Die Typen der Multiplikatorenringe elliptischer Funktionenkörper.

G. Herglotz zum 60. Geburtstag gewidmet.

Von MAX DEURING.

Einleitung.

1. In einer Reihe von Arbeiten hat H. HASSE die Theorie der Multiplikation der elliptischen Funktionen auf algebraischem Wege entwickelt[1]). Das Ziel, das er dabei vornehmlich verfolgte, war die Riemannsche Vermutung für die Kongruenzzetafunktionen vom Geschlechte 1, oder was auf das gleiche hinausläuft, die folgende Behauptung über die Lösungsanzahl elliptischer Kongruenzen zu beweisen: *K_0 sei ein elliptischer Funktionenkörper über dem Galoisfeld k_0 von $q = p^f$ Elementen (p Primzahl). Die Anzahl der Primdivisoren ersten Grades von K_0 oder auch, unter $f(x, y) = 0$ eine definierende Gleichung von K_0 verstanden, die Anzahl der in k_0 gelegenen Lösungen dieser Gleichung, vermehrt um die Anzahl der im Nenner von x oder y aufgehenden Primideale ersten Grades, ist gleich der Norm des Multiplikators $\pi - 1$ von K, wo π der Multiplikator $z \to z^q$ ist*[2]). Es scheint der Aufmerksamkeit der Mathematiker, die sich mit diesen Fragen beschäftigen, entgangen zu sein, daß dieser Satz über Kongruenzen vom Geschlechte 1 schon GAUSS, wenigstens in dem Sonderfall der lemniskatischen Funktionen, bekannt gewesen ist. Denn nichts anderes sagt die letzte Eintragung im Gaußschen Tagebuch aus, die folgendermaßen lautet:

Observatio per inductionem facta gravissima theoriam residuorum

---

[1]) H. HASSE, Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F. K. Schmidtschen Kongruenzzetafunktionen in gewissen elliptischen Fällen, Nachr. Ges. d. Wiss. Göttingen, Math.-Phys. Kl. 1933, S. 253—262; 2. Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern, Abh. Math. Semin. Hamburg. Univ. **10**, S. 325—348 (1934); 3. Zur Theorie der abstrakten elliptischen Funktionenkörper, I. Journ. f. d. r. u. ang. Math. **175**, S. 55—62, II., S. 69—88, III. S. 193—208 (1936). Eine einfachere Theorie in M. DEURING, Arithmetische Theorie der Korrespondenzen algebraischer Funktionenkörper, I. Journ. f. d. r. u. ang Math. **177**, S. 161—191 (1937), II. **183**, S. 25—36 (1941).

[2]) Siehe H. HASSE[1]), 3, III. S. 206.

biquadraticorum cum functionibus lemniscaticis elegantissime nectens. Puta si $a+bi$ est numerus primus, $a-1+bi$ per $2+2i$ divisibilis, multitudo omnium solutionum congruentiae

$$1 \equiv xx+yy+xxyy \pmod{a+bi}$$

inclusis

$$x = \infty, \quad y = \pm i; \quad x = \pm i, \quad y = \infty$$

fit

$$= (a-1)^2+bb.$$

1814 Iul. 9.

Für $N(a+bi) < 100$ ist dies von R. DEDEKIND nachgeprüft worden und R. FRICKE hat darauf hingewiesen, daß zwischen

$$x = \text{sinlemn } u \quad \text{und} \quad y = \text{coslemn } u$$

gerade die Gleichung

$$1 = x^2+y^2+x^2y^2$$

besteht[3]). Schließlich hat aber G. HERGLOTZ die Gaußsche Behauptung bewiesen[4]); seine Methode, die Teilung der elliptischen Funktionen durch $\pi-1 = a-1+bi$ zu verwenden, ist im Grunde die gleiche, die H. HASSE in seiner ersten Arbeit über die Riemannsche Vermutung benutzte[5]).

2. In den bisherigen Arbeiten über die Multiplikation der elliptischen Funktionen ist kaum näher untersucht worden, was für Multiplikatorenringe $\mathfrak{R}$ elliptischer Funktionenkörper K möglich sind. Für die Charakteristik 0 ist das natürlich bekannt und ergibt sich in einfachster Weise aus der Auffassung der elliptischen Funktionen als doppeltperiodische Funktionen: $\mathfrak{R}$ ist entweder der Ring Γ der ganzen rationalen Zahlen oder eine Ordnung in einem imaginären quadratischen Zahlkörper und alle diese Ringe kommen tatsächlich als Multiplikatorenringe vor. H. HASSE entdeckte, daß es für Primzahlcharakteristik noch eine dritte Möglichkeit gibt: $\mathfrak{R}$ kann dann auch eine Ordnung in einer definiten Quaternionenalgebra sein. Ich habe dann genauer gezeigt, daß die Verzweigungsstellen dieser Algebra ∞ und p sind[6]). Wir wollen diese Algebra mit

---

[3]) Vgl. GAUSS' Werke X, 1. Abt., S. 571/572.

[4]) G. HERGLOTZ, Zur letzten Eintragung im Gaußschen Tagebuch, Ber. d. Math.-Phys. Kl. d. Sächs. Ak. d. Wiss. Leipzig **73**, S. 271—276 (1921).

[5]) H. HASSE[1]), 1., S. 258/259.

[6]) M. DEURING[1]) II., insbesondere § 5, **6**.

$Q_{\varpi,p}$ bezeichnen. Es war aber bisher nicht bekannt, ob bei gegebener Primzahlcharakteristik p alle drei Fälle, nämlich

1. $\mathfrak{R} = \Gamma$, 2. $\mathfrak{R}$ eine vorgegebene Ordnung in einem vorgegebenen imaginären quadratischen Zahlkörper und 3. $\mathfrak{R}$ eine vorgegebene Ordnung in $Q_{\infty,p}$, möglich sind oder ob noch weitere Einschränkungen gemacht werden müssen. Im folgenden soll nun gezeigt werden, daß erstens im Falle 2. die Primzahl p in dem quadratischen Zahlkörper in zwei verschiedene Primideale zerfallen und der Führer von $\mathfrak{R}$ zu p teilerfremd sein muß und zweitens, daß im Falle 3. $\mathfrak{R}$ eine *Maximal*ordnung von $Q_{\varpi,p}$ sein muß. Aber alle dermaßen gekennzeichneten Typen von $\mathfrak{R}$ kommen wirklich vor.

3. Der Typus eines elliptischen Funktionenkörpers K kann durch die Invariante j gekennzeichnet werden, die für die Charakteristik 0 einfach die absolute Invariante aus der Theorie der Modulfunktionen ist, für $p \neq 2$ aus der Legendreschen Normalform sich ebenso erklären läßt wie für die Charakteristik 0, aber für $p = 2$ auf eine andere Weise eingeführt werden muß[7]).

Es ist bekannt, daß für die Charakteristik 0 die elliptischen Körper K mit komplexem $\mathfrak{R}$ *algebraische Zahlen* j als Invarianten haben. Und zwar gibt es, wenn h die Klassenzahl von $\mathfrak{R}$ ist, genau h verschiedene Invarianten j mit $\mathfrak{R}$ als zugehörigem Multiplikatorenring; diese h Werte von j sind konjugierte ganze algebraische Zahlen.

Für Primzahlcharakteristik p gilt etwas ganz Entsprechendes: $\mathfrak{R}$ sei eine vorgegebene Ordnung in einem vorgegebenen imaginären quadratischen Zahlkörper, in dem p in zwei verschiedene Primideale zerfällt. Es gibt genau so viel verschiedene Invarianten j, zu denen der Multiplikatorring $\mathfrak{R}$ gehört, wie die Klassenzahl h von $\mathfrak{R}$ beträgt; alle diese j sind absolut algebraisch (algebraisch über dem Primkörper). Wenn f der Exponent der Idealklasse von $\mathfrak{R}$ ist, der einem der beiden in p aufgehenden Primideale von $\mathfrak{R}$ angehört, so haben die j den Absolutgrad (Grad über dem Primkörper) f, sie zerfallen also in h/f Gruppen von je f untereinander konjugierten.

Wenn aber $\mathfrak{R}$ eine vorgegebene Maximalordnung in $Q_{\infty,p}$ ist, in der der Primteiler von p Hauptideal ist, so gibt es genau eine Invariante j, zu der dieser Multiplikatorenring gehört, sie ist absolut rational. Ist der Primteiler von p kein Hauptideal, so gibt es zwei konjugierte Invarianten vom Absolutgrad 2 zu diesem Multiplikatorenring. Die Anzahl der j, zu denen eine Maximalordnung von $Q_{\infty,p}$ als Multiplikatorenring gehört, ist gleich der Klassenzahl von $Q_{\infty,p}$.

[7]) M. Deuring, Invarianten und Normalformen elliptischer Funktionenkörper. Math. Zeitschr. **47**, 47–56 (1941).

Die Klassenzahl h ist gleich 1 für $p = 2$ und $p = 3$, weiter ist[8])

$$h = \begin{cases} \dfrac{p-1}{12} & \text{für } p \equiv 1 \bmod 12, \\ \dfrac{p-5}{12}+1 & \text{für } p \equiv 5 \bmod 12, \\ \dfrac{p-7}{12}+1 & \text{für } p \equiv 7 \bmod 12, \\ \dfrac{p-11}{11}+2 & \text{für } p \equiv 11 \bmod 12. \end{cases}$$

Ebenso groß ist mithin die Anzahl der j mit nichtkommutativem $\mathfrak{R}$. Wir werden zeigen, daß $\mathfrak{R}$ genau dann nichtkommutativ ist, wenn es in K keine Divisorenklassen vom Exponenten p gibt (wenn also der Fall $\sigma = 2$ vorliegt[9])). Nach H. Hasse[10]) tritt das genau dann ein, wenn eine gewisse Invariante A, für die er den Ausdruck

$$A = \begin{cases} \Delta^{\frac{p-1}{12}} P(j) & \text{für } p \equiv 1 \bmod 12, \\ g_2 \Delta^{\frac{p-5}{12}} P(j) & \text{für } p \equiv 5 \bmod 12, \\ g_3 \Delta^{\frac{p-7}{12}} P(j) & \text{für } p \equiv 7 \bmod 12, \\ g_2 g_3 \Delta^{\frac{p-11}{12}} P(j) & \text{für } p \equiv 11 \bmod 12 \end{cases}$$

angibt, gleich 0 wird, g_2 und g_3 sind dabei die Koeffizienten einer definierenden Gleichung

$$y^2 = 4x^3 - g_2 x - g_3$$

der Weierstraßschen Normalform von K, Δ ist die Diskriminante

$$\Delta = g_2^3 - 27 g_3^2$$

und $P(j)$ bedeutet ein Polynom der Invariante j, von dem wenigstens feststand, daß sein Grad höchstens gleich dem Exponenten der daneben-

---

[8]) Nach M. Eichler, Über die Idealklassenzahl total definiter Quaternionenalgebren, Math. Zeitschr. **43**, S. 102—109 (1937).

[9]) M. Deuring [1]), II. § 5, **6**.

[10]) H. Hasse, Existenz separabler zyklischer unverzweigter Erweiterungskörper vom Primzahlgrade p über elliptischen Funktionenkörpern der Charakteristik p, Journ. f. r. u. ang. Math. **172**, S. 77—85 (1934), § 1.

stehenden Potenz von Δ ist. Vergleichen wir mit der Klassenzahl, so erkennen wir, daß diese Gradzahl, wie von HASSE vermutet, genau ist, außerdem, daß $P(j)$ keine Doppelwurzeln hat. Die Wurzeln von $P(j)$ sind die Invariantenwerte mit nichtkommutativem Multiplikatorenringen, den einzelnen Typen von Maximalordnungen von $Q_{\infty,p}$ zugeordnet, wozu im Falle $p \equiv 5 \bmod 12$ $j = 0$, im Falle $p \equiv 7 \bmod 12$ $j = 2^6 3^3$ und im Falle $p \equiv 11 \bmod 12$ $j = 0$ und $j = 2^6 3^3$ kommen. Für $p = 2$ und 3 ist $j = 0$ die Invariante mit nichtkommutativem Multiplikatorenring.

Die Invariante A kann übrigens mit der von HASSE und WITT[11]) gegebenen Definition ohne weiteres explizit ausgerechnet werden; wir erhalten, je nachdem wir die Weierstraßsche oder die Legendresche Normalform zugrunde legen, die folgenden beiden Ausdrücke für A:

a)

$$A = \begin{cases} (-1)^{\frac{p-1}{4}} 3^{-\frac{p-1}{4}} \Delta^{\frac{p-1}{12}} \left(\frac{p-1}{2}\right)! \Phi_p(j) \text{ für } p \equiv 1 \bmod 12, \\ 2^2 (-1)^{\frac{p-1}{4}} 3^{-\frac{p-5}{4}} \Delta^{\frac{p-5}{12}} g_2 \left(\frac{p-1}{2}\right)! \Phi_p(j) \text{ für } p \equiv 5 \bmod 12, \\ 2^4 (-1)^{\frac{p-3}{4}} 3^{-\frac{p-7}{4}} \Delta^{\frac{p-7}{12}} g_3 \left(\frac{p-1}{2}\right)! \Phi_p(j) \text{ für } p \equiv 7 \bmod 12, \\ 2^6 (-1)^{\frac{p-3}{4}} 3^{-\frac{p-11}{4}} \Delta^{\frac{p-11}{12}} g_2 g_3 \left(\frac{p-1}{2}\right)! \Phi_p(j) \text{ für } p \equiv 11 \bmod 12, \end{cases}$$

wo

$$\Phi_p(j) = j^{\left[\frac{p}{12}\right]} \sum_{0 \le i < \frac{p}{12}} \frac{\left(-\frac{4}{27}\right)^i (1 - 2^6 \cdot 3^3 \cdot j^{-1})^i}{(2i)! \left(\frac{p-1}{4} - 3i\right)! \left(\frac{p-1}{4} + i\right)!}$$

für $p \equiv 1 \bmod 4$

und

$$\Phi_p(j) = j^{\left[\frac{p}{12}\right]} \sum_{0 \le i < \frac{p}{12}} \frac{\left(-\frac{4}{27}\right)^i (1 - 2^6 \cdot 3^3 \cdot j^{-1})^i}{(2i+1)! \left(\frac{p-7}{4} - 3i\right)! \left(\frac{p+1}{4} + i\right)!}$$

für $p \equiv -1 \bmod 4$;

b) $$A = (-1)^{\frac{p-1}{2}} \sum_{i=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{i}^2 \lambda^i \quad \text{für } p \geqq 3;$$

[11]) H. HASSE und E. WITT, Zyklische unverzweigte Erweiterungskörper vom Primzahlgrade p über einem algebraischen Funktionenkörper der Charakteristik p, Mh. Math. Phys. **43**, S. 477—492 (1936).

dabei ist λ eine der sechs Wurzeln von

$$j = 2^8 \cdot \frac{(1 - \lambda(1-\lambda))^3}{\lambda^2 (1-\lambda)^2}.$$

Die Form a) eignet sich auch zur numerischen Berechnung der „supersingulären" Invarianten (mit nichtkommutativem $\mathfrak{R}$) für kleine Werte von p.

4. Es ist leicht einzusehen, daß für Primzahlcharakteristik jeder elliptische Körper mit absolut algebraischer Invariante komplexe Multiplikatoren hat. Die p^f Elemente des Galoisfeldes G_{p^f} verteilen sich daher als Invarianten auf elliptische Körper mit komplexen $\mathfrak{R}$, und wenn wir untersuchen, welchen Bedingungen diese $\mathfrak{R}$ genügen müssen, so ergibt sich die folgende *Klassenzahlrelation:*

$d_{n,p}$ bezeichne diejenigen nicht durch p teilbaren Diskriminanten definiter binärer quadratischer Formen, deren zugehörige Hauptform die natürliche Zahl n eigentlich darstellt, und $h(d_{n,p})$ die Klassenzahl von $d_{n,p}$.

Dann gilt

$$\sum h(d_{p^f,p}) + t_{p^f} = p^f,$$

wobei t_{p^f} für gerades f die unter **3** angegebene Klassenzahl von $Q_{\infty,p}$ und für ungerades f das arithmetische Mittel von Klassen- und Typenzahl von $Q_{\infty,p}$ ist.

5. Um die obigen Ergebnisse herleiten zu können, müssen wir von elliptischen Körpern der Charakteristik 0 zu solchen von Primzahlcharakteristik übergehen können und umgekehrt. Darüber gelten die folgenden beiden allgemeinen Sätze:

1. *Im Konstantenkörper k des elliptischen Funktionenkörpers K sei durch eine Exponentenbewertung ein Primdivisor $\mathfrak{p}$ gegeben. Dann und nur dann, wenn die Invariante j von K $\mathfrak{p}$-ganz ist, gibt es eine definierende Gleichung $f(x, y) = 0$ von K, die auch modulo $\mathfrak{p}$ irreduzibel und vom Geschlechte 1 ist. Den Divisoren, Divisorenklassen und Multiplikatoren von K können dann bestimmte Divisoren, Divisorenklassen und Multiplikatoren des Restklassenkörpers $\bar{K}$ von K modulo $\mathfrak{p}$ als „Reste" so zugeordnet werden, daß die Relationen zwischen Elementen, Divisoren, Klassen und Multiplikatoren bei der Restklassenbildung erhalten bleiben.*

2. *Wenn der Körper $\bar{K}_0$ der Primzahlcharakteristik p einen Multiplikator $\bar{\mu}$ hat, so läßt er sich durch Reduktion modulo einem Primteiler* $\mathfrak{p}$ *von p aus einem Körper K_0 der Charakteristik 0 gewinnen, von dessen Multiplikatoren einer modulo* $\mathfrak{p}$ *in den vorgegebenen Multiplikator $\bar{\mu}$ übergeht.*

Der zweite Satz enthält die Methode von HERGLOTZ und HASSE als Sonderfall.

Aus dem ersten Satz ergibt sich, wie sich ein elliptischer Körper K der Charakteristik 0 mit komplexem $\mathfrak{R}$ bei der Reduktion nach einem im p aufgehenden Primideal $\mathfrak{p}$ verhält — wir können den Konstantenkörper von K als endlichen algebraischen Zahlkörper annehmen. $\mathfrak{R}$ wird bei dieser Reduktion auf einen Teil des Multiplikatorenringes $\bar{\mathfrak{R}}$ des Restklassenkörpers $\bar{K}$ von K mod $\mathfrak{p}$ abgebildet. $\bar{\mathfrak{R}}$ ist aber im allgemeinen größer als $\mathfrak{R}$. Wenn p im Quotientenkörper Σ von $\mathfrak{R}$ in zwei verschiedene Primideale zerfällt, so ist $\bar{\mathfrak{R}}$ diejenige Ordnung von Σ, deren Führer der von p freie Bestandteil des Führers von $\mathfrak{R}$ ist. Wenn p in Σ prim bleibt oder verzweigt ist, so ist $\bar{\mathfrak{R}}$ eine Maximalordnung in $Q_{\infty,p}$.

Aus diesen Beziehungen kann die Klassenkörpertheorie von Σ hergeleitet werden, worauf in einer späteren Arbeit genauer eingegangen werden soll.

Da die Invariante $\bar{j}$ von $\bar{K}$ die $\mathfrak{p}$-Restklasse der Invariante j von K ist, so folgt für jedes in Σ nicht voll zerlegte p, daß j modulo $\mathfrak{p}$ eine der h supersingulären Invarianten modulo p ist.

Hieraus ergeben sich neue bemerkenswerte Tatsachen über die Zerlegung von Primzahlen in gewissen algebraischen Zahlkörpern, die in einer späteren Arbeit untersucht werden sollen. Nur den einfachsten Fall wollen wir erwähnen: Da die supersinguläre Invariante modulo 2 gleich 0 ist, so sind die Klasseninvarianten jeder Ordnung eines imaginären quadratischen Zahlkörpers ungerade oder gerade (d. h. zu 2 teilerfremd oder nicht), je nachdem 2 in Σ voll zerlegt wird oder nicht. Dieser Satz ist nämlich die Folgerung, die aus einem Satze von H. WEBER über die Funktion

$$f(\omega) = e^{-\frac{\pi i}{24}} \frac{\eta\left(\frac{\omega+1}{2}\right)}{\eta(\omega)}, \qquad \eta(\omega) = e^{\frac{\pi i}{12}} \prod_{\nu=1}^{\infty} (1 - e^{2\pi i \nu})$$

für

$$j(\omega) = \frac{(f(\omega)^{24} - 16)^3}{f(\omega)^{24}}$$

zu ziehen ist. Jener Satz, den H. WEBER mittels der Kroneckerschen Grenzformel bewies, lautet: *Wenn ω einen imaginären quadratischen Zahlkörper erzeugt, in dem 2 voll zerfällt, so ist $f(\omega)2^{\frac{1}{2}}$ eine Einheit*[12]).

§ 1. Die Teilkörper eines elliptischen Funktionenkörpers.

1. K sei ein elliptischer Funktionenkörper mit dem algebraisch-abgeschlossenen Konstantenkörper k. Wir erhalten eine umkehrbar eindeutige Zuordnung der Klassen nullten Grades C zu den Primdivisoren von K, wenn wir, einen beliebigen Primdivisor $\mathfrak{o}$ von K als Normierungsprimdivisor zugrunde legend, der Klasse C den nach dem Riemann-Rochschen Satz eindeutig bestimmten Primdivisor $\mathfrak{p}$ der Klasse $\mathfrak{o}C$ zuordnen, oder umgekehrt, dem Primdivisor $\mathfrak{o}$ die Klasse von $\mathfrak{p}/\mathfrak{o}$. Wir wollen die Klasse von $\mathfrak{p}/\mathfrak{o}$ kurz mit $[\mathfrak{p}]$ bezeichnen und die Gruppe der Klassen nullten Grades additiv schreiben;

$$[\mathfrak{p}_1] + [\mathfrak{p}_2] = [\mathfrak{p}_3]$$

bedeutet also einfach

$$\frac{\mathfrak{p}}{\mathfrak{o}} \cdot \frac{\mathfrak{p}_2}{\mathfrak{o}} \sim \frac{\mathfrak{p}_3}{\mathfrak{o}}$$

Wir führen nun nach H. HASSE[13]) die Spiegelungs- und Translationsautomorphismen von K/k ein. $\mathfrak{q}_1$ und $\mathfrak{q}_2$ seien zwei (gleiche oder verschiedene) Primdivisoren von K. Nach dem Riemann-Rochschen Satz gibt es ein Element z mit dem genauen Nenner $\mathfrak{q}_1\mathfrak{q}_2$. K ist quadratisch und separabel über $k(z)$ (auch dann, wenn die Charakteristik von K 2 ist, weil die einzige inseparable quadratische Erweiterung $k(z^{\frac{1}{2}})$ von $k(z)$ das Geschlecht 0 hat) und hat daher einen von der Identität verschiedenen Automorphismus $\sigma_{\mathfrak{q}_1,\mathfrak{q}_2}$, der z fest läßt und $\mathfrak{q}_1$ mit $\mathfrak{q}_2$ vertauscht.

$\sigma_{\mathfrak{q}_1,\mathfrak{q}_2}$ heißt ein *Spiegelungsautomorphismus von K*. Vertauscht $\sigma_{\mathfrak{q}_1,\mathfrak{q}_2}$ die beiden Primdivisoren $\mathfrak{p}_1$ und $\mathfrak{p}_2$, so ist $\sigma_{\mathfrak{p}_1,\mathfrak{p}_2} = \sigma_{\mathfrak{q}_1,\mathfrak{q}_2}$, denn es gibt ein Element $\alpha z + \beta$ mit konstanten α, β, dessen Nenner $\mathfrak{q}_1\mathfrak{q}_2$ und dessen Zähler $\mathfrak{p}_1\mathfrak{p}_2$ ist, der Invariantenkörper von $\sigma_{\mathfrak{p}_1,\mathfrak{p}_2}$ fällt also mit dem von $\sigma_{\mathfrak{q}_1,\mathfrak{q}_2}$ zusammen. Es genügt daher die Spiegelungen $\sigma_{\mathfrak{o},\mathfrak{q}}$ zu betrachten.

Da, unter $\mathfrak{p}$ irgendeinen Primdivisor verstanden, $\frac{\mathfrak{p}}{\mathfrak{o}} \cdot \frac{\mathfrak{p}^{\sigma_{\mathfrak{o},\mathfrak{q}}}}{\mathfrak{o}}$ als

---

[12]) H. WEBER, Lehrbuch der Algebra, III, § 142, Die Normen der C-Klasseninvarianten.

[13]) H. HASSE, Zur Theorie der abstrakten elliptischen Funktionenkörper, II. Journ. f. d. r. u. ang. Math., **175**, S. 69–88 (1936), § 1.

Divisor von $k(z)$ äquivalent zu 1 ist, so gilt

$$[\mathfrak{p}^{\sigma_{\mathfrak{o},\mathfrak{q}}}] = [\mathfrak{q}] - [\mathfrak{p}], \qquad \text{insbesondere} \quad [\mathfrak{p}^{\sigma_{\mathfrak{o},\mathfrak{o}}}] = -[\mathfrak{p}],$$

woraus sich der Name Spiegelung erklärt.

Für den Automorphismus

$$\tau_{\mathfrak{o},\mathfrak{q}} = \sigma_{\mathfrak{o},\mathfrak{o}}\,\sigma_{\mathfrak{o},\mathfrak{q}}$$

von K/k gilt

$$(1) \qquad [\mathfrak{p}^{\tau_{\mathfrak{o},\mathfrak{q}}}] = [\mathfrak{p}^{\sigma_{\mathfrak{o},\mathfrak{o}}\sigma_{\mathfrak{o},\mathfrak{q}}}] = [\mathfrak{q}] - [\mathfrak{p}^{\sigma_{\mathfrak{o},\mathfrak{o}}}] = [\mathfrak{p}] + [\mathfrak{q}].$$

$\tau_{\mathfrak{o},\mathfrak{q}}$ heißt eine *Translation von* K.

2. Wir schließen jetzt an die Theorie der Multiplikatoren von K an, wie sie in den beiden unter [1]) angegebenen Arbeiten von M. Deuring entwickelt worden ist. Ein Multiplikator μ von K kann einerseits als eine homomorphe Abbildung $[\mathfrak{p}] \to \mu[\mathfrak{p}]$ der Gruppe der Klassen nullten Grades in sich aufgefaßt werden, andererseits als ein *normierter Meromorphismus* $z \to z^{\mu}$ *von* K. Zur Normierung der Meromorphismen benutzen wir den gleichen Primdivisor $\mathfrak{o}$ wie in **1.** zur Erklärung von $[\mathfrak{p}]$. Dann gilt zur Bildung von $\mu[\mathfrak{p}]$ die folgende *Regel*

$$(2) \qquad \mu[\mathfrak{p}] = [(N_{K/K^{\mu}}\mathfrak{p})^{\mu^{-1}}].$$

Denn μ wird dadurch auf die Klasse von $\mathfrak{p}/\mathfrak{o}$ angewandt, daß erst die Norm von $\mathfrak{p}/\mathfrak{o}$ in Beziehung auf K^{μ} genommen und diese dann durch μ^{-1} in K abgebildet wird.

Aus (2) folgt:

Die Primdivisoren $\mathfrak{p}$, *für welche*

$$\mu[\mathfrak{p}] = \mathfrak{q}$$

gilt, sind die Primteiler von $\mathfrak{q}^{\mu}$.

Die $[\mathfrak{p}]$ mit $\mu[\mathfrak{p}] = 0$ bilden eine Klassengruppe der Ordnung $N\mu/I_{\mu}$, weil ja die Anzahl der verschiedenen Primfaktoren in K eines Primdivisors von K^{μ} gleich dem Grade $N\mu$ dividiert durch den Inseparabilitätsgrad I_{μ} von K/K^{μ} ist [6]).

Eine Nebengruppe der Gruppe $\mu[\mathfrak{p}] = 0$ in der vollen Klassengruppe besteht aus allen $\mathfrak{p}$ mit $\mu[\mathfrak{p}] = \mathfrak{q}$ für ein festes $\mathfrak{q}$. Wenn $\mu[\mathfrak{p}] = 0$ ist, so bleibt jeder Primdivisor $\mathfrak{q}^{\mu}$ von K^{μ} bei der Translation $\tau_{\mathfrak{o},\mathfrak{p}}$ fest, denn $\mathfrak{q}^{\mu}$ ist die I_{μ}-te Potenz des Produktes der verschiedenen Lösungen $\mathfrak{x}$ von $\mu[\mathfrak{x}] = [\mathfrak{q}]$, die von $\tau_{\mathfrak{o},\mathfrak{p}}$ nur untereinander vertauscht werden. Daraus schließen wir, daß jedes Element von K^{μ} bei $\tau_{\mathfrak{o},\mathfrak{p}}$ fest

bleibt, denn es gilt der folgende Hilfssatz von H. HASSE[13]):

Ein Automorphismus τ eines Funktionenkörpers K, der alle Konstanten und alle Primdivisoren fest läßt, ist die Identität.

Beweis: τ kann jedes y aus K nur um einen konstanten Faktor ε_y ändern: $y^\tau = \varepsilon_y y$. Für konstante y ist $\varepsilon_y = 1$. Für nichtkonstantes y haben wir

$$(y+1)^\tau = \varepsilon_{y+1}(y+1) = y^\tau + 1 = \varepsilon_y y + 1,$$
$$(\varepsilon_{y+1} - \varepsilon_y) y = 1 - \varepsilon_{y+1}.$$

Da die rechte Seite der letzten Gleichung konstant ist, so muß $\varepsilon_{y+1} = 1$, d. h. $y^\tau = y$ sein, wie behauptet.

Da die Anzahl der Translationen $\tau_{\mathfrak{o},\mathfrak{p}}$ mit $\mu[\mathfrak{p}] = 0$ gleich dem Separabilitätsgrad von K/K^μ ist, so haben wir den Satz:

K ist über K^μ abelsch und die Galoisgruppe von K/K^μ besteht aus den Translationen $\tau_{\mathfrak{o},\mathfrak{p}}$ mit $\mu[\mathfrak{p}] = 0$.

Insbesondere besteht für einen natürlichen Multiplikator n die Galoisgruppe von K/K^n aus allen Translationen, deren Ordnung in n aufgeht. Sie ist daher eine abelsche Gruppe vom Typus (n, n), wenn die Charakteristik p nicht in n aufgeht und vom Typus $(n/p^f, n/p^f, p^{2f-2\sigma})$, wenn p^f die in n enthaltene Potenz von p ist; σ ist, nur vom Körper K abhängig, gleich 1 oder 2[6]).

3. Es sei jetzt K_0 ein beliebiger elliptischer Teilkörper von K mit dem gleichen Konstantenkörper k. K ist über K_0 unverzweigt. *Wir zeigen, daß die Galoisgruppe von K/K_0 eine endliche Translationsgruppe ist, so daß K_0 durch die Angabe dieser Translationsgruppe und des Inseparabilitätsgrades von K/K_0 innerhalb K gekennzeichnet ist.*

Wir können offenbar gleich annehmen, daß K über K_0 separabel ist. K' sei der von K über K_0 erzeugte Normalkörper. K' ist unverzweigt über K und daher elliptisch. ϱ sei ein Automorphismus von K'/K_0. Zeigen wir, daß ϱ eine Translation von K' ist, so ist der Beweis erbracht, weil sich dadurch K' als abelsch über K_0 erweist und daher mit K zusammenfällt. $\mathfrak{o}'$ sei ein Primdivisor von K', $\mathfrak{o}'^\varrho = \mathfrak{o}^*$. $\varepsilon = \varrho\tau_{\mathfrak{o}',\mathfrak{o}^*}^{-1}$ ist ein Automorphismus von K'/k, der $\mathfrak{o}'$ fest läßt, also ein für $\mathfrak{o}'$ normierter Meromorphismus von K', der eine Einheit des Multiplikatorenringes von K' darstellt. Für einen Primdivisor $\mathfrak{q}$ von K' gilt

$$\varepsilon^{-1}[\mathfrak{q}'] = [(N_{K'/K'^{\varepsilon^{-1}}}\mathfrak{q}')^\varepsilon] = [\mathfrak{q}'^\varepsilon].$$

Gesetzt, es wäre $\varepsilon \neq 1$. Dann gäbe es eine Klasse $[\mathfrak{q}']$ mit

$$(1-\varepsilon^{-1})[\mathfrak{q}'] = [\mathfrak{o}^*], \qquad [\mathfrak{q}'] - [\mathfrak{q}'^{\varepsilon}] = [\mathfrak{o}^*],$$
$$[\mathfrak{q}'] = [\mathfrak{q}'^{\varepsilon}] + [\mathfrak{o}^*] = [\mathfrak{q}'^{\varepsilon\tau_{\mathfrak{o},\mathfrak{o}^*}}] = [\mathfrak{q}'^{\varrho}].$$

ϱ wäre also eine Trägheitssubstitution von $\mathfrak{q}'$ über K_0, was der Unverzweigtheit von K'/K_0 widerspräche.

