Satz 24 und seinem Beweise ist:

$$\psi(n_1)\psi(n_2) = \psi(n).$$

Wir dürfen voraussetzen, daß für n_1 und n_2 schon bewiesen sei, daß Φ_{n_1} und Φ_{n_2} lauter ganze rationale Koeffizienten haben. Die Wurzeln von Φ_{n_1} seien $\tau_1, \tau_2, \ldots \tau_{\psi(n_1)}$, dann hat auch:

$$\Phi^* \equiv \prod_{h=1}^{\psi(n_1)} \Phi_{n_2}(t, \tau_h)$$

ganze rationale Zahlkoeffizienten. Unter den Wurzeln tritt auch $j\left(\frac{z}{n_1}\right)$ auf. Setzt man in der Identität:

$$\Phi_{n_2}\left(j\left(\frac{z}{n_2}\right),\ j(z)\right) \equiv 0$$

statt z: $\frac{z}{n_1}$, so folgt: $\Phi_{n_2}\left(j\left(\frac{z}{n_1 n_2}\right),\ j\left(\frac{z}{n_1}\right)\right) \equiv 0$.

Also hat Φ^* die Wurzel $t = j\left(\frac{z}{n_1 n_2}\right) = j\left(\frac{z}{n}\right)$, die auch Wurzel von Φ_n ist. Wegen der Irreduzibilität von Φ_n ist Φ^* durch Φ_n teilbar, und da beide denselben Grad haben, ist ihr Quotient eine Konstante, die wieder eins sein muß. Daher:

$$\Phi_n(t, \tau) \equiv \Phi^*(t, \tau) \equiv \prod_{h=1}^{\psi(n_1)} \Phi_{n_2}(t, \tau_h).$$

42. Satz: *Die Transformationsgleichung:*

$$\Phi_n(t, \tau) = 0$$

hat ganze rationale Zahlkoeffizienten, und die Koeffizienten der obersten Potenzen von t oder τ sind eins.

Jetzt gelingt es auch, den Zusammenhang der Funktionen

$$\eta_\nu = \frac{a_\nu^{12}\, G(T_\nu z)}{G(z)}$$

mit den τ_ν festzulegen. Die Funktion:

$$\Psi \equiv \Phi_n(t, \tau) \sum_{\nu=1}^{\psi(n)} \frac{\eta_\nu}{t - \tau_\nu} \tag{15}$$

ist eine ganze rationale Funktion in t, deren Koeffizienten ganze rationale Funktionen von $\tau = j(z)$ sind. Bei einer Substitution S von $\mathfrak{G}$ verändert sich Φ_n nicht, und nach Satz 33 wird:

$$S\frac{\eta_\nu}{t - \tau_\nu} = \frac{\eta_\mu}{t - \tau_\mu}.$$

Die einzelnen Glieder der Summe vertauschen sich nur, Ψ selbst bleibt ungeändert. Nach Satz 12 ist somit Ψ eine Funktion des Funktionskörpers von $j(z)$, d. h. nach Satz 32 eine ganze rationale Funktion von $j(z)$:

$$\Phi_n(t, \tau) \sum_{\nu=1}^{\psi(n)} \frac{\eta_\nu}{t - \tau_\nu} \equiv \Psi_n(t, \tau).$$

In der Grenze $t = \tau_\nu$ wird: $\eta_\nu = \dfrac{\Psi_n(\tau_\nu, \tau)}{\Phi_n'(\tau_\nu, \tau)}$.

Der Nenner ist wegen Satz 29 nicht identisch null.

43. Satz: *Die Funktion η_ν gehört dem Funktionskörper von $\tau_\nu = j(T_\nu z)$ und $\tau = j(z)$ an.*

Um über die Natur der Koeffizienten der Funktion (15) orientiert zu sein, setzen wir in Ψ_n für τ_ν und η_ν ihre Reihenentwicklungen ein. Nach den Formeln für $j(z)$ und $G(\omega_1, \omega_2)$ am Schlusse von Kapitel 1 S. 32 ist:

$$\eta_\nu = \frac{a_\nu^{12}\, G(T_\nu z)}{G(z)} = a_\nu^{12}\, e^{\frac{2\pi i b_\nu}{d_\nu}} q^{\frac{a_\nu}{d_\nu}-1} \prod_{h=1}^{\infty} \left(\frac{1 - e^{\frac{2\pi i b_\nu h}{d_\nu}} q^{\frac{a_\nu h}{d_\nu}}}{1 - q^h}\right)^{24},$$

$$\tau_\nu = j(T_\nu z) = \frac{\left[1 + 240 \sum_{h=1}^{\infty} h^3 \dfrac{e^{\frac{2\pi i b_\nu h}{d_\nu}} q^{\frac{a_\nu h}{d_\nu}}}{1 - e^{\frac{2\pi i b_\nu h}{d_\nu}} q^{\frac{a_\nu h}{d_\nu}}}\right]^3}{e^{\frac{2\pi i b_\nu}{d_\nu}} q^{\frac{a_\nu}{d_\nu}} \prod_{h=1}^{\infty} \left(1 - e^{\frac{2\pi i b_\nu h}{d_\nu}} q^{\frac{a_\nu h}{d_\nu}}\right)^{24}}.$$

Die Koeffizienten von q sind rationale Zahlen bis auf die Einheitswurzeln $e^{2\pi i \frac{b_\nu}{d_\nu}}$. Da aber über alle zu d_ν teilerfremden Zahlen b_ν zwischen 0 und d_ν summiert wird, so verschwinden diese Irrationalitäten wieder und die Koeffizienten sind rationale Zahlen. Durch Koeffizientenvergleichung erkennt man, daß Ψ_n selbst rationale Zahlkoeffizienten haben muß. Da auch Φ_n diese Eigenschaft hat, so gilt der

44. Satz: $\eta_\nu = \dfrac{a_\nu^{12}\, G(T_\nu z)}{G(z)}$ *ist eine rationale Funktion von $\tau_\nu = j(T_\nu z)$ und $\tau = j(z)$ mit rationalen Zahlkoeffizienten.*

Als einfachsten Fall einer Transformationsgleichung wollen wir noch Φ_2 aufschreiben:

$$\Phi_2(t, \tau) \equiv -(t^2 - \tau)(\tau^2 - t) + 2a_{21}(t^2\tau + t\tau^2) + 2a_{20}(t^2 + \tau^2) + 2a_{11}t\tau + 2a_{10}(t + \tau) + 2a_{00}.$$

Die in diesem Paragraphen angegebene Methode ergibt folgende Zahlwerte:

$$\begin{aligned} a_{21} &= 744 = 2^3 \cdot 3 \cdot 31 \\ a_{20} &= -81000 = -2^3 \cdot 3^4 \cdot 5^3 \\ a_{11} &= 20386688 = 2^7 \cdot 7 \cdot 61 \cdot 373 \\ a_{10} &= 4374000000 = 2^7 \cdot 3^7 \cdot 5^6 \\ a_{00} &= -78732000000000 = -2^{11} \cdot 3^9 \cdot 5^9. \end{aligned}$$

Man erkennt daraus, welch große Zahlen in den Gleichungen auftreten. Bei $p = 3$ werden dieselben noch ganz bedeutend größer.

III. Die singulären Werte der Modulfunktionen.

1. Der quadratische Körper.

Es sei m eine negative, quadratfreie ganze, rationale Zahl.

4. **Definition:** *Alle Zahlen, die aus 1 und $\sqrt{m}$ durch Addition, Subtraktion, Multiplikation und Division erhalten werden, bilden den quadratischen Körper $k(\sqrt{m})$.*

Da $(\sqrt{m})^2$ rational ist, haben alle Zahlen von $k(\sqrt{m})$ die Form:

$$\Omega = \frac{a\sqrt{m}+b}{c\sqrt{m}+d}, \quad c\sqrt{m}+d \neq 0,$$

wo a, b, c, d ganz und rational sind. Erweitert man den Bruch mit $-c\sqrt{m}+d$, so erhält er die Gestalt:

$$\Omega = \frac{x+y\sqrt{m}}{z}, \quad z \neq 0,$$

wo x, y, z ganz und rational sind.

45. **Satz:** *Jede Zahl von $k(\sqrt{m})$ läßt sich in der Form darstellen:*

$$\Omega = \frac{x+y\sqrt{m}}{z}, \quad z \neq 0,$$

wo x, y, z ganz und rational sind, und umgekehrt ist jede Zahl dieser Form in $k(\sqrt{m})$.

Die Zahl $$\Omega' = \frac{x-y\sqrt{m}}{z}$$

heißt die *konjugierte* von Ω, das Produkt

$$n(\Omega) \equiv \Omega\Omega' = \frac{x^2-y^2m}{z^2}$$

die *Norm* von Ω. Konjugierte Zahlen werden wir stets durch einen Strich bezeichnen. Jede Zahl von $k(\sqrt{m})$ genügt einer quadratischen Gleichung, deren Koeffizienten rationale Zahlen sind:

$$\Omega^2 - \frac{2x}{z}\Omega + \frac{x^2-y^2m}{z^2} = 0.$$

Wir setzen x, y, z ohne gemeinsamen Teiler voraus.

5. **Definition:** *Eine Zahl Ω heißt eine ganze Zahl von $k(\sqrt{m})$, falls $\frac{2x}{z}$ und $\frac{x^2-y^2m}{z^2}$ ganze rationale Zahlen sind.*

Ist Ω ganz und haben x und z den größten, gemeinsamen Teiler t, so muß my^2 durch t^2, also y durch t teilbar sein, da m ohne quadratischen Teiler ist. Somit muß $t = 1$ sein. z ist ein Teiler von 2. Ist $z = 2$, so wird:

$$x^2 - y^2 m \equiv 0 \pmod 4.$$

x, y sind beide ungerade und:

$$x^2 \equiv y^2 \equiv 1 \pmod 4, \quad 1 - m \equiv 0 \pmod 4, \quad m \equiv 1 \pmod 4.$$

Umgekehrt ist für $m \equiv 1 \pmod 4$ $\Omega = \frac{x + y\sqrt{m}}{2}$ immer ganz, falls x und y ungerade sind. Man schreibt in diesem Falle:

$$\Omega = \frac{x+y}{2} + y\,\frac{-1+\sqrt{m}}{2}.$$

$\frac{x+y}{2}$ und y können dann irgendwelche ganze rationale Zahlen sein. Ist $m \not\equiv 1 \pmod 4$, so ist z immer 1. Wir setzen:

$$m \not\equiv 1 \pmod 4\text{: } \omega = \sqrt{m}; \quad m \equiv 1 \pmod 4\text{: } \omega = \frac{-1+\sqrt{m}}{2}.$$

46. Satz: *Jede Zahl der Form:*

$$x + y\omega, \quad \omega = \sqrt{m}, \quad m \not\equiv 1 \pmod 4, \quad \omega = \frac{-1+\sqrt{m}}{2}, \quad m \equiv 1 \pmod 4,$$

wo x, y ganze rationale Zahlen sind, ist eine ganze Zahl von $k(\sqrt{m})$, und umgekehrt ist jede ganze Zahl von $k(\sqrt{m})$ in dieser Form darstellbar.

1, ω heißt eine *Basis der ganzen Zahlen von $k(\sqrt{m})$*. Dieselben werden somit durch Addition und Subtraktion aus 1 und ω erhalten.

6. Definition: *Ein Bereich von Zahlen, die aus gegebenen Zahlen nach endlich vielen Schritten durch Addition und Subtraktion erhalten werden, heißt ein Modul.*

Sind n Zahlen $\alpha_1, \alpha_2, \ldots \alpha_n$ gegeben, so wird der aus ihnen gebildete Modul $\mathfrak{a}$ mit:

$$\mathfrak{a} = [\alpha_1, \alpha_2, \ldots \alpha_n]$$

bezeichnet. Er heißt n-gliedrig. Der zweigliedrige Modul:

$$\mathfrak{o} = [1, \omega]$$

enthält alle ganzen Zahlen von k. Alle Zahlen α von $\mathfrak{a}$ sind in der Form enthalten:

$$\alpha = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n,$$

wo $x_1, x_2, \ldots x_n$ alle ganzen rationalen Zahlen durchlaufen.

7. Definition: *Zwei Moduln heißen gleich, wenn jede Zahl des einen im andern enthalten ist und umgekehrt.*

47. Satz: *Jeder n-gliedrige Modul von $k(\sqrt{m})$ ist einem zweigliedrigen gleich (n endlich).*

Wir brauchen bloß zu beweisen, daß sich jeder dreigliedrige Modul auf einen zweigliedrigen zurückführen läßt. Ist $\mathfrak{a} = [\alpha_1, \alpha_2, \alpha_3]$, so sieht

man sofort, daß es stets drei ganze rationale Zahlen n_1, n_2, n_3, die nicht alle drei $= 0$ sind, ohne gemeinsamen Teiler gibt, so daß:

$$n_1\alpha_1 + n_2\alpha_2 + n_3\alpha_3 = 0.$$

Ist ein n, z. B. $n_3 = 1$, so ist wegen $\alpha_3 = -\alpha_1 n_1 - \alpha_2 n_2$:

$$[\alpha_1, \alpha_2, \alpha_3] = [\alpha_1, \alpha_2].$$

Es sei daher $n_3 > 1$, $\alpha_3 = -\frac{n_1\alpha_1 + n_2\alpha_2}{n_3}$. Dann läßt sich jede Zahl α des Moduls in der Form darstellen:

$$\alpha = x_1\alpha_1 + x_2\alpha_2 + x_3\alpha_3 = \frac{(n_3x_1 - n_1x_3)\alpha_1 + (n_3x_2 - n_2x_3)\alpha_2}{n_3}.$$

Unter diesen gibt es, falls r der größte gemeinsame Teiler von n_2 und n_3 ist, eine Zahl:

$$\beta_2 = \frac{(n_3\bar{x}_1 - n_1\bar{x}_3)\alpha_1 + r\alpha_2}{n_3},$$

und jede Zahl des Moduls kann so dargestellt werden:

$$\alpha = \frac{X\alpha_1}{n_3} + t_2\beta_2,$$

wo t_2 alle ganzen Zahlen und X nur gewisse ganze Zahlen durchlaufen darf. Ist für $t_2 = 0$ $\overline{X}$ der absolut kleinste mögliche Wert $\neq 0$ in:

$$\beta_1 = \frac{\overline{X}\alpha_1}{n_3},$$

so hat jede Zahl des Moduls die Gestalt:

$$\alpha = t_1\beta_1 + t_2\beta_2,$$

wo t_1 und t_2 ganze Zahlen sind. Umgekehrt ist jede solche Zahl eine Zahl des Moduls, da es β_1 und β_2 sind.

48. Satz: *Alle Moduln, die nur ganze Zahlen enthalten, sind zweigliedrig oder eingliedrig.*

Denn alle seine Zahlen haben die Form: $x + y\omega$. Ist r_2 der größte gemeinsame Teiler aller y, so gibt es im Modul eine Zahl $\omega_2 = s_2 + r_2\omega$, und jede seiner Zahlen hat die Gestalt: $\overline{X} + t_2\omega_2$. Ist r_1 der größte gemeinsame Teiler aller $\overline{X}$, so gibt es eine Zahl $\omega_1 = r_1 + s_1\omega$ und jede Zahl hat die Gestalt: $t_1\omega_1 + t_2\omega_2$, d. h.

$$[\alpha_1, \alpha_2, \ldots] = [\omega_1, \omega_2].$$

8. Definition: *Unter dem Produkt zweier Moduln versteht man den Modul, der aus allen Produkten einer Zahl des einen Moduls und einer Zahl des andern Moduls entspringt.*

Für diese Multiplikation gilt das assoziative und kommutative Gesetz.

9. Definition: *Ein Modul, der Produkt aus* $\mathfrak{o} = [1, \omega]$ *und einem Modul mit lauter ganzen Zahlen ist, heißt ein Ideal.*

Da das Ideal nur ganze Zahlen besitzt, ist es ein zweigliedriger Modul, der so bezeichnet wird:

$$\mathfrak{w} = (\omega_1, \omega_2).$$

ω_1, ω_2 heißt eine *Basis des Ideals*. Alle Zahlen von $\mathfrak{w}$ lassen sich in der Form darstellen:

$$\nu = x_1\omega_1 + x_2\omega_2, \quad x_1, x_2 = \text{alle ganzen rationalen Zahlen.}$$

Der Bereich der ganzen Zahlen eines Ideals ist noch durch eine andere Eigenschaft charakterisiert.

49. Satz: *Ist ν eine Zahl des Ideals $\mathfrak{w}$ und μ eine beliebige ganze Zahl, so ist auch $\mu \cdot \nu$ eine Zahl des Ideals.*

Denn nach Definition ist:

$$\mathfrak{w} = [1, \omega][\nu_1, \nu_2, \ldots, \nu_h, \ldots] = [\ldots, (x + y\omega)\nu_h, \ldots].$$

Sind die Zahlen eines Ideals alle Vielfachen einer ganzen Zahl ν, so heißt das Ideal *Hauptideal*. ν und $\nu\omega$ sind seine Basis und man schreibt:

$$\mathfrak{w} = (\nu, \nu\omega) = (\nu).$$

$\mathfrak{w}' = (\omega_1', \omega_2')$ heißt das zu $\mathfrak{w}$ *konjugierte Ideal*, das Produkt $\mathfrak{w}\mathfrak{w}'$ die *Norm* $n(\mathfrak{w})$ *von* $\mathfrak{w}$. Letztere ist Hauptideal, alle ihre Zahlen sind Vielfache einer ganzen, rationalen positiven Zahl n; man identifiziert daher die Norm gewöhnlich mit n und setzt:

$$n = n(\mathfrak{w}), \quad (n) = \mathfrak{w}\mathfrak{w}'.$$

Wir werden in Zukunft die Basis ω_1, ω_2 von $\mathfrak{w}$ so numerieren, daß das Verhältnis $\omega_2 : \omega_1$ einen *positiven* Imaginärteil besitzt.

50. Satz: *Ist ω_1, ω_2 eine Basis von $\mathfrak{w}$, für die $\omega_2 : \omega_1$ einen positiven Imaginärteil besitzt, so ist jede andere Basis $\overline{\omega}_1, \overline{\omega}_2$ von $\mathfrak{w}$ und dieser Eigenschaft in der Form darstellbar:*

$$\overline{\omega}_2 = \alpha\omega_2 + \beta\omega_1,$$
$$\overline{\omega}_1 = \gamma\omega_2 + \delta\omega_1,$$

wo $S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ eine Substitution der Modulgruppe ist.

Denn da dann auch: $\omega_2 = \delta\overline{\omega}_2 - \beta\overline{\omega}_1,$

$$\omega_1 = -\gamma\overline{\omega}_2 + \alpha\overline{\omega}_1,$$

so ist jede Zahl von $(\overline{\omega}_1, \overline{\omega}_2)$ in (ω_1, ω_2) enthalten und umgekehrt. Außerdem ist wegen $\overline{\omega}_2 : \overline{\omega}_1 = S(\omega_2 : \omega_1)$ nach § 2, Kap. 1, S. 6 $\overline{\omega}_2 : \overline{\omega}_1$ wieder ein Punkt der obern Halbebene.

Aus Satz 50 folgt, daß die eine Basiszahl, z. B. ω_1, immer als ganze rationale Zahl gewählt werden kann:

$$\mathfrak{w} = (w, s + t\omega).$$

Nach Satz 49 ist auch ωw in $\mathfrak{w}$:

$$\omega w = xw + y(s + t\omega)$$

oder $$xw + ys = 0, \quad w = yt,$$

d. h. $$w \equiv s \equiv 0 \pmod{t}, \quad \mathfrak{w} = (t)(w_1, s_1 + \omega).$$

Jede ganze, rationale Zahl von $\mathfrak{w}$ ist Vielfaches von $w = tw_1$, somit:

$$(s_1 + \omega)(s_1 + \omega') \equiv 0 \pmod{w_1}.$$

Wie man sofort sieht, ist s_1 nur (mod. w_1) bestimmt. Man nennt jede solche spezielle Basis eine *kanonische Basis.*

Ist $\mathfrak{w} = (\omega_1, \omega_2)$, so kann man immer ein S bestimmen, so daß:

$$\omega_2 = \alpha(s + t\omega) + \beta w,$$
$$\omega_1 = \gamma(s + t\omega) + \delta w.$$

Bezeichnet man mit einem Strich die konjugierten Zahlen, so wird:

$$\frac{1}{\omega' - \omega}\begin{vmatrix} \omega_1 & \omega_2 \\ \omega_1' & \omega_2' \end{vmatrix} = \frac{1}{\omega' - \omega}\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix}\begin{vmatrix} s + t\omega' & w \\ s + t\omega & w \end{vmatrix} = tw.$$

Nun ist, wie man aus der Definition der Norm erkennt:

$$n(\mathfrak{w}) = tw.$$

Also folgt:

(16) $$\frac{1}{\omega' - \omega}\begin{vmatrix} \omega_1 & \omega_2 \\ \omega_1' & \omega_2' \end{vmatrix} = n(\mathfrak{w}).$$

Ist ν eine beliebige ganze Zahl, so liegt $\nu\omega_1$, $\nu\omega_2$ wieder in $\mathfrak{w}$:

$$\nu\omega_1 = x_1\omega_1 + x_2\omega_2, \quad \nu\omega_2 = x_3\omega_1 + x_4\omega_2;$$

somit ist:

(17) $$\nu\nu'\begin{vmatrix} \omega_1 & \omega_2 \\ \omega_1' & \omega_2' \end{vmatrix} = \begin{vmatrix} x_1 & x_2 \\ x_3 & x_4 \end{vmatrix}\begin{vmatrix} \omega_1 & \omega_2 \\ \omega_1' & \omega_2' \end{vmatrix} \quad \text{oder} \quad n(\nu) = \begin{vmatrix} x_1 & x_2 \\ x_3 & x_4 \end{vmatrix}.$$

10. Definition: *Sind* $\mathfrak{w}_1$ *und* $\mathfrak{w}_2$ *zwei Ideale und gibt es ein drittes Ideal* $\mathfrak{w}_3$, *so daß:*

$$\mathfrak{w}_1 = \mathfrak{w}_2\mathfrak{w}_3,$$

so heißt $\mathfrak{w}_1$ *teilbar durch* $\mathfrak{w}_2$.

Man kann zeigen, daß der Quotient $\mathfrak{w}_1 : \mathfrak{w}_2$ eindeutig bestimmt ist.

11. Definition: *Ein Ideal, das nur durch sich selbst und durch* $\mathfrak{o} = (1, \omega)$ *teilbar ist, heißt ein Primideal.*

Es sei $\mathfrak{p}$ ein Primideal, und wir wollen seine kanonische Basis bestimmen:

$$\mathfrak{p} = (t)(w_1, s_1 + \omega).$$

Sicherlich muß wegen der Definition von $\mathfrak{p}$ $t = 1$ oder $= p$ sein, wo p eine rationale Primzahl ist. Im ersten Falle muß w_1 eine rationale Primzahl sein, da sonst $\mathfrak{p}$ durch:

$$(p_1, s_1 + \omega)$$

teilbar wäre, wo p_1 ein Primteiler von w_1 wäre. Die Primideale dieser Form heißen Primideale ersten Grades:

$$\mathfrak{p} = (p, s + \omega), \quad \text{wo} \quad (s + \omega)(s + \omega') \equiv 0 \pmod{p}.$$

Ist $t = p$, so muß $\mathfrak{p}$ Hauptideal sein:

$$\mathfrak{p} = (p) = (p, p\omega).$$

$\mathfrak{p}$ heißt von zweitem Grade. Nach (16) ist die Norm der Primideale 1. Grades p, des 2. Grades p^2.

51. **Satz:** *Jedes Primideal* $\mathfrak{p}$ *hat die kanonische Basisdarstellung:*

$$\mathfrak{p} = (p, s + \omega), \ (s + \omega)(s + \omega') \equiv 0 \pmod{p},$$

oder $$\mathfrak{p} = (p, p\omega),$$

wo p *eine rationale Primzahl ist. Im ersten Falle heißt es von erstem Grade, seine Norm ist* p, *im zweiten Falle von zweitem Grade, seine Norm ist* p^2.

Es fragt sich, wann eine Primzahl von erstem oder zweitem Grade ist? Ist sie von erstem Grade, so muß es ein s geben, so daß:

$$(s + \omega)(s + \omega') \equiv 0 \pmod{p} \quad \text{ist. Also:}$$

$$m \not\equiv 1 \pmod 4\text{: } s^2 - m \equiv 0 \pmod{p}.$$

$$m \equiv 1 \pmod 4\text{: } (2s - 1)^2 - m \equiv 0 \pmod{4p}.$$

m muß quadratischer Rest (mod. p) sein. Ist umgekehrt diese Bedingung erfüllt, so existiert ein s, und p ist von erstem Grade. Ist p quadratischer Nichtrest (mod. p), so ist p von zweitem Grade. Im Falle $p = 2$ muß für $m \equiv 1 \pmod 4$ m Rest (mod. 8) bzw. Nichtrest (mod. 8) sein. Ist p vom ersten Grade, so ist $\mathfrak{p}$ dann und nur dann von seinem konjugierten Ideal $\mathfrak{p}'$ verschieden, falls

$$\text{für} \quad m \not\equiv 1 \pmod 4\text{: } p \neq 2 \quad \text{und} \quad m \not\equiv 0 \pmod{p},$$

$$\text{für} \quad m \equiv 1 \pmod 4\text{: } \qquad\qquad m \not\equiv 0 \pmod{p}.$$

Mit Hilfe des *Legendre*schen Symbols kann man diese Resultate zusammenfassen: Es sei $d = (\omega' - \omega)^2$ die *Diskriminante des Körpers* $k(\sqrt{m})$, d. h. $d = 4m$, falls $m \not\equiv 1 \pmod 4$, $d = m$, falls $m \equiv 1 \pmod 4$ ist. Dann sei $\left(\frac{d}{p}\right) = +1, -1, 0$, je nachdem d quadratischer Rest (mod. p), quadratischer Nichtrest (mod. p), oder p in d enthalten ist. Für $p = 2$ muß m quadratischer Rest oder Nichtrest (mod. 8) sein.

52. **Satz:** *Eine rationale Primzahl* p *zerfällt in* $k(\sqrt{m})$ *in zwei verschiedene Primideale, ist selbst Primideal, oder das Quadrat eines Primideals, je nachdem* $\left(\frac{d}{p}\right)$ *gleich* $+1, -1$ *oder* 0 *ist.*

Man kann den Satz beweisen:

53. Satz: *Jedes Ideal kann, abgesehen von der Reihenfolge, nur auf eine Weise als Produkt von Primidealen dargestellt werden.*

Zwei Ideale $\mathfrak{w}_1$ und $\mathfrak{w}_2$ heißen *äquivalent*, wenn es zwei ganze Zahlen ν_1 und ν_2 gibt, so daß:

$$(\nu_1)\,\mathfrak{w}_1 = (\nu_2)\,\mathfrak{w}_2 .$$

Man schreibt $\mathfrak{w}_1 \sim \mathfrak{w}_2$. Aus der Definition folgt:

54. Satz: *Sind zwei Ideale einem dritten äquivalent, so sind sie auch untereinander äquivalent.*

Alle einem Ideale äquivalenten Ideale liegen daher in einer *Klasse* $\mathfrak{k}$. Die Anzahl der Klassen ist endlich, sie heißt die *Klassenzahl* h. Sind $\mathfrak{w}_1$ und $\mathfrak{w}_2$ zwei Ideale, die in den Klassen $\mathfrak{k}_1$ und $\mathfrak{k}_2$ liegen, so sagt man, das Produkt der Ideale $\mathfrak{w}_1\mathfrak{w}_2$ liegt im Produkt der Klassen $\mathfrak{k}_1\mathfrak{k}_2$. Die Klassen können daher ebenfalls durch Multiplikation zusammengesetzt werden: $\mathfrak{k}_1 \cdot \mathfrak{k}_2 = \mathfrak{k}_3$. Für diese Zusammensetzung gilt das assoziative und kommutative Gesetz. Da es nur endlich viele Klassen gibt, so heißt das:

55. Satz: *Die Klassen von $k(\sqrt{m})$ bilden in bezug auf ihre Multiplikation eine Abelsche Gruppe, deren Ordnung gleich der Klassenzahl h ist.*

Die Klasse der Hauptideale heißt die *Hauptklasse*, sie ist *das Einheitselement der Abelschen Gruppe.*

56. Satz: *In jeder Klasse gibt es ein Ideal $\mathfrak{w}$ der Form:*

$$\mathfrak{w} = (w,\ s + \omega),$$

das zu einem beliebigen Ideal $\mathfrak{w}$ teilerfremd ist.

Wir übergehen den einfachen Beweis.

Eine ganze Zahl ε von $k(\sqrt{m})$, deren Norm ± 1 ist, heißt eine *Einheit* von k. Da $m < 0$ ist, so ist $\varepsilon\varepsilon' > 0$, jede Einheit hat daher die Norm $+1$. Die einfachsten Einheiten sind ± 1, sie treten in jedem Körper auf. Ist $\varepsilon = x + y\omega$, $y \neq 0$, so muß:

$$(x + y\omega)(x + y\omega') = 1$$

sein, also im Falle $m \not\equiv 1 \pmod 4$:

$$x^2 - y^2 m = 1,$$

was nur für $m = -1$ die Lösungen $\varepsilon = \pm i = \pm\sqrt{-1}$ zuläßt. Der Körper $k(i)$ besitzt somit vier Einheiten: $\pm i$, ± 1. Im Falle $m \equiv 1 \pmod 4$ ist:

$$x^2 - xy + y^2\,\frac{1-m}{4} = 1,$$

was nur im Falle $m = -3$ die Lösungen $\varepsilon = \pm\dfrac{-1 \pm \sqrt{-3}}{2} = \pm\varrho, \pm\varrho^2$ zuläßt. Der Körper $k(\sqrt{-3})$ hat daher 6 Einheiten: $\pm\varrho$, $\pm\varrho^2$, ± 1.

57. Satz: *Der Körper $k(\sqrt{m})$ hat $e = 2, 4, 6$ Einheiten, je nachdem $m \neq -1, \neq -3$ oder $m = -1$ oder $m = -3$ ist.*

12. Definition: *Kann die Zahl α von $k(\sqrt{m})$ so mit einer zum Ideal $\mathfrak{f}$ teilerfremden ganzen Zahl ξ multipliziert werden, daß $\alpha\xi$ eine Zahl von $\mathfrak{f}$ wird, so sagt man, α sei kongruent null, modulo $\mathfrak{f}$:*

$$\alpha \equiv 0 \pmod{\mathfrak{f}}.$$

Sind α und β zwei Zahlen, die durch Multiplikation mit einer zu $\mathfrak{f}$ teilerfremden ganzen Zahl zu einer ganzen Zahl gemacht werden können, und für die:

$$\alpha - \beta \equiv 0 \pmod{\mathfrak{f}},$$

so sagt man, α sei kongruent β, modulo $\mathfrak{f}$:

$$\alpha \equiv \beta \pmod{\mathfrak{f}}.$$

58. Satz: *Sind zwei Zahlen einer dritten kongruent (mod. $\mathfrak{f}$), so sind sie auch untereinander kongruent (mod. $\mathfrak{f}$).*

Denn aus: $\alpha \equiv \beta \pmod{\mathfrak{f}}$, $\alpha \equiv \gamma \pmod{\mathfrak{f}}$

folgt die Existenz von zwei ganzen, zu $\mathfrak{f}$ teilerfremden Zahlen ξ und η, so daß $\xi(\alpha - \beta)$, $\eta(\alpha - \gamma)$ in $\mathfrak{f}$ sind. Da das Ideal $\mathfrak{f}$ ein Modul ist, muß nach Definition 6 und Satz 49 auch:

$$\xi\eta(\alpha - \beta) - \xi\eta(\alpha - \gamma) = \xi\eta(\gamma - \beta)$$

eine Zahl von $\mathfrak{f}$ sein.

Eine Beziehung, wie sie durch Definition 12 gegeben wird, heißt eine *Kongruenz*.

59. Satz: *Summen, Differenzen und Produkte der linken und rechten Seiten von Kongruenzen (mod. $\mathfrak{f}$) sind einander kongruent (mod. $\mathfrak{f}$).*

Eine Kongruenz (mod. $\mathfrak{f}$) bleibt richtig, wenn man beide Seiten derselben mit derselben ganzen Zahl multipliziert, oder durch dieselbe, zu $\mathfrak{f}$ teilerfremde ganze Zahl dividiert.

Der Beweis erfolgt wie bei Satz 58.

60. Satz: *Die Anzahl aller zueinander (mod. $\mathfrak{f}$) inkongruenten Zahlen ist gleich der Norm $n(\mathfrak{f})$ von $\mathfrak{f}$.*

Wir dürfen uns auf die ganzen Zahlen beschränken, und nehmen $\mathfrak{f}$ durch die kanonische Basis $(w, s + t\omega)$ gegeben an. Durchläuft in $x + y\omega$ x alle Zahlen $0, 1, \ldots, w - 1$, y alle Zahlen $0, 1, \ldots, t - 1$, so erhält man tw Zahlen, die alle inkongruent sind. Da nach (16) $n(\mathfrak{f}) = tw$, so ist der Satz bewiesen. Denn umgekehrt ist jede Zahl einer dieser Zahlen (mod. $\mathfrak{f}$) kongruent.

Ist $\alpha = x + y\omega$ irgendeine ganze Zahl und $\mathfrak{p}$ ein Primideal, das in der rationalen Primzahl p aufgeht, so ist:

$$\alpha^p - \alpha \equiv (x + y\omega)^p - x - y\omega \equiv x^p + y^p\omega^p - x - y\omega \pmod{p}.$$

Wegen des Satzes von Fermat ist $x^p - x$, $y^p - y$ durch p teilbar, also:

$$\alpha^p - \alpha \equiv y(\omega^p - \omega) \pmod{p}.$$

Ist $\mathfrak{p}$ vom 1. Grade, so ist nach Satz 51 und 52, falls $p \neq 2$ und $\left(\frac{d}{p}\right) \neq 0$:

$$m \equiv u^2 \pmod{p}, \quad m^{\frac{p-1}{2}} \equiv u^{p-1} \equiv 1 \pmod{p},$$

also: $$\omega^p - \omega \equiv 0 \pmod{p}, \quad \alpha^p - \alpha \equiv 0 \pmod{p}.$$

Dasselbe tritt auch ein für $p = 2$ und $\left(\frac{d}{p}\right) \neq 0$, $m \equiv 1 \pmod{8}$.

Ist dagegen $\mathfrak{p}$ vom 2. Grade, so ist:

$$p \neq 2\colon\ m^{\frac{p-1}{2}} \equiv -1 \pmod{p}, \quad \omega^p - \omega' \equiv 0 \pmod{p}, \quad \alpha^p - \alpha' \equiv 0 \pmod{p}.$$

$$p = 2, \quad m \equiv 5 \pmod{8}, \quad \omega^2 \equiv \omega' \pmod{2}.$$

61. Satz: *Ist $\mathfrak{p}$ ein in (p) enthaltenes Primideal von $k(\sqrt{m})$, für das $\left(\frac{d}{p}\right) \neq 0$, so ist:* $\alpha^p \equiv \alpha$ oder $\equiv \alpha' \pmod{p}$,

je nachdem $\mathfrak{p}$ von erstem oder zweitem Grade ist.

62. Satz: *Die Anzahl $\varphi(\mathfrak{f})$ der zu $\mathfrak{f}$ teilerfremden, (mod. $\mathfrak{f}$) inkongruenten ganzen Zahlen in $k(\sqrt{m})$ ist:*

$$\varphi(\mathfrak{f}) = n(\mathfrak{f}) \prod_{(\mathfrak{p})} \left(1 - \frac{1}{n(\mathfrak{p})}\right) = \prod_{(\mathfrak{p})} n(\mathfrak{p}^{r-1})(n(\mathfrak{p}) - 1),$$

wo $\mathfrak{f} = \mathfrak{p}_1^{r_1} \mathfrak{p}_2^{r_2} \ldots \mathfrak{p}_n^{r_n}$ die Primidealzerlegung von $\mathfrak{f}$ in voneinander verschiedene Primideale $\mathfrak{p}_1, \mathfrak{p}_2, \ldots \mathfrak{p}_n$ bedeutet.

Denn zerlegen wir $\mathfrak{f}$ in zwei zueinander teilerfremde Faktoren $\mathfrak{f}_1$ und $\mathfrak{f}_2$, so ist:

$$\varphi(\mathfrak{f}) = \varphi(\mathfrak{f}_1)\,\varphi(\mathfrak{f}_2),$$

da man die zu $\mathfrak{f}_1$ teilerfremden, (mod. $\mathfrak{f}_1$) inkongruenten Zahlen auch zu $\mathfrak{f}_2$ als teilerfremd annehmen darf. Wir brauchen also die obige Formel nur noch für Primidealpotenzen zu beweisen. Ist $\mathfrak{f} = \mathfrak{p}^r = (p^r, s + \omega)$ und $\mathfrak{p}$ vom 1. Grade, so sind in den p^r inkongruenten Zahlen $x + y(s + \omega)$ vom Beweise zum Satze 60 die Anzahl der durch $\mathfrak{p}$ teilbaren zu subtrahieren. Das sind p^{r-1} Zahlen, für die x eine der Zahlen $0, p, 2p, \ldots (p^{r-1} - 1)\,p$ ist. Es bleiben:

$$\varphi(\mathfrak{p}^r) = p^{r-1}(p - 1) = n(\mathfrak{p}^{r-1})(n(\mathfrak{p}) - 1).$$

Ist $\mathfrak{f} = \mathfrak{p}^r$, $\mathfrak{p} = (p, p\omega)$ vom 2. Grade, so sind auch unter den y alle p^{r-1} durch p teilbaren wegzulassen, also im ganzen p^{2r-2}, und es wird:

$$\varphi(\mathfrak{p}^r) = p^{2r} - p^{2r-2} = n(\mathfrak{p}^{r-1})(n(\mathfrak{p}) - 1).$$

Wir fügen zum Schlusse noch folgenden Satz an, den wir später gebrauchen werden, und der sofort aus der Definition 5 und aus dem Gaußschen Satze über Zerlegung von rationalen Funktionen folgt:

63. Satz: *Genügt eine Zahl von $k(\sqrt{m})$ einer algebraischen Gleichung, deren Koeffizienten ganze Zahlen sind und deren oberster Koeffizient eins ist, so ist sie eine ganze Zahl von $k(\sqrt{m})$.*

2. Substitutionen n^{ter} Ordnung und quadratischer Körper.

Ist Ω irgendeine imaginäre Zahl von $k(\sqrt{m})$, so genügt sie einer quadratischen Gleichung:
$A\Omega^2 + B\Omega + C = 0$, wo $AC \neq 0$, A, B, C ganze rationale Zahlen ohne gemeinsamen Teiler sind.

Diese läßt sich so schreiben:

$$\Omega = \frac{-C}{A\Omega + B},$$

und Ω ist Fixpunkt der Substitution n^{ter} Ordnung $T = \begin{pmatrix} 0 & -C \\ A & B \end{pmatrix}$, wo $n = AC$.

Wir wollen umgekehrt fragen, gibt es zu einer gegebenen Ordnung n eine Substitution n^{ter} Ordnung T, deren Fixpunkte Zahlen von $k(\sqrt{m})$ sind? Ist $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $n = ad - bc$, so bestimmen sich die Fixpunkte aus der quadratischen Gleichung:

$$(c \neq 0) \quad \frac{az+b}{cz+d} = z, \quad cz^2 - (a-d)z - b = 0, \quad z_{1,2} = \frac{(a-d) \pm \sqrt{D}}{2c},$$

wo die Diskriminante D den Wert besitzt:

$$D = (a-d)^2 + 4bc = (a+d)^2 - 4n.$$

Damit die Wurzeln in $k(\sqrt{m})$ liegen, muß es eine rationale Zahl u geben, für die: $(a+d)^2 - 4n = u^2 m$ oder:

$$4n = (a+d)^2 - u^2 m, \quad n = n\left(\frac{a+d+u\sqrt{m}}{2}\right).$$

u ist eine ganze rationale Zahl, und zugleich mit $(a+d)$ gerade oder ungerade. Im ersteren Falle ist $\frac{a+d+u\sqrt{m}}{2}$ eine ganze Zahl von k, im zweiten Falle ist $\frac{(a+d)^2 - mu^2}{4}$ ganz, also $m \equiv 1 \pmod 4$. Nach Satz 46 ist dann $\frac{a+d+u\sqrt{m}}{2}$ ganz, also in jedem Falle:

$$n = n(x + y\omega), \quad \frac{a+d+u\sqrt{m}}{2} = x + y\omega,$$

wo x, y ganze, rationale Zahlen sein müssen.

64. Satz: *Damit die Fixpunkte einer Substitution n^{ter} Ordnung in $k(\sqrt{m})$ liegen, muß notwendig n Norm einer ganzen Zahl von $k(\sqrt{m})$ sein.*

Wir nehmen jetzt umgekehrt an, dies sei erfüllt, n sei Norm von $x + y\omega$: $n = n(x + y\omega)$, $y \neq 0$; x, y ganz und rational,

wobei *wir noch voraussetzen, daß $y \neq 0$ und x und y ohne gemeinsamen Teiler seien.* Eine solche Darstellung werden wir eine *eigentliche Dar-*

stellung von n in k nennen. Es sei ferner $\mathfrak{w} = (\omega_1, \omega_2)$ ein durch seine Basis gegebenes Ideal von k, wir fragen dann, ob $\omega_2 : \omega_1$ Fixpunkt einer Substitution T n^{ter} Ordnung werden kann? Wir dürfen uns auf den Fall beschränken, daß ω_1, ω_2 eine *kanonische* Basis von $\mathfrak{w}$ ist; denn jede andere wird nach Satz 50 aus ω_1, ω_2 durch eine Substitution S der Modulgruppe erhalten, und das zugehörige Verhältnis der Basiszahlen ist, falls $\omega_2 : \omega_1$ Fixpunkt von T ist, Fixpunkt von STS^{-1}, was dieselbe Ordnung besitzt. Es sei also $\omega_1 = tw$, $\omega_2 = t(s + \omega)$:

$$\frac{\omega_2}{\omega_1} = \frac{s+\omega}{w}, \quad \text{wo} \quad (s+\omega)(s+\omega') \equiv 0 \pmod{w}.$$

Ist $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, so muß $\omega_2 : \omega_1$ Wurzel von:

$$cz^2 - (a-d)z - b = 0, \quad \text{wo} \quad \frac{a+d+u\sqrt{m}}{2} = x + y\omega \quad \text{ist,}$$

sein. Daher:

$$a + d = 2x + y(\omega + \omega'), \quad \frac{s+\omega}{w} = \frac{\frac{a-d}{2} + \frac{u}{2}\sqrt{m}}{c} = \frac{-d + x + y\omega}{c},$$

$$d = x - sy, \quad c = wy, \quad ad - bc = n.$$

Aus diesen Gleichungen ergibt sich:

$$\begin{aligned} a &= x + sy + y(\omega + \omega') \\ d &= x - sy, \\ c &= wy \\ b &= -\frac{n - ad}{c} = -\frac{y}{w}(s+\omega)(s+\omega'). \end{aligned} \tag{18}$$

a, b, c, d sind somit durch x, y, w, s eindeutig gegebene, ganze, rationale Zahlen. Sie besitzen auch keinen gemeinsamen Teiler; denn wäre p eine in a, b, c, d aufgehende Primzahl, so wäre w oder y durch p teilbar. Aus $y \equiv 0 \pmod{p}$ würde aber sofort $x \equiv 0 \pmod{p}$ folgen, gegen die Annahme, daß n eigentlich dargestellt sei. Ist $w \equiv 0 \pmod{p}$, $y \not\equiv 0 \pmod{p}$, so folgt:

$$\begin{aligned} -b = \frac{y}{w}(s+\omega)(s+\omega') &\equiv 0 \pmod{p}, \\ (s+\omega)(s+\omega') &\equiv 0 \pmod{p^2}, \\ \frac{a-d}{y} = 2s + \omega + \omega' &\equiv 0 \pmod{p}. \end{aligned}$$

Quadriert man die letzte Kongruenz und subtrahiert von ihr die vierfache vorletzte, so folgt:

$$(\omega' - \omega)^2 \equiv 0 \pmod{p^2}.$$

Da $(\omega' - \omega)^2$ gleich m oder $4m$ ist und m quadratfrei, so kann nur $m \not\equiv 1 \pmod{4}$, $p = 2$ sein, und es muß:

$$s^2 - m \equiv 0 \pmod{4}$$

sein, was unmöglich ist. Die Annahme ist zu verwerfen, und $T = \binom{a\ b}{c\ d}$ ist eine Substitution n^{ter} Ordnung mit dem Fixpunkt $\omega_2 : \omega_1$. Denn die Wurzeln von

$$yw z^2 - y(2s + \omega + \omega')z + \frac{y}{w}(s + \omega)(s + \omega') = 0$$

sind:

$$s + \frac{\omega + \omega'}{2} \pm \frac{\omega - \omega'}{2} = \frac{s + \omega}{w}, \quad \frac{s + \omega'}{w}.$$

65. Satz: *Ist* $\mathfrak{w} = (\omega_1, \omega_2)$ *ein beliebiges Ideal von* $k(\sqrt{m})$, *so gibt es zu einer eigentlichen Darstellung von* n *eine und nur eine Substitution* n^{ter} *Ordnung* T, *deren Fixpunkt* $\frac{\omega_2}{\omega_1}$ *ist.*

Aus der obigen Darstellung (18) erkennt man, daß a, b, c, d einen gemeinsamen Teiler haben, sobald x und y einen solchen besitzen. Die Annahme der eigentlichen Darstellung ist somit wesentlich.

Nimmt man statt x, y die entgegengesetzten Werte $-x, -y$, so hat man wieder eine eigentliche Darstellung, zu der aber dasselbe $T = \binom{-a\ -b}{-c\ -d} = \binom{a\ b}{c\ d}$ gehört.

Der Basis eines Ideals $\mathfrak{w}$ und einer eigentlichen Darstellung von n kann nicht nur ein T, sondern die ganze durch T erzeugte Transformationsgruppe $\mathfrak{T}_n(T)$ zugeordnet werden. Es fragt sich, ob außer den beiden vorigen, voneinander verschiedenen eigentlichen Darstellungen noch andere *dieselbe* Transformationsgruppe in bezug auf $\mathfrak{w}$ hervorrufen? Es seien also:

$$T_1 = \binom{a_1\ b_1}{c_1\ d_1}, \quad a_1 d_1 - b_1 c_1 = n, \quad T_2 = \binom{a_2\ b_2}{c_2\ d_2}, \quad a_2 d_2 - b_2 c_2 = n$$

zwei verschiedene Substitutionen n^{ter} Ordnung, die die gleiche Transformationsgruppe erzeugen, d. h. zwischen denen eine Beziehung $T_1 = S T_2$, wo S der Modulgruppe angehört, existiert. Wir setzen voraus, T_1 und T_2 entspringen aus den beiden voneinander verschiedenen, eigentlichen Darstellungen: $n = n(x_1 + y_1\omega), \quad n = n(x_2 + y_2\omega), \quad y_1 \neq 0, \quad y_2 \neq 0,$

und beide T_1 und T_2 haben denselben Fixpunkt $\frac{\omega_2}{\omega_1} = \frac{s + \omega}{w}$, d. h.

$$T_1 \frac{\omega_2}{\omega_1} = \frac{\omega_2}{\omega_1}, \quad T_2^{-1} \frac{\omega_2}{\omega_1} = \frac{\omega_2}{\omega_1}, \quad T_1 T_2^{-1} \frac{\omega_2}{\omega_1} = T_1 \frac{\omega_2}{\omega_1} = \frac{\omega_2}{\omega_1}.$$

Ist also $T_1 = S T_2$, $S = T_1 T_2^{-1}$, so muß auch die Substitution S der Modulgruppe den Fixpunkt $\frac{\omega_2}{\omega_1}$ haben. Dieser ist ein Punkt der oberen Halbebene, S ist von elliptischem Typus und nach Kap. 1, § 2 a), S. 7 haben alle Fixpunkte von solchen S eine der beiden Formen: $\frac{\alpha + i}{\gamma}$ und $\frac{\alpha + \varrho}{\gamma}, \frac{(\alpha + 1) + \varrho}{\gamma}$, wo $\varrho = \frac{-1 + \sqrt{-3}}{2}$. Wenn daher $m \neq -1$ oder

$+ -3$ ist, so muß $T_1 = T_2$, $\pm a_1 = a_2$, $\pm b_1 = b_2$, $\pm c_1 = c_2$, $\pm d_1 = d_2$ sein, was den beiden Darstellungen von n:

$$x_1, y_1, \quad x_2 = -x_1, \quad y_2 = -y_1,$$

entspricht.

Im Falle $m = -1$ folgt aus

$$\frac{s+i}{w} = \frac{\alpha+i}{\gamma}, \quad \alpha + \delta = 0,$$

daß $\gamma = w$, $\alpha = s = -\delta$ sein muß, und:

$$S = \begin{pmatrix} s & -\frac{s^2+1}{w} \\ w & -s \end{pmatrix} + E, \quad S^2 = E.$$

$$ST_2 = \begin{pmatrix} sa_2 - \frac{s^2+1}{w}c_2, & sb_2 - \frac{s^2+1}{w}d_2 \\ wa_2 - sc_2, & wb_2 - sd_2 \end{pmatrix}.$$

Es gibt zwei T: T_2 und $T_1 = ST_2$, die den Fixpunkt $\omega_2 : \omega_1$ besitzen und dieselbe Transformationsgruppe erzeugen.

