Teilbarkeitseigenschaften der singulären Moduln der elliptischen Funktionen und die Diskriminante der Klassengleichung.

Autor(en): **Deuring, Max**

Objekttyp: **Article**

Zeitschrift: **Commentarii Mathematici Helvetici**

Band (Jahr): **19 (1946-1947)**

PDF erstellt am: **10.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-17335

Teilbarkeitseigenschaften der singulären Moduln der elliptischen Funktionen und die Diskriminante der Klassengleichung

Andreas Speiser zum sechszigsten Geburtstage gewidmet.

Von Max Deuring, Göttingen

1. In der Arbeit: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper (Abhandl. Math. Semin. Hans. Univ. 14, 197—272 (1941), im folgenden mit T bezeichnet) habe ich Kongruenzrelationen für die singulären Moduln der elliptischen Funktionen aufgestellt, die aus der Theorie der supersingulären Invarianten entspringen. Auf ähnliche Weise können noch andere Teilbarkeitseigenschaften der singulären Moduln abgeleitet werden, die hier mitgeteilt seien. Es handelt sich allgemein um die Primfaktoren der Differenz irgend zweier singulärer Moduln $j(\alpha_1)$, $j(\alpha_2)$, wo die Zahlen α_1, α_2 imaginär quadratisch sind, aber nicht notwendig den gleichen quadratischen Körper zu erzeugen brauchen. Insbesondere können die Primzahlen, die in der Diskriminante D_Σ der Klassengleichung

$$f_\Sigma(t) = \prod_{\nu=1}^{h} \left(t - j(\mathfrak{k}_\nu)\right) = 0$$

eines imaginären quadratischen Zahlkörpers Σ aufgehen — $\mathfrak{k}_1, \ldots, \mathfrak{k}_h$ bezeichne die Idealklassen der Hauptordnung von Σ und $j(\mathfrak{k})$ in bekannter Weise den Wert der Modulfunktion $j(\omega)$ für den Quotienten $\omega = \frac{\alpha_1}{\alpha_2}$ der Basis α_1, α_2 eines Ideals $\mathfrak{a}$ der Klasse $\mathfrak{k}$ — folgendermaßen gekennzeichnet werden:

D_Σ ist nur durch Primzahlen p teilbar, die in Σ nicht in zwei verschiedene Primzahlen zerfallen.

$Q_{\infty, p}$ bezeichne die definite Quaternionenalgebra mit der Grundzahl $-p$, die also bei $\cdot p$ und ∞ verzweigt ist; Σ kann als Teilkörper von $Q_{\infty, p}$ aufgefaßt werden. *p geht genau dann in D^Σ auf, wenn es Nichthauptideale $\mathfrak{a}$ der Hauptordnung $\mathfrak{o}$ von Σ gibt, die in einer $\mathfrak{o}$ umfassenden Maximalordnung $\mathbf{R}$ von $Q_{\infty, p}$ zu Hauptidealen $\mathfrak{a}\mathbf{R} = \alpha\mathbf{R}$ werden.*

Die weiteren Ergebnisse sind von ähnlicher Art.

2. Wir setzen im folgenden den Inhalt der oben genannten Arbeit T voraus, müssen aber einige Ergänzungen dazu machen. In T wurde auf die Zuordnung der singulären Invarianten zu den Idealklassen der quadratischen Körper, die sich in der analytischen Theorie ganz von selbst ergibt, nur nebenbei eingegangen. Sie kann aber auch, wie wir jetzt zeigen wollen, rein algebraisch erklärt werden, was für das folgende wichtig ist.