4. Wir wollen die Multiplikatoren eines elliptischen Teilkörpers K_0 von K mit denen von K selbst in Beziehung setzen. Die Multiplikatoren von K_0 sollen als Meromorphismen für die Norm $\mathfrak{o}_0$ von $\mathfrak{o}$ in K_0 normiert sein. $\mathfrak{o}$ geht in $\mathfrak{o}_0$ auf.

μ sei ein Multiplikator von K. *Für die Klassenbildung in K^μ gilt die Regel:*

3) $$[\mathfrak{p}^\mu] = [\mathfrak{p}]^\mu.$$

Denn $[\mathfrak{p}]^\mu$ ist die Klasse von $\mathfrak{p}^\mu/\mathfrak{o}^\mu$, $[\mathfrak{p}^\mu]$ aber zufolge der eben festgesetzten Normierung in $K_0 = K^\mu$ auch.

Hieraus leiten wir die folgende Darstellung der Translationen von K^μ durch die von K ab

$$\tau_{\mathfrak{o}^\mu,\mathfrak{q}^\mu} = \mu^{-1}\tau_{\mathfrak{o},\mathfrak{q}^\mu}.$$

Es gilt nämlich

$$[\mathfrak{p}^{\mu\mu^{-1}\tau_{\mathfrak{o},\mathfrak{q}^\mu}}] = [\mathfrak{p}^{\tau_{\mathfrak{o},\mathfrak{q}^\mu}}] = [\mathfrak{p}^{\tau_{\mathfrak{o},\mathfrak{q}}}]^\mu = [\mathfrak{p}]^\mu + [\mathfrak{q}]^\mu$$
$$= [\mathfrak{p}^\mu] + [\mathfrak{q}^\mu] = [\mathfrak{p}^{\mu\tau_{\mathfrak{o}^\mu,\mathfrak{q}^\mu}}],$$

der Automorphismus $\tau^{-1}_{\mathfrak{o}^\mu,\mathfrak{q}^\mu}\,\mu^{-1}\tau_{\mathfrak{o},\mathfrak{o}^\mu}$ von K^μ/k läßt daher alle Primdivisoren von K^μ fest und muß die Identität sein.

K_0 sei irgendein elliptischer Teilkörper von K. Wir wollen untersuchen, unter welcher Bedingung das von einem Meromorphismus μ von K entworfene Bild K_0^μ von K_0 in K_0 enthalten ist und also einen Meromorphismus von K_0 liefert, der dann für $\mathfrak{o}_0$ normiert ist. Zu diesem Zwecke berechnen wir die Galoisgruppe von K/K_0^μ aus der von K/K_0. Wir zeigen

$\tau_{\mathfrak{o},\mathfrak{x}}$ ist genau dann ein Automorphismus von K/K_0^μ, wenn, $\mu[\mathfrak{x}] = \mathfrak{q}$ gesetzt, $\tau_{\mathfrak{o},\mathfrak{q}}$ ein Automorphismus von K/K_0 ist.

Beweis: Die Automorphismen von K/K_0 seien $\tau_{\mathfrak{o},\mathfrak{q}}, \cdots, \tau_{\mathfrak{o},\mathfrak{q}_{n_0}}$, $\mathfrak{p}_0$ bedeute irgendeinen Primdivisor von K_0 und $\mathfrak{x}$ irgendeinen Primdivisor

von K. Wir berechnen $\mathfrak{p}_0^{\tau_{0,\xi}}$. Den Übergang von einer Klasse $[\mathfrak{p}]$ zu dem Primdivisor $\mathfrak{p}$ wollen wir dadurch andeuten, daß wir die Klasse in runde Klammern setzen: $([\mathfrak{p}]) = \mathfrak{p}$. $\mathfrak{p}_0$ ist die Norm eines Primdivisors $\mathfrak{p}$ von K nach K_0, also

$$\mathfrak{p}_0 = \prod_{i=1}^{n_0} ([\mathfrak{p}] + [q_i])^{I(K:K_0)}.$$

Wir haben daher

$$\mathfrak{p}_0^{\mu} = \prod_{i=1}^{n_0} ([\mathfrak{p}]^{\mu} + [q_i]^{\mu})^{I(K:K_0)} = \prod_{i=1}^{n_0} ([\mathfrak{p}^{\mu}] + [q_i^{\mu}])^{I(K:K_0)}.$$

$([\mathfrak{p}^{\mu}] + [q_i^{\mu}])$ sei die Norm des Primdivisors $\mathfrak{y}_i$ von K nach K^{μ}, also

$$[\mathfrak{p}^{\mu}] + [q^{\mu}] = \Big[\prod_{\mu[\mathfrak{r}]=0} ([\mathfrak{y}_i] + [\mathfrak{r}])^{I_{\mu}}\Big].$$

Nach (2) gilt

$$\mu[\mathfrak{y}_i] = [\mathfrak{p}] + [q_i].$$

Jetzt können wir $([\mathfrak{p}^{\mu}] + [q_i^{\mu}])^{\tau_{0,\xi}}$ ausrechnen

$$\begin{aligned}([\mathfrak{p}^{\mu}] + [q_i^{\mu}])^{\tau_{0,\xi}} &= \prod_{\mu[\mathfrak{r}]=0} ([\mathfrak{y}_i] + [\mathfrak{x}] + [\mathfrak{r}])^{I_{\mu}} \\ &= N_{K/K^{\mu}}([\mathfrak{y}_i] + [\mathfrak{x}]) \\ &= (\mu[\mathfrak{y}_i] + \mu[\mathfrak{x}])^{\mu} \\ &= ([\mathfrak{p}] + [q_i] + \mu[\mathfrak{x}])^{\mu}.\end{aligned}$$

Und daraus folgt

$$\mathfrak{p}_0^{\mu\tau_{0,\xi}} = \prod_{i=1}^{n_0} ([\mathfrak{p}] + [q_i] + \mu[\mathfrak{x}])^{\mu I(K:K_0)}.$$

Damit $\mathfrak{p}_0^{\mu\tau_{0,\xi}} = \mathfrak{p}_0^{\mu}$ wird, müssen offenbar die n_0 Klassen $[q_i] + \mu\mathfrak{x}$ bis auf die Reihenfolge mit den Klassen $[q_i]$ übereinstimmen, und das ist genau dann der Fall, wenn $\mu[\mathfrak{x}]$ zu der Gruppe der $[q_i]$ gehört, wie behauptet.

Um K_0^{μ} völlig festzulegen, müssen wir noch den Inseparabilitätsgrad von K/K_0^{μ} angeben. Der ist aber das Produkt der Inseparabilitätsgrade von K über K^{μ} und über K_0.

Aus dem bewiesenen Satz folgt ohne weiteres, daß, wenn $n = n_0 \cdot I(K:K_0)$ der Grad von K über K_0 ist, $K^{n\varepsilon}$ in K_0 enthalten ist.

Ferner haben wir die folgende Antwort auf die oben gestellte Frage, welche Multiplikatoren von K auch Multiplikatoren von K_0 seien:

μ ist genau dann ein Multiplikator von K_0, wenn die Gruppe der Klassen $[\mathfrak{q}_i]$, welche den Automorphismen $\tau_{0,\mathfrak{q}_1}, \cdots, \tau_{0,\mathfrak{q}_{n_0}}$ von K/K_0 entsprechen, durch μ in sich abgebildet wird:

$$\mu\,[\mathfrak{q}_i] = [\mathfrak{q}_j].$$

Insbesondere ist das n_0-fache jedes Multiplikators von K auch Multiplikator von K_0.

5. Wir zeigen jetzt, wie ein Multiplikator μ von K, der zugleich Multiplikator von K_0 ist, als Homomorphismus der Klassengruppe von K_0 aus seiner Wirkung auf die Klassen von K abgeleitet werden kann. *Es gilt einfach:*

$$\mu\,[N_{K/K_0}\mathfrak{p}] = [N_{K/K_0}(\mu\,[\mathfrak{p}])]. \tag{4}$$

Beweis:

$$\begin{aligned}\mu\,[N_{K/K_0}\mathfrak{p}] &= [(N_{K_0/K_0^{\mu}}(N_{K/K_0}\mathfrak{p}))^{\mu^{-1}}] = [(N_{K/K_0^{\mu}}\mathfrak{p})^{\mu^{-1}}]\\ &= [(N_{K^{\mu}/K_0^{\mu}}(N_{K/K^{\mu}}\mathfrak{p}))^{\mu^{-1}}] = [N_{K/K_0^{\mu}}((N_{K/K^{\mu}}\mathfrak{p})^{\mu^{-1}})]\\ &= [N_{K/K_0}(\mu\,[\mathfrak{p}])].\end{aligned}$$

6. *Durch $[\mathfrak{p}] \to [N_{K/K_0}\mathfrak{p}]$ wird die Klassengruppe von K homomorph auf die von K_0 abgebildet; dabei gehen gerade die Klassen $[\mathfrak{p}]$ in 0 über, für die $\tau_{0,\mathfrak{p}}$ zur Galoisgruppe von K/K_0 gehört.*

7. Aus dem vorstehenden folgt, daß die Multiplikatorenringe $\mathbf{R}$ und $\mathbf{R}_0$ von K und K_0 einen nichtleeren Durchschnitt haben. Es ist aber nicht von vornherein klar, daß für die Elemente dieses Durchschnittes die Rechenoperationen in $\mathbf{R}_0$ mit denen in $\mathbf{R}$ übereinstimmen. Für die Multiplikation allerdings folgt es sofort aus der Definition des Meromorphismenproduktes. Für die Addition beweisen wir es so:

μ_1, μ_2, μ_3 seien drei Elemente des Durchschnittes von $\mathbf{R}$ und $\mathbf{R}_0$, deren in $\mathbf{R}$ genommene Summe 0 ist. Wir müssen zeigen, daß auch ihre Summe in $\mathbf{R}_0$ gleich 0 ist. Zu μ_i gehört ein Primdivisor ersten Grades $\mathfrak{P}_{\mu_i}$ des Doppelkörpers KK^{φ}/K [14]), und $\mu_1+\mu_2+\mu_3 = 0$ bedeutet $\mathfrak{P}_{\mu_1}\cdot\mathfrak{P}_{\mu_2}\cdot\mathfrak{P}_{\mu_3} \sim (\mathfrak{o}^{\varphi})^3$ in KK^{φ}. In KK^{φ} ist der zu K_0 gehörige Doppel-

[14]) M. Deuring, Arithmetische Theorie der Korrespondenzen algebraischer Funktionenkörper, II. § 5, **2**. Journ. f. d. r. u. ang. Math. **183**, S. 25–36 (1941).

körper $K_0 K_0^{\varphi}$ enthalten, und zu μ_i als Meromorphismus von K_0 gehört offenbar der Primdivisor von $K_0 K_0^{\varphi}/K_0$, in dem $\mathfrak{P}_{\mu_i}$ aufgeht, also die Norm $\mathfrak{P}_{\mu_i}^{(0)}$ von $\mathfrak{P}_{\mu}$ nach $K_0 K_0^{\varphi}$. Die Norm von $\mathfrak{o}^{\varphi}$ ist $\mathfrak{o}_0^{\varphi}$. Aus der Äquivalenz $\mathfrak{P}_{\mu_1} \cdot \mathfrak{P}_{\mu_2} \cdot \mathfrak{P}_{\mu_3} \sim (\mathfrak{o}^{\varphi})^3$ folgt also durch Normbildung die Äquivalenz

$$\mathfrak{P}_{\mu_1}^{(0)} \cdot \mathfrak{P}_{\mu_2}^{(0)} \cdot \mathfrak{P}_{\mu_3}^{(0)} \sim (\mathfrak{o}_0^{\varphi})^3,$$

die aussagt, daß die Summe der μ_i als Meromorphismen von K_0 ebenfalls 0 ist.

§ 2. Die Multiplikatorenringe der Teilkörper.

1. Wieder sei wie in § 1 K ein elliptischer Körper mit algebraisch abgeschlossenem Konstantenkörper k. Die Charakteristik von K sei p ($= 0$ oder $\neq 0$). Der Quotientenkörper Σ des Multiplikatorenringes $\mathfrak{R}$ von K ist entweder der Körper P der rationalen Zahlen, ein imaginärquadratischer Zahlkörper oder die bei 1 und p verzweigte (definite) Quaternionenalgebra $Q_{\infty,p}$ (was nur für $p \neq 0$ möglich ist). $\mathfrak{R}$ ist eine Ordnung in Σ.

Ähnlich wie den Elementen μ von $\mathfrak{R}$ die Teilkörper K^{μ} lassen sich auch den Linksidealen $\mathfrak{a}$ von $\mathfrak{R}$ elliptische Teilkörper von K zuordnen.

$\mathfrak{a}$ sei ein Linksideal von $\mathfrak{R}$. Das Kompositum aller Körper K^{α}, $\alpha \equiv 0 \bmod \mathfrak{a}$, ist ein elliptischer Teilkörper von K, den wir mit $K^{\mathfrak{a}}$ bezeichnen. Wenn $\mathfrak{a} = \mathfrak{R}\alpha$ Hauptideal ist, so ist offenbar $K^{\mathfrak{a}} = K^{\alpha}$. (Aus dem Additionstheorem schließen wir leicht, daß, wenn

$$\mathfrak{a} = (\mathfrak{R}\alpha_1, \cdots, \mathfrak{R}\alpha_t)$$

gilt, $K^{\mathfrak{a}}$ das Kompositum der endlich vielen Körper K^{α_i} ist.)

Die Galoisgruppe von K über $K^{\mathfrak{a}}$ ist als der Durchschnitt der Galoisgruppen von K über allen K^{α}, $\alpha \equiv 0$ mod $\mathfrak{a}$, die Gruppe aller Translationen $\tau_{\mathfrak{o},\mathfrak{p}}$, $\mathfrak{a}[\mathfrak{p}] = 0$.

Wenn $\mathfrak{a}_1 \equiv 0 \bmod \mathfrak{a}$ ist, so gilt $K^{\mathfrak{a}_1} \subseteq K^{\mathfrak{a}}$.

2. Der Multiplikatorenring von $K^{\mathfrak{a}}$ hat, wie wir in § 1 **5.** zeigten, den gleichen Quotientenkörper Σ wie $\mathfrak{R}$. Darüber hinaus gilt aber:

Der Multiplikatorenring $\mathfrak{R}_0$ von $K^{\mathfrak{a}} = K_0$ ist die Rechtsordnung von $\mathfrak{a}$ in Σ.

Beweis. Vorläufig beweisen wir nur, daß $\mathfrak{R}_0$ die Rechtsordnung von $\mathfrak{a}$ umfaßt, daß $\mathfrak{R}_0$ auch nicht größer ist, beweisen wir später (**9.**).

Wir erklären, wie ein Element μ_0 der Rechtsordnung von $\mathfrak{a}$ auf die Elemente von K_0 anzuwenden ist. Ein Element z von K_0 ist eine rationale Funktion $z = R(z_1^{\alpha_1}, \cdots, z_t^{\alpha_t})$ einiger Elemente $z_i^{\alpha_i}$ aus Körpern K^{α_i}, $\alpha_i \equiv 0 \bmod \mathfrak{a}$, z_i aus K. Die $\alpha_i \mu_0$ liegen in $\mathfrak{a}$ und daher wird durch

$$z^{\mu_0} = R(z_1^{\alpha_1 \mu_0}, \cdots, z_t^{\alpha_t \mu_0})$$

ein Element von $K^{\mathfrak{a}}$ definiert. Es ist leicht einzusehen, daß z^{μ_0} nicht davon abhängt, wie z durch Elemente z^{α_i} dargestellt wird, anders ausgedrückt, daß

$$R(z_1^{\alpha_1 \mu_0}, \cdots, z_t^{\alpha_t \mu_0}) = 0$$

ist, sobald

$$R(z_1^{\alpha_1}, \cdots, z_t^{\alpha_t}) = 0$$

gilt: Es gibt eine natürliche Zahl n, so daß $n\mu_0$ in $\mathfrak{R}$ liegt. Aus

$$R(z_1^{\alpha_1}, \cdots, z_t^{\alpha_t}) = 0$$

folgt dann

$$0 = R(z_1^{\alpha_1}, \cdots, z_t^{\alpha_t})^{\mu_0 n} = R(z_1^{\alpha_1 \mu_0}, \cdots, z_t^{\alpha_t \mu_0})^n$$

und daraus

$$R(z_1^{\alpha_1 \mu_0}, \cdots, z_t^{\alpha_t \mu_0}) = 0,$$

Aus der Definition der Anwendung von μ_0 auf K_0 ergibt sich unmittelbar, daß μ_0 ein Meromorphismus von K_0 ist.

μ_0 ist für $\mathfrak{o}_0 = N_{K/K_0}\mathfrak{o}$ normiert, d. h. es ist $\mathfrak{o}_0^{\mu_0} = N_{K_0/K_0^{\mu_0}}\mathfrak{o}_0$, anders ausgedrückt, $\mathfrak{o}_0$ geht in $\mathfrak{o}_0^{\mu_0}$ auf. Zum Beweis sei α irgendein Element von $\mathfrak{a}$. $\mathfrak{o}_0$, $\mathfrak{o}^{\alpha}$ und $\mathfrak{o}^{\alpha\mu_0}$ sind durch $\mathfrak{o}$ teilbar, folglich ist der durch $\mathfrak{o}$, also durch $\mathfrak{o}_0$, teilbare Primdivisor des zwischen $K_0 = K^{\mathfrak{a}}$ und $K^{\alpha\mu_0}$ gelegenen Körpers $K^{\mathfrak{a}\mu_0}$ gleich $\mathfrak{o}_0^{\mu_0}$.

In dem Fall, wo $\mathfrak{a}$ ein Ideal mit maximalen Ordnungen ist, kann der Multiplikatorenring von $K^{\mathfrak{a}}$ natürlich nicht größer sein als die Rechtsordnung von $\mathfrak{a}$, die noch nötige Ergänzung des Beweises erübrigt sich dann.

3. *Es ist* $(K : K^{\mathfrak{a}}) = N\mathfrak{a}$.

Wir beweisen diesen Satz zunächst nur für den Fall, daß $\mathfrak{R}$ maximal ist und verschieben den allgemeinen Beweis auf **9.**

Die Linksordnung von $\mathfrak{a}$ sei $\mathfrak{R}_1$, die Rechtsordnung von $\mathfrak{a}$, also der Multiplikatorenring von $K^{\mathfrak{a}}$ sei $\mathfrak{R}_2$. Wir wollen ein Ideal mit der Linksordnung $\mathfrak{R}_i$ und der Rechtsordnung $\mathfrak{R}_j$ mit $\mathfrak{a}_{ij}$ bezeichnen und dementsprechend $\mathfrak{a}_{12}$ statt $\mathfrak{a}$ schreiben. Es sei jetzt $\mathfrak{a}_{23}$ ein zu $(K:K^{\mathfrak{a}})$ teilerfremdes ganzes Linksideal von $\mathfrak{R}_2$, für das $\mathfrak{a}_{12}\mathfrak{a}_{23} = \mathfrak{R}_1\alpha$ Hauptideal ist[15]). Wegen $K^{\alpha} \leqq K^{\mathfrak{a}_{12}}$ ist $(K:K^{\alpha}) \equiv 0 \mod (K:K^{\mathfrak{a}_{12}})$, aus

$$(K:K^{\mathfrak{a}}) = N\alpha = N\mathfrak{a}_{12}\cdot N\mathfrak{a}_{23}$$

folgt also

$$N\mathfrak{a}_{12} \equiv 0 \pmod{(K:K^{\mathfrak{a}})},$$

es sei etwa

$$N\mathfrak{a}_{12} = t\,(K:\overset{J}{K}{}^{\mathfrak{a}}).$$

Ebenso gilt

$$N\mathfrak{a}_{23} = t'\,(K^{\mathfrak{a}_{12}}:\ K^{\mathfrak{a}_{12}\mathfrak{a}_{23}})$$

mit ganzem t'. Da aber

$$N\mathfrak{a}_{12}\,N\mathfrak{a}_{23} = N\alpha = (K:K^{\mathfrak{a}}) = (K:K^{\mathfrak{a}_{12}})\,(K^{\mathfrak{a}_{12}}:K^{\mathfrak{a}_{12}\mathfrak{a}_{23}})$$

ist, so muß $t = t' = 1$, $(K:K^{\mathfrak{a}}) = N\mathfrak{a}$ sein, wie behauptet.

4. *Wenn Σ die Quaternionenalgebra $Q_{\infty,p}$ ist, so ist $\mathfrak{R}$ eine Maximalordnung von Σ.*

Beweis. Für ein Linksideal $\mathfrak{a}$ von $\mathfrak{R}$ mit maximalen Ordnungen ist der Multiplikatorenring von $K_0 = K^{\mathfrak{a}}$ maximal. Da in K_0 der zu K isomorphe Teilkörper $K^{N\mathfrak{a}\varepsilon}$ enthalten ist, so genügt es *anzunehmen*, daß $\mathfrak{R}$ *maximal ist* und zu *beweisen*, daß alle elliptischen Teilkörper von K ebenfalls *maximale* Multiplikatorenringe haben. Das werden wir daraus schließen, daß jeder elliptische Teilkörper K_0 von K zu einem Linksideal $\mathfrak{a}$ von $\mathfrak{R}$ gehört: $K_0 = K^{\mathfrak{a}}$. Das wiederum folgt daraus, daß es ebenso viele elliptische Teilkörper von K gibt, über denen K einen vorgegebenen Grad n hat, wie ganze Linksideale von $\mathfrak{R}$ mit der Norm n. Wir zerlegen n in eine Potenz p^f der Charakteristik und ein dazu teilerremdes Primzahlpotenzprodukt $n_0 = \prod q_i^{f_i}$. Jedes ganze Linksideal der Norm n von $\mathfrak{R}$ ist der Durchschnitt von eindeutig bestimmten Linksidealen der Normen p^f, $q_1^{f_1}$, $q_2^{f_2}\cdots$. Die Anzahl der ganzen Linksideale mit der Norm $q_i^{f_i}$ ergibt sich leicht zu $1+q_i+q_i^2+\cdots+q_i^{f_i}$, dagegen

[15]) Für kommutatives Σ ist das bekannt. Daß es auch für $Q_{\infty,p}$ gilt, wurde von Nehrkorn gezeigt: H. Nehrkorn, Über absolute Idealklassengruppe und Einheiten in algebraischen Zahlkörpern, diese Abh. **9**, S. 318—334 (1933). Siehe auch M. Deuring, Algebren. Ergebn. der Math. IV, 1, S. 106, Satz 27.

gibt es nur ein ganzes Linksideal der Norm p^f. Folglich gibt es

$$\prod (1 + q_i + q_i^2 + \cdots + q_i^{f_i})$$

ganze Linksideale der Norm n.

Da es in K keine Divisorenklassen der Ordnung p gibt, so ist die Galoisgruppe von K über einem Teilkörper K_0 mit $(K : K_0) = n$ von der Ordnung n_0 und K_0 ist die p^f-te Potenz des Invariantenkörpers dieser Galoisgruppe. Infolgedessen gibt es ebenso viele Körper K_0 wie Klassengruppen n_0-ter Ordnung in K. Da die Gruppe aller Klassen mit in n_0 aufgehender Ordnung das direkte Produkt zweier Zyklen der Ordnung n_0 ist, so wird diese Anzahl gerade gleich

$$\prod (1 + q_i + q_i^2 + \cdots + q_i^{f_i})$$

was zu beweisen war.

5. Die Gruppe $\mathfrak{C}_q$ der Klassen von K, deren Ordnung eine Potenz der Primzahl q ist, ist für $q \neq p$ zu der additiven Gruppe der Restklassen modulo 1 aller Paare (r_1, r_2) von rationalen Zahlen isomorph, deren Nenner Potenzen von q sind, für $q = p$ dagegen entweder zu der Gruppe der Restklassen modulo 1 aller rationalen Zahlen, deren Nenner Potenzen von p sind — Fall $\sigma = 1$, oder sie besteht nur aus der Klasse $0 = [\mathfrak{o}]$ — Fall $\sigma = 2$.

Ist $q \neq p$, so wollen wir das der Klasse $[\mathfrak{p}]$ zugeordnete Restklassenpaar mit $r[\mathfrak{p}]$ bezeichnen. Für einen Multiplikator μ gilt

$$r\mu[\mathfrak{p}] \equiv r[\mathfrak{p}] S_q(\mu) \mod 1,$$

wo $S_q(\mu)$ eine bestimmte ganzzahlige q-adische Matrix bezeichnet. $\mu \to S_q(\mu)$ ist eine treue Darstellung von $\mathbf{R}$[16]).

Für $q = p$, $\sigma = 1$, nennen wir die $[\mathfrak{p}]$ zugeordnete Restklasse $r_1[\mathfrak{p}]$. Es wird dann

$$r_1\mu[\mathfrak{p}] \equiv r_1[\mathfrak{p}] s_p(\mu) \mod 1$$

mit einer ganzen $\mathfrak{p}$-adischen Zahl $s_p[\mu]$. Wiederum ist $\mu \to s_p[\mu]$ eine treue Darstellung von $\mathbf{R}$.

Die Darstellung $S_q(\mu)$ oder $s_p(\mu)$ kann eindeutig zu einer treuen Darstellung von Σ erweitert werden. *Für Elemente μ von $\mathbf{R}$ sind alle $S_q(\mu)$ und $s_p(\mu)$ ganz. Wir zeigen, daß umgekehrt das Element μ von Σ*

[16]) M. Deuring, Arithmetische Theorie der Korrespondenzen algebraischer Funktionenkörper, II. § 5, **6**, Journ. f. d. r. u. ang. Math. **183**, S. 25—36 (1941).

in $\mathfrak{R}$ *liegt, wenn alle* $S_q(\mu)$ *ganz sind, und, falls* $p \neq 0$, *außerdem* μ *p-ganz ist.*

Beweis. n sei eine natürliche Zahl, für die das n-fache von μ in $\mathfrak{R}$ liegt. μ selbst gehört zu $\mathfrak{R}$, wenn jeder Automorphismus $\tau_{\mathfrak{o},\mathfrak{p}}$ von $K/K^{n\varepsilon}$ auch $K^{n\mu}$ elementweise fest läßt und wenn außerdem der Inseparabilitätsgrad $I(K:K^{n\varepsilon})$ in $I(K:K^{n\mu})$ aufgeht. Das erste ergibt sich so: Wir können annehmen, daß die Ordnung von $\tau_{\mathfrak{o},\mathfrak{p}}$ eine Potenz einer Primzahl q ist. Für $q \neq p$ wird nach § 1 **2.** $n \cdot r[\mathfrak{p}] \equiv 0 \bmod 1$, folglich

$$n \cdot r\mu[\mathfrak{p}] \equiv n \cdot r[\mathfrak{p}]\, S_q(\mu) \equiv 0 \bmod 1$$

und für $q = p$, $\sigma = 1$, da $s_p(\mu)$ für p-ganzes μ ganz ist,

$$n \cdot r_1[\mathfrak{p}] \equiv 0 \bmod 1, \qquad n \cdot r_1\mu[\mathfrak{p}] \equiv n \cdot r_1[\mathfrak{p}]\, s_p(\mu) \equiv 0 \bmod 1,$$

also ist nach § 1 **2.** $\tau_{\mathfrak{o},\mathfrak{p}}$ ein Automorphismus von $K/K^{n\mu}$.

$I(K:K^{n\varepsilon}) \mid I(K:K^{n\mu})$ zeigen wir so: p^f sei die in n enthaltene Potenz von p und p^λ die in $N\mu$ enthaltene. Es wird

$$I(K:K^{n\varepsilon}) = p^{f\sigma} \quad \text{und} \quad I(K:K^{n\mu}) = p^{f\sigma+\lambda},$$

aber λ ist nicht negativ, da μ p-ganz ist.

6. $\mathfrak{K}$ sei eine endliche Klassengruppe von K. $\mathfrak{K}_q$ bedeute die Untergruppe der Elemente von $\mathfrak{K}$, deren Ordnungen Potenzen der Primzahl q sind. Für $q \neq p$ bilden die rationalen q-adischen Matrizen

$$R = \begin{pmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{pmatrix},$$

deren beiden Zeilen (r_{i1}, r_{i2}), mod 1 genommen, in $\mathfrak{K}_q$ enthaltenen Klassen zugeordnet sind, ein Linksideal $\mathfrak{l}_q$ im Ring der ganzen q-adischen Matrizen. Denn die Differenz zweier Matrizen R ist wieder eine Matrix R, weil $\mathfrak{K}_q$ eine Gruppe ist, das Produkt GR einer ganzzahligen Matrix G mit einer Matrix R hat als Zeilen ganzzahlige Linearkombinationen der Zeilen von R und ist daher selbst eine Matrix R, schließlich ist das Produkt jeder Matrix R mit dem Hauptnenner der endlich vielen $r[\mathfrak{p}]$, $[\mathfrak{p}]$ aus $\mathfrak{K}_q$, ganz. Da alle ganzen Matrizen in $\mathfrak{l}_q$ enthalten sind, so ist $\mathfrak{r}_q = \mathfrak{l}_q^{-1}$ ein ganzes Rechtsideal. $\mathfrak{r}_q$ wird von einer ganzen q-adischen Matrix C_q erzeugt, die bis auf einen unimodularen Rechtsfaktor eindeutig bestimmt ist. R gehört genau dann zu $\mathfrak{l}_q$, wenn RC_q ganz ist. *Daher sind die Elemente* $[\mathfrak{p}]$ *der Gruppe* $\mathfrak{K}_q$ *durch*

$$r[\mathfrak{p}]\, C_q \equiv 0 \bmod 1 \tag{5}$$

gekennzeichnet und die Ordnung von $\mathfrak{R}_q$ ist die in der Determinante von C_q enthaltene Potenz von q. Fast alle C_q sind unimodular und können gleich der Einsmatrix E genommen werden.

Im Falle $p \neq 0$, $\sigma = 1$ kann $\mathfrak{R}$ auch eine p-Untergruppe $\mathfrak{R}_p$ haben. Die deren Elementen zugeordneten Restklassen $r_1[\mathfrak{p}]$ haben einen Hauptnenner c_p, der bis auf einen p-adischen Einheitsfaktor eindeutig bestimmt ist. *Die Elemente von $\mathfrak{R}_p$ sind dann durch*

$$r_1[\mathfrak{p}]\, c_p \equiv 0 \bmod 1 \tag{6}$$

gekennzeichnet und die Ordnung von $\mathfrak{R}_p$ ist die in c_p enthaltene Potenz von p.

Durch alle C_q und c_p ist $\mathfrak{R}$ festgelegt.

Wenn umgekehrt für jede Primzahl $q \neq p$ eine ganze q-adische Matrix C_q, die nur für endlich viele q nicht unimodular ist und außerdem im Falle $p \neq 0$, $\sigma = 1$ eine ganze p-adische Zahl c_p gegeben ist, so gehört zu ihnen eine endliche Klassengruppe $\mathfrak{R}$.

7. K_0 sei ein elliptischer Teilkörper von K und $\mathfrak{R}$ die durch $[\mathfrak{p}] \to \tau_{\mathfrak{o},\mathfrak{p}}$ mit der Galoisgruppe von K/K_0 isomorphe Klassengruppe. Innerhalb K ist K_0 durch $\mathfrak{R}$ und $I(K:K_0)$ oder, was auf das gleiche hinausläuft, durch die Matrizen C_q, c_p und $I(K:K_0)$ bestimmt.

