
Eigenformen und Anwendungen von Hecke-Operatoren

Vortrag zum Seminar zur Höheren Funktionentheorie, 04.06.2008

Cornelia Wirtz

Ziel dieses Vortrages ist es, die Eigenformen bezüglich des Hecke-Operators $T_n^{(k)}$ zu beschreiben und die Erkenntnisse dessen auf die Diskriminante und absolute Invariante anzuwenden. Weiterhin werden wir uns mit der sogenannten Modulargleichung beschäftigen und aus dieser letztendlich herleiten, dass $j(\tau)$ eine algebraische Zahl ist, falls $\tau \in \mathbb{H}$ zu einem imaginär-quadratischen Zahlkörper gehört.

§1 Simultane Eigenformen

Im ersten Paragraphen geht es um Eigenformen bezüglich des Hecke-Operators $T_n^{(k)}$ zu einem Eigenwert $\lambda_f(n) \in \mathbb{C}$, sowie um simultane Eigenformen. Am Ende des Paragraphen werden wir feststellen, dass die Diskriminante eine simultane Eigenform ist.

— Definition —

(1.1) Definition

Sei $0 \neq f \in V(\mathbb{H})$. Dann heißt f eine

- 1) *Eigenform bezüglich des Hecke-Operators $T_n^{(k)}$, für $n \geq 1$, zum Eigenwert $\lambda_f(n) \in \mathbb{C}$, wenn*

$$T_n^{(k)} f = \lambda_f(n) f \tag{1}$$

gilt, und

- 2) *simultane Eigenform, falls f eine Eigenform bezüglich aller Hecke-Operatoren $T_n^{(k)}$ für $n \geq 1$ ist.* ◇

— Erste Folgerungen —

Aus der Definition und dem ersten Vortrag zu Hecke-Operatoren erhalten wir das folgende

(1.2) Lemma

Eine in ∞ holomorphe Funktion $0 \neq f \in V(\mathbb{H})$ ist genau dann eine simultane Eigenform, wenn seine Fourierkoeffizienten die Bedingungen

$$\lambda_f(n) \cdot \alpha_f(m) = \sum_{d|(m,n)} d^{k-1} \cdot \alpha_f\left(\frac{mn}{d^2}\right) \quad (2)$$

für alle $m, n \in \mathbb{N}$ erfüllen. ◇

Beweis

Es bezeichne $\alpha_g(m)$ die Fourierkoeffizienten von $g = T_n^{(k)} f$ und $\lambda_f(n) \alpha_f(m)$ die Fourierkoeffizienten von $\lambda_f(n) f$. Es gilt $T_n^{(k)} f = \lambda_f(n) f$ für alle $n \geq 1$ genau dann, wenn die Fourierkoeffizienten von $T_n^{(k)} f$ gleich den Fourierkoeffizienten von $\lambda_f(n) f$ für alle $n \geq 1$ sind. Dies ist aber nach [K] Lemma IV. 1.1 (mit [K] wird im Folgenden das Buch *Elliptische Funktionen und Modulformen* von Koecher/Krieg bezeichnet) genau dann der Fall, wenn $\sum_{d|(m,n)} d^{k-1} \alpha_f\left(\frac{mn}{d^2}\right) = \lambda_f(n) \alpha_f(m)$ für alle $m, n \in \mathbb{N}$ gilt, da $\alpha_g(0) = \sigma_{k-1}(n) \alpha_f(0)$ immer gilt. □

Damit folgt sofort das überraschende

(1.3) Lemma

Für ein nicht-konstantes $f \in \mathbb{M}_k$ sind äquivalent:

- i) Die Funktion f ist eine simultane Eigenform.
- ii) Es ist $\alpha_f(1) \neq 0$ und für alle $m \in \mathbb{N}_0$, sowie für alle $n \in \mathbb{N}$ gilt

$$\alpha_f(m) \alpha_f(n) = \alpha_f(1) \cdot \sum_{d|(m,n)} d^{k-1} \alpha_f\left(\frac{mn}{d^2}\right).$$

In diesem Fall sind die Eigenwerte $\lambda_f(n)$ gegeben durch $\frac{\alpha_f(n)}{\alpha_f(1)}$ für alle $n \in \mathbb{N}$ und es gilt

$$\alpha_f(m) \alpha_f(n) = \alpha_f(1) \alpha_f(mn) \quad (3)$$

für alle teilerfremden m und n . ◇

Beweis

Wir zeigen zunächst, dass aus i) schon ii) folgt. Nach Lemma (1.2) ist f genau dann eine simultane Eigenform, wenn seine Fourierkoeffizienten die Bedingungen

$$\lambda_f(n) \cdot \alpha_f(m) = \sum_{d|(m,n)} d^{k-1} \cdot \alpha_f\left(\frac{mn}{d^2}\right) \text{ für alle } m, n \in \mathbb{N}$$

erfüllen. Setzt man speziell $m = 1$ ein, so erhält man

$$\lambda_f(n)\alpha_f(1) = \sum_{d|(1,n)} d^{k-1}\alpha_f\left(\frac{1 \cdot n}{d^2}\right) = 1^{k-1}\alpha_f\left(\frac{1 \cdot n}{1^2}\right) = \alpha_f(n) \text{ für alle } n \in \mathbb{N}. \quad (4)$$

Wäre nun $\alpha_f(1) = 0$, so würde aus obiger Formel $\alpha_f(n) = 0$ für alle $n \in \mathbb{N}$ folgen. Damit wäre aber f konstant gleich $\alpha_f(0)$ im Widerspruch zur Voraussetzung. Demnach gilt $\alpha_f(1) \neq 0$, das heißt wir können in (4) durch $\alpha_f(1)$ dividieren und es folgt

$$\lambda_f(n) = \frac{\alpha_f(n)}{\alpha_f(1)} \text{ für alle } n \in \mathbb{N}.$$

Folglich sind die Eigenwerte durch $\lambda_f(n) = \frac{\alpha_f(n)}{\alpha_f(1)}$ für alle $n \in \mathbb{N}$ gegeben. Setzt man nun $\frac{\alpha_f(n)}{\alpha_f(1)}$ für $\lambda_f(n)$ in (2) ein, so erhält man

$$\frac{\alpha_f(n)}{\alpha_f(1)} \cdot \alpha_f(m) = \sum_{d|(m,n)} d^{k-1} \alpha_f\left(\frac{mn}{d^2}\right) \text{ für alle } n, m \in \mathbb{N},$$

und nach Multiplikation mit $\alpha_f(1)$ ergibt sich

$$\alpha_f(m)\alpha_f(n) = \alpha_f(1) \cdot \sum_{d|(m,n)} d^{k-1} \alpha_f\left(\frac{mn}{d^2}\right) \text{ für alle } m, n \in \mathbb{N}.$$

Es bleibt zu zeigen, dass die Gleichheit auch für $m = 0$ gilt. Setzen wir $m = 0$ in die obige Formel ein, so erhalten wir

$$\alpha_f(0)\alpha_f(n) = \alpha_f(1) \sum_{d|n} d^{k-1} \alpha_f(0) = \alpha_f(1)\alpha_f(0)\sigma_{k-1}(n) \text{ für alle } n \in \mathbb{N}.$$

Ist nun $\alpha_f(0) = 0$, so ist die Gleichheit offensichtlich. Nehmen wir also $\alpha_f(0) \neq 0$ an. Dann bleibt zu zeigen (wenn man durch $\alpha_f(0)$ dividiert), dass

$$\alpha_f(n) = \alpha_f(1)\sigma_{k-1}(n) \text{ für alle } n \in \mathbb{N}$$

gilt. Nach Voraussetzung ist aber $T_n f = \lambda_f(n)f$ für alle $n \in \mathbb{N}$ gegeben. Es gilt also auch die Gleichheit für alle Fourierkoeffizienten, das heißt insbesondere

$$\alpha_{T_n f}(0) = \lambda_f(n)\alpha_f(0) \text{ für alle } n \in \mathbb{N}.$$

Nach [K] Lemma IV. 1.1 ist $\alpha_{T_n f}(0)$ gegeben durch $\sigma_{k-1}(n)\alpha_f(0)$. Das bedeutet

$$\sigma_{k-1}(n)\alpha_f(0) = \alpha_{T_n f}(0) = \lambda_f(n)\alpha_f(0) \text{ für alle } n \in \mathbb{N},$$

und damit folgt, da $\alpha_f(0) \neq 0$, dass

$$\sigma_{k-1}(n) = \lambda_f(n) \text{ für alle } n \in \mathbb{N}.$$

gilt. Wir haben aber eben bereits

$$\lambda_f(n) = \frac{\alpha_f(n)}{\alpha_f(1)} \text{ für alle } n \in \mathbb{N}$$

gezeigt. Daraus folgt dann

$$\sigma_{k-1}(n) = \frac{\alpha_f(n)}{\alpha_f(1)} \text{ für alle } n \in \mathbb{N},$$

also die Gleichheit für $m = 0$.

