

Die Algebra der Modulformen

Vortrag zum Seminar „Gitter und Codes“

Jendrik Brachter

04.05.2015

Abstract

Ziel des Vortrags ist es zu zeigen, dass die Menge der Modulformen eine durch das Gewicht graduierte \mathbb{C} -Algebra bildet. Wir werden sehen, dass die normierten Eisensteinreihen E_4 und E_6 ein Erzeugendensystem für diese Algebra bilden. Darüber hinaus erhält man als Folgerung die Eindeutigkeit des \mathbb{E}_8 -Gitters als unimodulares gerades Gitter von Rang ≤ 8 .

1 Die Gewichtsformel

Wir wollen im ersten Abschnitt die Gewichtsformel für Modulformen erarbeiten. Dazu zunächst einige Grundlagen und Definitionen.

Im Folgenden bezeichnen wir für jede ganze Zahl k die Menge der Modulformen von Gewicht k mit M_k .

Lemma 1.1 *Für jede ganze Zahl k ist M_k ein \mathbb{C} -Vektorraum.*

BEWEIS Seien $f, g \in M_k$ Modulformen von Gewicht k , $\alpha \in \mathbb{C}$. Dann sind f und g holomorph auf \mathbb{H} , also ist auch $\alpha f + g$ holomorph auf \mathbb{H} . Weiter gilt für jedes τ aus \mathbb{H}

$$\begin{aligned}(\alpha f + g) \left(\frac{a\tau + b}{c\tau + d} \right) &= \alpha(c\tau + d)^k \cdot f(\tau) + (c\tau + d)^k \cdot g(\tau) \\ &= (c\tau + d)^k \cdot (\alpha f + g)(\tau) ,\end{aligned}$$

für alle $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Eine Fourier-Entwicklung von $(\alpha f + g)$ ergibt sich aus den Fourier-Entwicklungen von f und g . ■

Wir wissen bereits, dass Modulformen in jedem Punkt $p \in \mathbb{H}$ in eine Potenzreihe entwickelbar sind. So wie wir die Modulformen eingeführt haben gilt per Definition, dass jede Modulform f außerdem eine Potenzreihenentwicklung in $q = e^{2\pi i\tau}$, also genauer eine Fourier-Entwicklung der Form

$$f(\tau) = \sum_{m \geq m_0}^{\infty} a_m q^m$$

besitzt, wobei wir $m_0 \geq 0$ voraussetzen. Wir werden diese Eigenschaften ausnutzen um die Ordnung einer Modulform in einem Punkt $p \in \mathbb{H}$ zu definieren.

Definition 1.2 Die kleinste nicht-negative ganze Zahl r , für die der Koeffizient a_r in der Potenzreihenentwicklung von f um p von Null verschieden ist, heißt die **Ordnung** von f in p und wird mit $\nu_p(f)$ bezeichnet. Außerdem bezeichne $\nu_{i\infty}(f)$ den Index des kleinsten von Null verschiedenen Koeffizienten in der Fourier-Entwicklung von f .

Zur Vorbereitung auf das nächste Lemma benötigen wir eine Aussage aus der Funktionentheorie, die wir ohne Beweis angeben.

Lemma 1.3 Seien $U \subset \mathbb{C}$ offen, $z_0 \in U$ und $f : U \rightarrow \mathbb{C}$ holomorph. Dann sind äquivalent:

(i) f hat in z_0 eine Nullstelle der Ordnung n .

(ii) Die Potenzreihenentwicklung von f um z_0 hat die Form

$$f(z) = \sum_{k=n}^{\infty} a_k (z - z_0)^k \text{ mit } a_n \neq 0.$$

(iii) Es gibt ein $r > 0$ und eine holomorphe Funktion $g : K_r(z_0) \rightarrow \mathbb{C}$ mit

$$f(z) = (z - z_0)^n g(z)$$

für alle $z \in K_r(z_0) \cap U$ und $g(z_0) \neq 0$.

Wir sehen also, dass $\nu_p(f)$ tatsächlich die Nullstellenordnung von f in p beschreibt. Die Darstellung aus (iii) wird sich im folgenden Beweis als sehr nützlich erweisen.

Lemma 1.4 Es ist $\nu_p(f) = \nu_{gp}(f)$ für alle $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G := \mathrm{SL}_2(\mathbb{Z})/\{\pm 1\}$.

BEWEIS Sei $q = g^{-1}p$. Aus dem vorangehenden Lemma erhält man, dass $\nu_p(f) = n$ gilt, genau dann, wenn eine in einer Umgebung von p holomorphe Funktion h existiert mit $h(p) \neq 0$ und $f(\tau) = (\tau - p)^n \cdot h(\tau)$. Also hat man

$$\begin{aligned} f(\tau) &= (c\tau + d)^{-k} f(g\tau) = (c\tau + d)^{-k} \cdot (g\tau - gq)^n h(g\tau) \\ &= (\tau - q)^n \cdot \underbrace{((c\tau + d)^{-k-n} (cq + d)^{-n} h(g\tau))}_{:=h'(\tau)}. \end{aligned}$$

Dabei ist $h'(\tau)$ holomorph auf einer Umgebung von q und $h'(q) \neq 0$, also ist $\nu_q(f) = n = \nu_p(f)$. ■

Somit hängt $\nu_p(f)$ also nur von der Restklasse von p in \mathbb{H}/G ab. Im Folgenden bezeichne stets $G := \mathrm{SL}_2(\mathbb{Z})/\{\pm 1\}$, sowie $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ und $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Lemma 1.5 *Für $p \in \mathbb{H}$ gilt*

$$|\mathrm{Stab}_G(p)| = \begin{cases} 2, & p \equiv i \pmod{G}, \\ 3, & p \equiv \eta \pmod{G}, \\ 1, & \text{sonst.} \end{cases}$$

BEWEIS Wir haben im Vortrag zu Modulformen bereits die Stabilisatoren für jedes $p \in D$ bestimmt, wobei D den Fundamentalbereich der Operation der Modulgruppe bezeichne. Der Beweis ergibt sich nun aus der Tatsache, dass $S\eta = -\bar{\eta}$ gilt und sich die Stabilisatorordnung unter Kongruenz erhält. ■

Um die Gewichtformel beweisen zu können benötigen wir erneut Aussagen aus der Funktionentheorie.