K sei ein elliptischer Funktionenkörper, dessen Multiplikatorenring $\mathfrak{o}$ dem quadratischen Zahlkörper Σ angehöre. Die Invariante j von K ordnen wir irgendeiner beliebigen, aber von jetzt ab festen Idealklasse $\mathfrak{k}_0$ von $\mathfrak{o}$ zu und bezeichnen sie demgemäß mit $j(\mathfrak{k}_0)$. Ist dann $\mathfrak{k} = \mathfrak{k}_0 \cdot \mathfrak{k}_1^{-1}$ eine beliebige andere Klasse von $\mathfrak{o}$, so nehmen wir ein ganzes Ideal $\mathfrak{a}_1$ der Klasse $\mathfrak{k}_1$ und verstehen unter $j(\mathfrak{k})$ die Invariante des Teilkörpers $K^{\mathfrak{a}_1}$ von K. Diese Zuordnung $\mathfrak{k} \to j(\mathfrak{k})$ weicht von der aus der analytischen Theorie entspringenden nur um einen Automorphismus des Klassenkörpers $\Sigma(j(\mathfrak{k}))/\Sigma$ ab; mehr dürfen wir von einer algebraischen Theorie, die zwischen den über Σ konjugierten algebraischen Zahlen $j(\mathfrak{k}_1), j(\mathfrak{k}_2), \ldots$ nicht unterscheiden kann, auch gar nicht erwarten, und für unsere Zwecke macht diese Unbestimmtheit gar nichts aus. Wir bemerken ausdrücklich, daß die auf algebraische Weise erklärte Zuordnung $\mathfrak{k} \to j(\mathfrak{k})$ auch für Primzahlcharakteristiken sinnvoll ist, worauf es im folgenden gerade ankommt. Allerdings entspricht bei einer Primzahlcharakteristik im allgemeinen verschiedenen $\mathfrak{k}$ das gleiche j.

Wir müssen die Zuordnung $\mathfrak{k} \to j(\mathfrak{k})$ auch auf die Idealklassen der übrigen Ordnungen $\mathfrak{o}^*$ von Σ ausdehnen. Um wieder im Einklange mit der analytischen Theorie zu bleiben, gehen wir so vor: $\mathfrak{o}$ sei in der Ordnung $\mathfrak{o}'$ enthalten. Um $j(\mathfrak{k}')$ für eine Klasse $\mathfrak{k}'$ von $\mathfrak{o}'$ zu erklären, betrachten wir die Klasse $\mathfrak{k}_0'$ von $\mathfrak{o}'$, die der Klasse $\mathfrak{k}_0$ von $\mathfrak{o}$ entspricht, die also die mit $\mathfrak{o}'$ multiplizierten Ideale von $\mathfrak{k}_0$ enthält und ein Ideal $\mathfrak{a}_1'$ von $\mathfrak{k}_0'\mathfrak{k}'^{-1}$; $j(\mathfrak{k}')$ soll dann die Invariante von $K^{\mathfrak{a}_1'}$ sein. Für $\mathfrak{o}' = \mathfrak{o}$ fällt diese Erklärung mit der oben gegebenen zusammen.

Wenn mehrere Ordnungen von Σ gleichzeitig betrachtet werden, so können wir die Zuordnung der Invarianten zu den Idealklassen aller dieser Ordnungen als erklärt annehmen, indem wir von dem Durchschnitte aller dieser Ordnungen ausgehen. Mittels einer induktiven Definition können wir auch alle Ordnungen überhaupt erfassen, das ist aber für unsere Zwecke ganz unnötig.

3. Wir stellen uns jetzt die folgende Frage: Σ sei ein imaginärer quadratischer Zahlkörper und $\mathfrak{k}_1$, $\mathfrak{k}_2$ je eine Idealklasse der Ordnungen $\mathfrak{o}_1$, $\mathfrak{o}_2$

von Σ. Diesen Klassen sind singuläre Invarianten $j(\mathfrak{k}_i)$ der Charakteristik 0 zugeordnet. Wie können die Primfaktoren der (ganzen algebraischen) Zahl $j(\mathfrak{k}_1) - j(\mathfrak{k}_2)$ bestimmt werden?

