Funktionentheorie II (elliptische Modulfunktionen)

Prof. Horst Knörrer

1997 und 1998

—

ausgearbeitet von Patrick Meyer und Felix Schlenk

Inhaltsverzeichnis

Einleitung

Elliptische Modulfunktionen treten in vielen Bereichen der Mathematik auf, vor allem in der Zahlentheorie und in der algebraischen Geometrie. Die Grundtatsachen über elliptische Modulfunktionen lassen sich aber alle mit elementarem Wissen über Funktionentheorie beweisen; es ist nur leicht übertrieben, wenn man sagt, dass die meisten Sätze mehr oder weniger komplizierte Anwendungen des Residuensatzes sind. Deshalb habe ich in den Sommersemestern 1997 und 1998 elliptische Modulfunktionen als Thema der zweistündigen Vorlesung *Funktionentheorie II* gewählt. Im Wesentlichen habe ich Standardthemen und Anwendungen im Zusammenhang mit Modulformen behandelt, wie den Beweis des Vierquadratesatzes, Partitionen, Hecke-Operatoren. Etwas ungewöhnlich ist Kapitel VII, in dem die Modulkurve von $\Gamma_0(11)$ explizit berechnet wird und die Aussage der Taniyama-Shimura-Weil Vermutung an diesem Beispiel beschrieben wird.

Bei der Vorbereitung auf diese Vorlesung habe ich die Notizen von Jürg Kramer über eine ähnliche Vorlesung an der Humboldt-Universität Berlin verwendet. Ihm danke ich auch für die Anregung, eine solche Vorlesung zu halten, sowie für viele nützliche Tips. Ausserdem danke ich W. Casselman, H. Darmon und K. Stevenson für viele interessante Diskussionen.
Das Skript zu der Vorlesung hat P. Meyer im Sommersemster 1997 geschrieben; F.Schlenk hat im Verlauf des Sommersemster 1998 wesentliche Verbesserungen angebracht. Ihnen und allen Hörern danke ich für ihr Interesse und ihre Hinweise.

Kapitel 1

Elliptische Funktionen

1.1 Gitter und Gitterbasen

Definition 1.1.1 *Ein Gitter $L \subset \mathbb{C}$ ist ein $\mathbb{Z}$-Modul der Form*

$$L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$$

wobei $\omega_1, \omega_2 \in \mathbb{C} \setminus \{0\}$ und $Im\,(\frac{\omega_2}{\omega_1}) \neq 0$, d.h. ω_2, ω_1 sind linear unabhängig über $\mathbb{R}$.

Notation 1.1.2 *L bezeichne immer ein Gitter.*
Für zwei Punkte $a, b \in \mathbb{C}$ bezeichne $[a, b]$ die gerichtete Strecke von a nach b, wobei die Endpunkte inbegriffen sind. Runde Klammern schliessen die Endpunkte aus.

Definition 1.1.3 *$\{\omega_1, \omega_2\}$ heisst eine Gitterbasis oder Basis von L, falls*

$$L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$$

gilt. Die Basis heisst orientiert, falls $Im\,(\frac{\omega_2}{\omega_1}) > 0$ ist.

Lemma 1.1.4 *Seien $\omega_1, \omega_2 \in L \setminus \{0\}$ mit $Im(\frac{\omega_2}{\omega_1}) \neq 0$. Folgende Aussagen sind äquivalent:*

(a) $\{\omega_1, \omega_2\}$ ist eine Basis von L.

(b) Das Dreieck $A = (0, \omega_1, \omega_2)$ enthält ausser seinen Ecken keine weiteren Gitterpunkte (Figur 1.1).

Beweis. Aus (a) folgt, dass jeder Gitterpunkt ω geschrieben werden kann als

$$\omega = m\omega_1 + n\omega_2$$

mit eindeutigen Koeffizienten $m, n \in \mathbb{Z}$. Da das Dreieck $(0, \omega_1, \omega_2)$ aber genau aus den Punkten $\{r\omega_1 + s\omega_2 |\, r, s \geq 0,\ r + s \leq 1\}$ besteht, enthält es keine ganzzahlige Linearkombination von ω_1, ω_2, also auch keine weiteren Gitterpunkte.
(b)$\Rightarrow$(a): Mit $(0, \omega_1, \omega_2)$ enthält auch das Parallelogramm $P = (0, \omega_1, \omega_2, \omega_1 + \omega_2)$ ausser seinen Ecken keine Gitterpunkte, denn jeder Gitterpunkt ω im Dreieck $(\omega_1, \omega_2, \omega_1 + \omega_2)$ liefert den Gitterpunkt $\omega_1 + \omega_2 - \omega$ im Dreieck A. Sei nun $\omega \in L$. Dann schreibt sich

$$\omega = (m + r)\omega_1 + (n + s)\omega_2$$

mit $m, n \in \mathbb{Z}$, $r, s \in [0, 1)$. Somit liegt $\omega' = r\omega_1 + s\omega_2$ in $L \cap P$. Also ist ω' ein Eckpunkt von P. Da $r, s < 1$ ist, kommt nur der Ursprung in Frage. Somit verschwinden r und s. $\square$

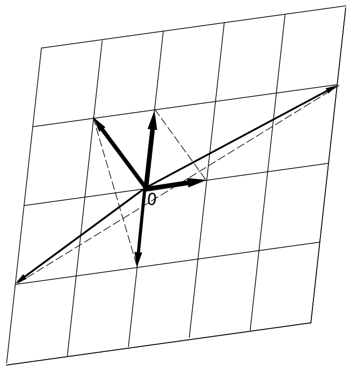

Abbildung 1.1: Basen von L

Definition 1.1.5 *$\omega \in L \setminus \{0\}$ heisst primitiv, falls aus $\omega = n\omega'$, $\omega' \in L \setminus \{0\}$ und $n \in \mathbb{Z}$ folgt dass $|n| = 1$.*

Bemerkung 1.1.6 Die primitiven Elemente aus L sind also genau die Gitterpunkte, welche man vom Ursprung aus sieht, d.h. die, welche nicht von anderen verdeckt werden (Figur 1.2). Man überlegt sich leicht, dass ein Gitterpunkt $\omega = m\omega_1 + n\omega_2$ aus L primitiv ist genau dann, wenn m und n teilerfremd sind.

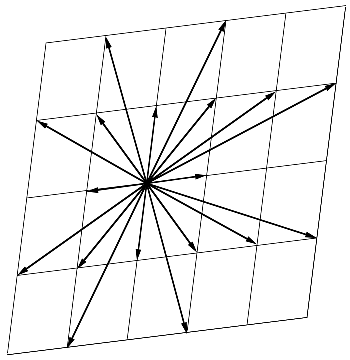

Abbildung 1.2: primitive Gitterpunkte

Lemma 1.1.7 *Ist $\omega \in \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = L$ primitiv, so kann man ω zu einer Basis ergänzen.*

Beweis. Wähle einen Vektor $\omega' \in L$, der von ω über $\mathbb{R}$ linear unabhängig ist und so, dass das Dreieck $(0, \omega, \omega')$ minimalen Flächeninhalt hat. Dann enthält dieses Dreieck neben ω' keinen weiteren von ω ueber $\mathbb{R}$ linear unabhängigen Gitterpunkt ω'', denn das Dreieck $(0, \omega, \omega'')$ hätte kleineren Flächeninhalt als das Dreieck $(0, \omega, \omega')$. Da ω primitiv ist, enthält das Dreieck $(0, \omega, \omega')$ auch keinen Gitterpunkt, der ein Vielfaches von ω ist und von 0 und ω verschieden ist. Nach Lemma 1.1.4 ist $\{\omega, \omega'\}$ eine Gitterbasis von L. $\square$

Satz 1.1.8 (Basiswechsel) *Seien $\{\omega_1, \omega_2\}$, $\{\omega_1', \omega_2'\}$ Gitterbasen von L, dann existiert eine Matrix*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbb{Z})$$

sodass

$$
\begin{aligned}
\omega_2' &= a\omega_2 + b\omega_1 && (1.1)\\
\omega_1' &= c\omega_2 + d\omega_1 && (1.2)
\end{aligned}
$$

Falls beide Basen dieselbe Orientierung haben, dann ist $\det(A) = 1$, *das heisst* $A \in SL(2,\mathbb{Z})$.

Bemerkung 1.1.9 $GL(2,\mathbb{Z})$ ist die Gruppe der invertierbaren 2×2-Matrizen mit ganzzahligen Einträgen. $SL(2,\mathbb{Z})$ ist die Untergruppe von $GL(2,\mathbb{Z})$ der Matrizen mit Determinante 1.

Übung 1.1.10 Zeige, dass $GL(2,\mathbb{Z})$ aus den ganzzahligen Matrizen A mit

$$|\det(A)| = 1$$

besteht. $SL(2,\mathbb{Z})$ ist also die Untergruppe von $GL(2,\mathbb{Z})$ der orientierungserhaltenden Matrizen.

Beweis. Man kann die neue Basis als Linearkombination der alten Basis schreiben. Die Koeffizienten müssen dann zwangsläufig ganzzahlig sein. Diese bilden aber genau die Einträge von A. Die Inverse zu A erhält man, wenn man die alte Basis als Linerearkombination der neuen Basis schreibt. Also hat A^{-1} auch ganzzahlige Einträge. Haben die Basen dieselbe Orientierung, so ist per Definition $\det(A) > 0$. □

Definition 1.1.11 *Ist* $\{\omega_1, \omega_2\}$ *eine Basis von* L, *so heisst*

$$P = \{r\omega_1 + s\omega_2 |\ 0 \le r, s \le 1\}$$

ein Fundamentalparallelogramm für L.

Korollar 1.1.12 *Die Fläche eines Fundamentalparallelogramms von* L *ist von der Basis unabhängig. Sie heisst die Diskriminante* $D(L)$ *von* L.

Beweis. Folgt sofort aus 1.1.8. □

1.2 Einfache Eigenschaften elliptischer Funktionen

Definition 1.2.1 *Eine elliptische Funktion bezüglich* L *ist eine meromorphe Funktion auf* $\mathbb{C}$, *welche* L*-periodisch ist, d.h.*

$$f(z + \omega) = f(z) \quad \forall \omega \in L$$

Wenn im Folgenden von Begriffen die Rede ist, welche von einem Gitter L abhängen, so soll für alle diese Begriffe immer das gleiche Gitter L gelten und L wird nicht mehr ausdrücklich erwähnt. P bezeichne immer ein Fundamentalparallelogramm und f eine elliptische Funktion, welche keine Nullstellen und keine Polstellen auf ∂P hat. Diese Einschränkung ist nicht von fundamentaler Bedeutung, da ein gegebenes f immer so zu einem $f_a(z) := f(z + a)$ verschoben werden kann, dass keine heiklen Stellen mehr auf dem Rand von P zu liegen kommen. Man überlege sich, warum das funktioniert!

Wenn von der Anzahl von Nullstellen oder von der Anzahl der Polstellen die Rede ist, so ist diese Anzahl immer im Parallelogramm P gemeint und mit deren Vielfachheit gezählt.

Es folgt nun eine Liste einfacher Eigenschaften elliptischer Funktionen, welche als Übungsaufgabe bewiesen werden können.

Bemerkung 1.2.2 Da P kompakt ist und die Null- bzw. Polstellen sich bei einer nichtkonstanten meromorphen Funktion nicht häufen können, kann P nur endlich viele Null- bzw. Polstellen enthalten.

Satz 1.2.3 *Eine elliptische Funktion ohne Pole ist konstant.*

Beweis. Mit Liouville. □

Satz 1.2.4 *Die Summe der Residuen einer elliptischen Funktion verschwindet.*

Beweis. Betrachte das Integral von f über den Rand von P und argumentiere mit dem Residuensatz. □

Korollar 1.2.5 *Es gibt keine elliptische Funktion mit nur einem einfachen Pol.*

Beweis. Folgt aus 1.2.4. □

Satz 1.2.6 *Eine nichtkonstante elliptische Funktion hat gleichviele Nullstellen wie Polstellen.*

Beweis. Benutzte die Formel

$$\#Nullstellen - \#Polstellen = \frac{1}{2\pi i} \int_{\partial P} \frac{f'(z)}{f(z)} dz$$

und die Elliptizität der Funktion unter dem Intgral.

Satz 1.2.7 *Sind $a_1, a_2, \ldots, a_n$ bzw. $b_1, b_2, \ldots, b_n$ die Null-bzw. Polstellen von f in P, dann gilt*

$$a_1 + \ldots + a_n = b_1 + \ldots + b_n \mod L$$

Beweis. Mit dem Residuenkalkül sieht man sofort, dass

$$\sum a_i - \sum b_i = \frac{1}{2\pi i} \int_{\partial P} \frac{z f'(z)}{f(z)} dz$$

Beim Integrieren über die Seiten $[0, \omega_1]$, $[\omega_2, \omega_1 + \omega_2]$ erhält man

$$\frac{1}{2\pi i} \left(\int_0^{\omega_1} - \int_{\omega_2}^{\omega_1+\omega_2} \right) \frac{z f'(z)}{f(z)} dz = -\frac{\omega_2}{2\pi i} \int_0^{\omega_1} \frac{f'(z)}{f(z)} dz$$

Das Integral auf der rechten Seite ohne Faktor ω_2 ist nichts anderes als das Integral der Funktion z^{-1} über den geschlossenen Weg $\gamma : z \to f(z)$, wo z die Strecke $[a, a + \omega_1]$ durchläuft. Da f keine Nullstellen auf ∂P hat, läuft γ nicht durch den Ursprung. Also ist dieses Integral die Umlaufszahl von γ um den Ursprung und somit ganzzahlig. Dasselbe erhält man bei Integration über die zwei verbleibenden Seiten von P. Also ist

$$\sum a_i - \sum b_i = m\omega_1 + n\omega_2$$

□

1.3 Beispiele elliptischer Funktionen

Beispiel 1.3.1 (Weierstraßsche $\wp$-Funktion) Sei

$$\Theta(z;\omega_1,\omega_2) := \sum_{n\in\mathbb{Z}} \exp(2\pi i\frac{z}{\omega_1})\exp(n^2\pi\frac{\omega_2}{\omega_1})$$

Die Weierstraßsche $\wp$-Funktion

$$\wp(z;\omega_1,\omega_2) := -\frac{d^2}{dz^2}\log\left(\exp(\frac{\pi i z}{\omega_1})\Theta\left(z+\frac{1}{2}(\omega_1+\omega_2)\right)\right) + const.$$

ist eine holomorphe, gerade L-periodische Funktion in $\mathbb{C}\setminus L$ und hat doppelte Pole mit Koeffizienten 1 in den Gitterpunkten, insbesondere also im Ursprung. Man kann also $\wp(z)$ in eine Laurentreihe um den Ursprung entwickeln.

$$\wp(z) = \frac{1}{z^2} + \sum_{n\in\mathbb{N}} a_n z^n$$

Die additive Konstante in der Definition der $\wp$-Funktion ist so gewählt, dass der holomorphe Teil der Laurentreihe im Ursprung verschwindet, d.h. $a_0 = 0$. $\wp$ erfüllt die nichtlineare Differentialgleichung

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3 \tag{1.3}$$

wobei die Konstanten g_2, g_3 von L abhängen.

Satz 1.3.2 *Sei C die elliptische Kurve*

$$C := \left\{(x,y)\in\mathbb{C}^2 |\ y^2 = 4x^3 - g_2x - g_3\right\}$$

Dann induziert

$$\begin{array}{rcl} \phi : \mathbb{C}\setminus L & \longrightarrow & C \\ z & \longmapsto & (\wp(z),\wp'(z)) \end{array}$$

eine Bijektion $\tilde{\phi} : \mathbb{C}/L - \{0\} \longrightarrow C$.