Aus der Darstellung $[\mathfrak{p}] \to r[\mathfrak{p}]$ der q-Klassengruppe $\mathfrak{C}_q$ von K kann eine entsprechende Darstellung der q-Klassengruppe von K_0 abgeleitet werden, indem

$$r[N_{K/K_0}\mathfrak{p}] \equiv r[\mathfrak{p}]\, C_q \bmod 1 \tag{7}$$

gesetzt wird. Denn der Homomorphismus $r[\mathfrak{p}] \to r[\mathfrak{p}]\, C_q$ bildet genau die $[\mathfrak{p}]$ auf 0 ab, für welche $\tau_{\mathfrak{o},\mathfrak{p}}$ ein Automorphismus von K/K_0 ist (§ 1 **6.**). Ebenso kann im Falle $p \neq 0$, $\sigma = 1$ für die p-Klassengruppe

$$r_1[N_{K/K_0}\mathfrak{p}] \equiv r_1[\mathfrak{p}]\, c_p \bmod 1 \tag{8}$$

gesetzt werden.

Wenn μ ein gemeinsamer Multiplikator von K und K_0 ist, so gilt für jedes Element $[\mathfrak{p}]$ von $\mathfrak{C}_q$

$$\begin{aligned} r\mu[N_{K/K_0}\mathfrak{p}] &\equiv r[N_{K/K_0}(\mu[\mathfrak{p}])] \equiv r\mu[\mathfrak{p}]\, C_q \equiv r[\mathfrak{p}]\, S_q(\mu)\, C_q \\ &\equiv r[N_{K/K_0}\mathfrak{p}]\, C_q^{-1} S_q(\mu)\, C_q \bmod 1 \end{aligned} \tag{9}$$

und ebenso im Falle $p \neq 0$, $\sigma = 1$ für ein Element $[\mathfrak{p}]$ von $\mathfrak{C}_p$

$$\begin{aligned} r_1\mu[N_{K/K_0}\mathfrak{p}] &\equiv r_1[N_{K/K_0}(\mu[\mathfrak{p}])] \equiv r_1\mu[\mathfrak{p}]\, c_p \equiv r_1[\mathfrak{p}]\, s_p(\mu)\, c_p \\ &\equiv r_1[N_{K/K_0}\mathfrak{p}]\, s_p(\mu) \bmod 1. \end{aligned} \tag{10}$$

Mit anderen Worten:

Die Matrix C_q transformiert die zu K gehörige q-adische Darstellung von Σ in die zu K_0 gehörige, während im Falle $p \nmid 0$, $\sigma = 1$ zu K und K_0 die gleiche p-adische Darstellung von Σ gehört.

8. Wir bestimmen jetzt die Darstellungen $S_q(\mu)$ und $s_q(\mu)$ genauer.

Da der natürliche Multiplikator n nichts weiter ist als die Bildung der n-ten Potenzen in der Klassengruppe, so gilt:

Ist Σ der rationale Zahlkörper, so ist

$S_q(n) = \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix}$ *die zweimal genommene identische Darstellung von Σ und $s_p(n) = n$.*

Ist $\Sigma = Q_{\infty,p}$, so ist $S_q(\mu)$ die irreduzible q-adische Darstellung zweiten Grades von Σ.

Denn andere irreduzible q-adische Darstellung von $Q_{\infty,p}$ gibt es nicht.

Es bleibt der Fall näher zu untersuchen, wo Σ ein imaginärquadratischer Zahlkörper ist. *Wir behaupten, daß dann für $q \nmid p$ $S_q(\mu)$ die reguläre Darstellung von Σ und, im Falle $p \nmid 0$, $\sigma = 1$, $s_p(\mu)$ die $\mathfrak{p}_1$-adische Darstellung von Σ ist, wo $\mathfrak{p}_1$ eins von zwei verschiedenen in p aufgehenden Primidealen von Σ bedeutet.*

Die Behauptung über $s_p(\mu)$ ist selbstverständlich, weil es andere p-adische Darstellungen ersten Grades von Σ nicht geben kann. Ebenso ist die Behauptung über jedes in Σ nicht voll zerfallende $q \nmid p$ selbstverständlich. $q \nmid p$ sei in Σ das Produkt zweier verschiedener Primideale $\mathfrak{q}_1$ und $\mathfrak{q}_2$. Es gibt dann zwei inäquivalente rationale q-adische Darstellungen ersten Grades $\mathcal{A}_1$ und $\mathcal{A}_2$ von Σ, und es ist zu zeigen, daß $S_q(\mu)$ mit der Summe $\mathcal{A}_1 + \mathcal{A}_2$ äquivalent ist. $\mathcal{A}_i$ bildet genau die durch $\mathfrak{q}_i$ teilbaren μ auf durch q teilbare Zahlen ab. Da wir nach **7.** die Behauptung nur für irgendeinen elliptischen Teilkörper von K zu beweisen brauchen, so können wir annehmen, daß $\mathfrak{R}$ die Maximalordnung von Σ ist. Gesetzt, $S_q(\mu)$ wäre nicht zu $\mathcal{A}_1 + \mathcal{A}_2$, sondern etwa zu $2\mathcal{A}_1$ äquivalent. Für ein durch $\mathfrak{q}_2$, aber nicht durch $\mathfrak{q}_1$ teilbares Element μ von $\mathfrak{R}$ wäre dann die Determinante $|S_q(\mu)|$ nicht durch q teilbar, und es gäbe daher keine Klasse der Ordnung q mit $r\mu\,[\mathfrak{p}] \equiv 0 \bmod 1$ oder $\mu\,[\mathfrak{p}] = 0$. Die Galoisgruppe von K/K^μ enthielte daher kein Element der Ordnung q, was dem widerspricht, daß $(K : K^\mu) = N\mu$ durch q teilbar ist.

9. Wir gehen jetzt noch genauer auf den Fall ein, daß Σ ein imaginärer quadratischer Zahlkörper ist.

Die Zahlen μ_q der q-adischen Erweiterung Σ_q von Σ, für welche $S_q(\mu_q)$ eine ganze q-adische Matrix ist ($\mu_q[\mathfrak{p}]$ ist durch

$$r\mu_q[\mathfrak{p}] = \lim_{i\to\infty} r\mu_i[\mathfrak{p}]$$

für eine gegen μ_q konvergente Folge von Zahlen μ_i aus $\mathbf{R}$ zu definieren), bilden eine Ordnung $\mathbf{R}_q$ in Σ_q. Bezeichnen wir noch im Falle $p \neq 0$ mit $\mathbf{R}_p$ die Maximalordnung von Σ_p, so ist $\mathbf{R}$ der Durchschnitt von allen $\mathbf{R}_q$ und $\mathbf{R}_p$, und $\mathbf{R}_q$ ($q \neq p$ oder $= p$) ist die q-adische Grenzmenge von $\mathbf{R}$.

Wir holen jetzt die für komplexes kommutatives $\mathbf{R}$ noch ausstehenden Beweise dafür nach, daß die Ordnung $\mathbf{R}'$ eines Ideals $\mathbf{a}$ von $\mathbf{R}$ der Multiplikatorenring von $K^{\mathbf{a}}$ ist und daß $(K : K^{\mathbf{a}}) = N\mathbf{a}$ ist.

Die Darstellung $S_q(\mu)$ wird durch eine passende Basis $\omega_1(q)$, $\omega_2(q)$ von $\mathbf{R}_q$ erzeugt:

$$\mu(\omega_1(q), \omega_2(q)) = (\omega_1(q), \omega_2(q))\, S_q(\mu).$$

α_1, α_2 sei eine Basis von $\mathbf{a}$,

$$(\alpha_1, \alpha_2) = (\omega_1(q), \omega_2(q))\, A_q.$$

Aus

$$\alpha(\omega_1(q), \omega_2(q)) = (\alpha_1, \alpha_2)\, A_q^{-1} S_q(\alpha)$$

folgt, daß $A_q S_q(\alpha)$ für α aus $\mathbf{a}$ ganz ist, A_q ist also ein gemeinsamer Linksteiler aller Matrizen $S_q(\alpha)$, $\alpha \equiv 0 \bmod \mathbf{a}$. Andererseits läßt sich A_q mittels zweier ganzen q-adischen Matrizen H_1 und H_2 in der Gestalt

$$A_q = S_q(\alpha) H_1 + S_q(\alpha_2) H_2$$

ausdrücken, wir brauchen die H_i nur aus

$$(\omega_1(q), \omega_2(q))\, H_1 = (1, 0),$$
$$(\omega_1(q), \omega_2(q))\, H_2 = (0, 1)$$

zu bestimmen. Daher ist A_q ein größter gemeinsamer Linksteiler aller $S_q(\alpha)$, $\alpha \equiv 0 \bmod \mathbf{a}$.

Für ein Element $\tau_{\mathfrak{v},\mathfrak{p}}$ der Galoisgruppe vom $K/K^{\mathbf{a}}$, dessen Ordnung eine Potenz von q ist, gilt $\mathbf{a}[\mathfrak{p}] = 0$, also $r\alpha[\mathfrak{p}] \equiv 0 \bmod 1$, wenn $\alpha \equiv 0 \bmod a$ oder $r[\mathfrak{p}] S_q(\alpha) \equiv 0 \bmod 1$ und daher $r[\mathfrak{p}] A_q \equiv 0 \bmod 1$. Ist umgekehrt $r[\mathfrak{p}] A_q \equiv 0 \bmod 1$ für eine Klasse $[\mathfrak{p}]$, deren Ordnung

eine Potenz von q ist, so wird

$$r\alpha\,[\mathfrak{p}] \equiv r\,[\mathfrak{p}]\,S_q(\alpha) \equiv 0 \bmod 1 \text{ für alle } \alpha \equiv 0 \bmod \mathfrak{a}$$

und daher ist $\tau_{\mathfrak{o},\mathfrak{p}}$ ein Automorphismus von $K/K^{\mathfrak{a}}$. Das bedeutet, daß wir für den Teilkörper $K_0 = K^{\mathfrak{a}}$ die Matrix S_q gleich A_q nehmen können. Zu $K^{\mathfrak{a}}$ gehört daher die q-adische Darstellung $A_q^{-1} S_q(\mu) A_q$, die q-adische Grenzmenge $\mathfrak{R}'_q$ des Multiplikatorenringes $\mathfrak{R}'$ von $K^{\mathfrak{a}}$ ist die Ordnung des Moduls $\mathfrak{a}_q$, der q-adischen Grenzmenge von $\mathfrak{a}$ und $\mathfrak{R}'$ ist der Durchschnitt aller $\mathfrak{R}'_q$ mit $\mathfrak{R}_p$, das ist aber die Ordnung von $\mathfrak{a}$.

$(K : K^{\mathfrak{a}}) = N\mathfrak{a}$ können wir jetzt wörtlich genau so beweisen wie für maximale $\mathfrak{R}$. Es ist nur zu bemerken, daß jetzt feststeht, daß $\mathfrak{R}_2$ der Multiplikatorenring von $\mathfrak{a}_{12}$ ist und daß auch für nichtmaximales $\mathfrak{R}_2$ ein zu $(K : K^{\mathfrak{a}})$ teilerfremdes Ideal $\mathfrak{a}_{23}$ so gewählt werden kann, daß $\mathfrak{a}_{12}\,\mathfrak{a}_{23}$ ein Hauptideal ist[17]).

10. Aus dem Vorstehenden ergeben sich einschränkende Bedingungen für den Typus des Multiplikatorenringes. Indem wir den Fall nur rationaler Multiplikatoren beiseite lassen, behaupten wir:

K habe einen komplexen Multiplikatorenring $\mathfrak{R}$ mit dem Quotientenkörper Σ. Wenn die Charakteristik von K 0 ist, so ist Σ ein imaginärer quadratischer Zahlkörper. Wenn die Charakteristik $p \neq 0$ ist und $\sigma = 1$, so ist Σ ein imaginärer quadratischer Zahlkörper, in dem p in zwei verschiedene Primideale zerfällt und $\mathfrak{R}$ eine Ordnung von Σ mit nicht durch p teilbarem Führer. Ist dagegen $\sigma = 2$, so ist $\Sigma = Q_{\infty,p}$ und $\mathfrak{R}$ eine Maximalordnung in $Q_{\infty,p}$.

Die Behauptung für $p = 0$ ist schon bewiesen. Sei $p \neq 0$ und $\sigma = 1$. Da es eine p-adische Darstellung $\mu \to s_p(\mu)$ von Σ gibt, so zerfällt p in zwei verschiedene Primideale von Σ. Da $\mathfrak{R}$ der Durchschnitt aller $\mathfrak{R}_q$ ist, so ist die im Führer von $\mathfrak{R}$ enthaltene Potenz von p der Führer von $\mathfrak{R}_p$, aber $\mathfrak{R}_p$ ist die Maximalordnung von Σ_p (**9.**), ihr Führer also 1. Im Falle $p \neq 0$, $\sigma = 2$ ist $K^{p^2} = K^{p^2}$ und daher $j^{p^2} = j$, es gibt folglich nur endlich viele nicht isomorphe Körpertypen dieser Art, insbesondere hat das gegebene K nur endlich viele nicht isomorphe elliptische Teilkörper. Wäre nun Σ ein imaginärer quadratischer Zahlkörper und nicht $Q_{\infty,p}$, so hätten, unter $q_1, q_2, \cdots$ die in Σ prim bleibenden Primzahlen verstanden, die Glieder einer Folge $K = K_1, K_2, \cdots$ von Teilkörpern von K, wo jeweils K_i über K_{i+1} zyklisch vom Grade q_i ist, lauter verschiedene Invarianten, weil es sonst in Σ ganze Zahlen mit Normen $q_i\, q_{i+1} \cdot \cdots \cdot q_{i+h}$ gäbe.

[17]) W. Weber, Bemerkungen zur arithmetischen Theorie der binären quadratischen Formen, Nachr. Ges. d. Wiss. Göttingen, 1929, S. 116–130; Satz 1.

§ 3. Multiplikatoren bei nicht algebraisch abgeschlossenem Konstantenkörper. Die durch das ganze Differential vermittelte Darstellung des Multiplikatorenringes.

1. Wir betrachten wie in den vorhergehenden Abschnitten einen elliptischen Funktionenkörper K mit algebraisch abgeschlossenem Konstantenkörper k. Wenn x, y ein erzeugendes Elementepaar von K/k ist und die Koeffizienten der irreduziblen Gleichung $f(x, y) = 0$ dem Teilkörper $k^{(0)}$ von k angehören, so gibt es einen Teilkörper $K^{(0)} = k^{(0)}(x, y)$ von K mit dem Konstantenkörper $k^{(0)}$, aus dem K durch Konstantenerweiterung hervorgeht. *$k^{(0)}$ enthält stets die Invariante j von K. Andererseits können x, y so gewählt werden, daß $k^{(0)} = P(j)$ und $K^{(0)} = P(j; x, y)$ ein elliptischer Körper mit wenigstens einem Primdivisor ersten Grades ist* (P bedeutet den Primkörper)[18]). $P(j)$ ist also der kleinstmögliche Konstantenkörper für einen Funktionenkörper $K^{(0)}$, aus dem sich K durch Konstantenerweiterung ergeben soll, $K^{(0)}k = K$.

2. $K^{(0)} = k^{(0)}(x, y)$ sei ein elliptischer Körper mit $K^{(0)}k = K$. Wir fragen danach, für welche zwischen $k^{(0)}$ und k gelegenen Körper $k^{(1)}$ ein gegebener Multiplikator μ von K/k schon in $k^{(1)}(x, y) = K^{(1)}$ möglich ist, das heißt, wann der mit einem durch $x \to x^{\varphi}$, $y \to y^{\varphi}$ zu $K^{(1)}/k^{(1)}$ isomorphen Körper $K^{(1)\varphi}/k^{(1)}$ gebildete Doppelkörper $K^{(1)}K^{(1)\varphi}$ als Funktionenkörper von x^{φ} über K einen Divisor $\mathfrak{D}$ hat, der den Multiplikator μ definiert.

Da es uns nur auf den Typus ankommt, so setzen wir voraus, daß $K^{(0)}$ einen Primdivisor ersten Grades $\mathfrak{o}$ hat. Wie für k können wir dann durch $\mathfrak{P}_{\mu} \sim \mathfrak{D}\mathfrak{o}^{\varphi}/\mathfrak{D}(\mathfrak{o})^{\varphi}$ eindeutig einen Primdivisor ersten Grades $\mathfrak{P}_{\mu}$ bestimmen, der den Multiplikator μ definiert und für den $\mathfrak{P}_{\mu}(\mathfrak{o}) = \mathfrak{o}$ gilt[19]). Das durch

$$z^{\varphi} \equiv z^{\mu} \bmod \mathfrak{P}_{\mu}$$

zu jedem z aus $K^{(1)}$ eindeutig bestimmte Element z^{μ} aus $K^{(1)}$ ergibt einen für $\mathfrak{o}$ normierten Meromorphismus $z \to z^{\mu}$ von $K^{(1)}/k^{(1)}$, *wenn also der Multiplikator μ in $K^{(1)}$ möglich ist, dann auch der zugehörige für $\mathfrak{o}$ normierte Meromorphismus.*

Die Multiplikatoren von $K^{(1)}/k^{(1)}$ bilden einen Teilring $\mathfrak{R}_1$ des vollen Multiplikatorenringes $\mathfrak{R}$ von K/k.

2. du sei ein ganzes Differential von $K^{(0)}$. Durch

$$(du)^{\mu} = \mu' du \tag{11}$$

[18]) Vgl. M. Deuring: Invarianten und Normalformen elliptischer Funktionenkörper und Zur Theorie der Moduln algebraischer Funktionenkörper. Math. Zeitschr. **47**, S. 34—56 (1941).

[19]) Loc. cit. [14]).

wird eine homomorphe Abbildung $\mu \to \mu'$ von $\mathbf{R}$ in den Konstantenkörper k definiert.

Wenn die Charakteristik p gleich 0 ist, so gilt für $\mu \neq 0$ auch $\mu' \neq 0$, und daher ist in diesem Falle die Darstellung $\mu \to \mu'$ treu. Ist dagegen $p \neq 0$, so kann sie nicht treu sein, weil dann k und $\mathbf{R}$ verschiedene Charakteristiken haben, sie muß dann den Restklassenring von $\mathbf{R}$ nach einem in p aufgehenden Primideal $\mathfrak{p}$ treu abbilden. Da nur dann $\mu \neq 0$ und $\mu' = 0$ sein kann, wenn K über K^μ inseparabel ist, *so besteht* $\mathfrak{p}$ *außer aus* $\mu = 0$ *aus allen den* $\mu \neq 0$, *für die* K *einen von* 1 *verschiedenen Inseparabilitätsgrad* I_μ *über* K^μ *hat. Ist* $\Sigma = P_0$, *so ist* $\mathfrak{p} = \mathbf{R}p$, *ist* Σ *ein imaginärer quadratischer Zahlkörper, so zerfällt nach § 2* **10.** p *in zwei verschiedene Primideale von* $\mathbf{R}$, *von denen eines* $\mathfrak{p}$ *ist; ist* $\Sigma = Q_{\infty, p}$, *so ist* $\mathfrak{p}$ *das einzige in* p *aufgehende Primideal von* $\mathbf{R}$.

3. Aus der Definition der Darstellung $\mu \to \mu'$ folgt unmittelbar:

Ist μ *schon in* $K^{(1)}$ *möglich, so liegt* μ' *in* $k^{(1)}$.

Davon gilt die folgende Umkehrung:

Wenn $\mathbf{R}$ *kommutativ ist, so ist* μ *in* $K^{(1)}$ *möglich, falls* μ' *in* $k^{(1)}$ *liegt.*

Beim Beweis setzen wir zunächst nicht voraus, daß μ' in k liege.

Eine endliche algebraische Erweiterung k^* *von* k *genügt, um* μ *in* $K^* = k^*(x, y)$ *zu ermöglichen.* Denn ist n der Grad von y *in* $k^{(1)}(x)$ und

$$x^\mu = \sum_{i=0}^{n-1} A_i(x)\, y^i, \qquad y^\mu = \sum_{i=0}^{n-1} B_i(x)\, y^i,$$

so genügt es, die Koeffizienten der eindeutig bestimmten rationalen Funktionen A_i und B_i zu adjungieren, diese aber sind algebraisch über $k^{(1)}$, weil ein transzendenter Koeffizient, algebraisch spezialisiert, zu unendlich vielen neuen Multiplikatoren Anlaß gäbe, deren Normen unter einer festen Schranke lägen. *Die Koeffizienten von* A_i *und* B_i *sind sogar separabel über* $k^{(1)}$. Wenn μ ganz rational ist, so liegen sie in $k^{(1)}$, weil die ganzen rationalen Multiplikatoren aus dem Einsmultiplikator $x \to x$, $y \to y$ durch Additionen gewonnen werden können. Für $p = 0$ ist nichts weiter zu beweisen. Für $p \neq 0$ und komplexes $\mathbf{R}$ ist aber die Invariante j von K absolut algebraisch, woraus die Separabilität der Koeffizienten von A_i und B_i folgt, weil $k^{(1)}$ vollkommen ist: Für $\sigma = 2$ ist $K^{\varepsilon p} = K^{p^2}$ und daher $j^{p^2} = j$; für $\sigma = 1$ zerfällt p nach § 2 **10.** in zwei verschiedene Primideale von $\mathbf{R}$ und für eins von diesen, $\mathfrak{p}$, muß, weil $N\mathfrak{p} = p$ gilt, nach **2.** $K^{\mathfrak{p}} = K^p$ sein. Ist $\mathfrak{p}^h = (\pi)$ Hauptideal, so ist $K^{p^h} = K^\pi \cong K$ und daher $j^{p^h} = j$.

Wir wollen k^* als endliche separable normale Erweiterung von $k^{(1)}$ annehmen. ϱ sei ein Automorphismus von $k^*/k^{(1)}$. Wir dehnen ihn auf $K^* = K^{(1)} k^*$ aus, indem wir $x^\varrho = x$, $y^\varrho = y$ setzen, was möglich ist, weil die Koeffizienten der Gleichung $f(x, y) = 0$ zwischen x und y in k_0 und um so mehr in $k^{(1)}$ liegen. x^μ und y^μ genügen ebenfalls der Gleichung

$$f(x^\mu, y^\mu) = 0,$$

und daraus folgt

$$f((x^\mu)^\varrho, (y^\mu)^\varrho) = 0.$$

Mithin ist $z \to (z^\mu)^\varrho$ ein Meromorphismus μ^ϱ von K^*/k^*. μ^ϱ ist für $\mathfrak{o}$ normiert, denn aus $\mathfrak{o} \mid \mathfrak{o}^\mu$ folgt $\mathfrak{o}^\varrho \mid \mathfrak{o}^{\mu^\varrho}$ oder $\mathfrak{o}\ \mathfrak{o}^{\mu^\varrho}$. $\mu \to \mu^\varrho$ *ist ein Automorphismus von* $\mathbf{R}$.

$$(\mu\nu)^\varrho = \mu^\varrho \nu^\varrho$$

folgt sofort aus der Definition von ϱ.

$$(\mu + \nu)^\varrho = \mu^\varrho + \nu^\varrho$$

beweisen wir, indem wir ϱ durch $(x^\Phi)^\varrho = x^\Phi$, $(y^\Phi)^\varrho = y^\Phi$ auf $K^* K^{*\Phi}$ ausdehnen und dann $\mathfrak{P}_{\mu^\varrho} = \mathfrak{P}_\mu^\varrho$ zeigen. Denn dann folgt aus $\mu + \nu + \lambda = 0$ zuerst $\mathfrak{P}_\mu \mathfrak{P}_\nu \mathfrak{P}_\lambda \sim$ const., daraus durch Anwendung von ϱ

$$\mathfrak{P}_{\mu^\varrho} \cdot \mathfrak{P}_{\nu^\varrho} \cdot \mathfrak{P}_{\nu^\varrho} \sim \text{const.},$$

und das bedeutet $\mu^\varrho + \nu^\varrho + \lambda^\varrho = 0$. Da

$$x^\Phi \equiv x^\mu,\ y^\Phi \equiv y^\mu \bmod \mathfrak{P}_\mu$$

ist, so wird

$$x^\Phi \equiv x^{\mu^\varrho}, \qquad y^\Phi \equiv y^{\mu^\varrho} \bmod \mathfrak{P}_\mu^\varrho,$$

das heißt aber, da $\mathfrak{P}_{\mu^\varrho}$ durch die Reste von x^Φ und y^Φ bestimmt ist, $\mathfrak{P}_{\mu^\varrho} = \mathfrak{P}_\mu^\varrho$.

Aus

$$(du)^\mu = \mu' du$$

folgt

$$(du)^{\mu^\varrho} = \mu'^\varrho du,$$

die Darstellung $\mu \to \mu'$ transformiert sich also bei ϱ ebenso wie $\mathbf{R}$ selbst.

Nehmen wir jetzt an, daß μ' in $k^{(1)}$ liegt, so gilt

$$(du)^{\mu^\varrho} = \mu' du.$$

Wenn die Charakteristik $p = 0$ ist, so folgt daraus wegen der Treue der Darstellung $\mu = \mu'$ sofort $\mu^\varrho = \mu$, folglich sind die Koeffizienten

von A_i und B_i bei jedem ϱ invariant und müssen daher in $k^{(1)}$ liegen, wie behauptet. Im Falle $p \neq 0$ können wir nicht so einfach schließen. Da wir $\mathfrak{R}$ als kommutativ vorausgesetzt haben, so zerfällt, wie schon erwähnt, p in zwei verschiedene Primideale $\mathfrak{p}_1$ und $\mathfrak{p}_2$ von $\mathfrak{R}$. Der einzige von der Identität verschiedene Automorphismus von $\mathfrak{R}$ vertauscht $\mathfrak{p}_1$ mit $\mathfrak{p}_2$. Wäre nun nicht $\mu^\varrho = \mu$, so würde ein durch $\mathfrak{p}_1$, aber nicht durch $\mathfrak{p}_2$ teilbarer Multiplikator μ auf einen nicht durch $\mathfrak{p}_1$ teilbaren Multiplikator μ^ϱ abgebildet werden, und es wäre einerseits $\mu' = 0$, weil μ in $\mathfrak{p}_1$ liegt, andererseits $\mu' \neq 0$, weil μ^ϱ nicht in $\mathfrak{p}_1$ liegt. Somit ist $\mu = \mu^\varrho$, und wir schließen wie oben, daß μ in $K^{(1)}$ möglich ist.

4. Nicht alle Translationen $\tau_{\mathfrak{o},\mathfrak{q}}$ von K sind schon in $K^{(0)}$ möglich, d. h. führen $K^{(0)}$ in sich über, sondern genau diejenigen, für welche $\mathfrak{q}$ schon Primdivisor von $K^{(0)}$ ist. Folglich ergibt sich der kleinste Konstantenkörper $k^{(1)}$, für den $\tau_{\mathfrak{o},\mathfrak{q}}$ möglich ist, aus $k^{(0)} = P(j)$ durch Adjunktion der Reste modulo $\mathfrak{q}$ der Elemente eines Körpers

$$K^{(0)} = k^{(0)}(x, y) = P(j; x, y),$$

wenn $\mathfrak{o}$ Primdivisor ersten Grades in diesem Körper $K^{(0)}$ ist. Dieser Körper $k^{(1)}$ ist endlich algebraisch über $k^{(0)} = P(j)$, wenn $\mathfrak{q}$ in einem Primdivisor $\mathfrak{q}^*$ von $K^{(0)}$ aufgeht, insbesondere also für die hier allein wichtigen Translationen von endlicher Ordnung. Denn sind $\tau_1, \cdots, \tau_{n_0}$ alle Translationen, deren Ordnung in n aufgeht, so ist $\left(\mathfrak{o}^{\sum_{i=1}^{n_0} \tau_i}\right)^{p^{f\sigma}}$ der durch $\mathfrak{o}$ teilbare Primdivisor von $K^{n\varepsilon}$, der schon Primdivisor in $K^{(0)n\varepsilon}$ ist; dabei ist p^f die in n enthaltene Potenz der Charakteristik p und $n_0 = n^2/p^{\sigma f}$. Zudem folgt weiter, daß $k^{(1)}$ für nicht durch p teilbares n separabel über $P(j)$ ist und für $\sigma = 1$ einen Inseparabilitätsgrad $\leqq p^f$ hat; für $\sigma = 2$ gibt es ja keine Translationen von durch p teilbarer Ordnung.

§ 4. Das Verhalten der Multiplikatoren bei Reduktion nach einem Primdivisor des Konstantenkörpers.

1. Wir setzen jetzt von dem elliptischen Funktionenkörper K nicht mehr voraus, daß sein Konstantenkörper k algebraisch abgeschlossen sei. In k sei durch eine diskrete Exponentenbewertung ein Primdivisor $\mathfrak{p}$ gegeben. $\mathfrak{p}$ werde hinsichtlich eines nichtkonstanten Elementes x auf K übertragen[20]). Wenn wir voraussetzen, daß 1. $\mathfrak{p}$ in K prim bleibt, 2. der Restklassenkörper $\bar{K}$ von K modulo $\mathfrak{p}$ auch elliptisch ist, und

[20]) Vgl. hierfür die in der Math. Zeitschr. erscheinende Arbeit: M. Deuring, Reduktion algebraischer Funktionenkörper nach Primdivisoren des Konstantenkörpers.

3. K den Konstantenkörper k hat, so können wir jedem Divisor $\mathfrak{a}$ von K einen Divisor $\mathfrak{a}$ von K als Restklasse modulo $\mathfrak{p}$ zuordnen, dergestalt, daß alle Relationen zwischen Divisoren, Elementen und Divisorenklassen bei der Reduktion modulo $\mathfrak{p}$ erhalten bleiben[20]).

2. Wir wollen untersuchen, wie sich die Multiplikatoren von K bei der Reduktion nach $\mathfrak{p}$ verhalten und betrachten zu diesem Zwecke wie in § 3 neben K den Doppelkörper KK^{φ}. $\mathfrak{p}$ kann unter Zugrundelegung von x^{φ} in der gleichen Weise von K auf KK^{φ} übertragen werden wie hinsichtlich x von k auf K. Der Restklassenkörper $\overline{K}\,\overline{K^{\varphi}} = \overline{K}\,\overline{K}^{\varphi}$ ist dann die entsprechende Konstantenerweiterung von K/k und $\bar{z} \to z^{\varphi}$ ist eine isomorphe Abbildung von $\overline{K}/\bar{k}$ auf $K^{\varphi}/\bar{k}$. Für KK^{φ} als Funktionenkörper von x^{φ} mit dem Konstantenkörper K sind dann die Voraussetzungen **1. 1. 2. 3.** für die Anwendbarkeit der Reduktionstheorie ebenfalls erfüllt. Es sind daher auch für die Divisoren von KK^{φ}/K die Reste modulo $\mathfrak{p}$ erklärt. Konstante Divisoren gehen modulo $\mathfrak{p}$ in konstante Divisoren über.

Ein Multiplikator μ von K wird durch eine Restklasse der Divisorengruppe von KK^{φ}/K nach der Untergruppe der konstanten Divisoren definiert. Diese Klasse geht modulo $\mathfrak{p}$ in eine entsprechende Restklasse für $\overline{K}\,\overline{K^{\varphi}}/\overline{K}$ über. Auf diese Weise ist dem μ ein Multiplikator $\bar{\mu}$ von $\overline{K}$ eindeutig zugeordnet. Wir können insbesondere μ durch einen für einen festen Primdivisor ersten Grades $\mathfrak{o}$ normierten Meromorphismus μ oder den zugeordneten Primdivisor ersten Grades $\mathfrak{P}_{\mu}$ von KK^{φ}/K darstellen.