Im Falle $m = -3$ folgt aus:

$$\frac{s+\varrho}{w} = \frac{\alpha+\varrho}{\gamma}, \text{ für } \alpha + \delta = +1; \quad \frac{s+\varrho}{w} = \frac{\alpha+1+\varrho}{\gamma}, \quad \text{für } \alpha + \delta = -1,$$

daß $\gamma = w$, $\alpha = s$ oder $= s-1$ sein muß, und zwei S existieren:

$$S = \begin{pmatrix} s & -\frac{1-s+s^2}{w} \\ w & -(s-1) \end{pmatrix}, \quad S^2 = \begin{pmatrix} s-1 & -\frac{1-s+s^2}{w} \\ w & -s \end{pmatrix}, \quad S^3 = E,$$

für die $\omega_2 : \omega_1$ Fixpunkt ist. Es gibt dann drei T: T_2, ST_2, S^2T_2, die $\omega_2 : \omega_1$ als Fixpunkt besitzen und dieselbe Transformationsgruppe erzeugen:

$$ST_2 = \begin{pmatrix} sa_2 - \frac{1-s+s^2}{w}c_2, & sb_2 - \frac{1-s+s^2}{w}d_2 \\ wa_2 - (s-1)c_2, & wb_2 - (s-1)d_2 \end{pmatrix},$$

$$S^2T_2 = \begin{pmatrix} (s-1)a_2 - \frac{1-s+s^2}{w}c_2, & (s-1)b_2 - \frac{1-s+s^2}{w}d_2 \\ wa_2 - sc_2, & wb_2 - sd_2 \end{pmatrix}.$$

Es fragt sich, ob die zwei ($m = -1$), oder drei ($m = -3$) Substitutionen T wirklich aus verschiedenen eigentlichen Darstellungen entspringen. Es ist nach (18) für:

a) $m = -1$, $\pm a_1 = sa_2 - \frac{1+s^2}{w}c_2$,

$$\pm c_1 = wa_2 - sc_2,$$

$$\pm y_1 = \frac{wa_2 - sc_2}{w} = x_2 + sy_2 - sy_2 = x_2,$$

also: $\pm x_1 = \pm a_1 - sx_2 = sx_2 + s^2y_2 - (s^2+1)y_2 - sx_2 = -y_2$.

Da x_2 und y_2 teilerfremd sein müssen, ist x_1, y_1 eine zweite eigentliche Darstellung, weil für $n \neq 1$ $x_2 \neq 0$ sein muß.

b) $m = -3$, $T_1 = ST_2$, $\pm a_1 = sa_2 - \frac{1-s+s^2}{w} c_2$,

$$\pm c_1 = wa_2 - (s-1)c_2,$$

$$\pm y_1 = \frac{wa_2 - (s-1)c_2}{w} = x_2 + sy_2 - y_2 - (s-1)y_2 = x_2,$$

also: $$\pm x_1 = \pm a_1 - sx_2 + x_2 = s(x_2 + (s-1)y_2) - (1-s+s^2)y_2 - (s-1)x_2$$
$$= x_2 - y_2.$$

$$T_1 = S^2 T_2, \quad \pm a_1 = (s-1)a_2 - \frac{1-s+s^2}{w} c_2,$$

$$\pm c_1 = wa_2 - sc_2,$$

$$\pm y_1 = \frac{wa_2 - sc_2}{w} = x_2 + sy_2 - y_2 - sy_2 = x_2 - y_2,$$

also: $$\pm x_1 = \pm a_1 - (s-1)(x_2 - y_2) = (s-1)(x_2 + sy_2 - y_2)$$
$$-(1-s+s^2)y_2 - s(x_2 - y_2) + (x_2 - y_2) = -y_2.$$

Auch hier sind für $n \neq 1$ alle drei Darstellungen eigentlich und voneinander verschieden.

Wir sehen, daß im Falle $m \neq -1$ oder $\neq -3$ zwei eigentliche, wegen $y \neq 0$ voneinander verschiedene Darstellungen x, y und $-x, -y$ dieselbe Gruppe $\mathfrak{T}_n(T)$, im Falle $m = -1$ vier eigentliche, voneinander verschiedene Darstellungen x, y; $-x, -y$; $-y, x$; $+y, -x$ dieselbe Gruppe $\mathfrak{T}_n(T)$, im Falle $m = -3$ sechs eigentliche, voneinander verschiedene Darstellungen x, y; $-x, -y$; $x-y, x$; $-x+y, -x$; $-y, x-y$; $y, -x+y$ dieselbe Gruppe $\mathfrak{T}_n(T)$ hervorrufen. Man erhält die Darstellungen, indem man eine Darstellung mit allen e Einheiten von $k(\sqrt{m})$ multipliziert (Satz 57).

66. Satz: *Ist $\mathfrak{w} = (\omega_1, \omega_2)$ ein beliebiges, durch eine Basis gegebenes Ideal, und gibt es genau v voneinander verschiedene, eigentliche Darstellungen von n in $k(\sqrt{m})$, so ist $\omega_2 : \omega_1$ Fixpunkt von Substitutionen T, die $v : e$ voneinander verschiedene Transformationsgruppen n^{ter} Ordnung $\mathfrak{T}_n(T)$ hervorrufen, wo e die Anzahl der Einheiten in $k(\sqrt{m})$ ist.*

3. Die singulären Moduln.

Es sei $\mathfrak{w} = (\omega_1, \omega_2)$ ein durch seine Basis gegebenes Ideal von $k(\sqrt{m})$, wo nach Voraussetzung $\omega_2 : \omega_1$ einen positiven Imaginärteil hat. Wir studieren die Werte $j\left(\frac{\omega_2}{\omega_1}\right)$.

67. Satz: *$j\left(\frac{\omega_2}{\omega_1}\right)$ hängt nicht von der Wahl der Basis in $\mathfrak{w}$ ab, sondern hat für jede Basis von $\mathfrak{w}$ denselben Wert.*

Ist $\overline{\omega}_1$, ω_2 eine andere Basis von $\mathfrak{w}$, so gibt es nach Satz 50 eine Substitution S der Modulgruppe $\mathfrak{G}$, so daß

$$\frac{\overline{\omega}_2}{\omega_1} = S\frac{\omega_2}{\omega_1},$$

somit nach der Grundeigenschaft von $j(z)$:

$$j\left(\frac{\overline{\omega}_2}{\overline{\omega}_1}\right) = j\left(S\frac{\omega_2}{\omega_1}\right) = j\left(\frac{\omega_2}{\omega_1}\right).$$

68. Satz: $j\left(\frac{\omega_2}{\omega_1}\right)$ *hängt nicht von dem Ideal* $\mathfrak{w} = (\omega_1, \omega_2)$ *ab, sondern nur von der Klasse* $\mathfrak{k}$, *in der* $\mathfrak{w}$ *liegt.* $j\left(\frac{\omega_2}{\omega_1}\right)$ *hat für alle Ideale von* $\mathfrak{k}$ *denselben Wert.*

Sind $\mathfrak{w}$ und $\overline{\mathfrak{w}}$ zwei äquivalente Ideale, d. h. liegen sie in derselben Klasse $\mathfrak{k}$, so gibt es zwei ganze Zahlen ν und $\overline{\nu}$, so daß:

$$(\nu)\mathfrak{w} = (\overline{\nu})\overline{\mathfrak{w}}, \quad \text{oder} \quad (\nu)(\omega_1, \omega_2) = (\overline{\nu})(\overline{\omega}_1, \overline{\omega}_2).$$

Nun ist $(\nu)(\omega_1, \omega_2) = (\nu\omega_1, \nu\omega_2)$, $(\overline{\nu})(\overline{\omega}_1, \overline{\omega}_2) = (\overline{\nu}\overline{\omega}_1, \overline{\nu}\overline{\omega}_2)$, d. h. $\nu\omega_1$ und $\nu\omega_2$ sind wieder eine Basis von $(\nu)\mathfrak{w}$, und entsprechend $\overline{\nu}\overline{\omega}_1$, $\overline{\nu}\overline{\omega}_2$ von $(\overline{\nu})\overline{\mathfrak{w}}$. Dasselbe Ideal ist also durch zwei verschiedene Basen gegeben, also muß es ein S von $\mathfrak{G}$ geben, so daß

$$\begin{aligned} \overline{\nu}\overline{\omega}_2 &= \alpha\nu\omega_2 + \beta\nu\omega_1, \\ \overline{\nu}\overline{\omega}_1 &= \gamma\nu\omega_2 + \delta\nu\omega_1, \end{aligned} \quad \text{oder} \quad \frac{\overline{\omega}_2}{\overline{\omega}_1} = S\frac{\omega_2}{\omega_1}.$$

Darum ist wie vorhin: $j\left(\frac{\overline{\omega}_2}{\overline{\omega}_1}\right) = j\left(S\frac{\omega_2}{\omega_1}\right) = j\left(\frac{\omega_2}{\omega_1}\right)$.

Da $j\left(\frac{\omega_2}{\omega_1}\right)$ nur von $\mathfrak{k}$ abhängt, setzen wir:

$$j\left(\frac{\omega_2}{\omega_1}\right) = j(\mathfrak{k}).$$

Man bezeichnet $j(\mathfrak{k})$ als eine *Klasseninvariante.* Sind $\mathfrak{k}_1, \mathfrak{k}_2, \ldots \mathfrak{k}_h$ die h verschiedenen Klassen von $k(\sqrt{m})$, so gibt es h Klasseninvarianten:

$$j(\mathfrak{k}_1), j(\mathfrak{k}_2), \ldots j(\mathfrak{k}_h).$$

Funktionentheoretisch heißen sie *singuläre Werte der elliptischen Modulfunktion* $j(z)$, oder kurz *singuläre Moduln.*

69. Satz: *Die singulären Moduln* $j(\mathfrak{k})$ *sind algebraische Zahlen.*

Eine Zahl heißt algebraisch, wenn sie einer algebraischen Gleichung mit rationalen Koeffizienten genügt. Es sei $\mathfrak{w} = (\omega_1, \omega_2)$ ein Ideal von $\mathfrak{k}$. Wir wählen $n > 1$ so, daß es wenigstens eine eigentliche Darstellung in $k(\sqrt{m})$ besitzt, z. B. $n = (1 + \omega)(1 + \omega')$. Dann ist $\frac{\omega_2}{\omega_1}$ Fixpunkt einer Substitution n^{ter} Ordnung $T = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$:

$$\frac{\omega_2}{\omega_1} = T\frac{\omega_2}{\omega_1} = \frac{a\omega_2 + b\omega_1}{c\omega_2 + d\omega_1}, \quad ad - bc = n.$$

Setzen wir in der Transformationsgleichung:

$$\Phi_n(t, \tau) = 0$$

$t = j(Tz)$, $\tau = j(z)$, so ist sie identisch erfüllt. Für $z = \frac{\omega_2}{\omega_1}$ ist aber $t = \tau$, und $j\left(\frac{\omega_2}{\omega_1}\right)$ ist daher Wurzel von:

$$\Phi_n(t, t) = 0.$$

Die linke Seite ist nicht identisch in allen t null, da sonst $\Phi_n(t, \tau)$ durch $t - \tau$ algebraisch teilbar wäre, was gegen die Irreduzibilität von Φ_n spräche (Satz 37). Die Koeffizienten von Φ_n sind ganze, rationale Zahlen (Satz 42). Damit ist der Satz bewiesen. Wir setzen von nun an:

$$\Phi_n(t, t) = f_n(t).$$

Nach Satz 65 genügen der Gleichung $f_n(t) = 0$ alle h singulären Moduln $j(\mathfrak{k}_1), j(\mathfrak{k}_2), \ldots j(\mathfrak{k}_h)$.

70. Satz: *Die h singulären Moduln $j(\mathfrak{k}_1), j(\mathfrak{k}_2), \ldots j(\mathfrak{k}_h)$ sind alle voneinander verschieden.*

Denn wäre $j(\mathfrak{k}) = j(\bar{\mathfrak{k}})$, oder $j\left(\frac{\omega_2}{\omega_1}\right) = j\left(\frac{\bar{\omega}_2}{\bar{\omega}_1}\right)$, so muß es, da $j(z)$ jeden Wert im Diskontinuitätsbereich nur einmal annimmt, ein S der Modulgruppe geben, für das:

$$\frac{\bar{\omega}_2}{\bar{\omega}_1} = S\,\frac{\omega_2}{\omega_1}, \quad \text{oder} \quad \begin{aligned} \nu\bar{\omega}_2 &= \alpha\nu\omega_2 + \beta\nu\omega_1, \\ \nu\bar{\omega}_1 &= \gamma\nu\omega_2 + \delta\nu\omega_1, \end{aligned} \qquad \alpha\delta - \beta\gamma = 1,$$

d. h. $\mathfrak{w}$ und $\bar{\mathfrak{w}}$ sind äquivalent, $\mathfrak{k} = \bar{\mathfrak{k}}$.

Wir setzen: $$H_m(t) = \prod_{r=1}^{h}(t - j(\mathfrak{k}_r)).$$

$f_n(t)$ ist durch $H_m(t)$ teilbar. Da es aber genau $\frac{\nu}{e}$ T n^{ter} Ordnung gibt, die verschiedene Transformationsgruppen $\mathfrak{T}_n(T)$ nach Satz 66 hervorrufen, ist jedes $j(\mathfrak{k}_r)$ genau $\frac{\nu}{e}$ fache Wurzel von $f_n(t) = \Phi_n(t, t)$, d. h. $f_n(t)$ ist genau durch $H_m(t)^{\frac{\nu}{e}}$ teilbar.

71. Satz: *$\Phi_n(t, t)$ ist genau durch die $\frac{\nu}{e}^{\text{te}}$ Potenz von $H_m(t)$ teilbar, und der Quotient hat keine Wurzeln mit $H_m(t)$ gemein.*

Um den Grad der Gleichung, dem die singulären Moduln genügen, zu bestimmen, beweisen wir den

72. Satz: *$H_m(t)$ hat rationale Koeffizienten. $j(\mathfrak{k})$ ist daher eine algebraische Zahl von höchstens h^{tem} Grade, wo h die Klassenzahl von $k(\sqrt{m})$ ist.*

$H_m(t) = 0$ heißt die *Klassengleichung* von $k(\sqrt{m})$.

Wir beweisen zuerst den Satz für $m = -1$. Hier ist $h = 1$, und als Ideal der einen Klasse können wir $\mathfrak{w} = (1, \sqrt{-1})$ nehmen; nun ist nach (14): $j(i) = 2^6 3^3$, daher: $H_{-1}(t) = t - 2^6 3^3$.

Ist $m = -3$, so ist ebenfalls $h = 1$, und die eine Klasse wird durch $\mathfrak{w} = \left(1, \frac{-1+\sqrt{-3}}{2}\right)$ repräsentiert. Nach (14) ist:

$$j(\varrho) = 0, \quad \text{daher} \quad H_{-3}(t) \equiv t.$$

Wir setzen von nun an m verschieden von -1 und -3 voraus. Dann ist $e = 2$, nach Satz 66 ist daher jedes $\omega_2 : \omega_1$ Fixpunkt von $\frac{v}{2}$ T, die verschiedene Gruppen $\mathfrak{T}_n(T)$ erzeugen. Ist $n = -m$, so besitzt:

$$\Phi_{-m}(t, t) = 0$$

alle $t = j(z)$ zu Wurzeln, für die es ein $T - m^{\text{ter}}$ Ordnung gibt, so daß $j(Tz) = j(z)$ ist. Dann ist aber auch $j(T^{-1}z) = j(z)$; für jedes solche z ist daher $t = j(z)$ Doppelwurzel von Φ_{-m}, außer wenn:

$$T = ST^{-1}, \quad T^2 = S$$

ist, wo S der Modulgruppe angehört. Setzt man:

$$\Phi_{-m}(t, t) = \Phi_1(t)\,\Phi_2^2(t),$$

so gehören alle Wurzeln von $\Phi_1 : t = j(z)$ zu solchen z, die Fixpunkte einer Substitution $-m^{\text{ter}}$ Ordnung T sind, für die $T^2 = S$. Es sei:

$$T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad ad - bc = -m, \quad T^2 = \begin{pmatrix} a^2 + bc & ab + bd \\ ca + dc & cb + d^2 \end{pmatrix}.$$

Dann folgt aus $T^2 = S$:

$$a^2 + bc \equiv 0, \quad b(a + d) \equiv 0, \quad c(a + d) \equiv 0, \quad cb + d^2 \equiv 0 \pmod{-m},$$

oder wegen $ad - bc = -m$:

$$a(a + d) \equiv 0, \; b(a + d) \equiv 0, \; c(a + d) \equiv 0, \; d(a + d) \equiv 0 \pmod{-m}.$$

Da a, b, c, d keinen gemeinsamen Teiler haben, folgt:

$$a + d \equiv 0 \pmod{-m}.$$

Der Fixpunkt von T ist:

$$z = \frac{a - d + \sqrt{(a+d)^2 + 4m}}{2c}.$$

Setzt man $(a + d)^2 + 4m = u^2\overline{m}$, wo $u \neq 0$ und $\overline{m}$ eine negative, quadratfreie, ganze Zahl ist, so wird wegen der vorigen Kongruenz:

$$4 = \frac{\overline{m}}{m} u^2 - m\left(\frac{a+d}{m}\right)^2 = \left|\frac{\overline{m}}{m}\right| u^2 + |m|\left(\frac{a+d}{m}\right)^2.$$

Ist $\overline{m} = m$, so sind nur die Lösungen $a + d = 0$, $u = \pm 2$ möglich. $-m$ hat zwei und nur zwei eigentliche Darstellungen in $k(\sqrt{m})$, Φ_1 ist wegen Satz 57 und unserer Annahme über m durch die $\frac{2}{2} = 1$. Potenz von $H_m(t)$ teilbar und Φ_2 hat keine Wurzel mit H_m gemein.

Ist $\overline{m} \neq m$ und u gerade, so ist $|\overline{m}| < |m|$ und

$$1 = \left|\frac{\overline{m}}{m}\right| \left(\frac{u}{2}\right)^2 + |m| \left(\frac{a+d}{2m}\right)^2.$$

Diese Gleichung hat keine Lösung.

Ist $\overline{m} \neq m$ und u ungerade, so muß $a + d$ ungerade, also $\neq 0$ sein; ferner muß $|m| < 4$ sein. Es bleibt wegen unserer Annahme nur $m = -2$ übrig; in diesem Falle ist aber $a + d$ und u gerade. Auch jetzt ergibt sich keine Lösung.

Daher muß: $\Phi_1(t) \equiv c H_m(t)$, $\Phi_{-m}(t, t) \equiv c H_m(t) \Phi_2(t)^2$

sein, wo $c \neq 0$ eine rationale Zahl ist. Φ_{-m} hat rationale Koeffizienten, H_m hat nach Satz 70 nur einfache Wurzeln und keine Wurzel mit Φ_2 gemein, also kann man H_m durch rationale Operationen finden, und H_m muß rationale Koeffizienten haben.

Ist p eine rationale Primzahl, die in $k(\sqrt{m})$ eigentlich darstellbar ist, so ist $\Phi_p(t, t)$ durch $H_m(t)$ teilbar. Nach Satz 39 ist aber $\Phi_p(t, t)$ vom Grade $2p$ in t, und t kommt wegen $a_{p,p} = 0$ nur einmal mit dem Koeffizienten -1 vor. $j(\mathfrak{k})$ ist dann eine *ganze* algebraische Zahl. Dies Resultat gilt allgemein, denn nach Definition ist identisch in z:

$$\Phi_n(j(z), j(z)) \equiv \prod_{(r)} \prod \left(j(z) - j\left(\frac{a_r z + b_r}{d_r}\right)\right).$$

Entwickelt man nach q (Satz 14), so ist der Koeffizient der niedersten Potenz von q zugleich der Koeffizient der obersten Potenz von $t = j(z)$ in $\Phi_n(t, t)$. Nach dem Vorhergehenden genügt es, n nicht als Quadrat vorauszusetzen. Dann ist die Reihenentwicklung von

$$j(z) - j\left(\frac{a_r z + b_r}{d_r}\right) = \frac{1}{q} + \cdots, \text{ falls } a_r < d_r,$$

$$= -\frac{e^{-\frac{2\pi i b_r}{d_r}}}{q^{\frac{a_r}{d_r}}} + \cdots, \quad \text{falls} \quad a_r > d_r \quad \text{ist.}$$

Der Koeffizient der niedersten Potenz von q ist somit eine Einheitswurzel, und daher $= \pm 1$, da er zugleich rational sein muß. Der Satz 72 spricht sich jetzt genauer so aus (Satz 42):

Korollar zu Satz 72: *$j(\mathfrak{k})$ ist eine ganze, algebraische Zahl von höchstens h^{tem} Grade.*

4. Die Gruppe der Klassengleichung.

Es sei $\mathfrak{w} = (\omega_2, \omega_1)$ ein Ideal der Klasse $\mathfrak{k}$ von $k(\sqrt{m})$. Wir dürfen annehmen, daß $\mathfrak{w}$ durch die kanonische Basis $(w, s_1 + \omega)$ gegeben sei, da es auf den ganzen, rationalen Faktor t nicht ankommt:

$$\mathfrak{w} = (w, s_1 + \omega), \quad (s_1 + \omega)(s_1 + \omega') \equiv 0 \ (\text{mod. } w).$$

Es sei ferner $\mathfrak{p}$ ein Primideal 1. Grades, das zu w und $(\omega' - \omega)^2$ teilerfremd sei. Es ist dann nach Satz 52 von seinem konjugierten $\mathfrak{p}'$ verschieden. $\mathfrak{p}$ falle in die Klasse $\mathfrak{k}_p$, $\mathfrak{p}'$ in $\mathfrak{k}'_p$. Wir setzen nach Satz 51:

$$\mathfrak{p} = (p, \bar{s} + \omega), \quad \mathfrak{p}' = (p, -(\bar{s} + \omega')), \quad (\bar{s} + \omega)(\bar{s} + \omega') \equiv 0 \pmod{p},$$

wo $\bar{s}$ nur (mod. p) bestimmt ist. Wir können es dann so bestimmen, daß:

$$(\bar{s} + \omega)(\bar{s} + \omega') \equiv 0 \pmod{p^r} \tag{19}$$

wird, wo r eine beliebige ganze Zahl ist. Denn ist die Kongruenz nur für r erfüllt, so kann man sie auch für $r + 1$ erfüllen; man setze bloß $\bar{s}_1 = \bar{s} + p^r x$, dann ergibt sich x aus:

$$(\bar{s} + p^r x + \omega)(\bar{s} + p^r x + \omega') \equiv 0 \pmod{p^{r+1}},$$

$$x(2\bar{s} + \omega + \omega') \equiv -\frac{(\bar{s} + \omega)(\bar{s} + \omega')}{p^r} \pmod{p},$$

und $2\bar{s} + \omega + \omega' = \bar{s} + \omega + \bar{s} + \omega'$ ist nach Annahme weder durch $\mathfrak{p}$ noch durch $\mathfrak{p}'$ teilbar, also ist $x \pmod{p}$ bestimmt.

Wir setzen daher (19) als erfüllt voraus, und bestimmen weiter eine Zahl s so, daß:

$$s \equiv \bar{s} \pmod{p^r}, \qquad \text{und} \qquad s \equiv s_1 \pmod{w}.$$

Da nach Annahme $\mathfrak{p}$ und w, also auch p und w teilerfremd sind, ist $s \pmod{p^r w}$ bestimmt. Dann ist:

$$\mathfrak{w} = (w, s + \omega), \mathfrak{p} = (p, s + \omega), \mathfrak{p}' = (p, -(s + \omega')), (s + \omega)(s + \omega') \equiv 0 \pmod{p^r w}. \tag{20}$$

Das Produkt $\mathfrak{w}\mathfrak{p}$ hat jetzt die Basisdarstellung: $\mathfrak{w}\mathfrak{p} = (wp, s + \omega)$ und liegt in der Klasse $\bar{\mathfrak{k}} = \mathfrak{k}_p \mathfrak{k}$. Somit ist:

$$j(\mathfrak{k}) = j\left(\frac{s + \omega}{w}\right), \quad j(\bar{\mathfrak{k}}) = j\left(\frac{s + \omega}{pw}\right),$$

beide sind Wurzeln der Klassengleichung $H_m(t) = 0$ und der Transformationsgleichung $\Phi_p(t, \tau) = 0$, wenn in letzterer $t = j(\bar{\mathfrak{k}})$, $\tau = j(\mathfrak{k})$ gesetzt wird.

73. **Satz:** *Die beiden Gleichungen:*

$$H_m(t) = 0, \qquad \Phi_p(t, j(\mathfrak{k})) = 0,$$

haben wenigstens die eine Wurzel $t = j(\bar{\mathfrak{k}})$ gemein.

Es fragt sich, ob sie noch mehr gemeinsame Wurzeln haben? Nun sind die übrigen Wurzeln von Φ_p:

$$j\left(p\,\frac{\omega + s}{w}\right), \qquad j\left(\frac{\frac{s + \omega}{w} + b}{p}\right), \quad b = 1, 2, \ldots p - 1.$$

Es treten somit dann und nur dann mehr gemeinsame Wurzeln auf, wenn es eine Klasse $\mathfrak{k}_1$ gibt, für die:

$$j(\mathfrak{k}_1) = j\left(p\,\frac{\omega+s}{w}\right) \quad \text{oder} = j\left(\frac{\frac{s+\omega}{w}+b}{p}\right), \quad b = 1, 2, \ldots p-1$$

ist. Es sei $\mathfrak{w}_1 = (w_1,\ s_1+\omega)$ ein Ideal von $\mathfrak{k}_1$, $(s_1+\omega)(s_1+\omega') \equiv 0 \pmod{w_1}$, wo wir $\mathfrak{w}_1$ zu pw teilerfremd voraussetzen dürfen (Satz 56). Dann folgt aus:

$$j(\mathfrak{k}_1) = j\left(\frac{s_1+\omega}{w_1}\right) = j\left(\frac{a\,\frac{s+\omega}{w}+b}{d}\right), \quad ad = p,$$

weil $j(z)$ jeden Wert im D.-B. nur einmal annimmt:

$$\frac{a\,\frac{s+\omega}{w}+b}{d} = S\,\frac{s_1+\omega}{w_1} = \frac{\alpha(s_1+\omega)+\beta w_1}{\gamma(s_1+\omega)+\delta w_1}, \quad \alpha\delta-\beta\gamma = 1,$$

wo S der Modulgruppe angehört. Daraus ergibt sich:

$$\frac{a(s+\omega)+bw}{dw} = \frac{\alpha\omega+(\alpha s_1+\beta w_1)}{\gamma\omega+(\gamma s_1+\delta w_1)},$$

$$(a\omega+as+bw)(\gamma\omega+\gamma s_1+\delta w_1) = dw(\alpha\omega+\alpha s_1+\beta w_1).$$

Wäre $a = p$, $d = 1$, $b = 0$, so müßte, weil p zu w teilerfremd ist,

$$\alpha\omega+(\alpha s_1+\beta w_1) \equiv 0 \pmod{(p)},\ (p) = \mathfrak{p}\mathfrak{p}',$$

sein. Nun ist 1, ω eine Basis der ganzen Zahlen von $k(\sqrt{m})$, also:

$$\alpha \equiv 0 \pmod{p}, \quad \alpha s_1+\beta w_1 \equiv 0 \pmod{p}, \text{ oder:}$$
$$\alpha \equiv \beta \equiv 0 \pmod{p},$$

da auch w_1 zu p teilerfremd ist. Dies ist unmöglich, wegen $\alpha\delta-\beta\gamma = 1$.

Ist $a = 1$, $d = p$, so muß:

$$(\omega+s+bw)(\gamma\omega+\gamma s_1+\delta w_1) \equiv 0 \pmod{(p)},\ (p) = \mathfrak{p}\mathfrak{p}'$$

sein. Keiner der Faktoren kann für sich durch p teilbar sein, da sonst, wie vorhin, $\gamma \equiv \delta \equiv 0 \pmod{p}$ folgte. Nun ist $(p) = \mathfrak{p}\mathfrak{p}'$, wo $\mathfrak{p}$ und $\mathfrak{p}'$ Primideale sind, also ist ein Faktor durch $\mathfrak{p}$, der andere durch $\mathfrak{p}'$ teilbar. Ist: $\omega+s+bw \equiv 0 \pmod{\mathfrak{p}}$, so muß $b = 0$ sein, da $s+\omega$ in $\mathfrak{p}$ liegt. Dies gibt die bekannte gemeinsame Wurzel $j(\bar{\mathfrak{k}}) = j\left(\frac{s+\omega}{pw}\right)$. Ist:

$$\omega+s+bw \equiv 0 \pmod{\mathfrak{p}'},$$

so wird wegen $s+\omega' = s+\omega+\omega'-\omega \equiv 0 \pmod{\mathfrak{p}'}$:

$$2s+\omega+\omega'+bw \equiv 0 \pmod{p}.$$

Dadurch ist $b \pmod{p}$, also zwischen 0 und p eindeutig bestimmt. Die zweite gemeinsame Wurzel ist:

$$j\left(\frac{\omega+s+bw}{pw}\right),$$

da aber $(wp,\ s+bw+\omega) = \mathfrak{w}\mathfrak{p}'$, und die Klasse von $\mathfrak{w}\mathfrak{p}'$ gleich $\mathfrak{f}'_p\mathfrak{f}$ ist, so muß:

$$j\left(\frac{\omega+s+bw}{pw}\right) = j(\mathfrak{f}'_p\mathfrak{f}) \quad \text{sein.}$$

74. Satz: *Die beiden Gleichungen:*

$$H_m(t) = 0, \quad \Phi_p(t, j(\mathfrak{f})) = 0,$$

haben nur die beiden Wurzeln $j(\mathfrak{f}_p\mathfrak{f})$ und $j(\mathfrak{f}'_p\mathfrak{f})$ gemein. Dabei ist p Norm eines Primideales ersten Grades $\mathfrak{p}$, dessen Klasse $\mathfrak{f}_p$ ist.

Wenn $\mathfrak{f}_p = \mathfrak{f}'_p$ ist, so besitzen die beiden Gleichungen nur eine gemeinsame Wurzel. Die Klasse heißt dann *ambig*. Beide Gleichungen haben rationale Zahlkoeffizienten, ihre gemeinsame Wurzel $j(\bar{\mathfrak{f}})$ kann darum rational durch $j(\mathfrak{f})$ mit rationalen Zahlkoeffizienten ausgedrückt werden:

$$j(\bar{\mathfrak{f}}) = R(j(\mathfrak{f})).$$

75. Satz: *Ist $\bar{\mathfrak{f}} = \mathfrak{f}_p\mathfrak{f}$, wo $\mathfrak{f}_p$ eine ambige Klasse ist, so ist $j(\bar{\mathfrak{f}})$ eine ganze, rationale Funktion mit rationalen Zahlkoeffizienten von $j(\mathfrak{f})$.*

Ist dagegen $\mathfrak{f}_p \neq \mathfrak{f}'_p$, $\bar{\mathfrak{f}} \neq \mathfrak{f}$, so haben die beiden Gleichungen einen in t quadratischen Faktor:

$$Q(t, j(\mathfrak{f})) = 0$$

gemeinsam, dessen Koeffizienten rationale Zahlen sind und dessen Wurzeln:

$$j(\bar{\mathfrak{f}}) = j(\mathfrak{f}_p\mathfrak{f}), \quad \text{und} \quad j(\mathfrak{f}'_p\mathfrak{f})$$

werden. Um diese quadratische Gleichung zu zerlegen, nehmen wir die Funktionen:

$$\eta = \frac{a^{12}G(Tz)}{G(z)}, \quad T = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, \quad ad = n,$$

zu Hilfe, und setzen speziell $T = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$, $n = p$, wo p die vorigen Annahmen erfüllt. Nach Satz 43 ist:

$$\eta = R\left(j\left(\frac{z}{p}\right), j(z)\right),$$

und die rationale Funktion R hat nach Satz 44 rationale Zahlkoeffizienten. Setzt man für z sukzessive $\frac{s+\omega}{w}$, $\frac{s+\omega}{pw}$, $\dots$ $\frac{s+\omega}{p^{r-1}w}$ ein, so kommt:

$$\eta^{(1)} = \frac{G\left(\frac{s+\omega}{pw}\right)}{G\left(\frac{s+\omega}{w}\right)} = R\left(j\left(\frac{s+\omega}{pw}\right), j\left(\frac{s+\omega}{w}\right)\right),$$

$$\eta^{(2)} = \frac{G\left(\frac{s+\omega}{p^2w}\right)}{G\left(\frac{s+\omega}{pw}\right)} = R\left(j\left(\frac{s+\omega}{p^2w}\right), j\left(\frac{s+\omega}{pw}\right)\right),$$

$$\dots\dots\dots\dots\dots\dots\dots\dots$$

$$\eta^{(r)} = \frac{G\left(\frac{s+\omega}{p^rw}\right)}{G\left(\frac{s+\omega}{p^{r-1}w}\right)} = R\left(j\left(\frac{s+\omega}{p^rw}\right), j\left(\frac{s+\omega}{p^{r-1}w}\right)\right).$$

Da die Gleichungen (20) gelten, so ist $(p^g w, s+\omega) = \mathfrak{w}\mathfrak{p}^g$, und $\mathfrak{w}\mathfrak{p}^g$ liegt in der Klasse $\mathfrak{f}_p^g\mathfrak{f}$. Dabei ist g irgendeine der Zahlen 1 bis r. Die obigen Gleichungen können daher auch so geschrieben werden:

$$\eta^{(1)} = R(j(\mathfrak{f}_p\mathfrak{f}), j(\mathfrak{f})),$$
$$\eta^{(2)} = R(j(\mathfrak{f}_p^2\mathfrak{f}), j(\mathfrak{f}_p\mathfrak{f})),$$
$$\cdots\cdots\cdots$$
$$\eta^{(r)} = R(j(\mathfrak{f}_p^r\mathfrak{f}), j(\mathfrak{f}_p^{r-1}\mathfrak{f})).$$

Dabei ist wichtig hervorzuheben, daß R von der Wahl von $\mathfrak{f}$ ganz unabhängig ist und nur von $\mathfrak{f}_p$ abhängt. Wir wählen r jetzt so, daß $\mathfrak{f}_p^r$ *die kleinste Potenz von* $\mathfrak{f}_p$ *ist, die zur Hauptklasse wird.* Nun hat die quadratische Gleichung: $Q(t, j(\mathfrak{f}_p^g\mathfrak{f})) = 0$

rationale Zahlkoeffizienten, und die beiden Wurzeln: $j(\mathfrak{f}_p^{g-1}\mathfrak{f})$ und $j(\mathfrak{f}_p^{g+1}\mathfrak{f})$, da $\mathfrak{f}_p\mathfrak{f}_p'$ die Hauptklasse ist; somit ist:

$$j(\mathfrak{f}_p^{g-1}\mathfrak{f}) + j(\mathfrak{f}_p^{g+1}\mathfrak{f}) = r(j(\mathfrak{f}_p^g\mathfrak{f})), \quad g = 1, 2, \ldots r-1, r,$$

wo $r(z)$ eine rationale Funktion mit rationalen Zahlkoeffizienten ist. Somit kann man sukzessive $j(\mathfrak{f}_p^2\mathfrak{f})$ durch $j(\mathfrak{f}_p\mathfrak{f})$ und $j(\mathfrak{f})$ rational und mit rationalen Zahlkoeffizienten, dann $j(\mathfrak{f}_p^3\mathfrak{f})$, schließlich $j(\mathfrak{f}_p^{r-1}\mathfrak{f})$ durch $j(\mathfrak{f}_p\mathfrak{f})$ und $j(\mathfrak{f})$ ausdrücken, wobei zuletzt noch zu bedenken ist, daß wegen der Festsetzung über r $j(\mathfrak{f}_p^r\mathfrak{f}) = j(\mathfrak{f})$ ist. Man darf jetzt die obigen Gleichungen so schreiben:

$$\eta^{(1)} = R^{(1)}(j(\mathfrak{f}_p\mathfrak{f}), j(\mathfrak{f})),$$
$$\eta^{(2)} = R^{(2)}(j(\mathfrak{f}_p\mathfrak{f}), j(\mathfrak{f})),$$
$$\cdots\cdots\cdots$$
$$\eta^{(r)} = R^{(r)}(j(\mathfrak{f}_p\mathfrak{f}), j(\mathfrak{f})),$$

wobei wieder zu beachten ist, daß alle $R^{(g)}$ nicht von $\mathfrak{f}$, sondern nur von $\mathfrak{p}$ respektive $\mathfrak{f}_p$ abhängen. Durch Multiplikation aller Gleichungen entsteht:

$$\eta^{(1)}\eta^{(2)}\ldots\eta^{(r)} = \overline{R}(j(\mathfrak{f}_p\mathfrak{f}), j(\mathfrak{f})).$$

Anderseits ist: $$\eta^{(1)}\eta^{(2)}\ldots\eta^{(r)} = \frac{G\left(\frac{s+\omega}{p^r w}\right)}{G\left(\frac{s+\omega}{w}\right)},$$

also: $$\frac{G\left(\frac{s+\omega}{p^r w}\right)}{G\left(\frac{s+\omega}{w}\right)} = \overline{R}(j(\mathfrak{f}_p\mathfrak{f}), j(\mathfrak{f})).$$

Die linke Seite kann man berechnen. Nach Voraussetzung ist $\mathfrak{w} \sim \mathfrak{w}\mathfrak{p}^r$, d. h. es gibt eine ganze Zahl π, für die $(\pi)\mathfrak{w} = \mathfrak{w}\mathfrak{p}^r$ oder

$(\pi w,\ \pi(s+\omega)) = (w p^r,\ s+\omega)$ ist. Nach Satz 50 gibt es dann ein S von $\mathfrak{G}$, so daß:

$$\left.\begin{aligned} s+\omega &= \pi(\alpha(s+\omega)+\beta w)\\ p^r w &= \pi(\gamma(s+\omega)+\delta w)\end{aligned}\right\},\quad \frac{s+\omega}{p^r w} = S\frac{s+\omega}{w},\quad S=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix},\quad \alpha\delta-\beta\gamma=1.$$

Dabei ist sicherlich $\gamma \neq 0$, da sonst $\alpha=\delta=\pm 1$, und $\frac{s+\omega}{p^r w} = \frac{s+\omega}{w}+\beta$ wäre, was unmöglich ist. Nach der Definition von $G(z)$, S. 40 vor Satz 31 ist: $G(Sz) = (\gamma z+\delta)^{12} G(z)$, also:

$$\frac{G\left(\frac{s+\omega}{p^r w}\right)}{G\left(\frac{s+\omega}{w}\right)} = \frac{G\left(S\frac{s+\omega}{w}\right)}{G\left(\frac{s+\omega}{w}\right)} = \left(\gamma\frac{s+\omega}{w}+\delta\right)^{12} = \left(\frac{p^r}{\pi}\right)^{12}$$

$$\left(\frac{p^r}{\pi}\right)^{12} = \left(\gamma\frac{s+\omega}{w}+\delta\right)^{12} = \bar{R}(j(\mathfrak{t}_p\mathfrak{t}),\ j(\mathfrak{t})).$$

Links steht eine komplexe Zahl $x+y\omega$, $y\neq 0$, da $\frac{p^r}{\pi}$ durch $\mathfrak{p}'$ teilbar ist und es sonst auch durch $\mathfrak{p}+\mathfrak{p}'$ teilbar sein müßte. ω ist somit eine rationale Funktion von $j(\mathfrak{t}_p\mathfrak{t})$ und $j(\mathfrak{t})$ mit rationalen Zahlkoeffizienten, Die quadratische Gleichung $Q(t, j(\mathfrak{t})) = 0$ muß daher nach Adjunktion von ω in zwei lineare Faktoren zerfallen, d. h. es existiert eine nur von $\mathfrak{p}$ und seiner Klasse abhängige Funktion $f_{\mathfrak{t}_p}$ mit rationalen Zahlkoeffizienten, für die:

$$j(\mathfrak{t}_p\mathfrak{t}) = f_{\mathfrak{t}_p}(j(\mathfrak{t}),\ \omega).$$

Entsprechend wird bei Vertauschung von ω mit ω':

$$j(\mathfrak{t}_p\mathfrak{t}) = f_{\mathfrak{t}_p}(j(\mathfrak{t}),\ \omega').$$

Sind $\bar{\mathfrak{t}}$ und $\mathfrak{t}$ zwei beliebige Klassen von $k(\sqrt{m})$, und: $\bar{\mathfrak{t}} = \mathfrak{t}_0\mathfrak{t}$, wo $\mathfrak{t}_0$ nicht die Hauptklasse ist, so wählen wir in $\mathfrak{t}_0$ ein Ideal $\mathfrak{w}_0 = (w_0, s_0+\omega)$, das zu $(\omega'-\omega)^2$ teilerfremd sei. $\mathfrak{w}_0$ ist nur durch Primideale 1. Grades, die von ihren Konjugierten verschieden sind, teilbar:

$$\mathfrak{w}_0 = \mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_n.$$

Die Normen der Primideale $\mathfrak{p}_1, \mathfrak{p}_2, \ldots \mathfrak{p}_n$ seien $p_1, p_2, \ldots p_n$ und ihre Klassen $\mathfrak{t}_{p_1}, \mathfrak{t}_{p_2}, \ldots \mathfrak{t}_{p_n}$. Es ist dann $\mathfrak{t}_0 = \mathfrak{t}_{p_1}\mathfrak{t}_{p_2}\ldots\mathfrak{t}_{p_n}$. Wir nehmen an, keine der Klassen $\mathfrak{t}_p$ sei die Hauptklasse, da wir sonst $\mathfrak{w}_0$ durch das entsprechende $\mathfrak{p}$ teilen könnten, ohne daß es seine Klasse veränderte. Dann ist:

$$\begin{aligned} j(\mathfrak{t}_{p_1}\mathfrak{t}) &= f_{\mathfrak{t}_{p_1}}(j(\mathfrak{t}),\ \omega),\\ j(\mathfrak{t}_{p_1}\mathfrak{t}_{p_2}\mathfrak{t}) &= f_{\mathfrak{t}_{p_2}}(j(\mathfrak{t}_{p_1}\mathfrak{t}),\ \omega),\\ &\cdots\cdots\cdots\\ j(\mathfrak{t}_0\mathfrak{t}) &= f_{\mathfrak{t}_{p_n}}(j(\mathfrak{t}_{p_1}\mathfrak{t}_{p_2}\ldots\mathfrak{t}_{p_{n-1}}\mathfrak{t}),\ \omega),\\ \text{(21)}\quad \text{also:}\quad j(\bar{\mathfrak{t}}) &= j(\mathfrak{t}_0\mathfrak{t}) = f_{\mathfrak{t}_0}(j(\mathfrak{t}),\ \omega),\end{aligned}$$

wo f_{t_0} eine rationale Funktion der Argumente mit rationalen Zahlkoeffizienten ist. Entsprechend ist:

$$j(\mathfrak{f}_0'\mathfrak{f}) = f_{t_0}(j(\mathfrak{f}),\ \omega'). \tag{22}$$

Die Funktion f_{t_0} ist nach dem vorigen unabhängig von der Wahl von $\mathfrak{f}$ und nur von $\mathfrak{f}_0$ abhängig. Sie ist dann und nur dann von ω unabhängig, wenn $\mathfrak{f}_0$ ambig ist.

Jede Wurzel von $H_m(t) = 0$ läßt sich somit rational durch jede andere ausdrücken, falls man als Rationalitätsbereich den Körper $k(\sqrt{m})$ wählt.

76. Satz: *Im Rationalitätsbereich $k(\sqrt{m})$ läßt sich jede Wurzel der Klassengleichung $H_m(t) = 0$ durch jede andere rational ausdrücken.*

Wie steht es mit der Irreduzibilität von $H_m(t)$ in $k(\sqrt{m})$? Nehmen wir an, H_m zerfalle in $k(\sqrt{m})$ in zwei Faktoren:

$$H_m(t) \equiv H_1(t) H_2(t),$$

und sei $j(\mathfrak{f})$ eine Wurzel von H_1, $j(\bar{\mathfrak{f}})$ eine solche von H_2. Wir setzen $\bar{\mathfrak{f}} = \mathfrak{f}_0\mathfrak{f}$, und nehmen wie oben ein Ideal $\mathfrak{w}_0 = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 \ldots \mathfrak{p}_n$ von $\mathfrak{f}_0$, das außer zu $(\omega' - \omega)^2$ auch zur Diskriminante von H_m teilerfremd sei. In der Reihe von singulären Moduln:

$$j(\mathfrak{f}),\ j(\mathfrak{f}_{p_1}\mathfrak{f}),\ j(\mathfrak{f}_{p_1}\mathfrak{f}_{p_2}\mathfrak{f}),\ \ldots\ j(\mathfrak{f}_{p_1}\mathfrak{f}_{p_2}\ldots\mathfrak{f}_{p_{n-1}}\mathfrak{f}),\ j(\bar{\mathfrak{f}}),$$

muß es zwei aufeinanderfolgende geben: $j(\mathfrak{f}_p\mathfrak{f}^*)$ und $j(\mathfrak{f}^*) \neq j(\mathfrak{f}_p\mathfrak{f}^*)$, von denen der eine Wurzel von H_1, der andere Wurzel von H_2 ist:

$$H_1(j(\mathfrak{f}^*)) = 0, \quad H_2(j(\mathfrak{f}_p\mathfrak{f}^*)) = 0.$$

Zwischen beiden besteht nach Satz 73 die Transformationsgleichung:

$$\Phi_p(j(\mathfrak{f}_p\mathfrak{f}^*),\ j(\mathfrak{f}^*)) = 0,$$

oder nach Satz 39:

$$(j(\mathfrak{f}_p\mathfrak{f}^*)^p - j(\mathfrak{f}^*))(j(\mathfrak{f}^*)^p - j(\mathfrak{f}_p\mathfrak{f}^*)) \equiv 0 \pmod{p}.$$

Der Primteiler $\mathfrak{p}$ von p ist vom 1. Grade, somit gilt für jede ganze Zahl α von $k(\sqrt{m})$ nach Satz 61, da $\left(\frac{d}{p}\right) \neq 0$:

$$\alpha^p \equiv \alpha \pmod{p}.$$

Ferner sind alle Binomialkoeffizienten von p zwischen dem 0^{ten} und p^{ten} durch p teilbar, somit ist:

$$H_1(j(\mathfrak{f}_p\mathfrak{f}^*))^p \equiv H_1(j(\mathfrak{f}_p\mathfrak{f}^*)^p) \equiv (j(\mathfrak{f}_p\mathfrak{f}^*)^p - j(\mathfrak{f}^*)) \ldots \pmod{p}$$
$$H_2(j(\mathfrak{f}^*))^p \equiv H_2(j(\mathfrak{f}^*)^p) \equiv (j(\mathfrak{f}^*)^p - j(\mathfrak{f}_p\mathfrak{f}^*)) \ldots \pmod{p}.$$

Aus der vorigen Kongruenz folgt daher:

$$[H_1(j(\mathfrak{f}_p\mathfrak{f}^*))(H_2(j(\mathfrak{f}^*))]^p \equiv 0 \pmod{p}.$$

Dies widerspricht der Annahme, daß $\mathfrak{w}_0$, also auch $\mathfrak{p}$ zur Diskriminante von H_m teilerfremd sei.

77. Satz: *Die Klassengleichung $H_m(t) = 0$ ist in $k(\sqrt{m})$ irreduzibel.*

Wir bezeichnen jetzt die h Klassen von $\mathfrak{k}$ mit $\mathfrak{k}_1, \mathfrak{k}_2, \ldots \mathfrak{k}_h$, und wählen $\mathfrak{k}_1$ als die Hauptklasse. Dann folgt aus (21):

$$j(\mathfrak{k}_n) = f_{\mathfrak{k}_n}(j(\mathfrak{k}_1), \omega), \quad n = 1, 2, \ldots h.$$

Die Operation der Ersetzung von $j(\mathfrak{k}_1)$ durch $j(\mathfrak{k}_n)$ bezeichnen wir mit O_n: $\qquad O_n = (j(\mathfrak{k}_1) : j(\mathfrak{k}_n)), \quad n = 1, 2, \ldots h.$

Die O bilden die Galoissche Gruppe der Klassengleichung in $k(\sqrt{m})$, ihr Einheitselement ist $O_1 = E$. Um die Zusammensetzung der O kennenzulernen, bedenken wir, daß nach (21):

$$O_n j(\mathfrak{k}_{n_1}) = O_n f_{\mathfrak{k}_{n_1}}(j(\mathfrak{k}_1), \omega) = f_{\mathfrak{k}_{n_1}}(j(\mathfrak{k}_n), \omega) = j(\mathfrak{k}_n \mathfrak{k}_{n_1})$$

ist, also $O_n O_{n_1} = O_{n_2}$, falls $\mathfrak{k}_n \mathfrak{k}_{n_1} = \mathfrak{k}_{n_2}$ ist. Die Operationen setzen sich genau zusammen, wie die Klassen, die Gruppe der O ist holoedrisch-isomorph mit der Gruppe der Klassen, und da letztere nach Satz 55 eine Abelsche Gruppe bilden, so ist die Gruppe der Klassengleichung eine Abelsche.

78. Satz: *Die Gruppe der Klassengleichung im Rationalitätsbereich $k(\sqrt{m})$ ist holoedrisch isomorph mit der Gruppe der Klassen, ist also eine Abelsche Gruppe h^{ter} Ordnung.*

Bezeichnen wir die Operation des quadratischen Grundkörpers mit o:

$$o = (\omega : \omega'), \quad o^2 = E,$$

so bilden die $2h$ Operationen, die aus O und o entstehen, die *absolute Galoissche Gruppe*, d. h. die Gruppe im Rationalitätsbereich der rationalen Zahlen. Da $j(\mathfrak{k}_1)$ einer Gleichung h^{ten} Grades mit *rationalen* Koeffizienten genügt, ändert o die Größe $j(\mathfrak{k}_1)$ nicht. Um die Zusammensetzung von O und o kennenzulernen, bedenken wir, daß nach (22):

$$oj(\mathfrak{k}_n) = of_{\mathfrak{k}_n}(j(\mathfrak{k}_1), \omega) = f_{\mathfrak{k}_n}(j(\mathfrak{k}_1), \omega') = j(\mathfrak{k}'_n)$$

ist, wo $\mathfrak{k}'_n$ die konjugierte Klasse von $\mathfrak{k}_n$ ist. Da aber $\mathfrak{k}'_n \mathfrak{k}_n = \mathfrak{k}_1$ die Hauptklasse ist, so entspricht $\mathfrak{k}'_n$ die inverse Operation O_n^{-1}, und die vorige Beziehung sagt aus:

(23) $$o O_n = O_n^{-1} o, \quad n = 1, 2, \ldots h.$$

o und O_n sind nur kommutativ, wenn $\mathfrak{k}_n$ ambig ist.

Wir bilden jetzt aus ω und $j(\mathfrak{k})$ den Oberkörper K. Derselbe ist im Bereiche der rationalen Zahlen *Galoissch vom Grade $2h$*. In bezug auf $k(\sqrt{m})$ ist er *relativ Abelsch vom Relativgrad h*. Er heißt der *Klassenkörper von $k(\sqrt{m})$*.