Anwendung 1.3.3 *Die elliptische Kurve C lässt sich durch $\wp(z)$ vollständig parametrisieren.*

Beweis. Sei

$$R = P\setminus(\{0\}\cup(\omega_1,\omega_1+\omega_2]\cup(\omega_2,\omega_2+\omega_1])$$

Die Projektion

$$\begin{array}{rcl} p : R & \longrightarrow & \mathbb{C}/L - \{0\} \\ z & \longmapsto & z + L \end{array}$$

ist eine Bijektion. Wegen (1.3) gilt

$$\tilde{\phi} := p^{-1}\circ\phi : \mathbb{C}/L - \{0\} \longrightarrow C$$

Sei $(x_0,y_0)\in C$. Wegen 1.2.6 hat dann $\wp(z) - x_0$ sicher eine Nullstelle $z_0\in R$. Da $\wp$ gerade ist, ist auch $z_1 := \omega_1+\omega_2-z_0\in R$ eine Nullstelle. Weil $\wp'$ ungerade ist, folgt mit

(1.3) $(x_0, y_0) = (\wp(z_0), \wp'(z_0))$ oder $(x_0, y_0) = (\wp(z_1), \wp'(z_1)) = (\wp(z_0), -\wp'(z_0))$ Also ist $\tilde{\phi}$ surjektiv.
Injektivität: Man setzt $\Omega := \{\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}\}$ die Menge der Halbperioden von L, und e_1, e_2, e_3 die Nullstellen $e_1 = \wp(\frac{\omega_1}{2})$, $e_2 = \wp(\frac{\omega_2}{2})$, $e_3 = \wp(\frac{\omega_1+\omega_2}{2})$ des kubischen Polynoms

$$4x^3 - g_2 x - g_3$$

[Apostol]. Sei zuerst z_0 aus $R \setminus \Omega$ und $(x_0, y_0) = (\wp(z_0), \wp'(z_0))$. Man hat dann $z_0 \neq -z_0$ mod L, weil sonst z_0 eine der obigen Halbperioden wäre. Da $\wp(z)$ gerade ist und genau zwei Nullstellen in R hat, besitzt $\wp(z) - x_0$ genau die beiden verschiedenen Nullstellen z_0, $z_1 := \omega_1 + \omega_2 - z_0 \in R$. Aber $y_0 = \wp'(z_0) \neq \wp'(z_1)$, weil $\wp'$ ungerade ist. Also wird nur z_0 von ϕ auf (x_0, y_0) abbgebildet.
Auf der Menge Ω ist aber ϕ offensichtlich injektiv, weil nämlich die Bilder der Halbperioden unter $\wp$ die Nullstellen e_i ergeben, und diese sind paarweise verschieden [Apostol]. □

Klassischer ist, die Weierstrass-Funktion über Partialbruchreihen zu definieren. Für ein Gitter L setzt man

$$f(z) = \frac{1}{z^2} + \sum_{\omega \in L \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

Es ist nicht schwer zu zeigen, dass diese Reihe in $\mathbb{C} \setminus L$ kompakt konvergiert, d.h. sie konvergiert absolut gleichmässig auf jeder kompakten Teilmenge von $\mathbb{C} \setminus L$. Man benutzt dazu die einfache Tatsache, dass die Reihe

$$\sum_{\omega \in L \setminus \{0\}} \frac{1}{|\omega|^\alpha}$$

genau dann konvergiert, wenn $\alpha > 2$ ist. Die Laurentreihe von f im Ursprung hat dann die Form

$$f(z) = \frac{1}{z^2} + \sum_{\omega \in L \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

Der holomorphe Teil von f verschwindet also im Ursprung. Da $\wp$ gerade ist, verschwindet aber auch der holomorphe Teil von $\wp$ im Ursprung. Sowohl f wie $\wp$ haben genau und nur in den Gitterpunkten Pole und zwar doppelte mit Koeffizienten 1. Also verschwindet die elliptische Funktion $f(z) - \wp(z)$ im Ursprung und hat keine Pole, womit $f \equiv \wp$ folgt.
Man kann nun die Koeffizienten des holomorphen Teils der Laurentreihe von $\wp$ berechnen.

Satz 1.3.4 (Koeffizienten der Laurentreihe von $\wp$) *Es gilt*

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) G_k z^{2k}$$

wobei die G_k durch die Eisensteinreihen

$$G_k = \sum_{\omega \in L \setminus \{0\}} \frac{1}{\omega^{2k}}\,, \quad k \geq 2$$

gegeben sind

Beweis. Sei

$$h(z) := \sum_{\omega \in L \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

Für $n \geq 1$ ist der n-te Taylorkoeffizient a_n von h im Ursprung

$$\begin{aligned} a_n &= \frac{1}{n!} \frac{d^n}{dz^n} h(z) \bigg|_{z=0} = (n+1) \sum_{\omega \in L \setminus \{0\}} \frac{1}{\omega^{n+2}} \\ &= \begin{cases} 0, & \text{für } n = 2k-1 \\ (2k+1) G_{k+1}, & \text{für } n = 2k \end{cases} \end{aligned}$$

□

Bemerkung 1.3.5 Durch Einsetzen der Laurentreihe in die Differentialgleichung

$$\wp'(z)^2 = 4\wp(z)^3 - g_2 \wp(z) - g_3$$

der $\wp$-Funktion erhält man

$$g_2 = 60 G_2 \ , \quad g_3 = 140 G_3 .$$

Da die Nullstellen des Polynoms $4x^3 - g_2 x - g_3$ paarweise verschieden sind, muss die Diskriminante verschieden von Null sein.

$$\Delta = g_2^3 - 27 g_3^2 \neq 0.$$

Beispiel 1.3.6 (Die Jacobische Thetafunktion) Die Jacobische Thetafunktion ist definiert als

$$\Theta(z, \tau) := \sum_{n \in \mathbb{Z}} \mathrm{e}^{2\pi i n z} \mathrm{e}^{\pi i n^2 \tau}$$

Man sieht leicht, dass

$$\Theta(z+1, \tau) = \Theta(z, \tau) \quad , \quad \Theta(z+\tau, \tau) = e^{-\pi i \tau - 2\pi i z}\, \Theta(z, \tau)$$

Die Jacobische Thetafunktion ist also selbst keine elliptische Funktion, aber beispielsweise durch Quotientenbildung kann man aus Θ elliptische Funktionen konstruieren. Man erhält so die Umkehrung von Satz 1.2.7.

Satz 1.3.7 *Seien $a_1, a_2, \ldots, a_n$ und $b_1, b_2, \ldots, b_n$ Punkte im Fundamentalparallelogramm P, so dass*

$$a_1 + \ldots + a_n = b_1 + \ldots + b_n \mod L$$

Dann ist

$$\frac{\prod_{j=1}^n \Theta\big(z + 1/2(1+\tau) - a_j, \tau\big)}{\prod_{j=1}^n \Theta\big(z + 1/2(1+\tau) - b_j, \tau\big)}$$

eine elliptische Funktion, deren Nullstellen bzw. Polstellen in P gerade $a_1, a_2, \ldots, a_n$ bzw. $b_1, b_2, \ldots, b_n$ sind.

Beweis. Siehe z.B. [Mumford] §6. □

Übung 1.3.8 Zeige, dass es Konstanten C_1, C_2 gibt, so dass

$$\wp(z;\tau) = C_1 \frac{d}{dz} \frac{\Theta'\big(z+1/2(1+\tau),\tau\big)}{\Theta\big(z+1/2(1+\tau),\tau\big)} + C_2$$

Übung 1.3.9 Sei L ein Gitter in $\mathbb{C}$ und $\wp(z)$ die assozierte Weierstrasssche $\wp$-Funktion. Sei

$$\begin{array}{rcl} \phi : \mathbb{C}/L - \{0\} & \longrightarrow & C = \big\{(x,y) \in \mathbb{C}^2 |\; y^2 = 4x^3 - g_2 x - g_3\big\} \\ z & \longmapsto & (\wp(z), \wp^{'}(z)) \end{array}$$

die Bijektion aus Satz 1.3.2, und γ ein Weg in $\mathbb{C} - L$ welcher zwei Punkte z_1 und z_2 aus $\mathbb{C} - L$ verbindet.
Zeigen Sie, dass

$$z_2 - z_1 = \int_{\phi(\gamma)} \frac{dx}{y}$$

Übung 1.3.10 Seien

$$\begin{array}{rcl} C & = & \big\{(x,y) \in \mathbb{C}^2 |\; y^2 = 1 - 20x + 56x^2 - 44x^3\big\} \\ C' & = & \big\{(x,y) \in \mathbb{C}^2 |\; y^2 + y = x^3 - x^2 - 10x - 20\big\} \\ C'' & = & \left\{(x,y) \in \mathbb{C}^2 |\; y^2 = 4x^3 - \frac{124}{3}x - \frac{41 \cdot 61}{27}\right\} \end{array}$$

Zeigen Sie die Äquivalenz von C,C' und C'', d.h. zeigen Sie, dass es invertierbare affine Selbstabbildungen F, F' von $\mathbb{C}^2$ mit rationalen Koeffizienten gibt, sodass $F(C) = C''$ und $F'(C') = C''$ gilt.

Übung 1.3.11 Für eine Primzahl p sei

$$N_p = \#\big\{(x,y) \in \mathbb{Z}_p^2 |\; y^2 + y = x^3 - x^2 - 10x - 20\big\}$$

Bestimmen Sie mit Hilfe des Computers N_p für alle $p \leq 100$.

Kapitel 2

Die Modulgruppe

2.1 Die Modulgruppe $PSL(2, \mathbb{Z})$

Notation 2.1.1 $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$ *soll die multiplikative Gruppe der komplexen Zahlen sein.* $H := \{z \in \mathbb{C} | \, Im\,(z) > 0\}$ *sei die offene obere Halbebene von* $\mathbb{C}$. *Man setzt* $L_\tau = \mathbb{Z} + \mathbb{Z}\tau$, *wobei* τ *immer aus* H *ist.* A *soll eine Matrix der Form*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

sein.

Im Folgenden wird der Unterschied zwischen zwei Gittern, welche sich nur durch eine Drehstreckung unterscheiden, keine wesentliche Rolle spielen. Man wird solche Gitter als äquivalent betrachten.

Definition 2.1.2 *Zwei Gitter* L, L' *heissen äquivalent (man schreibt* $L' \sim L$*), falls* $L' = \lambda L$ *mit* $\lambda \in \mathbb{C}^*$ *gilt.*

Lemma 2.1.3 *1. Jedes Gitter* L *ist äquivalent zu einem Gitter* L_τ *mit* $\tau \in H$.

2. Folgende Aussagen sind äquivalent:

(a) $L_\tau \sim L_{\tau'}$

(b) Es gibt eine Matrix $A \in SL(2, \mathbb{Z})$ *sodass*

$$\tau' = \frac{a\tau + b}{c\tau + d}$$

Beweis. 1. OBdA sei $L = \omega_1 \mathbb{Z} + \omega_2 \mathbb{Z}$ mit $\{\omega_1, \omega_2\}$ positiv orientiert, d.h. $\mathrm{Im}\,(\frac{\omega_2}{\omega_1}) > 0$. Dann ist

$$\frac{1}{\omega_1} L = \mathbb{Z} + \mathbb{Z}\frac{\omega_2}{\omega_1}$$

und somit ist $\tau = \frac{\omega_2}{\omega_1} \in H$ zu wählen.
2. Man hat folgende Äquivalenzen: $L_\tau \sim \mathrm{L}_{\tau'} \iff$ es gibt $\lambda \in \mathbb{C}^*$ sodass $\{\lambda, \lambda\tau'\}$ eine orientierte Gitterbasis von L_τ ist $\iff$ es gibt eine Matrix $A \in SL(2, \mathbb{Z})$ und ein $\lambda \in \mathbb{C}^*$, sodass

$$\begin{aligned} \lambda &= d + c\tau \\ \lambda\tau' &= b + a\tau \end{aligned}$$

$\Longleftrightarrow$

$$\tau' = \frac{a\tau + b}{c\tau + d}$$

□

Definition 2.1.4 *Für $A \in GL(2, \mathbb{C})$ heisst*

$$\begin{aligned} \varphi_A : \mathbb{C} \setminus \left\{-\frac{d}{c}\right\} &\longrightarrow \mathbb{C} \\ z &\longmapsto \frac{az + b}{cz + d} \end{aligned}$$

gebrochene lineare Transformation oder Möbiustransformation.

Satz 2.1.5 *1. Für A und B aus $GL(2, \mathbb{C})$ gilt*

$$\varphi_{AB} = \varphi_A \circ \varphi_B \text{ und } \varphi_{A^{-1}} = \varphi_A^{-1}$$

2. Seien $A, B \in GL(2, \mathbb{Z})$. Dann gilt

$$\varphi_A = \varphi_B \Longleftrightarrow A = \pm B$$

Beweis. 1.) Man könnte das direkt beweisen, indem man einfach A und B ausschreibt, einsetzt und ausrechnet, aber mehr Einsicht liefert der folgende Beweis: Schreibt man $z \in \mathbb{C} \setminus \left\{-\frac{d}{c}\right\}$ in der Form $z = \frac{z_1}{z_2}$ mit $z_i \in \mathbb{C}$, dann ist

$$\varphi_A(z) = \frac{w_1}{w_2}$$

wo

$$\begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = A \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$$

Führt man nun so die Abbildung $\varphi_A \circ \varphi_B$ aus, dann folgt sofort das obige Gesetz. $\varphi_{A^{-1}} = \varphi_A^{-1}$ folgt sofort aus Letzterem. Die 2. Aussage beweist man so: Ist $\varphi_A = \varphi_B$, so ist mit $C = A^{-1}B$ die Abbildung φ_C die Identität. Mit der obigen Überlegung folgt, dass jeder Vektor $\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$ mit $\operatorname{Im}\left(\frac{\omega_2}{\omega_1}\right) > 0$ ein Eigenvektor von C ist. Folglich ist $C = \lambda\, Id$ mit einem $\lambda \in \mathbb{C}^*$. Da aber $\det(C) = 1$ ist, muss $|\lambda| = 1$ sein. Also ist $C = \pm Id$. Die umgekehrte Richtung ist trivial. □

Übung 2.1.6 Man führe den Beweis von 2.1.5 im Detail aus.

Aus dieser Betrachtung folgt, dass die Gruppe $GL(2, \mathbb{C})$ isomorph ist zu der Gruppe der Projektivitäten des eindimensionalen projektiven Raumes $P_1\mathbb{C}$.

Bemerkung 2.1.7 Ist $A \in SL(2, \mathbb{R})$, so ist $\varphi_A : H \longrightarrow H$ biholomorph.

Beweis. Man folgt der Beobachtung im Beweis der Bemerkung 2.1.5. Sei wieder $z = \frac{z_1}{z_2} \in H$, also ist $\{z_1, z_2\}$ positiv orientiert. Weil A positive Determinante hat ist auch das Bild $\{w_1, w_2\}$ unter A positiv orientiert (1.1.8), also ist $\frac{w_1}{w_2} \in H$. Die Injektivität und Surjektivität folgt auch aus dem Beweis von 2.1.5 und aus $A^{-1} \in SL(2, \mathbb{R})$. $\varphi_{A^{-1}}$ ist nämlich die Inverse von φ_A. Die Holomorphie in beiden Richtungen ist klar. □

Bemerkung 2.1.8 Im Folgenden werden wir oft verwenden, dass für $A \in SL(2,\mathbb{Z})$

$$\frac{d}{dz}\left(\frac{az+b}{cz+d}\right) = \frac{1}{(cz+d)^2}$$

Von weiterer Bedeutung wird die Gruppe $PSL(2,\mathbb{Z})$ sein.

Definition 2.1.9 *Die Gruppe $\Gamma := PSL(2,\mathbb{Z}) := SL(2,\mathbb{Z})/\{\pm I\}$ heisst die Modulgruppe.*

Der Grund, warum man Γ anstatt $SL(2,\mathbb{Z})$ betrachtet, liegt darin, dass man $A \longrightarrow \varphi_A$ injektiv haben möchte (2.1.5). Dennoch vergisst man häufig den kleinen Unterschied zwischen den beiden Gruppen und arbeitet mit $SL(2,\mathbb{Z})$ als Modulgruppe.

Satz 2.1.10 (Erzeugende von $SL(2,\mathbb{Z})$) *Die Matrizen*

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

erzeugen ganz $SL(2,\mathbb{Z})$, d.h. jede Matrix aus der Modulgruppe ist ein Wort in S, S^{-1}, T, T^{-1}.

Bemerkung 2.1.11 Die zu S und T zugehörigen Abbildungen φ_S und φ_T lassen sich geometrisch folgendermassen deuten: $\varphi_T(z) = z+1$ ist eine reine Translation um 1. $\varphi_S(z) = -\frac{1}{z}$ ist nichts anderes als die Inversion am Einheitskreis gefolgt von der Spiegelung an der imaginären Achse.