Satz 1.6 (Identitätssatz) *Sei $G \subset \mathbb{C}$ ein Gebiet und $f : G \rightarrow \mathbb{C}$ holomorph. Dann sind äquivalent:*

(i) $f \equiv 0$,

(ii) *Die Nullstellenmenge von f hat einen Häufungspunkt in G .*

Satz 1.7 (Argumentprinzip) *Sei $U \subset \mathbb{C}$ offen, $f : U \rightarrow \mathbb{C} \cup \{\infty\}$ meromorph und auf keiner Wegzusammenhangskomponente von U konstant. Seien a_1, a_2, \dots die Nullstellen bzw. b_1, b_2, \dots die Polstellen von f in U jeweils mit Ordnung $\nu_{a_t}(f)$ bzw. $\mu_{b_t}(f)$. Dann gilt für jeden nullhomologen Zyklus Γ in U , der keinen dieser Punkte trifft*

$$\frac{1}{2\pi i} \int_{\Gamma} \frac{f'(z)}{f(z)} dz = \sum_t \nu_{a_t}(f) \cdot n_{\Gamma}(a_t) - \sum_{t'} \nu_{b_{t'}}(f) \cdot n_{\Gamma}(b_{t'}).$$

Dabei bezeichnet $n_{\Gamma}(a_t)$ die Umlaufzahl von a_t . Diese besitzt für Umlaufrichtung im Uhrzeigersinn ein negatives, sonst ein positives Vorzeichen. (Für eine exakte Definition der Umlaufzahl verweisen wir auf [2].)

Lemma 1.8 *Ist f auf \mathbb{H} holomorph und 1-periodisch, so existiert eine auf $K_1(0) \setminus \{0\}$ holomorphe Funktion F mit der Eigenschaft*

$$f(\tau) = F(e^{2\pi i \tau}).$$

Ist F auf $K_1(0)$ holomorph fortsetzbar, so ist f in eine Fourier-Reihe

$$f(\tau) = \sum_{m \geq m_0} a_m e^{2\pi i m \tau}$$

entwickelbar. In Übereinstimmung mit dem Verhalten von F bei 0 sagt man, dass f bei $i\infty$ holomorph ist, falls $m_0 \geq 0$ gilt und eine Nullstelle der Ordnung m_0 hat, falls $m_0 > 0$ gilt.

Nun haben wir die nötigen Voraussetzungen gegeben um die Gewichtformel zu formulieren.

Satz 1.9 (Gewichtformel für Modulformen) Sei $0 \neq f$ eine Modulform von Gewicht k . Es gilt

$$\nu_{i\infty}(f) + \sum_{p \in \mathbb{H}/G} \frac{1}{|\text{Stab}_G(p)|} \nu_p(f) = \nu_{i\infty}(f) + \frac{1}{2} \nu_i(f) + \frac{1}{3} \nu_\eta(f) + \sum_{\substack{p \neq [i], [\eta] \\ p \in \mathbb{H}/G}} \nu_p(f) = \frac{k}{12}.$$

BEWEIS Sei zunächst $0 \neq f$ konstant, dann ist $\nu_p(f) = 0$ für jedes $p \in \mathbb{H} \cup \{i\infty\}$ und f hat Gewicht 0, also ist die Gleichung erfüllt. Sei also im Folgenden f eine nicht konstante Modulform von Gewicht k .

Da f holomorph in $i\infty$ ist, existiert eine Funktion F wie in (1.8), welche in 0 holomorph fortsetzbar ist und ein $\rho > 0$, sodass F nach dem Identitätssatz keine Nullstellen für $0 < |q| < \rho$ besitzt. Wir definieren durch die Ungleichung $\text{Im}(\tau) \leq e^{2\pi\rho}$ eine kompakte Teilmenge D_ρ von D . Da f außerdem holomorph auf \mathbb{H} ist, können wir den Identitätssatz auf beliebige Gebiete in \mathbb{H} anwenden und können so insgesamt sicherstellen, dass höchstens endlich viele Nullstellen von f in D_ρ und keine Nullstellen von f außerhalb von D_ρ existieren. Wir wollen nun den Satz vom Argumentprinzip anwenden, also die logarithmische Ableitung von f entlang des Randes von D_ρ integrieren. Allerdings können wir nicht ausschließen, dass f Nullstellen im Integrationsweg besitzt. Deswegen modifizieren wir den Integrationsweg so, dass wir auftretende Nullstellen umlaufen. Das ist stets möglich, da f nur endlich viele Nullstellen besitzt (vgl. Abbildung 1).