Hieran schließt sich die Frage, welches der größte in K enthaltene *absolut Abelsche Körper* sei, d. h. derjenige größte Unterkörper von K, der im Rationalitätsbereich der rationalen Zahlen Abelsch ist? Seine Bestimmung ist eine gruppentheoretische Aufgabe. Wir haben diejenige invariante Untergruppe der Galoisschen Gruppe von K zu bestimmen, für die die Faktorgruppe die größte Abelsche Gruppe ist. Diese Untergruppe heißt die *Kommutatorgruppe* $\mathfrak{A}$.[1])

Letztere wird durch die Kommutatoren erzeugt, die wegen (23) die Operationen sind:

$$O_n O_m O_n^{-1} O_m^{-1} = E, \quad O_n o O_n^{-1} o = O_n^2,$$

d. h. $\mathfrak{A}$ wird aus allen Quadraten der O gebildet und besitzt daher die Ordnung $2h : 2 \cdot 2^g$, falls 2^g die Anzahl der ambigen Klassen in $k(\sqrt{m})$ ist. Denn entweder hat O_n einen ungeraden Grad, dann ist O_n^2 durch O_n ausdrückbar, oder es hat einen geraden Grad, dann gibt es Anlaß zu einer ambigen Klasse. Die Abelsche Faktorgruppe hat die Ordnung $2 \cdot 2^g$, und der größte in K enthaltene Abelsche Körper ist ebenfalls vom Grade $2 \cdot 2^g$. Da alle ihre Operationen, weil sie den ambigen Klassen und o entsprechen, vom Grade 2 sind, muß derselbe durch Adjunktion von lauter Quadratwurzeln erhalten werden. Eine derselben ist $\sqrt{m}$ selbst. Es gibt also noch g weitere, durch deren Adjunktion die Klassengleichung zerfallen muß.

79. Satz: *Die Klassengleichung zerfällt bei Adjunktion von g Quadratwurzeln aus rationalen Zahlen in 2^g Faktoren vom $h : 2^{g\text{ten}}$ Grade, wo 2^g die Anzahl der ambigen Klassen in $k(\sqrt{m})$ ist. Bei Adjunktion weiterer absolut Abelscher Körper zerfällt sie nicht weiter.*

5. Die Ringklassenkörper.

13. **Definition:** *Ein Bereich von Zahlen, die aus gegebenen Zahlen nach endlich vielen Schritten durch Addition, Subtraktion und Multiplikation erhalten werden, heißt ein Ring.*

Es sei f eine beliebige positive, ganze, rationale Zahl. Dann gilt, wie man sofort erkennt, der Satz:

80. Satz: *Alle Zahlen von $k(\sqrt{m})$, die* (mod. f) *einer ganzen, rationalen Zahl kongruent sind, bilden einen Ring.*

(f) heißt der *Führer des Ringes*. Wir kürzen den Ring mit $r(f)$ ab.

Eine Zahl ist eine *ganze Ringzahl*, wenn sie ganz ist, und zugleich im Ring liegt. Ist Ω eine solche, so muß also:

$$\Omega = x + y\omega, \quad x + y\omega \equiv z \pmod{f}, \quad x, y, z \text{ ganz, rational}$$

1) Siehe *Speiser* a. a. O. S. 26.

sein, woraus nach Satz 46 $y \equiv 0 \pmod{f}$ folgt. Umgekehrt ist jede Zahl der Form $x + fy\omega$ eine ganze Ringzahl, also ist $1, f\omega$ eine *Basis der ganzen Ringzahlen*.

81. Satz: *Alle ganzen Ringzahlen gehören dem Modul* $\mathfrak{o}_r = [1, f\omega]$ *an.*

Wir werden von nun an an Stelle des Körpers k den Ring $r(f)$ setzen, und alle Begriffe und Entwicklungen der Paragraphen 2, 3, 4 dieses Kapitels auf dieser Grundlage noch einmal aufbauen. Beweise, die genau wie die entsprechenden früheren sind, werden wir dabei übergehen.

14. Definition: *Unter einem Ringideal versteht man die Gesamtheit aller Ringzahlen eines gewöhnlichen Ideals, das zum Führer f teilerfremd ist.*

Es sei $\mathfrak{w} = (w, s + \omega)$ das durch seine kanonische Basis gegebene, zu f teilerfremde Ideal. Jede seiner Zahlen stellt sich dann in der Gestalt dar:

$$\Omega = xw + y(s + \omega), \quad (s + \omega)(s + \omega') \equiv 0 \pmod{w},$$

$$x, y \text{ ganz und rational;}$$

für alle seine Ringzahlen muß nach Satz 81 $y \equiv 0 \pmod{f}$ sein. Da s nur $\pmod{w}$ bestimmt ist, so kann man alle seine Ringzahlen auch so darstellen:

$$\Omega = xw + y(\bar{s} + f\omega), \quad (\bar{s} + f\omega)(\bar{s} + f\omega') \equiv 0 \pmod{w},$$

d. h. $w, \bar{s} + f\omega$ ist eine Basis und zwar die kanonische Basis aller Ringzahlen von $\mathfrak{w}$. Ein Ringideal ist daher wieder ein Modul.

82. Satz: *Jedes Ringideal ist ein zweigliedriger Modul* $\mathfrak{w}_r = (\omega_1, \omega_2)$. ω_1, ω_2 *heißt seine Basis (Imaginärteil von* $\frac{\omega_2}{\omega_1} > 0$*). Dieselbe kann immer in der kanonischen Form* $w, s + f\omega$ *gewählt werden. Ist* $\bar{\omega}_1, \bar{\omega}_2$ *irgendeine andere Basis, so gibt es eine Substitution S der Modulgruppe* $\mathfrak{G}$*, so daß:*

$$\frac{\bar{\omega}_2}{\bar{\omega}_1} = S\,\frac{\omega_2}{\omega_1}.$$

Man sieht daraus, daß jedem Ringideal umkehrbar eindeutig ein zu f teilerfremdes Ideal zugeordnet ist.

83. Satz: *Dem Produkt zweier Ringideale ist das Produkt der ihnen zugeordneten Ideale zugeordnet.*

Daraus folgt, daß die Teilbarkeitsverhältnisse der Ringideale genau dieselben sind, wie die der gewöhnlichen Ideale. Sie sind wiederum eindeutig in Primideale zerlegbar.

15. Definition: *Zwei Ringideale* $\mathfrak{w}$ *und* $\overline{\mathfrak{w}}$ *heißen äquivalent im Ring* $r(f)$*, wenn es zwei ganze, zu f teilerfremde Ringzahlen* ν *und* $\bar{\nu}$ *gibt, so daß:*

$$(\nu)\mathfrak{w} = (\overline{\nu})\overline{\mathfrak{w}}.$$

Alle einem Ideal äquivalenten Ringideale liegen in einer *Ringklasse* $\mathfrak{k}(f)$. Aus der Definition geht sofort hervor, daß die den beiden äquivalenten Ringidealen zugeordneten Ideale äquivalent sein müssen.

Ringideale sind somit nur dann einander äquivalent, wenn es die zugehörigen Ideale sind. Umgekehrt können die zugeordneten Ideale äquivalent sein, ohne daß die Ringideale im Ring einander äquivalent sind. Sind $\mathfrak{w}$ und $\overline{\mathfrak{w}}$ die beiden Ringideale, und gilt für ihre zugeordneten Ideale:

$$(\nu)\mathfrak{w} = (\overline{\nu})\overline{\mathfrak{w}},$$

so kann das Verhältnis $\overline{\nu} : \nu$, da ν und $\overline{\nu}$ zu f teilerfremd sind, (mod. f) noch $\varphi(f)$ verschiedene Reste ergeben. Sind von diesen $\varphi_r(f)$ in $r(f)$, so bleiben $\varphi(f) : \varphi_r(f)$ Reste (mod. f) übrig, so daß jeder Rest (mod. f) einem dieser Reste, multipliziert mit einer zu f teilerfremden, ganzen Ringzahl kongruent ist. Außerdem liegen die Einheiten ± 1 im Ring, dagegen im Falle $m = -1$ oder $= -3$ keine der anderen Einheiten, falls $f \neq 1$. Diese letzteren $\frac{1}{2}e$ Einheiten bestimmen ebenso viele Restklassen (mod. f), so daß jeder der Reste (mod. f) von $\overline{\nu} : \nu$ dem Produkt aus einer Ringzahl, einer der $\frac{1}{2}e$ Einheiten, und von noch einem Repräsentanten der $2\varphi(f) : e\varphi_r(f)$ Restklassen (mod. f) kongruent ist. Somit ist die Anzahl der Ringklassen, in die eine Klasse zerfällt, genau:

$$\frac{2}{e}\frac{\varphi(f)}{\varphi_r(f)}.$$

Denn wir dürfen die linke Seite der obigen Gleichung mit einer beliebigen zu f teilerfremden Ringzahl, und einer beliebigen Einheit multiplizieren, und erhalten rechts im Ring äquivalente Ideale. Ist die Restklasse von $+1$ verschieden, so sind anderseits $\mathfrak{w}$ und $\overline{\mathfrak{w}}$ sicherlich in $r(f)$ nicht äquivalent.

84. Satz: *Ist h die Anzahl der Klassen in $k(\sqrt{m})$, so ist die Anzahl h_r oder $h_r(f)$ der Ringklassen in $r(f)$:*

$$h_r = \frac{2}{e}\prod_{(l)} l^{r-1}\left(l - \left(\frac{d}{l}\right)\right) \cdot h, \quad f = l_1^{r_1} l_2^{r_2} \cdots l_n^{r_n}.$$

Die Ringklassen bilden eine in bezug auf ihre Multiplikation Abelsche Gruppe mit der Ordnung h_r.

Die Klassenanzahl h_r ist somit endlich, sie heißt die *Ringklassenzahl*.

Um den Satz zu beweisen, haben wir für $\varphi(f)$ und $\varphi_r(f)$ nur die Werte zu setzen. Nach Satz 62 ist, falls $f = l_1^{r_1} l_2^{r_2} \cdots l_n^{r_n}$ ist,

$$\varphi(f) = \prod_{(l)} \varphi(l^r).$$

Da nach Satz 52:

$$\varphi(l^r) = l^{2r}\left(1 - \frac{1}{l}\right)\left(1 - \left(\frac{d}{l}\right)\frac{1}{l}\right),$$

ist, wird:

$$\varphi(f) = \prod l^{2r-2}(l-1)\left(l - \left(\frac{d}{l}\right)\right).$$

Ferner ist $\varphi_r(f)$ die Anzahl aller zu f teilerfremden Kongruenzklassen (mod. f), in die die rationalen Zahlen zerfallen, oder:

$$\varphi_r(f) = \prod l^{r-1}(l-1),$$

also wird:

$$\frac{\varphi(f)}{\varphi_r(f)} = \prod l^{r-1}\left(l - \left(\frac{d}{l}\right)\right).$$

Daß die Gruppe Abelsch ist, wird wie früher gezeigt (Satz 55).

Es sei $\mathfrak{w}$ ein Ringideal mit der kanonischen Basis ω_1, ω_2. Dann ist:

$$\frac{\omega_2}{\omega_1} = \frac{s + f\omega}{w}, \quad (s + f\omega)(s + f\omega') \equiv 0 \pmod{w}.$$

Es fragt sich, ob $\omega_2 : \omega_1$ Fixpunkt einer Substitution n^{ter} Ordnung sein kann. Ist letztere $T = \binom{a\ b}{c\ d}$, so besitzt sie die Fixpunkte:

$$z_{1,2} = \frac{a - d \pm \sqrt{D}}{2c}, \quad ad - bc = n, \quad c \neq 0,$$

also muß sicher:

$$D = (a+d)^2 - 4n = u^2 f^2 m, \quad n = n\left(\frac{a + d + uf\sqrt{m}}{2}\right) = n(x + yf\omega),$$

($u \neq 0$, x, y ganz, rational) sein.

85. Satz: *Damit $\omega_2 : \omega_1$, wo ω_1, ω_2 Basis eines Ringideals in $r(f)$ ist, Fixpunkt einer Substitution n^{ter} Ordnung ist, muß notwendig n Norm einer ganzen Ringzahl in $r(f)$ sein.*

Wir nehmen diese Bedingung wieder als für n erfüllt an, und verlangen noch weiter, daß die Darstellung von n eine *eigentliche* sei, d. h. daß $y \neq 0$, und x und y ohne gemeinsamen Teiler seien. Dann folgt wieder:

$$a = x + sy + fy(\omega + \omega'),$$
$$d = x - sy,$$
$$c = wy,$$
$$b = -\frac{n - ad}{c} = -\frac{y}{w}(s + f\omega)(s + f\omega').$$

a, b, c, d sind eindeutig durch x, y bestimmt, ganz und ohne gemeinsamen Teiler.

86. Satz: *Ist $\mathfrak{w} = (\omega_1, \omega_2)$ ein beliebiges Ringideal in $r(f)$, so gibt es zu einer eigentlichen Darstellung von n eine und nur eine Substitution n^{ter} Ordnung T, deren Fixpunkt $\omega_2 : \omega_1$ ist.*

Wie früher ist zu beweisen:

87. Satz: *Ist* $\mathfrak{w} = (\omega_1, \omega_2)$ *ein beliebiges durch seine Basis gegebenes Ringideal von* $r(f)$, *und gibt es genau* v *voneinander verschiedene eigentliche Darstellungen von* n *in* $r(f)$, *so ist* $\omega_2 : \omega_1$ *Fixpunkt von Substitutionen* T, *die genau* $\frac{v}{e_r}$ *voneinander verschiedene Transformationsgruppen* n^{ter} *Ordnung* $\mathfrak{T}_n(T)$ *hervorrufen, wo* e_r *die Anzahl der Einheiten von* $r(f)$ *ist.*

Ist $f > 1$, so ist $e_r = 2$.

88. Satz: *Ist* $\mathfrak{w} = (\omega_1, \omega_2)$ *ein durch seine Basis gegebenes Ringideal von* $r(f)$, *so hängt* $j\left(\frac{\omega_2}{\omega_1}\right)$ *weder von der Wahl der Basis, noch der Wahl des Ideals* $\mathfrak{w}$ *ab, sondern nur von der Ringklasse* $\mathfrak{k}$ *von* $\mathfrak{w}$:

$$j\left(\frac{\omega_2}{\omega_1}\right) = j(\mathfrak{k}).$$

$j(\mathfrak{k})$ *ist eine algebraische Zahl. Sind* $\mathfrak{k}_1, \mathfrak{k}_2, \ldots \mathfrak{k}_{h_r}$ *alle* h_r *Ringklassen von* $r(f)$, *so sind die* h_r *Größen* $j(\mathfrak{k}_1), j(\mathfrak{k}_2), \ldots j(\mathfrak{k}_{h_r})$ *alle voneinander verschieden.*

Wir setzen:
$$H_{f^2 m}(t) \equiv \prod_{i=1}^{h_r} (t - j(\mathfrak{k}_i)),$$

und nennen $H_{f^2 m} = 0$ die *Ringklassengleichung.*

89. Satz: *Die Ringklassengleichung hat rationale Zahlkoeffizienten, sie ist irreduzibel in* $k(\sqrt{m})$, *und ihre Gruppe ist Abelsch und holoedrisch-isomorph mit der Gruppe der Ringklassen in* $r(f)$. $j(\mathfrak{k})$ *sind ganze algebraische Zahlen vom Grade* h_r.

Die Beweise dieser Sätze sind genau den Beweisen der Sätze 64 bis 78 entsprechend.

Aus $j(\mathfrak{k})$, wo $\mathfrak{k}$ jetzt eine Klasse von $r(f)$ ist, bilden wir den Oberkörper $K(f)$ von $k(\sqrt{m})$. Derselbe ist im Bereiche der rationalen Zahlen *Galoissch vom Grade* $2h_r$. In bezug auf $k(\sqrt{m})$ ist er *relativ-Abelsch* vom Relativgrade h_r. $K(f)$ heißt der *Ringklassenkörper.*

IV. Die elliptische Funktion.

1. Die Gruppe der Perioden und ihr Diskontinuitätsbereich.

Sind ω_1 und ω_2 zwei von null verschiedene komplexe Zahlen, für die der Quotient $\omega_2 : \omega_1$ einen *positiven* Imaginärteil besitzt:

$$\text{Imaginärteil } \left(\frac{\omega_2}{\omega_1}\right) > 0\,, \tag{24}$$

so bilden die Punkte ω_1, ω_2 in der Gaußschen Ebene mit dem Anfangspunkt O ein Dreieck. Die über ω_1 und ω_2 gemachten Voraussetzungen lassen sich dann so ins Geometrische übersetzen:

a) Der Flächeninhalt des Dreiecks ist von null verschieden. Denn sonst würden O, ω_1, ω_2 in einer Geraden liegen, $\omega_1 = r_1 e^{i\varphi}$, $\omega_2 = \pm\, r_2 e^{i\varphi}$, $\omega_2 : \omega_1 = \pm\, r_2 : r_1$ reell sein, gegen Annahme (24).

b) Wird das Dreieck im Sinne $O \to \omega_1 \to \omega_2$ durchlaufen, so liegt sein Inneres links (positiver Umlaufssinn). Haben nämlich ω_1 und ω_2 die Polarkoordinaten:

$$\omega_1 = r_1 e^{i\varphi_1}, \quad \omega_2 = r_2 e^{i\varphi_2}, \quad \frac{\omega_2}{\omega_1} = \frac{r_2}{r_1} e^{i(\varphi_2 - \varphi_1)}, \quad -\pi \leqq \begin{matrix}\varphi_1 \\ \varphi_2\end{matrix} < +\pi\,,$$

so muß wegen (24) $0 < \varphi_2 - \varphi_1 < \pi$ oder $-2\pi < \varphi_2 - \varphi_1 < -\pi$ sein, was nur bei positivem Umlaufssinn erfüllt ist.

Ist $z = x + iy$ eine komplexe Variable, so können mit Hilfe von ω_1 und ω_2 die beiden Operationen:

$$s_1 = (z : z + \omega_1), \quad \text{oder} \quad s_1 z = z + \omega_1,$$
$$s_2 = (z : z + \omega_2), \quad \text{oder} \quad s_2 z = z + \omega_2,$$

definiert werden. Sie besitzen die inversen Operationen:

$$s_1^{-1} = (z : z - \omega_1), \quad \text{oder} \quad s_1^{-1} z = z - \omega_1,$$
$$s_2^{-1} = (z : z - \omega_2), \quad \text{oder} \quad s_2^{-1} z = z - \omega_2.$$

Nimmt man noch die Einheitsoperation $e = (z : z)$ hinzu, so kann man mit s_1 und s_2 als Erzeugende eine Gruppe von unendlich vielen Operationen bilden. Da:

$$s_1 s_2 z = z + \omega_1 + \omega_2 = s_2 s_1 z,$$

gilt das kommutative Gesetz. Die Gruppe ist *Abelsch*, und jede ihrer Operationen besitzt die Form $s_1^{h_1} s_2^{h_2}$, oder

$$s_1^{h_1} s_2^{h_2} = s_2^{h_2} s_1^{h_1} = (z : z + h_1\omega_1 + h_2\omega_2), \quad \begin{matrix}h_1 \\ h_2\end{matrix} = 0, \pm 1, \pm 2, \pm 3, \cdots$$

Wir bezeichnen die Gruppe mit $\mathfrak{A}$.

16. Definition: *Zwei Punkte z_1 und z_2 der Ebene heißen ähnlich in bezug auf $\mathfrak{A}$, wenn es zwei ganze, rationale Zahlen h_1 und h_2 gibt, so daß:*

$$z_2 = s_1^{h_1} s_2^{h_2} z_1 = z_1 + h_1\omega_1 + h_2\omega_2 \quad \textit{ist.}$$

Geometrisch erhält man alle zu z ähnlichen Punkte, indem man die Geraden $z, z+\omega_1$ und $z, z+\omega_2$ zeichnet, auf denselben alle Punkte $z+h_1\omega_1$, $z+h_2\omega_2$ markiert, und durch dieselben die Parallelen zur anderen zieht. Die Schnittpunkte sind die gesuchten ähnlichen Punkte.

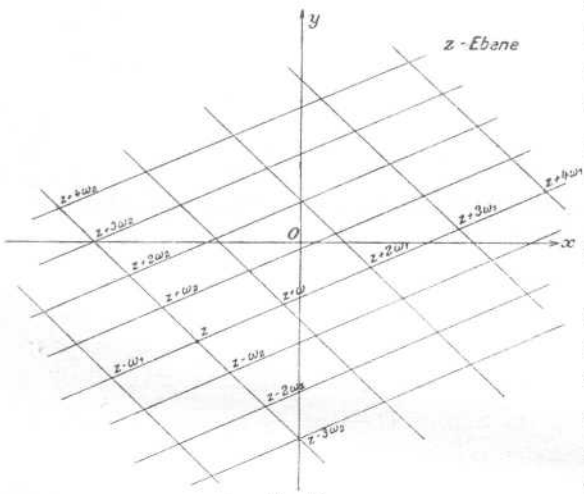

Fig. 13.

Gemäß Definition 2 ergibt sich:

90. Satz: *Jedes Parallelogramm mit den Ecken α, $\alpha+\omega_1, \alpha+\omega_2, \alpha+\omega_1+\omega_2$ ist ein D.-B. von $\mathfrak{A}$, falls von seiner Umgrenzung nur die Seiten α, $\alpha+\omega_1$, und α, $\alpha+\omega_2$, und von seinen Eckpunkten nur α ihm angehören.*

Denn die Punkte des Bereiches sind durch $z = \alpha + x_1\omega_1 + x_2\omega_2$, $0 \leqq x_1, x_2 < 1$ gegeben. Wären zwei Punkte z und $\bar{z}$ des Bereiches einander ähnlich, so müßte:

$$\begin{aligned} z &= \alpha + x_1\omega_1 + x_2\omega_2, \\ \bar{z} &= \alpha + \bar{x}_1\omega_1 + \bar{x}_2\omega_2, \end{aligned} \qquad 0 \leqq \begin{matrix} x_1, x_2 \\ \bar{x}_1, \bar{x}_2 \end{matrix} < 1, \quad \bar{z} = z + h_1\omega_1 + h_2\omega_2$$

sein, wo h_1, h_2 ganze rationale Zahlen sind. Daraus folgt wegen (24):

$$(\bar{x}_1 - x_1)\omega_1 + (\bar{x}_2 - x_2)\omega_2 = h_1\omega_1 + h_2\omega_2, \quad \bar{x}_1 - x_1 = h_1, \quad \bar{x}_2 - x_2 = h_2,$$

was wegen der Festsetzungen über den D.-B. nur die Lösung $h_1 = h_2 = 0$ zuläßt. Ferner ist jeder Punkt z einem Punkt des D.-B. ähnlich. Denn die Parallelen durch z zu den Seiten des D.-B. treffen die Verlängerungen der Seiten $\alpha \to \alpha + \omega_1$ und $\alpha \to \alpha + \omega_2$ in zwei ganz bestimmten Punkten ξ und η und es ist

$$\xi - \alpha = h_1\omega_1 + x_1\omega_1, \quad \eta - \alpha = h_2\omega_2 + x_2\omega_2, \quad 0 \leqq \begin{matrix} x_1 \\ x_2 \end{matrix} < 1,$$

also: $z = \alpha + (\xi - \alpha) + (\eta - \alpha) = \alpha + x_1\omega_1 + x_2\omega_2 + h_1\omega_1 + h_2\omega_2$,

und $\alpha + x_1\omega_1 + x_2\omega_2$ ist ein Punkt des D.-B.

Die Gruppe $\mathfrak{A}$ besitzt Untergruppen von endlichem Index. Nimmt man nur diejenigen Operationen $s_1^{h_1} s_2^{h_2}$, deren h_1 und h_2 der Bedingung unterliegen: $h_1 \equiv 0 \pmod{n_1}$, $h_2 \equiv 0 \pmod{n_2}$,

so erhält man eine Gruppe, deren Erzeugende durch:

$$s_1^{n_1} = (z : z + n_1\omega_1), \quad s_2^{n_2} = (z : z + n_2\omega_2),$$

oder

$$s_1^{n_1} z = z + n_1\omega_1, \quad s_2^{n_2} z = z + n_2\omega_2,$$

gegeben sind. Man hat somit bloß ω_1 und ω_2 durch $n_1\omega_1$ und $n_2\omega_2$ zu ersetzen. Der D.-B. der Untergruppe setzt sich aus $n_1 n_2$ D.-B. der ganzen Gruppe zusammen und $n_1 n_2$ ist ihr Index.

91. Satz: *Die Gruppe der Operationen $s_1^{n_1}$ und $s_2^{n_2}$ ist eine Untergruppe von $\mathfrak{A}$, vom Index $n_1 n_2$.*

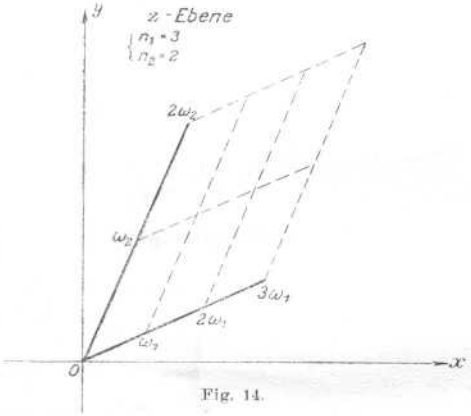

Fig. 14.

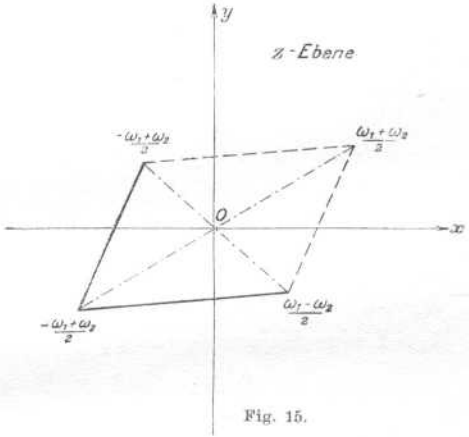

Fig. 15.

ω_1 und ω_2 werden als *Perioden*, $\mathfrak{A}$ als die *Gruppe der Perioden* bezeichnet. Der D.-B. heißt das *Periodenparallelogramm*. Wir werden im allgemeinen als Eckpunkt a des D.-B. die Zahl $-\frac{\omega_1+\omega_2}{2}$ wählen. Die übrigen Eckpunkte sind dann: $\frac{\omega_1-\omega_2}{2}$, $\frac{\omega_1+\omega_2}{2}$, $-\frac{\omega_1-\omega_2}{2}$. Dieser D.-B. ist dadurch ausgezeichnet, daß O sein Mittelpunkt ist.

2. Die elliptische Funktion.

17. Definition: *Eine analytische Funktion $f(z)$ heißt eine elliptische Funktion, wenn sie*

a) bei jeder Operation von $\mathfrak{A}$ ungeändert bleibt (doppeltperiodisch ist), und wenn sie

b) meromorph ist, d. h. im Endlichen keine wesentlichen Singularitäten, sondern höchstens Pole besitzt.

Um analytisch elliptische Funktionen zu konstruieren, geht man genau wie bei den Modulfunktionen vor. Wir setzen:

$$P_k(z) = \sum_{(\Omega)} \frac{1}{(z-\Omega)^k}, \qquad \Omega = h_1\omega_1 + h_2\omega_2,$$

wo die Summe über alle Ω, d. h. über alle Kombinationen h_1, h_2 der ganzen Zahlen zwischen $-\infty$ und $+\infty$ zu erstrecken ist.

92. Satz: *$P_k(z)$ konvergiert in jedem endlichen Bereich von z, der keinen Punkt Ω enthält, absolut und gleichmäßig, falls $k > 2$ ist.*

Da der Bereich endlich ist, so ist $|z|$ unter einer endlichen Grenze m: $|z| < m$. Außerdem kann man in P_k endlich viele Summanden weglassen. Wir nehmen daher die Summe nur noch über diejenigen Ω, für für die $|\Omega| > 2m$. Dann ist:

$$\left|\frac{z}{\Omega}\right| < \frac{1}{2}, \quad 1 - \frac{z}{\Omega}\Big| \geqq 1 - \left|\frac{z}{\Omega}\right| > \frac{1}{2}, \quad \frac{1}{\left|\frac{z}{\Omega} - 1\right|} < 2, \quad \frac{1}{|z - \Omega|} < \frac{2}{|\Omega|};$$

somit:
$$\sum_{(|\Omega|>2m)} \frac{1}{|z-\Omega|^k} < 2^k \sum_{(|\Omega|>2m)} \frac{1}{|\Omega|^k}.$$

Nach Satz 5 konvergiert:
$$\frac{1}{\omega_1^{2k_1}} G_{k_1}\left(\frac{\omega_2}{\omega_1}\right) = \sum_{n,\, m=-\infty}^{+\infty}{}' \frac{1}{(m\omega_1 + n\omega_2)^{2k_1}}$$

absolut, wenn $\omega_2 : \omega_1$ einen *positiven* Imaginärteil hat, was wegen (24) der Fall ist, und wenn $k_1 > 1$ ist. Setzt man $k_1 = \frac{1}{2}k$, so ist für alle $k > 2$ eine Majorante für P_k gefunden und der Satz bewiesen.

Aus Satz 92 folgt, daß $P_3(z) = \sum_{(\Omega)} \frac{1}{(z-\Omega)^3}$

eine elliptische Funktion ist. Denn $P_3(z)$ ist doppeltperiodisch, da P_3 wegen der absoluten Konvergenz unabhängig von der Reihenfolge seiner Summanden ist, und Ω mit $\Omega - \omega_1$ oder $\Omega - \omega_2$ gleichzeitig alle Perioden durchläuft. Ferner besitzt P_3 nur die singulären Punkte Ω im Endlichen, und dort hat $P_3(z)$ Pole 3. Ordnung.

Die Funktion $P_3(z) - \frac{1}{z^3}$ ist im Periodenparallelogramm der Figur 15 regulär. Liegt somit z in demselben, und nimmt man den Weg des Integrales

$$\int_0^z \left(-P_3(\zeta) + \frac{1}{\zeta^3}\right) d\zeta$$

ganz im Innern desselben an, so ist der Wert des Integrales vom Wege unabhängig. Anderseits darf man wegen der gleichmäßigen Konvergenz gliedweise integrieren. Bedeutet der Strich an $\sum$, daß $\Omega = 0$ bei der Summation auszulassen ist, so ergibt sich:

$$\int_0^z \left(-P_3(\zeta) + \frac{1}{\zeta^3}\right) d\zeta = -\int_0^z \sum_{(\Omega)}{}' \frac{1}{(\zeta-\Omega)^3}\, d\zeta = -\sum_{(\Omega)}{}' \int_0^z \frac{d\zeta}{(\zeta-\Omega)^3}$$
$$= \frac{1}{2} \sum_{(\Omega)}{}' \left(\frac{1}{(z-\Omega)^2} - \frac{1}{\Omega^2}\right).$$

Somit konvergiert auch die Reihe rechts in jedem endlichen Bereich, der keinen Punkt Ω enthält, gleichmäßig und stellt eine analytische Funktion dar. Setzt man nach Weierstraß:

$$\wp(z\,;\,\omega_1,\,\omega_2) = \frac{1}{z^2} + \sum_{(\Omega)}{}' \left(\frac{1}{(z-\Omega)^2} - \frac{1}{\Omega^2}\right), \tag{25}$$

so gilt der Satz:

93. Satz: *$\wp(z)$ ist eine elliptische Funktion mit den Perioden ω_1 und ω_2.*

Nach Definition besitzt $\wp(z)$ den Differentialquotienten:

$$\wp'(z;\,\omega_1,\,\omega_2) = -2\left(\frac{1}{z^3} + \sum_{(\Omega)}{}' \frac{1}{(z-\Omega)^3}\right) = -2\sum_{(\Omega)} \frac{1}{(z-\Omega)^3},$$

der nach obigem überall regulär ist, mit Ausnahme der Punkte Ω, wo er Pole 3. Ordnung besitzt. Nun ist:

$$\wp'(z+\omega_1) = \wp'(z), \qquad \wp'(z+\omega_2) = \wp'(z),$$

woraus durch Integration:

$$\wp(z+\omega_1) = \wp(z) + c_1, \qquad \wp(z+\omega_2) = \wp(z) + c_2.$$

c_1 und c_2 sind Integrationskonstanten. Zu ihrer Bestimmung setzen wir $z = -\frac{1}{2}\omega_1$ und $z = -\frac{1}{2}\omega_2$, wodurch

$$\wp\left(\frac{\omega_1}{2}\right) = \wp\left(-\frac{\omega_1}{2}\right) + c_1, \qquad \wp\left(\frac{\omega_2}{2}\right) = \wp\left(-\frac{\omega_2}{2}\right) + c_2$$

wird. $\wp(z)$ ist eine *gerade* Funktion von z, daher folgt $c_1 = c_2 = 0$. $\wp(z)$ besitzt somit die Perioden ω_1 und ω_2. Daß $\wp(z)$ gerade ist, ersieht man aus:

$$\wp(-z) = \frac{1}{z^2} + \sum_{(\Omega)}{}' \left(\frac{1}{(z+\Omega)^2} - \frac{1}{\Omega^2}\right) = \frac{1}{z^2} + \sum_{(\Omega)}{}' \left(\frac{1}{(z-\Omega)^2} - \frac{1}{\Omega^2}\right),$$

weil Ω und $-\Omega$ gleichzeitig alle Perioden durchlaufen.

94. Satz: *$\wp(z)$ ist eine gerade elliptische Funktion. Sie ist überall im Endlichen regulär mit Ausnahme der Punkte Ω, wo sie Pole 2. Ordnung besitzt.*

Eine weitere Eigenschaft ergibt sich direkt aus der Definition:

95. Satz: *$\wp(z;\,\omega_1,\,\omega_2)$ ist eine homogene Funktion -2. Dimension der drei Größen z, ω_1, ω_2:*

$$\wp(tz;\,t\omega_1,\,t\omega_2) = t^{-2}\wp(z;\,\omega_1,\,\omega_2).$$

Wenden wir auf die Perioden ω_1 und ω_2 eine Substitution S der Modulgruppe $\mathfrak{G}$ an:

$$S = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}, \quad \alpha\delta - \beta\gamma = 1, \quad \begin{cases}\omega_2 = \alpha\omega_2 + \beta\omega_1\\ \omega_1 = \gamma\omega_2 + \delta\omega_1\end{cases},$$

so wird:

$$S_\wp(z;\omega_1,\omega_2)=\wp(z;\omega_1,\omega_2)=\frac{1}{z^2}+\sum_{(\Omega)}{}'\left(\frac{1}{(z-\Omega)^2}-\frac{1}{\Omega^2}\right),$$

wo $\bar\Omega=h_1\bar\omega_1+h_2\bar\omega_2=(\bar h_1\delta+h_2\beta)\omega_1+(h_1\gamma+h_2\alpha)\omega_2$ ist. Da $\bar h_1$, h_2, $\alpha,\beta,\gamma,\delta$ ganze Zahlen sind, und die h nicht beide null sind, sind alle $\bar\Omega$ unter den Ω zu finden. Umgekehrt entspricht jedem Ω ein $\bar\Omega$, denn aus $\Omega=h_1\omega_1+h_2\omega_2$ folgt:

$$h_1=\bar h_1\delta+h_2\beta,\quad h_2=h_1\gamma+h_2\alpha,$$

oder wegen $\alpha\delta-\beta\gamma=1$:

$$\bar h_1=\alpha h_1-\beta h_2,\quad h_2=-\gamma h_1+\delta h_2.$$

Da sich somit die Ω und $\bar\Omega$ umkehrbar eindeutig entsprechen, so muß:

$$S_\wp(z;\omega_1,\omega_2)=\wp(z;\omega_1,\bar\omega_2)=\wp(z;\omega_1,\omega_2)\quad\text{sein.}$$

96. Satz: *Die elliptische Funktion $\wp(z)$ ändert sich nicht, wenn auf ihre Perioden eine Substitution der Modulgruppe ausgeübt wird.*

Wir können $\wp(z)$ in eine Potenzreihe nach geraden Potenzen von z um 0 entwickeln. Ihr Konvergenzkreis geht durch den 0 am nächsten liegenden Punkt Ω:

$$\wp(z)=\frac{1}{z^2}+c_0+c_1z^2+c_2z^4+\cdots.$$

Läßt man $\frac{1}{z^2}$ weg, so folgt aus:

$$\sum{}'\left(\frac{1}{(z-\Omega)^2}-\frac{1}{\Omega^2}\right)=c_0+c_1z^2+c_2z^4+\cdots$$

für $z=0$, daß $c_0=0$ ist; ferner nach (11), S. 31:

$$c_1=3\sum_{(\Omega)}{}'\frac{1}{\Omega^4}=\frac{g_2(\omega_1,\omega_2)}{20};\qquad c_2=5\sum_{(\Omega)}{}'\frac{1}{\Omega^6}=\frac{g_3(\omega_1,\omega_2)}{28};$$

$$c_n=(2n+1)\sum_{(\Omega)}{}'\frac{1}{\Omega^{2n+2}},\quad\text{also:}$$

$$\wp(z;\omega_1,\omega_2)=\frac{1}{z^2}+\frac{g_2}{20}z^2+\frac{g_3}{28}z^4+\cdots \tag{26}$$

3. Funktionentheoretische Sätze über elliptische Funktionen.

Es sei $f(z)$ eine elliptische Funktion mit den Perioden ω_1 und ω_2. Besitzt $f(z)$ um $z=\xi$ die Taylorentwicklung:

$$f(z)=c+c_r(z-\xi)^r+\cdots,\quad c_r\neq0,$$

oder um $z=\xi$ die Entwicklung:

$$f(z)=\frac{c_{-r}}{(z-\xi)^r}+\frac{c_{-r+1}}{(z-\xi)^{r-1}}+\cdots,\quad c_{-r}\neq0,$$

so sagt man, $f(z)$ nehme den Wert c, bzw. ∞ an der Stelle $z=\xi$ $r$mal an.

97. Satz: *$f(z)$ nimmt im Periodenparallelogramm jeden Wert gleich oft an.*

Dieser Satz folgt sofort aus dem *Residuensatz* der Funktionentheorie. Besitzt die analytische Funktion $F(z)$ im Periodenparallelogramm P nur Pole, so ist:

$$\frac{1}{2\pi i}\int_{(P)} F(z)\,dz = \sum c_{-1}, \tag{27}$$

wo die Summe über die Residuen aller Pole in P zu erstrecken ist.

Die Zahl, die angibt, wie oft $f(z)$ einen Wert c annimmt, ist jedenfalls endlich, da $f(z)$ sonst konstant oder in P eine wesentliche Singularität hätte. Wir verschieben P parallel so, daß auf seiner Umrandung weder ein Pol, noch eine Stelle liegt, an der sie den Wert c annimmt. Im Innern des so erhaltenen P nehme $f(z)$ den Wert c nur an den Stellen $z = \nu_1, \nu_2, \dots \nu_r$ von der Ordnung $n_1, n_2, \dots n_r$ und den Wert ∞ nur für $z = \mu_1, \mu_2, \dots \mu_s$ von der Ordnung $m_1, m_2, \dots m_s$ an. Nun ist

$$F(z) = \frac{f'(z)}{f(z) - c}$$

wieder eine elliptische Funktion mit den Perioden ω_1 und ω_2, und besitzt um $z = \nu$ die Entwicklung:

$$\frac{f'(z)}{f(z) - c} = \frac{n}{z - \nu} + \cdots,$$

und um $z = \mu$:

$$\frac{f'(z)}{f(z) - c} = \frac{-m}{z - \mu} + \cdots.$$

Nach (27) ist daher, falls die Umgrenzung von P positiv durchlaufen wird:

$$\frac{1}{2\pi i}\int_{(P)} \frac{f'(z)\,dz}{f(z) - c} = \sum_{i=1}^{r} n_i - \sum_{i=1}^{s} m_i.$$

Anderseits kann das Integral links direkt berechnet werden:

$$\frac{1}{2\pi i}\int_{(P)} \frac{f'(z)\,dz}{f(z) - c} = \frac{1}{2\pi i}\int_{\alpha}^{\alpha+\omega_1} + \frac{1}{2\pi i}\int_{\alpha+\omega_1}^{\alpha+\omega_1+\omega_2} + \frac{1}{2\pi i}\int_{\alpha+\omega_1+\omega_2}^{\alpha+\omega_2} + \frac{1}{2\pi i}\int_{\alpha+\omega_2}^{\alpha} = 0,$$

denn das 1. und 3., entsprechend das 2. und 4. Integral rechts sind wegen der Periodizität von $F(z)$ entgegengesetzt gleich. Somit wird:

$$\sum n - \sum m = 0, \quad \sum n = \sum m.$$

$\sum n$ ist die Zahl, die angibt, wie oft $f(z)$ in P den Wert c annimmt, $\sum m$ ist die Zahl, die angibt, wie oft $f(z)$ in P den Wert ∞ annimmt, daher wird $f(z)$ ebensooft c, wie unendlich.

Man nennt die Anzahl $\sum n = \sum m$ die *Ordnung der elliptischen Funktion.*

98. Satz: *Eine elliptische Funktion 0. Ordnung ist eine Konstante. Eine elliptische Funktion 1. Ordnung existiert nicht.*

Der erste Teil des Satzes folgt direkt aus Satz 97. Wäre $f(z)$ eine elliptische Funktion 1. Ordnung, so hätte sie einen Pol erster Ordnung in P für $z = \mu$:

$$f(z) = \frac{c_{-1}}{z - \mu} + \cdots, \quad c_{-1} \neq 0,$$

also nach (27), falls P so gewählt ist, daß μ im Innern liegt:

$$\frac{1}{2\pi i}\int_{(P)} f(z)\,dz = c_{-1}.$$

Anderseits findet man durch direkte Ausrechnung wie oben:

$$\frac{1}{2\pi i}\int_{(P)} f(z)\,dz = 0,$$

somit ist $c_{-1} = 0$, gegen die Annahme. Aus (25) folgt jetzt:

99. Satz: *$\wp(z)$ ist eine elliptische Funktion 2. Ordnung, $\wp'(z)$ eine solche 3. Ordnung.*

$\wp(z)$ hat daher die kleinste mögliche Ordnung. Wir legen jetzt wieder das Periodenparallelogramm von Figur 15 zugrunde und bezeichnen es mit P. Da $\wp(z)$ eine gerade Funktion ist, so nimmt sie für die beiden Punkte $+z$ und $-z$ in P denselben Wert an. Nach den Sätzen 97 und 99 folgt daher:

100. Satz: *Sind z_1 und z_2 zwei von einander verschiedene innere Punkte von P, für die $\wp(z_1) = \wp(z_2)$, so muß $z_2 = -z_1$ sein.*

Da $\wp'(z)$ die Perioden ω_1, ω_2 besitzt, so ist:

$$\wp'\left(-\frac{\omega_1}{2}\right) = \wp'\left(-\frac{\omega_1}{2} + \omega_1\right) = \wp'\left(\frac{\omega_1}{2}\right); \quad \wp'\left(-\frac{\omega_2}{2}\right) = \wp'\left(\frac{\omega_2}{2}\right);$$

$$\wp'\left(-\frac{\omega_1 + \omega_2}{2}\right) = \wp'\left(\frac{\omega_1 + \omega_2}{2}\right).$$

Anderseits ist $\wp'(z)$ als Differentialquotient einer geraden Funktion eine ungerade Funktion, somit:

$$\wp'\left(-\frac{\omega_1}{2}\right) = -\wp'\left(\frac{\omega_1}{2}\right); \; \wp'\left(-\frac{\omega_2}{2}\right) = -\wp'\left(\frac{\omega_2}{2}\right); \; \wp'\left(-\frac{\omega_1 + \omega_2}{2}\right) = -\wp'\left(\frac{\omega_1 + \omega_2}{2}\right).$$

Beide Resultate lassen sich, da $\wp'(z)$ nur für $z = 0$ unendlich wird, nur vereinigen, wenn:

$$\wp'\left(\frac{\omega_1}{2}\right) = \wp'\left(\frac{\omega_2}{2}\right) = \wp'\left(\frac{\omega_1 + \omega_2}{2}\right) = 0$$

ist. $\wp'(z)$ nimmt jeden Wert in P dreimal an, also kann es in P nirgends sonst null werden. Die Nullstellen sind von 1. Ordnung.

101. Satz: *$\wp'(z)$ wird in P nur an den drei Punkten $-\frac{\omega_1}{2}$, $-\frac{\omega_1+\omega_2}{2}$, $-\frac{\omega_2}{2}$, und zwar von 1. Ordnung null.*

$\wp(z)$ nimmt daher die drei Werte:

$$\wp\left(\frac{\omega_1}{2}\right)=e_1,\quad \wp\left(\frac{\omega_2}{2}\right)=e_2,\quad \wp\left(\frac{\omega_1+\omega_2}{2}\right)=e_3, \tag{28}$$

und nur diese von 2. Ordnung an, abgesehen von dem Werte ∞, der für $z=0$ ebenfalls von 2. Ordnung angenommen wird.

102. Satz: *$\wp(z)$ nimmt für jedes z seinen Wert von 1. Ordnung an, mit Ausnahme der Punkte 0, $-\frac{\omega_1}{2}$, $-\frac{\omega_2}{2}$, $-\frac{\omega_1+\omega_2}{2}$, an denen es die Werte ∞, e_1, e_2, e_3 von 2. Ordnung annimmt.*

Die Zahlen e_1, e_2, e_3 sind *voneinander verschieden*, da $\wp(z)$ sonst einen Wert viermal annehmen würde.

Bilden wir: $f(z)=\dfrac{\wp'(z)^2}{(\wp(z)-e_1)(\wp(z)-e_2)(\wp(z)-e_3)}$,

so ist $f(z)$ sicher eine elliptische Funktion. Sie ist in P überall endlich, da Zähler und Nenner beide für $z=0$ von 6. Ordnung unendlich, und für $z=-\frac{\omega_1}{2}$, $-\frac{\omega_1+\omega_2}{2}$, $-\frac{\omega_2}{2}$ von 2. Ordnung null werden. Nach Satz 98 ist daher $f(z)$ eine Konstante. Zur Berechnung setzt man für $\wp(z)$ und $\wp'(z)$ die Reihenentwicklung (26) ein:

$$\wp(z)=\frac{1}{z^2}+z^2\mathfrak{P}(z),\quad \wp'(z)=-\frac{2}{z^3}+(z^2\mathfrak{P}(z))',$$

$$f(z)=\frac{4-4z^3(z^2\mathfrak{P}(z))'+z^6(z^2\mathfrak{P}(z))'^2}{(1-e_1z^2+z^4\mathfrak{P}(z))(1-e_2z^2+z^4\mathfrak{P}(z))(1-e_3z^2+z^4\mathfrak{P}(z))}.$$

Somit $f(0)=4$, und:

$$\wp'(z)^2=4(\wp(z)-e_1)(\wp(z)-e_2)(\wp(z)-e_3). \tag{29}$$

Es sei t eine zweite komplexe Variable, und:

$$f(z,t)=\frac{\wp'(z)-\wp'(t)}{\wp(z)-\wp(t)}.$$

t sei $\neq 0$. $f(z,t)$ ist als Funktion von z elliptisch mit den Perioden ω_1, ω_2. Pole kann sie nur für $z=0$ und $z=\pm t$ besitzen. Für $z=0$ ist:

$$f(z,t)=\frac{2-z^3\wp'(t)+\cdots}{z(1-z^2\wp(t)+\cdots)}=-\frac{2}{z}+\cdots,$$

sie hat also einen Pol 1. Ordnung. Für $z=+t$ ist:

$$\lim_{z=t} f(z,t)=\frac{\wp''(t)}{\wp'(t)}$$

endlich, falls $t\neq -\frac{\omega_1}{2}$, $-\frac{\omega_1+\omega_2}{2}$, $-\frac{\omega_2}{2}$; und für $z=-t$ ist:

$$\lim_{z=-t}(z+t)f(z,t)=\lim_{z=-t}\frac{\wp'(z)-\wp'(t)+(z+t)\wp''(z)}{\wp'(z)}=2.$$

$f(z, t)$ ist somit eine elliptische Funktion 2. Ordnung mit den beiden einfachen Polen $z = 0$ und $z = -t$. $f^2(z, t)$ besitzt um $z = 0$, $+t$, $-t$ die Reihenentwicklungen:

$$f^2(z, t) = \frac{4}{z^2} + 8\wp(t) + 4\wp'(t)\,z + \cdots$$

$$= \frac{\wp''(t)^2}{\wp'(t)^2} + \cdots$$

$$= \frac{4}{(z+t)^2} + \cdots$$

und $\frac{1}{4} f^2(z, t) - \wp(z + t) - \wp(z) - \wp(t)$ ist wegen (27) eine überall in P reguläre Funktion von z, also von z unabhängig. Wegen der Symmetrie in z und t ist der Ausdruck aber auch von t unabhängig, somit eine absolute Konstante. Um diese zu berechnen, entwickelt man den Ausdruck um $z = 0$. $\frac{1}{z^2}$ hebt sich, und das von z freie Glied ebenfalls, die Konstante ist daher null, und:

$$(30) \qquad \frac{1}{4} f^2(z, t) = \frac{1}{4}\left(\frac{\wp'(z) - \wp'(t)}{\wp(z) - \wp(t)}\right)^2 = \wp(z + t) + \wp(z) + \wp(t).$$

Diese Formel heißt das *Additionstheorem der elliptischen Funktion* $\wp(z)$.

Setzt man $z = -\frac{\omega_1}{2}$, $t = -\frac{\omega_1 + \omega_2}{2}$, so wird wegen:

$$\wp'\left(-\frac{\omega_1}{2}\right) = \wp'\left(-\frac{\omega_1 + \omega_2}{2}\right) = 0, \qquad \wp\left(-\frac{\omega_1}{2} - \frac{\omega_1 + \omega_2}{2}\right) = \wp\left(-\frac{\omega_2}{2}\right) = e_2:$$

$$(31) \qquad e_1 + e_2 + e_3 = 0.$$

Daraus folgt, daß wir (29) so schreiben können:

$$\wp'(z)^2 = 4\wp(z)^3 + a\wp(z) - b, \quad \text{wo:} \begin{cases} a = 4(e_1e_2 + e_1e_3 + e_2e_3) \\ b = 4e_1e_2e_3 \end{cases} \text{ ist.}$$

Setzt man hier (26) ein:

$$\wp(z) = \frac{1}{z^2} + \frac{g_2}{20}z^2 + \frac{g_3}{28}z^4 + \cdots, \quad \wp'(z) = -\frac{2}{z^3} + \frac{2g_2}{20}z + \frac{4g_3}{28}z^3 + \cdots,$$

so ergibt die Koeffizientenvergleichung:

$$-\frac{8g_2}{20} = 4\,\frac{3g_2}{20} + a, \quad -\frac{16g_3}{28} = \frac{4 \cdot 3g_3}{28} - b, \quad \text{d. h. } a = -g_2, \quad b = g_3.$$

(29) schreibt sich jetzt so:

$$(32) \qquad \wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3,$$

woraus sich ergibt:

$$(33) \qquad \wp''(z) = 6\wp(z)^2 - \tfrac{1}{2}g_2.$$

(32) und (33) erlauben, alle Koeffizienten der Reihenentwicklung von $\wp(z)$ durch g_2 und g_3 auszudrücken. Setzt man in (33) die Reihenentwicklung:

$$\wp(z) = \frac{1}{z^2} + c_1 z^2 + c_2 z^4 + c_3 z^6 + \cdots,$$

$$c_1 = \frac{g_2}{20}, \quad c_2 = \frac{g_3}{28}, \quad c_n = (2n+1) \sum{}' \frac{1}{\Omega^{2n+2}}$$

ein, so folgen die Rekursionsformeln:

$$2k(2k-1)c_k = 6 \cdot 2c_k + 6 \sum_{h+l=k-1} c_h c_l,$$

oder: $$(2k+3)(k-2)c_k = 3 \sum_{h+l=k-1} c_h c_l, \quad k = 3, 4, \ldots.$$

Da c_1 und c_2 bekannt sind, folgt:

103. Satz: *Alle Koeffizienten:*

$$c_k = (2k+1) \sum{}' \frac{1}{\Omega^{2k+2}}$$

sind ganze rationale Funktionen von g_2 und g_3 mit positiven, rationalen Zahlkoeffizienten.