Wir fassen ein festes Primideal $\mathfrak{p}$ von $\Sigma(j(\mathfrak{k}_1), j(\mathfrak{k}_2))$ ins Auge — p sei die zugehörige Primzahl — und reduzieren einen elliptischen Funktionenkörper der Charakteristik 0, dessen Multiplikatorenring eine in $\mathfrak{o}_1$ und $\mathfrak{o}_2$ enthaltene Ordnung $\mathfrak{o}_0$ ist, modulo einem Primfaktor $\mathfrak{p}_1$ von $\mathfrak{p}$ im Konstantenkörper, von dem wir voraussetzen, daß er $\Sigma(j(\mathfrak{k}_1), j(\mathfrak{k}_2))$ umfasse, damit nämlich in K elliptische Teilkörper K_1 und K_2 mit den Invarianten $j(\mathfrak{k}_1), j(\mathfrak{k}_2)$ vorhanden sind (vgl. T § 3). Wir bezeichnen die Restklassen modulo $\mathfrak{p}_1$ durch Überstreichen. Nach T, § 4 kann die Reduktion modulo $\mathfrak{p}_1$ so eingerichtet werden, daß $\overline{K}$ ein elliptischer Funktionenkörper ist. Seine Charakteristik ist p. Die Teilkörper K_1, K_2 gehen modulo $\mathfrak{p}_1$ in elliptische Teilkörper $\overline{K}_1$, $\overline{K}_2$ von K über, und die Invarianten von $\overline{K}_1, \overline{K}_2$ sind $\overline{j(\mathfrak{k}_1)}, \overline{j(\mathfrak{k}_2)}$.

Die Kongruenz

$$j(\mathfrak{k}_1) \equiv j(\mathfrak{k}_2) \mod \mathfrak{p}$$

ist also damit gleichbedeutend, daß $\overline{K}_1$ und $\overline{K}_2$ die gleiche Invariante haben, also isomorph sind. Da wir annehmen können, daß K_2 in K_1 enthalten ist, so ist $j(\mathfrak{k}_1) \equiv j(\mathfrak{k}_2)$ damit gleichbedeutend, daß $\overline{K}_1$ einen Multiplikator μ hat, der $\overline{K}_1$ auf $\overline{K}_2$ abbildet, $\overline{K}_2 = \overline{K}_1^{\mu}$. Da K_2 nicht zu K_1 isomorph ist — denn wir setzen natürlich $j(\mathfrak{k}_1) \neq j(\mathfrak{k}_2)$ voraus — so muß μ bei der Erweiterung der Multiplikatorenringe, die im allgemeinen eintritt, wenn nach einem Primideal des Konstantenkörpers reduziert wird, neu hinzugekommen sein, und wir müssen die Bedingungen aufsuchen, unter denen das geschieht.

Wir unterscheiden zwei Fälle:

1. p zerfällt in Σ in zwei verschiedene Primideale $\mathfrak{P}_1$, $\mathfrak{P}_2$, von denen $\mathfrak{P}_1$ durch $\mathfrak{p}$ teilbar sein möge. Der Multiplikatorenring von K_i ist nach Voraussetzung $\mathfrak{o}_i$, dagegen ist der Multiplikatorenring von $\overline{K}_i$ die Ordnung $\mathfrak{o}_i^*$ von Σ, deren Führer f_i^* sich aus dem Führer f_i von $\mathfrak{o}_i$ durch Weglassen der in ihm enthaltenen Potenz von p ergibt. *Mithin gilt im gegenwärtigen Falle* $j(\mathfrak{k}_1) \equiv j(\mathfrak{k}_2) \mod \mathfrak{p}$ *genau dann, wenn* f_1 *und* f_2 *sich nur um eine Potenz von* p *unterscheiden, und die beiden Klassen* $\mathfrak{k}_1$, $\mathfrak{k}_2$ *zu der gleichen Klasse* $\mathfrak{o}_1^* \mathfrak{k}_1 = \mathfrak{o}_2^* \mathfrak{k}_2$ *von* $\mathfrak{o}_1^* = \mathfrak{o}_2^*$ *gehören.* Es zeigt sich, daß diese Bedingung von $\mathfrak{p}$ nicht weiter abhängt; *also* $j(\mathfrak{k}_1) - j(\mathfrak{k}_2)$ *entweder durch alle oder durch keine Primfaktoren von* p *teilbar ist.*