Wir zeigen

$\mu \to \bar{\mu}$ ist eine isomorphe Abbildung des Multiplikatorenringes $\mathfrak{R}$ *von K auf einen Teil des Multiplikatorenringes von $\overline{K}$.*

Zuerst beweisen wir, daß $\mu \to \bar{\mu}$ additionstreu ist: $\mu + \nu + \lambda = 0$ bedeutet $\mathfrak{P}_{\mu}\,\mathfrak{P}_{\nu}\,\mathfrak{P}_{\lambda} \sim$ const., daraus folgt $\overline{\mathfrak{P}}_{\mu}\,\overline{\mathfrak{P}}_{\nu}\,\overline{\mathfrak{P}}_{\lambda} \sim$ const. und daraus $\bar{\mu} + \bar{\nu} + \bar{\lambda} = 0$.

Zweitens zeigen wir, daß $\mu \to \bar{\mu}$ umkehrbar eindeutig ist. Es genügt, wegen $\overline{\mu + \nu} = \bar{\mu} + \bar{\nu}$ aus $\mu \neq 0$ auf $\bar{\mu} \neq 0$ zu schließen. $\mu \neq 0$ bedeutet, daß $\mathfrak{P}_{\mu}$ nicht konstant ist. Für jedes z aus K gilt

$$z^{\varphi} \equiv z^{\mu} \bmod \mathfrak{P}_{\mu}$$

und insbesondere

$$x^{\varphi} \equiv x^{\mu} \bmod \mathfrak{P}_{\mu}.$$

Es gibt ein Element z^{μ} von K^{μ}, das modulo $\mathfrak{p}$ nicht konstant ist. Denn die Koeffizienten der irreduziblen Gleichung für x in K^{μ}, die $\mathfrak{p}$-ganz, aber nicht sämtlich durch $\mathfrak{p}$ teilbar seien, können nicht alle modulo $\mathfrak{p}$ konstant sein, weil sonst $\bar{x}$ konstant wäre. Je nachdem x $\mathfrak{p}$-ganz ist

oder nicht, schreiben wir z als Quotienten zweier x-ganzer oder zweier $\frac{1}{x}$-ganzer Elemente s und t, $z = s/t$. Wir können annehmen, daß $\overline{t} \neq 0$ ist. Aus

$$s^{\varphi} \equiv s^{\mu}, \qquad t^{\varphi} \equiv t^{\mu} \bmod \mathfrak{P}_{\mu}$$

folgt[20])

$$\overline{s^{\varphi}} \equiv \overline{s^{\mu}}, \qquad \overline{t^{\varphi}} \equiv \overline{t^{\mu}} \bmod \overline{\mathfrak{P}_{\mu}},$$

also wegen $\overline{t^{\varphi}} \neq 0$

$$\overline{z^{\varphi}} = \overline{s^{\varphi}} / \overline{t^{\varphi}} \equiv \overline{s^{\mu}} / \overline{t^{\mu}} = \overline{z^{\mu}} \bmod \overline{\mathfrak{P}_{\mu}}.$$

Da also das K-Element z^{φ} den nichtkonstanten Rest $\overline{z^{\mu}}$ mod $\overline{\mathfrak{P}_{\mu}}$ hat, so ist $\overline{\mathfrak{P}_{\mu}}$ nicht konstant, wie behauptet.

Wir beweisen weiter die folgende *Regel über die Vertauschung der Restklassenbildung mod* $\mathfrak{p}$ *mit dem Meromorphismus* μ:

$$\overline{z}^{\overline{\mu}} = \overline{z^{\mu}} \tag{12}$$

für jedes $\mathfrak{p}$*-ganze* z. *Sie gilt dann auch für Divisoren*

$$\overline{\mathfrak{a}}^{\overline{\mu}} = \overline{\mathfrak{a}^{\mu}} \tag{13}$$

und für ganz K

$$\overline{K}^{\overline{\mu}} = \overline{K^{\mu}}. \tag{14}$$

Es genügt, (12) für x-ganze z zu beweisen, weil jedes z Quotient zweier x-ganzer Elemente ist. Zunächst zeigen wir, daß x^{μ} $\mathfrak{p}$-ganz und $\overline{x^{\mu}}$ nicht konstant ist. Anderenfalls wäre nämlich wegen $1/x^{\varphi} \equiv 0 \bmod \overline{\mathfrak{P}_{\mu}}$ oder $\overline{x^{\varphi}} \equiv \overline{x^{\mu}} \bmod \overline{\mathfrak{P}_{\mu}}$ der Divisor $\overline{\mathfrak{P}_{\mu}}$ konstant. Für jedes x-ganze z folgt jetzt aus der Kongruenz $z^{\varphi} \equiv z^{\mu} \bmod \mathfrak{P}_{\mu}$ die Kongruenz $\overline{z^{\varphi}} \equiv \overline{z^{\mu}} \bmod \overline{\mathfrak{P}_{\mu}}$ und daher $\overline{z}^{\overline{\mu}} = \overline{z^{\mu}}$.

Da sich die Normierung von μ durch $\mathfrak{o} \mid \mathfrak{o}^{\mu}$ ausdrückt, so ist $\overline{\mathfrak{o}} \mid \overline{\mathfrak{o}^{\mu}}$ oder $\overline{\mathfrak{o}} \mid \overline{\mathfrak{o}}^{\overline{\mu}}$, d. h. $\overline{\mu}$ ist für $\overline{\mathfrak{o}}$ normiert.

Wir zeigen jetzt schließlich, daß $\mu \to \overline{\mu}$ multiplikationstreu ist, d. h. $\overline{\mu\nu} = \overline{\mu}\,\overline{\nu}$. Wenn μ oder ν gleich 0 ist, so ist $\overline{\mu\nu} = 0$, und $\overline{\mu}\,\overline{\nu} = 0$. Ist $\mu \neq 0$ und $\nu \neq 0$, so gilt für jedes $\mathfrak{p}$-ganze z aus K

$$\overline{z}^{\overline{\mu}\,\overline{\nu}} = (\overline{z}^{\overline{\mu}})^{\overline{\nu}} = \overline{(z^{\mu})}^{\overline{\nu}} = \overline{(z^{\mu})^{\nu}} = \overline{z^{\mu\nu}} = \overline{z}^{\overline{\mu\nu}},$$

das bedeutet aber $\overline{\mu}\,\overline{\nu} = \overline{\mu\nu}$, wie behauptet.

3. Wenn K und in seinem Konstantenkörper k der Primdivisor $\mathfrak{p}$ gegeben ist, so hängt der Typus des Restklassenkörpers $\bar{K}$ noch davon ab, welches x wir der Ausdehnung von $\mathfrak{p}$ auf K zugrunde legen; wir werden versuchen, x so zu wählen, daß die Bedingungen 1. 2. 3. in **1.** erfüllt sind. Darüber gilt der folgende Satz:

x kann, unter der Voraussetzung, daß j $\mathfrak{p}$-ganz ist, so gewählt werden, daß $\mathfrak{p}$ in K prim bleibt und $\bar{K}$ elliptisch mit dem Konstantenkörper $\bar{k}$ wird. Die Invariante von $\bar{K}$ ist der $\mathfrak{p}$-Rest $\bar{j}$ von j. Um ein passendes x zu erlangen, ist unter Umständen k endlich algebraisch zu erweitern und dann $\mathfrak{p}$ durch einen seiner Primteiler in der Erweiterung zu ersetzen.

Beweis. Da eine endliche algebraische Erweiterung von k zugelassen sein soll, so können wir eine definierende Gleichung von K in der Normalform

$$y^2 = x(x-1)(x-\lambda) \quad \text{oder} \quad y^2 - y + \alpha xy = x^3$$

zugrunde legen, je nachdem die Charakteristik p von K von 2 oder von 3 verschieden ist[21]). Dabei ist

$$2^8(1-\lambda(1-\lambda))^3 = j\lambda^2(1-\lambda)^2 \quad \text{und } \lambda \neq 0, 1, \qquad (\alpha^3+24)^3 + j(\alpha^3+27) = 0 \quad \text{und } \alpha^3+27 \neq 0.$$

Aus der Voraussetzung, daß j $\mathfrak{p}$-ganz ist, folgt, daß λ $\mathfrak{p}$-ganz und $\bar{\lambda} \neq 0, 1$ oder α $\mathfrak{p}$-ganz und $\bar{\alpha}^3 + 27 \neq 0$ ist. Mithin ist, wenn x der Ausdehnung von $\mathfrak{p}$ auf K zugrunde gelegt wird,

$$\bar{y}^2 = \bar{x}(\bar{x}-1)(\bar{x}-\bar{\lambda}) \quad \text{oder} \quad \bar{y}^2 - \bar{y} + \bar{\alpha}\bar{x}\bar{y} = \bar{x}^3$$

irreduzibel und definiert einen elliptischen Körper $\bar{K}$ mit dem Konstantenkörper $\bar{k}$.

Von dem eben bewiesenen Satz gilt die folgende Umkehrung:

Wenn x in K so gewählt werden kann, daß $\mathfrak{p}$ in K prim bleibt und $\bar{K}$ elliptisch mit dem Konstantenkörper $\bar{k}$ wird, so ist j $\mathfrak{p}$-ganz und $\bar{K}$ hat die Invariante $\bar{j}$.

Beweis. Wir legen wieder eine definierende Gleichung von $\bar{K}$ in der Gestalt

$$\bar{y}^2 = \bar{x}(\bar{x}-1)(\bar{x}-\bar{\lambda}) \quad \text{oder} \quad \bar{y}^2 - \bar{y} + \bar{\alpha}\bar{x}\bar{y} = \bar{x}^3$$

---

[21]) Loc. cit. [18]).

zugrunde, da es auf eine endliche Konstantenerweiterung nicht ankommt. Der Nenner von $\bar{x}$ ist ein Primdivisorquadrat $\bar{\mathfrak{o}}^2$. Wir können annehmen, daß $\bar{\mathfrak{o}}$ der $\mathfrak{p}$-Rest eines Primdivisors $\mathfrak{o}$ von K ist, jedenfalls nach einer passenden endlichen algebraischen Konstantenerweiterung. $\mathfrak{q}$ sei ein Primdivisor ersten Grades von K, der modulo $\mathfrak{p}$ nicht in $\bar{\mathfrak{o}}$ übergeht, und x_1 ein Multiplum von $\mathfrak{q}\mathfrak{o}^{-2}$. x_1 kann zu $\mathfrak{p}$ prim angenommen werden. Dann ist $\bar{x}_1$ ein nichtkonstantes Multiplum von $\bar{\mathfrak{o}}^{-2}$, also $\bar{x}_1 = \bar{\varepsilon}\,\bar{x} + \bar{\delta}$ mit konstanten $\bar{\varepsilon}$, $\bar{\delta}$ und daher dürfen wir gleich $\bar{x}_1 = \bar{x}$ annehmen. In der gleichen Weise finden wir ein Element y_1 von K mit dem Nenner $\bar{\mathfrak{o}}^3$, das modulo $\mathfrak{p}$ in $\bar{y}$ übergeht. x_1 und y_1 erzeugen den Körper K und zwischen ihnen besteht eine Gleichung

$$(15) \qquad g y_1^2 + h y_1 + a x_1 y_1 = c_0 x_1^3 + c_1 x_1^2 + c_2 x_1 + c_3 = c_0 \varphi(x_1),$$

die wir gleich als $\mathfrak{p}$-primitiv annehmen können. Da sie modulo $\mathfrak{p}$ in die Gleichung zwischen x und y übergehen muß, so ist im ersten Falle

$$h \equiv a \equiv 0, \qquad g \equiv c_0 \not\equiv 0 \bmod \mathfrak{p}$$

und

$$\overline{\varphi(x_1)} = \bar{x}\,(\bar{x} - 1)\,(x - \bar{\lambda}).$$

$\varphi(x_1)$ hat daher drei Wurzeln $\xi_1\, \xi_2,\, \xi_3$ mit

$$\bar{\xi}_1 = 0, \quad \bar{\xi}_2 = 1 \quad \text{und} \quad \bar{\xi}_3 = \bar{\lambda}.$$

Setzen wir dann

$$\frac{x_1 - \xi_1}{\xi_2 - \xi_1} = x, \qquad \frac{\xi_3 - \xi_1}{\xi_2 - \xi_1} = \lambda, \qquad \left(y_1 + \frac{a x_1 + h}{2}\right)(\xi_2 - \xi_1)^{-\frac{3}{2}} = y$$

so wird

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

und x, y, λ gehen modulo $\mathfrak{p}$ in $x, \bar{y}, \bar{\lambda}$ über, woraus die Behauptung des Satzes unmittelbar folgt.

Im zweiten Falle ist

$$g \equiv -h \equiv c_0 \not\equiv 0 \bmod \mathfrak{p}$$

und

$$\overline{\varphi(x_1)} = \bar{x}^3.$$

Wir setzen eine lineare Transformation

$$(16) \qquad x_1 = Ax + B, \qquad y_1 = Fy + Cx + D$$

an, die

$$g y_1^2 + h y_1 + a x_1 y_1 = c_0 x_1^3 + c_1 x^2 + c_2 x + c_3 \tag{17}$$

auf die Normalform

$$y^2 - y + \alpha x y = x^3 \tag{18}$$

bringen soll. Vorerst nehmen wir an, daß die Charakteristik von K nicht 2 ist, dann können wir (17) in der Gestalt

$$\begin{aligned}&(g y_1 + \tfrac{1}{2}(a x_1 + h))^2 \\ &\quad = g c_0 x_1^3 + \left(g c_1 + \frac{a^2}{4}\right) x_1^2 + (g c_2 + \tfrac{1}{2} a h) x_1 + \left(g c_3 + \frac{h^2}{4}\right)\end{aligned} \tag{19}$$

und (18) in der Gestalt

$$(y + \tfrac{1}{2}(\alpha x - 1))^2 = x^3 + \frac{\alpha^2}{4} x^2 - \frac{\alpha}{2} x + \tfrac{1}{4} \tag{20}$$

schreiben. Das kubische Polynom rechts in (19) muß durch (16) bis auf den Faktor $g c_0 A^3$ in das kubische Polynom rechts in (20) transformiert werden. Das ergibt die folgenden beiden Gleichungen

$$\begin{aligned}g c_0 A^3 &= 4 g c_0 B^3 + (4 g c_1 + a^2) B^2 + (4 g c_2 + 2 a h) B + (4 g c_3 + h^2) \\ &= 4 g (c_0 B^3 + c_1 B^2 + c_2 B + c_3) + (a B + h)^2,\end{aligned} \tag{21}$$

$$\begin{aligned}&(6 g c_0 B^2 + (4 g c_1 + a^2) B + (2 g c_2 + a h))^2 \\ &\quad = g c_0 A^3 (12 B + (4 g c_1 + a^2));\end{aligned} \tag{22}$$

ferner den Ausdruck

$$\alpha = -\frac{6 g c_0 B^2 + (4 g c_1 + a^2) B + (2 g c_2 + a h)}{g c_0 A^2} \tag{23}$$

für α.

Elimination von A aus (21) und (22) ergibt die folgende biquadratische Gleichung für B

$$\begin{aligned}&3 g^2 c_0^2 B^4 + g c_0 (4 g c_1 + a^2) B^3 + 3 g c_0 (2 g c_2 + a h) B^2 \\ &\quad + 3 g c_0 (4 g c_3 + h^2) B \\ &\quad + (4 g c_1 c_3 + g c_3 a^2 + g c_1 h^2 - g c_2^2 - g h c_2 a) = 0.\end{aligned} \tag{24}$$

Alle Koeffizienten dieser Gleichung sind $\mathfrak{p}$-ganz, der letzte ist durch $\mathfrak{p}$ teilbar, aber der erste nicht, da ja die Charakteristik von drei verschieden ist. Mithin hat (24) eine durch $\mathfrak{p}$ teilbare Wurzel B — wir nehmen hier an, daß (24) alle Wurzeln in k hat, das läuft ja nur auf eine ausdrücklich zugelassene endliche algebraische Erweiterung von k

hinaus. Aus (22) ergeben sich dann drei Werte von A, von denen einer, A, kongruent 1 mod $\mathfrak{p}$ ist.

Jetzt setzen wir (16) unmittelbar in (17) ein und vergleichen die Koeffizienten mit denen von (18). Das konstante Glied ergibt

$$g D^2 + (aB + h) D = c_0 B^3 + c_1 B^2 + c_2 B + c_3, \tag{25}$$

diese Gleichung hat eine durch $\mathfrak{p}$ teilbare Wurzel D. Der Koeffizient von x ergibt

$$(aB + h + 2gD) C = 3 c_0 A B^2 + 2 c_1 A B + c_2 A.$$

Der Faktor von C links ist modulo $\mathfrak{p}$ zu h kongruent, er ist daher nicht durch $\mathfrak{p}$ teilbar und um so mehr von 0 verschieden. Daher wird

$$C = A \frac{3 c_0 B^2 + 2 c_1 B + c_2}{aB + h + 2gD}, \tag{26}$$

dies C ist ersichtlich durch $\mathfrak{p}$ teilbar. Schließlich vergleichen wir den Koeffizienten von y mit dem von x^3

$$2 g F D + h F + a B F = - c_0 A^3$$

oder

$$F = - \frac{c_0 A^3}{aB + h + 2gD}, \tag{27}$$

wegen $h + 2gD \equiv h \not\equiv 0 \bmod \mathfrak{p}$ ist $h + 2gD \neq 0$.

Es wird $F \equiv 1 \bmod \mathfrak{p}$. Aus (23) folgt weiter, daß der $\mathfrak{p}$-Rest von α gleich dem von a, also gleich dem gegebenen $\bar{\alpha}$ ist. Damit ist eine modulo $\mathfrak{p}$ zur Identität kongruente Transformation von (17) in die Normalform (18) gefunden. Sie bleibt auch für die Charakteristik 2 gültig, denn die Berechnung von B, A, D, C, F der Reihe nach aus (24), (22), (25), (26) und (27) geht auch für die Charakteristik 2, weil keiner der auftretenden Nenner für $2 = 0$ verschwindet.

Damit ist der behauptete Satz bewiesen, aber darüber hinaus die folgende Verschärfung:

Wenn die Ausdehnung von $\mathfrak{p}$ auf K so gewählt werden kann, daß $\mathfrak{p}$ in K prim bleibt und K elliptisch mit dem Konstantenkörper k ist, und wenn

$$\bar{y}^2 = \bar{x} (\bar{x} - 1) (\bar{x} - \bar{\lambda}) \quad \text{oder} \quad \bar{y}^2 - \bar{y} + \bar{\alpha} \bar{x} \bar{y} = \bar{x}^3$$

eine definierende Gleichung von $\bar{K}$ ist, so gibt es ein erzeugendes Elementpaar x, y von K, das modulo $\mathfrak{p}$ in $\bar{x}, \bar{y}$ übergeht, und das eine Gleichung

$$y^2(x-1)(x-\lambda) \qquad \text{oder} \qquad y^2 - y + \alpha xy = x^3$$

erfüllt. Dann ist auch $\bar{\lambda}$ *der* $\mathfrak{p}$*-Rest von* λ *oder* $\bar{\alpha}$ *der von* α*. Unter Umständen ist eine endliche algebraische Erweiterung von* k *nötig.*

4. Wir wollen jetzt untersuchen, wie sich die elliptischen Teilkörper von K modulo $\mathfrak{p}$ verhalten. $\mathfrak{G}$ sei eine endliche Automorphismengruppe von K/k, K^* ihr Invariantenkörper und $\mathfrak{p}^*$ der durch $\mathfrak{p}$ teilbare Primdivisor von K^*. Die Galoisgruppe von K/K^* ist die Faktorgruppe $\bar{\mathfrak{G}} = \mathfrak{Z}/\mathfrak{T}$ der Zerlegungsgruppe $\mathfrak{Z}$ nach der Trägheitsgruppe $\mathfrak{T}$ von $\mathfrak{p}$ hinsichtlich K^*. Dies wenden wir zunächst in dem Fall an, daß $\mathfrak{G}$ von einer Spiegelung $\sigma_{0,q}$ erzeugt wird. Da K^* vom Geschlechte 0 ist, so kann nicht $\overline{K^*} = \bar{K}$ sein, folglich ist $\mathfrak{Z} = \mathfrak{G}$ und $\mathfrak{T} = 1$, $\mathfrak{p}^* = \mathfrak{p}$ und $\sigma_{0,q}$ führt $\mathfrak{p}$-ganze Elemente in $\mathfrak{p}$-ganze über. $\sigma_{0,q}$ induziert in $\bar{K}$ die Spiegelung $\sigma_{\bar{0},\bar{q}}$, wir wollen daher sagen, *daß* $\sigma_{0,q}$ mod $\mathfrak{p}$ *in* $\sigma_{\bar{0},\bar{q}}$ *übergehe.*

Hieraus folgt weiter, daß die Translation $\tau_{0,q}$ von K modulo $\mathfrak{p}$ in die Translation $\tau_{\bar{0},\bar{q}}$ von $\bar{K}$ übergeht. Allerdings ist diese Abbildung der Translationsgruppe von K in die von $\bar{K}$ nicht notwendig treu, vielmehr gehen alle $\tau_{0,q}$ mit dem gleichen $\bar{q}$ in ein und dieselbe Translation $\tau_{\bar{0},\bar{q}}$ über. Da für uns nur die Translationen endlicher Ordnung wichtig sind, so wollen wir untersuchen, ob und welche von ihnen in die Identität übergehen können.

Zuerst betrachten wir die Gruppe aller Translationen, deren Ordnungen in einer nicht durch die Charakteristik p teilbaren natürlichen Zahl n aufgehen. Sie bilden bei hinreichend großem Konstantenkörper eine Gruppe $\mathfrak{G}$ vom Typus (n, n) mit dem Invariantenkörper $K^* = K^{n\varepsilon}$. Nach § 3 **2.** (14) geht $K^{n\varepsilon}$ modulo $\mathfrak{p}$ in $\bar{K}^{n\varepsilon}$ über. Es wird also wieder $\mathfrak{Z} = \mathfrak{G}$ (was auch daraus folgt, daß alle Translationen $\mathfrak{p}$-ganze Größen in $\mathfrak{p}$-ganze überführen), und $\mathfrak{T} = 1$ und alle n^2 Translationen $\tau_{0,q}$ mit $n[q] = 0$ gehen in ebenso viel verschiedene Translatiouen $\tau_{\bar{0},\bar{q}}$ von $\bar{K}$ mit $n[\bar{q}] = 0$ über, anders ausgedrückt, die Gruppe der Klassen von in n aufgehenden Ordnungen von K wird isomorph auf die entsprechende Gruppe von $\bar{K}$ abgebildet. Wir können das schließlich auch so fassen

Wenn die Primzahl q *von der Charakteristik von* $\bar{K}$ *verschieden ist, so geht die Gruppe* $\mathfrak{C}_q$ *aller Klassen von* K*, deren Ordnungen Potenzen von* q *sind, modulo* $\mathfrak{p}$ *isomorph in die entsprechende Gruppe* $\bar{\mathfrak{C}}_q$ *von* $\bar{K}$ *über.*

Weiter betrachten wir in dem Fall, daß K und $\bar{K}$ die gleiche Primzahlcharakteristik p haben, die Gruppe $\mathfrak{C}_p$ von K. Die $p^{f(2-\sigma(K))}$ Translationen mit in p^f aufgehender Ordnung von K lassen $K^{p^f\varepsilon}$ invariant,

aber außerdem hat K den Inseparabilitätsgrad $p^{\sigma f}$ über $K^{p^{f\varepsilon}}$. Da $K^{p^{f\varepsilon}}$ modulo $\mathfrak{p}$ in $\bar{K}^{p^{f\varepsilon}}$ übergeht, so haben wir

Ist $\sigma(\bar{K}) = \sigma(K)$, *so wird* $\mathfrak{C}_p$ *isomorph auf* $\bar{\mathfrak{C}}_p$ *abgebildet, dagegen geht für* $\sigma(K) = 1$ *und* $\sigma(\bar{K}) = 2$ *die von* 1 *verschiedene Gruppe* $\mathfrak{C}_p$ *in* $\bar{\mathfrak{C}}_p = 1$ *über.*

Schließlich gilt im Falle $Ch \cdot (K) = 0$, $Ch \cdot (\bar{K}) = p \neq 0$:

Für $\sigma(\bar{K}) = 2$ *geht ganz* $\mathfrak{C}_p$ *in* 1 *über, für* $\sigma(\bar{K}) = 1$ *nur eine Untergruppe, die zur additiven Gruppe aller Restklassen mod* 1 *von rationalen Zahlen mit Potenzen von* p *als Nennern isomorph ist.*

Aus dem Verhalten der Gruppen $\mathfrak{C}_q$ kann leicht abgeleitet werden, wie sich die elliptischen Teilkörper von K modulo $\mathfrak{p}$ verhalten. In jedem Fall ist $(\bar{K} : \bar{K}_0) = (K : K_0)$, weil das für die Teilkörper K^{n^ε} gilt. Die galoissche Gruppe von K/K_0 geht in die von $\bar{K}/\bar{K}_0$ über und $\bar{K}_0$ ist elliptisch. Der Inseparabilitätsgrad erhöht sich entsprechend der Verkleinerung der Gruppe. Wir betrachten weiter nur solche K_0, über denen K zyklisch ist, das genügt, weil für die größte natürliche Zahl m, für die K_0 in K^{m^ε} enthalten ist, der zu K isomorphe Körper K^{m^ε} zyklisch über K_0 ist.

Wenn n nicht durch die Charakteristik von K teilbar ist, so gibt es

$$\mu(n) = n \prod_{q/n} (1 + q^{-1}) \tag{28}$$

Körper K_0, über denen K zyklisch vom Grade n ist, sie gehen in ebensoviel verschiedene Körper $\bar{K}_0$ über, über denen $\bar{K}$ zyklisch vom Grade n ist.

Ähnlich ist es im Falle $Ch \cdot (K) = Ch \cdot (\bar{K}) = p \neq 0$, $\sigma(K) = \sigma(\bar{K}) = 1$ für $n = p^f$ (und daher für alle n). Es gibt dann genau einen Teilkörper K_0 von K, über dem K eine zyklische Gruppe der Ordnung p^{f_1} und den Inseparabilitätsgrad p^{f-f_1} hat, $0 \leqq f_1 \leqq f$, dieser Körper geht modulo $\mathfrak{p}$ in den entsprechenden Teilkörper von $\bar{K}$ über. Für $\sigma(K) = \sigma(\bar{K}) = 2$ gibt es an Körpern K_0 mit $(K : K_0) = p^f$ nur die Potenz K^{p^f}, die modulo $\mathfrak{p}$ in $\bar{K}^{p^f}$ übergeht. Ist dagegen $\sigma(K) = 1$ und $\sigma(\bar{K}) = 2$, so gehen die $f+1$ Körper K_0, über denen K den Grad p^f hat, alle in den einen Körper K^{p^f} über.

Es bleibt der Fall $Ch \cdot (K) = 0$, $Ch \cdot (\bar{K}) = p \neq 0$ zu untersuchen. Wenn $\sigma(\bar{K}) = 2$ ist, so gehen sämtliche Körper K_0 mit $(K : K_0) = p^f$ (nicht nur die, über denen K zyklisch ist) in den einen Körper $\bar{K}_0 = \bar{K}^{p^f}$ über.

Wenn $\sigma(\bar{K}) = 1$ ist, so gehen von den $p^f + p^{f-1}$ Teilkörpern, über denen K zyklisch vom Grade p^f ist, p^f in den Körper $\bar{K}_0$ über, über dem $\bar{K}$ zyklisch vom Grade p^f ist, einer in $\bar{K}^{p^f}$ und von den übrigen je $p^{f-i} - p^{f-i-1}$ in den Körper $\bar{K}_i$, über dem K zyklisch vom Grade p^{f-i} und inseparabel vom Grade p^i ist, $i = 1, 2, \cdots, f-1$.

Es sei nämlich τ_1, τ_2 eine Basis der Gruppe aller Translationen von K mit in p^f aufgehender Ordnung und dabei gehe τ_2 mod $\mathfrak{p}$ in 1 über. Dann gehen die p^f Invariantenkörper der Translationen $\tau_1 \tau_2^h$, $h = 1, \cdots, p^f$ in $\bar{K}_0$ über, die Invariantenkörper der $p^{f-i} - p^{f-i-1}$ Translationen $\tau_1^{p^i} \tau_2^h$, $h \bmod p^{f-i}$, $(h, p) = 1$, in $\bar{K}_i$ und der Invariantenkörper von τ_2 in $\bar{K}^{p^f}$. *Aber in diesem Falle gehen auch noch andere Teilkörper von K in $\bar{K}_i$ über, nämlich die Invariantenkörper derjenigen nicht zyklischen Translationsgruppen p^f-ter Ordnung, die* mod. $\mathfrak{p}$ *in die von $\tau_1^{p^i}$ erzeugte zyklische Gruppe übergehen.*

§ 5. Die Automorphismen der einparametrigen Normalformen und die Einheiten des Multiplikatorenrings.

1. K sei ein elliptischer Körper mit der Invariante j. Für einen algebraisch abgeschlossenen Konstantenkörper k können wir ihn durch die Gleichung

$$y^2 = x(x-1)(x-\lambda). \tag{29}$$

erzeugen, wenn die Charakteristik $p \neq 2$ ist, und durch

$$y^2 - y + \alpha x y = x^3, \tag{30}$$

wenn $p \neq 3$ ist. Dabei ist

$$2^8 (1 - \lambda(1-\lambda))^3 = j \lambda^2 (1-\lambda)^2, \tag{31}$$

$$\alpha^3(\alpha^3 + 24)^3 + j(\alpha^3 + 27) = 0. \tag{32}$$

Der Nennerprimdivisor $\mathfrak{o}$ von x und y kann dabei beliebig vorgeschrieben werden.

2. Wir betrachten zuerst den Fall $p \neq 2$. Die sechs Wurzeln von (33) seien $\lambda_1, \cdots, \lambda_6$. Zu jedem λ_ν muß es eine erzeugende Gleichung

$$y_\nu^2 = x_\nu(x_\nu - 1)(x_\nu - \lambda)$$

von K geben, die zu dem gleichen Primdivisor $\mathfrak{o}$ gehört wie (29). x_ν ist eine Linearkombination der beiden linear unabhängigen Multipla 1,

x von $\mathfrak{o}^{-2}$ und y_ν muß ein konstantes Vielfaches von y sein

$$(34) \qquad \begin{aligned} x &= a_\nu x_\nu + b_\nu \\ y &= c_\nu y_\nu \end{aligned} \quad ; \; a_\nu, b_\nu, c_\nu \text{ aus } k.$$

Es gilt dann

$$\begin{aligned} y^2 = c_\nu^2 y_\nu^2 &= x(x-1)(x-\lambda) \\ &= (a_\nu x_\nu + b_\nu)(a_\nu x_\nu + b_\nu - 1)(a_\nu x_\nu + b_\nu - \lambda_\nu) \\ &= a_\nu^3 (x_\nu + b_\nu/a_\nu)(x + (b_\nu - 1)/a_\nu)(x + (b_\nu - \lambda_\nu)/a_\nu) \\ &= c_\nu^2 x_\nu (x_\nu - 1)(x_\nu - \lambda_\nu), \end{aligned}$$

und daraus folgt zunächst

$$c_\nu^2 = a_\nu^3$$

und weiter die folgenden sechs Möglichkeiten für $a_\nu, b_\nu, \lambda_\nu, x_\nu$

$$\begin{aligned} a_1 &= 1, & b_1 &= 0, & \lambda_1 &= \lambda, & x_1 &= x, \\ a_2 &= \lambda, & b_2 &= 0, & \lambda_2 &= \frac{1}{\lambda}, & x_2 &= \frac{x}{\lambda}, \\ a_3 &= -1, & b_3 &= 1, & \lambda_3 &= 1-\lambda, & x_3 &= 1-x, \\ a_4 &= \lambda - 1, & b_4 &= 1, & \lambda_4 &= \frac{1}{1-\lambda}, & x_4 &= \frac{1-x}{1-\lambda}, \\ a_5 &= -\lambda, & b_5 &= \lambda, & \lambda_5 &= 1-\frac{1}{\lambda}, & x_5 &= \frac{\lambda - x}{\lambda}, \\ a_6 &= 1-\lambda, & b_6 &= \lambda, & \lambda_6 &= \frac{\lambda}{\lambda - 1}, & x_6 &= \frac{\lambda - x}{\lambda - 1}. \end{aligned}$$

Zu jedem dieser Wertsysteme gehören zwei Wertpaare von c_ν und y_ν

$$\begin{aligned} c_1 &= \pm 1, & y_1 &= \pm y, \\ c_2 &= \pm (\sqrt{\lambda})^3, & y_2 &= \pm (\sqrt{\lambda})^{-3} y, \\ c_3 &= \pm i, & y_3 &= \mp i y, \\ c_4 &= \pm i (\sqrt{1-\lambda})^3, & y_4 &= \mp i (\sqrt{1-\lambda})^{-3} y, \\ c_5 &= \pm i (\sqrt{\lambda})^3, & y_5 &= \mp i (\sqrt{\lambda})^{-3} y, \\ c_6 &= \pm (\sqrt{1-\lambda})^3, & y_6 &= \pm (\sqrt{1-\lambda})^{-3} y. \end{aligned}$$

Es gibt daher im ganzen 12 birationale Transformationen der Normalform (29) in eine andere, wenn verlangt wird, daß $\mathfrak{o}$ fest bleibe. Unter ihnen müssen die als für $\mathfrak{o}$ normierte Meromorphismen gedeuteten Einheiten des Multiplikatorenringes vorkommen, es sind nämlich gerade

die, welche λ in sich überführen. Auf diese Weise erhalten wir für jedes j die Einheitengruppe des Multiplikatorenrings:

Im allgemeinen gibt es nur die beiden Einheiten

$$x \to x, \qquad y \to \pm y,$$

also ± 1.