Betrachte nun teilerfremde $m, n \in \mathbb{N}$, das heißt $\text{ggT}(m, n) = 1$. Dann gilt

$$\alpha_f(m)\alpha_f(n) = \alpha_f(1) \cdot 1^{k-1} \cdot \alpha_f\left(\frac{mn}{1^2}\right) = \alpha_f(1)\alpha_f(mn). \quad (*)$$

Wir wollen nun zeigen, dass aus ii) auch i) folgt. Gilt also $\alpha_f(1) \neq 0$ und zudem

$$\alpha_f(m)\alpha_f(n) = \alpha_f(1) \sum_{d|(m,n)} d^{k-1} \alpha_f\left(\frac{mn}{d^2}\right)$$

für alle $m \in \mathbb{N}_0$, sowie für alle $n \in \mathbb{N}$, dann folgt mit $\lambda_f(n) := \frac{\alpha_f(n)}{\alpha_f(1)}$, wenn man in (*) durch $\alpha_f(1)$ dividiert, dass

$$\lambda_f(n)\alpha_f(m) = \sum_{d|(m,n)} d^{k-1} \alpha_f\left(\frac{mn}{d^2}\right) = \alpha_{T_n f}(m) \text{ für alle } m, n \in \mathbb{N}$$

gilt. Nach Lemma (1.2) ist dann f eine simultane Eigenform, da nach Voraussetzung $f \neq 0$ und f holomorph in ∞ gegeben ist. \square

Als erste und vielleicht wichtigste Anwendung betrachten wir für $k = 12$ die bereits aus der Funktionentheorie bekannte Diskriminante Δ beziehungsweise die normierte Diskriminante Δ^* . Nach [K] III 2.2(4) gilt hier

$$\Delta^*(\tau) = (2\pi)^{-12} \Delta(\tau) = \sum_{m=1}^{\infty} \tau(m) e^{2\pi i m \tau} \text{ mit } \tau(1) = 1$$

und alle $\tau(m)$ sind ganze Zahlen. Man erhält somit den fundamentalen

(1.4) Satz

Die Diskriminante Δ ist eine simultane Eigenform. Man hat

$$T_n \Delta = \tau(n) \cdot \Delta \text{ für alle } n \in \mathbb{N}$$

und es gilt

$$\tau(m) \cdot \tau(n) = \sum_{d|(m,n)} d^{11} \cdot \tau\left(\frac{mn}{d^2}\right). \quad (5)$$

für alle $m, n \in \mathbb{N}$. Speziell hat man

$$\tau(mn) = \tau(m)\tau(n), \text{ falls } \text{ggT}(m, n) = 1, \quad (6)$$

und für Primzahlen p

$$\tau(p^{r+1}) = \tau(p^r)\tau(p) - p^{11} \cdot \tau(p^{r-1}), \quad r \geq 1. \quad (7)$$

◇

Beweis

Nach [K] Korollar III. 4.1 B ist Δ bis auf einen konstanten Faktor die einzige Spitzenform vom Gewicht 12. Da die Hecke-Operatoren $T_n = T_n^{(k)}$ nach [K] Korollar IV. 1.3 Spitzenformen auf Spitzenformen abbilden, ist die Diskriminante eine simultane Eigenform, denn es gilt dann

$$T_n \Delta = f \text{ mit } f \in \mathcal{S}_{12} = \mathbb{C}\Delta,$$

also

$$f = \lambda_\Delta(n)\Delta \text{ mit } \lambda_\Delta(n) \in \mathbb{C} \text{ und damit } T_n \Delta = \lambda_\Delta(n)\Delta \text{ für alle } n \in \mathbb{N}.$$

Nach Lemma (1.3) ist $\lambda_\Delta(n)$ gegeben durch

$$\lambda_\Delta(n) = \frac{\alpha_\Delta(n)}{\alpha_\Delta(1)} = \frac{(2\pi)^{12}\tau(n)}{(2\pi)^{12}\tau(1)} = \frac{\tau(n)}{\tau(1)} = \tau(n) \text{ für alle } n \in \mathbb{N},$$

da $\tau(1) = 1$. Setzt man nun $\tau(n)$ in obige Formel für $\lambda_\Delta(n)$ ein, so erhält man

$$T_n \Delta = \tau(n)\Delta \text{ für alle } n \in \mathbb{N}.$$

Nach Lemma (1.3) gilt dann

$$\alpha_\Delta(m)\alpha_\Delta(n) = \alpha_\Delta(1) \cdot \sum_{d|(m,n)} d^{12-1} \alpha_\Delta\left(\frac{mn}{d^2}\right) \text{ für alle } m, n \in \mathbb{N},$$

da Δ eine simultane Eigenform ist. Verwendet man die Identität $\alpha_\Delta(n) = (2\pi)^{12}\tau(n)$ für alle $n \in \mathbb{N}$, dann folgt

$$(2\pi)^{12}\tau(m)(2\pi)^{12}\tau(n) = (2\pi)^{12}\underbrace{\tau(1)}_{=1} \cdot \sum_{d|(m,n)} d^{11}(2\pi)^{12}\tau\left(\frac{mn}{d^2}\right) \text{ für alle } m, n \in \mathbb{N}.$$

Dividiert man nun auf beiden Seiten durch $(2\pi)^{24}$, so erhält man

$$\tau(m)\tau(n) = \sum_{d|(m,n)} d^{11}\tau\left(\frac{mn}{d^2}\right) \text{ für alle } m, n \in \mathbb{N}$$

und damit Gleichung (5).

Ist nun zusätzlich $\text{ggT}(m, n) = 1$, so folgt mit Hilfe von Gleichung (5), dass

$$\tau(m)\tau(n) = 1^{11}\tau\left(\frac{mn}{1^2}\right) = \tau(mn),$$

also Gleichung (6), gilt.

Für Primzahlen p wissen wir, dass $\{d \mid (p^r, p)\} = \{1, p\}$ für alle $r \geq 1$ gilt und damit erhalten wir mit Hilfe von Gleichung (5), dass

$$\begin{aligned} \tau(p^r)\tau(p) &= \sum_{d \in \{1, p\}} d^{11}\tau\left(\frac{p^{r+1}}{d^2}\right) \\ \Leftrightarrow \tau(p^r)\tau(p) &= 1^{11}\tau\left(\frac{p^{r+1}}{1^2}\right) + p^{11}\tau\left(\frac{p^{r+1}}{p^2}\right) \\ \Leftrightarrow \tau(p^r)\tau(p) &= \tau(p^{r+1}) + p^{11}\tau(p^{r-1}) \\ \Leftrightarrow \tau(p^{r+1}) &= \tau(p^r)\tau(p) - p^{11}\tau(p^{r-1}) \end{aligned}$$

gilt, wodurch Gleichung (7) gezeigt ist. \square

Die Vektorräume S_k sind für $k = 16, 18, 20, 22, 26$ ebenfalls eindimensional (vergleiche [K] III. 4.2). Die Spitzenformen $G_{k-12}\Delta$ sind daher für diese k auch simultane Eigenformen (mit derselben Argumentation wie in Satz 1.4).