Nach Definition ist c_k eine homogene Funktion $-(2k+2)$. Dimension von ω_1 und ω_2. Satz 103 läßt c_k darum so darstellen:

$$c_k = \sum_{(n,m)} a_{n,m} g_2^n g_3^m, \qquad 2n + 3m = k + 1, \tag{34}$$

summiert über alle n, m, die positiv sind und der Bedingung

$$4n + 6m = 2(k+1) \quad \text{oder} \quad 2n + 3m = k + 1$$

genügen. Denn g_2 ist homogen von $-4.$, g_3 von $-6.$ Dimension. Die $a_{n,m}$ sind *rationale* Zahlen.

Aus $\wp(z)$ und $\wp'(z)$ bilden wir den *Funktionskörper* (vgl. den 11. Satz, S. 29).

104. Satz: *Jede elliptische Funktion mit den Perioden ω_1 und ω_2 gehört dem Funktionskörper von $\wp(z)$ und $\wp'(z)$ an.*

Aus dem Additionstheorem folgt, daß $\wp(z+t), \wp'(z+t), \wp''(z+t), \ldots$ dem Funktionskörper von $\wp(z)$ und $\wp'(z)$ angehören für einen beliebigen Zahlwert t (siehe Formel (30) und (33)). Ferner ist:

$$\wp^{(n)}(z+t) = (-1)^n \frac{(n+1)!}{(z+t)^{n+2}} + \mathfrak{P}(z+t),$$

wo $\mathfrak{P}$ eine reguläre Potenzreihe in $z = -t$ ist.

Es sei $z = \mu$ ein in P liegender Pol r^{ter} Ordnung der gegebenen elliptischen Funktion $f(z)$:

$$f(z) = \frac{c_{-r}}{(z-\mu)^r} + \cdots + \frac{c_{-1}}{(z-\mu)} + c_0 + c_1(z-\mu) + \cdots, \quad c_{-r} \neq 0.$$

Man setze:

$$\mu \neq 0\colon\ \varphi_\mu(z) \equiv \frac{(-1)^r c_{-r}}{(r-1)!}\wp^{(r-2)}(z-\mu) + \frac{(-1)^{r-1}c_{-r+1}}{(r-2)!}\wp^{(r-3)}(z-\mu) + \cdots + c_{-2}\wp(z-\mu) + \frac{c_{-1}}{2}\frac{\wp'(z)+\wp'(\mu)}{\wp(z)-\wp(\mu)};$$

$$\mu = 0\colon\ \varphi_0(z) \equiv \frac{(-1)^r c_{-r}}{(r-1)!}\wp^{(r-2)}(z) + \frac{(-1)^{r-1}c_{-r+1}}{(r-2)!}\wp^{(r-3)}(z) + \cdots + c_{-2}\wp(z).$$

Dann besitzt φ_μ für $z = \mu$ genau dieselben negativen Potenzen mit denselben Koeffizienten, wie $f(z)$ und

$$f(z) - \sum_{(\mu)} \varphi_\mu(z),$$

wo die Summe über alle Pole μ von $f(z)$ in P zu erstrecken ist, überhaupt keine Pole mehr. Sie ist aber eine elliptische Funktion, also nach Satz 98 eine Konstante:

$$f(z) = \sum_{(\mu)} \varphi_\mu(z) + \text{constans}.$$

Denn nur:
$$\frac{c_{-1}}{2}\frac{\wp'(z)+\wp'(\mu)}{\wp(z)-\wp(\mu)}$$
könnte für $z = 0$ einen Pol 1. Ordnung hinzubringen. Diese Funktion fällt aber, falls kein $\mu = 0$ ist, fort, da nach (27):

$$\frac{1}{2\pi i}\int_{(P)} f(z)\,dz = \sum_{(\mu)} c_{-1} = 0$$

ist. Ist ein $\mu = 0$, so erzeugt die Funktion an der Stelle $z = 0$ das vorgeschriebene Glied des Residuums. Nach dem Obigen läßt sich $\varphi_\mu(z)$ rational durch $\wp(z)$ und $\wp'(z)$ ausdrücken, womit der Satz bewiesen ist.

Nach (32) läßt sich $\wp'(z)^2$ rational durch $\wp(z)$ ausdrücken, somit kann man schreiben:

$$f(z) = R_1(\wp(z)) + \wp'(z)\,R_2(\wp(z)),$$

wo R_1 und R_2 rationale Funktionen von $\wp(z)$ allein sind. Ist $f(z)$ eine *gerade* elliptische Funktion, so muß:

$$R_1(\wp(z)) - \wp'(z)R_2(\wp(z)) \equiv R_1(\wp(z)) + \wp'(z)R_2(\wp(z)),$$

oder
$$R_2(\wp(z)) \equiv 0,$$

sein. Für eine ungerade Funktion $f(z)$ ist entsprechend $R_1(\wp(z)) \equiv 0$.

105. Satz: *Jede gerade elliptische Funktion der Perioden ω_1 und ω_2 ist eine rationale Funktion von $\wp(z)$. Jede ungerade elliptische Funktion der Perioden ω_1 und ω_2 ist das Produkt aus $\wp'(z)$ und einer rationalen Funktion von $\wp(z)$.*

Nach Satz 95 ist $\wp(z)$ in z, ω_1, ω_2 homogen von -2. Dimension. Im folgenden ist es notwendig eine in z, ω_1, ω_2 homogene Funktion 0. Dimension zu haben, die aber sonst alle Eigenschaften von $\wp(z)$ besitzt. Wir setzen:

$$\mathfrak{T}(z; \omega_1, \omega_2) = \frac{\wp\left(\frac{\bar\omega}{4}\right) - \wp\left(\frac{\bar\omega}{2}\right)}{\wp(z) - \wp\left(\frac{\bar\omega}{2}\right)}, \tag{35}$$

wo $\bar\omega$ irgendeine der drei Perioden ω_1, $\omega_1 + \omega_2$, ω_2 ist, für die $\wp\left(\frac{\bar\omega}{2}\right) \neq 0$ ist. Um die Gedanken zu fixieren, nehmen wir $\bar\omega = \omega_1 + \omega_2 = \omega_3$. Wegen Satz 96 ist dies keine Spezialisierung. Wir setzen ferner:

$$\mathrm{t} = \frac{4 \cdot 3 \wp\left(\frac{\omega_3}{2}\right)}{\wp\left(\frac{\omega_3}{4}\right) - \wp\left(\frac{\omega_3}{2}\right)}, \quad \text{also:} \quad \mathfrak{T}(z) = \frac{4 \cdot 3}{\mathrm{t}\left(\frac{\wp(z)}{\wp\left(\frac{\omega_3}{2}\right)} - 1\right)}. \tag{36}$$

Aus der Definition folgt:

$$\mathfrak{T}\left(\pm\tfrac{\omega_3}{4}; \omega_1, \omega_2\right) = 1. \tag{37}$$

106. Satz: *$\mathfrak{T}(z; \omega_1, \omega_2)$ ist eine gerade elliptische Funktion 2. Ordnung, die homogen von 0. Dimension in z, ω_1, ω_2 ist:*

$$\mathfrak{T}(tz; t\omega_1, t\omega_2) = \mathfrak{T}(z; \omega_1, \omega_2).$$

Sie hat für $z = 0$ eine Nullstelle 2. Ordnung, für $z = \frac{\omega_3}{2}$ einen Pol 2. Ordnung.

Diese Tatsachen ergeben sich direkt aus der Definition von $\mathfrak{T}(z)$. $\mathfrak{T}\left(z + \frac{\omega_3}{2}\right)$ hat umgekehrt für $z = 0$ einen Pol 2. Ordnung, für $z = \frac{\omega_3}{2}$ eine Nullstelle 2. Ordnung. Nach Satz 98 ist daher:

$$\mathfrak{T}(z)\,\mathfrak{T}\left(z + \tfrac{\omega_3}{2}\right) = \text{constans}.$$

Setzt man $z = \frac{\omega_3}{4}$, so findet man als Wert der Konstanten:

$$\mathfrak{T}\left(\tfrac{\omega_3}{4}\right)\mathfrak{T}\left(\tfrac{\omega_3}{4} + \tfrac{\omega_3}{2}\right) = \mathfrak{T}\left(-\tfrac{\omega_3}{4}\right) = 1, \quad \text{also:}$$

$$\mathfrak{T}\left(z + \tfrac{\omega_3}{2}\right) = \frac{1}{\mathfrak{T}(z)}. \tag{38}$$

Wegen $e_3 = \wp\left(\frac{\omega_3}{2}\right) \neq 0$, ist auch t von null verschieden. Wir setzen jetzt in $\mathfrak{T}(z)$ die Reihenentwicklung von $\wp(z)$ ein:

$$\mathfrak{T}(z) = \frac{4 \cdot 3}{\mathrm{t}\left(\frac{\wp(z)}{e_3} - 1\right)} = \frac{4 \cdot 3}{\mathrm{t}\left(\frac{1}{e_3 z^2} - 1 + \cdots\right)} = \frac{4 \cdot 3 \cdot e_3 z^2}{\mathrm{t}} + \cdots$$

Entsprechend ist nach Satz 101 und (33):

$$\frac{1}{\mathfrak{T}\left(z+\frac{\omega_3}{2}\right)} = \frac{\mathrm{t}}{4\cdot 3}\left(\frac{\wp\left(z+\frac{\omega_3}{2}\right)}{e_3} - 1\right) = \frac{\mathrm{t}}{4\cdot 3}\,\frac{\wp''\left(\frac{\omega_3}{2}\right)}{2!\,e_3}\,z^2 + \cdots$$

$$= \frac{\mathrm{t}}{8\cdot 3 e_3}\left(6e_3^2 - \frac{g_2}{2}\right)z^2 + \cdots$$

Die beiden Reihen müssen wegen (38) identisch gleich sein. Die Koeffizientenvergleichung ergibt:

$$\frac{4\cdot 3\cdot e_3}{\mathrm{t}} = \frac{\mathrm{t}\left(6e_3^2 - \frac{1}{2}g_2\right)}{8\cdot 3\cdot e_3} \qquad \text{oder:}$$

$$\frac{g_2}{e_3^2} = 12\,\frac{\mathrm{t}^2 - 3\cdot 2^4}{\mathrm{t}^2}. \tag{39}$$

Nun ist $e_3 = \wp\left(\frac{\omega_1+\omega_2}{2}\right)$ wegen (29) Wurzel von (32):

$$4e_3^3 - g_2 e_3 - g_3 = 0, \quad \text{oder:} \quad g_3 = 4e_3^3 - g_2 e_3,$$

somit kann man aus (39) auch g_3 berechnen:

$$\frac{g_3}{e_3^3} = 4\,\frac{2^4\cdot 3^2 - 2\mathrm{t}^2}{\mathrm{t}^2}. \tag{40}$$

Diese beiden Resultate berücksichtigen wir in der Reihenentwicklung:

$$\frac{\wp(z)}{e_3} = \frac{1}{(\sqrt{e_3}\,z)^2} + \sum_{k=1}^{\infty}\frac{c_k}{e_3^{k+1}}(\sqrt{e_3}\,z)^{2k},$$

wo nach Satz 103 und Formel (34):

$$\frac{c_k}{e_3^{k+1}} = \sum_{n,\,m} a_{n,m}\left(\frac{g_2}{e_3^2}\right)^n\left(\frac{g_3}{e_3^3}\right)^m, \quad 2n+3m = k+1,$$

indem wir für $\frac{g_2}{e_3^2}$ und $\frac{g_3}{e_3^3}$ die Werte in t einsetzen. Es wird dann:

$$\frac{\wp(z)}{e_3} = \frac{1}{(\sqrt{e_3}\,z)^2} + \frac{1}{\mathrm{t}}\sum_{k=1}^{\infty} A_k(\mathrm{t})\left(\sqrt{\frac{e_3}{\mathrm{t}}}\,z\right)^{2k},$$

wo die $A_k(\mathrm{t})$ ganze rationale Funktionen von t mit rationalen Zahlkoeffizienten sind. Kürzen wir den Ausdruck $2\sqrt{\frac{3e_3}{\mathrm{t}}}\,z$ mit ζ ab:

$$\zeta = 2\sqrt{\frac{3e_3}{\mathrm{t}}}\cdot z,$$

so lautet die Reihenentwicklung:

$$\frac{\wp(z)}{e_3} = \frac{4 \cdot 3}{\mathfrak{t}\xi^2} + \frac{1}{\mathfrak{t}} \sum_{k=1}^{\infty} A_k^*(\mathfrak{t})\xi^{2k}, \qquad \text{und:}$$

$$(41) \qquad \mathfrak{T}(z) = \frac{4 \cdot 3}{\mathfrak{t}\left(\frac{\wp(z)}{e_3} - 1\right)} = \xi^2 + \sum_{k=1}^{\infty} B_{k+1}(\mathfrak{t})\xi^{2k+2}, \quad \xi = 2\sqrt{\frac{3e_3}{\mathfrak{t}}} \cdot z,$$

wo die $B_k(\mathfrak{t})$ genau dieselben Eigenschaften wie die $A_k(\mathfrak{t})$ haben.

107. Satz: *Die Funktion $\mathfrak{T}(z)$ besitzt die Reihenentwicklung um $z = 0$:*

$$\mathfrak{T}(z) = \xi^2 + \sum_{k=1}^{\infty} B_{k+1}(\mathfrak{t})\xi^{2k+2}, \quad \xi = 2\sqrt{\frac{3e_3}{\mathfrak{t}}}\, z,$$

wo die $B_k(\mathfrak{t})$ ganze rationale Funktionen von $\mathfrak{t}$ mit rationalen Zahlkoeffizienten sind. Es ist:

$$B_2 = \frac{\mathfrak{t}}{4 \cdot 3}.$$

Entsprechend kann man $\mathfrak{T}(z)$ um den Punkt $z = -\frac{1}{2}\omega_3$ entwickeln. Man findet:

$$(42) \qquad \mathfrak{T}(z) = \frac{1}{\mathfrak{T}\left(z + \frac{\omega_3}{2}\right)} = \frac{1}{\xi_1^2} + \sum_{k=0}^{\infty} C_k(\mathfrak{t})\xi_1^{2k}, \quad \xi_1 = 2\sqrt{\frac{3e_3}{\mathfrak{t}}}\left(z + \frac{\omega_3}{2}\right),$$

wo die C_k dieselbe Eigenschaft wie die B_k haben. Als zweite Funktion führen wir statt $\wp'(z)$ die Funktion:

$$(43) \qquad \mathfrak{T}_1(z;\, \omega_1,\, \omega_2) = \frac{d\mathfrak{T}(z)}{d\xi}$$

ein. Es ist dann:

$$(43)' \qquad \mathfrak{T}_1(z) = -2\sqrt{\frac{3e_3}{\mathfrak{t}}}\,\frac{\wp'(z)}{(\wp(z) - e_3)^2}.$$

Aus den Definitionen von $\mathfrak{T}(z)$ und $\mathfrak{T}_1(z)$ ersieht man, daß $\wp(z)$ eine lineare Funktion von $\mathfrak{T}(z)$, und $\wp'(z)$ eine rationale Funktion von $\mathfrak{T}(z)$ und $\mathfrak{T}_1(z)$ ist. Wir können daher in Satz 104 und 105 $\wp(z)$ und $\wp'(z)$ durch $\mathfrak{T}(z)$ und $\mathfrak{T}_1(z)$ ersetzen:

108. Satz: *Jede elliptische Funktion der Perioden ω_1 und ω_2 ist eine rationale Funktion von $\mathfrak{T}(z)$ und $\mathfrak{T}_1(z)$. Jede gerade elliptische Funktion der Perioden ω_1 und ω_2 ist eine rationale Funktion von $\mathfrak{T}(z)$. Jede ungerade elliptische Funktion der Perioden ω_1 und ω_2 ist das Produkt aus $\mathfrak{T}_1(z)$ und einer rationalen Funktion von $\mathfrak{T}(z)$. $\mathfrak{T}(z)$ ist eine gerade, $\mathfrak{T}_1(z)$ eine ungerade elliptische Funktion der Perioden ω_1 und ω_2.*

Setzt man in (43)′ für $\wp(z)$ den Wert gemäß (29) ein, so wird:

$$\mathfrak{T}_1(z)^2 = 2^4 \frac{3\,e_3(\wp(z)-e_1)(\wp(z)-e_2)(\wp(z)-e_3)}{\mathfrak{t}\,(\wp(z)-e_3)^3} = 2^4 \frac{3\,e_3}{\mathfrak{t}}\,\mathfrak{T}(z)^3 \frac{(\wp(z)-e_1)(\wp(z)-e_2)}{\left(\frac{4\cdot 3\cdot e_3}{\mathfrak{t}}\right)^3},$$

oder, da nach (31) und (32): $e_1 + e_2 + e_3 = 0$, $e_1 e_2 e_3 = \frac{g_3}{4}$ ist:

$$\mathfrak{T}_1(z)^2 = \frac{\mathfrak{t}^2}{3^2\cdot 2^2}\,\mathfrak{T}(z)^3\left(\frac{\wp(z)}{e_3}-\frac{e_1}{e_3}\right)\left(\frac{\wp(z)}{e_3}-\frac{e_2}{e_3}\right) = \frac{\mathfrak{t}^2}{3^2\cdot 2^2}\,\mathfrak{T}(z)^3\left(\frac{\wp^2(z)}{e_3^2}+\frac{\wp(z)}{e_3}+\frac{g_3}{4\,e_3^3}\right).$$

Nach Definition (36) kann für $\frac{\wp(z)}{e_3}$ die Funktion $1+\frac{3\cdot 4}{\mathfrak{t}\,\mathfrak{T}(z)}$ genommen werden, somit wird wegen (40):

$$\mathfrak{T}_1(z)^2 = \frac{\mathfrak{t}^2}{3^2\cdot 2^2}\,\mathfrak{T}(z)\Big(\mathfrak{T}(z)^2 + \frac{6\cdot 4}{\mathfrak{t}}\,\mathfrak{T}(z) + \frac{9\cdot 4^2}{\mathfrak{t}^2} + \mathfrak{T}(z)^2 + \frac{3\cdot 4}{\mathfrak{t}}\,\mathfrak{T}(z) + \frac{9\cdot 4^2 - 2\,\mathfrak{t}^2}{\mathfrak{t}^2}\,\mathfrak{T}(z)^2\Big), \text{ oder}$$

$$\mathfrak{T}_1(z)^2 = \mathfrak{T}(z)(4\,\mathfrak{T}(z)^2 + \mathfrak{t}\,\mathfrak{T}(z) + 4). \tag{44}$$

109. Satz: *$\mathfrak{T}_1(z)$ ist in z, ω_1, ω_2 homogen von 0. Dimension, hat für $z = -\frac{1}{2}\omega_3$ einen Pol dritter Ordnung, und für $z = 0, \frac{\omega_1}{2}, \frac{\omega_2}{2}$ je eine einfache Nullstelle.*

Denn:
$$\mathfrak{T}_1(z) = \left(2^4 \frac{3\,e_3}{\mathfrak{t}} \frac{(\wp(z)-e_1)(\wp(z)-e_2)}{(\wp(z)-e_3)^3}\right)^{\frac{1}{2}}.$$

Wir können (44) auch so schreiben:

$$\mathfrak{T}_1(z)^2 = \mathfrak{T}(z)(4\,\mathfrak{T}(z)^2 + \mathfrak{t}\,\mathfrak{T}(z) + 4) \tag{44}′$$
$$= 4\,\mathfrak{T}(z)\left(\mathfrak{T}(z) - \mathfrak{T}\left(\frac{\omega_1}{2}\right)\right)\left(\mathfrak{T}(z) - \mathfrak{T}\left(\frac{\omega_2}{2}\right)\right).$$

Aus dem Additionstheorem von $\wp(z)$ folgt dasjenige von $\mathfrak{T}(z)$. Nach (36) und (38) wird:

$$\frac{\mathfrak{t}}{4\cdot 3}\left(\frac{\wp\left(z+t+\frac{\omega_3}{2}\right)}{e_3} - 1 + \frac{\wp\left(z+\frac{\omega_3}{2}\right)}{e_3} - 1 + \frac{\wp(t)}{e_3} - 1\right)$$
$$= \frac{1}{\mathfrak{T}\left(z+t+\frac{\omega_3}{2}\right)} + \frac{1}{\mathfrak{T}\left(z+\frac{\omega_3}{2}\right)} + \frac{1}{\mathfrak{T}(t)},$$

$$\frac{\mathfrak{t}}{4\cdot 3}\left(\frac{\wp\left(z+t+\frac{\omega_3}{2}\right)}{e_3} + \frac{\wp\left(z+\frac{\omega_3}{2}\right)}{e_3} + \frac{\wp(t)}{e_3}\right) = \mathfrak{T}(z+t) + \mathfrak{T}(z) + \frac{1}{\mathfrak{T}(t)} + \frac{\mathfrak{t}}{4}.$$

Ferner ist nach (43)′, (36) und (38):

$$\wp'(z) = -2^{-1}\sqrt{\frac{\mathfrak{t}}{3\,e_3}}\,(\wp(z)-e_3)^2\,\mathfrak{T}_1(z) = -\left(\frac{2^2\cdot 3\cdot e_3}{\mathfrak{t}}\right)^{\frac{3}{2}} \frac{\mathfrak{T}_1(z)}{\mathfrak{T}(z)^2},$$

$$\mathfrak{T}_1\left(z+\frac{\omega_3}{2}\right) = \frac{d\,\frac{1}{\mathfrak{T}(z)}}{d\zeta} = -\frac{\mathfrak{T}_1(z)}{\mathfrak{T}(z)^2}.$$

Somit folgt nach einfacher Rechnung:

$$\frac{1}{4}\,\frac{\mathfrak{t}}{4\cdot 3e_3}\left(\frac{\wp'\left(z+\frac{\omega_3}{2}\right)-\wp'(t)}{\wp\left(z+\frac{\omega_3}{2}\right)-\wp(t)}\right)^2=\frac{(\mathfrak{T}_1(z)\mathfrak{T}(t)^2+\mathfrak{T}_1(t))^2}{4\mathfrak{T}(t)^2(\mathfrak{T}(z)\mathfrak{T}(t)-1)^2}.$$

Jetzt kann man alle diese Werte in das Additionstheorem (30) einsetzen, nachdem man vorher noch z in $z+\frac{1}{2}\omega_3$ verwandelt hat und findet:

$$\mathfrak{T}(z+t)+\mathfrak{T}(z)+\frac{1}{\mathfrak{T}(t)}+\frac{\mathfrak{t}}{4}=\frac{(\mathfrak{T}_1(z)\mathfrak{T}(t)^2+\mathfrak{T}_1(t))^2}{4\mathfrak{T}(t)^2(\mathfrak{T}(z)\mathfrak{T}(t)-1)^2},\quad\text{oder:}$$

$$\mathfrak{T}(z+t)=\frac{\mathfrak{T}(z)\frac{\mathfrak{T}_1(t)^2}{\mathfrak{T}(t)}+2\mathfrak{T}_1(z)\mathfrak{T}_1(t)+\mathfrak{T}(t)\frac{\mathfrak{T}_1(z)^2}{\mathfrak{T}(z)}}{4(\mathfrak{T}(z)\mathfrak{T}(t)-1)^2}. \tag{45}$$

Für $z=t$ wird:

$$\mathfrak{T}(2z)=\frac{\mathfrak{T}_1(z)^2}{(\mathfrak{T}(z)^2-1)^2}=\frac{\mathfrak{T}(z)(4\mathfrak{T}(z)^2+\mathfrak{t}\mathfrak{T}(z)+4)}{(\mathfrak{T}(z)^2-1)^2}. \tag{46}$$

Durch Differentiation nach ξ findet man die entsprechenden Formeln für $\mathfrak{T}_1(z)$:

$$\mathfrak{T}_1(z+t)=-\frac{1}{2(\mathfrak{T}(z)\mathfrak{T}(t)-1)^3}\left\{\begin{array}{c}\mathfrak{T}_1(z)[6\mathfrak{T}(t)^2+\mathfrak{t}\mathfrak{T}(t)+2\\+\mathfrak{T}(z)\mathfrak{T}(t)(2\mathfrak{T}(t)^2+\mathfrak{t}\mathfrak{T}(t)+6)]\\+\mathfrak{T}_1(t)[6\mathfrak{T}(z)^2+\mathfrak{t}\mathfrak{T}(z)+2\\+\mathfrak{T}(z)\mathfrak{T}(t)(2\mathfrak{T}(z)^2+\mathfrak{t}\mathfrak{T}(z)+6)]\end{array}\right\} \tag{47}$$

$$\mathfrak{T}_1(2z)=-\frac{\mathfrak{T}_1(z)}{(\mathfrak{T}(z)^2-1)^3}\left\{2\mathfrak{T}(z)^4+\mathfrak{t}\mathfrak{T}(z)^3+12\mathfrak{T}(z)^2+\mathfrak{t}\mathfrak{T}(z)+2\right\}. \tag{48}$$

4. Die Multiplikationsformeln.

Die Hauptaufgabe der Additionstheoreme ist die Berechnung der Multiplikationsformeln. Setzt man in (45) und (47) sukzessive $t=2z$, $3z,\ldots(n-1)z$, so lassen sich $\mathfrak{T}(nz)$ und $\mathfrak{T}_1(nz)$ berechnen. Man erkennt:

110. Satz: $\mathfrak{T}(nz)$ und $\mathfrak{T}_1(nz):\mathfrak{T}_1(z)$ *sind rationale Funktionen von* $\mathfrak{T}(z)$, *deren Koeffizienten ganze rationale Funktionen von* $\mathfrak{t}$ *mit rationalen Zahlkoeffizienten sind (n eine positive ganze rationale Zahl).*

Der erste Teil des Satzes ergibt sich schon aus Satz 108. Das Additionstheorem orientiert dagegen erst über die Natur der Koeffizienten. Die Aufgabe ist, diese Funktionen noch näher zu bestimmen. Hierzu teilen wir das Periodenparallelogramm von Figur 15 in n^2 ähnliche Teilparallelogramme, deren Eckpunkte sind:

$$-\frac{\omega_1+\omega_2}{2}+\frac{h_1\omega_1+h_2\omega_2}{n},\quad \left.\begin{matrix}h_1\\h_2\end{matrix}\right\}=0,\,1,\,2,\ldots,(n-1),$$

und deren Mittelpunkte sind:

$$-\frac{\omega_1+\omega_2}{2}+\frac{\omega_1+\omega_2}{2n}+\frac{h_1\omega_1+h_2\omega_2}{n},\quad \left.\begin{matrix}h_1\\h_2\end{matrix}\right\}=0,\ 1,\ 2,\ \ldots,\ (n-1).$$

Wir unterscheiden zwei Fälle:

a) n ungerade. Unter den Mittelpunkten tritt der Nullpunkt auf. Je zwei andere Mittelpunkte sind in bezug auf 0 symmetrisch, die zugehörigen Werte von $\mathfrak{T}(z)$ nach Satz 106 also gleich. $\mathfrak{T}(z)$ nimmt an den Mittelpunkten außer $\mathfrak{T}(0)=0$ nur $\frac{n^2-1}{2}$ verschiedene Werte an, die durch:

$$(49)\qquad \left\{\begin{array}{ll}\mathfrak{T}\left(\frac{h_1\omega_1+h_2\omega_2}{n}\right), & \left\{\begin{array}{l}h_1=0,\pm 1,\pm 2,\cdots\pm\frac{n-1}{2}\\ h_2=-1,-2,\cdots-\frac{n-1}{2}\end{array}\right. \text{ und}\\ & \left\{\begin{array}{l}h_1=-1,-2,\cdots-\frac{n-1}{2}\\ h_2=0\end{array}\right.\end{array}\right.$$

gegeben werden können. Wir setzen

$$(50)\qquad \left\{\begin{array}{l}Z_1(\mathfrak{T}(z))\equiv 1,\\ Z_n(\mathfrak{T}(z))=\prod\limits_{(h_1h_2)}\left(\mathfrak{T}(z)-\mathfrak{T}\left(\frac{h_1\omega_1+h_2\omega_2}{n}\right)\right),\quad n>1,\end{array}\right.$$

wo die h die in (49) gegebenen Werte durchlaufen. $Z_n(\mathfrak{T}(z))$ ist eine ganze rationale Funktion $\frac{n^2-1}{2}$ ten Grades von $\mathfrak{T}(z)$.

An dem Eckpunkt $-\frac{\omega_2}{2}$ wird $\mathfrak{T}(z)$ unendlich. Wir lassen ihn weg. Von den übrigen sind je zwei symmetrisch in bezug auf den Nullpunkt, sofern sie nicht auf dem Rande des Parallelogramms liegen, ergeben daher denselben Wert von $\mathfrak{T}(z)$. Von den Randpunkten ergeben auch zwei, die in bezug auf den Mittelpunkt der Parallelogrammseite symmetrisch liegen, dasselbe $\mathfrak{T}(z)$, z. B.:

$$\mathfrak{T}\left(-\frac{\omega_1+\omega_2}{2}+\frac{h_1\omega_1}{n}\right)=\mathfrak{T}\left(-\frac{\omega_1+\omega_2}{2}+\frac{h_1\omega_1}{n}\right)=\mathfrak{T}\left(\frac{\omega_1-\omega_2}{2}-\frac{h_1\omega_1}{n}\right)$$
$$=\mathfrak{T}\left(-\frac{\omega_1+\omega_2}{2}+\frac{(n-h_1)\omega_1}{n}\right).$$

Somit nimmt $\mathfrak{T}(z)$ an den Eckpunkten nur die $\frac{n^2-1}{2}$ Werte an:

$$(51)\qquad \left\{\begin{array}{ll}\mathfrak{T}\left(-\frac{\omega_1+\omega_2}{2}+\frac{h_1\omega_1+h_2\omega_2}{n}\right), & \left\{\begin{array}{l}h_1=0,\ 1,\ 2,\ \ldots\ n-1\\ h_2=1,\ 2,\ \ldots\ \frac{n-1}{2}\end{array}\right.\\ & \left\{\begin{array}{l}h_1=1,\ 2,\ \ldots\ \frac{n-1}{2}\\ h_2=0\end{array}\right.\end{array}\right.$$

und wir setzen:

$$N_1(\mathfrak{T}(z)) \equiv 1,$$

$$(52)\quad N_n(\mathfrak{T}(z)) \equiv n \underset{(h_1 h_2)}{\prod\!\!\prod} \left(\mathfrak{T}(z) - \mathfrak{T}\left(-\frac{\omega_1+\omega_2}{2} + \frac{h_1\omega_1 + h_2\omega_2}{n}\right)\right),\ n > 1,$$

wo die h die in (51) festgelegten Werte durchlaufen. $N_n(\mathfrak{T}(z))$ ist eine ganze rationale Funktion $\frac{n^2-1}{2}^{\text{ten}}$ Grades von $\mathfrak{T}(z)$.

b) n gerade. Die Rolle der Eck- und Mittelpunkte vertauscht sich gegenüber dem Falle a). Die Eckpunkte $0, -\frac{\omega_1}{2}, -\frac{\omega_2}{2}$ treten nur einfach auf, alle übrigen lassen sich paarweise anordnen. Alle verschiedenen, an den Eckpunkten angenommenen Werte von $\mathfrak{T}(z)$ sind daher:

$$(53)\quad \begin{cases} \mathfrak{T}\left(-\frac{\omega_1}{2}\right),\ \mathfrak{T}\left(-\frac{\omega_2}{2}\right),\ \mathfrak{T}\left(-\frac{\omega_1+\omega_2}{2} + \frac{h_1\omega_1+h_2\omega_2}{n}\right), \\ \begin{cases} h_1 = 0, 1, \ldots n-1, \\ h_2 = 1, 2, \cdots \frac{n}{2} - 1 \end{cases} \quad \text{und} \quad \begin{cases} h_1 = 1, 2, \cdots \frac{n}{2} - 1, \\ h_2 = 0, \frac{n}{2} \end{cases} \end{cases}$$

und wir setzen:

$$(54)\quad \begin{cases} z_2(\mathfrak{T}(z)) \equiv 4\mathfrak{T}(z)^2 + t\mathfrak{T}(z) + 4, \\ Z_2(\mathfrak{T}(z)) \equiv 1, \\ Z_n(\mathfrak{T}(z)) \equiv \frac{n}{2} \prod\limits_{(h_1 h_2)} \left(\mathfrak{T}(z) - \mathfrak{T}\left(-\frac{\omega_1+\omega_2}{2} + \frac{h_1\omega_1+h_2\omega_2}{n}\right)\right),\ n > 2, \end{cases}$$

wo die h die in (53) fixierten Zahlenpaare durchlaufen. Z_n ist eine ganze rationale Funktion vom Grade:

$$n\left(\frac{n}{2} - 1\right) + 2\left(\frac{n}{2} - 1\right) = \left(\frac{n^2}{2} - 2\right)$$

in $\mathfrak{T}(z)$. Entsprechend sind:

$$(55)\quad \mathfrak{T}\left(-\frac{\omega_1+\omega_2}{2} + \frac{\omega_1+\omega_2}{2n} + \frac{h_1\omega_1+h_2\omega_2}{n}\right),\quad \begin{cases} h_1 = 0, 1, 2, \ldots n-1, \\ h_2 = 0, 1, 2, \cdots \frac{n}{2} - 1 \end{cases}$$

die verschiedenen Werte, die $\mathfrak{T}(z)$ an den Mittelpunkten annimmt. Man setzt:

$$(56)\quad N_n(\mathfrak{T}(z)) \equiv \underset{(h_1 h_2)}{\prod\!\!\prod} \left(\mathfrak{T}(z) - \mathfrak{T}\left(-\frac{\omega_1+\omega_2}{2} + \frac{\omega_1+\omega_2}{2n} + \frac{h_1\omega_1+h_2\omega_2}{n}\right)\right),$$

wo die h die in (55) festgelegten Werte durchlaufen. N_n ist eine ganze rationale Funktion $\frac{n^2}{2}^{\text{ten}}$ Grades von $\mathfrak{T}(z)$. Jetzt gilt der

III. Satz: *Es gelten die Formeln:*

a) n ungerade: $\mathfrak{T}(nz) = \frac{\mathfrak{T}(z) Z_n^2}{N_n^2}$,

b) n gerade: $\mathfrak{T}(nz) = \frac{\mathfrak{T}(z)z_2 Z_n^2}{N_n^2} = \frac{\mathfrak{T}_1^2(z) Z_n^2}{N_n^2}$.

Zum Beweise unterscheiden wir wieder

a) n ungerade. Die Funktion:

$$\mathfrak{T}(nz;\ \omega_1,\ \omega_2) = \mathfrak{T}\left(z;\ \frac{\omega_1}{n},\ \frac{\omega_2}{n}\right)$$

hat nach Satz 106 an allen und nur den Punkten $z = \frac{h_1\omega_1 + h_2\omega_2}{n}$ Nullstellen 2. Ordnung und an allen und nur den Stellen $z = -\frac{\omega_1+\omega_2}{2} + \frac{h_1\omega_1+h_2\omega_2}{n}$ Pole 2. Ordnung. Die linke und rechte Seite der zu beweisenden Gleichung sind daher nach Satz 98 bis auf einen konstanten Faktor einander gleich. Um letztern zu bestimmen, entwickeln wir beide Seiten um $z = -\frac{1}{2}\omega_3$. Nach (38) und (42) ist:

$$\mathfrak{T}(nz) = \frac{1}{\mathfrak{T}\left(nz + \frac{\omega_3}{2}\right)} = \frac{1}{\mathfrak{T}\left(n\left(z + \frac{\omega_3}{2}\right)\right)} = \frac{1}{n^2\zeta_1^2} + \cdots,$$

$$\zeta_1 = 2\sqrt{\frac{3e_3}{\mathfrak{t}}}\left(z + \frac{\omega_3}{2}\right).$$

Anderseits sind die Glieder höchster Potenz von $\mathfrak{T}(z)$ in Z_n und N_n $\mathfrak{T}(z)^{\frac{n^2-1}{2}}$ und $n\mathfrak{T}(z)^{\frac{n^2-1}{2}}$, somit ist:

$$\frac{\mathfrak{T}(z)\,Z_n^2}{N_n^2} = \frac{\mathfrak{T}(z)}{n^2} + \cdots = \frac{1}{n^2\zeta_1^2} + \cdots.$$

Der Vergleich der Koeffizienten von $\frac{1}{\zeta_1^2}$ zeigt, daß der konstante Faktor eins ist.

b) n gerade. $\mathfrak{T}(nz)$ wird null für alle und nur die Punkte $z = -\frac{\omega_1+\omega_2}{2} + \frac{h_1\omega_1+h_2\omega_2}{n}$, da $\mathfrak{T}(nz;\ \omega_1,\ \omega_2) = \mathfrak{T}\left(z;\ \frac{\omega_1}{n},\ \frac{\omega_2}{n}\right)$ und auch $\frac{1}{2}\omega_3 = \frac{\frac{n}{2}\omega_3}{n}$ ein Vielfaches der Perioden ist. Die Ordnung jeder Nullstelle ist 2. $\mathfrak{T}(nz)$ wird unendlich von 2. Ordnung an allen Stellen $z = -\frac{\omega_1+\omega_2}{2n} + \frac{h_1\omega_1+h_2\omega_2}{n}$. Somit haben die linke und rechte Seite der zu beweisenden Gleichung dieselben Nullstellen und Pole mit denselben Ordnungen, da nur an den Punkten $z = 0$, $-\frac{\omega_1}{2}$ und $-\frac{\omega_2}{2}$ $\mathfrak{T}(z)$ seinen Wert ebenfalls von 2. Ordnung annimmt. Die linke und rechte Seite können sich daher nur um einen konstanten Faktor unterscheiden, den man genau wie vorhin durch Reihenentwicklung findet:

$$\mathfrak{T}(nz) = \mathfrak{T}\left(n\left(z + \frac{\omega_3}{2}\right)\right) = n^2 \xi_1^2 + \cdots,$$

$$\frac{\mathfrak{T}(z)\, z_2\, Z_n^2}{N_n^2} = \frac{n^2}{\mathfrak{T}(z)} + \cdots = n^2\, \mathfrak{T}\left(z + \frac{\omega_3}{2}\right) + \cdots = n^2 \xi_1^2 + \cdots.$$

Der Faktor ist eins.

112. Satz: *Die Koeffizienten von Z_n und N_n sind ganze rationale Funktionen von* t *mit ganzen rationalen Zahlkoeffizienten, und zwar:*

a) n ungerade:

$$Z_n(0) = (-1)^{\frac{n-1}{2}}\, n, \quad N_n(0) = (-1)^{\frac{n-1}{2}},$$

$$\mathfrak{T}(z)^{\frac{n^2-1}{2}}\, Z_n\left(\frac{1}{\mathfrak{T}(z)}\right) = (-1)^{\frac{n-1}{2}}\, N_n(\mathfrak{T}(z)).$$

b) n gerade: $Z_n(0) = (-1)^{\frac{n}{2}-1}\, \frac{n}{2}$, $N_n(0) = (-1)^{\frac{n}{2}}$.

Beweis:

a) n ungerade: Setzt man in der Formel von Satz 111 an Stelle von z: $z + \frac{\omega_3}{2}$, so wird wegen (38):

$$\mathfrak{T}\left(z + \frac{\omega_3}{2}\right) = \frac{1}{\mathfrak{T}(z)}, \quad \mathfrak{T}\left(n\left(z + \frac{\omega_3}{2}\right)\right) = \mathfrak{T}\left(nz + \frac{\omega_3}{2}\right) = \frac{1}{\mathfrak{T}(nz)},$$

$$\frac{1}{\mathfrak{T}(nz)} = \frac{Z_n\left(\frac{1}{\mathfrak{T}(z)}\right)^2}{\mathfrak{T}(z)\, N_n\left(\frac{1}{\mathfrak{T}(z)}\right)^2}, \text{ oder } \mathfrak{T}(nz) = \frac{\mathfrak{T}(z)\left(\mathfrak{T}(z)^{\frac{n^2-1}{2}}\, N_n\left(\frac{1}{\mathfrak{T}(z)}\right)\right)^2}{\left(\mathfrak{T}(z)^{\frac{n^2-1}{2}}\, Z_n\left(\frac{1}{\mathfrak{T}(z)}\right)\right)^2} = \frac{\mathfrak{T}(z)\, Z_n^2}{N_n^2},$$

woraus sich sofort die Beziehungen ergeben:

$$N_n(\mathfrak{T}(z)) = \pm c\, \mathfrak{T}(z)^{\frac{n^2-1}{2}}\, Z_n\left(\frac{1}{\mathfrak{T}(z)}\right), \quad N_n(0) = \pm c,$$

$$Z_n(\mathfrak{T}(z)) = c\, \mathfrak{T}(z)^{\frac{n^2-1}{2}}\, N_n\left(\frac{1}{\mathfrak{T}(z)}\right), \quad Z_n(0) = cn.$$

Nimmt man daher den Satz für Z_n als bewiesen an, so ist $c = (-1)^{\frac{n-1}{2}}$, und er folgt auch für N_n; denn für $z = \frac{\omega_3}{2}$ ergibt die erste Gleichung $+n = \pm c\, Z_n(0) = \pm\, c^2 n$. Also gilt nur das obere Zeichen.

Für $n = 1$ ist $Z_1 = 1$, was den Bedingungen entspricht. Für $n = 3$ bedenkt man, daß $\mathfrak{T}(z) - \mathfrak{T}(2z)$ nur null und zwar von 1. Ordnung wird (Satz 106), falls $z \pm 2z$ ein Vielfaches der Perioden ist, d. h. wenn:

$$z = \frac{h_1 \omega_1 + h_2 \omega_2}{3}, \quad \left.\begin{matrix} h_1 \\ h_2 \end{matrix}\right\} = 0,\ 1,\ -1,$$

wird. Einzig für $h_1 = h_2 = 0$ ist die Nullstelle von 2. Ordnung. $\mathfrak{T}(z) - \mathfrak{T}(2z)$ wird nur unendlich, wenn $z = -\frac{\omega_3}{2}, \pm\frac{\omega_3}{4}, \pm\left(-\frac{\omega_3}{4} + \frac{\omega_1}{2}\right)$, und zwar von

2. Ordnung. $\mathfrak{T}(z) - \mathfrak{T}(2z)$ hat somit die gleichen Nullstellen und Pole mit derselben Ordnung, wie:

$$\frac{\mathfrak{T}(z)\, Z_2}{N_2^2},$$

und es muß, wie früher:

$$\mathfrak{T}(z) - \mathfrak{T}(2z) = C\,\frac{\mathfrak{T}(z)\, Z_3}{N_2^2}$$

sein, wo C eine Konstante ist. Dieselbe wird durch Reihenentwicklung um $z = -\frac{\omega_3}{2}$ als 1 erkannt. Somit ist, wenn für $\mathfrak{T}(2z)$ und N_2 der Wert von (46) eingesetzt wird:

$$Z_3 \equiv (\mathfrak{T}(z)^2 - 1)^2 - 4 - \mathfrak{t}\mathfrak{T}(z) - 4\mathfrak{T}(z)^2 \equiv \mathfrak{T}(z)^4 - 6\mathfrak{T}(z)^2 - \mathfrak{t}\mathfrak{T}(z) - 3$$

und:
$$\mathfrak{T}(3z) = \frac{\mathfrak{T}(z)(\mathfrak{T}(z)^4 - 6\mathfrak{T}(z)^2 - 1\mathfrak{T}(z) - 3)^2}{(3\mathfrak{T}(z)^4 + \mathfrak{t}\mathfrak{T}(z)^3 + 6\mathfrak{T}(z)^2 - 1)^2}.$$

Der Satz ist somit für $n = 1$ und 3 bewiesen. Wir nehmen ihn für $n = 1, 3, \ldots (n-2)$ als richtig an $(n > 3)$. Die Funktion:

$$\mathfrak{T}((n-2)z) - \mathfrak{T}(2z)$$

besitzt Nullstellen 1. Ordnung für:

$(n-2)z \pm 2z = h_1\omega_1 + h_2\omega_2$, oder $z = \frac{h_1\omega_1 + h_2\omega_2}{n}$ und $z = \frac{h_1\omega_1 + h_2\omega_2}{n-4}$

nur für $h_1 = h_2 = 0$ ist die Nullstelle von 2. Ordnung, Pole 2. Ordnung für alle Punkte, für die $N_2 = 0$ und $N_{n-2} = 0$ und für $-\frac{\omega_3}{2}$. Dieselbe Überlegung wie vorhin zeigt, daß daher:

$$\mathfrak{T}((n-2)z) - \mathfrak{T}(2z) = \frac{\mathfrak{T}(z)\, Z_n\, Z_{n-4}}{N_2^2\, N_{n-2}^2}.$$

Setzt man links die Werte ein, so folgt:

$$\frac{\mathfrak{T}(z)\, Z_{n-2}^2}{N_{n-2}^2} - \frac{\mathfrak{T}(z)\, z_2}{N_2^2} = \frac{\mathfrak{T}(z)\, Z_n\, Z_{n-4}}{N_2^2\, N_{n-2}^2} \qquad \text{oder:}$$

$$Z_{n-4}\, Z_n \equiv N_2^2\, Z_{n-2}^2 - N_{n-2}^2\, z_2. \tag{57}$$

Nach Annahme ist $Z_{n-4}(0) = (-1)^{\frac{n-5}{2}}(n-4)$, $Z_{n-2}(0) = (-1)^{\frac{n-3}{2}}(n-2)$, $N_{n-2}(0) = (-1)^{\frac{n-3}{2}}$, also folgt aus (57):

$(-1)^{\frac{n-5}{2}}(n-4)\, Z_n(0) = (n-2)^2 - 4 = (n-4)\, n$ oder: $Z_n(0) = (-1)^{\frac{n-1}{2}}\, n$

Ferner zeigt (57), daß Z_n ganze rationale Funktionen von t mit ganzen rationalen Zahlkoeffizienten als Koeffizienten hat, da Z_{n-4}, Z_{n-2} und N_{n-2} diese Eigenschaften haben, und Z_{n-4} und Z_{n-2} die obersten Koeffizienten 1 besitzen. Zugleich enthält (57) ein einfaches Mittel, um Z_n zu berechnen.

b) n gerade: Vertauscht man in $\mathfrak{T}(nz)$ z mit $z+\frac{\omega_3}{2}$, so bleibt jetzt $\mathfrak{T}(nz)$ ungeändert und die Formel geht über in:

$$\mathfrak{T}(nz)=\frac{z_2\left(\frac{1}{\mathfrak{T}(z)}\right)Z_n\left(\frac{1}{\mathfrak{T}(z)}\right)^2}{\mathfrak{T}(z)\,N_n\left(\frac{1}{\mathfrak{T}(z)}\right)^2}=\frac{\mathfrak{T}(z)\,z_2\left(\mathfrak{T}(z)^{\frac{n^2}{2}-2}Z_n\left(\frac{1}{\mathfrak{T}(z)}\right)\right)^2}{\left(\mathfrak{T}(z)^{\frac{n^2}{2}}N_n\left(\frac{1}{\mathfrak{T}(z)}\right)\right)^2}=\frac{\mathfrak{T}(z)\,z_2\,Z_n^2}{N_n^2},$$

d. h. es muß:

$$Z_n(\mathfrak{T}(z))=\pm c\,\mathfrak{T}(z)^{\frac{n^2}{2}-2}Z_n\left(\frac{1}{\mathfrak{T}(z)}\right),\quad N_n(\mathfrak{T}(z))=c\,\mathfrak{T}(z)^{\frac{n^2}{2}}N_n\left(\frac{1}{\mathfrak{T}(z)}\right)$$

werden. Daraus folgt $c^2=1$, $c=\pm 1$ und weiter $Z_n(0)=\pm c^{\frac{n}{2}}$, $N_n(0)=c$. Für $n=2$ und alle ungeraden n gilt der Satz. Wir dürfen ihn daher für $n=1, 2, 3, \ldots (n-1)$ als bewiesen annehmen. Dann folgt aus (46):

$\frac{1}{2}$ n *ungerade:*
$$\mathfrak{T}(nz)=\mathfrak{T}\left(2\,\frac{n}{2}z\right)=\frac{\mathfrak{T}\left(\frac{n}{2}z\right)z_2\left(\mathfrak{T}\left(\frac{n}{2}z\right)\right)}{\left(\mathfrak{T}\left(\frac{n}{2}z\right)^2-1\right)^2}$$
$$=\frac{\mathfrak{T}(z)\,Z_{\frac{n}{2}}^2\,N_{\frac{n}{2}}^2\left(4\,\mathfrak{T}(z)^2Z_{\frac{n}{2}}^4+t\,\mathfrak{T}(z)\,Z_{\frac{n}{2}}^2\,N_{\frac{n}{2}}^2+4N_{\frac{n}{2}}^4\right)}{\left(\mathfrak{T}(z)^2Z_{\frac{n}{2}}^4-N_{\frac{n}{2}}^4\right)^2},$$

$\frac{1}{2}$ n *gerade:*
$$\mathfrak{T}(nz)=\mathfrak{T}\left(2\,\frac{n}{2}z\right)=\frac{\mathfrak{T}\left(\frac{n}{2}z\right)z_2\left(\mathfrak{T}\left(\frac{n}{2}z\right)\right)}{\left(\mathfrak{T}\left(\frac{n}{2}z\right)^2-1\right)^2}$$
$$=\frac{\mathfrak{T}(z)\,z_2\,Z_{\frac{n}{2}}^2\,N_{\frac{n}{2}}^2\left(4\,\mathfrak{T}(z)^2z_2^2Z_{\frac{n}{2}}^4+t\,\mathfrak{T}(z)z_2\,Z_{\frac{n}{2}}^2\,N_{\frac{n}{2}}^2+4N_{\frac{n}{2}}^4\right)}{\left(\mathfrak{T}(z)^2z_2^2Z_{\frac{n}{2}}^4-N_{\frac{n}{2}}^4\right)^2},\qquad\text{also:}$$

$\frac{1}{2}$ n *ungerade:* $N_n\equiv Z_{\frac{n}{2}}^4\,\mathfrak{T}(z)^2-N_{\frac{n}{2}}^4$, $N_n(O)=-1=(-1)^{\frac{n}{2}}$,

$\frac{1}{2}$ n *gerade:* $N_n\equiv N_{\frac{n}{2}}^4-z_2^2Z_{\frac{n}{2}}^4\,\mathfrak{T}(z)^2$, $N_n(O)=N_{\frac{n}{2}}(O)^4=+1=(-1)^{\frac{n}{2}}$.