Dabei wählen wir den Radius ϵ der Kreise um die Nullstellen mit Hilfe des Identitätssatzes so klein, dass der modifizierte Weg \mathfrak{C} gerade die Nullstellen von f in D_ρ aber keine neuen Nullstellen umläuft. Mit dem Satz vom Argumentprinzip erhalten wir dann

$$\frac{1}{2\pi i} \int_{\mathfrak{C}} \frac{f'(\tau)}{f(\tau)} d\tau = \sum_{\substack{p \neq [i], [\eta] \\ p \in \mathbb{H}/G}} \nu_p(f).$$

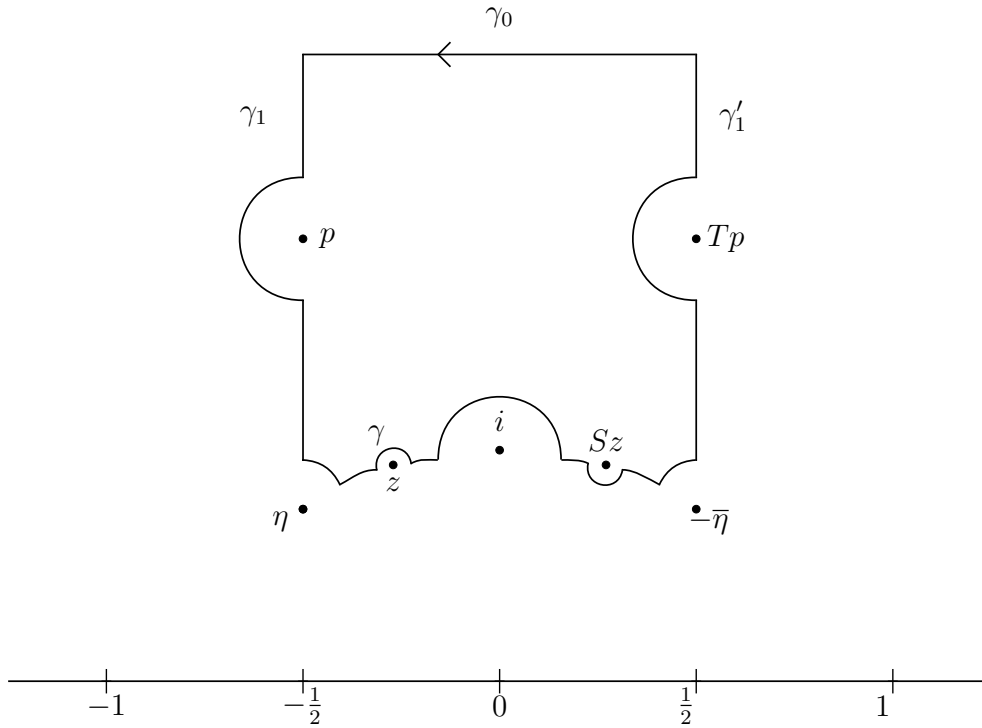


Abbildung 1: Modifizierter Integrationsweg \mathfrak{C}

Dabei ist per Wahl des Radius die Summe auf der rechten Seite nicht abhängig von ϵ , sodass wir den Grenzwert

$$\lim_{\epsilon \rightarrow 0} \int_{\mathfrak{C}} \frac{f'(\tau)}{f(\tau)} d\tau = \lim_{\epsilon \rightarrow 0} \sum_{\substack{p \neq [i], [\eta] \\ p \in \mathbb{H}/G}} \nu_p(f) = \sum_{\substack{p \neq [i], [\eta] \\ p \in \mathbb{H}/G}} \nu_p(f)$$

betrachten können. Wir teilen den Integrationsweg entsprechend Abbildung 1 auf und berechnen im Folgenden die Integrale entlang der Wegstücke.

Wir haben schon gesehen, dass Modulformen 1-periodisch sind. Also löschen sich Teile des Integrationsweges gegenseitig aus, denn es ist

$$\int_{\gamma_1} \frac{f'(\tau)}{f(\tau)} d\tau = - \int_{\gamma_1} \frac{f'(\tau)}{f(\tau)} d\tau = - \int_{\gamma_1} \frac{f'(\tau+1)}{f(\tau+1)} d\tau = - \int_{\gamma'_1} \frac{f'(\tau)}{f(\tau)} d\tau.$$

Betrachten wir als nächstes den Weg γ_0 unter der Transformation $\varphi : \tau \mapsto e^{2\pi i \tau}$. Es ist

$$\gamma_0 = \left\{ x + ie^{2\pi i \rho} \mid x \in \left[-\frac{1}{2}, \frac{1}{2} \right] \right\},$$

also wird $\tau \in \gamma_0$ abgebildet auf

$$e^{-2\pi e^{2\pi\rho}} \cdot e^{2\pi i x}$$

mit $x \in [-\frac{1}{2}, \frac{1}{2}]$, also $2\pi i x \in [-\pi i, \pi i]$. Somit wird der Weg γ_0 auf einen Kreis mit Radius $e^{-2\pi e^{2\pi\rho}} < 1$ um Null abgebildet, wobei eine Vergrößerung des Imaginärteils in einer Verkleinerung des Radius resultiert. Per Wahl von ρ gilt dann, dass die einzige Nullstelle von f im Inneren dieses Kreises bei $i\infty$ liegen kann. Somit erhalten wir wieder mit dem Argumentprinzip

$$\int_{\gamma_0} \frac{f'(\tau)}{f(\tau)} d\tau = \int_{\gamma_0} \frac{F'(e^{2\pi i \tau})}{F(e^{2\pi i \tau})} d\tau = \int_{\varphi(\gamma_0)} \frac{F'(\tau)}{F(\tau)} d\tau = -2\pi i \nu_{i\infty}(f).$$

Das negative Vorzeichen resultiert dabei aus der Umlaufrichtung im Uhrzeigersinn.