Die Eigenwerte können bei Spitzenformen nicht beliebig groß werden. Als einfache Abschätzung erhält man die

(1.5) Proposition

Seien $n > 1$ und $0 \neq f \in S_k$. Gilt $T_n f = \lambda_f(n)f$ mit einem $\lambda_f(n) \in \mathbb{C}$, so folgt

$$|\lambda_f(n)| \leq n^{\frac{k}{2}}\sigma_{-1}(n). \quad \diamond$$

Beweis

Nach [K] Satz III. 1.6 existiert ein $w = u + iv \in \mathbb{H}$ mit

$$\tilde{f}(\tau) := y^{\frac{k}{2}} |f(\tau)| \leq \tilde{f}(w) \text{ für alle } \tau \in \mathbb{H} \quad (\text{wobei } y = \text{Im}(\tau)), \quad (8)$$

da $0 \neq f \in \mathbb{S}_k$. Dann folgt mit [K] IV 1.1(6), dass

$$\begin{aligned} |\lambda_f(n)\tilde{f}(w)| &= \left| \lambda_f(n)v^{\frac{k}{2}} |f(w)| \right| \\ &= \left| v^{\frac{k}{2}} \right| |\lambda_f(n)f(w)| \\ &= \left| v^{\frac{k}{2}} \right| |T_n f(w)| \\ &= \left| n^{k-1}v^{\frac{k}{2}} \sum_{\substack{ad=n \\ d>0}} d^{-k} \sum_{b \pmod{d}} f\left(\frac{aw+b}{d}\right) \right| \\ &\leq n^{k-1}v^{\frac{k}{2}} \sum_{\substack{ad=n \\ d>0}} d^{-k} \sum_{b \pmod{d}} \left| f\left(\frac{aw+b}{d}\right) \right| \\ &\leq n^{k-1}v^{\frac{k}{2}} \sum_{\substack{ad=n \\ d>0}} 1 \sum_{b \pmod{d}} \left| f\left(\frac{aw+b}{d}\right) \right| \end{aligned}$$

gilt, wobei wir in der letzten Ungleichung verwendet haben, dass $k \geq 12$ (da $0 \neq f \in \mathbb{S}$) und damit $d^{-k} \leq 1$ ist (da nach Voraussetzung $d \geq 1$), sowie die Tatsache, dass $n \geq 1$ und $v > 0$ (da $w \in \mathbb{H}$) ist. Damit folgt weiterhin, dass für obigen Ausdruck

gilt

$$\begin{aligned}
& n^{k-1} v^{\frac{k}{2}} \sum_{\substack{ad=n \\ d>0}} \sum_{b \pmod{d}} \left| f\left(\frac{aw+b}{d}\right) \right| \\
\stackrel{(i)}{=} & n^{k-1} v^{\frac{k}{2}} \sum_{\substack{ad=n \\ d>0}} \sum_{b \pmod{d}} \left(\frac{a}{d}v\right)^{-\frac{k}{2}} \cdot \tilde{f}\left(\frac{aw+b}{d}\right) \\
= & n^{k-1} v^{\frac{k}{2}} v^{-\frac{k}{2}} \sum_{\substack{ad=n \\ d>0}} \left(\frac{a}{d}\right)^{-\frac{k}{2}} \sum_{b \pmod{d}} \tilde{f}\left(\frac{aw+b}{d}\right) \\
= & n^{k-1} \sum_{\substack{ad=n \\ d>0}} \left(\frac{a}{d}\right)^{-\frac{k}{2}} \sum_{b \pmod{d}} \tilde{f}\left(\frac{aw+b}{d}\right) \\
\stackrel{(ii)}{\leq} & n^{k-1} \sum_{\substack{ad=n \\ d>0}} n^{-\frac{k}{2}} \sum_{b \pmod{d}} \tilde{f}\left(\frac{aw+b}{d}\right) \\
= & n^{-1+\frac{k}{2}} \sum_{\substack{ad=n \\ d>0}} \sum_{b \pmod{d}} \tilde{f}\left(\frac{aw+b}{d}\right) \\
\stackrel{(iii)}{\leq} & n^{-1+\frac{k}{2}} \sum_{\substack{ad=n \\ d>0}} \sum_{b \pmod{d}} \tilde{f}(w) \\
= & n^{-1+\frac{k}{2}} \tilde{f}(w) \sum_{\substack{ad=n \\ d>0}} \underbrace{\sum_{b \pmod{d}} 1}_{=d} \\
= & n^{-1+\frac{k}{2}} \tilde{f}(w) \sum_{\substack{ad=n \\ d>0}} d \\
= & n^{-1+\frac{k}{2}} \tilde{f}(w) \sum_{\substack{d \in \mathbb{N} \\ d|n}} d^1 \\
= & n^{-1+\frac{k}{2}} \tilde{f}(w) \sigma_1(n) \\
\stackrel{(iv)}{=} & n^{-1+\frac{k}{2}} \tilde{f}(w) n \sigma_{-1}(n) \\
= & n^{\frac{k}{2}} \tilde{f}(w) \sigma_{-1}(n),
\end{aligned}$$

wobei wir in (i) verwendet haben, dass

$$\tilde{f}\left(\frac{aw+b}{d}\right) = \operatorname{Im}\left(\frac{aw+b}{d}\right)^{\frac{k}{2}} \left|f\left(\frac{aw+b}{d}\right)\right|,$$

also mit

$$\operatorname{Im}\left(\frac{aw+b}{d}\right)^{\frac{k}{2}} = \left(\frac{a}{d}v\right)^{\frac{k}{2}}$$

auch

$$\left|f\left(\frac{aw+b}{d}\right)\right| = \left(\frac{a}{d}v\right)^{-\frac{k}{2}} \tilde{f}\left(\frac{aw+b}{d}\right)$$

gilt. In (ii) haben wir ausgenutzt, dass für $a, d > 0$ mit $a, d \in \mathbb{N}$ und $ad = n$ auch $\frac{a}{d} \leq n$ gelten muss. Um die Ungleichung (iii) zu begründen, benötigt man Gleichung (8) sowie die Tatsache, dass $\frac{aw+b}{d} \in \mathbb{H}$ gilt, da $a, d, v > 0$. In (iv) nutzen wir folgende Gleichungskette, die durch Rückwärtssummation entsteht, aus:

$$n\sigma_{-1}(n) = n \sum_{\substack{d \in \mathbb{N} \\ d|n}} d^{-1} = \sum_{\substack{d \in \mathbb{N} \\ d|n}} \frac{n}{d} = \sum_{\substack{d \in \mathbb{N} \\ d|n}} d = \sigma_1(n).$$

Damit haben wir insgesamt gezeigt, dass

$$|\lambda_f(n)\tilde{f}(w)| = |\lambda_f(n)|\tilde{f}(w) \leq n^{\frac{k}{2}}\sigma_{-1}(n)\tilde{f}(w)$$

gilt. Weil $f \neq 0$ ist, haben wir auch $\tilde{f}(w) \neq 0$ und damit können wir durch $\tilde{f}(w)$ dividieren und erhalten

$$|\lambda_f(n)| \leq n^{\frac{k}{2}}\sigma_{-1}(n). \quad \square$$

Zum Abschluss dieses Paragraphen kommen wir noch zu folgender

(1.6) Bemerkung

Satz (1.4) wurde 1920 von L. J. Mordell (Proc. Cambridge. Phil. Soc. 19, 117–124) bewiesen. Sein Beweis benutzt im Wesentlichen die heute Hecke-Operatoren genannten Endomorphismen $T_n^{(12)}$. Aber erst E. Hecke erkannte 20 Jahre später (Math. Werke, 644–707) die universelle Bedeutung dieser Konstruktion. \diamond

§2 Anwendung auf die absolute Invariante

— Die absolute Invariante —

Nachdem wir uns im letzten Vortrag und im ersten Paragraphen mit Eigenschaften von Hecke-Operatoren beschäftigt haben, kommen wir nun auf deren Anwendung

auf die absolute Invariante j zu sprechen. Nach [K] III. (2.4) ist

$$j := \frac{(720G_4)^3}{\Delta} \quad (9)$$

eine auf \mathbb{H} holomorphe Modulfunktion, die bei ∞ einen Pol erster Ordnung hat und

$$j(\tau) = e^{-2\pi i\tau} + \sum_{m=0}^{\infty} j_m e^{2\pi i m\tau} \quad \text{für alle } \tau \in \mathbb{H} \quad (10)$$

mit positiven ganzen Zahlen j_m erfüllt.