Beweis. Man braucht nur zu zeigen, dass die von S und T erzeugte Untergruppe ganz $SL(2,\mathbb{Z})$ ist. Sei also $A \in SL(2,\mathbb{Z})$; dann passiert folgendes, wenn man A von links mit S bzw. mit T multipliziert:

$$\begin{aligned}
SA &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix} \\
TA &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix} \\
T^{-1}A &= \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a-c & b-d \\ c & d \end{pmatrix}
\end{aligned}$$

Man möchte jetzt den oberen rechten Eintrag der Matrix A sukzessive betragsmässig verkleinern, bis er verschwindet, indem man von links mit einem Wort in S und T multipliziert. Die entstehende Matrix A_n liegt dann wieder in $SL(2,\mathbb{Z})$. Ist $d = 0$, dann liefert SA das Verlangte. Sei also $d \neq 0$. ObdA $|b| \geq |d|$ (betrachte andernfalls die Matrix SA). Es gibt dann eine ganze Zahl k sodass $|b+kd| < |b|$. Der obere rechte Eintrag von T^kA ist $b+dk$, also dem Betrage nach kleiner als vorher. Also hat die Matrix A_1 in jedem Fall einen rechten oberen Eintrag mit kleinerem Betrag als es die Matrix A hatte. Man unterwirft A_1 demselben Prozess und erhält nach endlich vielen Schritten n (spätestens nach b Schritten) eine Matrix $A_n \in SL(2,\mathbb{Z})$, deren oberer rechter Eintrag verschwindet:

$$A_n = \begin{pmatrix} e & 0 \\ f & g \end{pmatrix}$$

Da $eg = \det(A) = 1$ ist und die Einträge ganzzahlig sind, geht das nur für $|g| = 1$ und $e = g$. Da $S^2 = -I$ gilt, kann man durch Linksmultiplizieren von A_n mit S^2 immer erreichen, dass $g = 1$. Also

$$A_n = \begin{pmatrix} 1 & 0 \\ f & 1 \end{pmatrix}$$

Man hat somit

$$T^{-f}SA_n = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = S$$

woraus die Behauptung folgt. □

Der Beweis liefert also nicht nur die Existenz der Zerlegung von A, sondern auch einen Algorithmus, der diese Zerlegung findet. Ein Beispiel soll diesen Prozess veranschaulichen.

Beispiel 2.1.12

$$A = \begin{pmatrix} 4 & 9 \\ 11 & 25 \end{pmatrix}, \quad SA = \begin{pmatrix} -11 & -25 \\ 4 & 9 \end{pmatrix}$$

$$T^3SA = \begin{pmatrix} 1 & 2 \\ 4 & 9 \end{pmatrix}, \quad T^4ST^3SA = \begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix}$$

$$T^{-2}ST^4ST^3SA = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I = S^2$$

Also ist

$$A = S^{-1}T^{-3}S^{-1}T^{-4}S^{-1}T^2S^2$$

Da $S^{-1} = -S$ und $S^2 = -I$, kann man noch vereinfachen:

$$A = ST^{-3}ST^{-4}ST^2$$

Korollar 2.1.13 *Für jedes $A \in SL(2,\mathbb{Z})$ ist*

$$\varphi_A : H \longrightarrow H$$

winkeltreu und bildet Kreise auf Kreise und Geraden auf Geraden ab (Kreise sind hier gewöhnliche Kreise, welche in H liegen, und Geraden sind Halbkreise, deren Zentren auf der reellen Achse liegen, oder zur imaginären Achse parallele Strahlen (Poincarémodell).

Beweis. Die Winkelerhaltung ist wegen der Holomorphie von φ_A klar. Der Rest folgt mit 2.1.5, 2.1.10 und der Erhaltung der oben genannten geometrischen Gebilde unter Inversion am Einheitskreis, Spiegelung an der imaginären Achse und Translation um 1. □

Bemerkung 2.1.14

1. Die Möbiustransformationen φ_A sind genau die Isometrien des Poincaréschen Modells der hyperbolischen Ebene.

2. Man kann jede Möbiustransformation schreiben als Hintereinanderschaltung von Translation, Drehstreckung und Inversion. Für $c \neq 0$ hat man nämlich

$$\frac{az+b}{cz+d} = \frac{1}{c}\left(a - \frac{1}{cz+d}\right) \quad \text{für} \quad c \neq 0$$

und für $c = 0$ gilt einfach

$$\frac{az+b}{cz+d} = \frac{a}{d}z + \frac{b}{d}$$

Übung 2.1.15 Drücke die Matrizen

$$\begin{pmatrix} 3 & 1 \\ 11 & 4 \end{pmatrix}, \quad \begin{pmatrix} 4 & 1 \\ 11 & 3 \end{pmatrix}$$

als Worte in den Matrizen

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

aus.

2.2 Fundamentalbereiche

Man möchte nun zu einem beliebigen Gitter ein äquivalentes Gitter L_τ auf eine eindeutige Art zuordnen. Dazu muss man den Bereich für τ weiter einschränken. Γ soll folgendermassen auf H operieren:

$$g \cdot \tau := \varphi_g(\tau)\ , \quad \forall g \in \Gamma$$

Man schreibt einfach $g\tau$ anstatt $g \cdot \tau$.

Definition 2.2.1 *Sei $\Gamma' \subset \Gamma$ eine Untergruppe. Ein Fundamentalbereich für Γ' ist eine offene Teilmenge $R_{\Gamma'} \subset H$ sodass*

(i) Ist $\tau \in H$, dann gibt es ein $g \in \Gamma'$ sodass $g\tau \in \overline{R_{\Gamma'}}$.

(ii) Keine zwei Punkte aus $R_{\Gamma'}$ sind äquivalent unter Γ', d.h. aus $\tau, \tau' \in R_{\Gamma'}$ und $g \in \Gamma'$ mit $g\tau = \tau'$ folgt $g = Id$.

Satz 2.2.2 *Sei*

$$\bar{F} := \left\{ \tau \in H \middle| \ |\tau| \geq 1,\ |Re\,(\tau)| \leq \frac{1}{2} \right\}$$

1. *Dann ist das Innere F von $\bar{F}$ ein Fundamentalbereich für Γ (Figur 2.1).*

2. *Sind $\tau, \tau' \in \bar{F}$ und gibt es ein $g \in \Gamma \setminus \{Id\}$, sodass $g\tau = \tau'$, dann liegen τ und τ' auf ∂F und gehen durch Spiegelung an der imaginären Achse ineinander über.*

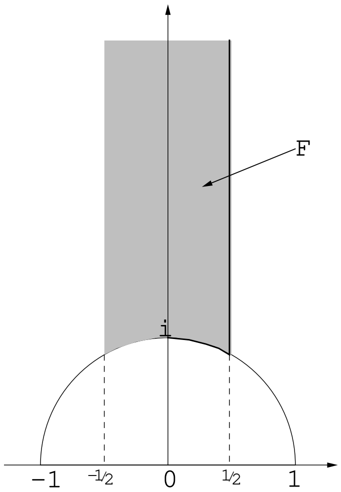

Abbildung 2.1: Ein Fundamentalbereich für Γ

Ein Lemma geht dem Beweis von 2.2.2 voran.

Lemma 2.2.3 *Folgende Aussagen sind äquivalent:*

(a) $\tau \in \bar{F}$

(b) 1 ist ein kürzester Vektor in $L_\tau \setminus \{0\}$ und τ ist ein kürzester von 1 über $\mathbb{R}$ linear unabhängiger Vektor in L_τ.

Beweis. $(b) \Rightarrow (a)$: Weil 1 ein kürzester nichttrivialer Gittervektor ist, muss sicher $|\tau| \geq 1$gelten. Wäre nun $\mathrm{Re}\,(\tau) > \frac{1}{2}$, dann hätte man: $|\mathrm{Re}\,(\tau - 1)| < |\mathrm{Re}\,(\tau)|$ und $\mathrm{Im}\,(\tau - 1) = \mathrm{Im}\,(\tau)$, insbesondere also $|\tau - 1| < |\tau|$ im Widerspruch zur Minimalität von $|\tau|$. Analog betrachtet man $\tau + 1$ falls $\mathrm{Re}\,(\tau) < -\frac{1}{2}$ angenommen.
$(a) \Rightarrow (b)$: Sei $\omega \in L_\tau$ nichttrivial, dann ist $\omega = m + n\tau$. Ist $n = 0$, dann ist $|\omega| = |m| \geq 1$. Für $n \neq 0$ und $m = 0$ ist $|\omega| \geq |n| \geq 1$. Für $n \neq 0$ und $m \neq 0$ ist $|\mathrm{Re}\,(\omega)| \geq \frac{1}{2}$ und $|\mathrm{Im}\,(\omega)| \geq \frac{\sqrt{3}}{2}$ also $|\omega| \geq 1$. Damit sind alle Fälle erfasst und 1 ist ein kleinster nichttrivialer Gittervektor. Es bleibt zu zeigen, dass τ ein kleinster von 1 linear unabhängiger Gittervektor ist. Sei also $\omega = m + n\tau \in L_\tau$ mit $n \neq 0$. Weil $\tau \in \bar{F}$ folgt $|(\tau)| \geq \sqrt{3}|\mathrm{Re}\,(\tau)|$, also $|\tau|^2 \leq \frac{4}{3}|\mathrm{Im}\,(\tau)|^2$. Ist also $|n| > 1$, dann folgt: $|\omega|^2 \geq |\mathrm{Im}\,(\omega)|^2 \geq 4|\mathrm{Im}\,(\tau)|^2 \geq 3|\tau|^2$. Der Fall $|n| = 1$ und $m = 0$ ist klar. Ist $|n| = 1$ und $m \neq 0$, dann ist $|\omega|^2 = |m \pm \mathrm{Re}\,(\tau)|^2 + |\mathrm{Im}\,(\tau)|^2 \geq (\frac{1}{2})^2 + |\mathrm{Im}\,(\tau)|^2 \geq |\tau|^2$. □

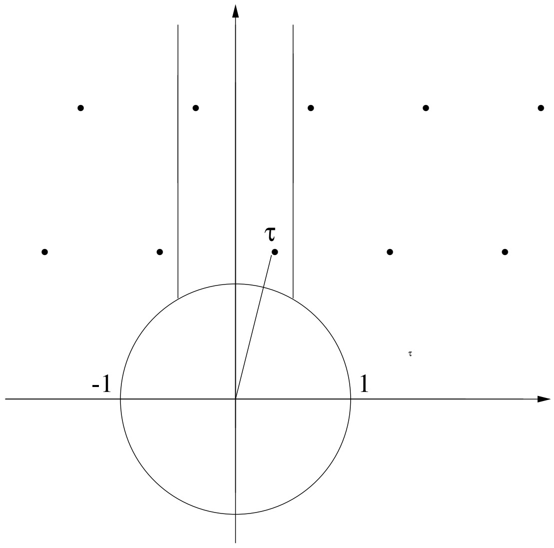

Abbildung 2.2:

Bemerkung 2.2.4 Ist L irgendein Gitter, so findet man also ein $\tau \in \bar{F}$ sodass $L \sim L_\tau$ folgendermassen: Wähle einen kürzesten Vektor $\omega_1 \in L \setminus \{0\}$ und anschliessend einen minimalen Vektor $\omega_2 \in L \setminus \mathbb{Z}\omega_1$. Nach Lemma 1.1.4 ist dann $\{\omega_1, \omega_2\}$ eine Basis von L, da nach Konstruktion das Dreieck $(0, \omega_1, \omega_2)$ keine weiteren Punkte von L enthält. Man kann annehmen, dass $\{\omega_1, \omega_2\}$ positiv orientiert ist, andernfalls wähle man einfach $-\omega_2$ statt ω_2. Nun ist $L \sim \frac{1}{\omega_1}L = \mathbb{Z} + \mathbb{Z}\frac{\omega_2}{\omega_1} = L_\tau$ mit $\tau = \frac{\omega_2}{\omega_1} \in H$. Da bei einer Drehstreckung $L \longrightarrow \lambda L$ mit $\lambda \in \mathbb{C}^*$ die Ordnungsrelationen zwischen den Längen zweier Vektoren erhalten bleiben, erfüllt τ die Bedingung (b) aus 2.2.3, und es folgt $\tau \in \bar{F}$.

Beweis von 2.2.2. Sei $\tau \in H$. Dann zeigt Bemerkung 2.2.4, dass ein $\tau' \in \bar{F}$ existiert mit $L_\tau \sim L_{\tau'}$. Aufgrund von Lemma 2.1.3 gilt daher $g\tau = \tau'$ für ein $g \in \Gamma$, und die Eigenschaft (i) in 2.2.1 ist bewiesen.

Sind $\tau, \tau' \in F$ mit $g\tau = \tau'$ für ein $g \in \Gamma$, so gilt wieder nach Lemma 2.1.3 $L_\tau \sim L_{\tau'}$, d.h. $L_\tau = \lambda L_{\tau'}$ mit $\lambda \in \mathbb{C}^*$. Da aber nach Lemma 2.2.3 1 der kürzeste Vektor in diesen beiden Gittern ist, und weil die Ordnungsrelationen unter den Längen der Vektoren bei der Multiplikation mit λ erhalten bleibt, folgt $\lambda 1 = \pm 1$, also $\lambda = \pm 1$, also $L_\tau = L_{\tau'}$. Beachte jetzt, dass alle anderen Vektoren in $L_\tau \cap \bar{F}$ echt länger sind als τ (dies folgt sofort aus der letzten Ungleichungskette im Beweis von Lemma 2.2.3, wo "$\geq$" durch "$>$" ersetzt werden muss, oder durch Betrachten von Abbildung 2.2). Daher folgt $\tau = \tau'$.

Seien noch $\tau, \tau' \in \bar{F}$ mit $\tau' = g\tau$ für ein $g \neq 1$. Wieder mit Lemma 2.1.3 folgt $L_\tau = \lambda L_{\tau'}$, und die Erhaltung der Ordnungsrelation zusammen mit Lemma 2.2.3 (b) impliziert jetzt $|\lambda| = 1$ und $|\lambda\tau| = |\tau'|$, also $|\tau| = |\tau'|$. Falls $|\tau| > 1$, folgt wieder $\lambda = \pm 1$, also $L_\tau = L_{\tau'}$, also $\tau = \tau' \pm 1$. Falls $|\tau| = 1$, zeigt $L_\tau = e^{i\theta} L_{\tau'}$ sofort, dass $g = S$. $\square$

Übung 2.2.5 Welche $\tau \in \bar{F}$ haben bezüglich der Operation von Γ eine nichttriviale Stabilisatoruntergruppe? Bestimme diese Stabilisatoruntergruppen!

Zum Abschluss folgt noch die Figur 2.3, welche einige Translate des Fundamentalbereichs unter der Gruppenoperation von Γ zeigt. Diese Translate sind natürlich wieder Fundamentalbereiche von Γ.

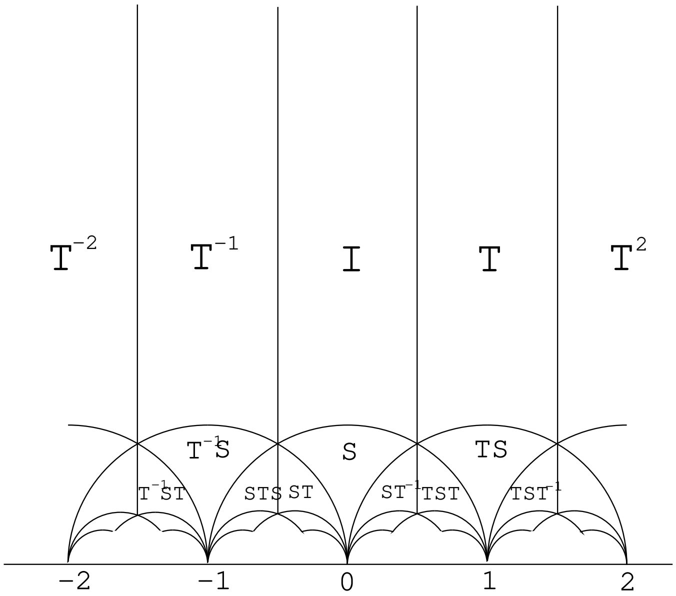

Abbildung 2.3: Translate des Fundamentalbereichs

Kapitel 3

Modulfunktionen

3.1 Eisensteinreihen

Auch in diesem Kapitel gelten dieselben Notationen wie in den bisherigen Kapiteln. Falls nichts anderes gesagt wird, soll Γ' immer eine Untergruppe von Γ und $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ eine Matrix aus $SL(2, \mathbb{Z})$ sein.

Definition 3.1.1 *Die Funktionen*

$$G_k(\tau) := \sum_{(m,n) \in \mathbb{Z}^2 \setminus \{(0,0)\}} (m\tau + n)^{-2k}$$

heissen Eisensteinreihen. Sie sind durch das Gitter $L_\tau = \mathbb{Z}\tau + \mathbb{Z}$ bestimmt.

Satz 3.1.2

$$G_k(\tau) = (c\tau + d)^{-2k} G_k\left(\frac{a\tau + b}{c\tau + d}\right)$$

für alle $A \in SL(2, \mathbb{Z})$. Häufig sagt man auch, dass $G_k(z)dz^k$ $SL(2, \mathbb{Z})$-invariant ist.

Zur Erinnerung sei nochmals erwähnt, dass Eisensteinreihen in der Laurententwicklung der $\wp$-Funktion vorkommen:

$$\wp(z; \omega_1, \omega_2) = \frac{1}{z^2} + \sum_{k \in \mathbb{N}} (2k+1) G_{k+1}(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2) z^{2k}$$

Man setzt $\wp(z; \tau) = \wp(z; 1, \tau)$, dann ist $G_k(\mathbb{Z} + \mathbb{Z}\tau) = G_k(\tau)$. Vor dem Beweis von 3.1.2 kommt ein Lemma.