2. p ist in Σ Primideal oder Primidealquadrat. Jetzt ist der Multiplikatorenring von $\overline{K}_i$ eine Maximalordnung $\mathfrak{m}_i$ der Quaternionenalgebra $Q_{\infty,p}$, in die Σ so eingebettet erscheint, daß der Durchschnitt von $\mathfrak{m}_i$ mit Σ die Ordnung $\mathfrak{o}_i^*$ ist, deren Führer f_i^* sich wie im Falle 1. von dem Führer f_i von $\mathfrak{o}_i$ nur durch das Fehlen der etwa in f_i enthaltenen Potenz von p unterscheidet. Daraus folgt zunächst, daß $j(\mathfrak{k}_1) \equiv j(\mathfrak{k}_2) \mod \mathfrak{p}$ sicher dann gilt, wenn die unter 1. angegebene Bedingung erfüllt ist. Aber diese Bedingung ist nicht notwendig, denn es kann auch unter den mit Σ nicht vertauschbaren Elementen von $Q_{\infty,p}$ einen Multiplikator μ geben, der $\overline{K}_1$ auf $\overline{K}_2$ abbildet. Um diese Möglichkeit bequem ausdrücken zu können, führen wir den Begriff der *Einbettung einer Ordnung* $\mathfrak{o}$ *von* Σ *in eine Maximalordnung* $\mathfrak{m}$ *von* $Q_{\infty,p}$ ein. Σ sei als Teilkörper von $Q_{\infty,p}$ gegeben. Der Durchschnitt einer gegebenen Maximalordnung $\mathfrak{m}$ von $Q_{\infty,p}$ mit Σ ist eine Ordnung $\mathfrak{o}$, deren Führer nicht durch p teilbar ist. Wir sagen, $\mathfrak{o}$ *sei in* $\mathfrak{m}$ *eingebettet*. Ist $\mathfrak{o}$ eine beliebige Ordnung von Σ und $\mathfrak{o}_0$ die Ordnung, deren Führer sich aus dem von $\mathfrak{o}$ durch Wegstreichen der etwa in ihm enthaltenen Potenz von p ergibt, *so heißt* $\mathfrak{o}$ *in* $\mathfrak{m}$ *eingebettet, wenn es* $\mathfrak{o}_0$ *ist*. Wenn α eine Zahl von Σ ist, so gilt $\Sigma \cap \mathfrak{m} = \Sigma \cap \alpha^{-1}\mathfrak{m}\alpha$; wenn $\mathfrak{o}$ in $\mathfrak{m}$ eingebettet ist, so ist es also auch in alle $\alpha^{-1}\mathfrak{m}\alpha$ eingebettet. Alle diese Einbettungen nennen wir *äquivalent*.

Wir können die Einbettungen der $\mathfrak{o}$ in die $\mathfrak{m}$ den Idealklassen von $\mathfrak{o}$ zuordnen. Da wir wieder mehrere Ordnungen $\mathfrak{o}, \mathfrak{o}', \ldots$ zugleich betrachten wollen, so gehen wir von einem elliptischen Körper K^* der Charakteristik 0 aus, dessen Multiplikatorenring $\mathfrak{o}^*$ eine in $\mathfrak{o}, \mathfrak{o}', \ldots$ enthaltene Ordnung von Σ ist. K^* reduzieren wir nach einem Primfaktor von $\mathfrak{p}$ zu einem elliptischen Körper $\overline{K}^*$ der Charakteristik p; dazu muß der Konstantenkörper passend gewählt werden (T, § 4). Die Multiplikatorenalgebra von $\overline{K}^*$ ist $Q_{\infty,p}$, in ihr ist Σ als maximaler Teilkörper enthalten. Ist nun $\mathfrak{k}$ eine Idealklasse der Ordnung $\mathfrak{o}$, K ein Teilkörper von K^* mit der Invariante $j(\mathfrak{k})$, so ist $\mathfrak{o}$ in den Multiplikatorenring $\mathfrak{m}$ von $\overline{K}$ eingebettet. Diese Einbettung heiße zu $\mathfrak{k}$ *modulo* $\mathfrak{p}$ *gehörig*. Offenbar gehören zu zwei Klassen von $\mathfrak{o}$, die in die gleiche Klasse von $\mathfrak{o}_0$ fallen, gleiche Einbettungen von $\mathfrak{o}$ modulo $\mathfrak{p}$. Gehen wir statt von K von einem anderen Teilkörper K' mit der Invariante $j(\mathfrak{k})$ aus, so ist $K' = K^\alpha$ mit α aus Σ, K' hat den Multiplikatorenring $\alpha^{-1}\mathfrak{m}\alpha$, die zu $\mathfrak{k}$ modulo $\mathfrak{p}$ gehörigen Einbettungen sind also bis auf Äquivalenz eindeutig bestimmt.