Damit ist für N_n eine Rekursionsformel gefunden, aus der sich die Richtigkeit aller Aussagen des Satzes auch für N_n ergibt. Zugleich ergibt sich für c der Wert $(-1)^{\frac{n}{2}}$.

Um auch für Z_n eine Rekursionsformel zu erhalten, berechnen wir zuerst aus der obigen Formel Z_4. Es wird:

$$Z_4^2=Z_2^2\,N_2^2(4\,\mathfrak{T}(z)^2z_2^2Z_2^4+t\,\mathfrak{T}(z)\,z_2\,Z_2^2N_2^2+4N_2^4)$$
$$=N_2^2(2\,\mathfrak{T}(z)^4+t\,\mathfrak{T}(z)^3+12\,\mathfrak{T}(z)^2+t\,\mathfrak{T}(z)+2)^2,$$
$$Z_4=N_2(2\,\mathfrak{T}(z)^4+t\,\mathfrak{T}(z)^3+12\,\mathfrak{T}(z)^2+t\,\mathfrak{T}(z)+2),\ Z_4(0)=-2.$$

Der Satz stimmt also für $n=2$ und 4, und da wieder wie im ersten Falle:

$$\mathfrak{T}((n-2)z)-\mathfrak{T}(2z)=\frac{\mathfrak{T}(z)\,z_2\,Z_{n-4}\,Z_n}{N_{n-2}^2\,N_2^2}$$

ist, wo z_2 hinzugefügt ist, da nach Satz 109 $-\frac{\omega_1}{2}$ und $-\frac{\omega_2}{2}$ Nullstellen 2. Ordnung sind, so muß die Gleichung gelten:

$$Z_{n-4} Z_n = N_2^2 Z_{n-2}^2 - N_{n-2}^2. \tag{57}'$$

Wir setzen voraus, Z_n erfülle alle Eigenschaften für 2, 4, ... $(n-2)$. Dann ergibt diese Rekursionsformel dieselben auch für n. Für $z = 0$ wird:

$$\frac{n-4}{2}(-1)^{\frac{n-4}{2}-1} Z_n(0) = \frac{(n-2)^2}{4} - 1 = \frac{n(n-4)}{4}, \quad Z_n(O) = \frac{n}{2}(-1)^{\frac{n}{2}-1}.$$

Der Satz ist jetzt in allen Teilen bewiesen.

5. Multiplikation der Perioden.

Es sei n eine *ungerade* positive, ganze rationale Zahl. Dann ist $\mathfrak{T}(z;\ \omega_1,\ \omega_2)$ auch eine zu den Perioden $n\omega_1$, ω_2 gehörende elliptische Funktion; denn sie besitzt die Perioden $n\omega_1$ und ω_2. Die Grundfunktion dieser Perioden ist aber $\mathfrak{T}(z;\ n\omega_1,\ \omega_2)$. Daher folgt aus Satz 108, da beide Funktionen gerade sind, daß $\mathfrak{T}(z;\ \omega_1,\ \omega_2)$ eine rationale Funktion von $\mathfrak{T}(z;\ n\omega_1,\ \omega_2)$ ist:

$$\mathfrak{T}(z;\ \omega_1,\ \omega_2) = R(\mathfrak{T}(z;\ n\omega_1,\ \omega_2)).$$

Die Aufgabe ist es, R genauer zu bestimmen. Das Periodenparallelogramm von $\mathfrak{T}(z;\ n\omega_1,\ \omega_2)$ hat die Seiten $|n\omega_1|$ und $|\omega_2|$, ist also n mal das Periodenparallelogramm von $\mathfrak{T}(z;\ \omega_1,\ \omega_2)$. In demselben wird $\mathfrak{T}(z;\ \omega_1,\ \omega_2)$ an den Punkten $z = 0,\ \omega_1,\ 2\omega_1,\ 3\omega_1,\ \ldots,\ (n-1)\omega_1$ von 2. Ordnung null und an den Punkten $z = \frac{\omega_1+\omega_2}{2},\ \frac{\omega_1+\omega_2}{2}+\omega_1,\ \frac{\omega_1+\omega_2}{2}+2\omega_1,\ \ldots\ \frac{\omega_1+\omega_2}{2}+(n-1)\omega_1$ unendlich von 2. Ordnung. Dabei haben wir hier das Periodenparallelogramm mit den Ecken, O, $n\omega_1$, $n\omega_1+\omega_2$, ω_2 zugrunde gelegt. Da n ungerade ist, nimmt $\mathfrak{T}(z;\ n\omega_1,\ \omega_2)$ an je zwei und nur zwei dieser Punkte, ausgenommen O und $\frac{\omega_1+\omega_2}{2}+\frac{n-1}{2}\omega_1$, denselben Wert an. Setzt man somit:

$$\begin{cases} Z_n(x) \equiv \prod_{h=1}^{\frac{n-1}{2}} (x - \mathfrak{T}(h\omega_1;\ n\omega_1,\ \omega_2)), \\ N_n(x) \equiv \prod_{h=0}^{\frac{n-3}{2}} \left(x - \mathfrak{T}\left(\frac{\omega_1+\omega_2}{2} + h\omega_1;\ n\omega_1,\ \omega_2\right)\right), \end{cases} \tag{58}$$

so muß wieder

$$\mathfrak{T}(z;\ \omega_1,\ \omega_2) = C\,\mathfrak{T}(z;\ n\omega_1,\ \omega_2)\frac{Z_n(\mathfrak{T}(z;\ n\omega_1,\ \omega_2))^2}{N_n(\mathfrak{T}(z;\ n\omega_1,\ \omega_2))^2} \tag{59}$$

sein, wo C eine Konstante in bezug auf z ist. Vertauscht man hier z

mit $z + \frac{n\omega_1 + \omega_2}{2}$, so geht nach (38), da n ungerade ist, $\mathfrak{T}(z;\ \omega_1,\ \omega_2)$ in $1 : \mathfrak{T}(z;\ \omega_1,\ \omega_2)$ und $\mathfrak{T}(z;\ n\omega_1,\ \omega_2)$ in $1 : \mathfrak{T}(z;\ n\omega_1,\ \omega_2)$ über, und (59) lautet:

$$\mathfrak{T}(z;\ \omega_1,\ \omega_2) = \frac{1}{C}\,\mathfrak{T}(z;\ n\omega_1,\ \omega_2)\,\frac{N_n\left(\frac{1}{\mathfrak{T}(z;\ n\omega_1,\ \omega_2)}\right)^2}{Z_n\left(\frac{1}{\mathfrak{T}(z;\ n\omega_1,\ \omega_2)}\right)^2},$$

woraus durch Vergleichung mit (59):

$$C^2\,\frac{Z_n(x)^2}{N_n(x)^2} \equiv \frac{x^{n-1}\,N_n\left(\frac{1}{x}\right)^2}{x^{n-1}\,Z_n\left(\frac{1}{x}\right)^2},$$

$$C_1 C Z_n(x) \equiv x^{\frac{n-1}{2}}\,N_n\left(\frac{1}{x}\right), \quad \pm C_1 N_n(x) \equiv x^{\frac{n-1}{2}}\,Z_n\left(\frac{1}{x}\right)$$

entsteht. Vertauscht man x mit $1 : x$, so wird:

$$C_1^2 = \pm\frac{1}{C}, \quad C_1 = (\pm)\frac{1}{\sqrt{\pm C}}, \qquad \text{also:}$$

$$(60)\quad \pm(\pm)\sqrt{\pm C}\,Z_n(x) \equiv x^{\frac{n-1}{2}}\,N_n\left(\frac{1}{x}\right), \quad \pm N_n(x) \equiv (\pm)\sqrt{\pm C}\,x^{\frac{n-1}{2}}\,Z_n\left(\frac{1}{x}\right),$$

und für $x = 0$ wegen (58):

$$(61)\quad \begin{cases} \pm C Z_n(0)^2 = 1, \ \pm C = Z_n(0)^{-2} = \left(\prod_{h=1}^{\frac{n-1}{2}} \mathfrak{T}(h\omega_1;\ n\omega_1,\ \omega_2)\right)^{-2}, \\ \pm C = N_n(0)^2. \end{cases}$$

Wir entwickeln noch $\mathfrak{T}(z;\ \omega_1,\ \omega_2)$ in die Reihe von Satz 107 um $z = 0$ nach Potenzen von ζ und entsprechend $\mathfrak{T}(z;\ n\omega_1,\ \omega_2)$ nach Potenzen von ζ_n.

ζ und ζ_n enthalten beide den Faktor z, aber die Koeffizienten $2\sqrt{\frac{3e_3}{\mathfrak{t}}}$ sind beide Male verschieden, da das eine Mal e_3 und $\mathfrak{t}$ für die Perioden ω_1 und ω_2, das andere Mal für die Perioden $n\omega_1$, ω_2 zu berechnen sind. Diese beiden Reihen setzen wir in (59) ein, dividieren beide Seiten durch ζ_n^2 und gehen zur Grenze $z = 0$ über. Dann folgt gemäß (61):

$$(62)\qquad \lim_{z=0}\frac{\zeta^2}{\zeta_n^2} = \left(\frac{\zeta}{\zeta_n}\right)^2 = C\,\frac{Z_n(0)^2}{N_n(0)^2} = C^{-1}, \quad \frac{\zeta_n}{\zeta} = \sqrt{C}.$$

Wir führen jetzt nur noch die Variable ζ ein, indem ζ_n^2 durch $C\zeta^2$ zu ersetzen ist, und setzen die Reihen in:

$$\mathfrak{T}(z;\ \omega_1,\ \omega_2)\,N_n(\mathfrak{T}(z;\ n\omega_1,\ \omega_2))^2 = C Z_n(\mathfrak{T}(z;\ n\omega_1,\ \omega_2))^2 \mathfrak{T}(z;\ n\omega_1,\ \omega_2)$$

ein. Die Koeffizientenvergleichung rechts und links ergibt, sofern (60) berücksichtigt wird, daß alle Koeffizienten von Z_n und N_n rationale Funktionen von $\sqrt{\pm C}$, $\mathfrak{t}(n\omega_1,\ \omega_2)$ und $\mathfrak{t}(\omega_1,\ \omega_2)$ sind mit rationalen Zahlkoeffizienten.

113. Satz: *Die Funktion* $\mathfrak{T}(z;\ \omega_1,\ \omega_2)$ *ist eine rationale Funktion von* $\mathfrak{T}(z;\ n\omega_1,\ \omega_2)$, *deren Koeffizienten rationale Funktionen von* $\sqrt{\pm C}$, $\mathfrak{t}(n\omega_1,\ \omega_2)$, $\mathfrak{t}(\omega_1,\ \omega_2)$ *mit rationalen Zahlkoeffizienten sind. Dabei ist:*

$$\pm\sqrt{\pm C} = Z_n(O)^{-1} = \prod_{h=1}^{\frac{n-1}{2}} \mathfrak{T}(h\omega_1;\ n\omega_1,\ \omega_2)^{-1}.$$

6. Die Modulfunktion t.

Nach Definition (36) ist:

$$\mathfrak{t} = \frac{4\cdot 3\,\wp\left(\frac{\omega_3}{2}\right)}{\wp\left(\frac{\omega_3}{4}\right) - \wp\left(\frac{\omega_3}{2}\right)}.$$

t ist eine homogene Funktion 0^{ter} Ordnung von ω_1 und ω_2, hängt somit nur von dem Verhältnis $\omega_2 : \omega_1$ ab.

114. Satz: t *ist eine Modulfunktion 4. Stufe, d. h. bleibt ungeändert bei jeder Substitution der Gruppe* $\mathfrak{G}^{(4)}$.

Denn ist $S = \begin{pmatrix} \alpha^{(4)} & \beta^{(4)} \\ \gamma^{(4)} & \delta^{(4)} \end{pmatrix}$ in $\mathfrak{G}^{(4)}$, also: $\alpha^{(4)} \equiv \delta^{(4)} \equiv \pm 1$, $\beta^{(4)} \equiv \gamma^{(4)} \equiv 0 \pmod 4$, so ist: $\bar\omega_2 = \alpha^{(4)}\omega_2 + \beta^{(4)}\omega_1$, $\bar\omega_1 = \gamma^{(4)}\omega_2 + \delta^{(4)}\omega_1$,

und wegen Satz 96:

$$\wp\left(\frac{\bar\omega_3}{2}\right) = \wp\left(\frac{\bar\omega_1 + \bar\omega_2}{2}\right) = \wp\left(\frac{\omega_1+\omega_2}{2} + \left(\frac{\beta^{(4)}}{2} + \frac{\delta^{(4)}-1}{2}\right)\omega_1 + \left(\frac{\alpha^{(4)}-1}{2} + \frac{\gamma^{(4)}}{2}\right)\omega_2\right)$$
$$= \wp\left(\frac{\omega_1+\omega_2}{2}\right) = \wp\left(\frac{\omega_3}{2}\right),$$

$$\wp\left(\frac{\bar\omega}{4}\right) = \wp\left(\frac{\bar\omega_1+\bar\omega_2}{4}\right) = \wp\left(\pm\frac{\omega_1+\omega_2}{4} + \left(\frac{\beta^{(4)}}{4} + \frac{\delta^{(4)}\mp 1}{4}\right)\omega_1 + \left(\frac{\alpha^{(4)}\mp 1}{4} + \frac{\gamma^{(4)}}{4}\right)\omega_2\right)$$
$$= \wp\left(\frac{\omega_1+\omega_2}{4}\right) = \wp\left(\frac{\omega_3}{4}\right).$$

Ferner ergeben die Formeln (39) und (40):

$$\frac{g_2}{e_3^{\,2}} = 12\,\frac{\mathfrak{t}^2 - 3\cdot 2^4}{\mathfrak{t}^2}, \qquad \frac{g_3}{e_3^{\,3}} = 4\,\frac{2^4\cdot 3^2 - 2\mathfrak{t}^2}{\mathfrak{t}^2},$$

für die Funktion $G(\omega_1, \omega_2)$ den Wert (11):

$$\frac{G}{e_3^{\,6}} = \frac{1}{16}\left(\left(\frac{g_2}{e_3^{\,2}}\right)^3 - 27\left(\frac{g_3}{e_3^{\,3}}\right)^2\right) = \frac{3^6\cdot 2^8}{\mathfrak{t}^6}(\mathfrak{t}^2 - 2^6).$$

Man kann daher nach (13) die vollständige Invariante $j(\omega_1, \omega_2)$ ebenfalls durch t einfach berechnen:

$$j(\omega_1, \omega_2) = \frac{4\cdot 27\cdot g_2^{\,3}}{G} = \frac{(\mathfrak{t}^2 - 3\cdot 2^4)^3}{\mathfrak{t}^2 - 2^6}. \tag{63}$$

Umgekehrt genügt t der Gleichung 6. Grades:

$$\mathfrak{t}^6 - 3^2 4^2 \mathfrak{t}^4 + (3^3\cdot 2^8 - j(\omega_1, \omega_2))\mathfrak{t}^2 - (3^3 2^6 - j(\omega_1, \omega_2))2^6 = 0. \tag{64}$$

Daraus erkennt man, daß bei Anwendung aller Substitutionen S der Modulgruppe t höchstens 6 verschiedene Werte annehmen kann. Je zwei sind entgegengesetzt gleich. Für $x = t^2 - 3 \cdot 4^2$ lautet die Gleichung:

$$x^3 - j(\omega_1, \omega_2)x + 4^2 \cdot j(\omega_1, \omega_2) = 0,$$

deren Diskriminante den Wert hat:

$$4(j(\omega_1, \omega_2)^3 - 3^3 \cdot 4^3 \cdot j(\omega_1, \omega_2)^2) = 4j(\omega_1, \omega_2)^2(j(\omega_1, \omega_2) - 27 \cdot 2^6)$$
$$= \frac{2^8 \cdot 3^{12} \cdot g_2{}^6 g_3{}^2}{G^5}.$$

Dieselbe ist somit nur null, falls g_2 oder g_3 null ist. Das ist nur für $\omega_2 : \omega_1 = i$ und $\omega_2 : \omega_1 = \varrho$, wo ϱ die dritte Einheitswurzel ist, und den ähnlichen Punkten möglich. Denn $j(\omega_1, \omega_2)$ nimmt im D.-B. nach Satz 10 die Werte 0 und $2^6 3^3$ nur einmal an, somit ist g_2 und g_3 nur einmal null. Nur in diesen beiden Fällen können somit zwei der Wurzeln von (64) einander gleich werden.

a) $\omega_1 = 1$, $\omega_2 = i$, $g_3 = 0$, $j(1, i) = 2^6 3^3$. Dann besitzt (64) die Doppelwurzeln: $\pm 2 \cdot 3\sqrt{2}$, 0.

Aus der Homogenität -2. Dimension von $\wp(z)$ erkennt man, daß $\wp\left(\frac{1+i}{2}, 1, i\right) = \wp\left(\frac{i-1}{2}, i, -1\right)$ gleich seinem entgegengesetzten Werte, also gleich null ist. Somit muß:

$$t(1, i) = 0, \quad t(1, \pm 1 + i) = \pm 2 \cdot 3 \cdot \sqrt{2}$$

sein. Nur für diesen Fall kann $t = 0$ sein.

b) $\omega_1 = 1$, $\omega_2 = \varrho$, $g_2 = 0$, $j(1, \varrho) = 0$. (64) besitzt die beiden dreifachen Wurzeln:

$$t\left(1, \frac{\mp 1 + \sqrt{-3}}{2}\right) = \pm 4\sqrt{3}.$$

c) $g_2 g_3 \neq 0$. Mit Hilfe der *Gaußschen* Transformation kann man $j\left(\frac{\omega_2 + \omega_1}{4\omega_1}\right)$ durch t darstellen. Wir betrachten hierzu die Funktion

$$\mathfrak{T}(z) = \mathfrak{T}(z; 2\omega_1, \omega_2 - \omega_1).$$

Die zu ihren Perioden gehörende Funktion t sei:

$$\bar{t} = t(2\omega_1, \omega_2 - \omega_1).$$

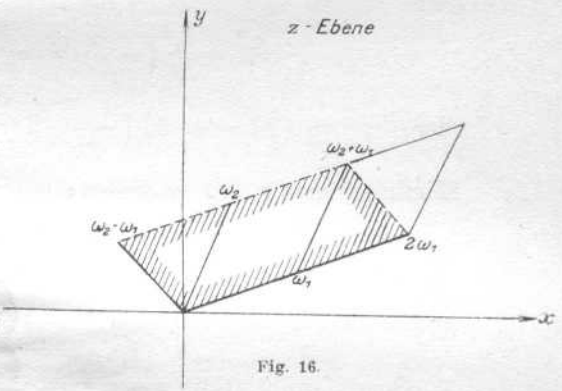

Fig. 16.

Das Periodenparallelogramm von $\bar{\mathfrak{T}}$ ist doppelt so groß, wie dasjenige von $\mathfrak{T}$. Wir wählen es so, wie es Figur 16 zeigt.

$\overline{\mathfrak{T}}$ hat bei $z = 0$ eine Nullstelle 2. Ordnung, bei $z = \frac{\omega_1 + \omega_2}{2} = \frac{\omega_3}{2}$ einen Pol 2. Ordnung. Für $z = \omega_1$ und $z = \frac{\omega_2 - \omega_1}{2}$ nimmt $\overline{\mathfrak{T}}$ die Werte $\overline{\mathfrak{T}}(\omega_1)$ und $\overline{\mathfrak{T}}\left(\frac{\omega_2 - \omega_1}{2}\right) = \overline{\mathfrak{T}}(\omega_1)^{-1}$ von 2. Ordnung an, und es ist:

$$4\overline{\mathfrak{T}}(\omega_1)^2 + \bar{t}\,\overline{\mathfrak{T}}(\omega_1) + 4 = 0. \tag{65}$$

(Satz 106 und Formel (44)') Dagegen hat $\mathfrak{T}$ im selben Periodenparallelogramm die beiden Nullstellen $z = 0$ und $z = \omega_1$ von 2. Ordnung und die beiden Pole $z = \frac{\omega_3}{2}$ und $z = \frac{\omega_3}{2} - \omega_1 = \frac{\omega_2 - \omega_1}{2}$ von 2. Ordnung. $\mathfrak{T}$ gehört dem Funktionskörper von $\overline{\mathfrak{T}}$ an, somit muß wieder:

$$\mathfrak{T}(z) = C\,\frac{\overline{\mathfrak{T}}(z)\left(\overline{\mathfrak{T}}(z) - \overline{\mathfrak{T}}(\omega_1)\right)}{1 - \overline{\mathfrak{T}}(z)\,\overline{\mathfrak{T}}(\omega_1)}$$

sein, wo C von z unabhängig ist. Um C zu berechnen, setzen wir $z = \frac{\omega_3}{4}$. Dann wird $\overline{\mathfrak{T}}\left(\frac{\omega_3}{4}\right) = \mathfrak{T}\left(\frac{\omega_3}{4}\right) = 1$, und $C = 1$. Somit ist:

$$\mathfrak{T}(z) = \frac{\overline{\mathfrak{T}}(z)\left(\overline{\mathfrak{T}}(z) - \overline{\mathfrak{T}}(\omega_1)\right)}{1 - \overline{\mathfrak{T}}(z)\,\overline{\mathfrak{T}}(\omega_1)}. \tag{66}$$

In (66) setzen wir die Reihenentwicklungen für $\overline{\mathfrak{T}}$ und $\mathfrak{T}$ ein, indem wir alle Größen von $\overline{\mathfrak{T}}$ überstreichen (Satz 107):

$$\overline{\mathfrak{T}}(z) = \bar{\xi}^2 + \frac{\bar{t}}{4\cdot 3}\bar{\xi}^4 + \cdots, \quad \bar{\xi}^2 = 4\cdot\frac{3\,\bar{e}_3}{\bar{t}}\,z^2,$$

$$\mathfrak{T}(z) = \xi^2 + \frac{t}{4\cdot 3}\xi^4 + \cdots, \quad \xi^2 = 4\cdot\frac{3\,e_3}{t}\,z^2.$$

Durch Koeffizientenvergleichung ergibt sich:

$$\frac{e_3}{t} = -\frac{\bar{e}_3}{\bar{t}}\,\overline{\mathfrak{T}}(\omega_1), \quad \text{oder} \quad \frac{e_3}{\bar{e}_3} = -\frac{t}{\bar{t}}\,\overline{\mathfrak{T}}(\omega_1),$$

$$\frac{t}{4\cdot 3}\frac{e_3^2}{t^2} = \frac{\bar{e}_3^2}{\bar{t}^2}\left(-\frac{\bar{t}}{4\cdot 3}\,\overline{\mathfrak{T}}(\omega_1) + 1 - \overline{\mathfrak{T}}(\omega_1)^2\right)$$

oder

$$\left(\frac{e_3}{\bar{e}_3}\right)^2 = 4\cdot 3\frac{t}{\bar{t}^2}\left(-\frac{\bar{t}}{4\cdot 3}\,\overline{\mathfrak{T}}(\omega_1) + 1 - \overline{\mathfrak{T}}(\omega_1)^2\right).$$

Eliminiert man $e_3 : \bar{e}_3$, so findet man:

$$(t + 2^2\cdot 3)\,\overline{\mathfrak{T}}(\omega_1)^2 + \bar{t}\,\overline{\mathfrak{T}}(\omega_1) - 2^2\cdot 3 = 0.$$

Mit Berücksichtigung von (65) läßt sich jetzt $\bar{t}$ durch t ausdrücken:

$$\bar{t}^2 = \frac{(t + 2^5\cdot 3)^2}{(t + 2^5)}. \tag{67}$$

Somit ergibt (63), wenn man in ihr für ω_1, ω_2 die Perioden $2\omega_1$, $\omega_2 - \omega_1$ setzt:

$$j\left(\frac{\omega_2 + \omega_1}{2\omega_1}\right) = j\left(\frac{\frac{\omega_2}{\omega_1} + 1}{2}\right) = \frac{(t^2 + 3\cdot 2^6)^3}{(t^2 - 2^6)^2}. \tag{68}$$

Wiederholt man die Operation, indem man aufs neue statt $2\omega_1, \omega_2 - \omega_1$ die Perioden $4\omega_1, (\omega_2 - \omega_1) - 2\omega_1 = \omega_2 - 3\omega_1$ setzt, so findet man durch Iteration:

$$(69) \qquad j\left(\frac{\omega_2 + \omega_1}{4\omega_1}\right) = j\left(\frac{\frac{\omega_2}{\omega_1} + 1}{4}\right) = \frac{(t^2 + 3\cdot 5\cdot 2^4 t + 3\cdot 11\cdot 2^6)^3}{(t + 2^3)(t - 2^5)^4}.$$

$j\left(\frac{\omega_2 + \omega_1}{4\omega_1}\right)$ gehört daher dem Körper von t an. Umgekehrt kann man t aus (63) und (69) rational durch $j\left(\frac{\omega_2}{\omega_1}\right)$ und $j\left(\frac{\omega_2 + \omega_1}{4\omega_1}\right)$ ausdrücken. Die Koeffizienten aller Funktionen sind *rationale* Zahlen. Die letzteren sind aber sehr groß und umständlich zu berechnen. Schon für t^2 erhält man die Formel:

$$\bar{j} = j\left(\frac{\omega_2 + \omega_1}{2\omega_1}\right):$$

$$t^2 = 2^6 \frac{j\bar{j}^2 - 2^6\cdot 11 j^2 - 2^4\cdot 3\cdot 31\cdot j\bar{j} - j^2 - 2^{10}\cdot 3^3\cdot 5\cdot 7\cdot 13\bar{j} + 2^6\cdot 3^3\cdot 5\cdot 7^2 j + 2^{14}\cdot 3^7\cdot 5^4}{j\bar{j}^2 - 2^8\cdot 3\cdot \bar{j}^2 - 2^4\cdot 3\cdot 31\cdot j\bar{j} - j^2 - 2^{15}\cdot 3^2\cdot 5\cdot 17\bar{j} + 2^9\cdot 3^2\cdot 5\cdot 7\cdot j - 2^{17}\cdot 3^5\cdot 5^4}.$$

Man kann aber die Tatsache, daß sich t rational durch $j\left(\frac{\omega_2}{\omega_1}\right)$ und $j\left(\frac{\omega_2 + \omega_1}{4\omega_1}\right)$ ausdrücken läßt, auch so einsehen (daß dann die Koeffizienten rationale Zahlen sind, ergibt sich aus obigem): Übt man auf $t(\omega_1, \omega_2)$ alle Substitutionen der Modulgruppe aus, so nimmt t nur die 6 voneinander verschiedenen Wurzelwerte der Gleichung (64) an. Andererseits ist $j\left(\frac{\frac{\omega_2}{\omega_1} + 1}{4}\right)$ Wurzel der zu $n = 4$ gehörenden Transformationsgleichung 6. Grades, deren Wurzeln sind:

$$j\left(\frac{\bar{\omega} + 1}{4}\right),\quad j\left(\frac{\bar{\omega} + 2}{4}\right),\quad j\left(\frac{\bar{\omega} + 3}{4}\right),\quad j\left(\frac{\bar{\omega}}{4}\right),\quad j(4\bar{\omega}),\quad j\left(\frac{2\bar{\omega} + 1}{2}\right),\quad \bar{\omega} = \frac{\omega_2}{\omega_1}.$$

Diese sind alle voneinander verschieden (Satz 29) und werden durch die Modulsubstitutionen:

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\quad \begin{pmatrix}1 & -1\\ 2 & -1\end{pmatrix},\quad \begin{pmatrix}2 & -3\\ -1 & 2\end{pmatrix},\quad \begin{pmatrix}0 & -1\\ 1 & 1\end{pmatrix},\quad \begin{pmatrix}1 & 1\\ -1 & 0\end{pmatrix},\quad \begin{pmatrix}1 & -2\\ 1 & -1\end{pmatrix},$$

aus der ersten erhalten. Durch dieselben S geht aber t in die 6 Wurzeln

$$t(\omega_1, \omega_2),\quad t(2\omega_2 - \omega_1, \omega_2 - \omega_1),\quad t(-\omega_2 + 2\omega_1, 2\omega_2 - 3\omega_1),$$
$$t(\omega_2 + \omega_1, -\omega_1),\quad t(-\omega_2, \omega_1 + \omega_2),\quad t(\omega_2 - \omega_1, \omega_2 - 2\omega_1)$$

über, die alle voneinander verschieden sind. Somit können, bei festgehaltenem $j\left(\frac{\bar{\omega} + 1}{4}\right)$ die Gleichungen (63) und (69) nur eine Wurzel gemein haben, und die Darstellung von t ist gewährleistet.

Durch die Modulsubstitution:

$$\begin{aligned}\bar{\omega}_2 &= 2\omega_2 - 3\omega_1,\\ \bar{\omega}_1 &= -\omega_2 + 2\omega_1,\end{aligned}\qquad \begin{vmatrix}2 & -3\\ -1 & 2\end{vmatrix} = +1,$$

geht t in $$t(\omega_1, \omega_2) = \frac{4 \cdot 3\wp\left(\frac{\omega_3}{2}\right)}{\wp\left(\frac{\omega_2 - \omega_1}{4}\right) - \wp\left(\frac{\omega_3}{2}\right)}$$

über. Nach (38) ist:

$$\frac{\wp\left(\frac{\omega_3}{4}\right) - \wp\left(\frac{\omega_3}{2}\right)}{\wp(z) - \wp\left(\frac{\omega_3}{2}\right)} = \frac{\wp\left(z + \frac{\omega_3}{2}\right) - \wp\left(\frac{\omega_3}{2}\right)}{\wp\left(\frac{\omega_3}{4}\right) - \wp\left(\frac{\omega_3}{2}\right)},$$

also für $z = \frac{\omega_2 - \omega_1}{4}$:

$$\wp\left(\frac{\omega_2 - \omega_1}{4}\right) - \wp\left(\frac{\omega_3}{2}\right) = -\left(\wp\left(\frac{\omega_3}{4}\right) - \wp\left(\frac{\omega_3}{2}\right)\right).$$

Denn das Pluszeichen kann nicht auftreten, da nach Satz 100 $\wp\left(\frac{\omega_3}{4}\right) + \wp\left(\frac{\omega_2 - \omega_1}{4}\right)$ sein muß. Somit ist

$$t(\bar{\omega}_1, \omega_2) = -t(\omega_1, \omega_2).$$

Andererseits geht $j\left(\frac{\bar{\omega}+1}{4}\right)$ durch dieselbe Substitution über in:

$$j\left(\frac{\frac{2\bar{\omega}-3}{-\bar{\omega}+2}+1}{4}\right) = j\left(\frac{\bar{\omega}-1}{4(-\bar{\omega}+2)}\right) = j\left(\frac{\frac{\bar{\omega}-1}{4}}{-4\frac{\bar{\omega}-1}{4}+1}\right) = j\left(\frac{\omega-1}{4}\right).$$

Daher ergibt (69):

$$j\left(\frac{\bar{\omega}-1}{4}\right) = j\left(\frac{\omega_2 - \omega_1}{4\omega_1}\right) = \frac{(t^2 - 3\cdot 5\cdot 2^4 \cdot t + 3\cdot 11\cdot 2^6)^3}{(-t+2^3)(-t-2^3)^4}.$$

115. Satz: *$j\left(\frac{\omega_2+\omega_1}{4\omega_1}\right)$ und $j\left(\frac{\omega_2-\omega_1}{4\omega_1}\right)$ sind rationale Funktionen von* t *mit rationalen Zahlkoeffizienten, und umgekehrt ist* t *eine rationale Funktion von $j\left(\frac{\omega_2}{\omega_1}\right)$ und $j\left(\frac{\omega_2+\omega_1}{4\omega_1}\right)$ oder von $j\left(\frac{\omega_2}{\omega_1}\right)$ und $j\left(\frac{\omega_2-\omega_1}{4\omega_1}\right)$ mit rationalen Zahlkoeffizienten.*

Daraus wird bewiesen, daß den Funktionen $j\left(\frac{\bar{\omega}}{4}\right)$ und $j\left(\frac{\bar{\omega}+2}{4}\right)$ und entsprechend den Funktionen $j(4\omega)$ und $j\left(\frac{2\bar{\omega}+1}{2}\right)$ entgegengesetzte gleiche Wurzeln von (64) entsprechen.

Man kann alle Wurzeln von (64) durch eine einzige ausdrücken. Sind t und $\bar{t}$ zwei nicht entgegengesetzt gleiche Wurzeln, so ergibt die Subtraktion der beiden Gleichungen von t und $\bar{t}$:

$$\bar{t}^4 + \bar{t}^2 t^2 + t^4 - 3^2 \cdot 2^4(\bar{t}^2 + t^2) + (3^3 2^8 - j(\omega_1, \omega_2)) = 0.$$

Man setzt hier für $j(\omega_1, \omega_2)$ den Wert von (63) ein:

$$\bar{t}^4 - (3^2 \cdot 2^4 - t^2)\bar{t}^2 - \frac{2^6}{t^2 - 2^6}(t^2 - 3^2 \cdot 2^3)^2 = 0,$$

woraus durch Auflösung:

$$(70)\quad 2\bar{t}^2 = 3^2 \cdot 2^4 - t^2 \pm \frac{t(t^2 - 3\cdot 2^4)}{\sqrt{t^2 - 2^6}},\quad \bar{t} = (\pm)\left(\frac{t}{2} \pm \frac{3}{2}\sqrt{t^2 - 2^6}\right)\sqrt{\frac{\pm t - \sqrt{t^2 - 2^6}}{2\sqrt{t^2 - 2^6}}}$$

erhalten wird.

V. Die komplexe Multiplikation der elliptischen Funktionen.

1. Strahlen im quadratischen Körper.

Es sei $\mathfrak{f}$ ein beliebiges Ideal in $k(\sqrt{m})$.

18. Definition: *Alle Zahlen* ξ *von* $k(\sqrt{m})$, *die der Kongruenz genügen:*

$$\xi \equiv 1 \pmod{\mathfrak{f}},$$

bilden den Strahl $s(\mathfrak{f})$. $\mathfrak{f}$ *heißt der Führer von* $s(\mathfrak{f})$, *jede Zahl von* $s(\mathfrak{f})$ *heißt Strahlzahl.*

Aus den Sätzen 58 und 59 über Kongruenzen folgt:

116. Satz: *Produkt und Quotient zweier Strahlzahlen von* $s(\mathfrak{f})$ *ist wieder eine Strahlzahl von* $s(\mathfrak{f})$.

Eine Strahlzahl, die zugleich Einheit ist, heißt *Strahleinheit von* $s(\mathfrak{f})$.

19. Definition: *Zwei zum Führer* $\mathfrak{f}$ *teilerfremde Ideale* $\mathfrak{a}$ *und* $\mathfrak{b}$ *von* $k(\sqrt{m})$ *heißen äquivalent* (mod. $\mathfrak{f}$), *wenn es zwei ganze Zahlen* α *und* β *gibt, so daß:*

1. $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$, *und*
2. *die Zahl* $\alpha : \beta$ *eine Strahlzahl von* $s(\mathfrak{f})$ *ist.*

$\alpha : \beta$ ist nur bis auf einen Einheitsfaktor bestimmt. Wenn daher $\mathfrak{a}$ und $\mathfrak{b}$ die Bedingung 1. erfüllen, so darf man $\alpha : \beta$ noch mit einer beliebigen Einheit multiplizieren, um zu sehen, ob 2. erfüllbar ist.

Für zwei (mod. $\mathfrak{f}$) äquivalente Ideale $\mathfrak{a}$ und $\mathfrak{b}$ schreiben wir:

$$\mathfrak{a} \cong \mathfrak{b} \pmod{\mathfrak{f}}.$$

Aus Satz 116 ergibt sich:

117. Satz: *Zwei Ideale, die einem dritten* (mod. $\mathfrak{f}$) *äquivalent sind, sind auch untereinander* (mod. $\mathfrak{f}$) *äquivalent.*

Denn aus: $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$, $(\bar{\alpha})\mathfrak{a} = (\gamma)\mathfrak{c}$

folgt: $(\bar{\alpha}\beta)\mathfrak{b} = (\alpha\gamma)\mathfrak{c}$ und $\bar{\alpha}\beta : \alpha\gamma = \dfrac{\bar{\alpha}}{\gamma} : \dfrac{\alpha}{\beta}$.

Mit Hilfe von Satz 117 kann man alle zu $\mathfrak{f}$ teilerfremden Ideale von $k(\sqrt{m})$ in *Strahlklassen* (mod. $\mathfrak{f}$) einteilen, indem man alle äquivalenten Ideale in eine Klasse tut. Die Anzahl der Strahlklassen, in die alle Ideale zerfallen, heißt die *Strahlklassenzahl* h_s oder $h_s(\mathfrak{f})$.

118. Satz: *Die Strahlklassenzahl h_s von $s(\mathfrak{f})$ in $k(\sqrt{m})$ ist endlich und gleich:*

$$h_s = \frac{e_s}{e}\varphi(\mathfrak{f})h,$$

wo e die Anzahl der Einheiten in $k(\sqrt{m})$, e_s der Strahleinheiten in $s(\mathfrak{f})$, $\varphi(\mathfrak{f})$ die Anzahl der zu $\mathfrak{f}$ teilerfremden (mod. $\mathfrak{f}$) *inkongruenten Zahlen und h die Klassenzahl von $k(\sqrt{m})$ ist.*

Im Falle $m \neq -1$ und $m \neq -3$ ist $e = 2$, also:

$h_s = \frac{1}{2}\varphi(\mathfrak{f})h$, falls $\mathfrak{f}$ kein Teiler von (2) ist,

$h_s = \varphi(\mathfrak{f})h$, falls $\mathfrak{f}$ ein Teiler von (2) ist.

Im *Falle* $m = -1$ ist $e = 4$, also:

$h_s = \frac{1}{4}\varphi(\mathfrak{f})h$, falls $\mathfrak{f}$ kein Teiler von (2) ist,
$h_s = h$, falls $\mathfrak{f} = (1+i)$ oder $= (2)$ ist. $\qquad h = 1.$

Im *Falle* $m = -3$ ist $e = 6$, also:

$h_s = \frac{1}{6}\varphi(\mathfrak{f})h$, falls $\mathfrak{f} \neq \left(\frac{-3+\sqrt{-3}}{2}\right), \neq (2)$ ist,

$h_s = \frac{1}{2}\varphi(\mathfrak{f})h = h$, falls $\mathfrak{f} = \left(\frac{-3+\sqrt{-3}}{2}\right)$ ist. $\qquad h = 1.$

$h_s = \frac{1}{3}\varphi(\mathfrak{f})h$, falls $\mathfrak{f} = (2)$ ist.

Beweis von Satz 118: Damit $\mathfrak{a}$ und $\mathfrak{b}$ (mod. $\mathfrak{f}$) äquivalent sind, müssen sie sicherlich auch im $k(\sqrt{m})$ äquivalent sein (Bedingung 1. der Definition 19 und die Definition S. 55). Wir brauchen deshalb nur zu bestimmen, in wie viel Strahlklassen eine Körperklasse zerfällt. Nun gibt es $\varphi(\mathfrak{f})$ verschiedene, (mod. $\mathfrak{f}$) inkongruente Werte, die $\alpha : \beta$ annehmen kann. Somit zerfällt eine Klasse in höchstens $\varphi(\mathfrak{f})$ Strahlklassen.

Es gibt $e : e_s$ Einheiten in $k(\sqrt{m})$, die mit Ausnahme von $+1$ nicht Strahleinheiten sind, und die (mod. $\mathfrak{f}$) inkongruent sind. Denn die Anzahl der Einheiten ist endlich, und sie bilden, ebenso wie die Strahleinheiten, eine Gruppe. Die Gruppe der Strahleinheiten ist eine Untergruppe der Gruppe aller Einheiten vom Index $e : e_s$. Es gibt somit $e : e_s$ Einheiten, die mit den Strahleinheiten multipliziert alle Einheiten ergeben. Wären zwei von diesen kongruent (mod. $\mathfrak{f}$), so wäre ihr Quotient eine Strahleinheit und die beiden würden, falls man die im Nenner stehende mit der Strahleinheit multipliziert, dieselbe Einheit ergeben gegen die Annahme.

Da nun $\alpha : \beta$ nur bis auf einen Einheitsfaktor gegeben ist, so erkennt man, daß je $e : e_s$ Kongruenzklassen (mod. $\mathfrak{f}$) äquivalente Ideale ergeben. Also zerfällt jede Klasse in genau $\frac{e_s}{e}\varphi(\mathfrak{f})$ Strahlklassen, und die h Klassen ergeben:

$$\frac{e_s}{e}\varphi(\mathfrak{f})h$$

Strahlklassen.

119. **Satz:** *Ist* $\mathfrak{a} \cong \mathfrak{b}$, $\bar{\mathfrak{a}} \cong \bar{\mathfrak{b}}$ (mod. $\mathfrak{f}$), *so ist auch:*

$$\mathfrak{a}\bar{\mathfrak{a}} \cong \mathfrak{b}\bar{\mathfrak{b}} \pmod{\mathfrak{f}}.$$

Aus den Annahmen folgt, daß:

$$(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}, \quad (\bar{\alpha})\bar{\mathfrak{a}} = (\bar{\beta})\bar{\mathfrak{b}},$$

wo $\alpha : \beta$ und $\bar{\alpha} : \bar{\beta}$ Strahlzahlen sind. Somit:

$$(\alpha\bar{\alpha})\mathfrak{a}\bar{\mathfrak{a}} = (\beta\bar{\beta})\mathfrak{b}\bar{\mathfrak{b}}$$

und $\alpha\bar{\alpha} : \beta\bar{\beta} = \alpha : \beta \cdot \bar{\alpha} : \bar{\beta}$ ist nach Satz 116 wieder Strahlzahl.

Man kann jetzt wieder als Produkt zweier Strahlklassen $\mathfrak{k}_1$ und $\mathfrak{k}_2$ die Klasse $\mathfrak{k}_3$ bezeichnen, deren Ideale dem Produkt der Ideale von $\mathfrak{k}_1$ und $\mathfrak{k}_2$ (mod. $\mathfrak{f}$) äquivalent sind:

$$\mathfrak{k}_3 = \mathfrak{k}_1 \mathfrak{k}_2.$$

Genau wie früher gilt dann:

120. **Satz:** *Die Strahlklassen von* $s(\mathfrak{f})$ *bilden in bezug auf ihre Multiplikation eine Abelsche Gruppe, deren Ordnung gleich der Strahlklassenzahl* h_s *ist.*

Das Einheitselement der Gruppe ist die Hauptklasse des Strahls, deren Ideale Hauptideale in $k(\sqrt{m})$ sind, und die in der Gestalt (α) gegeben werden können, wo α eine Strahlzahl ist.

2. Der singuläre Körper von t.

Es sei $\mathfrak{w} = (\omega_1, \omega_2)$ ein durch seine Basis gegebenes, zu (2) und $\mathfrak{f}$ teilerfremdes Ideal von $k(\sqrt{m})$. Nach Satz 115 gehört $\mathfrak{t}(\omega_1, \omega_2)$ dem Körper von $j\left(\frac{\omega_2}{\omega_1}\right)$ und $j\left(\frac{\omega_2 \pm \omega_1}{4\omega_1}\right)$ an. $j\left(\frac{\omega_2}{\omega_1}\right)$ ist gemäß Satz 68 und den folgenden Ausführungen eine Zahl des Klassenkörpers von $k(\sqrt{m})$. Es fragt sich, welchen Körper $j\left(\frac{\omega_2 \pm \omega_1}{4\omega_1}\right)$ festlegt?

a) $m \equiv 1 \pmod 8$. Die Basis der ganzen Zahlen wird durch 1, $\omega = \frac{-1+\sqrt{m}}{2}$ gegeben, und (2) ist nach Satz 52 Produkt von zwei voneinander verschiedenen Primidealen. Wir wählen in $\mathfrak{w}$ eine kanonische Basis (Seite 53) w, $s + \omega$. wo $(s + \omega)(s + \omega') = s(s - 1) + \frac{1-m}{4} \equiv 0$ (mod. w) sein muß. Setzt man dann:

$$\mathfrak{w} = (4\omega_1, \omega_2 \pm \omega_1) = (4w, s \pm w + \omega),$$

so ist auch $\bar{\mathfrak{w}}$ ein durch seine kanonische Basis gegebenes Ideal, falls man das obere oder untere Vorzeichen richtig wählt. Denn es ist:

$$(s \pm w + \omega)(s \pm w + \omega') = (s \pm w)^2 - (s \pm w) + \frac{1-m}{4}$$

$$= (s \pm w - 1)(s \pm w) + \frac{1-m}{4} \equiv 0 \pmod{4w};$$

diese Kongruenz ist für w erfüllt, und da (4) zu w teilerfremd ist, braucht man nur das Vorzeichen so zu wählen, daß sie auch für (4) erfüllt ist. Ist $\bar{\mathfrak{f}}$ die Klasse von $\mathfrak{w}$, so ist daher:

$$j\left(\frac{\omega_2 \pm \omega_1}{4\omega_1}\right) = j(\bar{\mathfrak{f}}),$$

und $j\left(\frac{\omega_2 \pm \omega_1}{4\omega_1}\right)$ gehört ebenfalls dem Klassenkörper an. t *ist somit, falls* ω_1, ω_2 *eine kanonische Basis ist, eine Zahl des Klassenkörpers von* $k(\sqrt{m})$. Die anderen Basen von $\mathfrak{w}$ erhält man aus der kanonischen Basis nach Satz 50, indem man alle Modulsubstitutionen S auf sie anwendet. Dadurch geht $j\left(\frac{\omega_2 \pm \omega_1}{4\omega_1}\right)$ nach Kap. 4, § 6, S. 107 in die vier Werte:

$$j\left(\frac{\omega_2}{4\omega_1}\right), \quad j\left(\frac{\frac{\omega_2}{\omega_1}+2}{4}\right), \quad j\left(4\frac{\omega_2}{\omega_1}\right), \quad j\left(\frac{2\frac{\omega_2}{\omega_1}+1}{2}\right),$$

über, von denen je zwei entgegengesetzt gleiche Werte von t ergeben. Den Werten $j\left(\frac{\omega_2}{4\omega_1}\right)$ und $j\left(\frac{\omega_2 + 2\omega_1}{4\omega_1}\right)$ entspricht die Basisdarstellung:

$$\mathfrak{w} = (w, s \pm w + \omega),$$

die ebenfalls kanonisch ist. Daher ist auch in diesem Falle t eine Zahl des Klassenkörpers.