Lemma 3.1.3 *Es gilt:*

$$\wp(z; \tau) = (c\tau + d)^{-2} \wp\left(\frac{z}{c\tau + d}; \frac{a\tau + b}{c\tau + d}\right)$$

Beweis. Zuerst folgt aus der Partialbruchdarstellung

$$\wp(z; \omega_1, \omega_2) = \frac{1}{z^2} + \sum_{\omega \in L \setminus \{(0,0)\}} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2}\right)$$

wo $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, dass

$$\lambda^2 \wp(\lambda z; \lambda\omega_1, \lambda\omega_2) = \wp(z; \omega_1, \omega_2)$$

für $\lambda \in \mathbb{C}^*$. Schreibt man

$$\begin{aligned} \omega_1 &= c\tau + d \\ \omega_2 &= a\tau + b \end{aligned}$$

dann ist $L_\tau = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, also ist

$$\begin{aligned} \wp(z;\tau) &= \wp(z;\omega_1,\omega_2) \\ &= \frac{1}{\omega_1^2}\left(\wp\left(\frac{z}{\omega_1}; 1, \frac{\omega_2}{\omega_1}\right)\right) \\ &= \frac{1}{(c\tau+d)^2}\wp\left(\frac{z}{c\tau+d}; 1, \frac{a\tau+b}{c\tau+d}\right) \end{aligned}$$

□

Beweis von 3.1.2.

$$\begin{aligned} & \frac{1}{z^2} + \sum_{k\in\mathbb{N}} (2k+1) G_{k+1}(\tau) z^{2k} = \wp(z;\tau) \\ = \; & \frac{1}{(c\tau+d)^2}\wp\left(\frac{z}{c\tau+d}; \frac{a\tau+b}{c\tau+d}\right) \qquad (3.1.3) \\ = \; & \frac{1}{(c\tau+d)^2}\left[\left(\frac{c\tau+d}{z}\right)^2 + \sum_{k\in\mathbb{N}}(2k+1)G_{k+1}\left(\frac{a\tau+b}{c\tau+d}\right)\left(\frac{z}{c\tau+d}\right)^{2k}\right] \qquad \text{(Laurent)} \\ = \; & \frac{1}{z^2} + \sum_{k\in\mathbb{N}}(2k+1)G_{k+1}\left(\frac{a\tau+b}{c\tau+d}\right)(c\tau+d)^{-2(k+1)} z^{2k} \end{aligned}$$

Mittels Koeffizientenvergleich erhält man die Behauptung. □

Definition 3.1.4 *Sei $f : H \longrightarrow \mathbb{C}$ meromorph. Dann heisst f schwach modular vom Gewicht $2k$ ($k \in \mathbb{N}_0$) bezüglich Γ', falls*

$$f(\tau) = \frac{1}{(c\tau+d)^{2k}} f\left(\frac{a\tau+b}{c\tau+d}\right) \quad \forall\, A \in \Gamma'$$

Bemerkung 3.1.5 3.1.2 besagt also genau, dass die Eisensteinreihen G_k schwach modular vom Gewicht $2k$ bezüglich Γ sind.

Bemerkung 3.1.6 Später (Korollar 4.3.10) werden wir zeigen, dass es für $n \geq 4$ Polynome $P_n(x,y) \in \mathbb{Q}[x,y]$ gibt, sodass

$$G_n(\tau) = P_n(G_2(\tau), G_3(\tau))$$

Beispielsweise ist (siehe [Serre] §4.2)

$$G_2^2 = G_4 \quad , \quad G_2 G_3 = G_5$$

Übung 3.1.7 f, g seien schwach modular vom Gewicht $2k$. Zeigen Sie, dass $fg' - f'g$ schwach modular vom Gewicht $4k+2$ ist.

Übung 3.1.8 Für ein Gitter L und $U := \{\mathrm{Re}(s) > \frac{1}{2}\}$ sei

$$E(L,s) := D(L)^s \sum_{\omega \in L\setminus\{0\}} |\omega|^{-2s}.$$

i) Zeigen Sie, dass obige Reihe auf U konvergiert und dort eine holomorphe Funktion ist. Zeigen Sie weiter, dass

$$E(L,s) = E(L',s)$$

falls L und L' äquivalente Gitter sind.

ii) Für $\tau \in H := \{\mathrm{Im}(\tau) > 0\}$ und $s \in U$ sei

$$E(\tau,s) := (\mathrm{Im}(\tau))^s \sum_{(m,n)\neq 0} |m\tau + n|^{-2s}.$$

Zeigen Sie, dass für alle $A \in SL(2,\mathbb{Z})$ gilt:

$$E(\varphi_A(\tau), s) = E(\tau, s),$$

wobei wie in der Vorlesung $\varphi_A(\tau) := \frac{a\tau+b}{c\tau+d}$ ist.

iii) Für $z \in \mathbb{C}\setminus\mathbb{Z}$ und $s \in U$ sei

$$S(z,s) := \sum_{n\in\mathbb{Z}} |z+n|^{-2s}.$$

Zeigen Sie, dass für jedes $z \in \mathbb{C}\setminus\mathbb{Z}$ diese Reihe in U konvergiert und dort eine holomorphe Funktion ist. Zeigen sie weiter, dass

$$(\mathrm{Im}(\tau))^{-s} E(\tau,s) = 2\zeta(2s) + \sum_{m\in\mathbb{Z}\setminus\{0\}} S(m\tau, s),$$

wobei ζ die Riemannsche Zeta-Funktion bezeichnet.

Übung 3.1.9 Sei $z = x + iy$ mit $y \neq 0$ und $\Re(s) > 1$. Man setzt

$$S(z,s) := \sum_{n=-\infty}^{\infty} |z+n|^{-2s}.$$

Ferner sei für $k \in \mathbb{R}$

$$\phi(k;s,y) := \int_{-\infty}^{\infty} |\xi + iy|^{-2s} \mathrm{e}^{-2\pi i k\xi} d\xi.$$

i) Zeigen Sie, dass

$$S(z,s) = \sum_{n=-\infty}^{\infty} \phi(n;s,y)\mathrm{e}^{2\pi i n x}.$$

ii) Zeigen Sie

$$\Gamma(s)\phi(k;s,y) = \int_{-\infty}^{\infty}\int_0^{\infty} \mathrm{e}^{-t(\xi^2+y^2)-2\pi i k\xi} t^{s-1} dt d\xi.$$

iii) Benutzen Sie obiges Reslultat, um zu zeigen, dass

$$\Gamma(s)\phi(k;s,y) = \sqrt{\pi}\int_0^\infty \mathrm{e}^{-ty^2-\frac{\pi^2k^2}{t}}t^{s-\frac{3}{2}}dt.$$

iv) Folgern Sie

$$\phi(0;s,y) = \sqrt{\pi}\frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)}|y|^{1-2s}.$$

v) Für $s \in \mathbb{C}$ und $u > 0$ sei

$$K_s(2u) := \frac{1}{2}\int_0^\infty \mathrm{e}^{-u(t+\frac{1}{t})}t^{s-1}dt.$$

Zeigen Sie, dass für festes $u > 0$ die Funktion $s \mapsto K_s(2u)$ holomorph in $\mathbb{C}$ ist.

vi) Zeigen Sie

$$\Gamma(s)\phi(k;s,y) = 2\sqrt{\pi}\left|\frac{\pi k}{y}\right|^{s-\frac{1}{2}} K_{s-\frac{1}{2}}(2|\pi k y|).$$

Übung 3.1.10 Für $x > 0$ und $s \in \mathbb{C}$ sei wie in Teil v) von übung 3.1.9

$$K_s(2x) := \frac{1}{2}\int_0^\infty \mathrm{e}^{-x(t+\frac{1}{t})}t^{s-1}dt$$

Beweisen Sie folgende Wahrheiten:

$$\begin{aligned}
K_{-s}(x) &= K_s(x)\\
K_{\frac{1}{2}}(x) &= \sqrt{\frac{\pi}{2x}}\mathrm{e}^{-x}\\
K_s(x) &= \int_0^\infty \mathrm{e}^{-x\cosh(t)}\cosh(st)dt\\
K_{s-1}(x) - K_{s+1}(x) &= -\frac{2s}{x}K_s(x)\\
K_{s-1}(x) + K_{s+1}(x) &= -2K_s'(x)\\
xK_s'(x) + sK_s(x) &= -xK_{s-1}(x)\\
xK_s'(x) - sK_s(x) &= -xK_{s+1}(x)
\end{aligned}$$

Zeigen Sie nun, dass K_s eine Lösung der Besselschen Differentialgleichung

$$x^2y'' + xy' - (x^2 + s^2)y = 0$$

ist.

Übung 3.1.11 Wie in Übung 3.1.8 sei für $\tau = x + iy \in H$, $\Re(s) > 1$

$$E(\tau,s) = (\Im(\tau))^s \sum_{(m,n)\neq(0,0)} |m\tau + n|^{-2s}$$

Zeigen Sie unter Verwendung der vorangehenden Aufgaben, dass

$$\begin{aligned}
\frac{1}{2}E(\tau,s) &= \zeta(2s)y^s + \sqrt{\pi}\frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)}\zeta(2s-1)\frac{1}{y^{s-1}}\\
&+\frac{4\pi^s\sqrt{y}}{\Gamma(s)}\sum_{N>0} N^{s-\frac{1}{2}}\left(\sum_{d|N}\frac{1}{d^{2s-1}}\right)K_{s-\frac{1}{2}}(2\pi Ny)\cos(2\pi Nx)
\end{aligned}$$

Folgern Sie daraus, dass sich für festes $\tau \in H$ die Funktion $s \mapsto E(s,\tau)$ zu einer meromorphen Funktion auf $\mathbb{C}$ fortsetzen lässt.

3.2 Fourierreihen der Eisensteinreihen G_k

Aus der Definition der Eisensteinreihen $G_k(\tau)$ folgt sofort, dass sie die Periode 1 haben, d.h. $G_k(\tau) = G_k(\tau+1)$. Man kann somit hoffen, dass $G_k(\tau)$ in eine Fourierreihe entwickelt werden kann.

Lemma 3.2.1 *Für $Im(\tau) > 0$, $k \geq 2$ ist*

$$\sum_{n\in\mathbb{Z}} \frac{1}{(n+\tau)^k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} n^{k-1} e^{2\pi i n\tau}$$

Beweis. Man benützt die Poissonsche Summenformel $\sum f(n) = \sum \hat{f}(n)$ (siehe [Dym–McKean] 2.7.5). Sei $f(x) = \frac{1}{(x+\tau)^k}$. Dann ist

$$\hat{f}(p) = \int_{-\infty}^{\infty} \frac{\mathrm{e}^{-2\pi i p z}}{(z+\tau)^k} dz$$

Mit Residuenkalkül lässt sich dieses Integral berechnen, indem man über den Weg γ_R^+ oder γ_R^- (siehe Figur 3.1) integriert, je nachdem ob p negativ oder positiv ist, und erhält $\hat{f}(p) = 0$ für $p \leq 0$ und

$$\begin{aligned}
\hat{f}(p) &= -2\pi i \ \mathrm{Res}_{z=-\tau} \left(\frac{\mathrm{e}^{-2\pi i p z}}{(z+\tau)^k} \right) \\
&= \frac{-2\pi i}{(k-1)!} \left(\frac{d}{dz} \right)^{k-1} \mathrm{e}^{-2\pi i p z}\Big|_{z=-\tau} \\
&= \frac{(-2\pi i)^k}{(k-1)!} p^{(k-1)} \mathrm{e}^{2\pi i p \tau}
\end{aligned}$$

für $p > 0$. Die Poissonsche Summenformel führt zum Ziel. □

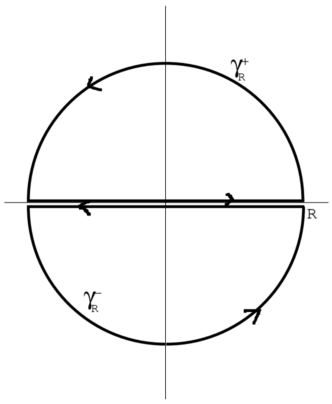

Abbildung 3.1: Residuum in τ

Satz 3.2.2 *Man hat folgende Fourierentwicklung der Eisensteinreihen G_k:*

$$G_k(\tau) = 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) e^{2\pi i n \tau}$$

wo $\sigma_k(n) = \sum_{d|n} d^k$.

Beweis.

$$\begin{aligned}
G_k(\tau) = \sum_{(p,m)\neq(0,0)} \frac{1}{(p\tau+m)^{2k}} &= \sum_{m\in\mathbb{Z}\setminus\{0\}} \frac{1}{m^{2k}} + \sum_{p\in\mathbb{Z}\setminus\{0\}} \sum_{m\in\mathbb{Z}} \frac{1}{(p\tau+m)^{2k}} \\
&= 2\zeta(2k) + 2\sum_{p=1}^{\infty} \sum_{m\in\mathbb{Z}} \frac{1}{(p\tau+m)^{2k}} \\
&= 2\zeta(2k) + 2\frac{1}{(2k-1)!}(2\pi i)^{2k} \sum_{p=1}^{\infty}\sum_{d=1}^{\infty} d^{2k-1} \mathrm{e}^{2\pi i d p\tau} \\
&= 2\zeta(2k) + \frac{2}{(2k-1)!}(2\pi i)^{2k} \sum_{n=1}^{\infty} \left(\sum_{d|n} d^{2k-1}\right) \mathrm{e}^{2\pi i n\tau}
\end{aligned}$$

Bei der vorletzten Identität wurde Lemma 3.2.1 verwendet. □

Bemerkung 3.2.3 Geht man mit dieser Darstellung der G_k in die Rekursionsformeln von Bemerkung 3.1.6, so erhält man die etwas merkwürdig anmutenden Identitäten

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{m=1}^{n-1} \sigma_3(m)\sigma_3(n-m)$$

$$11\sigma_9(n) = 21\sigma_5(n) - 10\sigma_3(n) + 5040 \sum_{m=1}^{n-1} \sigma_3(n)\sigma_5(n-m)$$

Diese Formeln sind vielleicht noch nicht von grossem Interesse, aber diese Strategie ist ein Weg, auch zahlentheoretische Beziehungen von Bedeutung zu finden.

Korollar 3.2.4 *Die Diskriminante* $\Delta(\tau)$ *aus Bemerkung 1.3.5 hat eine Fourierreihe*

$$\Delta(\tau) = g_2^3(\tau) - 27g_3^2(\tau) = (2\pi)^{12} \sum_{n=1}^{\infty} \tau(n) e^{2\pi i n\tau}$$

wo $\tau(n) \in \mathbb{Z}$, $\tau(1) = 1$, $\tau(2) = -24$. *Die Summe oben rechts heisst Ramanujan-Summe. Weiter ist* Δ *schwach modular vom Gewicht* 12*:*

$$\Delta(\tau) = \frac{1}{(c\tau+d)^{12}} \Delta\left(\frac{a\tau+b}{c\tau+d}\right), \quad A \in SL(2,\mathbb{Z})$$

Beweis. Durch Einsetzen von $G_2 = 60g_2$ und $G_3 = 140g_3$ in die Gleichung für G_k von 3.2.2. □

Definition 3.2.5

$$J(\tau) := \frac{g_2^3(\tau)}{12^3\Delta(\tau)}$$

heisst die J*-Invariante und ist eine holomorphe Funktion auf* H*, da* $\Delta(\tau)$ *nach Bemerkungg 1.3.5 keine Nullstelle in* H *besitzt.*

Satz 3.2.6 *J genügt*

$$J(\tau) = J\left(\frac{a\tau+b}{c\tau+d}\right), \;\; A \in SL(2,\mathbb{Z})$$

und J besitzt eine Fourierentwicklung für $Im(\tau)$ genügend gross:

$$J(\tau) = e^{-2\pi i\tau} + 744 + \sum_{n=1}^{\infty} c(n)\, e^{2\pi i n\tau}$$

wo man sich folgende Werte merken sollte: $c(1) = 196\,884$, $c(2) = 21\,493\,760$ und $c(n) \in \mathbb{Z} \;\; \forall n \in \mathbb{N}$.

Beweis. Einsetzen. □

3.3 Exkurs: Monstrous Moonshine

Definition 3.3.1 *Sei G eine Gruppe. Eine n-dimensionale Darstellung von G ist ein Homomorphismus*

$$\rho : G \longrightarrow GL(n, \mathbb{C})$$

ρ heisst irreduzibel, falls es keinen nichttrivialen Unterverktorraum $V \subset \mathbb{C}^n$ gibt, welcher invariant unter ρ ist, d.h. es gibt keinen nichttrivialen Unterverktorraum $V \subset \mathbb{C}^n$, sodass $\rho(g)v \in V \;\; \forall\, v \in V$.