Mit diesen Begriffsbildungen können wir jetzt sagen: *Ist* $\mathfrak{p}$ *ein Primfaktor der in* Σ *nicht voll zerfallenden Primzahl* p, *so gilt genau dann*

$$j(\mathfrak{k}_1) \equiv j(\mathfrak{k}_2) \mod \mathfrak{p},$$

wenn die zu $\mathfrak{k}_1$ *und* $\mathfrak{k}_2$ *gehörigen Einbettungen von* $\mathfrak{o}_1$ *und* $\mathfrak{o}_2$ *modulo* $\mathfrak{p}$ *in isomorphen Maximalordnungen* $\mathfrak{m}_1$ *und* $\mathfrak{m}_2$ *stattfinden.* Denn die Isomorphie von $\mathfrak{m}_1$ und $\mathfrak{m}_2$ ist notwendig und hinreichend dafür, daß $\mathfrak{m}_2 = \mu^{-1}\mathfrak{m}_1\mu$ oder $\overline{K}_2 = \overline{K}_1^{\mu}$ mit einem Element μ von $Q_{\infty,p}$ wird. Die anfangs festgestellte hinreichende Bedingung, die der von Fall 1 gleichlautet, ist hierin enthalten, denn wenn sie erfüllt ist, so sind die beiden Einbettungen von $\mathfrak{o}_1$ und $\mathfrak{o}_2$ sogar äquivalent.

Wir können unser Ergebnis auch noch anders ausdrücken, wenn wir von $\mathfrak{o}^*$ ausgehen. $\mathfrak{o}^*$ ist modulo $\mathfrak{p}$ in den Multiplikatorenring $\mathfrak{m}^*$ von K^* eingebettet. Es gibt je ein Ideal $\mathfrak{a}_i$ von $\mathfrak{o}_i$, so daß $K_i = K^{*\mathfrak{a}_i}$, daraus folgt $\overline{K}_i = \overline{K}^{*\mathfrak{m}\mathfrak{a}_i}$, so daß notwendig und hinreichend für

$$j(\mathfrak{k}_1) \equiv j(\mathfrak{k}_2) \quad \text{mod. } \mathfrak{p}$$

das Vorhandensein eines μ in $Q_{\infty,p}$ mit

$$\mathfrak{m}^*\mathfrak{a}_1\mu = \mathfrak{m}^*\mathfrak{a}_2$$

ist, und diese Bedingung kann auch so ausgesprochen werden:

$$j(\mathfrak{k}_1) \equiv j(\mathfrak{k}_2) \quad \text{mod. } \mathfrak{p}$$

gilt genau dann, wenn, falls $\mathfrak{o}^*$ *zu* $\mathfrak{k}^*$ *gehörig modulo* $\mathfrak{p}$ *in* $\mathfrak{m}^*$ *eingebettet ist, die Ideale* $\mathfrak{a}_1$ *der Idealklasse* $\mathfrak{k}_1\mathfrak{k}^{*-1}$ *von* $\mathfrak{o}_1$ *in die gleiche Linksidealklasse von* $\mathfrak{m}^*$ *fallen, wie die Ideale* $\mathfrak{a}_2$ *der Idealklasse* $\mathfrak{k}_2\mathfrak{k}^{*-1}$ *von* $\mathfrak{o}_2$.

4. Die letzten Ergebnisse können wir anwenden, um die Primfaktoren zu kennzeichnen, die in der Diskriminante der Klassengleichung einer Ordnung $\mathfrak{o}$ von Σ enthalten sind; denn diese Diskriminante ist ja nichts weiter als das Produkt

$$D_{\mathfrak{o}} = \prod_{i \neq l} \left(j(\mathfrak{k}_i) - j(\mathfrak{k}_l)\right),$$

erstreckt über alle Paare $j(\mathfrak{k}_i)$, $j(\mathfrak{k}_l)$ ungleicher Klasseninvarianten von $\mathfrak{o}$.