Betrachten wir nun das Integral entlang des unteren Randes von D_ρ . Für $(x + iy) \in \mathbb{H}$ gilt

$$S(x + iy) = \frac{-1}{x + iy} = \frac{1}{|x + iy|} (-x + iy).$$

Also ist $Si = i$ und Werte auf dem Einheitskreis werden an der imaginären Achse gespiegelt. Außerdem muss dann für $\text{Im } \tau > 1$ schon $\text{Im } S\tau < 1$ gelten und umgekehrt. Da die Operation mit S der stetigen Abbildung $(\tau \rightarrow -\frac{1}{\tau})$ entspricht erhalten wir zwei Wege γ und $S\gamma$ wie in Abbildung 2.

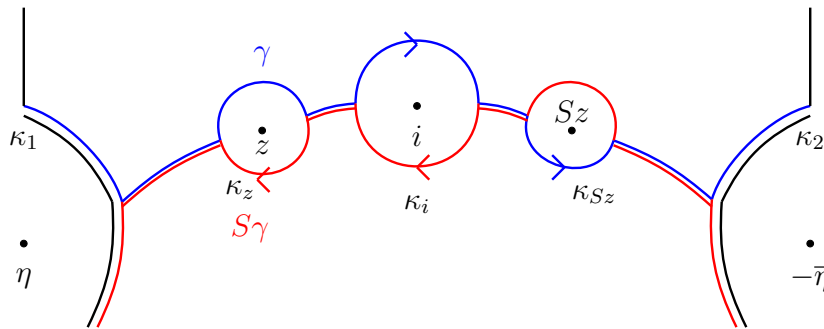


Abbildung 2: Die Wege γ und $S\gamma$

Mit der Identität $f(S\tau) = \tau^k f(\tau)$ erhält man

$$\frac{f'(S\tau)}{f(S\tau)} = \frac{k\tau^{k-1}f(\tau) + \tau^k f'(\tau)}{\tau^k f(\tau)} = k\frac{1}{\tau} + \frac{f'(\tau)}{f(\tau)}.$$

Damit gilt dann

$$\begin{aligned} & \int_{\kappa_1} \frac{f'(\tau)}{f(\tau)} d\tau + \int_{\kappa_z} \frac{f'(\tau)}{f(\tau)} d\tau + \int_{\kappa_i} \frac{f'(\tau)}{f(\tau)} d\tau + \int_{\kappa_{S_z}} \frac{f'(\tau)}{f(\tau)} d\tau + \int_{\kappa_2} \frac{f'(\tau)}{f(\tau)} d\tau = \\ & \int_{\gamma+S\gamma} \frac{f'(\tau)}{f(\tau)} d\tau = \int_{\gamma} \frac{f'(\tau)}{f(\tau)} d\tau + \int_{\gamma} \frac{f'(\tau)}{f(\tau)} d\tau + \int_{\gamma} \frac{k}{\tau} d\tau, \end{aligned}$$

wobei wir mit κ_1 bzw. κ_2 die Bögen um η und $-\bar{\eta}$ bezeichnen. Also ist

$$\begin{aligned} 2 \lim_{\epsilon \rightarrow 0} \int_{\gamma} \frac{f'(\tau)}{f(\tau)} d\tau &= \lim_{\epsilon \rightarrow 0} \left(\int_{\kappa_1} \frac{f'(\tau)}{f(\tau)} d\tau + \int_{\kappa_z} \frac{f'(\tau)}{f(\tau)} d\tau + \right. \\ & \left. \int_{\kappa_i} \frac{f'(\tau)}{f(\tau)} d\tau + \int_{\kappa_{S_z}} \frac{f'(\tau)}{f(\tau)} d\tau + \int_{\kappa_2} \frac{f'(\tau)}{f(\tau)} d\tau - \int_{\gamma} \frac{k}{\tau} d\tau \right) \\ &= 2\pi i (-\nu_i(f) - \nu_z(f) + \nu_z(f)) + \lim_{\epsilon \rightarrow 0} \left(\int_{\kappa_2} \frac{f'(\tau)}{f(\tau)} d\tau + \int_{\kappa_1} \frac{f'(\tau)}{f(\tau)} d\tau - \int_{\gamma} \frac{k}{\tau} d\tau \right) \end{aligned}$$

nach dem Argumentprinzip und wegen $\nu_z(f) = \nu_{S_z}(f)$. Der Winkel zwischen η und $S\eta$ ist $\frac{\pi}{3}$. Wenn wir den Integrationsweg geeignet parametrisieren erhalten wir

$$\lim_{\epsilon \rightarrow 0} \int_{\gamma} \frac{k}{\tau} d\tau = k \int_0^1 \frac{e^{-\frac{\pi i}{3}(2-\tau)}}{e^{\frac{\pi i}{3}(2-\tau)}} d\tau = -\frac{2\pi i k}{6}.$$