— Anwendung der Hecke-Operatoren auf die absolute Invariante —

Kommen wir nun zum ersten

(2.1) Satz

Für $T_n := T_n^{(0)}$ ist $T_n j$ eine Modulfunktion, die auf \mathbb{H} holomorph ist. \diamond

Beweis

Nach [K] Satz IV. 1.3 gehört für $j \in \mathbb{W}_0$ ebenfalls wieder $T_n j$ zu \mathbb{W}_0 und es gilt

$$\begin{aligned} (T_n^{(0)} j)(\tau) &= n^{0-1} \sum_{\substack{ad=n \\ d>0}} \underbrace{d^{-0}}_{=1} \sum_{b \pmod{d}} j\left(\frac{a\tau+b}{d}\right) \\ &= \frac{1}{n} \sum_{\substack{ad=n \\ d>0}} \sum_{b \pmod{d}} j\left(\frac{a\tau+b}{d}\right). \end{aligned}$$

Da j auf \mathbb{H} holomorph ist und die Funktion $f : \mathbb{H} \rightarrow \mathbb{H}, \tau \mapsto \frac{a\tau+b}{d}$ holomorph auf \mathbb{H} ist (da $a, d > 0$ nach Voraussetzung), ist auch die Funktion $j \circ f$ holomorph auf \mathbb{H} und als Summe holomorpher Funktionen damit auch $T_n^{(0)} j$. \square

Eine weitere interessante Eigenschaft der absoluten Invariante in Bezug auf Hecke-Operatoren liefert der folgende

(2.2) Satz

Für jedes $n \geq 1$ ist $T_n j$ ein Polynom vom Grad n in j . \diamond

Beweis

Nach Satz (2.1) ist $T_n j$ eine Modulfunktion, die auf \mathbb{H} holomorph ist. Mit [K] Korollar III. 5.2 B) ist $T_n j$ damit ein Polynom in j . Es bleibt zu zeigen, dass $T_n j$ Grad n hat. Dazu betrachten wir zunächst die Fourier-Entwicklung von j^n . Wie man in (10)

sieht, ist der erste Term die Fourier-Entwicklung von j gegeben durch $e^{-2\pi i\tau}$. Potenziert man diese Darstellung mit n , so erhält man, dass die Fourier-Entwicklung von j^n mit $e^{-2\pi i n\tau}$ beginnt, das heißt aber auch, dass j^n einen Pol der Ordnung n in ∞ hat. Da weitere Potenzen j^m mit $m < n$ nicht zu diesem Faktor beitragen, bedeutet dies, dass der Grad eines Polynoms in j mit der Polstellenordnung in ∞ übereinstimmt. Um nun zu zeigen, dass $T_n j$ Grad n hat, genügt es zu zeigen, dass die Fourier-Entwicklung mit einem nichtverschwindenden Summanden $a_{-n} e^{-2\pi i n\tau}$ beginnt. Nach [K] Lemma IV. 1.1 sind die Fourier-Koeffizienten von $g = T_n^{(k)} j$ gegeben durch

$$\alpha_g(m) = \sum_{d|(m,n)} d^{-1} \alpha_j\left(\frac{mn}{d^2}\right) \quad \text{für alle } m \geq -n$$

und $\alpha_g(m) = 0$ für alle $m \leq -n$. Es bleibt also zu zeigen, dass $\alpha_g(-n)$ nicht verschwindet. Es gilt nun

$$\alpha_g(-n) = \sum_{d|n} d^{-1} j_{\frac{-n^2}{d^2}} = \frac{1}{n} \neq 0,$$

wobei wir verwendet haben, dass

$$j_{\frac{-n^2}{d^2}} = 0 \quad \text{falls } d < n \quad \text{und } j_{\frac{-n^2}{d^2}} = 1 \quad \text{falls } d = n$$

gilt. Demnach ist $\frac{1}{n} e^{-2\pi i n\tau}$ der erste Term der Fourier-Entwicklung von $T_n j$, das heißt, $T_n j$ hat einen Pol n -ter Ordnung in ∞ und damit ist nach obigen Überlegungen $T_n j$ ein Polynom vom Grad n in j . \square

Betrachten wir nun die Fourier-Entwicklung von $T_n j$, so stellen wir fest, dass der Hauptteil der Fourier-Reihe von $T_n j$ ist denkbar einfach ist:

(2.3) Proposition

Für $n \geq 1$ gilt:

$$n(T_n j)(\tau) = e^{-2\pi i n\tau} + 744\sigma_1(n) + nj_n e^{2\pi i\tau} + \dots \quad \diamond$$

Beweis

Nach [K] IV. 1.1(9) hat man für $k = 0$ die Gleichung

$$\alpha_{T_n j}(m) = \sum_{d|(m,n)} d^{0-1} j_{\frac{mn}{d^2}} \quad \text{für alle } m \geq -n,$$

da $m_0 = -1$, was man an der Fourier-Reihe der j -Funktion ablesen kann. Aus dieser Fourier-Reihe und nach der Bemerkung hinter [K] Satz III. 2.4 erkennt man zudem, dass

$$\begin{aligned} j_m &= 0 \text{ für alle } m < -1, \\ j_{-1} &= 1, \\ j_0 &= 744 \text{ und} \\ j_n &\geq 0 \text{ für alle } n \geq 1 \end{aligned}$$

gilt. Damit erhält man einen von 0 verschiedenen Koeffizienten von j_{mnd-2} für negatives m , wobei $n \geq 1$ und $d^2 > 0$ gilt, nur dann, falls $\frac{mn}{d^2} = -1 \Leftrightarrow mn = -d^2$, wenn also $m = -n$ und $d = n$ gilt (da $d \mid (m, n)$). Damit gilt

$$\alpha_{T_n j}(-n) = \sum_{d \mid (-n, n)} d^{-1} j_{\frac{-n^2}{d^2}} = n^{-1} j_{-1} = \frac{1}{n}$$

für $m = -n$ (wie bereits im Beweis von (2.2) gesehen) und für alle weiteren $m < 0$ mit $m \neq -n$ gilt

$$\alpha_{T_n j}(m) = \sum_{d \mid (m, n)} d^{-1} \underbrace{j_{\frac{mn}{d^2}}}_{=0} = 0.$$

Nun betrachten wir noch den Fall $m = 0$ sowie $m = 1$. Für $m = 0$ hat man

$$\begin{aligned} \alpha_{T_n j}(0) &= \sum_{d \mid (0, n)} d^{0-1} j_{\frac{0 \cdot n}{d^2}} \\ &= \sum_{d \mid n} d^{-1} \underbrace{j_0}_{=744} \\ &= 744 \sum_{d \mid n} d^{-1} \\ &= 744 \sigma_{-1}(n) \end{aligned}$$

und für $m = 1$ ergibt sich

$$\begin{aligned} \alpha_{T_n j}(1) &= \sum_{d \mid (1, n)} d^{-1} j_{\frac{1 \cdot n}{d^2}} \\ &= 1^{-1} j_{\frac{n}{1^2}} \\ &= j_n. \end{aligned}$$

Damit folgt, dass $n(T_n j)(\tau)$ gegeben ist durch

$$\begin{aligned} n(T_n j)(\tau) &= n \left(\frac{1}{n} e^{-2\pi i n \tau} + 744 \sigma_{-1}(n) + j_n e^{2\pi i \tau} + \dots \right) \\ &= e^{-2\pi i n \tau} + 744 \underbrace{n \sigma_{-1}(n)}_{=\sigma_1(n)} + n j_n e^{2\pi i \tau} + \dots, \end{aligned}$$

mit $n \sigma_{-1}(n) = \sigma_1(n)$ wie im Beweis von (1.5)(iv). Damit folgt also die Behauptung. \square