Satz 3.3.2 *Ist G eine endliche Gruppe, so gibt es bis auf Isomorphie nur endlich viele irreduzible Darstellungen von G.*

Beweis. Ohne Beweis. □

In den siebziger Jahren begann man mit dem Programm, alle endlichen einfachen Gruppen zu klassifizieren (einfach heisst, dass die Gruppe keine nichttrivialen Normalteiler hat). Von besonderem Interesse sind die einfachen Gruppen, weil sie Bausteine der Gruppen sind. Dieses Programm konnte einige Jahre später mit Erfolg abgeschlossen werden. Das Resultat dieser Bemühungen ist:

- $\mathbb{Z}/p\mathbb{Z}$, p Primzahl
- die alternierenden Gruppen A_n, $n \geq 5$
- Gruppen vom Lie Typ
- 26 sporadische Gruppen

Das sind alle einfachen Gruppen, die es gibt. Alle Typen, bis auf die sporadischen, kennt man gut. Die sporadischen aber geben noch einige Rätsel auf. Die grösste unter ihnen, genannt das Monster M, hat folgende Gruppenordnung:
$|M| = 808\,017\,424\,794\,512\,875\,886\,459\,904\,961\,710\,757\,005\,754\,368\,000\,000\,000$. Die Anzahl ihrer irreduziblen Darstellungen ist 194 und die zugehörigen Dimensionen sind 1, 196 883, 21 296 876. Ruft man sich noch einmal die Fourierkoeffizienten der J-Invariante vom letzten Abschnitt in Erinnerung, so bemerkt man den seltsamen, ja fast mystischen Zusammenhang

$$\begin{aligned} c(1) &= 1 + 196\,883 \\ c(2) &= 1 + 196\,883 + 21\,296\,876 \end{aligned}$$

Es kann nun wirklich keinen mehr erstaunen, wenn sich Mathematiker auf die Suche nach einem Zusammenhang dieser zwei Objekte machen (Monstrous Moonshine), welche scheinbar nichts miteinander zu tun haben. Ich verweise hier für genauere Angaben auf den Artikel von [Conway].

3.4 Modulfunktionen

Definition 3.4.1 *Eine meromorphe Funktion $f : H \longrightarrow \mathbb{C}$ heisst Modulfunktion, falls sie folgende Eigenschaften besitzt:*

(a) $f\left(\frac{a\tau+b}{c\tau+d}\right) = f(\tau) \quad \forall\, A \in SL(2,\mathbb{Z}),\ \forall\, \tau \in H$

(b) Für $Im(\tau)$ genügend gross hat f eine Fourierentwicklung der Gestalt $f(\tau) = \sum_{n=-m}^{\infty} a_n e^{2\pi i n\tau},\ a_{-m} \neq 0$

m heisst die Polordnung in der Spitze ∞. Wir setzen $\nu_\infty(f) := -m$.

Beispiel 3.4.2 Die J-Invariante vom letzten Abschnitt ist eine Modulfunktion von der Polordnung 1 im Unendlichen.

Satz 3.4.3 *Sei f eine Modulfunktion, die nicht identisch Null ist. ν_{τ_0} sei die Nullstellenordnung in $\tau_0 \in H$, wobei diese negativ ist für Pole. Dann ist*

$$\nu_\infty(f) + \sum_{p\in H/\Gamma, p\notin\{\Gamma i,\Gamma\rho\}} \nu_p(f) + \frac{1}{2}\nu_i(f) + \frac{1}{3}\nu_\rho(f) = 0$$

wo $\rho = e^{\pi\frac{i}{3}}$ ist und H/Γ den Orbitraum bezüglich Γ bezeichnet.

Beweis. Zuerst beweisen wir die Aussage für den Fall, dass keine Nullstellen und keine Polstellen auf dem Rand ∂F des Fundamentalbereiches F liegen, also insbesondere $\nu_i(f) = \nu_\rho(f) = 0$ ist. Für eine Modulfunktion gilt

$$\int_{\varphi_A(\gamma)} \frac{f'}{f}dz = \int_\gamma \frac{f'(\varphi_A(z))}{f(\varphi_A(z))}\varphi_A'(z)dz = \int_\gamma \frac{f'}{f}dz \tag{3.1}$$

Sei $\gamma = L_1 + L_2 + L_3 + L_4 + L_5$ wie in Figur 3.2; dann ist $TL_1 = -L_4$ und $SL_2 = -L_3$, wo S, T die Erzeugenden von $SL(2,\mathbb{Z})$ sind. Mit (3.1) folgt dann

$$\int_{L_1} + \int_{L_2} + \int_{L_3} + \int_{L_4} \frac{f'}{f}dz = 0$$

Weiter hat man

$$\int_{L_5} \frac{f'}{f}dz = -\int_{-\frac{1}{2}}^{\frac{1}{2}} \frac{f'(u+iM)}{f(u+iM)}du$$

Da für M gross genug f eine Darstellung als Fourierreihe $f(\tau) = \sum_{n=-m}^{\infty} a_n \mathrm{e}^{2\pi i n\tau}$ mit $a_{-m} \neq 0$ hat, kann man für $x = \mathrm{e}^{2\pi i(u+iM)} = \mathrm{e}^{2\pi i z}$ schreiben

$$f(z) = \frac{a_{-m}}{x^m} + \frac{a_{-m+1}}{x^{m-1}} + \cdots =: F(x)$$

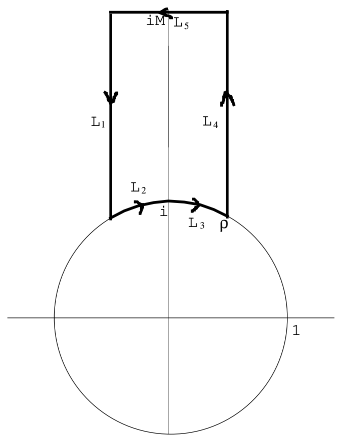

Abbildung 3.2: Keine kritischen Stellen auf dem Rand

und man hat nun alles zusammengesetzt

$$\begin{aligned}\sum_{p\in H/\Gamma, p\notin\{\Gamma i,\Gamma\rho\}} \nu_p(f) &= \sum_{p\in F}\nu_p(f)\\ &= \frac{1}{2\pi i}\int_{L_5}\frac{f'}{f}(z)dz\\ &= \int_\gamma \frac{F'}{F}(x)dx\\ &= -\nu_\infty(f)\end{aligned}$$

wo γ der im Uhrzeigersinn durchlaufene Kreis mit Radius $\mathrm{e}^{-2\pi M}$ um den Ursprung ist.

Als nächstes wird der Fall betrachtet, bei welchem kritische Stellen auf $\partial F \setminus \{i,\rho\}$ liegen können. In dieser Situation weicht man diesen Stellen einfach wie in der Figur 3.3 aus. Der Fall, wo eine kritische Stelle auf i zu liegen kommt behandelt man wie folgt:

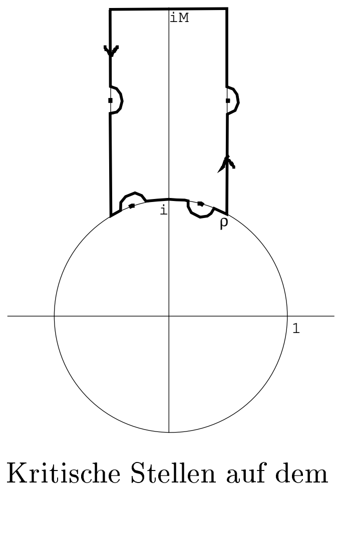

Abbildung 3.3: Kritische Stellen auf dem Rand ohne i,ρ

Man weicht auch hier der Stelle i aus (Figur 3.4) und beachtet, dass der Bogen α durch

S in α' übergeht. Also hat man hier

$$\begin{aligned}\frac{1}{2\pi i}\int_{\alpha}\frac{f'}{f}(z)dz &= \frac{1}{2\pi i}\int_{\alpha'}\frac{f'}{f}(z)dz\\ &= \frac{1}{4\pi i}\int_{\alpha+\alpha'}\frac{f'}{f}(z)dz\\ &= \frac{1}{2}\nu_i(f)\end{aligned}$$

Kommt eine kritische Stelle auf ρ zu liegen, so wird das ganze noch ein bisschen kompli-

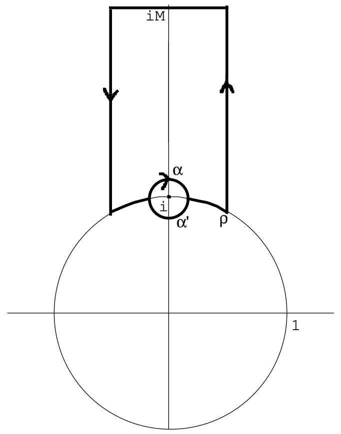

Abbildung 3.4: Kritische Stelle in i

zierter (Figur 3.5). Man erhält dann

$$\int_{\beta+\beta'}\frac{f'}{f}(z)dz = \frac{1}{3}\nu_\rho(f)$$

□

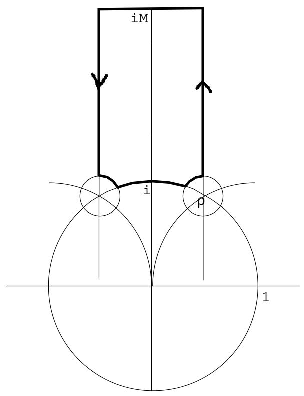

Abbildung 3.5: Kritische Stelle in ρ

Korollar 3.4.4 *Eine Modulfunktion ohne Nullstellen und ohne Polstellen ist konstant.*

Beweis. Als Übung. $\square$

Korollar 3.4.5 *Die J-Invariante induziert einen Homöomorphismus $H/\Gamma \longrightarrow \mathbb{C}$.*

Bemerkung 3.4.6 Man hat mit J somit eine Funktion gefunden, welche die äquivalenten Gitter charakterisiert, nämlich

$$L_\tau \sim L_{\tau'} \Longleftrightarrow J(\tau) = J(\tau')$$

Beweis von 3.4.5. Sei $c \in \mathbb{C}$ beliebig. Man hat $\nu_\infty(J-c) = -1$, und für $p \in H$ ist $\nu_p(J-c) \geq 0$, also existiert $p \in H/\Gamma \cup \{\Gamma i, \Gamma\rho\}$ sodass $\nu_p(J-c) > 0$. Ist dieses p nicht in $\{\Gamma i, \Gamma\rho\}$, dann ist $\nu_p(J-c) = 1$ und somit p die einzige Lösung der Gleichung $J(\tau) = c$. Ist $p = i$, so folgt $\frac{1}{2}\nu_i(J-i) + l + \frac{1}{3}k = 1$ wo $l, k \in \mathbb{N}$ und da $\frac{1}{2}\nu_i(J-i) \geq \frac{1}{2}$ ist, folgt $\nu_i(J-i) = 2$, also ist i die einzige Lösung der Gleichung $J(\tau) = c$. Genau gleich argumentiert man, falls $p = \rho$ ist. Die Stetigkeit in beide Richtungen bleibt dem Leser überlassen. $\square$

Bemerkung 3.4.7 Man kann zeigen, dass $J(i) = 1$ und $J(\rho) = 0$ ist.

Eine elliptische Kurve ist eine Kurve der Form

$$y^2 = 4x^3 - a_2 x - a_3$$

mit $a_2, a_3 \in \mathbb{C}$; $a_2^3 - 27a_3^2 \neq 0$. Die Surjektivität von J zeigt, dass sich jede elliptische Kurve durch elliptische Funktionen bezüglich eines geeigneten Gitters parametrisieren lässt. Dies ergibt sich aus 1.3.3, 1.3.5 und dem folgenden

Satz 3.4.8 *Seien $a_2, a_3 \in \mathbb{C}$ mit $a_2^3 - 27a_3^2 \neq 0$. Dann gibt es über $\mathbb{R}$ linear unabhängige Elemente $\omega_1, \omega_2 \in \mathbb{C}$, so dass*

$$a_2 = g_2(\omega_1, \omega_2) \quad , \quad a_3 = g_3(\omega_1, \omega_2)$$

Beweis. Setze

$$j_0 = \frac{a_2^3}{12^3\,(a_2^3 - 27\,a_3^2)}$$

Nach Korollar 3.4.5 gibt es ein $\tau \in H$ so dass $J(\tau) = j_0$, d.h.

$$\frac{g_2^3\,(\tau)}{12^3\,(g_2^3\,(\tau)\; - 27\,g_3^2\,(\tau))} = \frac{a_2^3}{12^3\,(a_2^3 - 27\,a_3^2)}$$

Da $g_2(\lambda,\,\lambda\tau) = \frac{1}{\lambda^4}\,g_2(\tau)$, $g_3(\lambda,\,\lambda\tau) = \frac{1}{\lambda^6}\,g_3\,(\tau)$ für $\lambda \in \mathbb{C}\setminus\{0\}$, gibt es $\lambda \in \mathbb{C}\setminus\{0\}$ so dass

$$a_2^3 = g_2^3\,(\lambda,\,\lambda\tau) \quad , \quad a_2^3 - 27\,a_3^2 = g_2^3\,(\lambda,\,\lambda\tau)\; - 27\,g_3^2\,(\lambda,\,\lambda\tau)$$

Indem wir eventuell λ mit einer geeigneten 12-ten Einheitswurzel multiplizieren, können wir annehmen, dass $a_2 = g_2(\lambda,\,\lambda\tau)$. Damit ist $a_3^2 = g_3^2(\lambda,\,\lambda\tau)$. Falls $a_3 = -g_3(\lambda, \lambda\tau)$, ersetzen wir λ durch $i\lambda$, wodurch dann

$$a_2 = g_2(\lambda,\,\lambda\tau) \quad , \quad a_3 = g_3(\lambda,\,\lambda\tau)$$

Setze $\omega_1 := \lambda,\ \omega_2 := \lambda\tau$. $\square$

Satz 3.4.9 *Sei f eine Modulfunktion. Dann gibt es $p(x), q(x) \in \mathbb{C}[x]$ mit $(p,q) = const$, sodass*

$$f(\tau) = \frac{p(J(\tau))}{q(J(\tau))} \quad \forall\, \tau \in H$$

Beweis. Seien $z_1, z_2, \ldots, z_m$ die Nullstellen (mod Γ) und $w_1, w_2, \ldots, w_n$ die Polstellen (mod Γ) mit Multiplizität von f. Setzt man

$$F(\tau) := \frac{(J(\tau) - J(z_1))(J(\tau) - J(z_2)) \cdots (J(\tau)) - J(z_m))}{(J(\tau) - J(w_1))(J(\tau) - J(w_2)) \cdots (J(\tau)) - J(w_n))}$$

folgt, dass $\frac{f(\tau)}{F(\tau)}$ eine Modulfunktion ohne Nullstellen und ohne Polstellen ist. Also ist diese Funktion nach 3.4.4 konstant und somit $f(\tau) = const\, F(\tau)$. $\square$

Bemerkung 3.4.10 *Hat die Fourierreihe $f(\tau) = \sum c_n\, e^{2\pi i\, n \tau}$ von f nur ganzzahlige Koeffizienten c_n, so kann man $p(x)$ und $q(x)$ als Polynome mit ganzzahligen Koeffizienten wählen.*

Beweis. Seien

$$p\,(x) = \sum_{n=0}^{d_p} a_n\, x^n \qquad , \quad q\,(x) = \sum_{m=0}^{d_q} b_m\, x^m$$

teilerfremde Polynome wie in Satz 3.4.9, so dass

$$f\,(\tau) = \frac{p\,(J\,(\tau))}{q\,(J(\tau))} \quad \text{für} \quad \tau \in H$$

Die rationale Funktion $\frac{p(x)}{q(x)}$ ist eindeutig bestimmt. Sei $n_0 := \min\{n|\, a_n \neq 0\}\,, m_0 := \min\{m|\, b_m \neq 0\}$. Wir können annehmen, dass $b_{m_0} = 1$ (ersetze $p(x)$ durch $\frac{1}{b_{m_0}}\, p(x)$ und $q(x)$ durch $\frac{1}{b_{m_0}}\, q(x)$). In der Fourierentwicklung von $\frac{p\,(J\,(\tau))}{q\,(J\,(\tau))}$ sind die Koeffizienten von $e^{2\pi i\, k \tau}$, $k < n_0 - m_0$, gleich Null und der Koeffizient von $e^{2\pi i\, (n_0 - m_0)\tau}$ ist a_{n_0}. Folglich ist $a_{n_0} \in \mathbb{Z}$.
Sei nun $K = \mathbb{Q}(a_0, \ldots a_{d_p}, b_0, \ldots, b_{d_q})$. Wir nehmen an, dass $K \neq \mathbb{Q}$. Dann gibt es einen nichttrivialen Automorphismus σ von $\mathbb{C}$ über $\mathbb{Q}$, der K nicht festhält. Dann ist $a_n^\sigma \neq a_n$ für ein n oder $b_m^\sigma \neq b_m$ für ein m. Setze

$$p^\sigma\,(x) := \sum_{n=0}^{d_p} a_n^\sigma\, x^n \quad , \quad q^\sigma\,(x) := \sum_{m=0}^{d_q} b_m^\sigma\, x^m$$