Durch anwenden von $T^{-1}S$ und $(T^{-1}S)^2$ auf κ_2 erhalten wir einen Zykel um $-\bar{\eta}$, also liefert uns das Argumentprinzip erneut zusammen mit der Unabhängigkeit der Nullstellenordnung vom Radius

$$\begin{aligned} 2\pi i \nu_{\eta}(f) &= 2\pi i \nu_{-\bar{\eta}}(f) = \lim_{\epsilon \rightarrow 0} \int_{\kappa_2 + (T^{-1}S)\kappa_2 + (T^{-1}S)^2\kappa_2} \frac{f'(\tau)}{f(\tau)} d\tau = \\ & 3 \lim_{\epsilon \rightarrow 0} \int_{\kappa_2} \frac{f'(\tau)}{f(\tau)} d\tau + \lim_{\epsilon \rightarrow 0} \int_{\kappa_2} \frac{k}{\tau} d\tau + \lim_{\epsilon \rightarrow 0} \int_{\kappa_2} \frac{k}{\tau-1} d\tau, \end{aligned}$$

wobei die beiden letzten Grenzwerte verschwinden. Also haben wir

$$\frac{1}{2\pi i} \lim_{\epsilon \rightarrow 0} \int_{\kappa_2} \frac{f'(\tau)}{f(\tau)} d\tau = \frac{1}{3} \nu_{\eta}(f).$$

Schließlich ergibt sich die gewünscht Formel durch

$$2\pi i \sum_{\substack{p \neq [i], [\eta] \\ p \in \mathbb{H}/G}} \nu_p(f) = \lim_{\epsilon \rightarrow 0} \int_{\mathfrak{C}} \frac{f'(\tau)}{f(\tau)} d\tau = 2\pi i \left(-\nu_{i\infty}(f) - \frac{1}{3} \nu_{\eta}(f) - \frac{1}{2} \nu_i(f) + \frac{k}{12} \right).$$

■

2 Die Algebra der Modulformen

Es sei $\mathcal{L} : M_k \rightarrow \mathbb{C}$, $f \mapsto f(i\infty)$ das lineare Funktional, welches eine Modulform von Gewicht k auf den Koeffizienten $a_0 = f(i\infty)$ in der Fourierentwicklung $f(\tau) = \sum_{r=0}^{\infty} a_r q^r$ abbildet. Der Kern dieser Abbildung bildet einen \mathbb{C} -Vektorraum, den wir mit M_k^0 bezeichnen. (Der Vektorraum der **Spitzenformen**.)

Lemma 2.1 Für $k \geq 4$ gerade gilt

$$M_k = M_k^0 \oplus \mathbb{C} E_k,$$

wobei E_k die normierte Eisensteinreihe von Gewicht k bezeichne.

BEWEIS Wegen der Linearität von \mathcal{L} gilt nach dem Homomorphiesatz

$$\dim(M_k/M_k^0) = \dim(M_k/\text{Ker}(\mathcal{L})) = \dim(\text{Img}(\mathcal{L})) \in \{0, 1\},$$

da $\text{Img}(\mathcal{L}) \subset \mathbb{C}$. Sei nun $k \geq 4$ gerade. Im Vortrag zu Eisensteinreihen haben wir bereits gesehen, dass für die normierte Eisensteinreihe immer $E_k \in M_k$ und $E_k(i\infty) = 1 \neq 0$ gilt. Also folgt zunächst $E_k \notin M_k^0$ und damit $\dim(M_k/M_k^0) = 1$. Wegen $E_k \in M_k \setminus M_k^0$ muss dann schon $M_k = M_k^0 \oplus \mathbb{C} E_k$ gelten. ■

Wir wollen nun Aussagen über die Struktur von M_k für wichtige Spezialfälle herleiten.

Satz 2.2 Es gilt

- (i) $M_k = \{0\}$ für $k < 0$, für k ungerade und für $k = 2$.
- (ii) $M_{k-12} \cong M_k^0$ vermöge Multiplikation mit $\Delta := \frac{1}{1728} (E_4^3 - E_6^2)$.
- (iii) $M_0 = \mathbb{C}$, $M_0^0 = \{0\}$ und für $k = 4, 6, 8, 10$ ist $M_k = \mathbb{C} E_k$.

BEWEIS Zu (i): Sei $0 \neq f \in M_k$. Die Gewichtsformel liefert

$$\nu_{i\infty}(f) + \frac{1}{2}\nu_i(f) + \frac{1}{3}\nu_\eta(f) + \sum_{\substack{p \neq [i, \eta] \\ p \in \mathbb{H}/G}} \nu_p(f) = \frac{k}{12}.$$

Per Definition sind alle Terme auf der linken Seite der Gleichung nicht-negativ, also gilt dies auch für k . Außerdem gilt $\nu_p \in \mathbb{N}_0$ für jedes $p \in \mathbb{H}$, sodass stets gelten muss

$$\frac{k}{12} = a \cdot \frac{1}{2} + b \cdot \frac{1}{3} + c,$$

für $a, b, c \in \mathbb{N}_0$. Insbesondere ist dann k gerade und $\frac{k}{12} \geq \frac{1}{3} > \frac{2}{12}$ für $k \neq 0$. Also ist $k \neq 2$. Insgesamt folgt damit die Behauptung.

Zu (ii): Die Multiplikation mit Δ ist linear.

Im Vortrag zu Eisensteinreihen haben wir bereits gesehen, dass $\nu_{i\infty}(\Delta) = 1$ gilt. Dann folgt wiederum aus der Gewichtsformel, dass für alle $p \in \mathbb{H}$ schon $\nu_p(\Delta) = 0$ gilt, was bedeutet, dass Δ auf \mathbb{H} stets ungleich 0 ist. Also liefert die Multiplikation mit Δ einen trivialen Kern und ist somit injektiv.