Damit es mehr Einheiten gebe, müssen zwei λ mit verschiedenen Indizes gleich sein. Das ergibt die folgenden Möglichkeiten:

1. $\lambda = \frac{1}{\lambda}$, $\lambda = -1$, $j = 2^6 3^3$ ($\lambda = 1$ ergäbe $j = \infty$). In diesem Falle ist $\lambda_1 = \lambda_2 = -1$, $\lambda_3 = \lambda_5 = 2$, $\lambda_4 = \lambda_6 = \frac{1}{2}$. Für $p \neq 3$ ergibt das die vier Einheiten

$$x \to x, \quad y \to \pm y; \qquad x \to -x, \quad y \to \mp iy,$$

die eine zyklische Gruppe bilden. Ist aber $p = 3$, so ist $j = 0$, alle sechs Werte λ_ν werden gleich -1 und es gibt daher zwölf Einheiten

$$\begin{aligned} &x \to x, && y \to \pm y,\\ &x \to x - 1, && y \to \pm y,\\ &x \to x + 1, && y \to \pm y,\\ &x \to -x, && y \to \mp iy,\\ &x \to 1 - x, && y \to \mp iy,\\ &x \to -x - 1, && y \to \mp iy. \end{aligned}$$

R ist die (dem Typus nach einzige) Maximalordnung von $Q_{\infty,3}$.

2. $\lambda = 1 - \lambda$, $\lambda = \frac{1}{2}$. Das ergibt wieder $j = 2^6 3^3$.

3. $\lambda = \frac{1}{1-\lambda}$, $\lambda = -\varepsilon$, ε eine primitive dritte Einheitswurzel, $j = 0$. Für $p \neq 3$ wird $\lambda_1 = \lambda_4 = \lambda_5 = -\varepsilon$, $\lambda_2 = \lambda_3 = \lambda_6 = -\varepsilon^2$, und wir haben sechs Einheiten

$$\begin{aligned} &x \to x, && y \to \pm y,\\ &x \to \varepsilon(x - 1), && y \to \pm y,\\ &x \to \varepsilon^2(x + \varepsilon), && y \to \pm y, \end{aligned}$$

die eine zyklische Gruppe bilden. Für $p = 3$ wird wieder $j = 0$.

Im Falle $p \neq 3$, $j = 2^6 3^3$ heißt die definierende Gleichung

$$y^2 = x^3 - x,$$

der Multiplikator $x \to -x$, $y \to iy$, den wir mit ι bezeichnen wollen, bildet mit 1 zusammen eine Basis der Maximalordnung des Gaußschen Zahlkörpers $P(\sqrt{-1})$, die im Multiplikatorenring enthalten ist.

Im Falle $p = 3$, $j = 0$ heißt die definierende Gleichung ebenfalls

$$y^2 = x^3 - x.$$

ι sei wieder der Multiplikator $x \to -x$, $y \to iy$ und η sei der Multiplikator $x \to x+1$, $y \to y$. ι ist eine primitive vierte und η eine primitive dritte Einheitswurzel. Es gilt, wie leicht nachzurechnen, die Vertauschungsregel

$$\iota\eta = \eta^2\iota,$$

wozu noch die additiven Relationen

$$\iota^2+1 = 0, \quad \eta^2+\eta+1 = 0$$

kommen. Alle zwölf Einheiten sind

$$\begin{array}{cccc} 1, & \iota, & -1, & -\iota, \\ \eta, & \eta\iota, & -\eta, & -\eta\iota, \\ \eta^2, & \eta^2\iota, & -\eta^2, & -\eta^2\iota. \end{array}$$

$\pm\iota$, $\pm\eta\iota$, $\pm\eta^2\iota$ haben die Ordnung 4, η, η^2 die Ordnung 3 und $-\eta$, $-\eta^2$ die Ordnung 6. Eine Basis von $\mathfrak{R}$ ist 1, η, ι, $\eta\iota$, denn die Diskriminante Δ dieser vier Größen ist

$$\Delta = \begin{vmatrix} +2 & -1 & 0 & 0 \\ -1 & -1 & 0 & 0 \\ 0 & 0 & -2 & 1 \\ 0 & 0 & 1 & -2 \end{vmatrix} = -9,$$

weil $Spur(\pm 1) = \pm 2$, $Sp(\pm\iota) = Sp(\pm\eta\iota) = Sp(\pm\eta^2\iota) = 0$, $Sp(\eta) = Sp(\eta^2) = -1$ und $Sp(-\eta) = Sp(-\eta^2) = 1$ ist.

Im Fall $p \neq 3$, $j = 0$ formen wir die Normalform $y^2 = x(x-1)(x+\varepsilon)$ durch $x = \dfrac{z-\varepsilon}{1-\varepsilon}$, $y = u(1-\varepsilon)^{-\frac{3}{2}}$ in

$$u^2 = z^3 - 1$$

um. Die sechs Einheiten lauten dann

$$z \to z, \quad u \to \pm u; \qquad z \to \varepsilon^h z, \quad u \to \pm u.$$

Der Multiplikator $z \to \varepsilon z$, $u \to u$ ist eine primitive dritte Einheitswurzel und bildet mit 1 zusammen eine Basis der Maximalordnung des Körpers der dritten Einheitswurzeln, die im Multiplikatorenring enthalten ist.

3. Mit Hilfe der Normalform (30) behandeln wir den Fall $p \neq 3$ in ganz ähnlicher Weise. Zu gegebenem j gibt es zwölf Wurzeln $\alpha_1, \cdots, \alpha_{12}$ von (32) und zu jeder dieser Wurzeln mindestens eine lineare Transformation

$$\begin{aligned} x &= a_\nu x_\nu + b_\nu, \\ y &= f_\nu y_\nu + c_\nu x_\nu + d_\nu, \end{aligned} \tag{35}$$

die (30) in

$$y_\nu^2 - y_\nu + \alpha_\nu x_\nu y_\nu = x_\nu^3$$

überführt. Zur Berechnung dieser Transformationen können wir die in § 4 **3.** behandelte Transformation von $g y_1^2 + h y_1 + a x_1 y_1 = c_0 x_1^3 + c_1 x_1^2 + c_2 x_1 + c_3$ auf die Normalform (30) heranziehen. Zur Berechnung von b erhalten wir aus (24) die Gleichung

$$3 b^4 + \alpha^2 b^3 - 3 \alpha b^2 + 3 b = 0. \tag{36}$$

Diese Gleichung hat eine Wurzel $b = 0$. Aus (22), (23), (25), (26), (27) erhalten wir die zugehörigen Werte von a, f, c, d, α; das gibt sechs Transformationen:

$$a_\nu = \varepsilon^\nu, \quad b_\nu = 0, \quad f_\nu = \begin{cases} +1 \\ -1, \end{cases} \quad c_\nu = \begin{cases} 0 \\ -\varepsilon^\nu \alpha, \end{cases} \quad d_\nu = \begin{cases} 0 \\ 1, \end{cases} \quad \alpha_\nu = \varepsilon^\nu \alpha,$$

ε bedeutet eine primitive dritte Einheitswurzel.

Für die übrigen b haben wir die kubische Gleichung

$$b^3 + \frac{\alpha^2}{3} b^2 - \alpha b + 1 = 0, \tag{37}$$

deren Wurzeln nach der Cardanischen Formel

$$b = -\frac{\alpha^2}{9} - \varepsilon^h \sqrt[3]{\left(\frac{\alpha}{3}\right)^3 + \left(\frac{\alpha}{3}\right)^6} - \varepsilon^{2h} \sqrt[3]{\left(1 + \left(\frac{\alpha}{3}\right)^3\right)^2}, \quad h = 1, 2, 3. \tag{38}$$

sind. (Zunächst nur für $p \neq 2$. Da die Endformel keine Divisionen durch 2 enthält, so gilt sie auch für $p = 2$.)

Ist β eine fest gewählte dritte Wurzel aus $\alpha^3 + 3^3$ — aus (32) ergibt sich im Falle $j \neq 0$ der Ausdruck

$$\beta = -\frac{\alpha(\alpha^3 + 24)}{\sqrt[3]{j}},$$

so können wir

$$b = -\frac{1}{9}(\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h}) \qquad h = 1, 2, 3$$

schreiben. Da zu jedem b drei Werte a gehören, so wollen wir

$$b_4 = b_5 = b_6 = -\frac{1}{9}(\alpha^2 + \alpha\beta + \beta^2),$$

$$b_7 = b_8 = b_9 = -\frac{1}{9}(\alpha^2 + \alpha\beta\varepsilon + \beta^2\varepsilon^2),$$

$$b_{10} = b_{11} = b_{12} = -\frac{1}{9}(\alpha^2 + \alpha\beta\varepsilon^2 + \beta^2\varepsilon)$$

setzen, kurz

$$b_{3h+\mu} = -\frac{1}{9}(\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h}) \qquad h = 1, 2, 3, \quad \mu = 1, 2, 3.$$

Für die zugehörigen a haben wir nach (22)

$$a^3_{3h+\mu} = -\frac{4}{3^6}(\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h})^3 + \frac{1}{3^4}\alpha^2(\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h})^2$$

$$+ \frac{2}{3^2}\alpha(\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h}) + 1.$$

Da nun

$$\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h} = \frac{\alpha^3 - \beta^3}{\alpha - \beta\varepsilon^h} = -\frac{3^3}{\alpha - \beta\varepsilon^h} \tag{39}$$

ist, so wird

$$a^3_{3h+\mu} = (\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h})^2$$

$$\times\left[-\frac{4}{3^6}(\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h}) + \frac{1}{3^4}\alpha^2 - \frac{2}{3^2}\alpha\frac{\alpha - \beta\varepsilon^h}{3} + \frac{1}{3^6}(\alpha - \beta\varepsilon^h)^2\right]$$

$$= -\frac{1}{3^5}\beta^2\varepsilon^{2h}(\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h}).$$

Unter γ_h verstehen wir eine fest gewählte Kubikwurzel aus

$$9\beta\varepsilon^h(\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h});$$

γ_h ist nach (39) von 0 verschieden. Mit dieser Abkürzung können wir

$$a_{3h+\mu} = -\frac{\varepsilon^\mu\gamma_h^2}{27} \tag{40}$$

setzen.

Für d haben wir nach (25) die quadratische Gleichung

$$d^2 + (\alpha b - 1)d = b^3.$$

Wir lösen sie zunächst unter der Annahme, daß $p \neq 2$ ist:

$$2d = 1 - \alpha b \pm \sqrt{(1-\alpha b)^2 + 4b^3}.$$

Für den Radikanden haben wir nach (37)

$$(1-\alpha b)^2 + 4b^3 = 1 - 2\alpha b + \alpha^2 b^2 - \frac{4}{3}\alpha^2 b^2 + 4\alpha b - 4$$

$$= -\frac{1}{3}(\alpha^2 b^2 - 6\alpha b + 9) = -\frac{1}{3}(\alpha b - 3)^2,$$

also ist $2d = 1 - \alpha b \pm \frac{\sqrt{-3}}{3}(\alpha b - 3)$.

Für $\sqrt{-3}$ können wir $2\varepsilon + 1$ einsetzen, damit erhalten wir die folgenden beiden Werte für $d_{3h+\mu}$

$$(41)\quad d_{3h+\mu} = \begin{cases} -\varepsilon + \frac{\varepsilon - 1}{3}\alpha b_{3h+\mu} = -\varepsilon - \frac{\varepsilon - 1}{27}\alpha(\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h}), \\ -\varepsilon^2 + \frac{\varepsilon^2 - 1}{3}\alpha b_{3h+\mu} = -\varepsilon^2 - \frac{\varepsilon^2 - 1}{27}\alpha(\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h}), \end{cases}$$

die auch für $p = 2$ gelten, weil keine Nenner auftreten, die für $2 = 0$ verschwinden.

(26) ergibt

$$(42)\quad c_{3h+\mu} = \begin{cases} \frac{\varepsilon^{\mu-h}}{27(2\varepsilon+1)} \frac{\gamma_h^2}{\beta}(\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h}), \\ \frac{\varepsilon^{\mu-h}}{27(2\varepsilon^2+1)} \frac{\gamma_h}{\beta}(\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h}). \end{cases}$$

(27) gibt f

$$(43)\quad f_{3h+\mu} = \begin{cases} -\frac{\varepsilon^h}{9(2\varepsilon+1)}\beta(\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h})^2, \\ -\frac{\varepsilon^h}{9(2\varepsilon^2+1)}\beta(\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h})^2 \end{cases}$$

und (23)

$$(44)\quad \alpha_{3h+\mu} = -\frac{3\varepsilon^\mu(\alpha + 2\beta\varepsilon^h)}{\gamma_h}.$$

Die Einheiten des Multiplikatorenrings können mit diesen Formeln ebenso berechnet werden wie oben. Ein neues Ergebnis erhalten wir nur für $p = 2$, worauf wir uns daher beschränken. Die Formeln für α_ν lauten in diesem Fall

$$\alpha_\nu = \varepsilon^\nu \alpha; \qquad \nu = 1, 2, 3;$$

$$\alpha_{3h+\mu} = \varepsilon^\mu \alpha/\gamma_\mu; \qquad h = 1, 2, 3; \qquad \mu = 1, 2, 3.$$

Der einzige Wert von α, für den zwei α_ν mit verschiedenen Indizes gleich werden, ist $\alpha = 0$ (aus der zweiten Formel ergibt sich noch die Lösung $\gamma_\mu = \varepsilon^\mu$, was aber auf $j = \infty$ führt). Eine von ± 1 verschiedene Einheitengruppe gibt es für $p = 2$ also nur im Falle $j = 0$, da dann alle α_ν gleich 0 werden, so gibt es dann 24 Einheiten und $\mathfrak{R}$ muß die Quaternionenmaximalordnung sein. Die 24 Einheiten ergeben sich zu

$$x \to \varepsilon^h x, \quad y \to y + \begin{cases} 0 \\ 1 \end{cases}, \quad h \bmod 3,$$

$$x \to \varepsilon^s x + \varepsilon^t, \quad y \to y + \varepsilon^{s-t} x + \begin{cases} \varepsilon \\ \varepsilon^2 \end{cases}; \quad s, t \bmod 3.$$

Die ersten sechs Einheiten bilden eine zyklische Gruppe, die von dem Multiplikator $x \to \varepsilon x$, $y \to 1 + y$ erzeugt wird, den wir mit $-\eta$ bezeichnen wollen. η ist also eine primitive dritte Einheitswurzel.

$$\begin{aligned} \iota_1&: \quad x \to x + 1, \quad y \to y + \quad x + \varepsilon, \\ \iota_2&: \quad x \to x + \varepsilon, \quad y \to y + \varepsilon^2 x + \varepsilon, \\ \iota_3&: \quad x \to x + \varepsilon^2, \quad y \to y + \varepsilon x + \varepsilon \end{aligned}$$

sind Quaternioneneinheiten, denn es gilt

$$\begin{aligned} \iota_1 \iota_2 &= -\iota_2 \iota_1 = \iota_3, \\ \iota_2 \iota_3 &= -\iota_3 \iota_2 = \iota_1, \\ \iota_3 \iota_1 &= -\iota_1 \iota_3 = \iota_2. \end{aligned}$$

Ferner ist

$$\begin{aligned} \eta \iota_1 &= \iota_2 \eta, \\ \eta \iota_2 &= \iota_3 \eta, \\ \eta \iota_3 &= \iota_1 \eta, \end{aligned}$$

η muß sich mit rationalen Koeffizienten a durch die ι ausdrücken

$$\eta = a_0 + a_1 \iota_1 + a_2 \iota_2 + a_3 \iota_3.$$

Aus

$$\begin{aligned} \eta \iota_1 &= a_0 \iota_1 - a_1 \quad - a_2 \iota_3 + a_3 \iota_2, & \iota_2 \eta &= a_0 \iota_2 - a_1 \iota_3 - a_2 \quad + a_3 \iota_1, \\ \eta \iota_2 &= a_0 \iota_2 + a_1 \iota_3 - a_2 \quad - a_3 \iota_1, & \iota_3 \eta &= a_0 \iota_3 + a_1 \iota_2 - a_2 \iota_1 - a_3, \\ \eta \iota_3 &= a_0 \iota_3 - a_1 \iota_2 + a_2 \iota_1 - a_3, & \iota_1 \eta &= a_0 \iota_1 - a_1 \quad + a_2 \iota_3 - a_3 \iota_2 \end{aligned}$$

folgen die Gleichungen

$$\begin{aligned} a_0 &= a_3, & a_1 &= a_2, \\ a_0 &= a_1, & a_2 &= a_3, \\ a_0 &= a_2, & a_3 &= a_1, \end{aligned}$$

mithin sind alle a einander gleich und weil die Spur der dritten Einheitswurzel η gleich -1 ist, so wird

$$\eta = -\tfrac{1}{2}(1+\iota_1+\iota_2+\iota_3).$$

Zusammen mit

$$\iota_1^2 = \iota_2^2 = \iota_3^2 = -1, \qquad \eta^2+\eta+1 = 0$$

sind damit auch alle additiven Relationen zwischen den Einheiten aufgestellt.

§ 6. Invariantengleichungen.

1. *K sei ein elliptischer Funktionenkörper mit der absolut transzendenten Invariante j. Zwischen j und der Invariante j_0 eines elliptischen Teilkörpers K_0 von K besteht eine algebraische Gleichung*

$$\Phi(j, j_0) = 0$$

mit ganzen rationalen Koeffizienten, in der die höchsten Potenzen von j und j_0 die Koeffizienten ± 1 haben.

Beweis. Wir können annehmen, daß der Konstantenkörper k von K die algebraisch abgeschlossene Hülle von $P(j)$ ist, P der Primkörper. Denn ein noch größerer Konstantenkörper kann keine neuen elliptischen Teilkörper mehr hervorbringen. Folglich hängt j_0 algebraisch von $P(j)$ ab, das bedeutet, daß eine in P irreduzible algebraische Gleichung

$$\Phi(j, j_0) = 0$$

mit Koeffizienten aus P besteht, die im Falle der Charakteristik 0 gleich als teilerfremde ganze Zahlen angenommen werden können. Wir zeigen nun, daß Φ als Polynom von j_0 einen konstanten höchsten Koeffizienten hat, oder was auf das gleiche hinauskommt, daß j_0 eine ganze algebraische Funktion von j ist. Dazu schränken wir, was offenbar möglich ist, k auf eine passende endliche algebraische Erweiterung von $P(j)$ ein. Nach § 4 **3.** können wir dann K nach einem nicht im Nenner von j aufgehenden Primdivisor $\mathfrak{p}$ von k zu einem Körper $\bar{K}$ mit der Invariante $\bar{j}$ reduzieren. Nach § 4 **4.** geht dabei K_0 in einen elliptischen Teilkörper $\bar{K}_0$ von $\bar{K}$ über. Folglich muß die Invariante j_0 von K_0 nach § 4 **3.** $\mathfrak{p}$-ganz sein. Da die Sachlage hinsichtlich j und j_0 symmetrisch ist — der Körper $K^{n\varepsilon}$ mit der Invariante j, $(K : K_0) = n$ ist in K_0 enthalten, so hat Φ auch als Polynom von j einen konstanten höchsten Koeffizienten.

In ganz ähnlicher Weise zeigen wir, daß für die Charakteristik 0 die höchsten Koeffizienten von j und j_0 in Φ gleich ± 1 sind. Einen Primdivisor $\mathfrak{p}$ von P (durch eine Primzahl gegeben) dehnen wir hinsichtlich j auf $P(j)$ und k aus. Die gleiche Schlußweise wie eben zeigt, daß j_0 $\mathfrak{p}$-ganz von j abhängen muß, und das ist für alle p nur möglich, wenn der höchste Koeffizient von j_0 gleich ± 1 ist.

2. Wir untersuchen die Polynome $\Phi(t, t_0)$ näher und können dabei annehmen, daß k endlich algebraisch über $P(j)$ ist. Ist m die größte ganze Zahl, für die $K^{m\varepsilon}$ noch K_0 enthält, so ist $K^{m\varepsilon}$ zyklisch über K_0. Da $K^{m\varepsilon}$ zu K isomorph ist, so können wir von vornherein annehmen, daß K über K_0 zyklisch ist.

n sei eine nicht durch die Charakteristik p teilbare Zahl. Die $\mu(n)$ Teilkörper $K_1, \cdots, K_{\mu(n)}$, über denen K zyklisch vom Grade n ist, haben nach § 3 **4.** über $P(j)$ separable Invarianten $j_1, \cdots, j_{\mu(n)}$. Wir zeigen, daß

$$\Phi_n(t, j) = \prod_{h=1}^{\mu(n)} (t - j_h) \tag{45}$$

ein Polynom von t und j mit ganzen rationalen Koeffizienten ist. Dazu betrachten wir ein Paar erzeugender Elemente x, y von K, zwischen denen eine irreduzible Gleichung mit Koeffizienten aus $P(j)$ besteht, und dehnen einen Isomorphismus ϱ von $k/P(j)$ durch die Festsetzung $x^\varrho = x$, $y^\varrho = y$ auf K aus. ϱ führt dann den zu der Translationsgruppe $1, \tau, \cdots, \tau^{n-1}$, gehörigen Körper K in den zu der Gruppe $1, \varrho^{-1}\tau\varrho, \cdots, \varrho^{-1}\tau^{n-1}\varrho$ gehörigen über, vertauscht also die Körper K_h und daher auch die Invarianten $j_{(h)}$ untereinander. Die Koeffizienten von $\Phi_n(t, j)$ als Polynom von t sind daher bei allen Isomorphismen von $k/P(j)$ invariante, separable ganze ganzzahlige algebraische Funktionen von j, also Polynome von j mit ganzen rationalen Koeffizienten, wie behauptet. $\Phi_n(t, j)$ ist ein Produkt von irreduziblen Polynomen der in **1.** betrachteten Art. *Wir nennen*

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

die Invariantengleichung n-ter Ordnung der betreffenden Charakteristik.

Bevor wir auf den Fall $n \equiv 0 \bmod p$ eingehen, bemerken wir:

Ist $\Phi_n(t, j) = 0$ die Invariantengleichung n-ter Ordnung für die Charakteristik 0, so ist dieselbe Gleichung, modulo der Primzahl p betrachtet, die Invariantengleichung n-ter Ordnung für die Charakteristik p, vorausgesetzt, daß p nicht in n aufgeht.

Das ergibt sich unmittelbar daraus, daß K modulo p in einen Körper $\bar{K}$ mit der absolut transzendenten Invariante $\bar{j}$ übergeht, während

dabei die Teilkörper K_h auf die entsprechenden Teilkörper von $\bar{K}$ abgebildet werden.

Wegen dieser Tatsache wollen wir für *alle* n unter der Invariantengleichung n-ter Ordnung für die Primzahlcharakteristik p die modulo p genommene Invariantengleichung n-ter Ordnung der Charakteristik 0 verstehen, obwohl dann unter den Nullstellen von $\Phi_n(t, j)$ außer den Invarianten der Teilkörper, über denen K zyklisch vom Grade n ist, auch die von anderen Teilkörpern vorkommen können.

Die Invariantengleichung p^f-ter Ordnung der Charakteristik p können wir leicht aufstellen. Der Körper über dem K zyklisch vom Grade p^f und separabel ist, hat die Invariante $j^{p^{-f}}$, denn seine p^f-te Potenz ist der zu K isomorphe Körper $K^{p^f e}$. Dagegen hat K^{p^f} die Invariante j^{p^f}. Nach § 4 **4.** wird also die Invariantengleichung p^f-ter Ordnung modulo p

$$(46) \qquad (t-j^{p^{-f}})^{p^f}(t-j^{p^f})\prod_{i=1}^{f-1}(t-j^{p^{2i-f}})^{p^{f-i}-p^{f-i-1}}$$

$$= (t^{p^f}-j)(t-j^{p^f})\prod_{i=1}^{f-1}(t^{p^{f-i-1}}-j^{p^{i-1}})^{p-1} = 0,$$

für $i = 1$ einfach

$$(47) \qquad (t^p-j)(t-j^p) = 0.$$

3. *n' und n'' seien zwei teilerfremde ganze Zahlen. Dann ist*

$$(48) \qquad \Phi_{n'n''}(t, j) = \prod_{h=1}^{\psi(n'')}\Phi_{n'}(t, j_h),$$

wenn

$$\Phi_{n''}(t, j) = \prod_{h=1}^{\psi(n'')}(t-j_h)$$

gilt.

Beweis. K_h sei der Körper der Invariante j_h über dem K zyklisch vom Grade n'' ist. In ihm sind $\psi(n')$ Körper K_{hl} enthalten, über denen K_h zyklisch vom Grade n'' ist. Sind j_{hl} die zugehörigen Invarianten, so gilt

$$\Phi(t, j_h) = \prod_{l=1}^{\psi(n')}(t-j_{hl}).$$

Über allen Körpern K_{hl} ist K zyklisch vom Grade $n'n''$ und weitere Körper mit dieser Eigenschaft gibt es nicht. Somit ist

$$\Phi_{n'n''}(t, j) = \prod_{h,l}(t-j_{hl}) = \prod_{h}\Phi_{n'}(t, j_h):$$

In ähnlicher Weise ergibt sich

$$(49)\qquad \Phi^{p^f}(t,j) = \prod_{h=1}^{p^{f+1}} \frac{\Phi^{p^{f-1}}(t,j_h)}{t-j}, \qquad \Phi_p(t,j) = \prod_{h=1}^{p+1}(t-j_h),$$

es ist nur zu beachten, daß aus $\Phi_{p^{f-1}}(t,j_h)$ einmal der Faktor $t-j$ wegzulassen ist für den in K^{p^ε} enthaltenen Körper, über dem K_h zyklisch vom Grade p^{f-1} ist.

Die Berechnung der Polynome $\Phi_n(t,j)$ ist auf die Berechnung der Polynome $\Phi_p(t,j)$, p Primzahl zurückgeführt.

Für $n \not\equiv 0 \bmod p$ hat $\Phi_n(t,j) = 0$ lauter verschiedene Wurzeln j_h.

Es genügt, dies für eine Primzahlcharakteristik p zu beweisen, weil ein mehrfacher Linearfaktor von $\Phi_n(t,j)$ bei der Reduktion modulo p erhalten bleibt. Gesetzt, etwa j_1 und j_2 wären gleich. Dann enthielte der Teilkörper K_1 mit der Invariante j_1 die beiden Teilkörper $K^{n\varepsilon}$ und $K_2^{n\varepsilon}$, die beide ebenfalls die Invariante $j_1 = j_2$ hätten und daher zu zwei nicht nur um das Vorzeichen unterschiedene Multiplikatoren gleicher Norm von K_1 Anlaß gäben. Nach § 3 **3.** wäre also j_1 und daher um so mehr die Invariante j des Teilkörpers $K^{n\varepsilon}$ von K_1 absolut algebraisch, gegen die Voraussetzung.

$$(50)\qquad \textit{Für } n>1 \textit{ ist } \Phi_n(t,j) = \Phi_n(j,t).$$

Beweis. Für jede Wurzel j_h von $\Phi_n(t,j) = 0$ gilt $\Phi_n(j,j_h) = 0$, weil K_h zyklisch vom Grade n über dem Körper $K^{n\varepsilon}$ mit der Invariante j ist. Da die j_h voneinander verschieden sind, so ist $\Phi_n(j,t)$ durch $\Phi_n(t,j)$ teilbar:

$$\Phi_n(j,t) = \Phi_n(t,j)\,\psi(t,j).$$

Daraus folgt

$$\Phi_n(t,j) = \Phi_n(j,t)\,\psi(j,t), \qquad \Phi_n(t,j) = \Phi_n(t,j)\,\psi(t,j)\,\psi(j,t).$$

$$\psi(t,j)\,\psi(j,t) = 1.$$

$\psi(t,j)$ ist daher eine Konstante, und weiter wird $\psi(j,t) = \pm 1$. Außer für $n = 1$, wo

$$\Phi(t,j) = t-j = -\Phi(j,t)$$

gilt, ist $\psi(t,j) = 1$, denn sonst wäre

$$\Phi(t,j) = -\Phi(j,t), \qquad \Phi(j,j) = 0$$

und K hätte einen zu sich selbst isomorphen Teilkörper K_h, also einen komplexen Multiplikator, was nach § 3 **3.** für $p \neq 0$ nicht geht.

4. Die $p+1$ Wurzeln j_h von $\Phi_p(t,j)=0$ sind ganze algebraische Funktionen von j, die nach Potenzen von $u=1/j$ entwickelt werden können. Wir schreiben jeweils nur das Anfangsglied der Entwicklung hin

$$j_h = \varrho_h u^{e_h} + \cdots, \quad \varrho_h \neq 0.$$

Die Anfangsexponenten e_h sind nicht positiv. Da kein j_h von j unabhängig sein kann — sonst wäre ja um so mehr die Invariante j des in K_h enthaltenen Körpers K^{p^2} von j unabhängig —, so sind die Anfangsexponenten e_h sogar negativ.

Nach (47) und (50) ist

$$\Phi_p(t,j) = (t^p - j)(t - j^p) + \sum_{\nu=0}^{p}\sum_{\mu=0}^{p} p c_{\nu\mu} t^\nu j^\mu$$

mit ganzzahligen $c_{\nu\mu}$. Da hieraus

$$\prod_{h=1}^{p+1} j_h = (-1)^{p-1} j^{p+1} + \sum_{\mu=0}^{p} p c_{0\mu} j^\mu$$

folgt, so gilt

$$\prod_{h=1}^{p+1} \varrho_h = (-1)^{p-1}, \qquad -\sum_{h=1}^{p+1} e_h = p+1.$$

Setzen wir die Reihenentwicklungen ein, so erhalten wir

$$(51)\quad \varrho_h^{p+1} u^{-e_h(p+1)} + (pc_{pp} - 1)\,\varrho_h^{p} u^{-p(e_h+1)} + u^{-p+1} + \cdots = 0,$$

wo die Punkte Glieder andeuten, in denen u mit einem höheren Exponenten als $-p(e_h+1)$ vorkommt. Es müssen daher zwei von den Zahlen

$$e_h(p+1), \qquad p(e_h+1), \qquad -p+1$$

einander gleich und nicht kleiner als die dritte sein. Das geht nur für $e_h = -p$ und $e_h = -1/p$. Wegen $-\Sigma e_h = 1+p$ kann höchstens ein e_h gleich p sein. Nun gilt für jede der Wurzeln j_h von $\Phi_p(t,j)=0$ auch die Gleichung $\Phi_p(j,j_h)=0$. Es gilt daher eine Reihenentwicklung

$$j = \varrho_{h^*} u_h^{e_{h^*}} + \cdots$$

von j nach Potenzen von

$$u_h = 1/j_h = \frac{1}{\varrho_h} u^{-e_h} + \cdots,$$

und daraus folgt $e_h e_{h^*} = 1$. Mit dem Exponenten e_h kommt also auch der Exponent $1/e_h$ in der Reihe $e_1, \cdots, e_{p+1}$ vor. Es ist daher wenigstens ein e_h gleich $-p$ und wenigstens eins gleich $-1/p$, und das geht nur,

wenn ein j_h, etwa j_{p+1}, gleich $-p$, und die übrigen, $e_1, \cdots, e_p$, gleich $-1/p$ sind. (Die Exponenten $-1/p$ müssen ja in Gruppen zu je p auftreten.)