Da $a_{n_0}\,,\, b_{m_0}\, \in \mathbb{Q}$, ist

$$\begin{aligned} &p^\sigma\,(x)\,\text{nicht proportional zu}\, p\,(x) \quad \text{oder} \\ &q^\sigma\,(x)\,\text{nicht proportional zu}\, q\,(x). \end{aligned}$$

Somit ist

$$\frac{p^\sigma(x)}{q^\sigma(x)} \neq \frac{p\,(x)}{q\,(x)}$$

Da J rationale Koeffizienten hat, gilt

$$\frac{p^\sigma\,(J\,(\tau))}{q^\sigma\,(J\,(\tau))} = \frac{\sum a_n^\sigma\, J\,(\tau)^n}{\sum b_m^\sigma\, J\,(\tau)^m} = \sum c_n^\sigma\, e^{2\pi i\, n \tau}$$

Da $c_n \in \mathbb{Z}$, folgt $\sum c_n^\sigma \, e^{2\pi i \, n\tau} = \sum c_n \, e^{2\pi i \, n\tau} = f(\tau)$. Somit ist

$$f(\tau) \;=\; \frac{p^\sigma(J\,(\tau))}{q^\sigma(J\,(\tau))} \quad ,$$

im Widerspruch zur Eindeutigkeit der Darstellung von f als rationale Funktion von J. Somit ist $K = \mathbb{Q}$, also ist $a_0, \ldots, a_{d_p}, b_0, \ldots, b_{d_q} \in \mathbb{Q}$. Durch Erweitern von $\frac{p(x)}{q(x)}$ mit dem Hauptnenner von $a_0, \ldots, a_{d_p}$, $b_0 , \ldots, b_{d_q}$ können wir erreichen, dass p und q ganzzahlige Koeffizienten haben und der grösste gemeinsame Teiler von $a_0, \ldots, a_{d_p}$, $b_0 , \ldots, b_{d_q}$ gleich 1 ist. $\square$

Kapitel 4

Modulformen und Vierquadratesatz

Die Notation bleibt auch in diesem Kapitel dieselbe. Das Hauptanliegen dieses Kapitels ist, den folgenden Satz von Lagrange zu beweisen.

Satz 4.0.11 (Vierquadratesatz von Lagrange) *Jede natürliche Zahl ist Summe von 4 Quadraten ganzer Zahlen.*

In der Tat gilt eine stärkere Aussage, welche auf Jacobi zurückgeht: Sei $r(n)$ die Anzahl der Möglichkeiten, n als Summe von 4 Quadraten ganzer Zahlen zu schreiben:

$$r(n) = \#\left\{(n_1, n_2, n_3, n_4) \in \mathbb{Z}^4 : n_1^2 + n_2^2 + n_3^2 + n_4^2 = n\right\}$$

Dann gilt

$$r(n) = \delta(n) \sum_{d|n,\ d \text{ ungerade}} d$$

wobei

$$\delta(n) := \begin{cases} 8 & \text{falls } n \text{ ungerade} \\ 24 & \text{falls } n \text{ gerade} \end{cases}$$

Beispiel 4.0.12 Wir berechnen $r(n)$ für $1 \leq n \leq 4$: Es gilt

$$\delta(1) = \delta(3) = 8 \text{ und } \delta(2) = \delta(4) = 24.$$

Weiter ist

$$\sum_{d|1, d \text{ ungerade}} d = 1, \quad \sum_{d|2, d \text{ ungerade}} d = 1, \quad \sum_{d|3, d \text{ ungerade}} d = 1 + 3 = 4 \text{ und } \quad \sum_{d|4, d \text{ ungerade}} d = 1,$$

also

$$\begin{aligned} r(1) &= 8 \\ r(2) &= 24 \\ r(3) &= 32 \\ r(4) &= 24 \end{aligned}$$

Wir verifizieren dies für n=3: Die Einträge derjenigen Vektoren in $\mathbb{Z}^4$, die zu 3 führen, müssen aus $\{-1, 0, 1\}$ sein, und zwar muss genau eine 0 auftreten. Die 0 kann an 4 verschiedenen Stellen stehen, und es gibt $2^3 = 8$ Möglichkeiten für die Vorzeichen der restlichen Einträge, also folgt in der Tat $r(3) = 4 \cdot 8 = 32$.

4.1 Kongruenzuntergruppen von Γ

Satz 4.1.1 *Sei $N \in \mathbb{N}$. Die Projektion*

$$p : SL(2, \mathbb{Z}) \longrightarrow SL(2, \mathbb{Z}/N\mathbb{Z})$$

ist ein surjektiver Gruppenhomorphismus.

Beweis. Nur die Surjektivität ist nicht sofort ersichtlich. Sei D bzw. B die Untergruppe aller Diagonalmatrizen bzw. die Untergruppe aller rechten oberen Dreiecksmatrizen von $SL(2, \mathbb{Z}/N\mathbb{Z})$. Wir zeigen zuerst, dass D und B im Bild von p enthalten sind:
Sei $Q = \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \in D$. Wähle einen Repräsentanten a bzw. d aus der Klasse α bzw. δ. Dann gibt es ein $k \in \mathbb{Z}$ sodass gilt

$$ad = 1 + kN$$

Weil $(a - akN)d = ad(1 - kN) = (1 + kN)(1 - kN) = 1 - k^2N^2$ ist, liegt die Matrix

$$A := \begin{pmatrix} a - akN & kN \\ -kN & d \end{pmatrix}$$

in $SL(2, \mathbb{Z})$ und $p(A) = Q$, womit gezeigt ist, dass D im Bild von p ist.
Sei nun $Q = \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \in B$. Wegen $\alpha\delta = 1$, ist α eine Einheit in $\mathbb{Z}/N\mathbb{Z}$. Es gibt also ein $t \in \mathbb{Z}/N\mathbb{Z}$ sodass $t\alpha = \beta$. Dann ist

$$\begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$$

Die erste Matrix auf der rechten Seite liegt aber nach dem bereits Bewiesenen in Bild von p und die zweite Matrix auf der rechten Seite ist das Bild unter p der Matrix $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$. Weil das Bild aber eine Gruppe ist, liegt auch das Produkt Q dieser beiden Matrizen im Bild von p. Die Surjektivität folgt jetzt so:
Sei

$$Q = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL(2, \mathbb{Z}/N\mathbb{Z})$$

Wähle Repräsentanten $0 \le a, c \le N$ von α, γ. Wie im Beweis von Satz 2.1.10 zeigt man durch Induktion über $\max(a, c)$, dass es ein Wort W in

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

gibt, sodass

$$W \cdot \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

in B liegt. Da aber natürlich S und T im Bild von p liegen, gilt dasselbe für W, und nun folgt aus $B \subset \mathrm{Bild}(p)$, dass auch Q im Bild von p ist. $\square$

Definition 4.1.2 *Die Hauptkongruenzenuntergruppe $\Gamma(N)$ der Stufe N für $N \in \mathbb{N}$ ist die Gruppe*

$$\Gamma(N) := \left\{ A \in \Gamma : A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}$$

Bemerkung 4.1.3 $\Gamma(N) = \mathrm{Kern}(p)$ wo p die Abbildung von Satz 4.1.1 ist.

Definition 4.1.4 *Mit $\Gamma_0(N)$ für $N \in \mathbb{N}$ bezeichnet man die Untergruppe*

$$\Gamma_0(N) := \{A \in \Gamma : c \equiv 0 \mod N\}$$

Bemerkung 4.1.5 Für $N > 2$ gilt folgende allgemeine Formel für den Index $[\Gamma, \Gamma(N)]$:

$$[\Gamma : \Gamma(N)] = \frac{N^3}{2} \prod_{p|N,\, p \text{ prim}} (1 - \frac{1}{p^2})$$

und

$$[\Gamma : \Gamma(2)] = 6$$

Ist N eine ungerade Primzahl, dann ist also

$$[\Gamma : \Gamma(N)] = \frac{1}{2} N(N^2 - 1)$$

Weiter hat man folgende geometrische Interpretation:

$$\begin{array}{rcl} \Gamma/\Gamma(2) & \simeq & S_3 \\ \Gamma/\Gamma(3) & \simeq & \text{Tetraedergruppe} \\ \Gamma/\Gamma(4) & \simeq & \text{Oktaedergruppe} \\ \Gamma/\Gamma(5) & \simeq & \text{Ikosaedergruppe} \simeq A_5 \end{array}$$

Beweis. Der Beweis kann in [Lehner] S. 356 und [Ford] S. 128 nachgeschlagen werden. In dieser Vorlesung wird im weiteren nur $[\Gamma : \Gamma(2)] = 6$ benutzt. Dies folgt auch sofort aus Bemerkung 4.1.3 und der Tatsache, dass die Gruppe $SL(2, \mathbb{Z}/2\,\mathbb{Z})$ aus sechs Elementen besteht. □

Definition 4.1.6 *Sei $L_\tau = \mathbb{Z} + \tau\mathbb{Z}$. Für $N \in \mathbb{N}$ heissen die Punkte*

$$\left[\frac{1}{N}(\mathbb{Z} + \mathbb{Z}\tau)\right]$$

N-Teilungspunkte in dem Torus $\mathbb{C}/L_\tau$ (Level-N-Strukturen).

Lemma 4.1.7 (Level-N-Strukturen) *Sei $N \in \mathbb{N}$ und $L_\tau = \mathbb{Z} + \mathbb{Z}\tau$. Weiter sei $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma(N)$ und $\tau' := \varphi_A(\tau) = \frac{\alpha\tau+\beta}{\gamma\tau+\delta}$. Dann gilt für jeden N-Teilungspunkt $\frac{1}{N}(a_1\tau + a_2)$ von L_τ*

$$\frac{\frac{1}{N}(a_1\tau + a_2)}{\gamma\tau + \delta} \equiv \frac{1}{N}(a_1\tau' + a_2) \mod L_{\tau'}$$

Multiplikation mit $\frac{1}{\gamma\tau+\delta}$ führt ja L_τ in $L_{\tau'}$ über. Das Lemma besagt, dass dabei der mit a_1, a_2 markierte N-Teilungspunkt von L_τ in den mit a_1, a_2 markierten N-Teilungspunkt von $L_{\tau'}$ übergeht.

Beweis. Für feste a_1, a_2 ist die Behauptung äquivalent zur Behauptung

$$a_1(\alpha\tau+\beta)+a_2(\gamma\tau+\delta)\equiv a_1\tau+a_2 \mod N(\mathbb{Z}(\gamma\tau+\delta)+\mathbb{Z}(\alpha\tau+\beta))$$

Diese Aussage ist wiederum äquivalent zu

$$[a_1(\alpha-1)+a_2\gamma]\tau+\beta a_1+a_2(\delta-1)\equiv 0 \mod NL_\tau$$

Da aber nach Voraussetzung $\alpha-1\equiv\delta-1\equiv\beta\equiv\gamma\equiv 0 \mod N$ gilt, ist dies erfüllt. □

Bemerkung 4.1.8 Sei Γ' eine Untergruppe von endlichem Index in Γ und R_Γ ein Fundamentalbereich für Γ. Weiter sei $A_1,\ldots,A_r$ ein Repräsentantensystem für die Rechtsnebenklassen von Γ' in Γ, das heisst Γ ist die disjunkte Vereinigung

$$\Gamma=\Gamma' A_1\cup\cdots\cup\Gamma' A_r=A_1^{-1}\Gamma'\cup\cdots\cup A_r^{-1}\Gamma'$$

Dann ist

$$R_{\Gamma'}:=\bigcup_{j=1}^{r}\varphi_{A_j}(R_\Gamma)$$

ein Fundamentalbereich für Γ'.

Beweis. Einfache Übung. □

Beispiel 4.1.9 Einen Fundamentalbereich für $\Gamma(2)$ erhält man nun auf folgende Art: I, T, S, $T^{-1}S$, ST, TST bilden ein Repräsentantensystem von $\Gamma/\Gamma(2)$, denn man hat $\Gamma/\mathrm{Kern}(p)\simeq PSL(2,\mathbb{Z}_2)=\Gamma/\Gamma(2)$, und die Bilder der obigen Repräsentanten geben ganz $PSL(2,\mathbb{Z}_2)$. Anstatt vom Standardfundamentalbereich R_Γ (Figur 4.1) auszugehen, wählt man den Fundamentalbereich R'_Γ (Figur 4.1) und lässt die Repräsentanten darauf los, was den Fundamentalbereich $R_{\Gamma(2)}$ für $\Gamma(2)$ ergibt (Figur 4.1).

Übung 4.1.10 Sei p eine Primzahl.

i) Zeigen Sie, dass $\Gamma_0(p)\backslash\Gamma$ aus den Rechtsnebenklassen von $Id, S, ST,\ldots,ST^{p-1}$ besteht.

ii) Zeigen Sie, dass

$$\{I,T\}\cup\left\{\begin{pmatrix}\alpha&\beta\\ p&\delta\end{pmatrix}:\alpha\delta-\beta p=1\right\}$$

ein Erzeugendensystem für $\Gamma_0(p)$ ist.

iii) Zeichnen Sie einen Fundamentalbereich für $\Gamma_0(11)$. Zeigen Sie, dass $\Gamma_0(11)$ fixpunktfrei auf $H=\{\mathrm{Im}(z)>0\}$ operiert.

Übung 4.1.11 Sei

$$J=\begin{pmatrix}0&-\frac{1}{\sqrt{N}}\\ \sqrt{N}&0\end{pmatrix}$$

Dann ist $J^2=-Id$ und $J\Gamma_0(N)J=\Gamma_0(N)$. Zeigen Sie, dass $\Gamma_0^*(N):=\Gamma_0(N)\cup\Gamma_0(N)J$ eine Gruppe ist und dass $[\Gamma_0^*(N):\Gamma_0(N)]=2$.

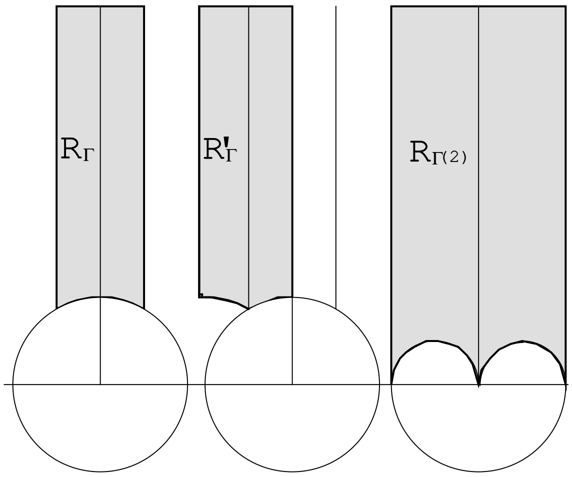

Abbildung 4.1: Fundamentalbereich für $\Gamma(2)$

4.2 Beispiele schwach modularer Funktionen

Schon im Kapitel 3 wurden schwach modulare Funktionen definiert, und nun soll eine weitere Betrachtung solcher Funktionen erfolgen, welche vom Ziel, den Vierquadratesatz zu beweisen, geleitet ist.

Beispiel 4.2.1 • Die J-Invariante ist schwach modular vom Gewicht 0 bezüglich Γ.

- Die Eisensteinreihen G_k sind schwach modular von Gewicht $2k$ bezüglich Γ.

Satz 4.2.2 *Sei*

$$\Theta(z,\tau) := \sum_{n\in\mathbb{Z}} e^{2\pi i n z} e^{\pi i n^2 \tau}$$

die Jacobische Thetafunktion aus Beispiel 1.3.6 und

$$\vartheta(\tau) := \Theta(0,\tau) = \sum_{n\in\mathbb{Z}} e^{\pi i n^2 \tau}$$

Dann ist ϑ^4 schwach modular vom Gewicht 2 bezüglich $\Gamma(2)$.