Zuerst sei p eine in Σ voll zerfallende Primzahl. Damit die Differenz $j(\mathfrak{k}_i) - j(\mathfrak{k}_l)$ durch einen Primfaktor von p teilbar sei, müssen nach 3. die Klassen $\mathfrak{k}_i$ und $\mathfrak{k}_l$ in die gleiche Klasse der Ordnung $\mathfrak{o}_0$ fallen, deren Führer aus dem Führer von $\mathfrak{o}$ sich durch Streichen der in ihm enthaltenen Potenz von p ergibt. Daraus ergibt sich, *daß* $D_{\mathfrak{o}}$ *genau dann durch* p *teilbar ist, wenn* p *in dem Führer der* $\mathfrak{o}$ *zugeordneten Idealgruppe aufgeht;* denn genau in diesem Falle gibt es von 1 verschiedene Idealklassen von $\mathfrak{o}$, die in die Hauptklasse von $\mathfrak{o}_0$ fallen.

Auch eine in Σ nicht voll zerfallende Primzahl p geht in $D_\mathfrak{o}$ auf, wenn sie den Führer der $\mathfrak{o}$ zugeordneten Idealgruppe teilt; aber die notwendige und hinreichende Bedingung für

$$D_\mathfrak{o} \equiv 0 \mod p$$

lautet in diesem Falle offenbar so: *bei irgendeiner Einbettung von* $\mathfrak{o}$ *in eine Maximalordnung* $\mathfrak{m}$ *von* $Q_{\infty,p}$ *müssen gewisse Nichthauptideale* $\mathfrak{a}$ *von* $\mathfrak{o}$ *in Hauptideale von* $\mathfrak{m}$ *übergehen:* $\mathfrak{a}\mathfrak{m} = \alpha\mathfrak{m}$.

5. Wir behandeln schließlich noch den Fall, daß $j(\mathfrak{k}_1)$ und $j(\mathfrak{k}_2)$ Klasseninvarianten zweier verschiedener Körper Σ_1 und Σ_2 sind. $\mathfrak{p}$ sei ein in $j(\mathfrak{k}_1) - j(\mathfrak{k}_2)$ aufgehendes Primideal, Teiler der Primzahl p. Da die Multiplikatorenalgebra eines elliptischen Funktionenkörpers der Charakteristik p, dessen Invariante der gemeinsame Kongruenzwert von $j(\mathfrak{k}_1)$ und $j(\mathfrak{k}_2)$ modulo $\mathfrak{p}$ ist, einen zu Σ_1 und einen zu Σ_2 isomorphen Teilkörper umfassen muß, so ist sie notwendigerweise nichtkommutativ, woraus folgt, daß p in keinem der beiden Körper Σ_i voll zerfällt:

In der Differenz zweier singulärer Moduln $j(\mathfrak{k}_1)$ *und* $j(\mathfrak{k}_2)$, *die zu zwei verschiedenen imaginären quadratischen Zahlkörpern* Σ_1 *und* Σ_2 *gehören, gehen nur solche Primideale auf, deren zugehörige Primzahlen* p *in beiden Körpern* Σ_1, Σ_2 *nicht voll zerfallen, die also, wenn* D_i *die Diskriminante von* Σ_i *ist, den Bedingungen* $\left(\frac{D_1}{p}\right) \neq 1$, $\left(\frac{D_2}{p}\right) \neq 1$ *genügen.* Sehen wir von den Primfaktoren der $D_1 D_2$ ab, so können diese Bedingungen zufolge dem quadratischen Reziprozitätsgesetze dahin ausgedrückt werden, daß p gewissen Restklassen modulo $D_1 D_2$ oder auch nur modulo dem kleinsten gemeinschaftlichen Vielfachen von D_1 und D_2 angehören muß.

Die Invariante $j = 0$ gehört zu der Hauptordnung des Körpers der dritten Einheitswurzeln. Daher gilt: *In einem singulären Modul, der nicht zum Körper der dritten Einheitswurzeln gehört, können nur Primfaktoren von* 3 *und von Primzahlen* $p \equiv -1 \mod 3$ *aufgehen.* Ebenso: *In* $j - 2^6 \cdot 3^3$ *können, wenn der singuläre Modul* j *nicht zum Körper der vierten Einheitswurzeln gehört, keine Primideale aufgehen, die nicht in* 2 *oder in einer Primzahl* $p \equiv -1 \mod 4$ *enthalten sind.*

Jeder singuläre Modul gibt zu einer Einzelaussage dieser Art Anlaß.