Sei nun $f \in M_k^0$ beliebig. Wegen $\Delta \neq 0$ auf \mathbb{H} können wir $g := \frac{f}{\Delta}$ setzen. Wir zeigen $g \in M_{k-12}$. Da f eine Modulform von Gewicht k ist und Δ eine Modulform von Gewicht 12, gilt

$$g\left(\frac{a\tau + b}{c\tau + d}\right) = \frac{(c\tau + d)^k f(\tau)}{(c\tau + d)^{12} \Delta(\tau)} = (c\tau + d)^{k-12} g(\tau).$$

Da Δ auf \mathbb{H} nicht verschwindet ist Δ^{-1} und damit auch g holomorph auf \mathbb{H} . Für $p \in \mathbb{H}$ haben wir gesehen, dass $\nu_p(g) = \nu_p(f)$ gilt. Wegen $\nu_{i\infty}(\Delta) = 1$ besitzt g in $i\infty$ einen Pol erster Ordnung. In diesem Fall ergibt sich die Ordnung von g in $i\infty$ durch

$$\nu_{i\infty}(g) = \nu_{i\infty}(f) - \nu_{i\infty}(\Delta) = \nu_{i\infty}(f) - 1,$$

also $\nu_{i\infty}(g) \geq 0$, da $f \in M_k^0$. Das bedeutet aber gerade, dass g holomorph in $i\infty$ ist. Also ist $g \in M_{k-12}$ und $\Delta g = f$. Das heißt die Multiplikation mit Δ ist auch surjektiv.

Zu (iii): Sei $k \leq 10$, also $k - 12 < 0$. Nach (i) und (ii) gilt dann $M_k^0 \cong M_{k-12} = \{0\}$. Also gilt $M_k = \mathbb{C} E_k$ für $k = 4, 6, 8, 10$. Sei nun f eine Modulform von Gewicht 0. Wäre f nicht konstant, würde die Gewichtsformel für $(f - f(i)) \in M_0$ einen Widerspruch liefern. Wäre nämlich f nicht konstant, so wäre $f - f(i) \neq 0$ und nach der Gewichtsformel müsste für jedes $p \in \mathbb{H}/G$ dann $\nu_p(f - f(i)) = 0$ gelten. Insbesondere wäre also $\nu_i(f - f(i)) = 0$ und man hätte

$$(f - f(i))(\tau) = \sum_{r=0}^{\infty} a_r (\tau - i)^r = a_0 + \sum_{r=1}^{\infty} a_r (\tau - i)^r,$$

wobei a_0 nicht Null wäre. Speziell für $\tau = i$ folgt dann

$$0 = f(i) - f(i) = (f - f(i))(i) = a_0$$

und somit ein Widerspruch. Andererseits ist jede konstante Funktion holomorph und eine Modulform von Gewicht 0, daher können wir M_0 mit \mathbb{C} identifizieren. ■

Lemma 2.3 Für $\tau \in D$ gilt

$$E_4(\tau) = 0 \text{ genau dann, wenn } \tau = \eta$$

und

$$E_6(\tau) = 0 \text{ genau dann, wenn } \tau = i.$$

Außerdem ist $\nu_i(E_6) = \nu_\eta(E_4) = 1$.

BEWEIS Es ist

$$\nu_{i\infty}(E_4) + \frac{1}{2}\nu_i(E_4) + \frac{1}{3}\nu_\eta(E_4) + \sum_{\substack{p \neq [i], [\eta] \\ p \in \mathbb{H}/G}} \nu_p(E_4) = \frac{4}{12} = \frac{1}{3}.$$

Also ist $\nu_\eta = 1$ und $\nu_p = 0$ für alle $p \neq \eta$. Insbesondere ist $E_4(p) = 0$ genau dann, wenn $p = \eta$ gilt. Der Beweis für E_6 verläuft analog. ■

Per Definition ist klar, dass $f \equiv 0$ eine Modulform beliebigen Gewichts ist. Wir wollen das Gewicht einer Modulform $f \neq 0$ untersuchen.

Lemma 2.4 Das Gewicht einer nichttrivialen Modulform ist eindeutig bestimmt.

BEWEIS Sei $0 \neq f$ eine Modulform von Gewicht k und k' , und $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in G$. Dann gilt für jedes $\tau \in \mathbb{H}$ mit $f(\tau) \neq 0$ per Definition $f(S\tau) = \tau^k f(\tau) = \tau^{k'} f(\tau)$, also $\tau^k = \tau^{k'}$. Die Periodizität von f garantiert nun, dass es unendlich viele verschiedene solcher $\tau \in \mathbb{H}$ geben muss. Das bedeutet, dass die Polynome $p(x) = x^k$ und $q(x) = x^{k'}$ an unendlich vielen, also insbesondere an mehr als $\max\{k + 1, k' + 1\}$ Stellen übereinstimmen. Der Identitätssatz für Polynome liefert dann $k = k'$. ■

Wir benötigen noch eine weitere Definition, bevor wir zur Algebra der Modulformen kommen.

Definition 2.5 Sei K ein Körper, $(\Gamma, +)$ kommutativer Monoid. Eine Γ -**Graduierung** auf einem K -Vektorraum ist ein System $(V_\gamma)_{\gamma \in \Gamma}$ von Untervektorräumen von V , sodass gilt:

$$V = \bigoplus_{\gamma \in \Gamma} V_\gamma$$

Eine Γ -**Graduierung** auf einer K -Algebra A ist eine Graduierung auf A als Vektorraum, die zusätzlich folgende Eigenschaft erfüllt:

$$A_\gamma \cdot A_\delta \subset A_{\gamma+\delta}$$

Korollar 2.6

$$M := \bigoplus_{k=0}^{\infty} M_k$$

ist eine graduierte \mathbb{C} -Algebra.