Beweis. Wir zeigen zunächst die **Jacobi-Identität**

$$\vartheta(\tau) = \sqrt{\frac{i}{\tau}}\vartheta\left(-\frac{1}{\tau}\right) \tag{4.1}$$

Diese zeigt man zuerst für $\tau = it$ mit $t > 0$ und wendet dann den Identitätssatz auf die holomorphe Funktion $\vartheta(\tau) - \sqrt{\frac{i}{\tau}}\vartheta\left(-\frac{1}{\tau}\right)$ auf H an. Für die Situation $\tau = it$ mit $t > 0$ hat man

$$\vartheta(it) = \sum_{n\in\mathbb{Z}} \mathrm{e}^{-\pi n^2 t}$$

Man erhält nun die Jacobi-Identität mit der Poissonschen Summenformel für die Funktion $e^{-\pi t x^2}$ (siehe [Dym–McKean] 2.7.5). Offensichtlich gilt auch $\vartheta(\tau+2)=\vartheta(\tau)$.

Mit der Jacobi-Identität folgt

$$\vartheta(\tau)^4 = -\frac{1}{\tau^2}\vartheta(-\frac{1}{\tau})^4$$

was bis auf das Vorzeichen die "schwache Modularität" bezüglich $S \in \Gamma$ ist. Die "schwache Modularität" bezüglich T^2 folgt aus der 2-Periodizität von ϑ. Man wird also die Elemente betrachten, welche von S und T^2 erzeugt werden und für welche das obige Vorzeichen in die richtige Richtung zeigt.

Satz 4.2.3 *Sei Γ_ϑ die von S und T^2 erzeugte Untergruppe von Γ. Dann ist*

$$\Gamma_\vartheta = \{A \in \Gamma : \ A \equiv I \mod 2\} \cup \{A \in \Gamma : \ A \equiv S \mod 2\}$$

Beweis. Die Menge auf der rechten Seite ist offenbar eine Gruppe, und da sie die Elemente S und T^2 enthält, ist sie Obermenge von Γ_ϑ. Ist nun A ein Element aus der rechten Menge, dann hat A eine der beiden Formen

$$A = \begin{pmatrix} 1+2k & 2l \\ 2m & 1+2n \end{pmatrix}, \text{ oder } A = \begin{pmatrix} 2k & -1+2l \\ 1+2m & 2n \end{pmatrix}$$

Man beweist nun ähnlich wie in 2.1.10, dass A als Wort in S und T^2 geschrieben werden kann (siehe auch [Knopp] 1.3, Corollary 4). □

Für den Rest des Beweises von Satz 4.2.2 betrachtet man den Gruppenhomomorphismus

$$\begin{array}{rcl} \chi : \Gamma_\vartheta & \longrightarrow & \{1,-1\} \\ \chi(A) & = & 1, \text{ falls } A \equiv I \mod 2 \\ \chi(A) & = & -1, \text{ falls } A \equiv S \mod 2 \end{array}$$

Lemma 4.2.4 *Es gilt*

$$\vartheta(\tau)^4 = \frac{\chi(A)}{(c\tau+b)^2}\vartheta^4(\varphi_A(\tau))$$

für alle $A \in \Gamma_\vartheta$ und für alle $\tau \in H$.

Beweis. Bestehe Γ' aus den Elementen von Γ_ϑ für welche die obige Behauptung stimmt. Dann ist Γ' natürlicherweise eine Untergruppe von Γ. Wegen der Jacobi-Identität und der 2-Periodizität von ϑ sind aber S und T^2 in Γ' enthalten, womit $\Gamma' = \Gamma_\vartheta$ ist. □

Die Modularität von ϑ^4 ist für die Elemente A aus Γ_ϑ gewährleistet, für welche $\chi(A)=1$ ist, also der Kern von χ. Diese Elemente bilden nach Satz 4.2.3 genau $\Gamma(2)$. □

Es folgen weitere Beispiele schwach modularer Funktionen.

Definition 4.2.5 *Sei $k \geq 1$, $N \in \mathbb{N}$ und $a_1, a_2 \in \mathbb{Z}$ so dass a_1 und a_2 nicht beide durch N teilbar sind. Man definiert die Eisensteinreihen vom Gewicht $2k$ zur Stufe N durch*

$$G_k(\tau; a_1, a_2, N) := \frac{1}{N^2(2k-1)!}\wp^{(2k-2)}\left(\frac{a_1\tau + a_2}{N}; \tau\right)$$

$\wp^{(2k-2)}$ bedeutet hier die $2k-2$-te Ableitung von $\wp$.

Bemerkung 4.2.6 Man rechnet nach, dass für $k > 1$, $0 \leq a_1, a_2 < N$ gilt

$$G_k(\tau; a_1, a_2, N) = \sum_{\substack{(m_1,m_2)\equiv(a_1,a_2) \\ \bmod N}} \left(\frac{1}{(m_1\tau + m_2)^{2k}} \right)$$

Ebenso sieht man, dass für $k = 1$ gilt

$$G_1(\tau; a_1, a_2, N) = {\sum}'_{\substack{(m_1,m_2)\equiv(a_1,a_2) \\ \bmod N}} \left(\frac{1}{m_1\tau + m_2)^2} - \frac{1}{((m_1 - a_1)\tau + (m_2 - a_2))^2} \right)$$

wobei $\sum'$ bedeutet, dass man nur über die sinnvollen Terme summiert, d.h. die Terme, welche keine 0 im Nenner haben.

Satz 4.2.7 *Die Eisensteinreihen vom Gewicht $2k$ zur Stufe N sind schwach modular vom Gewicht $2k$ bezüglich $\Gamma(N)$.*

Beweis. Wir benötigen nur den Fall $2k = 2$, und beweisen auch nur diesen. Sei also $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma(N)$. Dann gilt nach Lemma 3.1.3

$$\wp(z, \tau) = \frac{1}{(\gamma\tau + \delta)^2} \wp \left(\frac{z}{\gamma\tau + \delta}, \frac{\alpha\tau + \beta}{\gamma\tau + \delta} \right)$$

Also ist mit $z = \frac{a_1\tau + a_2}{N}$

$$G_1(\tau; a_1, a_2, N) = \frac{1}{N^2} \frac{1}{(\gamma\tau + \delta)^2} \wp \left(\frac{1}{N} \frac{a_1\tau + a_2}{\gamma\tau + \delta}; \frac{\alpha\tau + \beta}{\gamma\tau + \delta} \right)$$

Nach Definition ist

$$G_1 \left(\frac{\alpha\tau + \beta}{\gamma\tau + \delta}; a_1, a_2, N \right) = \frac{1}{N^2} \wp \left(\frac{1}{N} (a_1 \frac{\alpha\tau + \beta}{\gamma\tau + \delta} + a_2); \frac{\alpha\tau + \beta}{\gamma\tau + \delta} \right)$$

Vergleicht man die beiden obigen Ausdrücke, so muss also nur noch gezeigt werden, dass

$$\frac{1}{N} \Big(a_1 \frac{\alpha\tau + \beta}{\gamma\tau + \delta} + a_2 \Big) \equiv \frac{1}{N} \frac{a_1\tau + a_2}{\gamma\tau + \delta} \mod \mathbb{Z} + \mathbb{Z} \frac{\alpha\tau + \beta}{\gamma\tau + \delta}$$

Dies wurde aber im Lemma 4.1.7 über Level-N-Strukturen bewiesen. □

Wir beweisen ein weiteres Resultat, welches wir für den Vierquadratesatz benötigen.

Satz 4.2.8 *Man hat die Identitäten*

$$G_1(\tau; 1, 0, 2) = -\frac{\pi^2}{12} - 2\pi^2 \sum_{n \in \mathbb{N}} \left(\sum_{\substack{d|n \\ \frac{n}{d} \text{ ungerade}}} d - \sum_{\substack{d|n \\ \frac{n}{d} \text{ gerade}}} d \right) e^{\pi i n \tau}$$

und

$$G_1(\tau; 0, 1, 2) = \frac{\pi^2}{6} + 4\pi^2 \sum_{n \in \mathbb{N}} \left(\sum_{\substack{d|n, \ \frac{n}{d} \text{ gerade} \\ d \text{ ungerade}}} d \right) e^{\pi i n \tau}$$

Beweis.

$$\begin{aligned}
&G_1(\tau;1,0,2)\\
&= \sum_{m_1 \text{ ungerade}} \sum_{\substack{m_2 \text{ gerade}\\ m_2\neq 0 \text{ falls } m_1=1}} \left(\frac{1}{(m_1\tau+m_2)^2} - \frac{1}{((m_1-1)\tau+m_2)^2}\right)\\
&= -\sum_{\substack{m_2 \text{ gerade}\\ m_2\neq 0}} \frac{1}{m_2^2} + \sum_{\substack{m_1 \text{ ungerade}\\ m_1\geq 1}} \sum_{m_2 \text{ gerade}} \left(\frac{1}{(m_1\tau+m_2)^2} - \frac{1}{((m_1+1)\tau+m_2)^2}\right)\\
&+ \sum_{\substack{m_1 \text{ ungerade}\\ m_1\leq -1}} \sum_{m_2 \text{ gerade}} \frac{1}{(m_1\tau+m_2)^2} - \frac{1}{((m_1-1)\tau+m_2)^2}\\
&= -\sum_{\substack{m\in\mathbb{Z}\\ m\neq 0}} \frac{1}{(2m)^2} + 2\sum_{\substack{m_1 \text{ ungerade}\\ m_1\geq 1}} \sum_{m_2 \text{ gerade}} \left(\frac{1}{(m_1\tau+m_2)^2} - \frac{1}{((m_1+1)\tau+m_2)^2}\right)\\
&= -\frac{1}{2}\sum_{m=1}^{\infty} \frac{1}{m^2} + \frac{1}{2}\sum_{\substack{m_1 \text{ ungerade}\\ m_1\geq 1}} \sum_{m\in\mathbb{Z}} \left(\frac{1}{(\frac{m_1}{2}\tau+m)^2} - \frac{1}{(\frac{m_1+1}{2}\tau+m)^2}\right)\\
&= -\frac{\pi^2}{12} - 2\pi^2 \sum_{\substack{m_1 \text{ ungerade}\\ m_1\geq 0}} \left(\sum_{d\in\mathbb{N}} d\mathrm{e}^{\pi i d m_1\tau} - \sum_{d\in\mathbb{N}} d\mathrm{e}^{\pi i d(m_1+1)\tau}\right)\\
&= -\frac{\pi^2}{12} - 2\pi^2 \sum_{n\in\mathbb{N}} \left(\Bigg(\sum_{\substack{d|n\\ \frac{n}{d} \text{ ungerade}}} d\Bigg) \mathrm{e}^{\pi i n\tau} - \Bigg(\sum_{\substack{d|n\\ \frac{n}{d} \text{ gerade}}} d\Bigg) \mathrm{e}^{\pi i n\tau}\right)
\end{aligned}$$

Im Übergang zur vorletzten Zeile wurde Lemma 3.2.1 verwendet. Der Beweis für $G_1(\tau;0,1,2)$ geht analog. □

Die Beweisstrategie des Vierquadratesatzes ist nun so: Wir haben gezeigt, dass $\vartheta(\tau)^4 = 1 + \sum_{n\in\mathbb{N}} r(n)\mathrm{e}^{\pi i n\tau}$ schwach modular vom Gewicht 2 bezüglich $\Gamma(2)$ ist. Dasselbe haben wir aber auch für $G_1(\tau;1,0,2)$, $G_1(\tau;0,1,2)$. Wir werden weiter zeigen, dass der Vektorraum $M_1(\Gamma(2))$, welcher aus den auf $\{\mathrm{Im}(\tau)\geq 1\}$ beschränkten schwach modularen Funktionen vom Gewicht 2 bezüglich $\Gamma(2)$ besteht, 2-dimensional ist, und dass $G_1(\tau;1,0,2)$, $G_1(\tau;0,1,2)$ eine Basis ist. Somit ist ϑ^4 eine Linearkombination dieser Eisensteinreihen. Genauer gilt der folgende Satz, welchen wir später beweisen werden.

Satz 4.2.9 *Es gilt*

$$\vartheta(\tau)^4 = -\frac{4}{\pi^2}G_1(\tau;1,0,2) + \frac{4}{\pi^2}G_1(\tau;0,1,2)$$

Der Vierquadratesatz folgt dann aus obigem Satz wie folgt:

Beweis (Vierquadratesatz)**.** Aus der Definition der Thetafunktion folgt, dass

$$\vartheta(\tau)^4 = \sum_{n_1,n_2,n_3,n_4\in\mathbb{Z}} e^{\pi i(n_1^2+n_2^2+n_3^2+n_4^2)\tau} = \sum_{n\in\mathbb{N}} r(n)\, e^{\pi i n\tau}$$

Einsetzen in Satz 4.2.9 und Koeffizientenvergleich mit Satz 4.2.8 ergibt

$$r(n) = 8\Big(\sum_{\substack{d|n \\ \frac{n}{d} \text{ ungerade}}} d - \sum_{\substack{d|n \\ \frac{n}{d} \text{ gerade}}} d\Big) + 16 \sum_{\substack{d \text{ ungerade},\ d|n \\ \frac{n}{d} \text{ gerade}}} d$$

Für n ungerade trägt nur die erste Summe etwas zu $r(n)$ bei und man hat

$$r(n) = 8 \sum_{d|n} d$$

Für n gerade schreibt man $n = 2^a m$ mit m ungerade und $a \geq 1$. Dann ist

$$\sum_{\substack{d \text{ ungerade},\ d|n \\ \frac{n}{d} \text{ gerade}}} d = \sum_{d|m} d$$

und

$$\sum_{\substack{d|n \\ \frac{n}{d} \text{ ungerade}}} d = 2^a \sum_{d|m} d$$

Weiter ist

$$\sum_{\substack{d|n \\ \frac{n}{d} \text{ gerade}}} d = (1 + 2 + \cdots + 2^{a-1}) \sum_{d|m} d$$

und somit

$$\begin{aligned} 8 \left(\sum_{\substack{d|n \\ \frac{n}{d} \text{ ungerade}}} d - \sum_{\substack{d|n \\ \frac{n}{d} \text{ gerade}}} d \right) + 16 \sum_{\substack{d|n \\ \frac{n}{d} \text{ gerade} \\ d \text{ ungerade}}} d = \\ 8[(2^a - (1 + 2 + \cdots + 2^{a-1}) + 2] \sum_{d|m} d \ = \ 24 \sum_{\substack{d|n \\ d \text{ ungerade}}} d \end{aligned}$$

womit der Vierquadratesatz bis auf die Lücke 4.2.9, welche im nächsten Abschnitt bewiesen wird, erledigt wäre. □

Übung 4.2.10 Für eine positiv definite symmetrische $k \times k$-Matrix Q und für $\Im(\tau) > 0$ setzt man:

$$\vartheta_Q(\tau) := \sum_{m \in \mathbb{Z}^k} e^{\pi i \tau \langle m, Qm \rangle}$$

i) Zeigen Sie, dass

$$\vartheta_Q(\tau) = \frac{1}{\sqrt{\det(Q)}} \left(\frac{i}{\tau}\right)^{\frac{k}{2}} \vartheta_{Q^{-1}}\left(-\frac{1}{\tau}\right)$$

Hinweis: Zeigen Sie obige Identität für $\tau = it$, $t > 0$ und setzen Sie dann analytisch fort.

ii) Zeigen Sie, dass für

$$Q = \begin{pmatrix} 2 & 1 \\ 1 & 6 \end{pmatrix}$$

gilt:

$$\vartheta_Q(\tau) = \frac{i}{\sqrt{11}\tau} \vartheta_Q\left(\frac{-1}{11\tau}\right)$$

Übung 4.2.11 Sei Q eine positiv definite, symmetrische, ganzzahlige Matrix, sodass $\langle Qm, m\rangle$ gerade ist für $m \in \mathbb{Z}^k$, N die kleinste natürliche Zahl mit NQ^{-1} ganzzahlig und $h \in \mathbb{Z}^k$, sodass $Qh \equiv 0 \mod N$. Setze für $\tau \in H = \{\mathrm{Im}(z) > 0\}$

$$\vartheta_{Q,h}(\tau) = \sum_{m \in \mathbb{Z}^k} \mathrm{e}^{\langle \pi i \tau (m + \frac{h}{N}), Q(m + \frac{h}{N})\rangle}$$

Zeigen Sie:

i)

$$\vartheta_{Q,h}(\tau + 1) = \mathrm{e}^{\langle \pi i h, Q \frac{h}{N^2}\rangle} \vartheta_{Q,h}(\tau)$$

falls $\langle m, Qm\rangle = 1 \; \forall \, m \in \mathbb{Z}^k$

ii) Ist $c \in \mathbb{N}$, so ist

$$\vartheta_{Q,h}(\tau) = \sum_{g \mod cN,\; g \equiv h \mod N} \vartheta_{cQ,g}(c\tau)$$

Dabei bedeutet $g \mod cN$, dass über eine Familie von Vektoren $g \in \mathbb{Z}^k$ summiert wird, welche ein Erzeugendensystem von $\mathbb{Z}^k / cN\mathbb{Z}^k$ repräsentieren.