Anders dagegen im Falle $j\left(4\frac{\omega_2}{\omega_1}\right)$. In diesem Falle ist $\mathfrak{w}$ durch die Basis:

$$\mathfrak{w} = (-s - \omega, w \pm s \pm \omega)$$

gegeben. Setzen wir das zum Führer 4 gehörige Ringideal, das $\mathfrak{w}$ entspricht, gleich $\mathfrak{w}_r$:

$$\mathfrak{w}_r = (w, 4s + 4\omega),$$

und ist $\mathfrak{f}_r$ seine Ringklasse in $r(4)$, so wird:

$$j\left(\frac{4\omega_2}{\omega_1}\right) = j\left(\frac{4s + 4\omega}{w}\right) = j(\mathfrak{f}_r).$$

$j(\mathfrak{f}_r)$ ist eine bestimmende Zahl des Ringklassenkörpers in bezug auf $k(\sqrt{m})$, der Relativgrad ist $h_r(4)$, wo nach Satz 84:

$$h_r(4) = 4\left(1 - \left(\frac{m}{2}\right)\frac{1}{2}\right)h = 4\left(1 - \frac{1}{2}\right)h = 2h$$

ist. Da derselbe den Klassenkörper von $k(\sqrt{m})$ in sich enthält, wie Gleichung (63) zeigt, so ist t *eine bestimmende Zahl des Ringklassenkörpers von* $r(4)$. *Die Basis von* $\mathfrak{w}$ *ist in diesem Falle dadurch eindeutig charakterisiert, daß eine Basiszahl durch das eine Primideal von* (2), *die andere durch das andere Primideal von* (2) *teilbar ist.* Wir setzen von nun an immer voraus, daß die Wahl der Basis in dieser Form getroffen sei. t hängt dann nur von der Ringklasse von $\mathfrak{w}_r$ ab und wir schreiben:

$$\mathrm{t} = \mathrm{t}(\mathfrak{f}_r).$$

b) $m \equiv 5 \pmod 8$. Es ist $1, \omega = \frac{-1+\sqrt{m}}{2}$ eine Basis der ganzen Zahlen, dagegen ist jetzt (2) selbst Primideal. Wir nehmen wieder zuerst $\mathfrak{w}$ durch seine kanonische Basis gegeben an:

$$\mathfrak{w} = (w, s+\omega), \quad (s+\omega)(s+\omega') \equiv 0 \pmod w.$$

Ist dann:

$$(s+w+\omega)(s+w+\omega') = (s+w)(s+w-1) + \frac{1-m}{4} = w\bar{w},$$

so muß w *ungerade* sein, da $\frac{1-m}{4}$ ungerade ist, und

$$\mathfrak{w} = (w, s+w+\omega)$$

ist ein durch eine kanonische Basis gegebenes Ideal von $k(\sqrt{m})$, das zu (2) teilerfremd ist. Also ist:

$$j\left(\frac{\omega_2+\omega_1}{4\omega_1}\right) = j\left(\frac{s+w+\omega}{4w}\right) = j\left(\frac{-4w}{s+w+\omega}\right) = j\left(\frac{-4(s+w+\omega')}{\bar{w}}\right) = j\left(\frac{s_1+4\omega}{\bar{w}}\right),$$

$$\text{wo} \quad s_1 = 4 - 4(s+w) + w \quad \text{ist.}$$

$\bar{w}, s_1 + 4\omega$ ist aber die kanonische Basis des $\bar{\mathfrak{w}}'$ zugeordneten Ringideals $\bar{\mathfrak{w}}_r'$ des Ringes $r(4)$ mit dem Führer 4. Ist $\bar{\mathfrak{k}}_r$ die Ringklasse von $\bar{\mathfrak{w}}_r'$, so wird, wie oben:

$$j\left(\frac{\omega_2+\omega_1}{4\omega_1}\right) = j(\bar{\mathfrak{k}}_r),$$

und t muß in dem zu $r(4)$ gehörenden Ringklassenkörper liegen. Derselbe hat den Relativgrad:

$$h_r(4) = 4\left(1 - \left(\frac{m}{2}\right)\frac{1}{2}\right)h = 6h.$$

Legen wir eine andere Basis von $\mathfrak{w}$ zugrunde, so erhalten wir nur eine andere Wurzel der Ringklassengleichung, denn (64) ist in diesem Falle wegen der Irreduzibilität der Klassen- und Ringklassengleichung (Sätze 77 und 89) nichts anderes wie die Relativgleichung des Ringklassenkörpers zum Klassenkörper von $k(\sqrt{m})$. t *ist also in jedem Falle eine Zahl des Ringklassenkörpers von* $r(4)$. *Die kanonische Basis ist dadurch ausgezeichnet, daß beide Basiszahlen zu* (2) *teilerfremd sind.* Zugleich erkennt man, daß t nur von der Ringklasse $\bar{\mathfrak{k}}_r$ von $\bar{\mathfrak{w}}_r'$ abhängt. Man schreibt:

$$\mathrm{t} = \mathrm{t}(\bar{\mathfrak{k}}_r).$$

Da in $k(\sqrt{m})$ $\mathfrak{w}\bar{\mathfrak{w}} \sim 1$, $\mathfrak{w} \sim \bar{\mathfrak{w}}'$ ist, so ist $\bar{\mathfrak{k}}_r$ eine der Ringklassen, in die die Klasse von $\mathfrak{w}$ zerfällt.

c) $m \not\equiv 1 \pmod 4$. Die ganzen Zahlen werden durch 1 und $\omega = \sqrt{m}$ gegeben, und (2) ist Quadrat eines Primideales. Wir wählen zunächst wieder: $\mathfrak{w} = (w, s+\omega), \quad (s+\omega)(s+\omega') = s^2 - m \equiv 0 \pmod w,$

und s so, daß auch $s \equiv m \pmod 2$ ist. Dies können wir immer, da w ungerade und s nur (mod. w) bestimmt ist. Dann ist in:

$$(s + w + \omega)(s + w + \omega') = (s + w)^2 - m = w w,$$

w sicher *ungerade*, und $\mathfrak{w} = (w, s + w + \omega)$ ist ein durch seine kanonische Basis gegebenes, zu (2) teilerfremdes Ideal von $k(\sqrt{m})$. Ist $\bar{\mathfrak{k}}_r$ die Ringklasse des dem Ideal $\mathfrak{w}'$ zugeordneten Ringideals $\mathfrak{w}_r' = (w, -4(s+w+\omega'))$ in $r(4)$, so wird:

$$j\left(\frac{\omega_2 + \omega_1}{4\omega_1}\right) = j\left(\frac{s + w + \omega}{4w}\right) = j\left(\frac{-4(s + w + \omega')}{w}\right) = j(\bar{\mathfrak{k}}_r).$$

Ist somit ω_1, ω_2 eine kanonische Basis, für die $s \equiv m \pmod 2$ ist, so ist t *eine Zahl des Ringklassenkörpers von $r(4)$.* Der Relativgrad ist:

$$h_r(4) = 4\left(1 - \left(\frac{4m}{2}\right)\frac{1}{2}\right)h = 4h.$$

Die Gleichung (64) zerfällt in einen biquadratischen und einen quadratischen Faktor.

Ist dagegen $s \equiv m + 1 \pmod 2$, so ist:

$$(s + w + \omega)(s + w + \omega') = (s + w)^2 - m = 2ww,$$

und w ist ungerade. $\mathfrak{w} = (\overline{w}, s + w + \omega)$ ist ein durch seine kanonische Basis gegebenes, zu (2) teilerfremdes Ideal. Ist $\bar{\mathfrak{k}}_r$ die Ringklasse, die dem $\mathfrak{w}'$ zugeordneten Ringideal von $r(2)$ $\mathfrak{w}_r' = (w, -2(s + w + \omega'))$ entspricht, so ist:

$$j\left(\frac{\omega_2 + \omega_1}{4\omega_1}\right) = j\left(\frac{s + w + \omega}{4w}\right) = j\left(\frac{-2(s + w + \omega')}{\overline{w}}\right) = j(\bar{\mathfrak{k}}_r).$$

t ist jetzt eine Zahl des Ringklassenkörpers von $r(2)$, dessen Relativgrad nur:

$$h_r(2) = 2\left(1 - \left(\frac{4m}{2}\right)\frac{1}{2}\right)h = 2h$$

ist. Das zugehörige t genügt dann dem quadratischen Faktor von (64).

Wir werden in Zukunft immer voraussetzen, daß eine kanonische Basis der Art $s \equiv m \pmod 2$ vorliege.

Alle übrigen Basen können wieder keine anderen Werte ergeben. t hängt also nur von der Ringklasse von $\overline{\mathfrak{w}}_r'$ ab. Wir schreiben:

$$\mathrm{t} = \mathrm{t}(\bar{\mathfrak{k}}_r).$$

Aus der Definition von $\mathfrak{w}$ geht wieder hervor, daß in $k(\sqrt{m})$ $\mathfrak{w} \sim \overline{\mathfrak{w}}'$ ist. Also ist $\bar{\mathfrak{k}}_r$ eine der Ringklassen, in die die Klasse von $\mathfrak{w}$ zerfällt.

Ist $m = -1$ oder $= -3$, so ist t schon auf Seite 105 berechnet. Da jetzt $h_r(4)$ beide Male gleich 2 ist, so stimmt das Resultat mit dem obigen überein.

121. Satz: *Ist $\mathfrak{w} = (\omega_1, \omega_2)$ ein durch seine Basis gegebenes, zu* f *und* (2) *teilerfremdes Ideal, so ist $\mathrm{t}(\omega_1, \omega_2)$ eine ganze, algebraische Zahl. Man*

kann die Basis stets so wählen, daß t *eine bestimmende Zahl des zu* $k(\sqrt{m})$ *relativ Abelschen Ringklassenkörpers des Führers* (4) *mit dem Relativgrad* h_r *wird.* t *hängt dann nur ab von einer bestimmten Ringklasse, in die die Klasse von* $\mathfrak{w}$ *zerfällt:* $t = t(\mathfrak{k}_r)$. $\mathfrak{k}_r$ *ist durch die Wahl der Basis von* $\mathfrak{w}$ *eindeutig bestimmt.*

Daß t eine *ganze* algebraische Zahl ist, folgt nach Satz 63 aus (64) und aus dem Satz, daß die singulären Moduln ganze Zahlen sind (siehe Korollar zu Satz 72 und Satz 89).

Ist umgekehrt $\mathfrak{k}_r$ eine beliebige Ringklasse, in die die Klasse $\mathfrak{k}$ von $k(\sqrt{m})$ in $r(4)$ zerfällt, so nehme man ein beliebiges Ideal $\mathfrak{w}$ von $\mathfrak{k}$, das zu (2) und $\mathfrak{f}$ teilerfremd ist. Das zugehörige t ist dann sicher gleich $t(\mathfrak{k}^*)$, wo $\mathfrak{k}^*$ eine der Ringklassen ist, in die $\mathfrak{k}$ in $r(4)$ zerfällt. Durch Anwendung einer Modulsubstitution auf die Basis von $\mathfrak{w}$ kann dann nach obigem immer erreicht werden, daß $\mathfrak{w}$ durch eine Basis gegeben ist, für die $t = t(\mathfrak{k}_r)$ wird.

122. Satz: *Ist* $\mathfrak{k}_r$ *eine beliebige Ringklasse von* $r(4)$, *so gibt es stets ein zu* $\mathfrak{f}$ *und* (2) *teilerfremdes Ideal* $\mathfrak{w} = (\omega_1, \omega_2)$, *so daß das zugehörige* $t(\omega_1, \omega_2) = t(\mathfrak{k}_r)$ *wird.*

Da $t(\mathfrak{k}_r)$ im Ringklassenkörper von $r(4)$ liegt, so gehören alle konjugierten von t wieder diesem Ringklassenkörper an, da nach Satz 89 der Ringklassenkörper relativ-Abelsch zu $k(\sqrt{m})$ ist. Die Formeln (70) ergeben daher, *daß auch die Ausdrücke:*

$$\sqrt{t^2 - 2^6}, \quad \text{und} \quad \sqrt{\frac{\pm t - \sqrt{t^2 - 2^6}}{2\sqrt{t^2 - 2^6}}}$$

Zahlen des Ringklassenkörpers von $r(4)$ *sind.*

Wir wollen nochmals die Annahmen zusammenstellen, die wir von nun an stets über $\mathfrak{w}$ machen werden:

1. $\mathfrak{w}$ ist zu (2) und $\mathfrak{f}$ teilerfremd.

2. $\mathfrak{w}$ ist durch eine Basis ω_1, ω_2 gegeben, die folgende Bedingungen erfüllt:

$m \equiv 1 \pmod 8$: ω_1 und ω_2 sind je durch eines der beiden Primideale von (2) teilbar.

$m \equiv 5 \pmod 8$: ω_1 und ω_2 sind beide zu (2) teilerfremd.

$m \not\equiv 1 \pmod 4$: ω_1 ist zu (2) teilerfremd, ω_2 ist durch das in (2) enthaltene Primideal teilbar, oder umgekehrt.

Letzteres entspricht, wie man sofort erkennt, der Annahme $s \equiv m \pmod 2$.

Entsprechend zerfällt die Klasse $\mathfrak{k}$ in $r(4)$ in $h_r : h$ Ringklassen, und denselben entsprechen folgende $h_r : h$ Werte von t: ($m + -1, + -3$):

$m \equiv 1 \pmod 8$: $t(\omega_1, \omega_2)$, $t(-\omega_2 + 2\omega_1, 2\omega_2 - 3\omega_1) = -t(\omega_1, \omega_2)$,

$m \equiv 5 \pmod 8$: $t(\omega_1, \omega_2)$, $t(-\omega_2 + 2\omega_1, 2\omega_2 - 3\omega_1) = -t(\omega_1, \omega_2)$,

$t(\omega_2 + \omega_1, -\omega_1)$, $t(2\omega_2 - \omega_1, \omega_2 - \omega_1) = -t(\omega_2 + \omega_1, -\omega_1)$,

$t(-\omega_2, \omega_1 + \omega_2)$, $t(\omega_2 - \omega_1, \omega_2 - 2\omega_1) = -t(-\omega_2, \omega_1 + \omega_2)$.

$m \not\equiv 1 \pmod 4$: $t(\omega_1, \omega_2)$, $t(-\omega_2 + 2\omega_1, 2\omega_2 - 3\omega_1) = -t(\omega_1, \omega_2)$,

$t(-\omega_2, \omega_1 + \omega_2)$, $t(\omega_2 - \omega_1, \omega_2 - 2\omega_1) = -t(-\omega_2, \omega_1 + \omega_2)$.

Die Zuordnung der Ringklassen ist die folgende:

$m \equiv 1 \pmod 8$: Ist $\mathfrak{k}_r$ die Ringklasse von $\mathfrak{w}_r$ und $\mathfrak{k}_r^0$ die Ringklasse von $(1 + 2\omega)$, so ist:

$$t(\omega_1, \omega_2) = t(\mathfrak{k}_r),\ t(-\omega_2 + 2\omega_1, 2\omega_2 - 3\omega_1) = t(\mathfrak{k}_r^0 \mathfrak{k}_r).$$

$m \equiv 5 \pmod 8$: Wählt man in $\mathfrak{w} = (w, s + \omega) : \omega_1 = w - s - \omega$, $\omega_2 = s + \omega$, so ist ω_1, ω_2 eine Basis von $\mathfrak{w}$, und wie man sofort sieht: $t(\omega_1, \omega_2) = t(\mathfrak{k}_r)$, wo $\mathfrak{k}_r$ die Ringklasse von $\mathfrak{w}_r$ ist. $t(-\omega_2 + 2\omega_1, 2\omega_2 - 3\omega_1)$ gehört dann zu der Ringklasse von $\left(\overline{w}, 4s + 4\omega - 8\frac{n(s+\omega)}{w}\right)$, wo $w\overline{w} = n(-w + 2s + 2\omega)$ ist. Setzt man die Ringklasse von ω, falls $m \equiv 5 \pmod{16}$, von $\omega + 2$, falls $m \equiv 13 \pmod{16}$ gleich $\mathfrak{k}_r^0$, so ist dieses Ideal in $\mathfrak{k}_r^{03}\mathfrak{k}_r$, also:

$$t(-\omega_2 + 2\omega_1, 2\omega_2 - 3\omega_1) = t(\mathfrak{k}_r^{03}\mathfrak{k}_r).$$

Entsprechend ist, falls $s \pmod w$ so gewählt wird, daß $(s + \omega')$ in $\mathfrak{k}_r^0$ liegt:

$$t(\omega_2 + \omega_1, -\omega_1) = t(\mathfrak{k}_r^0 \mathfrak{k}_r),\quad t(2\omega_2 - \omega_1, \omega_2 - \omega_1) = t(\mathfrak{k}_r^{04}\mathfrak{k}_r),$$

$$t(-\omega_2, \omega_1 + \omega_2) = t(\mathfrak{k}_r^{02}\mathfrak{k}_r),\quad t(\omega_2 - \omega_1, \omega_2 - 2\omega_1) = t(\mathfrak{k}_r^{05}\mathfrak{k}_r),$$

$$w \equiv -1 \pmod 4.$$

$m \not\equiv 1 \pmod 4$: Wählt man in $\mathfrak{w} = (\omega_1, \omega_2) : \omega_1 = w$, $\omega_2 = s + \omega$, und ist $\mathfrak{k}_r$ die Ringklasse von $\mathfrak{w}_r$, $\mathfrak{k}_r^0$ diejenige von $(s + w + \omega)$, so ist:

$$t(\omega_1, \omega_2) = t(\mathfrak{k}_r^0 \mathfrak{k}_r).$$

Dagegen ist, wie man sofort sieht:

$$t(-\omega_2, \omega_1 + \omega_2) = t(\mathfrak{k}_r),\quad t(\omega_2 - \omega_1, \omega_2 - 2\omega_1) = t(\bar{\mathfrak{k}}_r^0 \mathfrak{k}_r),$$

wo $\bar{\mathfrak{k}}_r^0$ die Ringklasse von $(1 + 2\omega)$ ist. Schließlich ist:

$$t(-\omega_2 + 2\omega_1, 2\omega_2 - 3\omega_1) = t(\bar{\mathfrak{k}}_r^0 \mathfrak{k}_r^0 \mathfrak{k}_r).$$

Für $m = -1$ ist $t(1, 1 + i) = t(\mathfrak{k}_r) = -2 \cdot 3\sqrt{2}$, $t(1 - i, -1 + 2i) = t(\mathfrak{k}_r^2) = +2 \cdot 3\sqrt{2}$, wo $\mathfrak{k}_r$ die Ringklasse von $(1 + 2i)$, $\mathfrak{k}_r^2$ die Hauptring-

klasse ist. Für $m=-3$ ist $\mathfrak{t}(1,\varrho)=\mathfrak{t}(\mathfrak{f}_r^2)=+4\sqrt{3}$, $\mathfrak{t}\left(\frac{5-\sqrt{-3}}{2}, -4+\sqrt{-3}\right)$ $=\mathfrak{t}(\mathfrak{f}_r)=-4\sqrt{3}$, wo $\mathfrak{f}_r$ die Ringklasse von $(\varrho-1)$, $\mathfrak{f}_r^2$ die Hauptringklasse ist.

3. Die singulären elliptischen Funktionen und die komplexe Multiplikation.

Wir wollen von nun an alle Ideale von $k(\sqrt{m})$, die keinen Teiler mit (2) gemein haben, als *ungerade Ideale*, diejenigen, die einen Teiler mit (2) gemein haben, als *gerade Ideale* bezeichnen. Das der Betrachtung zugrunde gelegte Ideal $\mathfrak{w}$ ist somit ungerade. Wir nehmen seine nach dem vorigen Paragraphen ausgewählte Basis ω_1, ω_2 als Perioden der elliptischen Funktion $\mathfrak{T}(z;\omega_1,\omega_2)$. Diese heiße dann eine *singuläre elliptische Funktion*. Das zugehörige $\mathfrak{t}(\omega_1,\omega_2)$ ist nach Satz 121 eine ganze, algebraische Zahl. Es sei ν eine *ganze*, zu $\mathfrak{w}$ teilerfremde Zahl von $k(\sqrt{m})$, deren Norm $n(\nu)=n$ sei. Dann ist in:

$\mathfrak{T}\left(\frac{x_1\omega_1+x_2\omega_2}{\nu}\right)=\mathfrak{T}\left(\frac{x_1\nu'\omega_1+x_2\nu'\omega_2}{n}\right)$, x_1 und x_2 ganze rationale Zahlen,

der Zähler $\nu'(x_1\omega_1+x_2\omega_2)$ nach Satz 49 wieder eine Zahl von $\mathfrak{w}$, also:

$$\nu'(x_1\omega_1+x_2\omega_2)=y_1\omega_1+y_2\omega_2,$$

wo y_1 und y_2 wieder ganz und rational sind. Somit folgt:

$$\mathfrak{T}\left(\frac{x_1\omega_1+x_2\omega_2}{\nu}\right)=\mathfrak{T}\left(\frac{y_1\omega_1+y_2\omega_2}{n}\right).$$

Nach den Sätzen 111 und 112 ist:

$$\mathfrak{T}(nz)=R(\mathfrak{T}(z)),$$

wo R eine rationale Funktion ist, deren Koeffizienten ganze rationale Funktionen von $\mathfrak{t}$ mit ganzen rationalen Koeffizienten sind. Setzt man hier $z=\frac{x_1\omega_1+x_2\omega_2}{\nu}=\frac{y_1\omega_1+y_2\omega_2}{n}$, so ist wegen $\mathfrak{T}(y_1\omega_1+y_2\omega_2)=0$ (Satz 106):

$$R\left(\mathfrak{T}\left(\frac{x_1\omega_1+x_2\omega_2}{\nu}\right)\right)=0.$$

Daher ist $\mathfrak{T}\left(\frac{x_1\omega_1+x_2\omega_2}{\nu}\right)$ Wurzel des Zählers von R, dessen Koeffizienten algebraische Zahlen sind und $\mathfrak{T}\left(\frac{x_1\omega_1+x_2\omega_2}{\nu}\right)$ selbst muß eine algebraische Zahl sein.

123. Satz: *Die Zahlen* $\mathfrak{T}\left(\frac{x_1\omega_1+x_2\omega_2}{\nu}\right)$, *wo* ν *eine ganze Zahl von* $k(\sqrt{m})$, x_1 *und* x_2 *ganze rationale Zahlen und* ω_1, ω_2 *die Basis von* $\mathfrak{w}$ *ist, sind algebraische Zahlen.*

Im Falle $\nu=2$ ist $x_1\equiv x_2\equiv 1 \pmod 2$ auszuschließen, weil dann $\mathfrak{T}$ unendlich wird.

Es handelt sich darum, für diese Zahlwerte die Gleichung kleinsten Grades und deren Gruppe zu bestimmen. Dazu dient das *Prinzip der komplexen Multiplikation*. Die elliptische Funktion:

$$\mathfrak{T}(\nu z;\ \omega_1,\ \omega_2)$$

besitzt nämlich wieder die Perioden ω_1 und ω_2. Denn da ω_1, ω_2 eine Basis des Ideals $\mathfrak{w}$ ist und ν ganz ist, so muß:

$$\nu\omega_1 = y_1\omega_1 + y_2\omega_2,$$
$$\nu\omega_2 = y_3\omega_1 + y_4\omega_2,$$

wo alle y ganze rationale Zahlen sind. Also ist:

$$\mathfrak{T}(\nu(z+\omega_1);\ \omega_1,\ \omega_2) = \mathfrak{T}(\nu z + y_1\omega_1 + y_2\omega_2;\ \omega_1,\ \omega_2) = \mathfrak{T}(\nu z;\ \omega_1,\ \omega_2),$$
$$\mathfrak{T}(\nu(z+\omega_2);\ \omega_1,\ \omega_2) = \mathfrak{T}(\nu z + y_3\omega_1 + y_4\omega_2;\ \omega_1,\ \omega_2) = \mathfrak{T}(\nu z;\ \omega_1,\ \omega_2).$$

Da $\mathfrak{T}(\nu z)$ eine gerade Funktion ist, gehört sie nach Satz 108 dem Funktionskörper von $\mathfrak{T}(z)$ an: $\mathfrak{T}(\nu z) = R(\mathfrak{T}(z))$.

$\mathfrak{T}(\nu z)$ besitzt an allen Punkten:

$$\mu = \frac{x_1\omega_1 + x_2\omega_2}{\nu},\ x_1 \text{ und } x_2 \text{ ganze rationale Zahlen,}$$

Nullstellen 2. Ordnung und an den Punkten:

$$\mu + \frac{\omega_1+\omega_2}{2\nu} = \frac{\omega_1+\omega_2}{2\nu} + \frac{x_1\omega_1 + x_2\omega_2}{\nu},\ x_1 \text{ und } x_2 \text{ ganze rationale Zahlen,}$$

Pole 2. Ordnung. Um die Nullstellen und Pole zu erhalten, denen alle Nullstellen und Pole eines Periodenparallelogrammes ähnlich sind, muß $\Omega = (x_1\omega_1 + x_2\omega_2)$ bloß alle (mod. ν) inkongruenten Zahlen dieser Form durchlaufen. Denn ist $\Omega \equiv \overline{\Omega}$ (mod. ν), so ist $\overline{\Omega} - \Omega : \nu$ ganz und liegt in $\mathfrak{w}$, da (ν) zu $\mathfrak{w}$ teilerfremd ist, also:

$$\frac{\overline{\Omega}-\Omega}{\nu} = y_1\omega_1 + y_2\omega_2,\quad \frac{\Omega}{\nu} \equiv \frac{\overline{\Omega}}{\nu} \pmod{\mathfrak{w}},\quad \mathfrak{T}\left(\frac{\overline{\Omega}}{\nu}\right) = \mathfrak{T}\left(\frac{\Omega}{\nu}\right).$$

Es gibt $n(\nu)$ (mod. ν) inkongruente Zahlen, die wir alle durch $\mathfrak{w}$ teilbar, also von der Form $x_1\omega_1 + x_2\omega_2$ annehmen dürfen, da (ν) zu $\mathfrak{w}$ teilerfremd ist. Wir müssen noch angeben, wie viele der so ausgewählten $\mathfrak{T}(\mu)$ voneinander verschieden sind. Ist $\mathfrak{T}(\bar{\mu}) = \mathfrak{T}(\mu)$, so dürfen wir nach Satz 100 $\bar{\mu} \equiv -\mu$ (mod. $\mathfrak{w}$) setzen. Ist $\mu \not\equiv -\mu$ (mod. $\mathfrak{w}$), so kommt jeder Funktionswert $\mathfrak{T}(\mu)$ zweimal vor. Ist dagegen $\mu \equiv -\mu$ oder $2\mu \equiv 0$ (mod. $\mathfrak{w}$), so hat μ (mod. $\mathfrak{w}$) eine der Formen $0, \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}$, für die die Funktionswerte von 2. Ordnung angenommen werden oder unendlich sind. Entsprechend kommen alle Funktionswerte $\mathfrak{T}\left(\frac{\omega_1+\omega_2}{2\nu} + \mu\right)$ zweimal vor, außer wenn $\frac{\omega_1+\omega_2}{2\nu} + \mu \equiv -\frac{\omega_1+\omega_2}{2\nu} - \mu$ oder $2\mu \equiv -\frac{\omega_1+\omega_2}{\nu}$ (mod. $\mathfrak{w}$)

ist. Dann hat wieder $\mu + \frac{\omega_1 + \omega_2}{2\nu}$ eine der Gestalten $0, \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1 + \omega_2}{2}$.

Setzt man: $$Z_\nu(x) = \prod_{(\mu)}' (x - \mathfrak{T}(\mu)),$$

$$N_\nu(x) = \prod_{(\mu)}' \left(x - \mathfrak{T}\left(\mu + \frac{\omega_1 + \omega_2}{2\nu}\right)\right),$$

wo die Produkte über die $n(\nu)$ (inkongruenten) μ, mit Ausnahme von $\mu = 0$ und $\mu = \frac{\omega_1 + \omega_2}{2}$ oder $\mu + \frac{\omega_1 + \omega_2}{2\nu} \equiv \frac{\omega_1 + \omega_2}{2}$ (mod. $\mathfrak{w}$), falls sie auftreten, zu erstrecken sind, so muß wie früher:

$$\mathfrak{T}(\nu z) = c \frac{\mathfrak{T}(z)\, Z_\nu(\mathfrak{T}(z))}{N_\nu(\mathfrak{T}(z))} \tag{71}$$

sein, wo c eine Konstante. Dieselbe berechnet sich so:

$$\lim_{z=0} \frac{\mathfrak{T}(\nu z)}{\mathfrak{T}(z)} = \nu^2 = c \frac{Z_\nu(0)}{N_\nu(0)} = \pm c \frac{\Pi'(\mathfrak{T}(\mu))}{\Pi'\left(\mathfrak{T}\left(\mu + \frac{\omega_1 + \omega_2}{2\nu}\right)\right)}. \tag{72}$$

c ist also nach Satz 123 sicherlich eine algebraische Zahl. Der Grad von Z_ν ist höchstens $n(\nu) - 1$, derjenige von N_ν höchstens $n(\nu)$. Das Maximum des Zählers muß nur dann nicht erreicht werden, wenn (ν) ein gerades Ideal ist, dasjenige des Nenners nur dann nicht, wenn (ν) ein ungerades Ideal ist.

Die Koeffizienten von Z_ν und N_ν sind nach Satz 123 sicherlich algebraische Zahlen. Um sie genauer zu bestimmen, erweitern wir in (71) Zähler und Nenner mit denjenigen Funktionen N_ν, deren Koeffizienten die konjugierten der algebraischen Koeffizienten von N_ν sind. Der Nenner N^* ist dann ein Polynom von $\mathfrak{T}(z)$, dessen Koeffizienten rationale Zahlen sind. Wir schreiben:

$$\mathfrak{T}(\nu z) = \frac{Z^*}{N^*}, \text{ oder: } N^*(\mathfrak{T}(z))\, \mathfrak{T}(\nu z) = Z^*(\mathfrak{T}(z))$$

und setzen für $\mathfrak{T}(\nu z)$ und $\mathfrak{T}(z)$ die Reihenentwicklungen nach $\nu\zeta$ und ζ gemäß Satz 107 ein. Die Koeffizientenvergleichung links und rechts gleichhoher Potenzen von ζ ergibt sukzessive das Resultat, daß die Koeffizienten von Z^* ganze rationale Funktionen von t mit in $k(\sqrt{m})$ liegenden Zahlkoeffizienten sind. Auf rationalem Wege kann man jetzt den größten gemeinsamen Teiler von Z^* und N^* bestimmen, dessen Koeffizienten ebenfalls rational von t mit in $k(\sqrt{m})$ liegenden Zahlkoeffizienten abhängen. Dividiert man Z^* und N^* durch denselben, so erhält man wieder Funktionen von diesem Charakter. Diese Quotienten sind aber nichts anderes wie $c\,\mathfrak{T}(z) Z_\nu$ und N_ν, denn diese sind nach der obigen Betrachtung ohne gemeinsamen Teiler. Daher haben cZ_ν und N_ν dieselbe Eigenschaft.

124. Satz: *$\mathfrak{T}(\nu z)$ ist eine rationale Funktion von $\mathfrak{T}(z)$, deren Zähler und Nenner höchstens den Grad $n(\nu)$ besitzen und deren Koeffizienten im Ringklassenkörper von $r(4)$ liegen.*

Im Falle $\nu \equiv 1 \pmod 2$ kann die rationale Funktion in (71) genau bestimmt werden. Dieser Fall ist darum ausgezeichnet, weil für ihn der Satz gilt:

Korollar zum 123. Satz: *Ist ν eine ganze Zahl von $k(\sqrt{m})$, für die $\nu \equiv 1$ (mod. 2), so sind alle Werte $\mathfrak{T}\left(\frac{x_1\omega_1 + x_1\omega_2}{\nu}\right)$, wo x_1 und x_2 irgendwelche ganze, rationale Zahlen sind, ganze algebraische Zahlen.*

Denn dann ist $n(\nu) = n$ ungerade und $\mathfrak{T}\left(\frac{x_1\omega_1 + x_2\omega_2}{\nu}\right)$ ist nach Satz 111 Wurzel von:

$$\mathfrak{T}(z)\, Z_n(\mathfrak{T}(z))^2 = 0,$$

wo nach Satz 112 die Koeffizienten von Z_n ganze algebraische Zahlen sind und der Koeffizient der obersten Potenz eins ist.

Im Produkt Z_ν von (71) kommt bei $\nu \equiv 1 \pmod 2$ $\mu = 0, \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}$ nicht vor, also ist Z_ν ein Quadrat: $Z_\nu = z_\nu^2$. Ferner ist im Produkt von N_ν: $\mu + \frac{\omega_1+\omega_2}{2\nu} = \frac{\nu-1}{2}\cdot\frac{\omega_1+\omega_2}{\nu} + \frac{\omega_1+\omega_2}{2\nu} = \frac{\omega_1+\omega_2}{2}$ auszuschließen. N_ν hat den Grad $n(\nu) - 1$. $\mu + \frac{\omega_1+\omega_2}{2\nu} = \frac{\omega_1}{2}$ oder $\frac{\omega_2}{2}$ kann nicht auftreten, also ist auch N_ν ein Quadrat, wir setzen $n_\nu^2 = \nu^2 N_\nu$ und erhalten jetzt:

$$\mathfrak{T}(\nu z) = \nu^2 c \frac{\mathfrak{T}(z) z_\nu^2(\mathfrak{T}(z))}{n_\nu(\mathfrak{T}(z))^2},$$

wo c für $z = \frac{\omega_1+\omega_2}{2}$ berechnet werden kann:

$$\lim_{z=\frac{\omega_1+\omega_2}{2}} \frac{\mathfrak{T}(\nu z)}{\mathfrak{T}(z)} = \lim_{z=0} \frac{\mathfrak{T}\left(\nu\left(z+\frac{\omega_1+\omega_2}{2}\right)\right)}{\mathfrak{T}\left(z+\frac{\omega_1+\omega_2}{2}\right)} = \lim_{z=0} \frac{\mathfrak{T}\left(\nu z + \frac{\omega_1+\omega_2}{2}\right)}{\mathfrak{T}\left(z+\frac{\omega_1+\omega_2}{2}\right)}$$

$$= \lim_{z=0} \frac{\mathfrak{T}(z)}{\mathfrak{T}(\nu z)} = \frac{1}{\nu^2}, \qquad \lim_{z=\frac{\omega_1+\omega_2}{2}} \nu^2 c \frac{z_\nu^2(\mathfrak{T}(z))}{n_\nu^2(\mathfrak{T}(z))} = \frac{\nu^2 c}{\nu^2} = c, \quad c = \frac{1}{\nu^2}.$$

(73) Also wird: $$\mathfrak{T}(\nu z) = \frac{\mathfrak{T}(z) z_\nu^2(\mathfrak{T}(z))}{n_\nu^2(\mathfrak{T}(z))}, \qquad \nu \equiv 1 \pmod 2.$$

Alle Koeffizienten von z_ν und n_ν gehören dem Ringklassenkörper von $r(4)$ an.

Setzt man statt z: $z + \frac{\omega_1+\omega_2}{2}$, so geht nach (38) $\mathfrak{T}(z)$ in $1 : \mathfrak{T}(z)$ über, und es wird:

$$\mathfrak{T}\left(\nu\left(z+\frac{\omega_1+\omega_2}{2}\right)\right) = \mathfrak{T}\left(\nu z + \frac{\nu(\omega_1+\omega_2)}{2}\right)$$

$$= \mathfrak{T}\left(\nu z + \frac{\nu-1}{2}(\omega_1+\omega_2) + \frac{\omega_1+\omega_2}{2}\right) = \frac{1}{\mathfrak{T}(\nu z)},$$

was in (73) berücksichtigt ergibt:

$$\mathfrak{T}(\nu z) = \frac{\mathfrak{T}(z) n_\nu^2\left(\frac{1}{\mathfrak{T}(z)}\right)}{z_\nu^2\left(\frac{1}{\mathfrak{T}(z)}\right)} \equiv \frac{\mathfrak{T}(z) z_\nu^2(\mathfrak{T}(z))}{n_\nu^2(\mathfrak{T}(z))}.$$

Das ist nur möglich, wenn:

$$(\sqrt{-1})^\alpha \mathfrak{T}(z)^{\frac{n(\nu)-1}{2}} n_\nu\left(\frac{1}{\mathfrak{T}(z)}\right) \equiv z_\nu(\mathfrak{T}(z)),$$

$$\pm(\sqrt{-1})^\alpha \mathfrak{T}(z)^{\frac{n(\nu)-1}{2}} z_\nu\left(\frac{1}{\mathfrak{T}(z)}\right) \equiv n_\nu(\mathfrak{T}(z)); \quad \alpha = 0, 1, 2, 3;$$

also für $z = 0$:

$$z_\nu(0) = (\sqrt{-1})^\alpha \nu, \quad n_\nu(0) = \pm(\sqrt{-1})^\alpha.$$

Nach dem Korollar zu Satz 123 sind die Wurzeln von z_ν *ganze* Zahlen, also sind auch die Koeffizienten von z_ν als deren symmetrischen Funktionen ganze Zahlen des Ringklassenkörpers von $r(4)$ und die zweite der obigen Beziehungen zeigt, daß auch dasselbe für n_ν gilt. $(\sqrt{-1})^\alpha$ ist auch in $r(4)$ enthalten.

125. Satz: *Ist $\nu \equiv 1$ (mod. 2) eine ganze Zahl von $k(\sqrt{m})$, so ist:*

$$\mathfrak{T}(\nu z) = \frac{\mathfrak{T}(z) z_\nu^2(\mathfrak{T}(z))}{n_\nu^2(\mathfrak{T}(z))},$$

wo z_ν und n_ν ganze rationale Funktionen von $\mathfrak{T}(z)$ vom Grade $\frac{1}{2}(n(\nu)-1)$ sind, deren Koeffizienten ganze Zahlen des Ringklassenkörpers von $r(4)$ sind. Der Koeffizient der obersten Potenz in z_ν ist 1, in n_ν ist er ν, $z_\nu(0) = (\sqrt{-1})^\alpha \nu$, $n_\nu(0) = \pm(\sqrt{-1})^\alpha$ und:

$$n_\nu(\mathfrak{T}(z)) \equiv \pm(\sqrt{-1})^\alpha \mathfrak{T}(z)^{\frac{n(\nu)-1}{2}} z_\nu(\mathfrak{T}(z)^{-1}).$$

Man kann $\mathfrak{T}(\nu z)$ noch auf eine zweite Art darstellen, falls ν keine Einheit und $\nu \equiv 1$ (mod. 2) ist. Das Produkt:

$$\mathfrak{T}(z) \prod_{(\mu \neq 0)} \mathfrak{T}(z + \mu), \quad \mu = \frac{x_1 \omega_1 + x_2 \omega_2}{\nu}, \quad x_1 \text{ und } x_2 \text{ ganze rationale Zahlen,}$$

wo $x_1\omega_1 + x_2\omega_2$ ein Restsystem (mod. ν) mit Ausnahme von 0 durchläuft, hat genau dieselben Nullstellen und Pole von derselben Ordnung wie $\mathfrak{T}(\nu z)$. Denn es wird von 2. Ordnung null für $z = -\mu$ und von 2. Ordnung unendlich für $z = \frac{\omega_1 + \omega_2}{2} - \mu = \frac{\omega_1 + \omega_2}{2\nu} + \frac{\nu - 1}{2}\frac{\omega_1 + \omega_2}{\nu} - \mu$.

Somit ist: $$\mathfrak{T}(\nu z) = c\,\mathfrak{T}(z) \prod_{(\mu \neq 0)} \mathfrak{T}(z + \mu), \quad c = \text{konstans.}$$

Zur Bestimmung von c setzt man für z: $z + \frac{\omega_1 + \omega_2}{2}$; dann geht jede $\mathfrak{T}$-Funktion in ihren reziproken Wert über, also ist:

$$c = \frac{1}{c} \text{ oder } c = \pm 1 \text{ und } \pm \mathfrak{T}(\nu z) = \mathfrak{T}(z) \prod_{(\mu)} \mathfrak{T}(z + \mu),$$

126. Satz: *Ist ν eine ganze Zahl von $k(\sqrt{m})$, die $\equiv 1$ (mod. 2) ist, so gilt:*

$$\pm \mathfrak{T}(\nu z) = \mathfrak{T}(z) \prod_{(\mu)} \mathfrak{T}(z+\mu),$$

wo $\mu = \frac{x_1\omega_1 + x_2\omega_2}{\nu}$ und $x_1\omega_1 + x_2\omega_2$ ein Restsystem (mod. ν) mit Ausschluß von 0 durchläuft.

Wir beginnen jetzt mit dem Fall $\nu = 2$. Da $\mathfrak{T}\left(\frac{\omega_1+\omega_2}{2}\right) = \infty$ ist, so ist nur $\mathfrak{T}\left(\frac{\omega_1}{2}\right)$ und $\mathfrak{T}\left(\frac{\omega_2}{2}\right)$ zu betrachten. Diese Werte sind nach (44)' Wurzeln von:

$$4\mathfrak{T}(z)^2 + t\,\mathfrak{T}(z) + 4 = 0,$$

was die Lösungen gibt:

$$\mathfrak{T}\left(\frac{\omega_{1,2}}{2}\right) = \frac{-t \pm \sqrt{t^2-2^6}}{8}.$$

Nach der Bemerkung auf Seite 115 liegt $\sqrt{t^2-2^6}$ im Ringklassenkörper von $r(4)$.

127. Satz: $\mathfrak{T}\left(\frac{\omega_1}{2}\right)$ *und* $\mathfrak{T}\left(\frac{\omega_2}{2}\right)$ *sind Zahlen des Ringklassenkörpers von* $r(4)$.

Im Falle $\nu = 4$ ist zunächst nach (37) und wegen (46):

$$\mathfrak{T}\left(\frac{\omega_1 \pm \omega_2}{4}\right) = \pm 1,$$

außerdem gibt es noch 4 Werte:

$$\mathfrak{T}\left(\frac{\omega_1}{4}\right),\ \mathfrak{T}\left(\frac{\omega_1+2\omega_2}{4}\right) = \frac{1}{\mathfrak{T}\left(\frac{\omega_1}{4}\right)},\ \mathfrak{T}\left(\frac{\omega_2}{4}\right),\ \mathfrak{T}\left(\frac{2\omega_1+\omega_2}{4}\right) = \frac{1}{\mathfrak{T}\left(\frac{\omega_2}{4}\right)}.$$

Dieselben findet man als Wurzeln von (46):

$$\mathfrak{T}(2z) = \frac{\mathfrak{T}(z)\,(4\mathfrak{T}(z)^2 + t\mathfrak{T}(z) + 4)}{(\mathfrak{T}(z)^2-1)^2},$$

wenn man $z = \frac{\omega_1}{4}$ oder $= \frac{\omega_2}{4}$ setzt. Links tritt $\mathfrak{T}\left(\frac{\omega_{1,2}}{2}\right)$ auf, somit hat man die Gleichung zu lösen:

$$\frac{-t \pm \sqrt{t^2-2^6}}{8} = \frac{x(4x^2+tx+4)}{(x^2-1)^2} = \frac{4\left(x+\frac{1}{x}\right)+t}{\left(x+\frac{1}{x}\right)^2-2^2},$$

woraus:

$$x + \frac{1}{x} = -\frac{t \pm \sqrt{t^2-2^6}}{4},$$

$$x = -\frac{t \pm \sqrt{t^2-2^6}}{8} \pm \frac{\sqrt{t^2-2^6}}{4}\sqrt{\frac{\pm t + \sqrt{t^2-2^6}}{2\sqrt{t^2-2^6}}}$$

$$= -\frac{t \pm \sqrt{t^2-2^6}}{8} \pm \frac{1}{\sqrt{\frac{\pm t - \sqrt{t^2-2^6}}{2\sqrt{t^2-2^6}}}}.$$

Alle diese Größen sind nach der Bemerkung Seite 115 im Ringklassenkörper von r (4).

128. Satz: *Alle Größen* $\mathfrak{T}\left(\frac{x_1\omega_1 + x_2\omega_2}{4}\right)$ *sind Zahlen des Ringklassenkörpers von* r (4).

Es ist daher einleuchtend, daß wir uns auf die Größen

$$\mathfrak{T}\left(\frac{x_1\omega_1 + x_2\omega_2}{4\nu}\right)$$

beschränken können, da die Teilung durch 4 nichts neues ergibt. In der Tat werden wir für diese Zahlen klassisch schöne und einfache Resultate finden.

Setzt man in (71) für z: $\frac{x_1\omega_1 + x_2\omega_2}{4\nu}$, so wird:

$$\mathfrak{T}\left(\frac{x_1\omega_1 + x_2\omega_2}{4}\right) = c\,\frac{\mathfrak{T}\left(\frac{x_1\omega_1 + x_2\omega_2}{4\nu}\right) Z_\nu\left(\mathfrak{T}\left(\frac{x_1\omega_1 + x_2\omega_2}{4\nu}\right)\right)}{N_\nu\left(\mathfrak{T}\left(\frac{x_1\omega_1 + x_2\omega_2}{4\nu}\right)\right)}.$$

Links ist nach Satz 128 eine Zahl des Ringklassenkörpers von r (4), also ist $x = \mathfrak{T}\left(\frac{x_1\omega_1 + x_2\omega_2}{4\nu}\right)$ Wurzel der Gleichung $n(\nu)^{\text{ten}}$ Grades:

$$N_\nu(x)\,\mathfrak{T}\left(\frac{x_1\omega_1 + x_2\omega_2}{4}\right) - cxZ_\nu(x) = 0,$$

deren Koeffizienten alle im Ringklassenkörper von r (4) liegen. Im Falle

(74) $$x_1 \equiv x_2 \equiv \pm 1 \pmod 4$$

ist $\mathfrak{T}\left(\frac{x_1\omega_1 + x_2\omega_2}{4}\right) = 1$. Dieser Fall ist besonders einfach und wird einzig weiter behandelt werden. Die übrigen Fälle sind gleich zu behandeln und würden eine Periodentransformation bedeuten. Unter Voraussetzung von (74) genügt $\mathfrak{T}\left(\frac{x_1\omega_1 + x_2\omega_2}{4\nu}\right) = x$ der Gleichung:

$$F_{4\nu}(x) \equiv cxZ_\nu(x) - N_\nu(x) = 0.$$

Dieselbe ist sicherlich nicht identisch erfüllt und von $n(\nu)^{\text{tem}}$ Grade in x. Alle Wurzeln werden erhalten, wenn $x_1\omega_1 + x_2\omega_2$ ein volles Restsystem (mod. 4ν), unter Berücksichtigung von (74), durchläuft. Das ganze Restsystem (mod. 4ν) enthält $2^4 n(\nu)$ Zahlen, von denen nur der achte Teil der Bedingung (74) genügt, was $2n(\nu)$ Reste macht. Von diesen geben nur die (mod. 4ν) entgegengesetzt kongruenten das gleiche $\mathfrak{T}$. Denn wäre $\mathfrak{T}\left(\frac{\bar{x}_1\omega_1 + \bar{x}_2\omega_2}{4\nu}\right) = \mathfrak{T}\left(\frac{x_1\omega_1 + x_2\omega_2}{4\nu}\right)$, so müßte:

$$\frac{(\bar{x}_1 \mp x_1)\omega_1 + (\bar{x}_2 \mp x_2)\omega_2}{4\nu} = \frac{\frac{\bar{x}_1 \mp x_1}{2}\omega_1 + \frac{\bar{x}_2 \mp x_2}{2}\omega_2}{2\nu}$$

eine Zahl von $\mathfrak{w}$ sein. Wegen (74) sind $\frac{\bar{x}_1 \mp x_1}{2}$ und $\frac{\bar{x}_2 \mp x_2}{2}$ nur für eines der Vorzeichen beide gerade, und für dieses ist:

$$\pm \bar{x}_1 \omega_1 \pm \bar{x}_2 \omega_2 \equiv x_1 \omega_1 + x_2 \omega_2 \pmod{4\nu}.$$

Für das andere Vorzeichen sind $\frac{\bar{x}_1 \mp x_1}{2}$ und $\frac{\bar{x}_2 \mp x_2}{2}$ beide ungerade, was unmöglich eine Zahl von $\mathfrak{w}$ ergäbe, da nach Annahme $\frac{1}{2}(\omega_1 + \omega_2)$ niemals ganz ist (siehe die Voraussetzungen über ω_1 und ω_2 S. 115). Daher bleiben genau $n(\nu)$ verschiedene $\mathfrak{T}$-Werte übrig.

Es sei $\mathfrak{f}$ ein beliebiges, zu $\mathfrak{w}$ teilerfremdes Ideal von $k(\sqrt{m})$, das wenigstens ein Primideal enthalte. Man kann dann zwei ganze Zahlen ν_1 und ν_2 angeben, deren größter, gemeinsamer Teiler $\mathfrak{f}$ ist:

$$(\nu_1) = \mathfrak{f}_1 \mathfrak{f}, \quad (\nu_2) = \mathfrak{f}_2 \mathfrak{f},$$

wo $\mathfrak{f}_1$ und $\mathfrak{f}_2$ ungerade, zueinander und zu $\mathfrak{w}$ teilerfremd sind. Außerdem darf man noch voraussetzen, daß:

$$\frac{\nu_1}{\nu_2} \equiv 1 \pmod{4}$$

ist. Denn da $\mathfrak{f}_1$ und $\mathfrak{f}_2$ ungerade sind, kann man eine ganze, zu $\mathfrak{w}$, (2) und (ν_2) teilerfremde Zahl ξ so bestimmen, daß $\xi \frac{\nu_1}{\nu_2} \equiv 1 \pmod{4}$ wird. Dann genügen $\xi \nu_1$ und ν_2 allen Bedingungen.

Welche Wurzeln haben:

$$F_{4\nu_1}(x) = 0 \quad \text{und} \quad F_{4\nu_2}(x) = 0$$

gemein? Sind $\mathfrak{T}\left(\frac{x_1\omega_1 + x_2\omega_2}{4\nu_1}\right)$ und $\mathfrak{T}\left(\frac{\bar{x}_1\omega_1 + \bar{x}_2\omega_2}{4\nu_2}\right)$ die beiden gemeinsamen Wurzeln, so muß sicherlich für eines der beiden Zeichen:

$$\frac{x_1\omega_1 + x_2\omega_2}{4\nu_1} \mp \frac{\bar{x}_1\omega_1 + \bar{x}_2\omega_2}{4\nu_2}$$

eine Zahl von $\mathfrak{w}$ sein. Da $(4\nu_1)$ und $(4\nu_2)$ den größten gemeinsamen Teiler $(4\mathfrak{f})$ haben, so ist dies nur möglich, wenn $x_1\omega_1 + x_2\omega_2 \equiv 0 \pmod{\mathfrak{f}_1}$ ist. Wegen (74) und den Annahmen über ω_1 und ω_2 sind alle Zahlen $x_1\omega_1 + x_2\omega_2$ ungerade. Daher ist $\frac{\nu_2}{\nu_1}(x_1\omega_1 + x_2\omega_2)$ eine Zahl von $\mathfrak{w}$, und:

$$\frac{x_1\omega_1 + x_2\omega_2}{4\nu_1} = \frac{\frac{\nu_2}{\nu_1}(x_1\omega_1 + x_2\omega_2)}{4\nu_2} = \frac{x_1^*\omega_1 + x_2^*\omega_2}{4\nu_2}, \quad x_1^*, x_2^* \text{ ganz, rational;}$$

wegen der Annahmen über ν_1 und ν_2 wird:

$$\frac{\nu_2}{\nu_1}(x_1\omega_1 + x_2\omega_2) \equiv \pm(\omega_1 + \omega_2), \quad \text{also:} \quad x_1^* \equiv x_2^* \equiv \pm 1 \pmod{4}.$$

$\mathfrak{T}\left(\frac{x_1\omega_1 + x_2\omega_2}{4\nu_1}\right)$ ist somit wirklich auch Wurzel von $F_{4\nu_2}(x) = 0$. Von

den $n(\nu_1)$ Werten von $(x_1\omega_1 + x_2\omega_2)$ sind genau $n(\nu_1) : n(\mathfrak{f}_1) = n(\mathfrak{f})$ durch $\mathfrak{f}_1$ teilbar. Daher haben $F_{4\nu_1}$ und $F_{4\nu_2}$ genau $n(\mathfrak{f})$ Wurzeln gemein. $F_{4\nu_1}$ und $F_{4\nu_2}$ haben den gemeinsamen Teiler

$$F_{4\mathfrak{f}}(x) = 0, \tag{75}$$

der vom $n(\mathfrak{f})^{\text{ten}}$ Grade ist, und den man auf rationalem Wege aus $F_{4\nu_1}$ und $F_{4\nu_2}$ berechnen kann. Die Koeffizienten von $F_{4\mathfrak{f}}$ sind daher ebenfalls Zahlen des Ringklassenkörpers von $r(4)$. Alle Wurzeln $\mathfrak{T}\left(\frac{x_1\omega_1 + x_2\omega_2}{4\nu_1}\right)$ von $F_{4\mathfrak{f}}$ müssen sich in Idealform so schreiben lassen:

$$\frac{(x_1\omega_1 + x_2\omega_2)}{(4\nu_1)} = \frac{\mathfrak{j}\mathfrak{w}}{(4)\mathfrak{f}},$$

wo $\mathfrak{j}$ ein ungerades Ideal von $k(\sqrt{m})$ ist, und entsprechend für $\mathfrak{T}$:

$$\mathfrak{T}\left(\frac{\mathfrak{j}\mathfrak{w}}{(4)\mathfrak{f}}\right).$$

$\mathfrak{j}$ durchläuft ein System von $n(\mathfrak{f})$ ungeraden Idealen von $k(\sqrt{m})$, falls $x_1\omega_1 + x_2\omega_2$ ein System von (mod. $4\mathfrak{f}$) inkongruenten, der Nebenbedingung (74) genügenden Zahlen durchläuft. Wir werden von nun an die Wurzeln immer so abkürzen.