Wir können die Bedingung für

$$j(\mathfrak{k}_1) \equiv j(\mathfrak{k}_2) \mod \mathfrak{p}$$

auch im vorliegenden Falle genauer folgendermaßen aussprechen: *Es gilt genau dann*

$$j(\mathfrak{k}_1) \equiv j(\mathfrak{k}_2) \mod \mathfrak{p}$$

wenn es eine Maximalordnung $\mathfrak{m}$ *von* $Q_{\infty,p}$ *gibt, in der sowohl eine zu* $\mathfrak{k}_1$ *gehörige Einbettung von* $\mathfrak{o}_1$ *modulo* $\mathfrak{p}$ *wie auch eine zu* $\mathfrak{k}_2$ *gehörige Einbettung von* $\mathfrak{o}_2$ *modulo* $\mathfrak{p}$ *möglich ist.*

Es wäre wünschenswert, die Zuordnung der Einbettung von Ordnungen von Σ in Maximalordnungen von $Q_{\infty,p}$ zu den Idealklassen und Primidealen unabhängig von den elliptischen Funktionenkörpern zu leisten.

6. Angesichts der Ergebnisse der vorhergehenden Abschnitte werden wir uns fragen, wieso gerade die singulären Invarianten, die doch zunächst nur die Rolle von erzeugenden Zahlen der Klassenkörper spielen, durch solche merkwürdigen Teilbarkeitseigenschaften ausgezeichnet sind. Dieser Umstand läßt sich aber verstehen, wenn wir sowohl die algebraische wie die arithmetische Bedeutung von $j(\omega)$ betrachten. j ist erzeugende Funktion des Körpers der Modulfunktionen und kann als solche nur durch eine lineare Transformierte $j_0 = \dfrac{aj+b}{cj+d}$ ersetzt werden. Sollen auch die singulären Werte dieser Transformierten als Erzeugende der Klassenkörper brauchbar sein, so müssen offenbar a, b, c, d rationale Zahlen sein; natürlich können sie dann gleich ganzzahlig gewählt werden. Auf die gleiche Bedingung kommen wir, wenn wir fordern, daß j_0 dem kleinsten Konstantenkörper angehöre, mit dem ein elliptischer Funktionenkörper der Invariante j möglich ist; denn dieser kleinste Körper entsteht durch Adjunktion von j zum Primkörper, also zum Körper der rationalen Zahlen im vorliegenden Falle (T, § 3, **1**). Nach T, § 4 ist j auch für jede Primzahlcharakteristik als Invariante brauchbar, und, was noch mehr ist, es geht ein elliptischer Körper der Charakteristik 0 mit der Invariante j, wenn er nach einem Primideal des Konstantenkörpers, das in p aufgeht, reduziert wird, in einen elliptischen Körper der Charakteristik p über, dessen Invariante die Restklasse von j ist, wovon wir ja in den ersten Abschnitten dieser Abhandlung immer Gebrauch gemacht haben. Soll j_0 auch diese Eigenschaft haben, so muß $ad - bc = \pm 1$ sein. Fordern wir schließlich noch, daß der Ausartungsfall des Körpers vom Geschlechte 0 zum Werte ∞ der Invariante gehöre, so muß $c = 0$, also $j_0 = \pm j + g$ mit einer ganzen rationalen Zahl g sein. Für j und j_0 unterscheiden sich aber die entsprechenden Differenzen singulärer Werte nur ums Vorzeichen. Auf diese Weise sind also die ausgezeichneten Teilbarkeitseigenschaften der singulären Moduln zu verstehen.

Gleichzeitig wird durch diese Betrachtung auch Licht geworfen auf die Tatsache, daß die funktionentheoretische Entwicklung von $j(\omega)$ nach Potenzen von $q = e^{2\pi i\omega}$ ganzzahlige teilerfremde Koeffizienten hat. Sie kann in dieser Hinsicht ja durch die in T § 6, **4** aufgestellten u-Entwicklungen ersetzt werden, von denen dort gezeigt wurde, daß sie für *alle* Charakteristiken gültig sind, eben weil j eine für alle Charakteristiken brauchbare Invariante ist.