BEWEIS Nach Lemma(2.4) ist das Gewicht einer nichttrivialen Modulform eindeutig. Damit folgt, dass $M = \bigoplus_{k=0}^{\infty} M_k$ eine direkte Summe von \mathbb{C} -Vektorräumen ist. Auf dieser ist durch $M_k \times M_l \rightarrow M_{k+l}$, $(f, g) \mapsto f \cdot g$ eine Multiplikation definiert. Denn es ist $fg(\frac{a\tau+b}{c\tau+d}) = (c\tau+d)^k(c\tau+d)^l \cdot f(\tau) \cdot g(\tau) = (c\tau+d)^{k+l} \cdot fg(\tau)$. Außerdem ist fg holomorph auf \mathbb{H} , da f und g jeweils auf \mathbb{H} holomorph sind. Eine geeignete Fourier-Entwicklung erhält man durch das Produkt der Fourier-Entwicklungen von f und g . Also haben wir eine wohldefinierte Multiplikation bezüglich welcher sich das Gewicht additiv verhält, was M zu einer graduierten \mathbb{C} -Algebra macht. ■

Definition 2.7 Sei A eine K -Algebra. $f_1, \dots, f_n \in A$ heißen **algebraisch abhängig** über K genau dann, wenn ein $0 \neq p \in K[x_1, \dots, x_n]$ existiert, mit $p(f_1, \dots, f_n) = 0$. Existiert ein solches p nicht, so heißen f_1, \dots, f_n **algebraisch unabhängig** über K .

Satz 2.8 Es gilt

$$M = \mathbb{C}[E_4, E_6].$$

Das heißt die Algebra M der Modulformen ist isomorph zur Polynomialgebra $\mathbb{C}[E_4, E_6]$ der komplexen Polynome in den normierten Eisensteinreihen E_4 und E_6 .

BEWEIS Wir zeigen zuerst, dass jedes $f \in M_k$ Linearkombination von Elementen aus $\left\{ E_4^\alpha E_6^\beta \mid 4\alpha + 6\beta = k \right\}$ ist. Nach (2.2) ist dies für $k = 0, 4, 6$ bereits gezeigt. Außerdem ist $M_k = 0$ für $k = 2$ und k ungerade. Sei also $k \geq 8$ gerade, $f \in M_k$. Dann ist $k \equiv 0 \pmod{4}$ oder $k \equiv 2 \pmod{4}$. Wir setzen

$$g := E_4^\alpha E_6^\beta$$

mit $\alpha = r$, $\beta = 0$, falls $k = 4r$ und $\alpha = r - 1$, $\beta = 1$, falls $k = 4r + 2$. Dann ist g eine Modulform von Gewicht $4\alpha + 6\beta = k$ mit $g(i\infty) \neq 0$. Also existiert ein λ in \mathbb{C} , sodass $(f - \lambda g)(i\infty) = 0$ ist.

Wir unterscheiden zwei Fälle. Für $k \leq 10$ ist $f - \lambda g = 0$ nach Satz(2.2(ii)). Für $k \geq 12$ existiert nach Satz(2.2(iii)) ein h in M_{k-12} mit $f - \lambda g = \Delta h$. Wir zeigen schließlich per Induktion über k , dass f als komplexes Polynom in E_4 und E_6 darstellbar ist.

(IA) Für $k = 12$ ist $k - 12 = 0$, also $M_k \cong \mathbb{C}$. Demnach existiert ein $c \in \mathbb{C}$, sodass $f = c\Delta + \lambda g$. Dabei ist die rechte Seite per Definition ein Polynom in E_4 und E_6 .

(IS) $k \rightarrow k + 2$: Es ist $f = \lambda g + \Delta h$ mit $h \in M_{(k+2)-12}$. Somit ist h nach Induktionsvoraussetzung als komplexes Polynom in E_4 und E_6 darstellbar. Wieder folgt per Definition von g und Δ , dass dann auch f in gewünschter Weise darstellbar ist.

Es bleibt die algebraische Unabhängigkeit zu zeigen. Sei dazu $p(E_4, E_6)$ eine algebraische Abhängigkeit. Dann ist jedes in $p(E_4, E_6)$ vorkommende Monom von gewichtetem Grad k eine Modulform von Gewicht k . Wir können p so wählen, dass dieses Gewicht stets dasselbe ist, da wir sonst einen Widerspruch zur Gradiertheit erhielten. Also können wir ObdA davon ausgehen, dass p ein homogenes Polynom von gewichtetem Grad k für ein $k \in \mathbb{N}$ ist. Angenommen E_6 teilt nicht jedes Monom in $p(E_4, E_6)$. Dann können wir $p(E_4, E_6)$ schreiben als

$$p(E_4, E_6) = cE_4^\beta + E_6q(E_4, E_6),$$

mit $0 \neq c \in \mathbb{C}$, $\beta \in \mathbb{N}_{\geq 1}$ und q homogen von gewichtetem Grad $k - 6$. Da aber $E_6(i) = 0$ und $E_4(i) \neq 0$ gilt muss $c = 0$ gelten, da sonst nicht $p(E_4, E_6) \equiv 0$ gelten könnte. Also teilt E_6 jedes Monom in p . Wir können nun E_6 einmal abspalten und die Argumentation wiederholen, bis E_6 nicht mehr jedes Monom teilt und wir so einen Widerspruch erhalten. ■

3 Anwendung und Beispiele

Als Anwendung der letzten Resultate wollen wir schließlich zwei Beispiele betrachten. Zum einen werden die Eindeutigkeit des \mathbb{E}_8 -Gitters als gerades unimodulares Gitter von Rang ≤ 8 zeigen, zum anderen bestimmen wir die ϑ -Reihe des Leech-Gitters.