Damit ist aber noch nicht die Gleichung niedersten Grades gefunden, der $\mathfrak{T}$ genügt. Es sei $\mathfrak{z}$ der größte in $\mathfrak{f}$ enthaltene *gerade* Idealteiler, der nur Teiler von (2) enthält, also $\mathfrak{f} = \mathfrak{z}\bar{\mathfrak{f}}$, wo $\bar{\mathfrak{f}}$ ungerade ist. Die Norm von $\mathfrak{z}$ ist eine Potenz von 2. $\bar{\mathfrak{f}}$ besitze die Primidealzerlegung:

$$\bar{\mathfrak{f}} = \mathfrak{p}_1^{r_1}\mathfrak{p}_2^{r_2}\ldots\mathfrak{p}_n^{r_n},$$

wo alle $\mathfrak{p}$ ungerade und voneinander verschieden sind. Dann setzt man:

$$\mathfrak{S}_{4\mathfrak{f}}(x) = \frac{F_{4\mathfrak{f}}\, F_{\frac{4\mathfrak{f}}{\mathfrak{p}_1\mathfrak{p}_2}} \cdots F_{\frac{4\mathfrak{f}}{\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4}} \cdots}{F_{\frac{4\mathfrak{f}}{\mathfrak{p}_1}} \cdots F_{\frac{4\mathfrak{f}}{\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3}} \cdots}. \tag{76}$$

Im Zähler stehen alle $F_{4\mathfrak{a}}$, deren Index $\mathfrak{a}$ die Form $\mathfrak{f} : \mathfrak{f}'$ hat, wo $\mathfrak{f}'$ alle möglichen Produkte aus $\mathfrak{p}_1, \mathfrak{p}_2, \ldots \mathfrak{p}_n$ mit *gerader* Faktorenzahl sein kann. Im Nenner ist letztere Faktorenzahl *ungerade*. Dabei tritt jeder Faktor $\mathfrak{p}$ nur einfach auf.

$\mathfrak{S}_{4\mathfrak{f}}(x)$ ist eine ganze rationale Funktion von x mit Koeffizienten, die dem Ringklassenkörper von $r(4)$ angehören. Denn ist $\mathfrak{T}\left(\frac{\mathfrak{j}\mathfrak{w}}{4\mathfrak{f}}\right)$ eine Wurzel von $F_{4\mathfrak{f}}$, dessen $\mathfrak{j}$ zu $\mathfrak{f}$ teilerfremd ist, so tritt der Faktor $\left(x - \mathfrak{T}\left(\frac{\mathfrak{j}\mathfrak{w}}{4\mathfrak{f}}\right)\right)$ nur in $F_{4\mathfrak{f}}$, d. h. nur einfach im Zähler auf. Hat dagegen $\mathfrak{j}$ den größten gemeinsamen Teiler $\mathfrak{f}_1$ mit $\mathfrak{f}$, und sind $\mathfrak{p}_1, \mathfrak{p}_2, \ldots \mathfrak{p}_i$, die

verschiedenen in $\mathfrak{f}_1$ aufgehenden Primideale, so ist $\mathfrak{T}\left(\frac{\mathfrak{f}\mathfrak{w}}{4\mathfrak{f}}\right)$ Wurzel von:

$$F_{4\mathfrak{f}},\ F_{4\mathfrak{f}:\mathfrak{p}_1},\ \ldots\ F_{4\mathfrak{f}:\mathfrak{p}_1\mathfrak{p}_2},\ \ldots\ F_{4\mathfrak{f}:\mathfrak{p}_1\cdots\mathfrak{p}_i}.$$

Der Zähler von $\mathfrak{S}_{4\mathfrak{f}}(x)$ ist durch die

$$1+\binom{i}{2}+\binom{i}{4}+\cdots,$$

der Nenner durch die

$$\binom{i}{1}+\binom{i}{3}+\cdots$$

Potenz von $\left(x-\mathfrak{T}\left(\frac{\mathfrak{f}\mathfrak{w}}{4\mathfrak{f}}\right)\right)$ teilbar. Da aber:

$$(1-1)^i=1+\binom{i}{2}+\binom{i}{4}+\cdots-\binom{i}{1}-\binom{i}{3}-\cdots=0$$

ist, so hebt sich der Faktor ganz weg. Somit ist in der Tat $\mathfrak{S}_{4\mathfrak{f}}(x)$ eine ganze rationale Funktion. Die Koeffizienten gehören, wie die von $F_{4\mathfrak{f}}$, dem Ringklassenkörper an. Die Wurzeln von $\mathfrak{S}_{4\mathfrak{f}}(x)$ sind nur noch diejenigen $\mathfrak{T}\left(\frac{\mathfrak{f}\mathfrak{w}}{4\mathfrak{f}}\right)$, deren $\mathfrak{f}$ zu $(4)\mathfrak{f}$ teilerfremd ist.

Der Grad von $F_{4\mathfrak{f}:\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_i}$ ist nach dem vorigen:

$$n\left(\mathfrak{z}\frac{\bar{\mathfrak{f}}}{\mathfrak{p}_1\cdots\mathfrak{p}_i}\right)=n(\mathfrak{z})\,\frac{n(\bar{\mathfrak{f}})}{n(\mathfrak{p}_1)n(\mathfrak{p}_2)\cdots n(\mathfrak{p}_i)},$$

derjenige von $\mathfrak{S}_{4\mathfrak{f}}(x)$ somit nach Satz 62:

$$n(\mathfrak{z})n(\bar{\mathfrak{f}})\left(1-\frac{1}{n(\mathfrak{p}_1)}\right)\left(1-\frac{1}{n(\mathfrak{p}_2)}\right)\cdots\left(1-\frac{1}{n(\mathfrak{p}_n)}\right)=n(\mathfrak{z})\varphi(\bar{\mathfrak{f}}).$$

129. Satz: *Ist $\mathfrak{f}$ ein zu $\mathfrak{w}$ teilerfremdes Ideal von $k(\sqrt{m})$, so genügen die Funktionswerte $\mathfrak{T}\left(\frac{\mathfrak{f}\mathfrak{w}}{4\mathfrak{f}}\right)$, wo $\mathfrak{f}$ zu $(4)\mathfrak{f}$ teilerfremd ist, einer algebraischen Gleichung:*

$$\mathfrak{S}_{4\mathfrak{f}}(x)=0,$$

deren Koeffizienten im Ringklassenkörper von $r(4)$ liegen, und deren Grad gleich $n(\mathfrak{z})\varphi(\bar{\mathfrak{f}})$ ist, falls $\mathfrak{f}$ das größte in $\mathfrak{f}$ enthaltene ungerade Ideal, und $\mathfrak{f}=\mathfrak{z}\mathfrak{f}$ ist. Dabei bedeutet $\frac{\mathfrak{f}\mathfrak{w}}{4\mathfrak{f}}$ eine Zahl $\frac{x_1\omega_1+x_2\omega_2}{4\nu_1}$, für die $x_1\equiv x_2\equiv\pm1\pmod 4$, $(\nu_1)=\mathfrak{f}_1\mathfrak{f}$, $\mathfrak{f}_1$ ungerade und zu $\mathfrak{w}$ teilerfremd, und $x_1\omega_1+x_2\omega_2\equiv 0\pmod{\mathfrak{f}_1}$ ist.

Kennt man eine Wurzel $\mathfrak{T}\left(\frac{\mathfrak{f}\mathfrak{w}}{4\mathfrak{f}}\right)$ von $\mathfrak{S}_{4\mathfrak{f}}(x)=0$, so findet man alle übrigen, indem man in $\mathfrak{T}\left(\xi\frac{\mathfrak{f}\mathfrak{w}}{4\mathfrak{f}}\right)$ ξ alle $(\mathrm{mod.}\ 4\mathfrak{f})$ inkongruenten ganzen, zu $\mathfrak{f}$ teilerfremden Zahlen durchlaufen läßt, für die $\xi\equiv\pm1\pmod 4$ ist. Es gibt genau $2n(\mathfrak{z})\varphi(\bar{\mathfrak{f}})$ solche Zahlen; denn es gibt $\varphi(4\mathfrak{z}\bar{\mathfrak{f}})=\varphi(4\mathfrak{z})\varphi(\bar{\mathfrak{f}})$ primitive Kongruenzklassen $(\mathrm{mod.}\ 4\mathfrak{f})$. Von diesen ist nur der $\varphi(4)^{\text{te}}$ Teil $\equiv+1\pmod 4$, und der gleiche Teil $\equiv-1\pmod 4$. Nun ist nach Satz 62:

$$\frac{\varphi(4\mathfrak{z})}{\varphi(4)}=n(\mathfrak{z}),$$

womit die Behauptung erwiesen ist. Je zwei dieser Werte können entgegengesetzt gleich gewählt werden, für dieselben ist dann $\mathfrak{T}$ gleich groß. Somit werden wirklich die $n(\mathfrak{z})\varphi(\mathfrak{f})$ Wurzeln so alle erhalten.

130. Satz: *Man erhält alle Wurzeln der Gleichung:*

$$\mathfrak{S}_{4\mathfrak{f}}(x) = 0,$$

aus einer Wurzel $\mathfrak{T}\left(\frac{\mathfrak{j}\mathfrak{w}}{4\mathfrak{f}}\right)$, *falls man in* $\mathfrak{T}\left(\xi\frac{\mathfrak{j}\mathfrak{w}}{4\mathfrak{f}}\right)$ *die Zahl* ξ *von* $k(\sqrt{m})$ *alle diejenigen* (mod. $4\mathfrak{f}$) *inkongruenten ganzen Zahlen durchlaufen läßt, die zu* $(4\mathfrak{f})$ *teilerfremd sind und der Bedingung genügen:*

$$\xi \equiv \pm 1 \text{ (mod. 4)}.$$

Die Resultate werden besonders einfach für ein *ungerades* $\mathfrak{f}$. Statt $\mathfrak{T}\left(\frac{\mathfrak{j}\mathfrak{w}}{4\mathfrak{f}}\right)$ können dann die Größen $\mathfrak{T}\left(\frac{\mathfrak{j}\mathfrak{w}}{\mathfrak{f}}\right)$ eingeführt werden. Denn nach Satz 124 ist für $\nu = 4$:

$$\mathfrak{T}\left(\frac{\mathfrak{j}\mathfrak{w}}{\mathfrak{f}}\right) = R\left(\mathfrak{T}\left(\frac{\mathfrak{j}\mathfrak{w}}{4\mathfrak{f}}\right)\right),$$

wo alle Koeffizienten der rationalen Funktion R dem Ringklassenkörper von $r(4)$ angehören.

131. Satz: *Die Funktionswerte* $\mathfrak{T}\left(\frac{\mathfrak{j}\mathfrak{w}}{\mathfrak{f}}\right)$ *gehören dem aus* $\mathfrak{T}\left(\frac{\mathfrak{j}\mathfrak{w}}{4\mathfrak{f}}\right)$ *und* t *in* $k(\sqrt{m})$ *gebildeten Körper an.*

Ist $\mathfrak{f}$ *ungerade*, so darf in:

$$\mathfrak{T}\left(\frac{\mathfrak{j}\mathfrak{w}}{\mathfrak{f}}\right) = \mathfrak{T}\left(\frac{x_1\omega_1 + x_2\omega_2}{\nu}\right) \quad (\mathfrak{j} \text{ teilerfremd zu } \mathfrak{f})$$

ν immer an die Bedingung $\nu \equiv 1$ (mod. 2) geknüpft werden, wie man sofort einsieht. Die Zahl $\mathfrak{T}\left(\frac{x_1\omega_1 + x_2\omega_2}{\nu}\right)$ ist aber nach Satz 125 Wurzel von:

$$z_\nu(x) = 0,$$

dessen oberster Koeffizient 1, und dessen übrige Koeffizienten ganze Zahlen des Ringklassenkörpers sind. $\mathfrak{T}$ ist daher selbst ganz.

132. Satz: *Ist* $\mathfrak{f}$ *ein ungerades Ideal von* $k(\sqrt{m})$, *so sind alle Werte* $\mathfrak{T}\left(\frac{\mathfrak{j}\mathfrak{w}}{\mathfrak{f}}\right)$ *ganze algebraische Zahlen.*

Ist $\mathfrak{f}$ größter gemeinsamer Teiler zweier ganzen Zahlen ν_1 und ν_2, die der Bedingung genügen: $\nu_1 \equiv \nu_2 \equiv 1$ (mod. 2), so kann wieder wie vorhin die Theorie entwickelt werden. Es sei $F_\mathfrak{f}(x)$ der größte gemeinsame Teiler von $z_{\nu_1}(x)$ und $z_{\nu_2}(x)$; dann hat $F_\mathfrak{f}(x)$ wieder den obersten Koeffizienten 1 und ganze Zahlen des Ringklassenkörpers von $r(4)$ als übrige Koeffizienten. Die Grade von z_{ν_1} und z_{ν_2} sind $\frac{1}{2}(n(\nu_1) - 1)$ und $\frac{1}{2}(n(\nu_2) - 1)$, derjenige von $F_\mathfrak{f}$ somit $\frac{1}{2}(n(\mathfrak{f}) - 1)$. Ist $\mathfrak{f} = \mathfrak{p}_1^{r_1}\mathfrak{p}_2^{r_2}\ldots\mathfrak{p}_n^{r_n}$,

wo die $\mathfrak{p}$ alles voneinander verschiedene, ungerade Primideale sind, so setzt man:

$$\mathfrak{S}_{\mathfrak{f}}(x) = \frac{F_{\mathfrak{f}} F_{\mathfrak{f}} \cdots F_{\mathfrak{f}} \cdots}{F_{\mathfrak{f}} \cdots F_{\mathfrak{f}} \cdots} \quad \begin{matrix} \mathfrak{p}_1\mathfrak{p}_2 & \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4 \\ \mathfrak{p}_1 & \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 \end{matrix} \tag{77}$$

Wie oben beweist man den Satz:

133. Satz: *Die Funktionswerte* $\mathfrak{T}\left(\frac{\mathfrak{j}\mathfrak{w}}{\mathfrak{f}}\right)$, *wo* $\mathfrak{f}$ *ein ungerades, zu* $\mathfrak{w}$ *teilerfremdes Ideal und* $\mathfrak{j}$ *ein zu* $\mathfrak{f}$ *teilerfremdes Ideal ist, genügen der Gleichung:*

$$\mathfrak{S}_{\mathfrak{f}}(x) = 0,$$

deren oberster Koeffizient eins, deren übrige Koeffizienten ganze Zahlen des Ringklassenkörpers von $r(4)$ *sind, und dessen Grad gleich* $\frac{1}{2}\varphi(\mathfrak{f})$ *ist.*

Man erhält alle Wurzeln der Gleichung aus einer $\mathfrak{T}\left(\frac{\mathfrak{j}\mathfrak{w}}{\mathfrak{f}}\right)$, *wenn man in* $\mathfrak{T}\left(\nu\frac{\mathfrak{j}\mathfrak{w}}{\mathfrak{f}}\right)$ ν *alle* (mod. $\mathfrak{f}$) *inkongruenten, zu* $\mathfrak{f}$ *teilerfremden ganzen Zahlen durchlaufen läßt, für die* $\nu \equiv 1$ (mod. 2) *ist.*

Sind $\mathfrak{T}\left(\frac{\mathfrak{j}\mathfrak{w}}{\mathfrak{f}}\right)$ und $\mathfrak{T}\left(\nu\frac{\mathfrak{j}\mathfrak{w}}{\mathfrak{f}}\right)$, wo $\nu \equiv 1$ (mod. 2) zu $\mathfrak{f}$ teilerfremd und keine Einheit ist, zwei beliebige Wurzeln von (77):

$$\mathfrak{T}\left(\frac{\mathfrak{j}\mathfrak{w}}{\mathfrak{f}}\right) = \mathfrak{T}\left(\frac{x_1\omega_1 + \bar{x}_2\omega_2}{\nu_1}\right), \quad (\nu_1) = \mathfrak{f}\mathfrak{f}_1, \quad \bar{x}_1\omega_1 + \bar{x}_2\omega_2 \equiv 0 \pmod{\mathfrak{f}_1},$$

$$\mathfrak{T}\left(\nu\frac{\mathfrak{j}\mathfrak{w}}{\mathfrak{f}}\right) = \mathfrak{T}\left(\nu\frac{\bar{x}_1\omega_1 + \bar{x}_2\omega_2}{\nu_1}\right),$$

so ergibt sich aus Satz 126 für $z = \frac{\bar{x}_1\omega_1 + \bar{x}_2\omega_2}{\nu_1}$:

$$\pm\frac{\mathfrak{T}\left(\nu\frac{\mathfrak{j}\mathfrak{w}}{\mathfrak{f}}\right)}{\mathfrak{T}\left(\frac{\mathfrak{j}\mathfrak{w}}{\mathfrak{f}}\right)} = \prod_{(\alpha)} \mathfrak{T}\left(\frac{\bar{x}_1\omega_1 + \bar{x}_2\omega_2}{\nu_1} + \frac{x_1\omega_1 + x_2\omega_2}{\nu}\right).$$

Da $\nu\nu_1 \equiv 1$ (mod. 2) ist, stehen nach Satz 132 rechts alles ganze, algebraische Zahlen. Daher ist auch der Quotient links eine ganze Zahl. Nun hätten wir ebensogut von Anfang an die beiden beliebigen Wurzeln miteinander vertauschen können. Somit ist der reziproke Wert:

$$\mathfrak{T}\left(\frac{\mathfrak{j}\mathfrak{w}}{\mathfrak{f}}\right) : \mathfrak{T}\left(\nu\frac{\mathfrak{j}\mathfrak{w}}{\mathfrak{f}}\right)$$

ebenfalls eine ganze algebraische Zahl, oder die Zahl ist eine Einheit.

134. Satz: *Der Quotient zweier Wurzeln der Gleichung* $\mathfrak{S}_{\mathfrak{f}}(x) = 0$ *ist eine algebraische Einheit, falls* $\mathfrak{f}$ *ein ungerades zu* $\mathfrak{w}$ *teilerfremdes Ideal von* $k(\sqrt{m})$ *ist.*

Umgekehrt ist auch jede Zahl $\mathfrak{T}\left(\frac{\bar{x}_1\omega_1 + \bar{x}_2\omega_2}{\nu_1} + \frac{x_1\omega_1 + x_2\omega_2}{\nu}\right)$ eine Einheit, sobald ν, ν_1 und $\mathfrak{w}$ teilerfremd, ν und $\nu_1 \equiv 1$ (mod. 2) sind, und

auch ν_1 wenigstens ein Primideal enthält, das nicht in (ν) und im Zähler $\bar{x}_1\omega_1 + \bar{x}_2\omega_2$ aufgeht. Kann man daher $\mathfrak{f}$ in zwei teilerfremde Ideale zerspalten, $\mathfrak{f} = \mathfrak{f}_1\mathfrak{f}_2$, die wieder ungerade sein werden, so gibt es zwei unter sich und zu $\mathfrak{w}$ teilerfremde Zahlen ν_1 und ν_2 in $\mathfrak{f}_1$ respektive $\mathfrak{f}_2$, für die $\nu_1 \equiv \nu_2 \equiv 1 \pmod 2$ ist. Dann kann man $\bar{x}_1$, $\bar{x}_2$, x_1, x_2 so berechnen, daß:

$$\frac{(\bar{x}_1\omega_1 + \bar{x}_2\omega_2)}{(\nu_1)} = \frac{\mathfrak{j}_1\mathfrak{w}}{\mathfrak{f}_1}, \quad \frac{(x_1\omega_1 + x_2\omega_2)}{(\nu_2)} = \frac{\mathfrak{j}_2\mathfrak{w}}{\mathfrak{f}_2},$$

$$\frac{\bar{x}_1\omega_1 + \bar{x}_2\omega_2}{\nu_1} + \frac{x_1\omega_1 + x_2\omega_2}{\nu_2} = \frac{X_1\omega_1 + X_2\omega_2}{\nu} = \frac{\mathfrak{j}\mathfrak{w}}{\mathfrak{f}},$$

wo ν ein Teiler von $\nu_1\nu_2$ ist, der sicherlich durch $\mathfrak{f} = \mathfrak{f}_1\mathfrak{f}_2$ teilbar ist, und wo $\mathfrak{j}$ zu $\mathfrak{f}$ teilerfremd ist. Denn $\frac{\nu_1\nu_2(X_1\omega_1 + X_2\omega_2)}{\nu}$ ist nach Voraussetzung ganz, kann also immer in der Form $\nu_2(\bar{x}_1\omega_1 + \bar{x}_2\omega_2) + \nu_1(x_1\omega_1 + x_2\omega_2)$ dargestellt werden. $\mathfrak{T}\left(\frac{\mathfrak{j}\mathfrak{w}}{\mathfrak{f}}\right)$ ist daher stets eine Einheit.

135. **Satz:** *Ist das ungerade Ideal $\mathfrak{f}$ von $k(\sqrt{m})$ wenigstens durch zwei voneinander verschiedene Primideale teilbar, so ist jede Wurzel $\mathfrak{T}\left(\frac{\mathfrak{j}\mathfrak{w}}{\mathfrak{f}}\right)$, wo $\mathfrak{j}$ zu $\mathfrak{f}$ teilerfremd ist, eine algebraische Einheit.*

Mit Hilfe dieser Resultate kann das konstante Glied von $F_{\mathfrak{f}}(x)$ berechnet werden. Nach Definition ist $F_{\mathfrak{f}}$ größter gemeinsamer Teiler von z_{ν_1} und z_{ν_2}, wo ν_1 und ν_2 die oben festgelegten Bedingungen erfüllen. $F_{\mathfrak{f}}(0)$ ist somit Teiler von $z_{\nu_1}(0)$ und $z_{\nu_2}(0)$. Nun ist nach Satz 125 $(z_{\nu_1}(0)) = (\nu_1)$, $(z_{\nu_2}(0)) = (\nu_2)$, daher muß $F_{\mathfrak{f}}(0)$ Teiler des größten gemeinsamen Teilers $\mathfrak{f}$ von ν_1 und ν_2 sein. Ist:

$$z_{\nu_1}(x) \equiv F_{\mathfrak{f}}(x)\bar{z}_{\nu_1}(x), \quad z_{\nu_1}(0) = F_{\mathfrak{f}}(0)\bar{z}_{\nu_1}(0) = (\sqrt{-1})^{\alpha}\nu_1,$$

und setzt man $\mathfrak{f}_1\mathfrak{f} = (\nu_1)$, so ist $\bar{z}_{\nu_1}(0)$ sicher Teiler von $\mathfrak{f}_1$, also zu $\mathfrak{f}$ nach Voraussetzung teilerfremd. Somit muß $F_{\mathfrak{f}}(0)$ durch $\mathfrak{f}$ teilbar sein, d. h.

$$\mathfrak{f} = (F_{\mathfrak{f}}(0)). \tag{78}$$

136. **Satz:** *Alle Ideale von $k(\sqrt{m})$ sind im Ringklassenkörper von $r(4)$ Hauptideale.*

Denn nach (78) folgt der Satz für alle ungeraden Ideale $\mathfrak{f}$, da wir $\mathfrak{w}$ stets zu $\mathfrak{f}$ teilerfremd annehmen können. Jede Klasse von $k(\sqrt{m})$ enthält aber unendlich viele ungerade Ideale, also gilt der Satz für alle Ideale.

Ist $\mathfrak{f} = \mathfrak{p}^r$ Potenz eines Primideals $\mathfrak{p}$, dessen Norm die rationale Primzahl p oder das Quadrat einer solchen p^2 ist, so folgt aus (77):

$$(\mathfrak{S}_{\mathfrak{p}^r}(0)) = \left(\frac{F_{\mathfrak{p}^r}(0)}{F_{\mathfrak{p}^{r-1}}(0)}\right) = \mathfrak{p}.$$

Ist $\mathfrak{f} = \mathfrak{p}_1^{r_1}\mathfrak{p}_2^{r_2}\cdots\mathfrak{p}_n^{r_n}$, wo alle $\mathfrak{p}$ voneinander verschieden sind und $n > 1$ ist, so ist $\mathfrak{p}$ im Zähler von $\mathfrak{S}_\mathfrak{f}(x)$ in (77) zur

$$r\left(1 + \binom{n}{2} + \binom{n}{4} + \cdots\right) - \left(\binom{n-1}{1} + \binom{n-1}{3} + \cdots\right)$$

und im Nenner zur:

$$r\left(\binom{n}{1} + \binom{n}{3} + \cdots\right) - \left(1 + \binom{n-1}{2} + \binom{n-1}{4} + \cdots\right)$$

Potenz enthalten. Da beide Exponenten gleich sind, ist $\mathfrak{S}_\mathfrak{f}(0)$ nicht durch $\mathfrak{p}$ teilbar. Da andere Primideale nicht in $\mathfrak{S}_\mathfrak{f}(0)$ aufgehen können, so ist $\mathfrak{S}_\mathfrak{f}(0)$ eine algebraische Einheit.

137. Satz: *Ist das ungerade Ideal* $\mathfrak{f}$ *Potenz eines Primideals* $\mathfrak{p}$, *so ist:*

$$\mathfrak{p} = (\mathfrak{S}_\mathfrak{f}(0));$$

gehen in $\mathfrak{f}$ *mehr als ein Primideal auf, so ist* $S_\mathfrak{f}(0)$ *eine algebraische Einheit.*

Nun ist $\mathfrak{S}_\mathfrak{f}(0)$ das Produkt aller $\frac{1}{2}\varphi(\mathfrak{f})$ Wurzeln $\mathfrak{T}\left(\frac{\mathfrak{f}\mathfrak{w}}{\mathfrak{f}}\right)$, und nach Satz 134 ist der Quotient von zweien derselben eine Einheit. Im Falle, daß $\mathfrak{f} = \mathfrak{p}^r$ Primidealpotenz ist, können wir daher schreiben:

$$\mathfrak{p} = \left(\mathfrak{T}\left(\frac{\mathfrak{f}\mathfrak{w}}{\mathfrak{p}^r}\right)\right)^{\frac{\varphi(\mathfrak{p}^r)}{2}}, \tag{79}$$

wo $\mathfrak{T}\left(\frac{\mathfrak{f}\mathfrak{w}}{\mathfrak{p}^r}\right)$ irgendeine der Wurzeln von $\mathfrak{S}_{\mathfrak{p}^r}$ bedeutet. Ist $\mathfrak{p}$ teilerfremd zu $4m$ und zur Diskriminante der Ringklassengleichung, so ist $\mathfrak{p}$ im Ringklassenkörper niemals durch das Quadrat eines Ideals teilbar, es wird dagegen im Körper der $\mathfrak{T}$ die $\frac{1}{2}\varphi(\mathfrak{f})^{\text{te}}$ Potenz eines Ideals.

Es sei nun $\mathfrak{p} = (\pi)$ ein Primideal ersten Grades, das in der Hauptklasse von $k(\sqrt{m})$ liegt. Es sei ungerade und $\pi \equiv 1 \pmod 2$, was keine Einschränkung bedeutet. In diesem Falle ist:

$$\mathfrak{S}_\mathfrak{p}(x) \equiv F_\mathfrak{p}(x) \equiv z_\pi(x).$$

Alle Koeffizienten von z mit Ausnahme des obersten sind symmetrische Funktionen der $\mathfrak{T}\left(\frac{\mathfrak{f}\mathfrak{w}}{\mathfrak{p}}\right)$, also durch $\mathfrak{T}\left(\frac{\mathfrak{f}\mathfrak{w}}{\mathfrak{p}}\right)$ teilbar. Sie liegen aber im Ringklassenkörper, daher müssen sie wegen (79) auch durch $\mathfrak{p}$ teilbar sein.

138. Satz: *Ist* $\mathfrak{p} = (\pi)$, $\pi \equiv 1 \pmod 2$, *ein ungerades Primideal ersten Grades der Hauptklasse von* $k(\sqrt{m})$, *so sind in*

$$\mathfrak{T}(\pi z) = \frac{\mathfrak{T}(z)z_\pi(\mathfrak{T}(z))^2}{n_\pi(\mathfrak{T}(z))^2}$$

alle Koeffizienten von z_π *und* n_π *mit Ausnahme des ersten bzw. letzten, ganze, durch* $\mathfrak{p}$ *teilbare Zahlen des Ringklassenkörpers.*

Siehe dazu Satz 125.

4. Der Strahlklassenkörper und seine Gruppe.

Den Entwicklungen sei wieder das ungerade Ideal $\mathfrak{w} = (\omega_1, \omega_2)$ zugrunde gelegt, dessen Basis den auf S. 115 angegebenen Bedingungen genügt. $t(\omega_1, \omega_2)$ ist dann eine bestimmende Zahl des Ringklassenkörpers von $r(4)$.

In $k(\sqrt{m})$ bilden wir jetzt den Strahl $s(4\mathfrak{f})$ mit dem Führer $(4)\mathfrak{f}$, der teilerfremd zu $\mathfrak{w}$ sei. Seine Klassenanzahl ist nach Satz 118:

$$h_s(4\mathfrak{f}) = \frac{1}{e}\varphi(4\mathfrak{f})h,$$

wo h die Klassenzahl des Körpers $k(\sqrt{m})$ und $e = 2$, 4 oder 6 ist, je nachdem $m \neq -1$, -3, $m = -1$, oder $m = -3$ ist. Das e_s von Satz 118 ist hier immer gleich eins. Die Ringklassenzahl von $r(4)$ ist nach Satz 84:

$$h_r(4) = \frac{2}{e}2^2 \cdot \left(1 - \tfrac{1}{2}\left(\frac{d}{2}\right)\right)h, \quad (d \text{ die Diskriminante von } k(\sqrt{m}))$$

und ist der Relativgrad von $\mathfrak{t}$ in bezug auf $k(\sqrt{m})$. Wir betrachten eine Wurzel $\mathfrak{T}\left(\frac{\mathfrak{j}\mathfrak{w}}{4\mathfrak{f}}\right)$ von $\mathfrak{S}_{4\mathfrak{f}}(x) = 0$.

139. Satz: *Die Funktionswerte* $\mathfrak{T}\left(\frac{\mathfrak{j}\mathfrak{w}}{4\mathfrak{f}}\right)$ *genügen im Körper* $k(\sqrt{m})$ *einer Gleichung vom Grade* $h_s(4\mathfrak{f})$.

Denn $\mathfrak{T}\left(\frac{\mathfrak{j}\mathfrak{w}}{4\mathfrak{f}}\right)$ genügt in bezug auf den Ringklassenkörper von $r(4)$ nach Satz 129 einer Gleichung vom Grade $n(\mathfrak{z})\varphi(\bar{\mathfrak{f}})$, falls $\mathfrak{f} = \mathfrak{z}\bar{\mathfrak{f}}$, und $\bar{\mathfrak{f}}$ das größte in $\mathfrak{f}$ enthaltene ungerade Ideal ist. Der Relativgrad von $\mathfrak{T}\left(\frac{\mathfrak{j}\mathfrak{w}}{4\mathfrak{f}}\right)$ in bezug auf $k(\sqrt{m})$ ist also höchstens:

$$H = n(\mathfrak{z})\varphi(\bar{\mathfrak{f}})h_r(4).$$

Andererseits ist nach den Sätzen 52, 62 und 118:

a) $m \equiv 1 \pmod 8$: $h_r(4) = \frac{2}{e}2h$,

$$h_s(4\mathfrak{f}) = \frac{1}{e}\varphi(4\mathfrak{f})h = \frac{1}{e}\varphi(4\mathfrak{z})\varphi(\bar{\mathfrak{f}})h = \frac{1}{e}n(4\mathfrak{z})(1 - \tfrac{1}{2})^2\varphi(\bar{\mathfrak{f}})h$$

$$= \frac{2}{e}2h \cdot n(\mathfrak{z})\varphi(\bar{\mathfrak{f}}) = h_r(4)n(\mathfrak{z})\varphi(\bar{\mathfrak{f}}) = H.$$

b) $m \equiv 5 \pmod 8$: $h_r(4) = \frac{2}{e}2 \cdot 3h$,

$$h_s(4\mathfrak{f}) = \frac{1}{e}\varphi(4\mathfrak{f})h = \frac{1}{e}\varphi(4\mathfrak{z})\varphi(\bar{\mathfrak{f}})h = \frac{1}{e}n(4\mathfrak{z})(1 - \tfrac{1}{4})\varphi(\bar{\mathfrak{f}})h$$

$$= \frac{2}{e}2 \cdot 3h \cdot n(\mathfrak{z})\varphi(\bar{\mathfrak{f}}) = h_r(4)n(\mathfrak{z})\varphi(\bar{\mathfrak{f}}) = H.$$

c) $m \not\equiv 1 \pmod 4$: $h_r(4) = \frac{2}{e}4h$,

$$h_s(4\mathfrak{f}) = \frac{1}{e}\varphi(4\mathfrak{f})h = \frac{1}{e}\varphi(4_\mathfrak{z})\varphi(\bar{\mathfrak{f}})h = \frac{1}{e}n(4_\mathfrak{z})(1-\tfrac{1}{2})\varphi(\bar{\mathfrak{f}})h$$
$$= \frac{2}{e}4h \cdot n(\mathfrak{z})\varphi(\bar{\mathfrak{f}})h = h_r(4)n(\mathfrak{z})\varphi(\bar{\mathfrak{f}}) = H.$$

Jeder Strahlklasse von $s(4\mathfrak{f})$ kann umkehrbar eindeutig eine Wurzel $\mathfrak{T}\left(\frac{\mathfrak{f}\mathfrak{w}}{4\mathfrak{f}}\right)$ von $\mathfrak{S}_{4\mathfrak{f}}(x) = 0$ zugeordnet werden. Nach Satz 122 ist durch $\mathfrak{w}$ eine bestimmte Ringklasse von $r(4)$ $\mathfrak{f}_r$ bestimmt, für die $t = t(\mathfrak{f}_r)$. Nach den eben hergeleiteten Formeln zerfällt jede Ringklasse in bezug auf $s(4\mathfrak{f})$ in $n(\mathfrak{z})\varphi(\bar{\mathfrak{f}})$ Strahlklassen. Wir greifen irgendeine dieser Strahlklassen heraus: $\mathfrak{f}_s$, und ordnen ihr die Wurzel $\mathfrak{T}\left(\frac{\mathfrak{f}\mathfrak{w}}{4\mathfrak{f}}\right)$ zu. Falls $\mathfrak{f}_r$ die Hauptringklasse ist, soll $\mathfrak{f}_s$ die Hauptstrahlklasse sein. Ist dann $\bar{\mathfrak{f}}_s$ eine andere Strahlklasse, in die $\mathfrak{f}_r$ zerfällt, und sind $\bar{\mathfrak{a}}$ und $\mathfrak{a}$ zwei Ideale aus $\bar{\mathfrak{f}}_s$ und $\mathfrak{f}_s$, für die also:

$$\frac{\bar{\mathfrak{a}}}{\mathfrak{a}} = \frac{(\bar{\nu})}{(\nu)}, \qquad \alpha = \frac{\bar{\nu}}{\nu},$$

wo $\alpha = \frac{\bar{\nu}}{\nu}$ im Ring $r(4)$ liegen muß, so darf man $\alpha \equiv 1 \pmod 4$ voraussetzen, da $\bar{\nu}$ und ν zu (2) teilerfremd, und nur bis auf den Faktor ± 1 bestimmt sind. Ist dann ξ eine ganze Zahl von $k(\sqrt{m})$, die den Bedingungen genügt: $\xi \equiv 1 \pmod 4$, $\xi \equiv \alpha \pmod{4\mathfrak{f}}$,

so ordnet man der Klasse $\bar{\mathfrak{f}}_s$ die Wurzel $\mathfrak{T}\left(\xi\frac{\mathfrak{f}\mathfrak{w}}{4\mathfrak{f}}\right)$ zu. Nach Satz 130 ist damit jeder Wurzel eine Strahlklasse $\mathfrak{f}_s$ zugeordnet. Umgekehrt ist durch $\mathfrak{T}\left(\xi\frac{\mathfrak{f}\mathfrak{w}}{4\mathfrak{f}}\right)$ auch die Strahlklasse $\bar{\mathfrak{f}}_s$ eindeutig bestimmt, da durch $\mathfrak{w}$ zunächst $\mathfrak{f}_r$, und durch ξ die Klasse $\bar{\mathfrak{f}}_s$, in die $\mathfrak{f}_r$ im $s(4\mathfrak{f})$ zerfällt, eindeutig bestimmt ist, da alle Ideale $\bar{\mathfrak{a}}$ für die:

$$\frac{\bar{\mathfrak{a}}}{\mathfrak{a}} = \frac{(\bar{\nu})}{(\nu)}, \quad \alpha = \frac{\bar{\nu}}{\nu} \equiv \xi \pmod{4\mathfrak{f}}, \quad \xi \equiv 1 \pmod 4$$

ist, in derselben Strahlklasse liegen.

140. Satz: *Jeder Strahlklasse $\mathfrak{f}_s$ von $s(4\mathfrak{f})$ in $k(\sqrt{m})$ kann umkehrbar eindeutig eine Wurzel $\mathfrak{T}\left(\frac{\mathfrak{f}\mathfrak{w}}{4\mathfrak{f}}\right)$ einer Gleichung $\mathfrak{S}_{4\mathfrak{f}}(x)=0$ zugeordnet werden.*

Dieser Satz zeigt, daß wir:

$$\mathfrak{T}\left(\frac{\mathfrak{f}\mathfrak{w}}{4\mathfrak{f}}\right) = \mathfrak{T}(\mathfrak{f}_s) \tag{80}$$

setzen dürfen, wo $\mathfrak{f}_s$ die der Wurzel zugeordnete Strahlklasse ist. Um $\mathfrak{T}(\mathfrak{f}_s)$ zu erhalten, ist es ganz gleichgültig, von welchem Ideal der Strahlklasse $\mathfrak{f}_s$ man ausgeht. Man bestimmt zuerst $\mathfrak{f}_r$, in der $\mathfrak{f}_s$ liegt, wodurch $t = t(\mathfrak{f}_r)$ gegeben ist, und dann aus den oben angegebenen Kongruenzen ξ,

wodurch $\mathfrak{k}_s$ gegeben ist, nachdem für jede Strahlklasse eine Zuordnung willkürlich festgesetzt worden ist. Eine Ausnahme bildet nur die Hauptringklasse, der zunächst immer die Hauptstrahlklasse zugeteilt ist. Wir können speziell die Zuteilung so vornehmen: Es sei ω_1^0, ω_2^0 so gewählt, daß $\mathfrak{t}(\omega_1^0, \omega_2^0) = \mathfrak{t}(\mathfrak{k}_r^0)$ wird, wo $\mathfrak{k}_r^0$ die Hauptringklasse ist. $\mathfrak{w}_0 = (\omega_1^0, \omega_2^0)$ sei ein zu (ν) teilerfremdes Ideal von $\mathfrak{k}_r^0$ und:

$$\frac{x_1\omega_1^0 + x_2\omega_2^0}{4\nu} = \frac{\mathfrak{f}^0\mathfrak{w}_0}{(4)\mathfrak{f}}, \quad \mathfrak{T}\left(\frac{x_1\omega_1^0 + x_2\omega_2^0}{4\nu}; \omega_1^0, \omega_2^0\right) = \mathfrak{T}\left(\frac{\mathfrak{f}^0\mathfrak{w}_0}{(4)\mathfrak{f}}; \omega_1^0, \omega_2^0\right) = \mathfrak{T}(\mathfrak{k}_s^0),$$

wo $\mathfrak{k}_s^0$ die Hauptstrahlklasse ist. Ist $\xi \equiv 1 \pmod 4$, und $\bar{\mathfrak{k}}_s^0$ die Strahlklasse von (ξ), so ist:

$$\mathfrak{T}\left(\xi\frac{\mathfrak{f}\mathfrak{w}_0}{(4)\mathfrak{f}}; \omega_1^0, \omega_2^0\right) = \mathfrak{T}(\bar{\mathfrak{k}}_s^0).$$

Es sei $\mathfrak{w}$ ein zweites, zu (ν) und $\mathfrak{w}_0$ teilerfremdes Ideal, und seine Basis ω_1, ω_2 so gewählt, daß $\mathfrak{t}(\omega_1, \omega_2) = \mathfrak{t}(\mathfrak{k}_r)$, wo $\mathfrak{k}_r$ die Ringklasse von $\mathfrak{w}_r$ ist. Man bestimme die ganze Zahl η so, daß:

$$\eta \equiv 0 \pmod{\mathfrak{w}}, \quad \eta \equiv x_1\omega_1^0 + x_2\omega_2^0 \pmod{(4\nu)\mathfrak{w}_0}$$

ist. Dann ist auch $\mathfrak{T}\left(\frac{\eta}{4\nu}; \omega_1^0, \omega_2^0\right) = \mathfrak{T}(\mathfrak{k}_s^0)$ und man setze, falls $\mathfrak{k}_s$ die Strahlklasse von $\mathfrak{w}$ ist:

$$\mathfrak{T}\left(\frac{\eta}{4\nu}; \omega_1, \omega_2\right) = \mathfrak{T}(\mathfrak{k}_s).$$

Es muß dann wieder: $\mathfrak{T}\left(\xi\frac{\eta}{4\nu}; \omega_1, \omega_2\right) = \mathfrak{T}(\bar{\mathfrak{k}}_s^0\mathfrak{k}_s)$

sein. Macht man dies für je ein Ideal $\mathfrak{w}_r$ aus jeder Ringklasse $\mathfrak{k}_r$, so ist dadurch die Zuteilung ausgeführt.

Sind $\mathfrak{k}_s$ und $\bar{\mathfrak{k}}_s$ zwei in derselben Ringklasse liegende Strahlklassen von $s(4\mathfrak{f})$ und:

$$\mathfrak{T}(\mathfrak{k}_s) = \mathfrak{T}\left(\frac{\mathfrak{f}\mathfrak{w}}{4\mathfrak{f}}\right), \quad \mathfrak{T}(\bar{\mathfrak{k}}_s) = \mathfrak{T}\left(\xi\frac{\mathfrak{f}\mathfrak{w}}{4\mathfrak{f}}\right), \quad \xi \equiv 1 \pmod 4,$$

so ist ξ durch das Verhältnis $\bar{\mathfrak{k}}_s : \mathfrak{k}_s$ bestimmt. Dieses Verhältnis ist aber eine Strahlklasse $\mathfrak{k}_s^0$, die in der Hauptringklasse liegt:

$$\bar{\mathfrak{k}}_s : \mathfrak{k}_s = \mathfrak{k}_s^0,$$

und die nach unseren Festsetzungen durch die Zahl ξ festgelegt wird. Nach Satz 125 ist jetzt:

$$(81) \qquad \mathfrak{T}(\bar{\mathfrak{k}}_s) = R(\mathfrak{T}(\mathfrak{k}_s)) = R_{\mathfrak{t}_s^0}(\mathfrak{T}(\mathfrak{k}_s), \mathfrak{t}(\mathfrak{k}_r)), \quad \bar{\mathfrak{k}}_s : \mathfrak{k}_s = \mathfrak{k}_s^0.$$

$R_{\mathfrak{t}_s^0}$ ist eine rationale Funktion, die nur von $\mathfrak{k}_s^0$ abhängt, und deren Koeffizienten rationale Funktionen von $\mathfrak{t}(\mathfrak{k}_r)$ mit in $k(\sqrt{m})$ rationalen Zahlkoeffizienten sind. *Somit liegen alle Wurzeln von* $\mathfrak{S}_{4\mathfrak{f}}(x) = 0$ *im Körper von* $\mathfrak{T}(\mathfrak{k}_s)$, $\mathfrak{t}(\mathfrak{k}_r)$ *und* $k(\sqrt{m})$.

Es seien $\mathfrak{k}_r$ und $\mathfrak{k}_r^*$ zwei verschiedene Ringklassen von $r(4)$. Die zugehörigen Modulfunktionen $t(\mathfrak{k}_r)$ und $t(\mathfrak{k}_r^*)$ seien durch $\mathfrak{w}$ und $\mathfrak{w}^*$ (teilerfremd zu $\mathfrak{f}$) gegeben (Satz 122). Ist $\overline{\mathfrak{w}}$ ein Ideal der Ringklasse $\mathfrak{k}_r : \mathfrak{k}_r^* = \overline{\mathfrak{k}}_r$, so kann man für $\mathfrak{w}$ stets $\overline{\mathfrak{w}}\mathfrak{w}^*$ nehmen. Den Klassen $\mathfrak{k}_r$ und $\mathfrak{k}_r^*$ seien die Strahlklassen $\mathfrak{k}_s$ und $\mathfrak{k}_s^*$ zugeordnet, d. h. es sei:

$$\mathfrak{T}(\mathfrak{k}_s) = \mathfrak{T}\left(\frac{\mathfrak{f}\mathfrak{w}}{4\mathfrak{f}};\ \omega_1, \omega_2\right), \quad \mathfrak{T}(\mathfrak{k}_s^*) = \mathfrak{T}\left(\frac{\mathfrak{f}^*\mathfrak{w}^*}{4\mathfrak{f}};\ \omega_1^*, \omega_2^*\right).$$

Wegen $\mathfrak{w} = \overline{\mathfrak{w}}\mathfrak{w}^*$ hat: $\mu = \frac{x_1\omega_1 + x_2\omega_2}{4\nu} = \frac{\mathfrak{f}\mathfrak{w}}{4\mathfrak{f}}$

auch die Form $\frac{\mathfrak{f}^*\mathfrak{w}^*}{4\mathfrak{f}}$. Wir wählen die noch willkürliche Klasse $\mathfrak{k}_s^*$ von $\mathfrak{k}_r^*$ so, daß auch:

$$\frac{\mathfrak{f}^*\mathfrak{w}^*}{4\mathfrak{f}} = \mu = \frac{x_1\omega_1 + x_2\omega_2}{4\nu}.$$

Dann ist: $\mathfrak{T}(\mathfrak{k}_s) = \mathfrak{T}(\mu;\ \omega_1, \omega_2)$, $\mathfrak{T}(\mathfrak{k}_s^*) = \mathfrak{T}(\mu;\ \omega_1^*, \omega_2^*)$.

Wir können $\overline{\mathfrak{w}}$ als zu $\mathfrak{w}^*$, d, $4\mathfrak{f}$ teilerfremd und ohne rationalen Teiler annehmen. Ferner sei ω_2^* in $\mathfrak{w}^*$ so gewählt, daß $\omega_2^* \equiv 0 \pmod{\overline{\mathfrak{w}}}$ und die Basis von $\overline{\mathfrak{w}}$ $\overline{w}$, ω_2^* ist:

$$\overline{\mathfrak{w}} = (\overline{w}, \omega_2^*).$$

Dann muß $\mathfrak{w} = (\overline{w}\omega_1^*, \omega_2^*)$ durch seine Basis $\overline{w}\omega_1^*, \omega_2^*$ gegeben sein, und wir können setzen:

$$\mathfrak{T}(\mathfrak{k}_s) = \mathfrak{T}(\mu;\ \overline{w}\omega_1^*, \omega_2^*), \quad \mathfrak{T}(\mathfrak{k}_s^*) = \mathfrak{T}(\mu;\ \omega_1^*, \omega_2^*).$$

Nach Satz 113 ist somit:

$$\mathfrak{T}(\mathfrak{k}_s^*) = \overline{R}(\mathfrak{T}(\mathfrak{k}_s),\ t(\mathfrak{k}_r),\ t(\mathfrak{k}_r^*),\ \sqrt{\pm C}),$$

wo $\overline{R}$ eine nur von $\overline{\mathfrak{w}}$ abhängende, rationale Funktion ihrer Argumente mit rationalen Zahlkoeffizienten ist. Da $\overline{\mathfrak{w}}$ durch $\mathfrak{k}_r : \mathfrak{k}_r^*$ bestimmt ist, hängt $\overline{R}$ von $\overline{\mathfrak{k}}_r = \mathfrak{k}_r : \mathfrak{k}_r^*$ ab. Nach Satz 89 ist:

$$t(\mathfrak{k}_r^*) = r(t(\mathfrak{k}_r)),$$

wo auch die rationale Funktion $r(x)$ mit Koeffizienten in $k(\sqrt{m})$ nur von dem Quotienten $\overline{\mathfrak{k}}_r$ abhängt. Also wird:

$$\mathfrak{T}(\mathfrak{k}_s^*) = R^*(\mathfrak{T}(\mathfrak{k}_s),\ t(\mathfrak{k}_r),\ \sqrt{m},\ \sqrt{\pm C}).$$

Nach Satz 113 ist:

$$\pm\sqrt{\pm C} = \prod_{h=1}^{\frac{\overline{w}-1}{2}} \mathfrak{T}(h\omega_1^*;\ \overline{w}\omega_1^*,\ \omega_2^*)^{-1}.$$

Wir wählen eine Zahl $\overline{\omega}$ in $\overline{\mathfrak{w}}'$ so, daß sie zu $\overline{\mathfrak{w}}$ und $(4)\mathfrak{f}$ teilerfremd ist und der Kongruenz $\overline{\omega} \equiv \overline{w} \pmod 4$ genügt. Da $(\overline{w}) = \overline{\mathfrak{w}}\overline{\mathfrak{w}}'$ ist, sind:

$$\overline{\omega}_1 = \omega_1^*\overline{\omega},\ \overline{\omega}_2 = \frac{\omega_2^*\overline{\omega}}{\overline{w}},$$

ganze Zahlen und Basis eines Ideals:

$$\mathfrak{v} = (\overline{\omega}_1, \overline{\omega}_2) = \frac{(\overline{\omega})\mathfrak{w}}{(\overline{w})} = \frac{(\overline{\omega})\mathfrak{w}^*}{\overline{\mathfrak{w}}'}.$$

$\mathfrak{v}$ ist sicherlich zu $\overline{\mathfrak{w}}$ teilerfremd, da $\overline{\omega}$ und $\mathfrak{w}^*$ zu $\mathfrak{w}$ teilerfremd sind. $\mathfrak{T}(z; \omega_1, \omega_2)$ ist in z, ω_1, ω_2 homogen von nullter Ordnung, daher:

$$\mathfrak{T}(h\omega_1^*; \overline{w}\omega_1^*, \omega_2^*) = \mathfrak{T}\left(h\frac{\omega_1^*\overline{\omega}}{\overline{w}}; \omega_1^*\overline{\omega}, \frac{\omega_2^*\overline{\omega}}{\overline{w}}\right) = \mathfrak{T}(h\frac{\overline{\omega}_1}{\overline{w}}; \overline{\omega}_1, \overline{\omega}_2).$$

Die Zahl $\frac{\overline{\omega}_1}{\overline{w}}$ als Idealbruch geschrieben ergibt:

$$\frac{(\omega_1)}{(\overline{w})} = \frac{\overline{\mathfrak{f}}\mathfrak{v}}{\overline{\mathfrak{w}}}$$

und läßt sich nicht weiter kürzen, da $\overline{\omega}$ und ω_1^* zu $\overline{\mathfrak{w}}$ teilerfremd sind.