Wir können jetzt weiter die Anfangskoeffizienten berechnen, indem wir bedenken, daß in (51) die Glieder mit dem kleinsten Exponenten die Summe 0 haben müssen. Das gibt für $h = p+1$

$$\varrho_{p+1}^{p+1} + (p c_{pp} - 1)\, \varrho_{p+1}^{p} = 0, \qquad \varrho_{p+1} = 1 - p c_{pp},$$

und für $h = 1, 2, \cdots, p$

$$(p c_{pp} - 1)\, \varrho_h^p + 1 = 0,$$

mithin bei passender Numerierung

$$\varrho_h = \frac{\zeta_p^h}{\sqrt[p]{1 - p c_{pp}}}, \quad \zeta_p \text{ primitive } p\text{-te Einheitswurzel.}$$

$$j_h = \frac{\zeta_p^h}{\sqrt[p]{1 - p c_{pp}}}\, u^{-\frac{1}{p}} + \cdots; \qquad h = 1, 2, \cdots, p;$$

$$j_{p+1} = (1 - p c_{pp})\, u^{-p} + \cdots.$$

Wir wollen jetzt weiter zeigen, daß

(52) $$c_{pp} = 0,$$

also

(53) $$\begin{cases} j_h = \zeta_p^h u^{-\frac{1}{p}} + \cdots; & h = 1, 2, \cdots, p; \\ j_{p+1} = u^{-p} + \cdots \end{cases}$$

gilt. Zu diesem Zwecke nehmen wir eine von p verschiedene Primzahl q und berechnen mittels (48) die Anfangsglieder der u-Entwicklungen für die Wurzeln j_{hl} von $\Phi_{pq}(t, j) = 0$:

$$j_{hl} = \frac{\zeta_q^l\, \zeta_p^{hq}}{\sqrt[q]{1 - q c_{qq}^{(q)}}\, \left(\sqrt[p]{1 - p c_{pp}^{(p)}}\right)^q}\, u^{-\frac{1}{pq}} + \cdots; \qquad \begin{matrix} h = 1, 2, \cdots, p, \\ l = 1, 2, \cdots, q \end{matrix}$$

$$j_{p+1,l} = \frac{\zeta_q^l}{\sqrt[q]{1 - q c_{qq}^{(q)}}}\, (1 - p c_{pp}^{(p)q})\, u^{-\frac{p}{q}} + \cdots; \qquad l = 1, 2, \cdots, q;$$

$$j_{h,q+1} = (1 - q c_{qq}^{(q)}) \frac{\zeta_p^{hq}}{\left(\sqrt[p]{1 - p c_{pp}^{(p)}}\right)^q}\, u^{-\frac{q}{p}} + \cdots; \qquad h = 1, 2, \cdots, p;$$

$$j_{p+1,q+1} = (1 - q c_{qq}^{(q)})\, (1 - p c_{pp}^{(p)q})\, u^{-pq} + \cdots.$$

(Wir haben die zu p und q gehörigen c durch obere Indizes unterschieden.) Vertauschen wir die Rollen von p und q, so erhalten wir aus der Entwicklung von $j_{p+1,q+1}$

$$(1 - q\,c_{qq}^{(q)})^{p-1} = (1 - p\,c_{pp}^{(p)})^{q-1}.$$

Hieraus folgt, daß $1 - p\,c_{pp}^{(p)}$ durch keine von p verschiedene Primzahl q teilbar ist. Da es auch durch p nicht teilbar ist, so ist $1 - p\,c_{pp}^{(p)} = \pm 1$. Im Falle $p > 2$ ergibt sich sogar $1 - p\,c_{pp}^{(p)} = 1$, also $c_{pp}^{(p)} = 0$. Das Vorzeichen von $1 - 2\,c_{22}^{(2)}$ bleibt noch unsicher. Wir bestimmen es durch die vollständige Berechnung von $\Phi_2(t, j)$.

Eine Methode zur Berechnung von $\Phi_n(t, j)$ die grundsätzlich zum Ziele führt, ist die folgende. Wir erzeugen K durch eine Gleichung der Form $y^2 = f(x)$, etwa durch die Legendresche Normalform

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

Für gerades n ist

$$1, x, y, x^2, xy, x^3, x^2y, \cdots, x^{\frac{1}{2}n-1}y, x^{\frac{1}{2}n},$$

für ungerades n

$$1, x, y, x^2, xy, \cdots, x^{\frac{1}{2}(n-1)}, x^{\frac{1}{2}(n-1)}y$$

eine linear unabhängige Basis der Multipla von $\mathfrak{o}^{-n}$. Daraus lassen sich nach HASSE[22]) Vertreter $\mathfrak{p}_1/\mathfrak{o}, \cdots, \mathfrak{p}_{n^2}/\mathfrak{o}$ der n^2 Divisorenklassen finden, deren n-te Potenzen 1 sind, und zwar ergeben sich Elemente $y_i \cong (\mathfrak{p}_i/\mathfrak{o})^n$. Sind $\mathfrak{p}_1/\mathfrak{o}, \cdots, \mathfrak{p}_{\psi(n)}/\mathfrak{o}$ die Klassen von der genauen Ordnung n, so sind

$$k\left(x, y, \sqrt[n]{y_1}\right), \cdots, k\left(x, y, \sqrt[n]{y_{\psi(n)}}\right)$$

die $\psi(n)$ zyklischen unverzweigten Erweiterungskörper n-ten Grades von K und deren Invarianten sind die Wurzeln von $\Phi_n(t, j)$. Für $p = 2$ ist das Verfahren noch ziemlich einfach durchzuführen. Wir nehmen die Legendresche Normalform

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

Die drei Elemente y_1, y_2, y_3 sind offenbar $y = x$, $y = x - 1$ und $y_3 = x - \lambda$.

---

[22]) H. HASSE, Zur Theorie der abstrakten elliptischen Funktionenkörper. I. Journ. f. d. r. u. ang. Math. **175**, S. 55—62 (1936), S. 57.

Es ist

$$y^2 = (\sqrt{x})^2(\sqrt{x^2}-1)(\sqrt{x^2}-\lambda),$$

$$\left(\frac{y}{\sqrt{x}}\right)^2 = (\sqrt{x}-1)(\sqrt{x}+1)(\sqrt{x}-\sqrt{\lambda})(\sqrt{x}+\sqrt{\lambda}).$$

Aus dieser definierenden Gleichung von K_1 können wir den zu K_1 gehörigen Wert λ_1 des Parameters λ berechnen

$$\lambda_1 = \frac{1-\sqrt{\lambda}}{1+\sqrt{\lambda}} : \frac{-1-\sqrt{\lambda}}{-1+\sqrt{\lambda}} = \left(\frac{1-\sqrt{\lambda}}{1+\sqrt{\lambda}}\right)^2,$$

und daraus folgt

$$j_1 = 2^8 \frac{(1-\lambda_1(1-\lambda_1))^3}{\lambda_1^2(1-\lambda_1)^2} = 2^4 \frac{((1-\lambda)^2+16\lambda)^3}{\lambda(1-\lambda)^4}.$$

In ähnlicher Weise ergibt sich

$$j_2 = 2^4 \frac{(\lambda^2+16(1-\lambda))^3}{\lambda^4(1-\lambda)},$$

$$j_3 = 2^4 \frac{(16\lambda(1-\lambda)-1)^3}{\lambda(1-\lambda)}.$$

Die Invariantengleichung zweiter Ordnung sei

$$\Phi_2(t,j) = t^3+j^3+at^2j^2+bt^2j+btj^2+ct^2+cj^2+dtj+et+ej+f = 0.$$

Dann ist

$$aj^2+bj+c = -(j_1+j_2+j_3), \tag{54}$$

$$bj^2+dj+e = j_1j_2+j_2j_3+j_3j_1, \tag{55}$$

$$j^3+cj^2+ej+f = -j_1j_2j_3. \tag{56}$$

Hier setzen wir spezielle Werte von λ ein und erhalten so lineare Gleichungen zur Bestimmung der Koeffizienten a, b, c, d, e, f. $\lambda = -\varepsilon$ (ε primitive dritte Einheitswurzel) gibt $j = 0$, $j_1 = j_2 = j_3 = 2^4 3^3 5^3$, folglich ist

$$c = -2^4 3^4 5^3, \qquad e = 2^8 3^7 5^6, \qquad f = -2^{12} 3^9 5^9.$$

Wir setzen weiter $\lambda = 0$, nachdem wir vorher mit einer passenden Potenz von λ multipliziert haben. Es wird

$$\lambda^2 j\big|_{\lambda=0} = 2^8, \qquad \lambda j_1\big|_{\lambda=0} = 2^4, \qquad \lambda^4 j_2\big|_{\lambda=0} = 2^{16}, \qquad \lambda j_3\big|_{\lambda=0} = -2^4.$$

(54) multiplizieren wir mit λ^4, setzen $\lambda = 0$ und finden

$$a = -1.$$

55) multiplizieren wir ebenfalls mit λ^4 und setzen $\lambda = 0$. Auf der linken Seite steht dann $2^{16} b$, auf der rechten Seite wird $\lambda^4 j_1 j_3 = 0$, aber für

$$\lambda^4 (j_1 j_2 + j_2 j_3) = \lambda^4 j_2 (j_1 + j_3)$$

ergibt sich

$$\lambda^4 (j_1 j_2 + j_2 j_3)_{\lambda = 0} = 2^{20} \cdot 3 \cdot 31,$$

mithin ist

$$b = 2^4 \cdot 3 \cdot 31.$$

Schließlich setzen wir $\lambda = 2$, das gibt

$$j = 2^6 \cdot 3^3, \qquad j_1 = 2^3 3^3 11^3, \qquad j_2 = 2^6 3^3, \qquad j_3 = 2^3 3^3 11^3.$$

In (55) eingesetzt, ergibt das eine Gleichung für d, die dann zu

$$d = 3^3 \cdot 5^3 \cdot 4027$$

führt. Mithin ist die Invariantengleichung zweiter Ordnung[23])

$$\begin{aligned} (57) \qquad \Phi_2 (t, j) = {} & t^3 + j^3 - t^2 j^2 + 2^4 3 \cdot 31 (t^2 j + t j^2) - 2^4 3^4 5^3 (t^2 + j^2) \\ & + 3^3 5^3 4027\, tj + 2^8 3^5 5^6 (t + j) - 2^{12} 3^9 5^9 = 0. \end{aligned}$$

Oder

$$\begin{aligned} \Phi_2 (t, j) = {} & (t^2 - j)(t - j^2) + 2^4 3 \cdot 31 (t^2 j + t j^2) - 2^4 3^4 5^3 (t^2 + j^2) \\ & 2 \cdot 6795563\, tj + 2^8 3^5 5^6 (t + j) - 2^{12} 3^9 5^9 = 0. \end{aligned}$$

In der Tat ist also auch $c_{22}^{(2)} = 0$.

Wir können jetzt die Anfangsglieder der u-Entwicklungen für die Wurzeln einer beliebigen Invariantengleichung $\Phi_n (t, j) = 0$ berechnen. Zunächst betrachten wir den Fall $n = p^2$. j_h sei eine Wurzel von $\Phi_p (t, j) = 0$. Die Entwicklungen der Wurzeln j_{hl} von $\Phi_{p^2} (t, j_h)$ lauten für $l = 1, 2, \cdots, p$

$$j_{hl} = \zeta_p^l u_h^{-\frac{1}{p}} + \cdots, \qquad u_h = 1/j_h,$$

also

$$j_{hl} = \zeta_{p^2}^{h+lp} u^{-\frac{1}{p^2}} + \cdots \qquad \text{für } h = 1, 2, \cdots, p,$$

dabei bedeutet ζ_{p^2} eine feste p-te Wurzel aus ζ_p, und

$$j_{p+1,l} = \zeta_p^l u_{p+1}^{-\frac{1}{p}} + \cdots = \zeta_p^l u^{-1} + \cdots$$

---

[23]) Vgl. etwa W. Weber, Lehrbuch der Algebra III, S. 248. Gleichung (5) dort ist die Invariantengleichung zweiter Ordnung für $\gamma_2 (\omega) = \sqrt[3]{j(\omega)}$.

für $l = p+1$ dagegen

$$j_{h,p+1} = u_h^{-p} + \cdots = u^{-1} + \cdots; \qquad h = 1, 2, \cdots, p,$$
$$j_{p+1,p+1} = u_{p+1}^{-p} + \cdots = u^{-p^2} + \cdots.$$

An diesen Formeln ist ohne weiteres zu erkennen, welche Wurzel von $\Phi_p(t, j_h)$ gleich j wird, nämlich $j_{h,p+1}$ für $h = 1, 2, 3, \cdots, p$ und $j_{p+1,p}$ für $h = p+1$. Nach (33) sind daher die sämtlichen Wurzeln von $\Phi_{p^2}(t, j)$

$$j_{hl} = \zeta_{p^2}^{h+lp}\, u^{-\frac{1}{p^2}} + \cdots, \qquad h, l = 1, 2, \cdots, p,$$
$$j_{p+1,l} = \zeta_p^l\, u^{-1} + \cdots, \qquad l = 1, 2, \cdots, p-1,$$
$$j_{p+1,p+1} = u^{-p^2} + \cdots.$$

So fortfahrend, erhalten wir die Entwicklungsanfänge der Wurzeln von $\Phi_{p^f}(t, j)$

$$j_h = \zeta_{p^f}^h\, u^{-\frac{1}{p^f}}, \quad h \bmod p^f,$$
$$j_{h,1} = \zeta_{p^{f-1}}^h\, u^{-\frac{1}{p^{f-1}}}, \quad h \bmod p^{f-1}, \qquad (h, p) = 1,$$
$$j_{h,2} = \zeta_{p^{f-2}}^h\, u^{-\frac{1}{p^{f-2}}}, \quad h \bmod p^{f-2}, \qquad (h, p) = 1,$$
$$j_{h,f-1} = \zeta_p^h\, u^{-p^{f-1}} + \cdots, \quad h \bmod p, \qquad (h, p) = 1,$$
$$j_{h,f} = u^{-p^f} + \cdots.$$

Dabei ist jeweils ζ_{p^i} eine feste p-te Wurzel aus $\zeta_{p^{i-1}}$, $i = 2, \cdots, f$.

Mit Hilfe von (48) können wir schließlich die Anfangsglieder der u-Entwicklungen der Wurzeln von $\Phi_n(t, j) = 0$ für ein beliebiges zusammengesetztes n aufstellen und finden ohne Mühe für die in neuer Weise numerierten Wurzeln $j_{s,h}$, wo s alle Teiler von n und h bei festem s alle zu $\left(s, \frac{n}{s}\right)$ teilerfremden Reste modulo s durchläuft

$$j_{s,h} = \zeta_s^h\, u^{-n/s} + \cdots, \quad s \mid n, \quad h \bmod s, \quad (h, s, n/s) = 1; \tag{58}$$

unter ζ_s eine primitive s-te Einheitswurzel verstanden.

Wir wollen schließlich noch beweisen:

Die Koeffizienten der Reihen (58) sind für die Charakteristik 0 ganze Zahlen des Körpers der s-ten Einheitswurzeln. Wir erhalten daher die entsprechende Reihen für eine Primzahlcharakteristik q, indem wir sie nach einem Primfaktor von q im Körper der n-ten Einheitswurzeln reduzieren.

Die Herleitung der Reihen (58) zeigt, daß diese Behauptung nur für $n = p =$ Primzahl zu beweisen ist. Hier genügt es, die Reihe

$$j_p = u^{-p} + \cdots$$

zu betrachten, weil wegen der Symmetrie von $\Phi_p(t, j)$ die p anderen Reihen $j_h = \zeta_p^h u^{-\frac{1}{p}} + \cdots$ Umkehrungen dieser Reihe sind.

Wir schreiben der Deutlichkeit halber $\Phi_p(t, j)\, u^{p^2+p}$ als Polynom von $z = tu^p$ und $1/j = u$ und deuten dabei Glieder mit positiven Potenzen von u durch Punkte an

$$z^{p+1} - z^p + \cdots = \Phi_p(t, j)\, u^{p^2+p}.$$

Die Koeffizienten dieses Polynoms sind ganze Zahlen. Die Koeffizienten d_i der Reihe

$$z = 1 + d_1 u + \cdots,$$

die dieses Polynom zu 0 macht, berechnen sich bekanntlich aus den Koeffizienten des Polynoms durch Additionen, Subtraktionen, Multiplikationen und außerdem Divisionen durch den Wert der partiellen Ableitung des Polynoms nach z für $z = 1$, $u = 0$. Der ist aber offensichtlich gleich 1.

Die solchermaßen aufgestellten u-Entwicklungen für die Wurzeln der Invariantenpolynome leisten für die Theorie der komplexen Multiplikation das gleiche wie die q-Entwicklungen (Entwicklungen nach $q = e^{2\omega i}$) in der analytischen Theorie. Es kommt also auf die Konvergenz der q-Entwicklungen gar nicht an. Die Galoissche Theorie der Invariantengleichungen kann mit Hilfe der u-Entwicklungen genau so behandelt werden wie mittels der q-Entwicklungen, worauf wir nicht näher eingehen, weil sich kaum Änderungen ergeben (vgl. WEBER, Lehrbuch der Algebra III, achter Abschnitt).

§ 7. Singuläre und supersinguläre Invarianten.

Da der Typus eines elliptischen Funktionenkörpers durch seine Invariante j völlig festgelegt ist, so muß sich insbesondere die Struktur des zugehörigen Multiplikatorenrings durch j ausdrücken. Mit der Untersuchung dieses Zusammenhangs befaßt sich der Rest dieser Arbeit.

Wir nennen eine Invariante j *singulär*, wenn der Multiplikatorenring komplex und kommutativ ist, *supersingulär*, wenn er nichtkommutativ ist.

Die singulären und die supersingulären Invarianten sind absolut algebraisch (algebraisch über dem Primkörper), die supersingulären Invarianten haben sogar höchstens den Grad 2 über dem Primkörper.

Beweis. Die Behauptung über die supersingulären Invarianten haben wir schon zweimal benutzt, sie folgte ja unmittelbar aus der Tatsache, daß wegen $\sigma = 2$ $K^{\varepsilon p} = K^{p^2}$ und daher $j^{p^2} = j$ ist.

Für die singulären Invarianten von Primzahlcharakteristik haben wir die Behauptung ebenfalls in § 3 **3.** schon bewiesen, sie ergibt sich aber im folgenden noch einmal.

$K = k(x, y)$ sei ein Körper mit absolut transzendenter Invariante j und einer endlichen algebraischen Erweiterung k von $P(j)$ als Konstantenkörper. Gesetzt, der Multiplikatorenring $_j\mathbf{R}$ von K wäre komplex. Er müßte auch für Primzahlcharakteristik kommutativ sein, weil $\sigma = 1$ ist. q sei eine im Quotientenkörper Σ von $\mathbf{R}$ prim bleibende Primzahl und j^* eine Nullstelle der Gleichung

$$\Phi_q(j, j) = 0.$$

Reduzieren wir K nach einem Primteiler von $j - j^*$, so erhalten wir nach § 4 **2.**, **3.** einen elliptischen Körper $\bar{K}$ mit der Invariante j^*. Der Multiplikatorenring $\mathbf{R}$ von K umfaßte einerseits $\mathbf{R}$, enthielte aber andererseits auch einen Multiplikator der Norm q, weil einer der Teilkörper von $\bar{K}$, über denen K zyklisch vom Grade q ist, wegen $\Phi_q(j^*, j^*) = 0$ zu K isomorph wäre. Da Σ keine Zahlen der Norm q enthält, so müßte $\mathbf{R}$ nichtkommutativ sein, was für $p = 0$, aber auch für $p \neq 0$ nicht möglich ist, weil Σ nicht in $Q_{\infty, p}$ eingebettet werden kann.

Wenn K komplexe Multiplikatoren hat, so gibt es solche, die kein ganzzahliges Vielfaches eines anderen Multiplikators sind, aber eine Norm > 1 haben. Ist n die Norm eines solchen Multiplikators μ, so ist K über K^u zyklisch vom Grade n und daher genügt die Invariante j von K der Gleichung

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

Die singulären Invarianten der Charakteristik 0 *sind ganze algebraische Zahlen.*

Um dies zu beweisen, wollen wir den höchsten Koeffizienten einer Gleichung

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

berechnen, der die singuläre Invariante j genügt. Der höchste Koeffizient von $\Phi_n(j, j)$ ist der Koeffizient der niedrigsten Potenz von u in der Entwicklung von $\Phi_n(j, j)$ nach Potenzen von u. Wir zerlegen $\Phi_n(t, j)$ in Linearfaktoren

$$\Phi_n(t, j) = \prod_{\substack{s \mid n \\ h \bmod s \\ \left(h, s, \frac{n}{s}\right) = 1}} (t - j_{s,h})$$

und setzen für die $j_{s,h}$ die Reihenentwicklungen (58) ein

$$\Phi_n(j, j) = \prod_{\substack{s \mid n \\ h \bmod s, \left(h, s, \frac{n}{s}\right) = 1}} (u^{-1} - \zeta_s^h u^{-n s^2} + \cdots).$$

Das niedrigste Glied des Faktors (s, h) ist

$$\begin{aligned} u^{-1} &\quad \text{für} \quad s^2 > n, \\ (1 - \zeta_s^h)\, u^{-1} &\quad \text{für} \quad s^2 = n, \\ -\zeta_s^h\, u^{-n/s^2} &\quad \text{für} \quad s^2 < n. \end{aligned}$$

Mithin heißt das höchste Glied von $\Phi_n(j, j)$

$$j^{\sum_{s \mid n,\, s^2 > n} s \frac{\varphi(s, n/s)}{(s, n/s)}} \quad j^{\sum_{s \mid n,\, s^2 < n} s \frac{\varphi(s, n/s)}{(s, n/s)}} = j^{\sum_{s \mid n,\, s^2 > n} 2 s \frac{\varphi(s, n/s)}{(s, n/s)}} \tag{59}$$

falls n keine Quadratzahl ist, und

$$\prod_{\substack{h \bmod m \\ (h, m) = 1}} (1 - \zeta_m^h)\, j^{\sum_{s \mid m^2,\, s > m} 2 s \frac{\varphi(s, m^2/s)}{(s, m^2/s)} + \varphi(m)} \tag{60}$$

für eine Quadratzahl $n = m^2$.

Da es in einem komplexen Multiplikatorenring immer Elemente mit nichtquadratischer Norm gibt, so genügt eine singuläre Invariante j der Charakteristik 0 einer Gleichung

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

mit ganzen rationalen Koeffizienten und dem höchsten Koeffizienten 1. sie ist daher eine ganze algebraische Zahl[24]).

§ 8. Existenz und Berechnung der supersingulären Invarianten.

1. Für eine supersinguläre Invariante der Charakteristik p ist das zugehörige σ gleich 2, d. h. der elliptische Körper K mit der Invariante j hat keine Divisorenklassen der Ordnung p. Es gilt aber auch umgekehrt:

[24]) Dies ist der klassische Beweis, vgl. W. Weber, Lehrbuch der Algebra III, S. 422.

Wenn $\sigma = 2$ ist, K also keine Divisorenklassen der Ordnung p hat, so hat K eine Maximalordnung von $Q_{\infty,p}$ als Multiplikatorenring, die zugehörige Invariante j ist also supersingulär.

Nach § 2, **10.** genügt es zu zeigen, daß K überhaupt komplexe Multiplikatoren hat. Die Invariante von K genügt der Gleichung $j^{p^2} = j$. Das gleiche gilt, unter q eine Primzahl $\neq p$ verstanden, für die $q+1$ elliptischen Teilkörper $K_{q,i}$ von K, über denen K zyklisch vom Grade q ist. Da $j^{p^2} = j$ nur p^2 Lösungen hat, so muß es zwei verschiedene Primzahlen q_1, q_2 geben, derart, daß einer der Körper K_{q_1,i_1} die gleiche Invariante hat wie einer der Körper K_{q_2,i_2}. Daraus folgt aber, daß K_{q_1,i_1} einen Multiplikator der Norm $q_1 q_2$ hat, der nicht rational sein kann. Damit ist aber schon alles bewiesen.

2. Da die Divisorenklassengruppen der Ordnung p nach § 1 umkehrbar eindeutig den unverzweigten zyklischen Erweiterungskörpern p-ten Grades von K entsprechen, so folgt die Existenz von supersingulären Invarianten aus der Existenz von elliptischen Körpern ohne zyklische Erweiterungen p-ten Grades. Diese können wir aber nach einer Untersuchung von HASSE[25]) leicht aufstellen.

Nach HASSE ordnen wir einem elliptischen Körper K der Primzahlcharakteristik p eine bis auf einen Faktor s^{1-p}, $s \neq 0$ konstant, eindeutig bestimmte *Invariante* A auf die folgende Weise zu: $\mathfrak{o}$ sei ein Primdivisor von K, ω ein zugehöriges Primelement und r das bis auf eine additive Konstante eindeutig bestimmte ganze Multiplum von $\mathfrak{o}^{-p}$ das der Kongruenz

$$r \equiv \omega^{-p} \bmod \mathfrak{o}^{-1}$$

genügt. Dann gilt eine Kongruenz

$$r \equiv \omega^{-p} - A/\omega \bmod \mathfrak{o}^{0}$$

mit einer Konstanten A. Dies A ist die Invariante; sie ist, wie gesagt, von der Wahl von $\mathfrak{o}$ und ω unabhängig bis auf einen Faktor s^{1-p}, $s \neq 0$ konstant. K hat zyklische unverzweigte Erweiterungen oder nicht, je nachdem $A \neq 0$ oder $A = 0$ ist. Daher sind die supersingulären Invarianten diejenigen Werte von j, welche die Invariante A des Körpers K mit absolut transzendenter Invariante j zu 0 machen. Wir wollen daher A für diesen Körper berechnen.

a) $p = 2$. Wir gehen von der Normalform

$$y^2 - y + \alpha x y = x^3$$

[25]) H. HASSE, loc. cit. [22]), Nr. 1.

aus. Für den Nennerprimdivisor $\mathfrak{o}$ von x und y ist $x/y = \omega$ ein Primelement. Die ganzen Vielfachen von $\mathfrak{o}^{-2}$ haben die Form

$$\xi + \eta x.$$

Wir haben also

$$v = \eta x$$

aus

$$\eta x \equiv y^2/x^2 \bmod \mathfrak{o}^{-1}$$

zu bestimmen oder aus

$$\frac{\eta}{(1+\alpha x)yx^{-3}+1} \equiv 1 \bmod \mathfrak{o}.$$

Das gibt $\eta = 1$, $v = x$. A finden wir dann aus

$$x \equiv y^2/x^2 - Ay/x \bmod \mathfrak{o}^0$$

oder

$$x^3/y^2 \equiv 1 - Ax/y \bmod \mathfrak{o}^2$$

oder

$$(1+\alpha x)y^{-1}+1 \equiv 1 - Ax/y \bmod \mathfrak{o}^2,$$

was wegen $1/y \equiv 0 \bmod \mathfrak{o}^3$ mit

$$\alpha x/y \equiv Ax/y \bmod \mathfrak{o}^2$$

gleichbedeutend ist. Mithin ist einfach

$$A = \alpha,$$

und die einzige supersinguläre Invariante der Charakteristik 2 ist

$$j = 0,$$

was mit dem Ergebnis von § 5 **3.** übereinstimmt, daß $j = 0$ die einzige Invariante ist, zu der eine größere Gruppe von Multiplikatoreneinheiten als ± 1 gehört.

b) $p \neq 2$. Wir erzeugen K durch eine Gleichung

$$y^2 = f(x),$$

wo $f(x) = a_0 x^3 + a_1 x^2 + a_2 x + a_3$ ein kubisches Polynom bedeutet und nehmen für $\mathfrak{o}$ den Nennerprimdivisor von x und y. Dann ist x/y ein zugehöriges Primelement und

$$1, x, x^2, \cdots, x^{\frac{1}{2}(p-1)}, y, xy, \cdots, x^{\frac{1}{2}(p-3)}y$$

ist eine Basis der Multipla von $\mathfrak{o}^{-p}$. Daher können wir v eindeutig in der Gestalt

$$v = \alpha_1 x + \cdots + \alpha_{\frac{p-1}{2}} x^{\frac{1}{2}(p-1)} + y\left(\beta_0 + \beta_1 x + \cdots + \beta_{\frac{p-3}{2}} x^{\frac{1}{2}(p-3)}\right)$$

ansetzen. Der Automorphismus von $K/k(x)$ macht aus der Kongruenz

$$\left(\alpha_1 x + \cdots + \alpha_{\frac{p-1}{2}} x^{\frac{1}{2}(p-1)}\right) + y\left(\beta_0 + \cdots + \beta_{\frac{1}{2}(p-3)} x^{\frac{1}{2}(p-3)}\right)$$
$$\equiv y^p/x^p \bmod \mathfrak{o}^{-1}$$

die andere

$$\left(\alpha_1 x + \cdots + \alpha_{\frac{p-1}{2}} x^{\frac{1}{2}(p-1)}\right) - y\left(\beta_0 + \cdots + \beta_{\frac{1}{2}(p-3)} x^{\frac{1}{2}(p-3)}\right)$$
$$\equiv -y^p/x^p \bmod \mathfrak{o}^{-1},$$

so daß

$$2\left(\alpha_1 x + \cdots + \alpha_{\frac{p-1}{2}} x^{\frac{1}{2}(p-1)}\right) \equiv 0 \bmod \mathfrak{o}^{-1},$$

das heißt

$$\alpha_1 = \alpha_2 = \cdots = \alpha_{\frac{p-1}{2}} = 0$$

gilt.

Zur Bestimmung von A haben wir die Kongruenz

$$y\left(\beta_0 + \cdots + \beta_{\frac{p-3}{2}} x^{\frac{1}{2}(p-3)}\right) \equiv y^p/x^p - A\,y/x \bmod \mathfrak{o}^0.$$

Wir multiplizieren sie mit x/y und setzen für y^{p-1} den Ausdruck $f(x)^{\frac{1}{2}(p-1)}$ ein

$$A \equiv f(x)^{\frac{1}{2}(p-1)} x^{1-p} - x\left(\beta_0 + \beta_1 x + \cdots + \beta_{\frac{p-3}{2}} x^{\frac{1}{2}(p-3)}\right) \bmod \mathfrak{o}.$$

Da y nicht mehr vorkommt, so kann die Kongruenz auch modulo $\mathfrak{o}^2$ oder x^{-1} genommen oder schließlich in die Gestalt

$$\left(f(x)/x^3\right)^{\frac{1}{2}(p-1)} \equiv A x^{\frac{1}{2}(p-1)} + \beta_0 x^{\frac{1}{2}(p-3)} + \cdots + \beta_{\frac{p-3}{2}} \bmod x^{-\frac{p-1}{2}}$$

gesetzt werden. Mithin ist A nichts weiter als der Koeffizient von $x^{-\frac{1}{2}(p-1)}$ in dem Polynom

$$\left(f(x)/x^3\right)^{\frac{1}{2}(p-1)} = \left(a_3 x^{-3} + a_2 x^{-2} + a_1 x^{-1} + a_0\right)^{\frac{1}{2}(p-1)}$$

von x^{-1}.