— Anwendung der Hecke-Operatoren auf Potenzen von j —

Wir erhalten weiterhin folgendes

(2.4) Korollar

Zu jedem $m \in \mathbb{N}$ gibt es γ_m und γ_{mn} aus \mathbb{Z} mit

$$j^m = \gamma_m + \sum_{n=1}^m n \gamma_{mn} T_n j.$$

\diamond

Beweis

Durch Potenzieren von (10) erhält man eine Fourier-Reihe für j^m mit Koeffizienten aus \mathbb{Z} , da bereits die Koeffizienten von j , also die j_n , positive ganze Zahlen sind. Damit ergibt sich

$$j^m(\tau) = e^{-2\pi i m \tau} + c_{m-1} e^{-2\pi i (m-1) \tau} + \dots + c_1 e^{-2\pi i \tau} + \dots$$

mit $c_1, c_2, \dots, c_{m-1} \in \mathbb{Z}$. Betrachtet man weiterhin $\sum_{n=1}^m n \gamma_{mn} T_n j(\tau)$, so erhält man mit Proposition (2.3):

$$\sum_{n=1}^m n \gamma_{mn} T_n j(\tau) = \gamma_{mm} e^{-2\pi i m \tau} + \gamma_{m(m-1)} e^{2\pi i (m-1) \tau} + \dots + \gamma_{m1} e^{-2\pi i \tau} + \dots.$$

Für $\gamma_{mn} = c_n \in \mathbb{Z}$ für $n = 1, \dots, m$ ist daher $j^m - \sum_{n=1}^m n \gamma_{mn} T_n j$ eine in \mathbb{H} und bei ∞ holomorphe Modulfunktion, da sich die Terme $e^{2\pi i m \tau}$ für $m < 0$ wegheben und $j^m - \sum_{n=1}^m n \gamma_{mn} T_n j$ als Summe (beziehungsweise Differenz) von Modulfunktionen wieder eine Modulfunktion ist. Damit ist $j^m - \sum_{n=1}^m n \gamma_{mn} T_n j =: g$ aber schon eine ganze Modulform vom Gewicht 0, also gilt $g \in \mathbb{M}_0 = \mathbb{C}$ nach [K] Proposition III. 4.1 B), das heißt $\gamma_m := j^m - \sum_{n=1}^m n \gamma_{mn} T_n j \in \mathbb{C}$. Weil j^m und alle $n T_n j$ ganzzahlige Fourierkoeffizienten haben, da alle Fourierkoeffizienten gegeben sind durch

$$n \alpha_{T_n j}(m) = \sum_{d|(m,n)} \underbrace{\frac{n}{d}}_{\in \mathbb{Z}} \underbrace{\frac{j_{mn}}{d^2}}_{\in \mathbb{Z}} \in \mathbb{Z},$$

ist auch γ_m ganz. \square

Zum Abschluss dieses Paragraphen kommen wir noch zu einem letzten, aber für den folgenden Abschnitt wichtigen

(2.5) Korollar

Für $n \geq 1$ gilt

$$T_n \mathbb{Q}[j] \subset \mathbb{Q}[j]. \quad \diamond$$

Beweis

Sei $f \in \mathbb{Q}[j]$ beliebig. Dann gilt nach [K] Korollar III. 5.2 B), dass f in \mathbb{K} liegt und auf \mathbb{H} holomorph ist und damit nach [K] Satz IV. 1.3, dass $T_n f \in \mathbb{V}_0 = \mathbb{K}$ gilt. Mit derselben Argumentation wie in Satz (2.1), dass j^m , sowie $g : \mathbb{H} \rightarrow \mathbb{H}, \tau \mapsto \frac{a\tau+b}{d}$ holomorph auf \mathbb{H} sind und damit auch die Verkettung, ist $T_n f$ als Summe holomorpher Funktionen holomorph auf \mathbb{H} und damit wieder nach [K] Korollar III. 5.2 B) ein Polynom in j . Da die T_n für $n \geq 1$ Endomorphismen sind, genügt es zu zeigen, dass $T_n j^m \in \mathbb{Q}[j]$ für alle $m \geq 1$ und $T_n q \in \mathbb{Q}$ für alle $q \in \mathbb{Q}$. Für letzteres ist die Aussage jedoch klar, wenn man sich die Darstellung in [K] IV. 1.1(6) genauer ansieht. Dann gilt nämlich

$$(T_n q)(\tau) = n^{-1} \sum_{\substack{ad=n \\ d>0}} 1 \sum_{b \pmod{d}} q = n^{-1} q \sum_{d|n} d = \frac{1}{n} q \underbrace{\sigma_1(n)}_{\in \mathbb{Q}} \in \mathbb{Q}.$$

Für $T_n j^m$ mit $m \geq 1$ führen wir einen Koeffizientenvergleich durch. Wir wissen einerseits, dass $T_n(j^m)$ ein Polynom in j ist, das heißt wir haben eine Darstellung

$$T_n(j^m) = \sum_{p=0}^l a_p j^p \quad \text{mit } a_p \in \mathbb{C} \quad \text{für alle } 0 \leq p \leq l$$

gegeben. Da wir bereits im Beweis von (2.4) die Fourier-Entwicklung der j^p betrachten haben, können wir diese nun in obiges Polynom einsetzen und erhalten

$$\begin{aligned} T_n(j^m) &= a_0 \\ &+ a_1 e^{-2\pi i \tau} + a_1 c_{0,1} + \dots \\ &+ a_2 e^{-2\pi i 2\tau} + a_2 c_{-1,2} e^{-2\pi i \tau} + a_2 c_{0,2} + \dots \\ &+ \dots \\ &+ a_l e^{-2\pi i l \tau} + a_l c_{-(l-1),l} e^{-2\pi i (l-1)\tau} + \dots + a_l c_{-1,l} e^{-2\pi i \tau} + a_l c_{0,l} + \dots \end{aligned}$$

mit $c_{q,p} \in \mathbb{Z}$ für $0 \leq p \leq l$ und $q = -l, -(l-1), \dots -1, 0, \dots$. Nach [K] Lemma IV. 1.1 gilt für die Fourierkoeffizienten von $T_n(j^m)$ aber auch folgende Gleichheit

$$\alpha_{T_n(j^m)}(m_0) = \sum_{d|(m_0, n)} d^{-1} \alpha_{j^m}\left(\frac{m_0 n}{d^2}\right) \quad \text{für alle } m_0 \geq -nm,$$

wobei die $\alpha_{j^m}(\frac{mm}{d^2})$ aufgrund der bekannten Fourierentwicklung von j^m in \mathbb{Z} liegen. Damit gilt aber

$$\alpha_{T_n(j^m)}(m_0) \in \mathbb{Q} \text{ für alle } m_0 \geq -nm \text{ und } \alpha_{T_n(j^m)}(m_0) = 0 \text{ sonst.}$$

Daraus erhalten wir aber auch, dass der Grad l des Polynoms höchstens $l \leq nm$ sein kann, da die Ordnung der Polstelle in ∞ mit dem Grad des Polynoms übereinstimmt (wie wir bereits gesehen haben). Wir können nun einen Koeffizientenvergleich durchführen und erhalten für $a_l = a_{nm}$ zunächst

$$a_{nm} = \alpha_{T_n(j^m)}(-nm) \in \mathbb{Q}.$$

Weiter gilt

$$a_{nm-1} + \underbrace{a_{nm}}_{\in \mathbb{Q}} \underbrace{c_{-nm+1, nm}}_{\in \mathbb{Q}} = \alpha_{T_n(j^m)}(-nm+1) \in \mathbb{Q},$$

also $a_{nm-1} \in \mathbb{Q}$. Allgemein gilt folgende Gleichheit

$$a_p + a_{p+1}c_{-p, p+1} + \dots + a_{nm}c_{-p, nm} = \alpha_{T_n(j^m)}(-p) \in \mathbb{Q} \text{ für alle } 0 \leq p \leq nm - 1.$$

Rekursiv erhält man also, dass $a_p \in \mathbb{Q}$ für alle $0 \leq p \leq nm$ gilt und damit ist $T_n(j^m) \in \mathbb{Q}[j]$ für alle $m \geq 1$, was noch zu zeigen war. \square

§3 Die Modulargleichung

Die Modulargleichung ist als Analogon der n -Teilungsgleichung der \wp -Funktion (vergleiche [K] I. 7.3) für die j -Funktion anzusehen. Dabei wird die Hecke-Theorie verwendet.