Zur Erinnerung:

Γ	Γ^*/Γ	$ \Gamma^*/\Gamma $	$ R $
A_n	$\mathbb{Z}/(n+1)\mathbb{Z}$	$n+1$	$n(n+1)$
D_n	$\begin{cases} (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) & , n \text{ gerade} \\ (\mathbb{Z}/4\mathbb{Z}) & , n \text{ ungerade} \end{cases}$	4	$2n(n-1)$
E_6	$\mathbb{Z}/3\mathbb{Z}$	3	72
E_7	$\mathbb{Z}/2\mathbb{Z}$	2	126
E_8	$\{0\}$	1	240

Dabei sei $R := \{x \in \Gamma \mid (x, x) = 2\}$. Die Tabelle zeigt eine vollständige Charakterisierung der irreduziblen Wurzelgitter. Im Folgenden Beweis interessiert uns vor allem die Anzahl der Wurzeln.

Satz 3.1 Sei Γ ein gerades unimodulares Gitter in \mathbb{R}^8 . Dann ist Γ isomorph zu \mathbb{E}_8 .

BEWEIS Sei Γ ein gerades unimodulares Gitter in \mathbb{R}^8 und ϑ_Γ die zugehörige Theta-Reihe. Dann haben wir bereits früher gesehen, dass ϑ_Γ eine Modulform von Gewicht 4 ist und in (2.2) haben wir gesehen, dass dann

$$M_4 = \mathbb{C} \cdot E_4$$

ist. Da Γ Gitter ist, besitzt ϑ_Γ konstanten Term 1. Man hat daher

$$\vartheta_\Gamma(\tau) = E_4 = 1 + 240q + [\dots],$$

also

$$|\{x \in \Gamma \mid x \cdot x = 2\}| = 240.$$

Das heißt, dass Γ 240 Wurzeln besitzt. Diese erzeugen ein Teilgitter, welches von Rang ≤ 8 sein muss. Die obige Tabelle zeigt allerdings, dass abgesehen von \mathbb{E}_8 alle Wurzelgitter von geeignetem Rang weniger Wurzeln enthalten. Also ist das erzeugte Wurzelgitter von Typ \mathbb{E}_8 . Da sowohl \mathbb{E}_8 als auch Γ unimodular sind, gilt $\det(\mathbb{E}_8) = \det(\Gamma) = 1$, also schließlich $|\Gamma/\mathbb{E}_8| = \frac{\det(\Gamma)}{\det(\mathbb{E}_8)} = 1$. Damit folgt die Isomorphie. ■

Wir konnten also durch die Struktur der Algebra der Modulformen auf die ϑ -Reihe und damit die Struktur des Gitters schließen. Wir wollen zum Schluss noch ein Beispiel betrachten, bei dem wir ausgehend von Eigenschaften des Gitters die zugehörige ϑ -Reihe bestimmen.

Lemma 3.2 Sei $L \subset \mathbb{R}^{24}$ ein gerades unimodulares Gitter, das keine Wurzeln enthält. Dann gilt

$$\vartheta_L = E_4^3 - 720\Delta.$$

BEWEIS L ist gerade und unimodular, also ist die zugehörige ϑ -Reihe eine Modulform von Gewicht 12, das heißt $\vartheta_L \in M_{12}$. Es ist $\dim(M_{12}) = \dim(\mathbb{C}E_{12}) + \dim(M_0) = 2$. Wir haben gesehen, dass dann $M_{12} = \langle E_4^3, E_6^2 \rangle$ gilt, also haben wir

$$\vartheta_L = aE_4^3 + bE_6^2,$$

mit $a, b \in \mathbb{C}$. Wir bestimmen jeweils die ersten 3 Koeffizienten der Erzeuger zu

$$\begin{aligned} E_4^3 &= 1 + 3 \cdot 240q + 747 \cdot 240q^2 + \dots \\ E_6^2 &= 1 - 2 \cdot 504q + 438 \cdot 504q^2 + \dots \end{aligned}$$

Nun stellen wir zwei Bedingungen an ϑ_L . Wir verlangen zum einen wie oben, da es einen eindeutigen Vektor der Länge 0 gibt, dass

$$a + b = 1$$

gilt. Zum anderen soll L per Voraussetzung keine Wurzeln besitzen, also haben wir

$$720a + (-1008)b = 0.$$

Mit diesen beiden Bedingungen ergeben sich a und b eindeutig zu

$$a = \frac{7}{12} \text{ und } b = \frac{5}{12}.$$

Also erhalten wir

$$\vartheta_L = \frac{7}{12}E_4^3 + \frac{5}{12}E_6^2 = E_4^3 - 720\Delta.$$

Damit wissen wir nun außerdem, dass ein solches Gitter $\frac{7}{12} \cdot 747 \cdot 240 + \frac{5}{12} \cdot 438 \cdot 504 = 196560$ kürzeste Vektoren der Länge 4 besitzen muss. ■

Im nächsten Vortrag „Gewichtszähler von Codes“ werden wir eine Verallgemeinerung dieser Aussage sehen und im Vortrag „Golay-Code und Leech-Gitter“ werden wir sehen, dass das Leech-Gitter ein 24-dimensionales, gerades unimodulares Gitter ohne Wurzeln ist.

Literatur

- [1] W. Ebeling: *Lattices and Codes*, Springer Fachmedien Wiesbaden, 2013.
- [2] A. Krieg, S. Walcher, O. Wittich: *Funktionentheorie I*, Aachen 2014.
- [3] A. Krieg: *Funktionentheorie II*, Aachen 2013.