Alle Größen $\mathfrak{T}\left(h\frac{\overline{\mathfrak{f}}\mathfrak{v}}{\overline{\mathfrak{w}}}; \overline{\omega}_1, \overline{\omega}_2\right)$, $h = 1, 2, \ldots \frac{n(\overline{\mathfrak{w}})-1}{2}$,

sind, da $\mathfrak{w}$ ungerade ist, nach Satz 133 Wurzeln von $F_{\overline{\mathfrak{w}}}(x) = 0$, daher muß:

$$\pm\sqrt{\pm C^{-1}} = \prod_{h=1}^{\frac{\overline{w}-1}{2}} \mathfrak{T}\left(h\frac{\overline{\mathfrak{f}}\mathfrak{v}}{\overline{\mathfrak{w}}}; \overline{\omega}_1, \overline{\omega}_2\right) = \pm F_{\overline{\mathfrak{w}}}(0)$$

sein. $F_{\overline{\mathfrak{w}}}(O)$ ist aber nach Satz 133 und den vorhergehenden Überlegungen eine rationale Funktion von $\mathfrak{t}(\overline{\omega}_1, \overline{\omega}_2)$ mit in $k(\sqrt{m})$ rationalen Koeffizienten. Aus der Definition von $\mathfrak{v}$ folgt:

$$(\overline{w})\mathfrak{v} = (\overline{\omega})\mathfrak{w},$$

d. h. $\mathfrak{v}$ und $\mathfrak{w}$ liegen wegen $\overline{w} \equiv \overline{\omega}$ (mod. 4) in derselben Ringklasse von $r(4)$. Somit ist $\mathfrak{t}(\overline{\omega}_1, \overline{\omega}_2) = \mathfrak{t}(\mathfrak{k}_r)$, und $\sqrt{\pm C}$ eine rationale Funktion von $\mathfrak{t}(\mathfrak{k}_r)$ mit in $k(\sqrt{m})$ rationalen Koeffizienten, die nur von $\overline{\mathfrak{w}}$ abhängt.

Aus all dem geht hervor, daß wir setzen dürfen:

$$\mathfrak{T}(\mathfrak{k}_s^*) = \overline{R}_{\overline{\mathfrak{k}}_r}(\mathfrak{T}(\mathfrak{k}_s), \mathfrak{t}(\mathfrak{k}_r), \sqrt{m}), \quad \mathfrak{k}_r^* : \mathfrak{k}_r = \overline{\mathfrak{k}}_r, \tag{82}$$

wo $\overline{\mathfrak{k}}_r$ in Abweichung der bisherigen Bezeichnung die Ringklasse ist, in der $\mathfrak{k}_s^* : \mathfrak{k}_s$ liegt.

Es seien schließlich $\mathfrak{k}_s^*$ und $\mathfrak{k}_s$ zwei ganz beliebige Strahlklassen von $s(4\mathfrak{f})$ und $\mathfrak{k}_r^*$ und $\mathfrak{k}_r$ die Ringklassen von $\mathfrak{k}_s^*$ und $\mathfrak{k}_s$. Ferner setzen wir:

$$\mathfrak{k}_s^* : \mathfrak{k}_s = \overline{\mathfrak{k}}_s, \quad \mathfrak{k}_r^* : \mathfrak{k}_r = \overline{\mathfrak{k}}_r.$$

Wir bestimmen in $\mathfrak{k}_r^*$ diejenige Strahlklasse $\mathfrak{k}_s'$, die mit $\mathfrak{k}_s$ in der obigen Beziehung steht, so daß (82) anzuwenden ist:

$$\mathfrak{T}(\mathfrak{k}_s') = \overline{R}_{\overline{\mathfrak{k}}_r}(\mathfrak{T}(\mathfrak{k}_s), \mathfrak{t}(\mathfrak{k}_r), \sqrt{m}), \quad \mathfrak{k}_r^* : \mathfrak{k}_r = \overline{\mathfrak{k}}_r.$$

$\overline{\mathfrak{k}}_r$ ist die Ringklasse von $\mathfrak{k}_s$. Weiter liegen $\mathfrak{k}_s^*$ und $\mathfrak{k}_s'$ in derselben Ringklasse. Also wird nach (81):

$$\mathfrak{T}(\mathfrak{k}_s^*) = R_{\mathfrak{k}_s^0}^*(\mathfrak{T}(\mathfrak{k}_s'), \mathfrak{t}(\mathfrak{k}_r)), \quad \mathfrak{k}_s^* : \mathfrak{k}_s' = \mathfrak{k}_s^0.$$

$\mathfrak{f}_s^0$ ist aber nur von $\bar{\mathfrak{f}}_s$ abhängig. Denn ist $\mathfrak{f}_s^e$ diejenige Strahlklasse von $\bar{\mathfrak{f}}_r$, der die Hauptstrahlklasse im Sinne von (82) entspricht, und ist $\mathfrak{w}_e$ ein Ideal von $\mathfrak{f}_s^e$, $\mathfrak{e}$ ein solches der Hauptstrahlklasse, so kann man dieselben so wählen, daß:

$$\frac{\mathfrak{j}_e \mathfrak{w}_e}{(4)\mathfrak{f}} = \frac{\mathfrak{j}_e \mathfrak{e}}{(4)\mathfrak{f}},$$

und diese Idealbrüche sind unkürzbar. Erweitert man mit einem Ideal $\mathfrak{w}'$ von $\mathfrak{f}_s'$, so ist:

$$\frac{\mathfrak{j}_e \mathfrak{w}_e \mathfrak{w}'}{(4)\mathfrak{f}} = \frac{\mathfrak{j}_e \mathfrak{e} \mathfrak{w}'}{(4)\mathfrak{f}},$$

$\mathfrak{w}'\mathfrak{e}$ liegt in $\mathfrak{f}_s'$, $\mathfrak{w}_e \mathfrak{w}'$ in der Ringklasse $\mathfrak{f}_s^*$, somit muß $\mathfrak{f}_s^* = \mathfrak{f}_s^e \mathfrak{f}_s'$ und $\mathfrak{f}_s^0 = \mathfrak{f}_s^e$ sein, und $\mathfrak{f}_s^0$ ist nur von $\bar{\mathfrak{f}}_s$ abhängig, also:

$$\mathfrak{T}(\mathfrak{f}_s^*) = R_{\bar{\mathfrak{f}}_s}^*(\mathfrak{T}(\mathfrak{f}_s'), \mathfrak{t}(\mathfrak{f}_r)).$$

Aus beiden gefundenen Beziehungen folgt:

(83) $\mathfrak{T}(\mathfrak{f}_s^*) = R_{\bar{\mathfrak{f}}_s}(\mathfrak{T}(\mathfrak{f}_s), \mathfrak{t}(\mathfrak{f}_r))$, $\mathfrak{f}_s^* : \mathfrak{f}_s = \bar{\mathfrak{f}}_s$, $\mathfrak{f}_r$ die Ringklasse von $\mathfrak{f}_s$,

wo $R_{\bar{\mathfrak{f}}_s}$ eine nur von der Strahlklasse $\bar{\mathfrak{f}}_s$ abhängige rationale Funktion mit Koeffizienten, die dem Körper $k(\sqrt{m})$ angehören, ist.

141. Satz: *Der aus den Funktionswerten $\mathfrak{T}(\mathfrak{f}_s)$, $\mathfrak{t}(\mathfrak{f}_r)$ gebildete Körper ist im Bereiche des Körpers $k(\sqrt{m})$ Galoissch.*

Der aus $\mathfrak{T}(\mathfrak{f}_s)$ und $\mathfrak{t}(\mathfrak{f}_r)$ gebildete Körper heißt *Strahlklassenkörper*. Er ist in bezug auf $k(\sqrt{m})$ Galoissch und höchstens vom Grade $h_s(4\mathfrak{f})$. Wir bezeichnen ihn mit $*(4\mathfrak{f})$, da er, wie wir im zweiten Teile sehen werden, in gewissem Sinne alle zu einem Führer $(4)\mathfrak{f}$ möglichen Strahlklassenkörper umfaßt.

Um die Gruppe von $*(4\mathfrak{f})$ bezüglich $k(\sqrt{m})$, die höchstens von der Ordnung $h_s(4\mathfrak{f})$ sein kann, zu bestimmen, nehmen wir zu den beiden Strahlklassen $\mathfrak{f}_s^*$ und $\mathfrak{f}_s$ noch eine beliebige dritte Strahlklasse $\mathfrak{f}_s^{**}$ und setzen:

$$\mathfrak{f}_s^* = \bar{\mathfrak{f}}_s \mathfrak{f}_s, \quad \mathfrak{f}_s^{**} = \bar{\bar{\mathfrak{f}}}_s \mathfrak{f}_s^*.$$

Dann folgt nach (83):

$$\mathfrak{T}(\mathfrak{f}_s^{**}) = R_{\bar{\mathfrak{f}}_s}(\mathfrak{T}(\mathfrak{f}_s^*), \mathfrak{t}(\mathfrak{f}_r^*)) = R_{\bar{\mathfrak{f}}_s}(\mathfrak{T}(\bar{\bar{\mathfrak{f}}}_s \mathfrak{f}_s), \mathfrak{t}(\bar{\bar{\mathfrak{f}}}_r \mathfrak{f}_r)) = R_{\bar{\mathfrak{f}}_s \bar{\bar{\mathfrak{f}}}_s}(\mathfrak{T}(\mathfrak{f}_s), \mathfrak{t}(\mathfrak{f}_r)),$$

wo die rationalen Funktionen R jeweils nur von der Strahlklasse ihres Index abhängen. Da die Strahlklassen nach Satz 120 in bezug auf ihre Multiplikation eine Abelsche Gruppe bilden, und rechts eine Funktion steht, die nur von dem Produkt $\bar{\mathfrak{f}}_s \bar{\bar{\mathfrak{f}}}_s$ abhängt, dürfen wir bei der Zusammensetzung der Funktionen die Reihenfolge vertauschen, d. h.:

$$R_{\bar{\mathfrak{f}}_s}(\mathfrak{T}(\bar{\bar{\mathfrak{f}}}_s \mathfrak{f}_s), \mathfrak{t}(\bar{\bar{\mathfrak{f}}}_r \mathfrak{f}_r)) = R_{\bar{\mathfrak{f}}_s}(\mathfrak{T}(\bar{\bar{\mathfrak{f}}}_s \mathfrak{f}_s), \mathfrak{t}(\bar{\bar{\mathfrak{f}}}_r \mathfrak{f}_r)).$$

Die Galoissche Gruppe ist somit Abelsch und holomorph mit der Gruppe der Strahlklassen.

Um die Ordnung der Gruppe zu bestimmen, setzen wir in der Formel von Satz 138 $z = \frac{\mathfrak{f}\mathfrak{w}}{(4)\mathfrak{f}}$; dann wird wegen $n_\pi^s(x) \equiv \pm 1 \pmod{\mathfrak{p}}$:

$$\mathfrak{T}\left(\pi \frac{\mathfrak{f}\mathfrak{w}}{4\mathfrak{f}}\right) \equiv \mathfrak{T}\left(\frac{\mathfrak{f}\mathfrak{w}}{4\mathfrak{f}}\right)^p \pmod{\mathfrak{p}},$$

oder wenn $\mathfrak{f}_s$ die Strahlklasse von $\frac{\mathfrak{f}\mathfrak{w}}{4\mathfrak{f}}$, $\mathfrak{f}_\mathfrak{p}$ diejenige von $\mathfrak{p}$ ist:

$$\mathfrak{T}(\mathfrak{f}_\mathfrak{p}\mathfrak{f}_s) \equiv \mathfrak{T}(\mathfrak{f}_s)^p \pmod{\mathfrak{p}}. \tag{84}$$

Wäre nun der Grad der Gleichung, der $\mathfrak{T}(\mathfrak{f}_s)$ genügt, kleiner als $h_s(4\mathfrak{f})$, so müßte $\mathfrak{S}_{4\mathfrak{f}}(x)$, dessen Wurzel $\mathfrak{T}(\mathfrak{f}_s)$ ist, im Ringklassenkörper von $r(4)$ zerfallen, da letzterer nach Satz 89 in $k(\sqrt{m})$ irreduzibel ist und $h_s(4\mathfrak{f})$ das Produkt des Grades von $\mathfrak{S}_{4\mathfrak{f}}(x)$ und des Grades des Ringklassenkörpers ist. Wir nehmen an, es sei:

$$\mathfrak{S}_{4\mathfrak{f}}(x) \equiv \mathfrak{S}'_{4\mathfrak{f}}(x)\mathfrak{S}''_{4\mathfrak{f}}(x),$$

wo auch die Koeffizienten von $\mathfrak{S}'_{4\mathfrak{f}}$ und $\mathfrak{S}''_{4\mathfrak{f}}$ im Ringklassenkörper liegen. $\mathfrak{T}(\mathfrak{f}_s)$ sei Wurzel von $\mathfrak{S}'_{4\mathfrak{f}}$. Ist $\mathfrak{T}(\bar{\mathfrak{f}}_s)$ eine Wurzel von $\mathfrak{S}''_{4\mathfrak{f}}$, so ist $\bar{\mathfrak{f}}_s$ und $\mathfrak{f}_s$ in derselben Ringklasse $\mathfrak{f}_r$, also $\bar{\mathfrak{f}}_s : \mathfrak{f}_s$ durch eine Ringzahl α darstellbar. Wir werden im zweiten Teil unabhängig von der hier zu beweisenden Tatsache den Satz beweisen, daß es immer unendlich viele Primideale der Hauptringklasse $\mathfrak{p} = (\pi)$ gibt, für die π dieser Ringzahl $(\alpha) \pmod{4\mathfrak{f}}$ kongruent ist. $\mathfrak{p}$ liegt dann in der Strahlklasse $\bar{\mathfrak{f}}_s : \mathfrak{f}_s = \mathfrak{f}_\mathfrak{p}$, und nach (84) ist

$$\mathfrak{T}(\bar{\mathfrak{f}}_s) \equiv \mathfrak{T}(\mathfrak{f}_s)^p \pmod{\mathfrak{p}}.$$

Wir dürfen $\mathfrak{p}$ zur Diskriminante der Klassengleichung von $j(\mathfrak{f}_r)$ und der Gleichung $\mathfrak{S}_{4\mathfrak{f}}(x) = 0$ teilerfremd und ungerade annehmen. Nun ist nach der auf S. 72 abgeleiteten Formel entsprechend für Ringklassen, da $\mathfrak{f}_\mathfrak{p} \sim 1$ ist in $r(4)$:

$$(j(\mathfrak{f}_r)^p - j(\mathfrak{f}_r))(j(\mathfrak{f}_r) - j(\mathfrak{f}_r)^p) \equiv 0 \pmod{\mathfrak{p}},$$

also:

$$j(\mathfrak{f}_r)^p - j(\mathfrak{f}_r) \equiv 0 \pmod{\mathfrak{p}}.$$

Da $j(\mathfrak{f}_r)$ in $k(\sqrt{m})$ bestimmende Zahl des Ringklassenkörpers von $r(4)$ ist, so gilt für alle zur Diskriminante der Ringklassengleichung von $j(\mathfrak{f}_r)$ teilerfremden Zahlen α desselben (Satz 61):

$$\alpha^p \equiv \alpha \pmod{\mathfrak{p}}, \text{ also:}$$

$$\mathfrak{S}'_{4\mathfrak{f}}(x)^p \equiv \mathfrak{S}'_{4\mathfrak{f}}(x^p) \pmod{\mathfrak{p}}, \quad \text{und} \quad \mathfrak{S}'_{4\mathfrak{f}}(\mathfrak{T}(\mathfrak{f}_s))^p \equiv \mathfrak{S}'_{4\mathfrak{f}}(\mathfrak{T}(\mathfrak{f}_s)^p) \pmod{\mathfrak{p}}.$$

Wegen der obigen Kongruenz ist:

$$\mathfrak{S}'_{4\mathfrak{f}}(\mathfrak{T}(\mathfrak{f}_s)^p) \equiv \mathfrak{S}'_{4\mathfrak{f}}(\mathfrak{T}(\bar{\mathfrak{f}}_s)) \pmod{\mathfrak{p}}.$$

Also muß, da $\mathfrak{T}(\mathfrak{f}_s)$ Wurzel von $\mathfrak{S}'_{4\mathfrak{f}}$ ist:

$$\mathfrak{S}'_{4\mathfrak{f}}(\mathfrak{T}(\bar{\mathfrak{f}}_s)) \equiv 0 \pmod{\mathfrak{p}},$$

werden. Da

$$\mathfrak{S}'_{4\mathfrak{f}}(\mathfrak{T}(\bar{\mathfrak{f}}_s)) = (\mathfrak{T}(\bar{\mathfrak{f}}_s) - \mathfrak{T}(\mathfrak{f}_s)) \ldots,$$

und $\mathfrak{p}$ zur Diskriminante von $\mathfrak{S}_{4\mathfrak{f}}(x)$ teilerfremd vorausgesetzt wurde, so ist der Widerspruch gefunden und die Annahme zu verwerfen.

Daß aber die Diskriminante von null verschieden ist, $\mathfrak{p}$ also wirklich zu ihr teilerfremd gewählt werden kann, sieht man daraus, daß alle Wurzeln $\mathfrak{T}\left(\xi\frac{\mathfrak{j}\mathfrak{w}}{4\mathfrak{f}}\right)$ beim Durchlaufen eines zu $(4)\mathfrak{f}$ teilerfremden, (mod. $4\mathfrak{f}$) inkongruenten Systems von ganzen Zahlen ξ lauter verschiedene Werte annehmen.

142. Satz: *Der Strahlklassenkörper* $*(4\mathfrak{f})$ *ist ein im Bereiche von* $k(\sqrt{m})$ *Abelscher Körper vom Relativgrade* $h_s(4\mathfrak{f})$ *in bezug auf* $k(\sqrt{m})$. *Seine Gruppe ist holoedrisch isomorph mit der Gruppe der Strahlklassen von* $s(4\mathfrak{f})$ *in* $k(\sqrt{m})$.

Wir haben in Satz 131 gesehen, daß auch $\mathfrak{T}\left(\frac{\mathfrak{j}\mathfrak{w}}{\mathfrak{f}}\right)$ dem Strahlklassenkörper angehört. Wenn $\mathfrak{f}$ ein ungerades Ideal ist, können wir hieraus noch weitere Schlüsse ziehen. Setzt man in:

$$\mathfrak{T}(2z) = \frac{\mathfrak{T}(z)\left(4\mathfrak{T}(z) + t\,\mathfrak{k}(z) + 4\right)}{\left(\mathfrak{T}(z)^2 - 1\right)^2} = \frac{\mathfrak{T}_1(z)^2}{\left(\mathfrak{T}(z)^2 - 1\right)^2}$$

für $z = \frac{x_1\omega_1 + x_2\omega_2}{4\nu} = \frac{\mathfrak{j}\mathfrak{w}}{4\mathfrak{f}}$, wo $x_1 \equiv x_2 \equiv \pm 1$ (mod. 4) sein soll, so folgt:

$$\sqrt{\mathfrak{T}\left(\frac{\mathfrak{j}\mathfrak{w}}{2\mathfrak{f}}\right)} = \pm\frac{\mathfrak{T}_1\left(\frac{\mathfrak{j}\mathfrak{w}}{4\mathfrak{f}}\right)}{\mathfrak{T}\left(\frac{\mathfrak{j}\mathfrak{w}}{4\mathfrak{f}}\right)^2 - 1}.$$

Da $\mathfrak{f}$ ungerade ist, kann $\nu \equiv 1$ (mod. 2) gemacht werden, so daß wegen (38):

$$\mathfrak{T}\left(\frac{\mathfrak{j}\mathfrak{w}}{2\mathfrak{f}}\right) = \mathfrak{T}\left(\frac{x_1\omega_1 + x_2\omega_2}{2\nu}\right) = \mathfrak{T}\left(\frac{\frac{x_1 - \nu}{2}\omega_1 + \frac{x_2 - \nu}{2}\omega_2}{\nu} + \frac{\omega_1 + \omega_2}{2}\right)$$

$$= \frac{1}{\mathfrak{T}\left(\frac{x_1'\omega_1 + x_2'\omega_2}{\nu}\right)} = \frac{1}{\mathfrak{T}\left(\frac{\bar{\mathfrak{j}}\mathfrak{w}}{\mathfrak{f}}\right)}$$

wird. Daher lautet die gefundene Formel:

$$\sqrt{\mathfrak{T}\left(\frac{\bar{\mathfrak{j}}\mathfrak{w}}{\mathfrak{f}}\right)} = \pm\frac{\mathfrak{T}\left(\frac{\mathfrak{j}\mathfrak{w}}{4\mathfrak{f}}\right)^2 - 1}{\mathfrak{T}_1\left(\frac{\mathfrak{j}\mathfrak{w}}{4\mathfrak{f}}\right)}.$$

Um $\mathfrak{T}_1\left(\frac{\mathfrak{j}\mathfrak{w}}{4\mathfrak{f}}\right)$ zu berechnen, bedenken wir, daß $\mathfrak{T}_1(\nu z) : \mathfrak{T}_1(z)$ als gerade Funktion von z eine rationale Funktion von $\mathfrak{T}(z)$ ist:

$$\mathfrak{T}_1(z) = \mathfrak{T}_1(\nu z)\,R(\mathfrak{T}(z)).$$

Die Koeffizienten von R liegen im Ringklassenkörper von $r(4)$; denn man findet sie durch Differentiation der Formel von Satz 125 nach ξ

gemäß der Definitionsformel (43). Setzt man jetzt $z = \frac{x_1\omega_1 + x_2\omega_2}{4\nu}$, so wird:

$$\mathfrak{T}_1\left(\frac{\mathfrak{f}\,\mathfrak{w}}{4\mathfrak{f}}\right) = \pm\,\mathfrak{T}_1\left(\frac{\omega_1+\omega_2}{4}\right) R\left(\mathfrak{T}\left(\frac{\mathfrak{f}\,\mathfrak{w}}{4\mathfrak{f}}\right)\right),$$

da wegen $x_1 \equiv x_2 \equiv \pm 1 \pmod 4$ $\mathfrak{T}_1\left(\frac{x_1\omega_1 + x_2\omega_2}{4}\right) = \pm\,\mathfrak{T}_1\left(\frac{\omega_1+\omega_2}{4}\right)$ sein muß. Nun ist $\mathfrak{T}\left(\frac{\omega_1+\omega_2}{4}\right) = 1$, also:

$$\mathfrak{T}_1\left(\frac{\omega_1+\omega_2}{4}\right)^2 = \mathfrak{T}\left(\frac{\omega_1+\omega_2}{4}\right)\left(4\mathfrak{T}\left(\frac{\omega_1+\omega_2}{4}\right)^2 + t\,\mathfrak{T}\left(\frac{\omega_1+\omega_2}{4}\right) + 4\right)$$
$$= 4 + t + 4 = 8 + t,$$

$$\mathfrak{T}_1\left(\frac{\omega_1+\omega_2}{4}\right) = \pm\sqrt{t+8}. \tag{85}$$

Setzt man dies oben ein, so erhält man:

$$\mathfrak{T}_1\left(\frac{\mathfrak{f}\,\mathfrak{w}}{4\mathfrak{f}}\right) = \pm\sqrt{(t+8)}\,R\left(\mathfrak{T}\left(\frac{\mathfrak{f}\,\mathfrak{w}}{4\mathfrak{f}}\right)\right),$$

also:
$$\sqrt{(t+8)\,\mathfrak{T}\left(\frac{\bar{\mathfrak{f}}\,\mathfrak{w}}{\mathfrak{f}}\right)} = R^*\left(\mathfrak{T}\left(\frac{\mathfrak{f}\,\mathfrak{w}}{4\mathfrak{f}}\right)\right),$$

wo R^* Koeffizienten hat, die im Ringklassenkörper von $r(4)$ liegen.

143. Satz: *Ist* $\mathfrak{f}$ *ein ungerades Ideal, so liegen die Funktionswerte* $\sqrt{(t+8)\,\mathfrak{T}\left(\frac{\bar{\mathfrak{f}}\,\mathfrak{w}}{\mathfrak{f}}\right)}$ *im Strahlklassenkörper* $*(4\mathfrak{f})$. *Sie sind ganze, algebraische Zahlen*

Denn $\mathfrak{T}\left(\frac{\bar{\mathfrak{f}}\,\mathfrak{w}}{\mathfrak{f}}\right)$ ist nach Satz 132 ganz, und $(t+8)$ ist ganz, da t ganz ist (Satz 121). Die Relativnorm von $(t+8)$ findet man aus (64), indem man dort für $t: -8$ einsetzt. Man findet: 2^{12}.

144. Satz: *Die ganze Zahl* $(t+8)$ *hat nur gerade Idealteiler, d. h. ist nur durch die Primideale von* (2) *teilbar.*

Ist $\mathfrak{f} = \mathfrak{p}^r$ die Potenz eines ungeraden Primideals $\mathfrak{p}$, so ist nach (79):

$$\mathfrak{p} = \left(\mathfrak{T}\left(\frac{\bar{\mathfrak{f}}\,\mathfrak{w}}{\mathfrak{p}^r}\right)\right)^{\frac{1}{2}\varphi(\mathfrak{p}^r)}.$$

Bildet man aus $\mathfrak{T}\left(\frac{\bar{\mathfrak{f}}\,\mathfrak{w}}{\mathfrak{p}^r}\right)$ und $\sqrt{(t+8)\,\mathfrak{T}\left(\frac{\bar{\mathfrak{f}}\,\mathfrak{w}}{\mathfrak{p}^r}\right)}$ das Ideal $\mathfrak{P}$, so sieht man, daß wegen Satz 144:

$$\mathfrak{p} = \mathfrak{P}^{\varphi(\mathfrak{p}^r)} \quad \text{sein muß.} \tag{86}$$

145. Satz: *Ist* $\mathfrak{f} = \mathfrak{p}^r$ *Potenz eines ungeraden Primideals* $\mathfrak{p}$, *so wird* $\mathfrak{p}$ *im Strahlklassenkörper* $*(4\mathfrak{p}^r)$ *die* $\varphi(\mathfrak{p}^r)^{\text{te}}$ *Potenz eines Ideals.*

Ist $\mathfrak{p}$ zur Diskriminante des Ringklassenkörpers teilerfremd, so folgt hieraus schon die Irreduzibilität von $*(4\mathfrak{p}^r)$.

Verzeichnis der Definitionen.

Verzeichnis der Sätze.

I. Kapitel.

II. Kapitel.

III. Kapitel.

IV. Kapitel.

V. Kapitel.

Namenverzeichnis.

Sachverzeichnis.

Zahlentheorie. Von weil. Prof. Dr. *F. Bachmann* in Weimar. Versuch einer Gesamtdarstellung dieser Wissenschaft in ihren Hauptteilen.
I. Teil: Die Elemente der Zahlentheorie. [XII u. 264 S.] gr. 8. Neudruck 1921. Geh. M. 6.—, geb. M. 7.80. II. Teil: Die analytische Zahlentheorie. [XVI u. 494 S.] gr. 8. Neudruck 1921. Geh. M. 11.60, geb. M. 13.—. III. Teil: Die Lehre von der Kreisteilung und ihre Beziehungen zur Zahlentheorie. 2., unv. Aufl. [XII u. 299 S.] gr. 8. 1921. Geh. M. 6.80, geb. M. 8.80. IV. Teil: Die Arithmetik der quadrat. Formen. I. Abt. [XVI u. 668 S.] gr. 8. 1898. Geb. M. 17.—. II. Abt. Hrsg. von Dr. *R. Haußner*, Prof. an der Universität Jena. Mit einem Titelbild und 20 Textfiguren. [XXII u. 537 S.] gr. 8. 1923. Geh. M. 17.60, geb. M. 19.60. V. Teil: Allgemeine Arithmetik der Zahlenkörper. [XXII u. 548 S.] gr. 8. 1905. Geh. M. 12.60, geb. M. 14.60

Diophantische Approximationen. Eine Einführung in die Zahlentheorie. Von Dr. *H. Minkowski*, weil. Prof. a. d. Univ. Göttingen. Mit 82 Textfig. [VIII u. 236 S.] gr. 8. 1907. Geb. M. 8.—

Die komplexen Veränderlichen und ihre Funktionen. Fortsetzung der Grundzüge der Differential- u. Integralrechnung, zugleich eine Einführung in d. Funktionentheorie. Von Dr. *G. Kowalewski*, Prof. a. d. deutschen Universität zu Prag. Mit 124 Fig. [IV u. 455 S.] gr. 8. 1911. M. 10.60, geb. M. 12.60

Lehrbuch der Funktionentheorie. Von Dr. *W. F. Osgood*, Prof. an der Harvard-Univ. Cambridge, Mass. I. Bd. 2. Aufl. Mit 158 Fig. [XII u. 766 S.] gr. 8. 1912. Geh. M. 17.—, geb. M. 19.—. II. Bd. [1. Teil u. d. Pr. 1924.]

Lehrbuch der Funktionentheorie. Von Dr. *L. Bieberbach*, Prof. an der Univ. Berlin. Bd. I: Elemente der Funktionentheorie. Mit 80 Fig. im Text. [VI u. 314 S.] gr. 8. 1921. Geh. M. 6.—, geb. M. 8.—. Bd. II. [In Vorb. 24.]

Vorlesungen über Zahlen- und Funktionenlehre. Von Geh. Hofrat Dr. *A. Pringsheim*, Prof. a. d. Univ. München. 2 Bde. (TmL XL.) I. Bd. I. Abt. Reelle Zahlen und Zahlenfolgen. 2. Aufl. [XII u. 292 S.] gr. 8. 1923. Geh. M. 7.—, geb. M. 8.40. II. Abt. Unendliche Reihen m. reellen Gliedern. [VIII u. 514 S.] gr. 8. 1916. Geh. M. 5.—, geb. M. 6.40. III. Abteilung. Komplexe Zahlen, Reihen mit komplexen Gliedern, unendliche Produkte und Kettenbrüche. [IX u. 461 S.] gr. 8. 1921. Geh. M. 11.60, geb. M. 13.60. II. Bd. [In Vorb. 1924.]

Vorlesungen über reelle Funktionen. Von Dr. *C. Carathéodory*, Prof. a. d. Universität Athen. [X u. 704 S.] gr. 8. 1918. Geh. M. 15.60, geb. M. 18.—

Die elliptischen Funktionen und ihre Anwendungen. Von Dr. *R. Fricke*, Prof. a. d. Techn. Hochschule in Braunschweig. I. Teil: Die funktionentheoretischen u. analyt. Grundlagen. Mit 83 Textfig. [X u. 500 S.] gr. 8. 1916. Geh. M. 12.60, geb. M. 14.60. II. Teil: Die algebraischen Ausführungen. Mit 40 Textfig. [VIII u. 546 S.] gr. 8. 1922. Geh. M. 14.–, geb. M. 16.–. III. Teil. [In Vorb. 1924.]

Entwicklung der Funktionen einer komplexen Variablen nach den Funktionen des elliptischen Zylinders. Von Dr. *O. Volk*, Assistent a. math. Seminar der Universität München. [38 S.] 8. 1920. Geh. M. 1.20

Über Systeme analytischer Funktionen, welche ein Additionstheorem besitzen. Von *P. J. Myrberg*, Dozent a. d. Univ. Helsingfors. (Preisschriften der Jablonowski-Gesellschaft, 50.) M. 2.20

Lehrbuch der Thetafunktionen. Von Geh. Hofrat Dr. *A. Krazer*, Prof. an der Technischen Hochschule in Karlsruhe. Mit 10 Textfig. [XXIV u. 509 S.] gr. 8. 1903. Geb. M. 14.60

Die Lehre von den Kettenbrüchen. Von Dr. *O. Perron*, Prof. an der Universität München. [XII u. 520 S.] gr. 8. 1913. Geh. M. 12.60, geb. M. 14.60

Verlag von B. G. Teubner in Leipzig und Berlin

Neuere Werke aus dem Gebiete der Mathematik

Abhandlungen über den mathematischen Unterricht in Deutschland, veranlaßt durch die Internationale Mathematische Unterrichtskommission, hrsg. von F. Klein. 5 Bände. Auch in 38 einzeln käuflichen Heften. 1909—1916. Geb. bzw. steif geh. Sonderprospekt erschienen.

Berichte und Mitteilungen, veranlaßt durch die Internationale Mathematische Unterrichtskommission. 2 Folgen in 1 Bande.

Abhandlungen u. Vorträge auf d. Geb. d. Mathem., Naturwiss. u. Technik.

Heft 3: A. Brill, Das Relativitätsprinzip. Eine Einführung in die Theorie. 4. Auflage. Mit 6 Figuren im Text. [IV u. 44 S.] gr. 8. 1920. Geh. n. ℳ 1.20

— 4: H. Hohenner, Der Hohennersche Präzisionsdistanzmesser und seine Verbindung mit einem Theodolit. Mit 7 Abb. [64 S.] gr. 8. 1919. Geh. n. ℳ 1.60

— 5: L. Schlesinger, Raum, Zeit und Relativitätstheorie. Gemeinverständliche Vorträge. Mit 8 Figuren im Text. [IV u. 40 S.] gr. 8. 1920. Geh. n. ℳ —.70

— 6: Hochmuth, K., Der Kreiselkompaß. Mit 20 Fig. [33 S.] gr. 8. 1921. Geh. n. ℳ 50.—

— 7: A. Lotze, Die Grundgleichungen der Mechanik, insbes. starrer Körper. Neu entwickelt mit Graßmanns Punktrechnung. [50 S.] gr. 8. 1922. Geh. n. ℳ —.90

— 8: Mises, R. v., Naturwissenschaft und Technik der Gegenwart. Eine akademische Rede mit Zusätzen. [II u. 32 S.] gr. 8. 1922. Geh. n. ℳ —.50

Ahrens, W., Math. Unterhaltungen u. Spiele. I. Bd. 3., verb. Aufl. Mit 200 Fig. [VIII u. 400 S.] 1921. II. Bd. 2. Aufl. Mit 128 Fig. [X u. 455 S.] gr. 8. 1918. Geh. je n. ℳ 5.90 geb. je n. ℳ 5.70

Bachmann, L., Das Schachspiel u. seine historische Entwicklung, dargestan an der Spielführung der hervorragendsten Schachmeister. [Ersch. Ende Sommer 23.]

Bachmann, P., Die Arithmetik der quadratischen Formen. Hrsg. von R. Haußner. (4. Teil der Zahlentheorie.) Mit 20 Textfig. Abt. II. [U. d. Pr. 23.]

Bibliothek, Mathematisch-physikalische. Gemeinverständliche Darstellungen aus der Elementar-Mathematik u. Physik für Schule u. Leben. Hrsg. von W. Lietzmann und A. Witting. kl. 8. Kart. je n. ℳ —.70 Neue Bände:

10. B. Kerst, Ebene Geometrie. 1923.
42. Schips, M., Mathematik und Biologie. 1922.
43. A. Witting, Einführung i. d. Trigonometrie. Eine elem. Darstellung ohne Logarithmen. 1922.
44/45. P. Kirchberger, Atom- und Quantentheorie. I. Atomtheorie. 1922. II. Quantentheorie. 1923.
46. H. Schütze, Die mathematischen Grundlagen der Lebensversicherung. 1922.
47. A. Witting, Abgekürzte Rechnung nebst einer Einführung in die Rechnung mit Funktionstafeln insbes. mit Logarithmen. 1922.
48. A. Witting, Funktionen, Schaubilder und Funktionstafeln. Eine elementare Einführung in die graphische Darstellung und in die Interpolation. 1922.
49. E. Fettweis, Wie man einstens rechnete. 1923.
51. H. Onnen, Kreisevolventen und ganze algebraische Funktionen. 1923.
52. W. Lietzmann u. V. Trier, Wo steckt der Fehler? 3. Aufl. 1923.
53. W. Lietzmann, Trugschlüsse. 3. Aufl. des I. Teiles von: Wo steckt der Fehler? 1923.
54. R. Rothe, Elementarmathematische Aufgaben mit Beziehungen zur Technik. 1923.]

Bieberbach, L., Lehrbuch der Funktionentheorie. Teil I. Elemente der Funktionentheorie. 2., verb. Aufl. Mit 80 Figuren. [VI u. 314 S.] gr. 8. 1923.

Birkemeier, W., Über den Bildungswert der Mathematik. Ein Beitrag zur philosophischen Pädagogik. (Wissensch. u. Hypothese. Bd. XXV.) [VI u. 191 S.] 8. 1923. Geh. n. ℳ 4.50, geb. n. ℳ 5.—

Borel, E., Die Elemente der Mathematik. Dtsch. v. P. Stäckel. I. Bd.: Arithmetik u. Algebra nebst d. Elementen d. Differentialrechn. 2. Aufl. Mit 56 Textfig. u. 3 Taf. [XVI u. 404 S.] 8. 1919. n. ℳ 5.—, geb. n. ℳ 6.60. II. Bd.: Geometrie. Mit 1 Einführung i. d. eb. Trigonom. 2. Aufl. Mit 442 Textfig. u. 2 Taf. [XVI u. 380 S.] 8. 1920. n. ℳ 4.70, geb. n. ℳ 6.20

Carathéodory, C., Vorlesungen über reelle Funktionen. Mit 47 Fig. im Text. [X u. 704 S.] gr. 8. 1918. Geh. n. ℳ 10.—, geb. n. ℳ 12.—

Cesàro, E., Einleitung in die Infinitesimalrechnung. Mit zahlr. Übungsbeispielen. Nach einem Manuskript des Verf. deutsch hrsg. von G. Kowalewski. 2., gekürzte Aufl. Mit 26 Fig. [IV u. 488 S.] gr. 8. 1922. Geb. n. ℳ 7.70

Neuere Werke aus dem Gebiete der Mathematik

Czuber, E., Wahrscheinlichkeitsrechnung u. ihre Anwend. a. Fehlerausgleichung, Statistik u. Lebensversich. In 2. Bde. II. Bd. Math.. Statistik. Mathemat. Grundl. d. Lebensversicherung. 3. Aufl. Mit 34 Fig. [X u. 470 S.] gr. 8. 1921. Geh. n. ℳ 6.20, geb. n. ℳ 7.70

———— Einführung in die höhere Mathematik. 3. Aufl. Mit 114 Fig. im Text. [X u. 382 S.] gr. 8. 1922. Geb. n. ℳ 6.20

———— Die philosophischen Grundlagen der Wahrscheinlichkeitsrechnung. (Wissenschaft und Hypothese. Bd. XXIV.) [VIII u. 343 S.] 8. 1923. Geh. n. ℳ 10.—, geb. n. ℳ 10.60

———— Mathematische Bevölkerungstheorie. Mit 71 Fig. i. Text. [XIV u. 357 S.] gr. 8. [Erscheint Juli 1923.]

Dingeldey, F., Sammlung von Aufgaben zur Anwendung der Differential- und Integralrechnung. I. Teil: Aufgaben zur Anwendung der Differentialrechnung. Mit 99 Fig. [V u. 202 S.] gr. 8. 1922. 2. Aufl. Geh. n. ℳ 2.10, geb. n. ℳ 3.30. II. Teil: Aufgaben zur Anwendung der Integralrechnung. 3. Aufl. Mit 96 Fig. i. Text. [IV u. 387 S.] gr. 8. 1923. Geh. n. ℳ 4.50, geb. n. ℳ 6.20

Fricke, R., Die elliptischen Funktionen und ihre Anwendungen. I. Teil: Die funktionentheoretischen u. analyt. Grundlagen. Mit 83 Textfig. [X u. 500 S.] gr. 8. 1916. Geh. n. ℳ 6.50, geb. n. ℳ 8.— II. Teil. Die algebraischen Ausführungen. Mit 40 in den Text gedr. Fig. [VIII u. 546 S.] gr. 8. 1922. Geh. n. ℳ 7.10, geb. n. ℳ 8.60

———— Lehrbuch d. Differential- u. Integralrechnung u. ihrer Anwendg.

I. Band: Differentialrechnung. 2. u. 3. Aufl. Mit 129 in d. Text gedruckten Fig., einer Sammlung von 253 Aufgaben und einer Formeltabelle. [X u. 388 S.] gr. 8. 1921. Geh. n. ℳ 4.80, geb. n. ℳ 6.30

II. Band: Integralrechnung. 2. u. 3. Aufl. Mit 100 in den Text gedruckten Figuren, einer Sammlung von 242 Aufgaben und 1 Formeltabelle. [IV u. 406 S.] gr. 8. 1921. Geh. n. ℳ 4.80, geb. n. ℳ 6.30

Gutzmer, A., Die Tätigkeit des Deutschen Ausschusses für den mathematischen und naturwissenschaftlichen Unterricht in den Jahren 1908—1913. [VIII u. 482 S.] gr. 8. 1914. Geh. n. ℳ 5.50, geb. n. ℳ 6.—

Handbuch d. angewandt. Mathem. Hrsg. v. H. E. Timerding. In 6 Teil. M. Textfig. 8.

I. Praktische Analysis, von H. v. Sanden. 2., verb. Aufl. Mit 32 Fig. [XVIII u. 195 S.] 1923. Kart. n. ℳ 4.60

II. Darstellende Geometrie, v. J. Hjelmslev. [IX u. 320 S.] 1914. Geh. n. ℳ 5.60, geb. n. ℳ 6.60

III. Grundzüge der Geodäsie, v. M. Näbauer. [XVI u. 420 S.] 1915. Geh. n. ℳ 7.50, geb. n. ℳ 8.70

Heffter, L., Die Grundlagen der Geometrie als Unterbau für die analytische Geometrie. Mit 11 Fig. im Text. [IV, 27 u. VIII S.] 1921. Geh. n. ℳ —.70

———— Lehrbuch der analytischen Geometrie. II. Bd.: Geometrie im Bündel und im Raum. Mit 101 Fig. i. Text. [XII u. 423 S.] gr. 8. 1923. Geh. n. ℳ 9.50, geb. n. ℳ 11.— Früher erschien: I. Bd.: Geometrie in den Grundgebilden erster Stufe und in der Ebene. Geb. n. ℳ 13.60

Kommerell, K., Der Begriff des Grenzwertes i. d. Elementarmathematik. Ein Versuch zur Vertief. d. math. Unterr. Mit 25 Fig. i. T. [IV u. 62 S.] gr. 8. 1922. Geh. n. ℳ 1.30

Kowalewski, G., Grundzüge der Differential- u. Integralrechn. 3. Aufl. Mit 31 Textfig. [IV u. 416 S.] gr. 8. 1923. Geh. n. ℳ 6.30, geb. n. ℳ 7.80

———— Die komplexen Veränderlichen und ihre Funktionen. 2. Aufl. Mit 124 Textfig. [IV u. 455 S.] gr. 8. 1923. Geh. n. ℳ 6.20, geb. n. ℳ 7.20

Kultur der Gegenwart, Die. Herausg. von P. Hinneberg. III. Teil. Abt. I. Die mathematischen Wissenschaften. Unter Leitung von F. Klein. In 5 Lieferungen:

A) A. Voß, Die Beziehungen der Mathematik zur Kultur der Gegenwart. H. E. Timerding, Die Verbreitung mathem. Wissens und mathem. Auffassung. 2. Lieferung. 1914. Geh. n. ℳ 2.60

B) H. G. Zeuthen, Die Mathematik im Altertum und im Mittelalter. 1. Lieferung. 1912. n. ℳ 1.60

E) A. Voß, Über die mathematische Erkenntnis. 3. Lieferung. 1914. n. ℳ 2.40

Landau, E., Einführung in die elementare u. analyt. Theorie der algebraischen Zahlen u. der Ideale. Mit 14 Textfig. [VII u. 143 S.] 1918. Geh. n. ℳ 2.40

Lie, S., Gesammelte Abhandlungen. 7 Bände. Herausgegeben von Fr. Engel u. P. Heegaard. Bd. III: Abhandlungen zur Theorie der Differentialgleichungen 1. Abt. Hrsg. von Fr. Engel. [XVI u. 789 S.] 1922. Kart. n. ℳ 5.—. Bd. V: Transformationsgruppen. Hrsg. von Fr. Engel. [U. d. Pr. 1923.]

Neuere Werke aus dem Gebiete der Mathematik

Müller, E., Lehrbuch der darst. Geometrie für Techn. Hochschulen. 2 Bde. gr. 8. I. Bd. 3. Aufl. Mit 289 Fig. im Text u. 3 Taf. [XIV u. 370 S.] 1920. Geh. n. ℳ 4.—, geb. n. ℳ 5.50. II. Bd. 3. Aufl. Mit 328 Fig. [X u. 362 S.] 1923. Geh. n. ℳ 4.—, geb. n. ℳ 5.50

Myrberg, P. J., Über Systeme analytischer Funktionen, welche ein Additionstheorem besitzen. [II u. 23 S.] 1922. Geh. n. ℳ 1.50

Osgood, W. F., Lehrbuch der Funktionentheorie. I. Bd. 4. Aufl. [U. d. Pr. 1923.] II. Bd. [In Vorb.]

Perry, J., Höhere Mathematik für Ingenieure. Autor. deutsche Bearbeitung von R. Fricke und F. Süchting. 4. Aufl. [Erscheint Juli 1923.]

Pringsheim, A., Vorles. über Zahlen- und Funktionenlehre. Bd. I. In 3 Abt. Abt. I. Reelle Zahlen u. Zahlenfolgen. 2. Aufl. [XII u. 292 S.] gr. 8. 1923. Geh. n. ℳ 6.—, geb. n. ℳ 6.90. Abt. II. Unendliche Reihen mit reellen Gliedern. [VIII S., S. 293–514.] gr. 8. 1916. Geh. n. ℳ 4.60, geb. n. ℳ 5.30. Abt. III. Komplexe Zahlen. Reihen mit kompl. Gliedern. Unendl. Produkte u. Kettenbrüche. [IX u. S. 515–976.] gr. 8. 1921. Geh. n. ℳ 8.90, geb. n. ℳ 10.30

Repertorium der höh. Mathematik. II. Bd. 2. Hälfte: Raumgeometrie. Von H. E. Timerding. 2., umgearb. Aufl. Mit 12 Fig. i. T. 1922. Geh. n. ℳ 7.80, geb. n. ℳ 9.90
Bisher liegen vor: I. Bd.: Analysis. 1. Hälfte. Geb. n. ℳ 8.—. II. Bd.: Geometrie. 1. Hälfte n. ℳ 8.—

Salmon, G., u. W. Fiedler, Analytische Geometrie des Raumes. Neu hrsg. von K. Kommerell. I. Teil. Die Elemente u. die Theorie d. Flächen 2. Ordnung. 5. Aufl. Mit 71 Fig. [X u. 612 S.] gr. 8. Geb. n. ℳ 12.70. 1. Lieferung. Mit 48 Fig. [X u. 366 S.] gr. 8. 1922. Geh. n. ℳ 6.60. 2. Lieferung. Mit 23 Fig. [IV u. 246 S.] gr. 8. 1922. Geh. n. ℳ 4.30. II. Teil. Analytische Geometrie der Kurven im Raume der Strahlensysteme und der algebraischen Flächen. 4. Aufl. [U. d. Pr. 1923.]

Schilling, F., Über die Nomographie von M. d'Ocagne. Eine Einführung in dieses Gebiet. Mit 28 Abb. 3., unv. Aufl. [47 S.] gr. 8. 1922. Geh. n. ℳ —.90

Schrutka, L., Zahlenrechnen. [X u. 146 S.] 8. 1923. Kart. n. ℳ 3.60

Severi, F., Vorlesungen über algebraische Geometrie, Geometrie auf einer Kurve, Riemannsche Flächen, Abelsche Integrale. Berechtigte deutsche Übersetzung von E. Löffler. Mit einem Einführungswort von A. Brill u. 20 Figuren. [XVI u. 408 S.] gr. 8. 1921. Geh. n. ℳ 6.—, geb. n. ℳ 7.50

Teubners technische Leitfäden. 8. Kart.

1. **R. Fricke,** Analytische Geometrie. 2. Aufl. Mit 96 Fig. [VI u. 135 S.] 1922. n. ℳ 1.80
2. **M. Großmann,** Darstellende Geometrie. Bd. I. 2., durchges. Aufl. Mit 134 Fig. und 100 Übungsaufgaben im Text. [VI u. 81 S.] 1922. n. ℳ 1.30
3. —— Darstellende Geometrie. Bd. II. 2., umg. Aufl. Mit 144 Fig. im Text. [VI u. 154 S.] n. ℳ 2.—
4. **L. Bieberbach,** Differentialrechnung. 2., verm. u. verb. Aufl. Mit 34 Fig. im Text. [VI u. 131 S.] 1922. n. ℳ 2.20
5. —— Integralrechnung. 2., verb. Aufl. Mit 25 Fig. [IV u. 152 S.] [Erscheint Aug. 1923.]
14. —— Funktionentheorie. Mit 34 Fig. [IV u. 118 S.] 8. 1922. n. ℳ 1.60
18. **V. Happach,** Ausgleichsrechnung nach der Methode der kleinsten Quadrate in ihrer Anwendung auf Physik, Maschinenbau, Elektrotechnik und Geodäsie. Mit 7 Fig. [IV u. 74 S.] 8. 1923. n. ℳ 1.50

Urban, F. M., Grundlagen der Wahrscheinlichkeitsrechnung und der Theorie der Beobachtungsfehler. [VI u. 274 S.] gr. 8. 1923. Geh. n. ℳ 3.60, geb. n. ℳ 4.30

Voß, A., Über das Wesen d. Mathematik. 3., verb. Aufl. [IV u. 123 S.] 1922. Geh. n. ℳ 2.—

Weber, H., u. J. Wellstein, Enzyklopädie der Elementar-Mathematik. Ein Handbuch für Lehrer u. Studierende. In 3 Bdn. gr. 8. I. Bd.: Arithmetik, Algebra u. Analysis. Neubearb. v. P. Epstein. 4. Aufl. Mit 28 Fig. [XVI u. 568 S.] Geb. n. ℳ 9.20
II. Bd.: Elemente der Geometrie. 3. Aufl. [XII u. 596 S.] 1915. Geb. n. ℳ 9.50
III. Bd.: Angewandte Elementarmathematik. In 2 Teil. [3. Aufl. i. Vorb. 1923.]

Weyl, H., Die Idee der Riemannschen Fläche. 2. verb. Aufl. Mit 28 in den Text gedruckten Fig. [VIII u

Ausführliche Kataloge, die der Ver
Betrages (zuzügl Porto) sendet: Volks
schaften u. Technik. 1908. ℳ —.60. S
Sommer 1915). ℳ —.20. Schweiz fr.
bieten der Mathematik und ihrer An

Verlag von B. G. Te

Anfr

Druck