— Rückblick auf die lineare Algebra —

Um die Modulargleichung beweisen zu können, benötigen wir zunächst noch einen Satz (vergleiche Koecher/Krieg *Lineare Algebra und analytische Geometrie*) aus der linearen Algebra:

(3.1) Satz

Sind $\lambda_1, \dots, \lambda_n$ beliebige Elemente aus einem Körper K , so gibt es eine Darstellung

$$\varphi(\xi) := \prod_{i=1}^n (\xi - \lambda_i) = \sum_{l=0}^n (-1)^l \varepsilon_l \xi^{n-l} \text{ für alle } \xi \in K. \quad (11)$$

Die Koeffizienten $\varepsilon_l = \varepsilon_l(\lambda_1, \dots, \lambda_n)$ nennt man die elementarsymmetrischen Funktionen von $\lambda_1, \dots, \lambda_n$. Speziell hat man

$$\varepsilon_0 = 1, \quad \varepsilon_1 = \sum_{i=1}^n \lambda_i, \quad \varepsilon_2 = \sum_{1 \leq k < p \leq n} \lambda_k \lambda_p \quad \text{und} \quad \varepsilon_n = \prod_{x=1}^n \lambda_x. \quad (12)$$

Neben den elementarsymmetrischen Funktionen der $\lambda_1, \dots, \lambda_n$ hat man manchmal die Potenzsummen $\sigma_k := \sigma_k(\lambda_1, \dots, \lambda_n) := \sum_{i=1}^n \lambda_i^k$ für $k \geq 0$ zu betrachten. Speziell gilt

$$\sigma_0 = n \quad \text{und} \quad \sigma_1 = \varepsilon_1. \quad (13)$$

Eine einfache Verifikation ergibt weiter

$$\sigma_1^2 = \sigma_2 + 2\varepsilon_2.$$

Setzt man $\varepsilon_l = 0$ für $l > n$, so gilt

$$\sum_{k=1}^l (-1)^{k+1} \sigma_k \varepsilon_{l-k} = l \varepsilon_l \quad \text{für alle } l \geq 1. \quad \diamond$$

— Die Modulargleichung —

Als erstes wichtiges Ergebnis erhalten wir die folgende

(3.2) Proposition

Zu jedem $n \in \mathbb{N}$ existiert ein eindeutig bestimmtes Polynom $F_n(X, Y) \in \mathbb{Q}[X, Y]$ mit der Eigenschaft

$$F_n(X, j(\tau)) = \prod_{M \in \Gamma_n} (X - j(M\tau)) \quad \text{für alle } \tau \in \mathbb{H}. \quad (14)$$

Als Polynom in X beziehungsweise Y hat $F_n(X, Y)$ jeweils den Grad $\sigma_1(n)$. \diamond

Beweis

Sei

$$F_n(X) := \prod_{M \in \Gamma_n} (X - j(M\tau)) \quad (15)$$

mit $\tau \in \mathbb{H}$ beliebig aber fest. Weil j bereits Γ -invariant ist, hängt (15) nicht von der Wahl des Vertretersystems ab. Sei also $r = \sigma_1(n)$ und M_1, M_2, \dots, M_r das Standard-Rechtsvertretersystem aus [K] IV. 1.2(2). Dann folgt

$$\begin{aligned} F_n(X) &= \prod_{k=1}^r (X - j(M_k\tau)) \\ &= \sum_{k=0}^r (-1)^k P_k(j(M_1\tau), \dots, j(M_r\tau)) X^{r-k}, \end{aligned}$$

wobei P_k das k -te elementarsymmetrische Polynom in r Unbestimmten (also $\varepsilon_k(X_1, \dots, X_t)$) ist. Für die Potenzsummen gilt dann

$$\sigma_k(\tau) \stackrel{(3.1)}{=} \sum_{m=1}^r j(M_m\tau)^k \stackrel{[\text{K}] \text{ IV. 1.1(3)}}{=} (nT_n(j^k))(\tau) \in \mathbb{Q}[j(\tau)] \quad (16)$$

nach Korollar (2.5). Nach Satz (3.1) wissen wir zudem, dass man die elementarsymmetrischen Polynome rational durch die Potenzsummen ausdrücken kann, das heißt

$$P_k(j(M_1\tau), \dots, j(M_r\tau)) \in \mathbb{Q}[j(\tau)] \quad \text{nach (16)}. \quad (17)$$

Da $F_n(X) \in \mathbb{Q}[j(\tau), X]$ gilt, ist $F_n(X)$ eindeutig darstellbar als

$$F_n(X) = \sum_{\substack{0 \leq k \leq m_1 \\ 0 \leq l \leq m_2}} a_{k,l} j(\tau)^k X^l,$$

mit $a_{k,l} \in \mathbb{Q}$, für $0 \leq k \leq m_1$ sowie $0 \leq l \leq m_2$ und $m_1, m_2 \in \mathbb{N}$. Definiere nun

$$F_n(X, Y) := \sum_{\substack{0 \leq k \leq m_1 \\ 0 \leq l \leq m_2}} a_{k,l} Y^k X^l \in \mathbb{Q}[X, Y] \text{ mit } a_{k,l}, m_1, m_2 \text{ wie oben.}$$

Dann gilt

$$\begin{aligned} F_n(X, j(\tau)) &= \sum_{\substack{0 \leq k \leq m_1 \\ 0 \leq l \leq m_2}} a_{k,l} j(\tau)^k X^l \\ &= F_n(X) \\ &= \prod_{M \in \Gamma: \Gamma_n} (X - j(M\tau)) \\ &= \prod_{k=1}^r (X - j(M_k\tau)). \end{aligned}$$

Weil j nach [K] III. 5.2 transzendent ist, folgt, dass $F_n(X, Y) \in \mathbb{Q}[X, Y]$ mit der Eigenschaft (14) eindeutig ist, denn angenommen, es gäbe ein weiteres Polynom $G_n(X, Y) \in \mathbb{Q}[X, Y]$ mit der Darstellung $G_n(X, j(\tau)) = \prod_{M \in \Gamma: \Gamma_n} (X - j(M\tau))$, dann wäre aber $F_n(X, j(\tau)) - G_n(X, j(\tau)) = 0$ für alle $\tau \in \mathbb{H}$ im Widerspruch zur Transzendenz von j . Offenbar hat $F_n(X, Y)$ damit den Grad r in X .

Bei den Funktionen $P_k(j(M_1\tau), \dots, j(M_r\tau)) \in \mathbb{Q}[j(\tau)]$ hat die höchste auftretende Polordnung in ∞ die Ordnung $r = \sigma_1(n)$ und diese tritt nur bei P_r auf, wie man an der genaueren Darstellung der P_k nach Satz (3.1) sehen kann, denn einzig für $k = r$ werden hier r Funktionen mit einem Pol der Ordnung 1 bei ∞ multipliziert. Für $0 \leq k < r$ werden hingegen höchstens $r - 1$ Funktionen mit einem Pol der Ordnung 1 bei ∞ multipliziert, wodurch diese nicht die Ordnung r in ∞ besitzen können. Da die Ordnung des Pols aber mit dem Grad des Polynoms in $\mathbb{Q}[j]$ übereinstimmen muss (das ergibt ein einfacher Koeffizientenvergleich, den wir auch schon in Paragraph 2 gesehen haben), sind alle $P_k(j(M_1\tau), \dots, j(M_r\tau))$ für $0 \leq k < r$ Polynome in $j(\tau)$ von einem Grad $< r$ und für $k = r$ ein Polynom in $j(\tau)$ vom Grad r . Demnach hat $F_n(X, Y)$ in Y ebenfalls den Grad r . \square

In Anlehnung an [K] I. 7.3 nennt man $F_n(X, Y) = 0$ die Modulargleichung vom Grad n . Wir wollen diese an einem Beispiel noch etwas genauer betrachten.