Wir nehmen zuerst die Legendresche Normalform mit

$$f(x) = x(x-1)(x-\lambda).$$

A ist der Koeffizient von $x^{\frac{1}{2}(p-1)}$ in

$$((1-x^{-1})(1-\lambda/x))^{\frac{1}{2}(p-1)},$$

das heißt

$$A = (-1)^{\frac{1}{2}(p-1)} \sum_{i=1}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{i}^2 \lambda^i = s_p(\lambda). \tag{61}$$

Offenbar gilt

$$s_p(1/\lambda) = \lambda^{\frac{1}{2}(p-1)} s_p(\lambda).$$

Da $1-\lambda$ zu der gleichen Invariante wie λ gehört, so muß sich $s_p(1-\lambda)$ von $s_p(\lambda)$ um einen von λ unabhängigen Faktor unterscheiden. Das gibt

$$s_p(1-\lambda) = (-1)^{\frac{1}{2}(p-1)} s_p(\lambda).$$

Für $p = 3$ haben wir

$$A = -1-\lambda$$

folglich ist

$$j = 0$$

die einzige supersinguläre Invariante modulo 3, in Übereinstimmung mit § 5 **2.**

Für $p > 3$ liefert (61) wenigstens die Existenz von supersingulären Invarianten, wir haben uns nur davon zu überzeugen, daß die Wurzeln von $s_p(\lambda) = 0$ nicht 0 oder 1 sind ($j = \infty$):

$$s_p(0) = 1, \quad s_p(1) = \sum_{i=0}^{\frac{p-1}{2}} \binom{p-1}{2}^2 = \binom{p-1}{\frac{p-1}{2}} \neq 0.$$

Zur Berechnung der supersingulären Invarianten ist es vorteilhafter, von der Weierstraßschen Normalform auszugehen, also $f(x) = 4x^3 - g_2 x - g_3$ zu nehmen. A ist der Koeffizient von $x^{-\frac{1}{2}(p-1)}$ in

$$(-g_3 x^{-3} - g_2 x^{-2} + 4)^{\frac{1}{2}(p-1)},$$

also

$$A = \sum_{3i+2h=\frac{p-1}{2}} \frac{\left(\frac{p-1}{2}\right)!}{i!\,h!\left(\frac{p-1}{2}-i-h\right)!} (-g_3)^i (-g_2)^h 4^{\frac{p-1}{2}-i-h} \tag{62}$$

Es ist

$$j = 2^6 3^3 g_2^3/\Delta \text{ mit } \Delta = g_2^3 - 27 g_3^2.$$

daher

$$g_2 = j^{\frac{1}{3}} \Delta^{\frac{1}{3}}/12, \quad g_3 = (j - 2^6 3^3)^{\frac{1}{2}} \Delta^{\frac{1}{2}}/216.$$

Setzen wir diese Werte in (62) ein, so erhalten wir

für $p \equiv 1 \pmod{12}$

$$A = (-1)^{\frac{p-1}{4}} \frac{\left(\frac{p-1}{2}\right)!}{3^{\frac{p-1}{4}}} \Delta^{\frac{p-1}{2}}$$

(63.1)

$$\times \sum_{i=0}^{\frac{p-1}{12}} \frac{\left(-\frac{4}{27}\right)^i}{(2i)!\left(\frac{p-1}{4} - 3i\right)!\left(\frac{p-1}{4} + i\right)!} j^{\frac{p-1}{12} - i} (j - 2^6 \cdot 3^3)^i,$$

für $p \equiv 5 \pmod{12}$

$$A = 4(-1)^{\frac{p-1}{4}} \frac{\left(\frac{p-1}{2}\right)!}{3^{\frac{p-5}{4}}} \Delta^{\frac{p-5}{12}} g_2$$

(63.5)

$$\times \sum_{i=0}^{\frac{p-5}{12}} \frac{\left(-\frac{4}{27}\right)^i}{(2i)!\left(\frac{p-1}{4} - 3i\right)!\left(\frac{p-1}{4} + i\right)!} j^{\frac{p-5}{12} - i} (j - 2^6 \cdot 3^3)^i,$$

für $p \equiv 7 \pmod{12}$

$$A = 16(-1)^{\frac{p-3}{4}} \frac{\left(\frac{p-1}{2}\right)!}{3^{\frac{p-7}{4}}} \Delta^{\frac{p-7}{4}} g_3$$

(63.7)

$$\times \sum_{i=0}^{\frac{p-7}{4}} \frac{\left(-\frac{4}{27}\right)^i}{(2i+1)!\left(\frac{p-7}{4} - 3i\right)!\left(\frac{p+1}{4} + i\right)!} j^{\frac{p-7}{12} - i} (j - 2^6 \cdot 3^3)^i$$

und für $p \equiv 11 \pmod{12}$

$$A = 64(-1)^{\frac{p-3}{4}} \frac{\left(\frac{p-1}{2}\right)!}{3^{\frac{p-11}{12}}} \Delta^{\frac{p-11}{12}} g_2 g_3$$

(63.11)

$$\times \sum_{i=0}^{\frac{p-11}{12}} \frac{\left(-\frac{4}{27}\right)^i}{(2i+1)!\left(\frac{p-7}{4} - 3i\right)!\left(\frac{p+1}{4} + i\right)!} j^{\frac{p-11}{12} - i} (j - 2^6 \cdot 3^3)^i.$$

Die Summen auf den rechten Seiten dieser Formeln sind bis auf einen konstanten Faktor die von HASSE[26]) mit $P(j)$ bezeichneten Polynome. Wir erkennen, daß die von HASSE vermutete Gradzahl $[p/12]$ richtig ist.

Führen wir

$$t = -4\,(j - 2^6 3^3)/27\,j$$

als neue Veränderliche ein, so wird

$$\text{(64.1)}\qquad \text{const.}\, j^{-\left[\frac{p}{12}\right]} P(j) = \sum_{0 \leqq i < \frac{p}{12}} \frac{t^i}{(2i)!\left(\frac{p-1}{4} - 3i\right)!\left(\frac{p-1}{4} + i\right)!}, \quad \text{wenn } p \equiv 1 \bmod 4,$$

$$\text{(64.—1)}\qquad \text{const.}\, j^{-\left[\frac{-p}{12}\right]} P(j) = \sum_{0 \leqq i < \frac{p}{12}} \frac{t^i}{(2i+1)!\left(\frac{p-7}{4} - 3i\right)!\left(\frac{p+1}{4} + i\right)!}, \quad \text{wenn } p \equiv -1 \bmod 4.$$

In dieser Gestalt lassen sie sich verhältnismäßig bequem berechnen. Wir lassen eine Tabelle der Polynome $P(j)$ und der supersingulären Invarianten für $p < 100$ folgen.

Supersinguläre Invarianten modulo p.

(65)

p	$P_p(j)$	Wurzeln von $P_p(j)$	$2^6 3^3$	0
2	*	*	0	0
3	*	*	0	0
5	1	*	*	0
7	1	*	6	*
11	1	*	1	0
13	$j-5$	5	*	*
17	$j-8$	8	*	0
19	$j-7$	7	18	*
23	$j-19$	19	3	0
29	$j^2+2j+21$	2, 25	*	0

[26]) H. HASSE, Existenz separabler zyklischer unverzweigter Erweiterungskörper vom Primzahlgrade p über elliptischen Funktionenkörpern der Charakteristik p. Journ. f. d. r. u. ang. Math. **172**, S. 77—85 (1934), S. 81.

(65)

p	$P_p(j)$	Wurzeln von $P_p(j)$	$2^6 3^3$	0
31	$j^2+25j+8$	2, 4	23	*
37	$j^3+23j^2+5j+11$	$8,\ 3\pm 10\sqrt{2}$	*	*
41	$j^3+19j^2+10j+18$	3, 28, 32	*	0
43	$j^3+21j^2+11j+32$	$41,\ 12+8\sqrt{2}$	8	*
47	$j^3+31j^2+33j+35$	9, 10, 44	36	0
53	$j^4+7j^3+30j^2+9j+24$	$46,\ 50,\ 28+9\sqrt{2}$	*	0
59	$j^4+39j^3+35j^2+31j+39$	15, 28, 47, 48	17	0
61	$j^5+60j^4+8j^3+27j^2+21j+60$	$9,\ 41,\ 50,\ 42+4\sqrt{2}$	*	*
67	$j^5+53j^4+4j^3+47j^2+36j+8$	$66, 45\pm 30\sqrt{2}, 63\pm 32\sqrt{2}$	53	*
71	$j^5+j^4+33j^3+28j^2+54j+18$	17, 40, 41, 48, 66	24	0
73	$j^6+19j^5+18j^4+34j^3+31j^2+67j+7$	$9, 56, 39\pm 5\sqrt{5}, 8\pm 37\sqrt{5}$	*	*
79	$j^6+55j^5+57j^4+63j^3+j^2+25j+10$	$15,\ 17,\ 21,\ 64.\ 72\pm 38\sqrt{3}$	69	*
83	$j^6+11j^5+62j^4+81j^3+81j^2+72j+43$	$17,\ 28,\ 50,\ 67,\ 38\pm 35\sqrt{2}$	68	0
89	$j^7+60j^6+86j^5+37j^4+22j^3+23j^2+79j+42$	$6, 7, 13, 52, 66, 76+39\sqrt{3}$	*	0
97	$j^8+60j^7+10j^6+96j^5+2j^4+74j^3+3j^2+69j+78$	$1,\ 20,\ 45\pm 28\sqrt{5}$, $76\pm 3\sqrt{5},\ 81\pm 22\sqrt{5}$	*	*

Als allgemeines Ergebnis der vorstehenden Betrachtungen halten wir fest:

Es gibt zu jedem Typus von Maximalordnungen in $Q_{\infty,p}$ supersinguläre Invarianten modulo p.

Denn da es überhaupt einen supersingulären Körper K modulo p gibt, so gibt es unter dessen Teilkörpern solche mit einer vorgegebenen Maximalordnung von $Q_{\infty,p}$ als Multiplikatorenring.

§ 9. Existenz der singulären Invarianten.

1. Die Existenz singulärer Invarianten der Charakteristik 0, und zwar zu jeder Ordnung in einem vorgegebenen imaginären quadratischen Zahlkörper von gerade so vielen, wie die Klassenzahl dieser Ordnung angibt, ist bekanntlich eine ganz einfache Folge aus der analytischen Theorie der elliptischen Funktionen. Da diese singulären Invarianten ganze algebraische Zahlen sind, so können daraus nach § 4, **2.**, **3.** durch Reduktion nach Primidealen des von ihnen erzeugten Zahlkörpers singuläre Invarianten von Primzahlcharakteristik p gewonnen werden, und zwar, wie wir uns leicht überzeugen, zu jeder Ordnung mit nicht durch p

teilbarem Führer eines vorgegebenen imaginären quadratischen Zahlkörpers so viele wie die Klassenzahl der Ordnung angibt.

Es bleibt aber offen, ob es nicht noch weitere gibt, die nicht durch Reduktion erhalten werden können. Um dies zu entscheiden und alles auf algebraischem Wege herzuleiten, brauchen wir den folgenden Hilfssatz:

Wenn der Körper K_0 der Primzahlcharakteristik p einen Multiplikator $\bar{\mu}$ hat, so läßt er sich durch Reduktion modulo einem Primteiler $\mathfrak{p}$ *von p aus einem Körper K_0 der Charakteristik* 0 *gewinnen, von dessen Multiplikatoren einer in den vorgegebenen Multiplikator $\bar{\mu}$ von $\bar{K}_0$ übergeht.*

Er erlaubt uns, von dem im vorigen Abschnitt aufgestellten supersingulären Invarianten modulo p zu den singulären Invarianten der Charakteristik 0 und dann von da zu den singulären Invarianten modulo p zu gelangen.

Beweis des Hilfssatzes. Wir können von vornherein annehmen, daß $\bar{\mu}$ komplex ist, denn für rationales $\bar{\mu}$ ist der Satz selbstverständlich. Weiter können wir annehmen, daß die Norm n von $\bar{\mu}$ nicht durch p teilbar und daß $\bar{\mu}$ kein Vielfaches eines rationalen Multiplikators m ist, denn wir können $\bar{\mu}$ durch $m^{-1}\bar{\mu}$ oder $m^{-1}\bar{\mu}+1$ ersetzen. $\bar{K}_0$ ist also zyklisch von nicht durch p teilbarem Grade n über $\bar{K}_0^{\bar{\mu}}$, wenn wir den Konstantenkörper als hinreichend großes Galoisfeld annehmen. Σ sei ein endlicher algebraischer Zahlkörper über den wir noch verfügen werden. Zu Σ adjungieren wir eine Unbestimmte j und eine Wurzel λ von

$$2^8(1-\lambda(1-\lambda))^3 = j\lambda^2(1-\lambda)^2$$

oder eine Wurzel α von

$$\alpha^3(\alpha^8+24)^3+j(\alpha^3+27) = 0$$

je nachdem $p \neq 2$ oder $p \neq 3$ ist. Über dem Konstantenkörper $\Sigma(j, \lambda)$ oder $\Sigma(j, \alpha)$ bilden wir durch die definierende Gleichung

$$y^2 = x(x-1)(x-\lambda)$$

oder

$$y^2 - y + \alpha x y. = x^3$$

einen elliptischen Körper $\Sigma(j, \lambda; x, y)$ oder $\Sigma(j, \alpha; x, y)$ mit der Invariante j. Wir erweitern den Konstantenkörper $\Sigma(j, \lambda)$ oder $\Sigma(j, \alpha)$ endlich algebraisch zu einem Körper k derart, daß in $k(x, y) = K\ \mu(n)$ Teilkörper $K_1, \cdots, K_{\mu(n)}$ enthalten sind, über denen K zyklisch unverzweigt vom Grade n ist; die Invarianten dieser Körper sind die Wurzeln

$j_1, \cdots, j_{\mu(n)}$ der Invariantengleichung n-ter Ordnung $\Phi_n(t, j) = 0$. Die j_i liegen daher in k, wir wollen außerdem annehmen, daß für jedes i alle Wurzeln $\lambda_i^{(h)}$ der Gleichung

$$2^8(1 - \lambda_i(1 - \lambda_i))^3 = j_i \lambda_i^2 (1 - \lambda)_i^2$$

oder alle Wurzeln $\alpha_i^{(h)}$ der Gleichung

$$\alpha_i^3(\alpha_i^3 + 24)^3 + j_i(\alpha_i^3 + 27) = 0$$

in k enthalten sind.

Die zu einem in p aufgehenden Primideal von Σ gehörende Bewertung dehnen wir hinsichtlich j auf $\Sigma(j)$ aus und verstehen unter $\mathfrak{p}$ einen ihrer Primteiler in k. Die Restklassenbildung modulo $\mathfrak{p}$ bezeichnen wir durch überstreichen. $\mathfrak{p}$ wird hinsichtlich x auf $k(x)$ übertragen, da $\bar{\lambda}$ über $\bar{\Sigma}$ transzendent ist, so bleibt $\mathfrak{p}$ in K prim und $\bar{K} = \bar{k}(x, \bar{y})$ ist elliptisch mit der absolut transzendenten Invariante $\bar{j}$ über dem Konstantenkörper $\bar{k}$. $K_1, \cdots, K_{\mu(n)}$ gehen modulo $\mathfrak{p}$ in die entsprechenden Teilkörper $\bar{K}_1, \cdots, \bar{K}_{\mu(n)}$ von $\bar{K}$ mit den Invarianten $\bar{j}_1, \cdots, \bar{j}_{\mu(n)}$ über.

Wir kehren zu dem gegebenen Körper $\bar{K}_0$ der Charakteristik p zurück. $\bar{j}_0$ sei seine Invariante und $\bar{\lambda}_0$ eine Wurzel der Gleichung

$$2^8(1 - \bar{\lambda}_0(1 - \bar{\lambda}_0))^3 = \bar{j}_0 \bar{\lambda}_0^2 (1 - \bar{\lambda}_0)^2$$

oder $\bar{\alpha}_0$ eine Wurzel der Gleichung

$$\bar{\alpha}_0^3(\bar{\alpha}_0^3 + 24)^3 + \bar{j}_0(\bar{\alpha}_0^3 + 27) = 0.$$

Wir wählen nun den Körper Σ so, daß er eine Zahl $\lambda_0(\alpha_0)$ enthält, deren Rest modulo $\mathfrak{p}$ mit diesem $\bar{\lambda}_0(\bar{\alpha}_0)$ identifiziert werden kann. Außerdem verlangen wir von Σ, daß die Divisoren der ganzen algebraischen Funktionen $j - j_0$ und $\lambda - \lambda_i^{(h)}$, $i = 1, \cdots, \mu(n)$; $h = 1, \cdots, 6$ oder $\alpha - \alpha_i^{(h)}$, $i = 1, \cdots, \mu(n)$; $h = 1, \cdots, 12$ von j im Zähler nur Primdivisoren ersten Grades haben. k_j sei der Ring der ganzen algebraischen Funktionen von j in k. $\bar{k}_j$ besteht dann aus ganzen algebraischen Funktionen von $\bar{j}$, möglicherweise aber nicht aus allen, die in $\bar{k}$ enthalten sind, was die nachfolgenden Überlegungen ein wenig umständlicher macht.

$\wp$ sei ein in $\bar{j} - j_0$ aufgehendes Primideal von k_j. Es gibt wenigstens einen Primdivisor von $\bar{k}$ mit der Eigenschaft, daß alle durch ihn teilbaren Elemente von $\bar{k}_j$ das Primideal $\wp$ bilden, wir bezeichnen ihn

ebenfalls mit $\bar{\wp}$. K geht dann modulo $\bar{\wp}$ in einen Körper mit der vorgegebenen Invariante $\bar{j}_0$ über, wir können, da es auf den genauen Konstantenkörper nicht ankommt, annehmen, daß es der gegebene Körper $\bar{K}_0$ ist. Wird Σ hinreichend groß gewählt, so ist der vorgegebene Multiplikator $\bar{\mu}$ in $\bar{K}_0$ möglich. $\bar{K}_0^{\bar{\mu}}$ muß sich bei der Reduktion modulo $\bar{\wp}$ aus einem der Körper $\bar{K}_i$ ergeben, etwa aus $\bar{K}_1$.

Das erzeugende Elementepaar $\bar{x}$, $\bar{y}$ von $\bar{K}$ mit

$$\bar{y}^2 = \bar{x}(\bar{x}-1)(\bar{x}-\bar{\lambda}) \qquad \left[\bar{y}^2 - \bar{y} + \bar{\alpha}\,\bar{x}\,\bar{y} = \bar{x}^3\right]$$

geht modulo $\bar{\wp}$ in ein erzeugendes Elementepaar $\bar{x}_0$, $\bar{y}_0$ von $\bar{K}_0$ mit

$$\bar{y}_0^2 = \bar{x}_0(\bar{x}_0-1)(\bar{x}_0-\bar{\lambda}_0) \qquad \left[\bar{y}_0^2 - y_0 + \bar{\alpha}_0 x_0 y_0 = x_0^3\right]$$

über. Das erzeugende Elementepaar $\bar{x}_0^{\bar{\mu}}$, $\bar{y}_0^{\bar{\mu}}$ von $\bar{K}_0^{\bar{\mu}}$ mit

$$\bar{y}_0^{\bar{\mu}2} = \bar{x}_0^{\bar{\mu}}(\bar{x}_0^{\bar{\mu}}-1)(\bar{x}_0^{\bar{\mu}}-\bar{\lambda}_0), \qquad \left[\bar{y}_0^{\bar{\mu}2} - \bar{y}_0^{\bar{\mu}} + \bar{\alpha}_0\,\bar{x}_0^{\bar{\mu}}\,\bar{y}_0^{\bar{\mu}} = \bar{x}_0^{\bar{\mu}}\right]$$

ergibt sich nach § 4 **3.** aus einem erzeugenden Elementepaar $\bar{x}_1$, $\bar{y}_1$ von $\bar{K}_1$ mit

$$\bar{y}_1^2 = \bar{x}_1(\bar{x}_1-1)(\bar{x}_1-\bar{\lambda}_1), \qquad \left[\bar{y}_1^2 - \bar{y}_1 + \bar{\alpha}_1 x_1 y_1 = \bar{x}_1^3\right],$$

wo $\lambda_1(\alpha_1)$ eine gewisse Wurzel von

$$2^8(1-\bar{\lambda}_1(1-\bar{\lambda}_1))^3 = \bar{j}_1\,\bar{\lambda}_1^2(1-\bar{\lambda}_1)^2$$

$$\left[\text{von } \bar{\alpha}_1^3(\bar{\alpha}_1^3+24)^3 + \bar{j}_1(\bar{\alpha}_1^3+27) = 0\right]$$

ist, die der Kongruenz

$$\bar{\lambda}_1 \equiv \bar{\lambda} \bmod \bar{\wp} \quad (\bar{\alpha}_1 \equiv \bar{\alpha} \bmod \bar{\wp})$$

genügt, etwa $\lambda_1^{(1)}(\alpha_1^{(1)})$. Weiter sind nach § 4 **3.** $\bar{x}_1$, $\bar{y}_1$ die $\mathfrak{p}$-Reste eines erzeugenden Elementepaares x_1, y_1 von K_1 mit

$$y_1^2 = x_1(x_1-1)(x_1-\lambda_1) \qquad (y_1^2 - y_1 + \alpha_1 x_1 y_1 = x_1^3).$$

Es finden also die folgenden Übergänge statt

$$x,\ y,\ \lambda(\alpha) \text{ modulo } \mathfrak{p} \text{ in } \bar{x},\ \bar{y},\ \bar{\lambda}(\bar{\alpha}) \xrightarrow{} \text{modulo } \bar{\wp} \text{ in } \bar{x}_0,\ \bar{y}_0,\ \bar{\lambda}_0(\bar{\alpha}_0),$$

$$\downarrow$$

$$x_1, y_1, \lambda_1(\alpha_1) \text{ modulo } \mathfrak{p} \text{ in } \bar{x}_1,\ \bar{y}_1,\ \bar{\lambda}_1(\bar{\alpha}_1) \xleftarrow{} \text{modulo } \bar{\wp} \text{ in } \bar{x}_0^{\bar{\mu}},\ \bar{y}_0^{\bar{\mu}},\ \bar{\lambda}_0(\bar{\alpha}_0).$$

Die Pfeile geben die Reihenfolge an, in der diese Tripel eines aus dem anderen gewonnen wurden.

Wir werden weiter unten zeigen, daß es ein in $\lambda - \lambda_1$ $(\alpha - \alpha_1)$ aufgehendes Primideal $\wp$ von k_j gibt, das modulo $\mathfrak{p}$ in das Primideal $\bar{\wp}$ von $\bar{k}_j$ übergeht. Den zugehörigen Primdivisor $\wp$ dehnen wir hinsichtlich x auf K aus, K geht dann modulo $\wp$ in einen Körper $K_0 = k_0(x_0, y_0)$ über; wir bezeichnen die Reduktion modulo $\wp$ durch Anhängen eines Index 0. K_0 hat einen durch $x_0 \to x_{10}$, $y_0 \to y_{10}$ gegebenen Multiplikator μ, da ja $\lambda_0 = \lambda_{10}$ ist. Zufolge der Vertauschungsregel (12), § 4 **2.** gehen x, y mod $\mathfrak{p}$ in x_0, y_0 und x_{10}, y_{10} in $x_0^{\bar{\mu}}$, $y_0^{\bar{\mu}}$ über. Dem μ entspricht folglich bei der Reduktion der gegebene Multiplikator $\bar{\mu}$ von K_0.

Es bleibt noch die Behauptung über $\bar{\wp}$ und $\wp$ zu beweisen, wir untersuchen zu diesem Zweck etwas allgemeiner, wie sich die Ideale von $\bar{k}_j$ zu denen von k_j verhalten.

Für jedes Ideal $\mathfrak{a}$ von k_j ist die Menge $\bar{\mathfrak{a}}$ der Reste modulo $\mathfrak{p}$ von $\mathfrak{p}$-ganzen in $\mathfrak{a}$ enthaltenen Elementen ein Ideal von $\bar{k}_j$.

Für zwei Ideale $\mathfrak{a}$ und $\mathfrak{b}$ gilt offenbar

$$\mathfrak{a}\mathfrak{b} \supseteq \bar{\mathfrak{a}} \cdot \mathfrak{b}$$

$$\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b},$$

und $\mathfrak{a} \subseteq \mathfrak{b}$, wenn $\mathfrak{a} \subseteq \mathfrak{b}$.

Aus der Primfaktorzerlegung

$$\mathfrak{a} = \wp_1^{e_1} \cdot \ldots \cdot \wp_h^{e_h}$$

eines Ideals von k_j folgt also

$$\wp_1^{e_1} \bar{\wp}_2^{e_2} \cdots \wp_h^{e_h} \subseteq \bar{\mathfrak{a}} \subseteq \bar{\wp}_1^{e_1} \cap \cdots \cap \bar{\wp}_h^{e_h}.$$

Ein Primidealteiler $\bar{\wp}$ von $\bar{\mathfrak{a}}$ geht daher in einem der Ideale $\bar{\wp}_i^{e_i}$, wegen $\wp_i^{e_i} \supseteq \bar{\wp}_i^{e_i}$ also in einem der Ideale $\bar{\wp}_i$ auf. Andererseits geht ein Primidealteiler $\bar{\wp}$ von $\bar{\wp}_i$ in $\bar{\wp}_i^{e_i}$ und daher in $\bar{\mathfrak{a}}$ auf. Die Primidealteiler von $\bar{\mathfrak{a}}$ sind also genau die der $\bar{\wp}_i$.

Wir zeigen nun, daß für ein Primideal ersten Grades $\wp$ entweder $\bar{\wp} = \bar{k}_j$ oder wieder ein Primideal ersten Grades von $\bar{k}_j$ ist, so daß, wenn wie oben für $\mathfrak{a} = (\lambda - \lambda_1)$, $\mathfrak{a}$ nur Primfaktoren ersten Grades enthält, jeder Primfaktor $\bar{\wp}$ von $\bar{\mathfrak{a}}$ aus einem Primfaktor $\wp$ von $\mathfrak{a}$ hervorgeht und den Grad 1 hat. Wir betrachten zu jedem $\mathfrak{p}$-ganzen z aus k_j seinen konstanten Rest ζ modulo $\wp$. Wenn für ein solches z der Rest ζ nicht $\mathfrak{p}$-ganz ist, so ist $\bar{\wp} = k_j$, denn es wird $1 - z/\zeta \equiv 0 \bmod \wp$, also wegen $\overline{z/\zeta} = 0$, $1 \equiv 0 \bmod \bar{\wp}$. Wenn $\bar{\wp}$ nicht gleich k_j wird, so sind

alle ζ $\mathfrak{p}$-ganz und aus $z \equiv \zeta \bmod \varphi$ folgt $\bar{z} \equiv \bar{\zeta} \bmod \bar{\varphi}$, $\bar{\varphi}$ ist daher ein Primideal ersten Grades.

3. *Zu jeder imaginär quadratischen Zahlkörperordnung* $\mathbf{R}$ *gibt es singuläre Invarianten der Charakteristik* 0, *denen dies* $\mathbf{R}$ *als Multiplikatorenring zugeordnet ist.*

Beweis. Es genügt, einen elliptischen Körper K_0 der Charakteristik 0 anzugeben, dessen Multiplikatorenring $\mathbf{R}_0$ den gleichen Quotientenkörper Σ hat wie das vorgegebene $\mathbf{R}$. Denn sei für jede Primzahl q $(\omega_{01}(q), \omega_{02}(q))$ eine Basis von $\mathbf{R}_{0_q}$, welche die Darstellung $S_q(\mu)$ (§ 2 **5.**) von $\mathbf{R}_0$ vermittelt und C_q eine ganze q-adische Matrix, welche sie in eine Basis $\omega_1(q)$, $\omega_2(q)$ eines Moduls der Ordnung $\mathbf{R}_q$ transformiert. Diese Matrizen C_q können fast alle unimodular gewählt werden, sie legen dann nach § 2 **6.** einen Teilkörper K von K_0 fest, dessen Multiplikatorenring $\mathbf{R}$ ist.

Es sei p eine Primzahl, die in Σ prim bleibt. $Q_{\infty,p}$ enthält dann einen zu Σ isomorphen Teilkörper, der Multiplikatorenring eines Körpers $\bar{K}$ der Charakteristik p mit supersingulärer Invariante also ein Element $\bar{\mu}$, das diesen Körper erzeugt. Nach dem in **2.** bewiesenen Hilfssatz kann $\bar{K}$ durch Reduktion modulo einem in p aufgehenden Primdivisor aus einem Körper K der Charakteristik 0 gewonnen werden, von dem ein Multiplikator μ in $\bar{\mu}$ übergeht. μ genügt aber derselben quadratischen Gleichung wie $\bar{\mu}$ und erzeugt daher Σ, womit alles bewiesen ist.

Σ sei ein imaginärer quadratischer Zahlkörper, in dem die Primzahl p in zwei verschiedene Primideale zerfällt, und $\mathbf{R}$ *eine Ordnung von Σ, deren Führer nicht durch p teilbar ist. Es gibt singuläre Invarianten der Charakteristik p, zu denen der Multiplikatorenring* $\mathbf{R}$ *gehört.*

Beweis. Wir gehen von einem Körper K_0 der Charakteristik 0 aus, dessen Multiplikatorenring $\mathbf{R}_0$ den Quotientenkörper Σ hat. Da seine Invariante j eine ganze algebraische Zahl ist, so können wir als Konstantenkörper einen endlichen algebraischen Zahlkörper nehmen, und wenn wir, eine passende Veränderliche x zugrunde legend, einen Primfaktor von p in diesem Zahlkörper auf K übertragen, so erhalten wir nach § 4 **3.** durch Reduktion nach diesem Primfaktor einen elliptischen Körper $\bar{K}$ der Charakteristik p mit der Invariante $\bar{j}$, dessen Multiplikatorenring $\mathbf{R}_{00}$ eine Ordnung von Σ ist. Wie oben nehmen wir zu jeder Primzahl $q \neq p$ eine ganze q-adische Matrix C_q, die eine die Darstellung S_q von $\mathbf{R}_{00}$ vermittelnde Basis $(\omega_1(q), \omega_2(q))$ von $\mathbf{R}_{00q}$ in eine Basis eines Moduls von $\mathbf{R}_q$ transformiert. Nach § 2 **6.** legen sie zusammen mit beliebigen c_p und $I(K_0 : K)$ einen Teilkörper K von K_0 mit dem Multiplikatorenring $\mathbf{R}$ fest.

4. Wir bemerken zum Schluß noch, daß es für jede Charakteristik auch elliptische Körper gibt, die nur rationale Multiplikatoren haben solche mit absolut transzendenter Invariante.

§ 10. Die vollständigen singulären Invariantensysteme. Klassenzahlrelationen.

1. Wir wollen die Beziehungen untersuchen, die zwischen singulären Invarianten mit Multiplikatorenringen gleichen Quotientenkörpers bestehen.