7. Beispiele. Wir betrachten noch einige Zahlenbeispiele zu den Kongruenzrelationen.

Zur Ordnung vom Führer 3 im Gaußschen Zahlkörper gehören die beiden Klasseninvarianten

$$\left.\begin{matrix} j(3i) \\ j\left(\dfrac{-1+3i}{2}\right) \end{matrix}\right\} = \pm 2^4 \cdot 3^3 \cdot \sqrt{3} \cdot (1 \pm \sqrt{3})^4 (1 \pm 2\sqrt{3})^3 (2 \pm 3\sqrt{3})^3 .$$

Daraus ergibt sich

$$j(3i) - j\left(\frac{-1+3i}{2}\right) = 2^{10} \cdot 3 \cdot \sqrt{3} \cdot 7^2 \cdot 19 \cdot 31 ,$$

und daher ist die Diskriminante der Klassengleichung

$$-2^{20} \cdot 3^3 \cdot 7^4 \cdot 19^2 \cdot 31^2 ,$$

in ihr gehen in der Tat außer 3 nur 2 und Primzahlen $\equiv -1 \pmod 4$ auf.

In der Hauptordnung des Körpers von $\sqrt{-5}$ sind die beiden Klasseninvarianten

$$\left.\begin{matrix} j(\sqrt{-5}) \\ j\left(\dfrac{-1+\sqrt{-5}}{2}\right) \end{matrix}\right\} = \left[\pm 2^2 \sqrt{5}\,(4 \mp \sqrt{5}) \left(\frac{1 \pm \sqrt{5}}{2}\right)^4\right]^3 ,$$

woraus

$$j(\sqrt{-5}) - j\left(\frac{-1+\sqrt{-5}}{2}\right) = 2^{15} \cdot 5 \cdot \sqrt{5} \cdot 13 \cdot 17$$

folgt; die Diskriminante der Klassengleichung ist demzufolge

$$-2^{30} \cdot 5^3 \cdot 13^2 \cdot 17^2 ,$$

alle ihre Primfaktoren neben 5 sind quadratische Nichtreste modulo 5.

Ein Beispiel für die Teilbarkeit einer Differenz $j(\mathfrak{k}_1) - j(\mathfrak{k}_2)$ zweier zu verschiedenen Ordnungen des gleichen Körpers gehörigen Klasseninvarianten durch einen Primfaktor einer voll zerfallenden Primzahl geben:

$$j(\sqrt{-2}) = 2^6 \cdot 5^3 \quad \text{zum Führer 1}$$

und

$$\left.\begin{matrix} j(3\sqrt{-2}) \\ j(\tfrac{3}{2}\sqrt{-2}) \end{matrix}\right\} = 2^6 \cdot 5^3 \cdot (5 \pm 2\sqrt{6})^2 (49 \pm 12\sqrt{6})^3 \quad \text{zum Führer 3.}$$

Es ist ohne weiteres zu erkennen, daß $j(3\sqrt{-2}) - j(\sqrt{-2})$ mit $j(\tfrac{3}{2}\sqrt{-2}) - j(\sqrt{-2})$ durch $\sqrt{3}$ teilbar sind.

Schließlich betrachten wir noch die Differenzen von Klasseninvarianten verschiedener Stammdiskriminanten:

$$j(\sqrt{-2}) - j(\sqrt{-1}) = 2^6 \cdot 5^3 - 2^6 \cdot 3^3 = 2^7 \cdot 7^2 \ .$$

2 und 7 zerfallen beide in $(\sqrt{-1})$ und $(\sqrt{-2})$ nicht voll. Ähnlich

$$j\left(\frac{-1+\sqrt{-11}}{2}\right) - j(\sqrt{-2}) = -2^{15} - 2^6 \cdot 5^3 = -2^6 \cdot 3 \cdot 11 \cdot 19 \ .$$

Wieder sind 2, 3, 11, 19 Primzahlen, die weder in $(\sqrt{-2})$ noch in $(\sqrt{-11})$ voll zerfallen.

(Eingegangen den 12. März 1946.)