(3.3) Beispiel

Es gilt $F_1(X, Y) = X - Y$. Betrachte dazu

$$\begin{aligned} F_1(X, j(\tau)) &= \prod_{M \in \Gamma: \Gamma_1} (X - j(M\tau)) \\ &= X - j\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tau\right) \\ &= X - j(\tau) \quad \text{für alle } \tau \in \mathbb{H}. \end{aligned}$$

Wegen der Eindeutigkeit von $F_1(X, Y)$ nach Proposition (3.2) gilt damit bereits $F_1(X, Y) = X - Y$. \diamond

— *Eigenschaften von $F_n(X, Y)$* —

Für das weitere Vorgehen benötigen wir als Hilfsmittel das folgende

(3.4) Lemma

Ist $n \in \mathbb{N}$ quadratfrei, so gibt es zu jedem $M \in \Gamma_n$ Matrizen $K, L \in \Gamma$ mit

$$KML = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}. \quad \diamond$$

Beweis

Wegen [K] IV. 1.2 (2) können wir von der Form

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

mit $ad = n$ und $b \pmod{d}$ ausgehen. Weil n quadratfrei ist, sind a und d teilerfremd. Nach [K] Lemma II. 3.2 existiert ein $x \in \mathbb{Z}$, so dass $xa + b$ und d bereits teilerfremd sind. Wähle nun $\alpha, \beta \in \mathbb{Z}$ mit $\alpha(xa + b) + \beta d = 1$. Dann folgt mit

$$K = \begin{pmatrix} \alpha & \beta \\ -d & xa + b \end{pmatrix} \text{ und } L = \begin{pmatrix} x & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & \alpha a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} x & \alpha ax - 1 \\ 1 & \alpha a \end{pmatrix}$$

(wobei K und L offensichtlich in Γ liegen, da sie beide Determinante 1 haben) die Behauptung, denn es gilt dann

$$\begin{aligned} KML &= \begin{pmatrix} \alpha & \beta \\ -d & xa + b \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} x & \alpha ax - 1 \\ 1 & \alpha a \end{pmatrix} \\ &= \begin{pmatrix} \alpha a & \alpha b + \beta d \\ -ad & -bd + dxa + bd \end{pmatrix} \begin{pmatrix} x & \alpha ax - 1 \\ 1 & \alpha a \end{pmatrix} \\ &= \begin{pmatrix} \alpha ax + \alpha b + \beta d & \alpha^2 a^2 x - \alpha a + \alpha^2 ab + \alpha a \beta d \\ -ad x + ad x & -\alpha a^2 x d + ad + \alpha d x a^2 \end{pmatrix} \\ &= \begin{pmatrix} \alpha(ax + b) + \beta d & \alpha^2 a(ax - b) + \alpha a \beta d - \alpha a \\ 0 & ad \end{pmatrix} \\ &= \begin{pmatrix} 1 & \alpha a \cdot 1 - \alpha a \\ 0 & n \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}. \quad \square \end{aligned}$$

Dieses Lemma wollen wir nun noch mit einem Beispiel verdeutlichen und zudem zeigen, dass die Darstellung keinesfalls eindeutig ist.

(3.5) Beispiel

Sei $n = 10$ und $M = \begin{pmatrix} 2 & 3 \\ 0 & 5 \end{pmatrix}$. Da der Beweis des obigen Lemmas konstruktiv ist, wissen wir, dass wir nun $xa + b = 2x + 3$ so wählen müssen, dass $2x + 3$ und 5 teilerfremd sind. Es sind -1 und 2 zwei Möglichkeiten, diese Bedingung zu erfüllen. Nun sollen $\alpha, \beta \in \mathbb{Z}$ so gewählt werden, dass

$$\alpha(2x + 3) + \beta \cdot 5 = \alpha(-2 + 3) + \beta \cdot 5 = \alpha + \beta \cdot 5 = 1 \text{ für } x = -1,$$

beziehungsweise so, dass

$$\alpha(2x + 3) + \beta \cdot 5 = \alpha(4 + 3) + \beta \cdot 5 = \alpha \cdot 7 + \beta \cdot 5 = 1 \text{ für } x = 2.$$

Wähle also zum Beispiel $\alpha = 6$ und $\beta = -1$ für $x = -1$ sowie $\alpha = -2$ und $\beta = 3$ für $x = 2$. Dann ergeben sich

$$K = \begin{pmatrix} 6 & -1 \\ -5 & 1 \end{pmatrix} \text{ und } L = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 12 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & -13 \\ 1 & 12 \end{pmatrix} \text{ für } x = -1,$$

sowie

$$K = \begin{pmatrix} -2 & 3 \\ -5 & 7 \end{pmatrix} \text{ und } L = \begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -4 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & -9 \\ 1 & -4 \end{pmatrix} \text{ für } x = 2,$$

und damit

$$\begin{aligned} KML &= \begin{pmatrix} 6 & -1 \\ -5 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 0 & 5 \end{pmatrix} \begin{pmatrix} -1 & -13 \\ 1 & 12 \end{pmatrix} \\ &= \begin{pmatrix} 12 & 13 \\ -10 & -10 \end{pmatrix} \begin{pmatrix} -1 & -13 \\ 1 & 12 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 10 \end{pmatrix} \quad \text{für } x = -1, \end{aligned}$$

sowie

$$\begin{aligned} KML &= \begin{pmatrix} -2 & 3 \\ -5 & 7 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 0 & 5 \end{pmatrix} \begin{pmatrix} 2 & -9 \\ 1 & -4 \end{pmatrix} \\ &= \begin{pmatrix} -4 & 9 \\ -10 & 20 \end{pmatrix} \begin{pmatrix} 2 & -9 \\ 1 & -4 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 10 \end{pmatrix} \quad \text{für } x = 2. \end{aligned}$$

◇

Sei nun $\mathbb{K} = \mathbb{V}_0$ wieder der Körper der Modulfunktionen. Dann kommen wir zu dem zentralen

(3.6) Satz

Sei $n \in \mathbb{N}, n \geq 2$, quadratfrei. Dann ist

$$F_n(X, j) \in \mathbb{K}[X]$$

irreduzibel. Es gilt

$$F_n(X, Y) = F_n(Y, X) \quad \text{und} \quad F_n(X, X) \in \mathbb{Q}[X] \setminus \{0\}. \quad \diamond$$

Beweis

Für festes $L \in \Gamma$ durchläuft nach dem Beweis von [K] IV. 1.3 mit M auch ML ein Rechtsvertretersystem von Γ_n nach Γ . Nach Proposition (3.2) ist $F_n(X, j) \in \mathbb{Q}[X, j]$, also gilt $F_n(X, j) \in \mathbb{K}[X]$, da $j \in \mathbb{K}$. Betrachte nun die Abbildung

$$\varphi : \mathbb{K}' \rightarrow \mathbb{K}', f \mapsto f \circ L, \text{ mit } \mathbb{K}' = \mathbb{K}[\tau \mapsto j(M\tau), M \in \Gamma_n].$$

Für alle $M \in \Gamma_n$ gilt

$$\varphi(\tau \mapsto j(M\tau)) = (\tau \mapsto j(ML\tau)) \in \mathbb{K}' \text{ für alle } \tau \in \mathbb{H}$$

da für $L \in \Gamma$ die Matrix ML offenbar wieder in Γ_n liegt. Damit ist φ wohldefiniert. Es gilt sogar für $f \in \mathbb{K}$ und $L \in \Gamma$, dass

$$f(L\tau) = f(\tau) \text{ für alle } \tau \in \mathbb{H}, \text{ also } \varphi|_{\mathbb{K}} = \text{Id}|_{\mathbb{K}}.$$

Zudem ist

$$\varphi(f + g) = (f + g) \circ L = f \circ L + g \circ L = \varphi(f) + \varphi(g) \text{ für alle } f, g \in \mathbb{K}'$$

und

$$\varphi(f \cdot g) = (f \cdot g) \circ L = (f \circ L)(g \circ L) = \varphi(f)\varphi(g) \text{ für alle } f, g \in \mathbb{K}',$$

das heißt φ ist ein Homomorphismus. Definiere nun $\psi : \mathbb{K}' \rightarrow \mathbb{K}', f \mapsto f \circ L^{-1}$. Dann gilt

$$(\varphi \circ \psi)(f) = \varphi(f \circ L^{-1}) = f \circ L^{-1} \circ L = f$$

und

$$(\psi \circ \varphi)(f) = \psi(f \circ L) = f \circ L \circ L^{-1} = f$$

für alle $f \in \mathbb{K}'$, das heißt φ ist bijektiv mit Umkehrabbildung ψ . Insgesamt ist φ also ein Automorphismus des Zerfällungskörpers \mathbb{K}' von $F_n(X, j)$ über \mathbb{K} .