Zuerst betrachten wir einen elliptischen Körper K, dessen Multiplikatorenring $\mathfrak{R}$ eine Ordnung in dem imaginären quadratischen Zahlkörper Σ ist. Wenn die Charakteristik p von K nicht 0 ist, so zerfällt sie in Σ in zwei verschiedene Primideale $\mathfrak{p}_1$ und $\mathfrak{p}_2$. Ist $\mathfrak{a}$ ein Ideal von $\mathfrak{R}$, so hat $K^{\mathfrak{a}}$ die Ordnung $\mathfrak{R}_1$ von $\mathfrak{a}$ als Multiplikatorenring (§ 2 **2.**, **9.**). Zu Teilkörpern $K^{\mathfrak{a}}$ mit dem gleichen Multiplikatorenring $\mathfrak{R}$ wie K führen also die *eigentlichen* Ideale von $\mathfrak{R}$, die die Ordnung $\mathfrak{R}$ haben. Zwei von ihnen, $K^{\mathfrak{a}_1}$ und $K^{\mathfrak{a}_2}$, sind genau dann isomorph, haben also die gleiche Invariante, wenn $\mathfrak{a}_1$ und $\mathfrak{a}_2$ äquivalent sind. *Es gibt daher unter den Teilkörpern K genau soviel nichtisomorphe wie Idealklassen in* $\mathfrak{R}$, wenn wir noch beweisen, daß jeder Teilkörper K_0 von K, dessen Multiplikatorenring gleich $\mathfrak{R}$ ist, in der Gestalt $K_0 = K^{\mathfrak{a}}$ mit einem Ideal $\mathfrak{a}$ von R geschrieben werden kann. *Es erscheint dann jeder Idealklasse von* $\mathfrak{R}$ *eine singuläre Invariante zugeordnet.* Um $K_0 = K^{\mathfrak{a}}$ zu zeigen, betrachten wir für jedes $q \neq p$ die zu K gehörige Darstellung S_q von Σ (§ 2 **5.**) und die zu K_0 gehörigen Matrizen C_q, außerdem für $p \neq 0$ die Darstellung s_p und das zu K_0 gehörige c_p. $\omega_1(q), \omega_2(q)$ sei eine Basis von $\mathfrak{R}_q$, die S_q vermittelt. $(\omega_1(q), \omega_2(q))C_q$ muß dann Basis eines Moduls $\mathfrak{a}_q$ der Ordnung $\mathfrak{R}_q$ sein (§ 2 **7.**). Für $p \neq 0$ setzen wir weiter, wenn s_p die $\mathfrak{p}_1$-adische Darstellung von Σ ist und K den Inseparabilitätsgrad p^f über K_0 hat, $\mathfrak{a}_p = \mathfrak{R}_p \mathfrak{p}_1^h \mathfrak{p}_2^f$, wo h den Exponenten der in c_p enthaltenen Potenz von p bedeutet. $\mathfrak{a}_q$ ist nur für endlich viele q nicht gleich $\mathfrak{R}_q$ und daher gibt es ein Ideal $\mathfrak{a}$ von $\mathfrak{R}$, dessen q-adische Komponenten diese $\mathfrak{a}_q$ sind. Wir zeigen $K_0 = K^{\mathfrak{a}}$. Zunächst stimmen die Inseparabilitätsgrade $I(K : K_0)$ und $I(K : K^{\mathfrak{a}})$ überein, sie sind beide gleich p^f. Da ferner sowohl die in $(K : K_0)$ als auch die in $(K : K^{\mathfrak{a}})$ enthaltene Potenz von p gleich $p^{h \cdot f}$ ist, so stimmen auch die in den Separabilitätsgraden von K über K_0 und von K über $K^{\mathfrak{a}}$ enthaltenen Potenzen von p überein. Schließlich haben nach § 2 **9.** die Matrizen C_q für $K^{\mathfrak{a}}$ die gleiche Bedeutung wie für K_0. Daher ist nach § 2 **6.** in der Tat $K^{\mathfrak{a}} = K_0$.

Wir wollen die Gesamtheit aller Invarianten der Teilkörper von K ein *vollständiges singuläres Invariantensystem zum Körper* Σ nennen. In ihm gibt es zu jeder Klasse einer Ordnung von Σ eine Invariante, also soviel Invarianten, zu denen diese Ordnung als Multiplikatorenring gehört, wie Klassen in der Ordnung. Die Existenz *eines* vollständigen Invariantensystems zu Σ haben wir bewiesen. Es könnte aber mehrere geben.

2. Entsprechende Überlegungen können wir für die supersingulären Invarianten der Charakteristik p anstellen. K sei ein elliptischer Körper der Charakteristik p, dessen Multiplikatorenring $\mathfrak{R}_i$ eine Maximalordnung von $Q_{\infty,p}$ ist. Ist $\mathfrak{a}_{ih}$ ein Linksideal von $\mathfrak{R}_i$, so ist der Multiplikatorenring von $K^{\mathfrak{a}_{ih}}$ die Rechtsordnung $\mathfrak{R}_h$ von $\mathfrak{a}_{ih}$. Da zwei Körper $K^{\mathfrak{a}_{ih}}$ und $K^{\mathfrak{a}_{il}}$ genau dann isomorph sind, wenn $\mathfrak{a}_{ih}$ und $\mathfrak{a}_{il}$ äquivalent sind, so gibt es unter den Teilkörpern von K genau soviel nichtisomorphe, wie Idealklassen in $Q_{\infty,p}$. Ebenso groß ist die Anzahl der supersingulären Invarianten der Charakteristik p, soweit sie bei den Teilkörpern von K überhaupt vorkommen. Wir wollen ihre Gesamtheit wieder ein *vollständiges System von supersingulären Invarianten der Charakteristik* p nennen.

Zu zwei supersingulären Invarianten j_1 und j_2 des vollständigen Systems gehören genau dann isomorphe Multiplikatorenringe $\mathfrak{R}_{h_1}$ und $\mathfrak{R}_{h_2}$, wenn die zugehörigen Körper $K^{\mathfrak{a}_{ih_1}}$ und $K^{\mathfrak{a}_{ih_2}}$ in einer Beziehung $\mathfrak{a}_{ih_2} = \mathfrak{c}_{ii}\,\mathfrak{a}_{ih_1}\,\gamma$ stehen, $\mathfrak{c}_{ii}$ zweiseitiges Ideal von $\mathfrak{R}_i$, denn genau dann haben $\mathfrak{a}_{ih_1}$ und $\mathfrak{a}_{ih_2}$ isomorphe (oder zum gleichen Typus gehörige) Rechtsordnungen $\mathfrak{R}_{h_1}$ und $\mathfrak{R}_{h_2}$[27]). Statt $\mathfrak{a}_{ih_2} = \mathfrak{c}_{ii}\,\mathfrak{a}_{ih_1}\,\gamma$ können wir auch $\mathfrak{a}_{ih_2} = \mathfrak{a}_{ih_1}\,\mathfrak{c}_{h_1h_1}\,\gamma$ schreiben. $\mathfrak{p}_{h_1h_1}$ sei das zweiseitige Primideal von $\mathfrak{R}_{h_1}$, dessen Quadrat p ist. Ein zweiseitiges Ideal von $\mathfrak{R}_{h_1}$ ist dann entweder gleich $\mathfrak{R}_{h_1}\,n$ oder gleich $\mathfrak{p}_{h_1h_1}\,n$, unter n eine rationale Zahl verstanden. *Mithin gibt es ein oder zwei supersinguläre Invarianten in dem vollständigen System, deren zugeordnete Multiplikatorenringe vom gleichen Typus sind, je nachdem* $\mathfrak{p}$ *in diesem Typus Hauptideal ist oder nicht. Im ersten Fall ist die Invariante offenbar rational, im zweiten sind die beiden Invarianten vom Grade zwei und zueinander konjugiert.* Daß beide Fälle vorkommen, zeigt die Tabelle (65).

3. *Es gibt zu jedem möglichen Quotientenbereich* Σ *nur ein vollständiges singuläres oder supersinguläres Invariantensystem.*

Beweis. Wir betrachten zuerst den Fall $\Sigma = Q_{\infty,p}$. Die Anzahl aller supersingulären Invarianten der Charakteristik p ist nach **2.** ein Vielfaches der Klassenzahl von $Q_{\infty,p}$. Die von EICHLER[28]) berechnete Klassenzahl von $Q_{\infty,p}$,

[27]) Vgl. M. DEURING, Algebren, Ergebn. der Math. IV,1, S. 89.

[28]) M. EICHLER, Über die Idealklassenzahl total definierter Quaternionenalgebren, Math. Zeitschr. **43**, S. 102–109 (1937).

$$(66)\qquad \begin{aligned} &\frac{p-1}{12} && \text{für } p \equiv 1 \bmod 12,\\ &\frac{p-5}{12}+1 && \text{für } p \equiv 5 \bmod 12,\\ &\frac{p-7}{12}+1 && \text{für } p \equiv 7 \bmod 12,\\ &\frac{p-11}{12}+2 && \text{für } p \equiv 11 \bmod 12, \end{aligned}$$

stimmt aber nach (63) mit der Anzahl aller supersingulären Invarianten der Charakteristik p überhaupt überein, wenn wir annehmen, daß das Polynom $P(j)$ lauter verschiedene Wurzeln hat. *Damit ist die Einzigkeit des vollständigen Invariantensystems bewiesen, und zugleich, daß $P(j)$ in der Tat lauter verschiedene Wurzeln hat.* Dies unmittelbar dem Ausdruck (63) (oder auch (61) oder (64)) für $P(j)$ anzusehen scheint nicht leicht zu sein.

Wir wollen die Einzigkeit des supersingulären Invariantensystems für die Fälle $p \not\equiv 1 \bmod 12$ beweisen, ohne uns auf die Eichlersche Klassenzahlformel zu stützen. Für $p = 2$ und $p = 3$ haben wir schon in § 8 **2.** gezeigt, daß es nur eine supersinguläre Invariante gibt. Es sei jetzt $p \equiv 2 \bmod 3$. Da in diesem Falle $Q_{\infty,p}$ den Körper der dritten Einheitswurzeln enthält, so gibt es wenigstens eine Maximalordnung, in der dritte Einheitswurzeln liegen. Nach § 5 **2.** ist das nur für die Invariante $j = 0$ möglich. Durch *eine* Invariante ist aber das vollständige supersinguläre Invariantensystem bestimmt. Es gibt also nur eins. Ganz ebenso schließen wir für $p \equiv -1 \bmod 4$. In $Q_{\infty,p}$ gibt es eine Maximalordnung mit vierten Einheitswurzeln, zu der nach § 5 **2.** die Invariante $j = 2^6 3^3$ gehört und dadurch ist das vollständige System festgelegt. Die Primzahlen $p \equiv 1 \bmod 12$ entziehen sich dieser Schlußweise.

Wir betrachten daher zunächst den Fall der Charakteristik 0. Wenn wir uns auf die analytische Theorie stützen wollen, so ist natürlich nichts mehr zu beweisen. Verzichten wir darauf, so können wir folgendermaßen vorgehen. Σ sei der gegebene imaginäre quadratische Zahlkörper. S_1 und S_2 seien zwei vollständige Invariantensysteme zu Σ, die wir als gleich erkennen wollen. Wir betrachten nur die h Invarianten $j_{i,1} \cdots j_{i,h}$ des Systems S_i, die zur *Maximal*ordnung $\mathfrak{R}$ von Σ gehören. Wir betrachten einen elliptischen Körper K_1 der Invariante $j_{1,1}$ und einen Körper K_2 der Invariante $j_{2,1}$. Von den beiden gemeinsamen Konstantenkörper k setzen wir voraus, daß er den Körper Σ enthält, nach § 3 **3.** sind dann alle Multiplikatoren, die zu $j_{i,1}$ bei algebraisch abgeschlossenem Konstantenkörper gehören, schon in K_i möglich. q sei

eine Primzahl $\equiv 2 \bmod 3$, die in Σ prim bleibt, $\mathfrak{q}$ ein Primfaktor von q in k, und k der Restklassenkörper von k modulo $\mathfrak{q}$. $\overline{K^*}$ sei ein elliptischer Körper der Charakteristik 0 mit supersingulärer Invariante und dem Konstantenkörper k. Wir dehnen nach § 4 **3.** $\mathfrak{q}$ so auf K_i aus, daß K_i modulo $\mathfrak{q}$ in einen elliptischen Körper $\bar{K}_i$ der Invariante $j_{i,1}$ mit dem Konstantenkörper k übergeht. Nach § 4 **2.** und § 2 **10.** ist der Multiplikatorenring von K_i eine Maximalordnung $\bar{\mathfrak{R}}_i$ von $Q_{\infty,p}$, die einen zur Maximalordnung von Σ isomorphen Teilring $\bar{\mathfrak{o}}_i$ enthält.

Wegen der Einzigkeit des supersingulären Invariantensystems modulo q kann daher $\bar{K}_i$ isomorph auf einen Teilkörper $\overline{K_i^*}$ von $\overline{K^*}$ abgebildet werden, wobei k elementweise in sich übergehen soll. Es gibt ein Element ξ von $\mathfrak{R}_2$, das $\mathfrak{o}_2$ in $\mathfrak{o}_1$ transformiert, $\bar{\mathfrak{o}}_1 = \bar{\xi}^{-1}\bar{\mathfrak{o}}_2\bar{\xi}$. Der Multiplikatorenring $\bar{\xi}^{-1}\bar{\mathfrak{R}}_2\bar{\xi}$ von $K_2^{*\bar{\xi}}$ enthält dann ebenso wie $\bar{\mathfrak{R}}_1$ den Ring $\bar{\mathfrak{o}}_1$. Daraus folgt aber, daß es ein Ideal $\bar{\mathfrak{a}}$ von $\bar{\mathfrak{o}}_1$ gibt, für welches $\bar{\xi}^{-1}\bar{\mathfrak{R}}_2\bar{\xi} = \bar{\mathfrak{a}}^{-1}\bar{\mathfrak{R}}_1\bar{\mathfrak{a}}$ gilt[29]). $K_1^{\mathfrak{a}}$ geht modulo $\mathfrak{q}$ in einen Teilkörper $\bar{K}_1^{\mathfrak{a}}$ von $\bar{K}_1$ über, dessen Bild in $\overline{K_1^*}$, $\overline{K_1^{*\bar{\mathfrak{a}}}}$, die Maximalordnung $\bar{\mathfrak{a}}^{-1}\bar{\mathfrak{R}}_1\bar{\mathfrak{a}} = \bar{\xi}^{-1}\bar{\mathfrak{R}}_2\bar{\xi}$ als Multiplikatorenring hat. $\bar{K}_1^{\mathfrak{a}}$ hat daher die gleiche Invariante wie $\bar{K}_2$, und das bedeutet, daß eine Kongruenz

$$j_{2,1} \equiv j_{1,l(q)} \bmod \mathfrak{q}$$

besteht, wo $l(q)$ einen gewissen der Indizes $1, \cdots, h$ bezeichnet. Die Primzahlen q können nun gekennzeichnet werden als diejenigen Primzahlen, die in dem von Σ und $P(\sqrt{-3})$ verschiedenen quadratischen Teilkörper des biquadratischen Körpers $\Sigma(\sqrt{-3})$ in Primfaktoren ersten Grades aufspalten, welche ihrerseits in $\Sigma(\sqrt{-3})$ prim bleiben. Solcher Primzahlen q gibt es aber nach dem Bauerschen Satz[30]) unendlich viele. Für unendlich viele von ihnen hat $l(q)$ ein und denselben Wert l. Da $j_{2,1}$ nach unendlich viel verschiedenen Primidealen von k mit $j_{1,l}$ kongruent ist, so gilt $j_{2,1} = j_{1,l}$ und damit ist die Einzigkeit des vollständigen singulären Invariantensystems der Charakteristik 0 zum Körper Σ bewiesen.

Es bleibt jetzt noch zu zeigen, daß auch die singulären Invariantensysteme von Primzahlcharakteristiken und die supersingulären Invarianten von Charakteristiken $q \equiv 1 \bmod 12$ einzig sind. Wir greifen dazu aus

[29]) Vl. Kořínek, Maximale kommutative Körper in einfachen Systemen von hyperkomplexen Zahlen, Mém. Soc. Roy. Sci. Bohême 1932, S. 1—24 (1933); § 3, Satz 3.

[30]) Vgl. etwa M. Deuring, Neuer Beweis des Bauerschen Satzes, Journ. f. d. r. u. ang. Math.

zwei Invariantensystemen der Charakteristik q, die wir als gleich erkennen wollen, je eine, j_1 und j_2 heraus, wobei wir annehmen können, daß in dem zu j_1 gehörigen Multiplikatorenring $\mathfrak{R}_i$ ein Teilring $\mathfrak{o}_i$ enthalten ist, der zu der Maximalordnung $\mathfrak{o}$ eines gewissen imaginären quadratischen Zahlkörpers Σ isomorph ist. $1, \omega$ sei eine Basis von $\mathfrak{o}$. Nach dem Hilfssatz in **2** können wir $\bar{K}_i$ durch Reduktion modulo einem in q aufgehenden Primdivisor $\mathfrak{q}$ aus einem Körper K_i der Charakteristik 0 gewinnen, dessen Multiplikatorenring ω enthält, und daher die Maximalordnung von Σ ist. K_1 und K_2 sollen dabei einen endlichen algebraischen Zahlkörper k als gemeinsamen Konstantenkörper haben, der modulo $\mathfrak{q}$ in den gemeinsamen Konstantenkörper $\bar{k}$ von $\bar{K}_1$ und $\bar{K}_2$ übergeht. Wir können sogar, da es nur ein singuläres Invariantensystem der Charakteristik 0 zu Σ gibt, K_2 als Teilkörper von K_1 auffassen. Dadurch wird $\bar{K}_2$ zu einem Teilkörper von $\bar{K}_1$; $\bar{j}_1$ und $\bar{j}_2$ gehören folglich zu dem gleichen Invariantensystem, was zu beweisen war.

4. Nachdem die Einzigkeit der singulären Invariantensysteme der Charakteristik 0 bewiesen ist, können wir in der üblichen Weise die klassischen Klassenzahlrelationen von KRONECKER[31]) ableiten. Wir gehen darauf nicht weiter ein.

Wir können aber in ähnlicher Weise aus den singulären und supersingulären Invariantensystemen von Primzahlcharakteristik neue Klassenzahlrelationen ableiten. Vorher beweisen wir:

Jede absolut algebraische Invariante j einer Primzahlcharakteristik p ist singulär oder supersingulär.

Es sei $j^{p^f} = j$. Wenn j nicht supersingulär ist, so gilt für einen Körper K der Invariante j $\sigma = 1$. K ist zu seinem Teilkörper K^{p^f} isomorph (einen hinreichend großen Konstantenkörper vorausgesetzt), da er die gleiche Invariante hat. Mithin hat K einen Multiplikator π der Norm p^f, der aber keine Potenz von p sein kann, weil K^{p^e} wegen $\sigma = 1$ nicht rein inseparabel unter K ist. π ist daher komplex, womit der Satz bewiesen ist.

Nach § 3 **2.** gilt für eins der beiden Primideale, in die p im Multiplikatorenring $\mathfrak{R}$ von K zerfällt, etwa für $\mathfrak{p}_1$, $K^{\mathfrak{p}_1} = K^p$. Es ist dann $\mathfrak{p}_1^f = (\pi)$ Hauptideal in $\mathfrak{R}$. Wir können das auch anders ausdrücken: d sei die Diskriminante der Ordnung $\mathfrak{R}$. Wir betrachten die binären quadratischen Formen der Diskriminante d. $\mathfrak{p}_1^f =$ Hauptideal bedeutet, daß p^f eine *eigentliche* Darstellung durch die Hauptform der Diskriminante d gestattet, also durch $x^2 - y^2 d/4$ oder $x^2 + xy - y^2 (d-1)/4$, je nachdem $d \equiv 0$ oder $d \equiv 1 \bmod 4$ ist.

[31]) Vgl. etwa W. WEBER, Lehrbuch der Algebra III, S. 423.

Die Anzahl der singulären Invarianten j der Charakteristik p mit dem gleichen Multiplikatorenring ist gleich der Klassenzahl $h(d)$ von d.

Wir betrachten in ähnlicher Weise auch die supersingulären Invarianten j.

Wenn $j^p = j$ ist; so gibt es nach **2.** im zugehörigen Multiplikatorenring ein Element der Norm p, d. h. p ist durch die quaternäre Normenform der Diskriminante $-p^2$ des Multiplikatorenrings (eigentlich) darstellbar. Ist dagegen $j^p \neq j$, aber $j^{p^2} = j$, so ist p durch die Normenform nicht darstellbar, aber p^2. Im ersten Fall sind alle Potenzen von p durch die Normenform darstellbar, im zweiten nur die mit geradem Exponenten.

Überlegen wir nun, wie sich alle p^f Elemente des Galoisfeldes f-ten Grades auf die singulären und supersingulären Invarianten verteilen, so erhalten wir die folgende Klassenzahlrelation:

Es gilt

$$\sum h(d_{p^f}) + t_{p^f} = p^f. \tag{67}$$

Dabei durchläuft d_{p^f} alle nicht durch p teilbaren Diskriminanten definiter binärer quadratischer Formen, für die p^f durch die zugehörige Hauptform eigentlich darstellbar ist, und t_{p^f} bedeutet die Anzahl derjenigen Idealklassen einer gegebenen Maximalordnung $\mathfrak{R}$ *von $Q_{\infty,p}$, welche* $\mathfrak{R}$ *in solche Maximalordnungen transformieren, deren quaternäre Normenformen p^f darstellen.*

Nach **2.** können wir auch sagen:

Für gerades f ist t_{p^f} die durch (66) gegebene Klassenzahl von $Q_{\infty,p}$ und für ungerades f die Anzahl der Typen von Maximalordnungen von $Q_{\infty,p}$, in denen das in p aufgehende Primideal Hauptideal ist, deren Normenformen also p darstellen; oder auch

$$t_{p^2} = t_{p^4} = \cdots = h, \qquad t_p = t_{p^3} = \cdots = \frac{h+t}{2},$$

wo h die Klassen- und t die Typenzahl von $Q_{\infty,p}$ bedeutet.

§ 11. Kongruenzrelationen für die singulären Invarianten.

1. Der Übergang von elliptischen Körpern der Charakteristik 0 zu solchen von Primzahlcharakteristik, den wir schon wiederholt anwandten, ergibt bemerkenswerte Kongruenzrelationen zwischen den singulären Invarianten.

K sei ein elliptischer Körper der Charakteristik 0 mit singulärer Invariante j. Der Konstantenkörper sei ein endlicher algebraischer Zahlkörper k, von dem wir annehmen, daß er j und den imaginären quadratischen Zahlkörper Σ enthält, auf den der Quotientenkörper Σ des Multiplikatorenrings $\mathfrak{R}$ von K durch das ganze Differential von K

isomorph abgebildet wird (§ 3 **2.**). Alle Multiplikatoren sind dann in K möglich (§ 3 **3.**).

$\mathfrak{p}$ sei ein Primideal von k, das wir nach § 4 **3.** so auf K ausdehnen, daß K modulo $\mathfrak{p}$ in einen elliptischen Körper $\bar{K}$ der Invariante j mit dem Konstantenkörper k übergeht. Wir wollen untersuchen, wie der Multiplikatorenring von K mit dem von $\bar{K}$ zusammenhängt. Wir wollen uns in dieser Arbeit auf den Fall beschränken, daß die durch $\mathfrak{p}$ teilbare Primzahl p in Σ nicht voll zerfällt, so daß j supersingulär ist; der andere Fall ist einer weiteren Arbeit über die Klassenkörper der komplexen Multiplikation vorbehalten.

Wir behaupten: *Der Multiplikatorenring* $\bar{\mathbf{R}}$ *von* $\bar{K}$ *ist eine Maximalordnung von* $Q_{\infty,p}$, *die mit dem Körper* Σ *diejenige Ordnung gemeinsam hat, deren Führer aus dem Führer von* $\mathbf{R}$ *durch weglassen der in ihm enthaltenen Potenz von* p *entsteht.*

Zum Beweis brauchen wir nur zu beachten, daß nach § 4 **4.** die in § 2 **5.** eingeführte Darstellung $S_q(\mu)$ von Σ für $\bar{K}$ die gleiche Bedeutung hat wie für K, falls q eine von p verschiedene Primzahl ist; während also $\mathbf{R}$ der Durchschnitt aller q-adischen Hüllen $\mathbf{R}_q$ von $\mathbf{R}$ mit $\mathbf{R}_p$ ist, ist der in $\bar{\mathbf{R}}$ liegende Teil von Σ der Durchschnitt aller $\mathbf{R}_q$, soweit er aus p-ganzen Zahlen besteht und daher ist der Führer dieses Teils das Produkt der Führer aller $\mathbf{R}_q$, aber der von $\mathbf{R}$ das Produkt der Führer aller $\mathbf{R}_q$ mit dem von $\mathbf{R}_p$.

Betrachten wir zuerst den Fall $p = 2$. Da es nur die eine supersinguläre Invariante 0 gibt, so gilt:

Eine singuläre Invariante j *der Charakteristik* 0 *ist entweder durch keinen Primfaktor von* 2 *teilbar oder durch jeden, je nachdem* 2 *in dem zugehörigen imaginär quadratischen Körper* Σ *voll zerfällt oder nicht.*

Dies Ergebnis ist bemerkenswert, weil es mit einem von H. Weber auf merkwürdige Weise mittels der Kroneckerschen Grenzformel bewiesenen Satze in Zusammenhang steht. Dieser Satz[32]) heißt folgendermaßen: Es sei

$$f(\omega) = \frac{e^{-\frac{\pi i}{24}}\,\eta\left(\frac{\omega+1}{2}\right)}{\eta(\omega)},$$

wo

$$\eta(\omega) = e^{\frac{2\pi i}{24}} \prod_{n=1}^{\infty} \left(1 - e^{\frac{2\pi i n}{24}}\right)$$

die Dedekindsche η-Funktion bedeutet; durch f kann die absolute Invariante $j(\omega)$ folgendermaßen ausgedrückt werden:

$$j(\omega) = \frac{(f(\omega)^{24} - 16)^3}{f(\omega)^{24}}$$

[32]) W. Weber, Lehrbuch der Algebra III, S. 540/541.

$\omega = \omega_1/\omega_2$ sei der Quotient zweier Zahlen ω_1, ω_2, die die Basis eines Ideals irgendeiner Ordnung in einem imaginären quadratischen Zahlkörper Σ bilden, dann ist

$$f(\omega)/\sqrt{2}$$

eine Einheit, wenn 2 in Σ voll zerfällt, sonst ist erst das Produkt von $f(\omega)/\sqrt{2}$ mit einer gewissen Potenz von 2 mit positivem Exponenten eine Einheit.

Die Folgerung, die hieraus für $j(\omega)$ zu ziehen ist, ist offenbar der oben bewiesene Satz: $j(\omega)$ ist durch keinen Primfaktor von 2 teilbar oder durch jeden, je nachdem 2 in Σ voll zerfällt oder nicht.

Nur der erste Fall erfordert bei WEBER die transzendente Methode, im zweiten Fall kann die in $f(\omega)$ enthaltene Potenz von 2 auf algebraischem Wege bestimmt werden. Beschränkt man sich auf die entsprechende Frage für j, so kann das mittels der in § 6 **4.** berechneten Invariantengleichung zweiter Ordnung geschehen. Wir gehen nicht weiter darauf ein.

Ähnlich scharfe Aussagen wie für $p = 2$ erhalten wir für die übrigen Primzahlen, für die $Q_{\infty,p}$ nur eine Klasse hat, also für $p = 3$, 5, 7, 13. Für 3 und 5 lauten die Aussagen ganz entsprechend:

j ist durch keinen Primfaktor von 3 *oder* 5 *teilbar oder durch jeden, je nachdem* 3 (5) *in Σ voll zerfällt oder nicht.*

Ferner

$j - 2^6 3^3 \equiv j + 1$ ist durch keinen Primfaktor von 7 *teilbar oder durch jeden, je nachdem* 7 *in Σ voll zerfällt oder nicht.*

$j - 5$ ist durch keinen Primfaktor von 13 *teilbar oder durch jeden, je nachdem* 13 *in Σ voll zerfällt oder nicht.*

Für die übrigen p müßte genauer bekannt sein, wie sich die supersingulären Invarianten auf die verschiedenen Maximalordnungstypen verteilen, andererseits, in welchen Maximalordnungstypen eine gegebene Ordnung von Σ enthalten ist.

2. Beispiele.

$j(\sqrt{-1}) = 2^6 \cdot 3^3$ ist durch 2 und durch 3 teilbar, denn 2 und 3 werden in $P(\sqrt{-1})$ nicht voll zerlegt. $j - 5 \equiv 7 \bmod 13$ ist nicht durch 13 teilbar, 13 wird voll zerlegt. Aber $2^6 \cdot 3^3 - 2^6 \cdot 3^3 = 0$ ist durch 7 teilbar, denn 7 wird nicht voll zerlegt.

Überhaupt wird $2^6 \cdot 3^3$ für jede in $P(\sqrt{-1})$ nicht voll zerfallende Primzahl p supersingulär, da ja $p \equiv 7$ oder $11 \bmod 12$ ist.

Betrachten wir dagegen $j(\sqrt{-4}) = 2^3 \cdot 3^3 \cdot 11^3$, zum gleichen singulären System gehörig wie $j(\sqrt{-1})$. Wieder ist $j(\sqrt{-4})$ durch 2 und 3 teilbar. Weiter ist

$$2^3 \cdot 3^3 \cdot 11^3 - 2^6 \cdot 3^3 \equiv 2^3 \cdot 3^3 (1331 - 8) \equiv 0 \bmod 7,$$

aber

$$2^8 \cdot 3^8 \cdot 11^8 \equiv 0 \bmod 11,$$

für 11 kommt also eine andere supersinguläre Invariante heraus als bei $j(\sqrt{-1})$.

Ebenso für 19:

$$2^8 \cdot 3^8 \cdot 11^8 = 66^8 \equiv 9^8 = 9 \cdot 81 \equiv 9 \cdot 5 = 45 \equiv 7 \bmod 19.$$

23: $2^8 \cdot 3^8 \cdot 11^8 = 66^8 \equiv 20^8 \equiv -3^8 = -27 \equiv 19 \bmod 23.$

31: $2^8 \cdot 3^8 \cdot 11^8 = 66^8 \equiv 4^8 \equiv 2 \bmod 31.$

43: $2^8 \cdot 3^8 \cdot 11^8 = 66^8 \equiv -20^8 = -8000 \equiv 41 \bmod 43,$

47: $2^8 \cdot 3^8 \cdot 11^8 = 66^8 \equiv 44 \bmod 47.$

In $P(\sqrt{-3})$ mit $j(-\frac{1}{2}+\frac{1}{2}\sqrt{-3}) = 0$ zerfallen die Primzahlen $\equiv -1 \bmod 3$, also $\equiv 5, 11 \bmod 12$ nicht voll, für die in der Tat $j = 0$ supersingulär ist. Für $j(\sqrt{-3}) = 2^4 \cdot 3^8 \cdot 5^8$ haben wir

$$2^4 \cdot 3^8 \cdot 5^8 \equiv 0 \bmod 5, \quad \equiv 2^6 \cdot 3^8 \bmod 11, \quad \equiv 8 \bmod 17,$$
$$\equiv 19 \bmod 23, \quad \equiv 2 \bmod 29, \quad \equiv 3 \bmod 41, \quad \equiv 44 \bmod 47.$$

In $P(\sqrt{-5})$ mit $j(\sqrt{-5}) = 2^6 \cdot 5\sqrt{5}(16+7\sqrt{5})^3(9-4\sqrt{5})$ zerfallen 11, 13, 17, 19, 31, 37 nicht voll. Es wird

$$j(\sqrt{-5}) \equiv \begin{cases} 0, & \text{wenn } \sqrt{5} \equiv 4 \\ 1 \equiv 2^6 \cdot 3^8, & \text{wenn } \sqrt{5} \equiv -4 \end{cases} \bmod 11,$$

$$j(\sqrt{-5}) \equiv 5\sqrt{5}(3+7\sqrt{5})^3(4+4\sqrt{5})$$
$$\equiv 5\sqrt{5}(-4+6\sqrt{5})(4+4\sqrt{5})$$
$$\equiv \sqrt{5}(-2+3\sqrt{5})(1+\sqrt{5}) = \sqrt{5}(13+\sqrt{5}) \equiv 5 \bmod 13,$$

$$j(\sqrt{-5}) \equiv -3\sqrt{5}(-1+7\sqrt{5})^3(9-4\sqrt{5}) \equiv 8 \bmod 17,$$

$$j(\sqrt{-5}) \equiv \begin{cases} 2^6 \cdot 3^8 \\ 7 \end{cases} \bmod 19, \text{ je nachdem } \begin{matrix} \sqrt{5} \equiv 9 \\ \sqrt{5} \equiv -9 \end{matrix} \bmod 19,$$

$$j(\sqrt{-5}) \equiv \begin{cases} 2 \\ 4 \end{cases} \bmod 31, \text{ je nachdem } \begin{matrix} \sqrt{5} \equiv 6 \\ \sqrt{5} \equiv -6 \end{matrix} \bmod 31,$$

$$j(\sqrt{-5}) \equiv 3 \pm 2\sqrt{13} \bmod 37.$$