Zu $M \in \Gamma_n$ wähle nun $K, L \in \Gamma$ nach Lemma (3.5), also so, dass $KML = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}$. Damit erhält man, dass

$$KM\tau = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} L^{-1}\tau = \frac{L^{-1}\tau}{n}$$

und damit

$$j(M\tau) = j(KM\tau) = j\left(\frac{L^{-1}\tau}{n}\right)$$

gilt. Folglich entstehen alle Nullstellen $X = j(M\tau)$ für $M \in \Gamma_n$ des Polynoms $F_n(X, j)$ aus der speziellen Nullstelle $X = j(\frac{\tau}{n})$ für $M = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}$ durch Anwendung von Automorphismen von \mathbb{K}' über \mathbb{K} . Angenommen, $F_n(X, j)$ wäre nicht irreduzibel über \mathbb{K} , dann hätte $F_n(X, j)$ eine Darstellung $F_n(X, j) = pq$ mit $p, q \in \mathbb{K}[X]$ und p, q keine Einheiten. Sei nun x Nullstelle von $F_n(X, j)$. Dann ist ohne Einschränkung x auch Nullstelle von p (sonst vertausche p und q), aber damit gilt auch $p(\sigma_1(x)) = \sigma_1(p(x)) = \sigma_1(0) = 0$ für jeden beliebigen Automorphismus σ_1 von \mathbb{K}' über \mathbb{K} . Da alle Nullstellen von $F_n(X, j)$ aber durch Anwendung von Automorphismen von \mathbb{K}' über \mathbb{K} entstehen, haben $F_n(X, j)$ und p bereits denselben Grad, und somit muss q eine Einheit sein, im Widerspruch zur Voraussetzung. Deshalb ist $F_n(X, j)$ irreduzibel über \mathbb{K} .

Es bleibt also zu zeigen, dass

$$F_n(X, Y) = F_n(Y, X) \quad \text{und} \quad F_n(X, X) \in \mathbb{Q}[X] \setminus \{0\}$$

gilt. Aus $\begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} \in \Gamma_n$ folgt

$$F_n(j(n\tau), j(\tau)) = \prod_{M \in \Gamma: \Gamma_n} (j(n\tau) - j(M\tau)) = 0 \quad \text{für alle } \tau \in \mathbb{H},$$

wobei man ohne Einschränkung das Standard-Rechtsvertreterssystem wählen kann (denn dann gilt $\begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} \in \Gamma : \Gamma_n$). Ersetzt man nun τ durch $\frac{\tau}{n}$, so folgt

$$F_n(j(\tau), j(\frac{\tau}{n})) = 0 \quad \text{für alle } \tau \in \mathbb{H},$$

also ist $F_n(j(\tau), Y) \in \mathbb{K}[Y]$ durch $Y - j(\frac{\tau}{n})$ teilbar. Weil das Polynom

$$F_n(Y, j(\tau)) = \prod_{M \in \Gamma: \Gamma_n} (Y - j(M\tau))$$

wie oben gezeigt irreduzibel ist und mit dem Standard-Rechtsvertreterssystem der Faktor $Y - j(\frac{\tau}{n})$ auftaucht (nämlich für $M = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}$), also $F_n(Y, j(\tau))$ durch $Y - j(\frac{\tau}{n})$ teilbar ist, folgt, dass auch das Polynom $F_n(j(\tau), Y) \in \mathbb{K}[Y]$ durch $F_n(Y, j(\tau))$ teilbar ist. Da beide Polynome nach Proposition (3.2) in Y den Grad $\sigma_1(n) = r$ haben und in $\mathbb{Q}[X, Y]$ liegen, gibt es ein $c \in \mathbb{Q}$ mit

$$F_n(X, Y) = cF_n(Y, X).$$

Setze nun $X = Y$, dann folgt

$$F_n(X, X) = cF_n(X, X),$$

also $c = 1$ oder $F_n(X, X) = 0$. Für $F_n(X, X) = 0$ hätte aber $F_n(X, j)$ die Funktion j als Nullstelle, wäre also durch $X - j$ teilbar, was wegen $r = \sigma_1(n) > 1$ aber der Irreduzibilität widerspricht. Demnach muss bereits $F_n(X, X) \neq 0$ und damit $c = 1$ gelten. \square

— Folgerung aus Satz (3.6) —

Als Anwendung von Satz (3.6) zeigen wir den folgenden

(3.7) Satz

Gehört $\tau \in \mathbb{H}$ zu einem imaginär-quadratischen Zahlkörper, so ist $j(\tau)$ eine algebraische Zahl. \diamond

Beweis

Gehört $\tau \in \mathbb{H}$ zu einem imaginär-quadratischen Zahlkörper, so besitzt τ eine Darstellung

$$\tau = \frac{1}{d}(b + ia\sqrt{D}), \quad b \in \mathbb{Z}, \quad a, d, D \in \mathbb{N}, \quad D \text{ quadratfrei.}$$

Zunächst gilt dann:

$$\begin{pmatrix} 1 & 0 \\ 0 & D \end{pmatrix} \langle i\sqrt{D} \rangle = \frac{i\sqrt{D}}{D} = \frac{i}{\sqrt{D}} = \frac{-1}{i\sqrt{D}} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \langle i\sqrt{D} \rangle = J \langle i\sqrt{D} \rangle,$$

also

$$j(i\sqrt{D}) \stackrel{J \in \Gamma}{=} j(J \langle i\sqrt{D} \rangle) = j\left(\frac{i}{\sqrt{D}}\right) = j\left(\frac{i\sqrt{D}}{D}\right).$$

Für $D = 1$ hat man $j(i\sqrt{1}) = j(i) = 1728 \in \mathbb{Q}$ und für $D > 1$ ist $j(i\sqrt{D})$ nach Proposition (3.2) und Satz (3.6) Nullstelle des Polynoms $F_D(X, X) \in \mathbb{Q}[X] \setminus \{0\}$, denn

$$F_D(j(i\sqrt{D}), j(i\sqrt{D})) = \prod_{M \in \Gamma_D} (j(i\sqrt{D}) - j(Mi\sqrt{D})) = 0,$$

da für $\tilde{M} = \begin{pmatrix} 1 & 0 \\ 0 & D \end{pmatrix} \in \Gamma_D$ gilt $j(\tilde{M}i\sqrt{D}) = j\left(\frac{i\sqrt{D}}{D}\right)$ und $F_n(j(\tau), j\left(\frac{\tau}{n}\right)) = 0$ für alle $\tau \in \mathbb{H}$ nach dem Beweis zu (3.6), also insbesondere für $\tau = i\sqrt{D}$ und $n = D$. Folglich ist $j(i\sqrt{D})$ algebraisch über \mathbb{Q} .

Sei nun $ad = n$ und $b \in \mathbb{Z}$, also

$$M = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \Gamma_n \text{ mit } M \langle i\sqrt{D} \rangle = \frac{ai\sqrt{D} + b}{d} = \tau.$$

Nach Proposition (3.2) ist $j(\tau)$ Nullstelle des normierten Polynoms

$$F_n(X, j(i\sqrt{D})) = \prod_{\tilde{M} \in \Gamma_n} (X - \underbrace{j(\tilde{M}i\sqrt{D})}_{=j(\tau) \text{ für } \tilde{M}=M}) \in \mathbb{Q}(j(i\sqrt{D}))[X],$$

also algebraisch über $\mathbb{Q}(j(i\sqrt{D}))$ und damit ebenfalls algebraisch über \mathbb{Q} , da die Erweiterungen $\mathbb{Q}(j(i\sqrt{D})) : \mathbb{Q}$ und $\mathbb{Q}(j(\tau), j(i\sqrt{D})) : \mathbb{Q}(j(i\sqrt{D}))$ endlich sind, und damit nach Algebra I auch die Erweiterung $\mathbb{Q}(j(\tau), j(i\sqrt{D})) : \mathbb{Q}$ endlich ist. \square