iii)

$$\vartheta_{Q,h}(\tau) = \frac{1}{\sqrt{\det(Q)}} \left(\frac{i}{\tau}\right)^{\frac{k}{2}} \sum_{g \mod N,\; Qg \equiv 0 \mod N} \mathrm{e}^{\langle 2\pi i g, Q \frac{h}{N^2}\rangle} \vartheta_{Q,g}\left(-\frac{1}{\tau}\right)$$

Übung 4.2.12 Sei Q eine positiv definite symmetrische $(k \times k)$-Matrix für welche $\langle Qm, m\rangle$ gerade ist, falls $m \in \mathbb{Z}^k$ und $N \in \mathbb{N}$ die kleinste natürliche Zahl, sodass NQ^{-1} ganzahlig ist. Ferner sei $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z})$ mit $c \geq 1$. Man setzt für $g \in \mathbb{Z}^k$ mit $Qg \equiv 0 \mod N$

$$\phi(g) := \sum_{h \mod c} \mathrm{e}^{\frac{\pi i}{cN^2}(aN^2 h \cdot Qh + 2Nh \cdot Qg + dg \cdot Qg)}$$

Zeigen Sie, dass

i)

$$\phi(g) = \sum_{h \mod c} \mathrm{e}^{\frac{\pi i}{cN^2}(a(Nh + dg) \cdot Q(Nh + dg) - bcdg \cdot Qg)}$$

und dass $\phi(g) = \phi(g')$ falls $g \equiv g' \mod N$.

ii) Zeigen Sie unter Verwendung von Aufgabe 4.2.11 und von i), dass

$$\vartheta_Q\left(\frac{a\tau + b}{c\tau + d}\right) = \frac{(-i)^{\frac{k}{2}} (c\tau + d)^{\frac{k}{2}}}{c^{\frac{k}{2}} \sqrt{\det Q}} \sum_{g \mod N,\; Qg \equiv 0 \mod N} \phi(g) \vartheta_{Q,g}(\tau)$$

Hinweis: $\frac{a\tau + b}{c\tau + d} = \frac{1}{c}(a - \frac{1}{c\tau + d})$

iii) Man bezeichnet mit $S(Q, a, c)$ die Gauss'sche Summe

$$S(Q, a, c) := \sum_{h \mod c} \mathrm{e}^{\frac{a\pi i}{c} h \cdot Qh}$$

Zeigen Sie, dass für N ungerade, $d \equiv 0 \mod N$ und für alle $g \in \mathbb{Z}^k$ mit $Qg \equiv 0 \mod N$ gilt

$$\phi(g) = S(Q, a, c)$$

iv) Es seien die gleichen Voraussetzungen wie in (iii) erfüllt. Zeigen Sie:

$$\frac{S(Q, a, c)}{(-c)^{\frac{k}{2}}} \vartheta_Q(\tau) = \frac{1}{(d\tau - c)^{\frac{k}{2}}} \vartheta_Q\left(\frac{b\tau - a}{d\tau - c}\right)$$

Hinweis: $\frac{b\tau - a}{d\tau - c} = \frac{a(-\frac{1}{\tau}) + b}{c(-\frac{1}{\tau}) + d}$

v) Sei $Q = \begin{pmatrix} 2 & 1 \\ 1 & 6 \end{pmatrix}$, $A = \begin{pmatrix} 3 & 1 \\ 11 & 4 \end{pmatrix}$. Zeigen Sie, dass für $\tau \in H$

$$\vartheta_Q(\tau) = \frac{1}{11\tau + 4} \vartheta_Q(\phi_A(\tau))$$

und

$$\vartheta_Q(\tau + 1) = \vartheta_Q(\tau)$$

4.3 Modulformen

Definition 4.3.1 *Sei $\Gamma' \subset \Gamma$ eine Untergruppe. Eine Modulform vom Gewicht $2k$ bezüglich Γ' ist eine holomorphe Funktion $f : H \longrightarrow \mathbb{C}$, welche schwach modular vom Gewicht $2k$ bezüglich Γ' ist, und sodass für jedes $A \in \Gamma$ die Funktion*

$$\frac{1}{(c\tau + d)^{2k}} f(\varphi_A(\tau))$$

auf $\{\tau \in H : Im(\tau) \geq 1\}$beschränkt ist.

Bemerkung 4.3.2 Ist f schwach modular vom Gewicht $2k$ bezüglich Γ' und ist $A_1, \ldots, A_r$ ein Repräsentantensystem für die Rechtsnebenklassen von Γ' in Γ, so ist f Modulform vom Gewicht $2k$, falls nur die Funktionen

$$\frac{1}{(c\tau + d)^{2k}} f(\varphi_A(\tau)) \quad , \quad A = A_1, \ldots, A_r$$

auf $\{\tau \in H : \mathrm{Im}(\tau) \geq 1\}$ beschränkt sind.

Beweis. Ist $A' \in \Gamma$ beliebig, so gibt es $i \in \{1, \ldots, r\}$ und $B \in \Gamma'$ so dass $A' = B\, A_i$. Dann ist

$$\begin{aligned} \left(\varphi'_{A'}(\tau)\right)^k f(\varphi_{A'}(\tau)) &= \left[\varphi'_B(\varphi_{A_i}(\tau))\, \varphi'_{A_i}(\tau)\right]^k \cdot f\left(\varphi_B(\varphi_{A_i}(\tau))\right) \\ &= \left(\varphi'_{A_i}(\tau)\right)^k \cdot f\left(\varphi_{A_i}(\tau)\right) \end{aligned}$$

da ja $B \in \Gamma'$. $\square$

Bemerkung 4.3.3 *Zu festem k und Γ' bilden die Modulformen vom Gewicht $2k$ einen Vektorraum. Man nennt diesen Vektorraum $M_k(\Gamma')$. Es gilt offenbar*

$$M_k(\Gamma') \cdot M_l(\Gamma') \subset M_{k+l}(\Gamma')$$

Es ist die zur schwachen Modularität zusätzlich verlangte Beschränktheitsbedingung in Definition 4.3.1, welche ähnlich wie beim Satz von Liouville starke Einschränkungen an die Modulformen gibt, aber doch nicht so stark, dass keine interessanten Aussagen mehr möglich wären. Es sind also viel eher die Modulformen als nur die schwach modularen Funktionen von Interesse.

Beispiel 4.3.4 Die Eisensteinreihen G_k sind Modulformen vom Gewicht $2k$ bezüglich der vollen Modulgruppe Γ.
Ist $\Gamma' = \Gamma(2)$, dann ist ϑ^4 eine Modulform vom Gewicht 2 bezüglich Γ'. Man braucht, um dies einzusehen, die Beschränktheitsbedingung von Bemerkung 4.3.2 nur für die Matrizen $I, S, T, T^{-1}S, ST, TST$ nachzuweisen, denn diese bilden nach Beispiel 4.1.9 ein Repräsentantensystem für $\Gamma/\Gamma(2)$. Unter Verwendung der Jacobi-Identität (4.1) für die Thetafunktion ist dies einfach.
Schliesslich sind die Eisensteinreihen $G_k(\tau; a_1, a_2, N)$ der Stufe N Modulformen vom Gewicht $2k$ bezüglich $\Gamma(N)$. Dass sie schwach modular sind, wurde bereits in Satz 4.2.7 nachgeprüft. Aus der Definition ist klar, dass die Bedingung aus Bemerkung 4.3.2 für $A = Id$ erfüllt ist. Ist nun $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL(2, \mathbb{Z})$, so zeigt man wie im Beweis von Satz 4.2.7, dass

$$\frac{1}{(\gamma\tau + \delta)^{2k}} G_k(\tau; a_1, a_2, N) = G_k(\tau; a_1', a_2', N)$$

mit $a_1' = \alpha a_1 + \gamma a_2,\ a_2' = \beta a_1 + \delta a_2$. Daraus folgt, dass die Bedingung aus Bemerkung 4.3.2 für alle $A \in SL(2, \mathbb{Z})$ erfüllt ist.

Wir betrachten nun Räume von Modulformen bezüglich der vollen Modulgruppe Γ.

Satz 4.3.5 *Sei $f \not\equiv 0$ aus $M_k(\Gamma)$. Dann gilt*

$$\nu_\infty(f) + \frac{1}{2}\nu_i(f) + \frac{1}{3}\nu_\rho(f) + \sum_{\substack{p \in H/\Gamma \\ [p] \notin \{[i], [\rho]\}}} \nu_p(f) = \frac{k}{6} \tag{4.2}$$

wobei wieder $\rho = e^{\pi i/3}$ ist.

Beweis. Der Beweis ist ähnlich wie der von Satz 3.4.3. Formel 3.1 muss dabei durch

$$\int_\gamma \frac{f'(z)}{f(z)} dz - \int_{\varphi_A(\gamma)} \frac{f'(z)}{f(z)} dz = -k \int_{\varphi_A(\gamma)} \frac{\varphi_A''(z)}{\varphi_A'(z)} dz$$

ersetzt werden. Siehe auch [Serre] VII, §3.1. □

Definition 4.3.6 *Eine Modulform $f \in M_k(\Gamma)$ heisst Spitzenform, falls $\nu_\infty(f) \geq 1$ ist. Der Vektorraum der Spitzenformen wird mit $M_k^0(\Gamma)$ bezeichnet.*

Beispiel 4.3.7 $\Delta = g_2^3 - 27g_3^2 \in M_6^0(\Gamma)$, *denn der nullte Koeffizient der Fourierreihe von Δ ist nach Korollar 3.2.4 gleich* 0.

Satz 4.3.8 *Es gilt*

(a) $M_1(\Gamma) = \{0\}$

(b) $\dim(M_k(\Gamma)) = 1$ *für* $k = 0, 2, 3, 4, 5$. *Für festes solches* k *wird eine Basis gegeben durch* G_k, *wobei man* $G_0 = 1$ *setzt.*

(c) *Man hat den Isomorphismus*

$$\begin{array}{rcl} M_{k-6} & \longmapsto & M_k^0 \\ f & \longrightarrow & \Delta \cdot f \end{array}$$

Beweis. (a): Folgt sofort aus (4.2).
(b): Für festes $k \in \{0, 2, 3, 4, 5\}$ hat nach (4.2) jedes $f \in M_k(\Gamma)$ dieselbe Nullstellenkonfiguration. Sind also $f, g \in M_k(\Gamma)$, so ist $\frac{f}{g} \in M_0(\Gamma)$, also konstant.
(c): Ist $g \in M_{k+6}^0(\Gamma)$, so ist $g/\Delta \in M_k(\Gamma)$, da Δ nullstellenfrei ist (Korollar 3.2.4). □

Bemerkung 4.3.9 *Da für* $k \geq 6$

$$\dim(M_k / M_k^0) = 1$$

ist, lässt sich aus (c) von 4.3.8 $\dim(M_k)$ *bestimmen, nämlich*

$$\dim(M_k) = \begin{cases} [k/6] & \textit{falls } k \equiv 1 \mod 6 \\ [k/6 + 1] & \textit{falls } k \not\equiv 1 \mod 6 \end{cases}$$

Korollar 4.3.10 *Sei* $k \geq 4$ *und* $f \in M_k(\Gamma)$. *Dann gibt es ein Polynom* $P(x, y)$ *so dass* $f(\tau) = P(G_2(\tau), G_3(\tau))$. *Insbesondre gibt es ein Polynom* $P_k(x, y)$ *so dass* $G_k(\tau) = P(G_2(\tau), G_3(\tau))$. *Man kann* $P_k \in \mathbb{Q}[x, y]$ *wählen.*

Beweis. Aus Teil (b) von Satz 4.3.8 folgt, dass G_2^2 beziehungsweise $G_2 G_3$ Basen von M_4 beziehungsweise M_5 sind. Wir führen jetzt Induktion nach k. Sei also $f \in M_k$ mit $k \geq 6$. Wähle $a, b \in \mathbb{N}$ so dass $2a + 3b = k$. Dann ist $G_2^a G_3^b \in M_k \setminus M_k^0$. Da $\dim(M_k / M_k^0) = 1$, gibt es $\lambda, \mu \in \mathbb{C}$ und $\tilde{f} \in M_k^0$ so dass $f = \lambda G_2^a G_3^b + \mu \tilde{f}$. Nach Teil (c) von Satz 4.3.8 gibt es eine Form $g \in M_{k-6}$ so dass $\tilde{f} = \Delta g$. Nach Induktionsvoraussetzung kann g als Polynom in G_2 und G_3 geschrieben werden, und nach Definition ist auch Δ ein Polynom in G_2 und G_3. Folglich ist auch f ein Polynom in G_2 und G_3.
Aus dem Bewiesenen folgt, dass es ein Polynom $P_k(x, y)$ gibt mit $G_k(\tau) = P_k(G_2(\tau), G_3(\tau))$. Da G_k, G_2, G_3 rationale Fourierkoeffizienten haben, folgt wie im Beweis von Bemerkung 3.4.10, dass P_k mit rationalen Koeffizienten gewählt werden kann. □

In Satz 4.3.5 tritt mit $\nu_\infty(f)$ ein Term auf, der die Ordnung der Nullstelle von f in der Spitze ∞ beschreibt. Das Beispiel $\Gamma(2)$ suggeriert, dass es im Allgemeinen mehrere Spitzen gibt. Sieht man sich Figur 4.1 des Fundamentalbereichs für $\Gamma(2)$ an, so sieht man, dass neben ∞ auch -1, 0, $+1$ als Spitzen behandelt werden sollten. Die Spitzen -1 und $+1$ sind allerdings äquivalent, da sie durch $T^2 \in \Gamma(2)$ ineinander übergefürt werden.

Definition 4.3.11 *Sei* Γ' *eine Untergruppe von endlichem Index in* Γ *und* $A_1, \ldots, A_r$ *ein Repräsentantensystem für die Rechtsnebenklassen von* Γ' *in* Γ.

i) Die Punkte $\varphi_{A_j}(\infty)$, $j = 1, \dots, r$, heissen Spitzen von Γ'.

i) Sei f eine Modulform für Γ' und $\sigma = \varphi_{A_j}(\infty)$ eine Spitze von Γ'. Dann ist $f \circ \varphi_{A_j}$ schwach modular vom Gewicht 0 bezüglich $\Gamma'' = \varphi_{A_j}^{-1} \circ \Gamma' \circ \varphi_{A_j}$. Da Γ'' von endlichem Index in Γ ist, gibt es ein minimales $k \geq 1$, sodass $T^k \in \Gamma''$. Folglich hat $f \circ \varphi_{A_j}$ eine Fourierreihe

$$f \circ \varphi_{A_j}(\tau) = \sum_{n=0}^{\infty} a_n \, e^{2\pi i n \tau / k}$$

Wir setzen

$$\nu_\sigma(f) := \min\{n \,|\, a_n \neq 0\}$$

iii) f heisst Spitzenform, falls $\nu_\sigma(f) \geq 1$ für alle Spitzen σ.

Die obige Definition macht Sinn, denn ist $\varphi_{A_i}(\infty) = \sigma = \varphi_{A_j}(\infty)$, so ist $\varphi_{A_i^{-1} \circ A_j}(\infty) = \infty$. Somit gibt es $\ell \in \mathbb{Z}$ so dass $A_j = A_i \circ T^\ell$.

Wir betrachten jetzt speziell für den Vierquadratesatz Räume von Modulformen für $\Gamma' = \Gamma(2)$, d.h. die Räume $M_k(\Gamma(2))$.

Satz 4.3.12 *Sei $f \not\equiv 0$ aus $M_k(\Gamma(2))$. Dann gilt:*

$$\nu_0(f) + \nu_1(f) + \nu_\infty(f) + \sum_{p \in H/\Gamma(2)} \nu_p(f) = k$$

Beweis. Der Beweis verläuft ähnlich wie der Beweis von Satz 3.4.3 bzw. Satz 4.3.5, wobei hier natürlich über den Rand des Fundamentalbereiches von $\Gamma(2)$ integriert werden muss. Man verwendet, dass $S T^{-2} S \in \Gamma(2)$ den linken unteren Kreisbogen im Rand von $R_{\Gamma(2)}$ aus Figur 4.1 auf den rechten unteren Kreisbogen abbildet. □

Korollar 4.3.13 *(a) $M_0(\Gamma(2))$ besteht nur aus den konstanten Funktionen.*

(b) $\dim(M_1(\Gamma(2)) = 2$, und $G_1(\tau; 1, 0, 2)$, $G_1(\tau; 0, 1, 2)$ bilden eine Basis von $M_1(\Gamma(2))$.

Beweis. (a): Sei $f \not\equiv 0$ aus $M_0(\Gamma(2))$ und c in der Wertemenge von f. Dann ist $f - c$ auch aus $M_0(\Gamma(2))$ und hat eine Nullstelle. Nach 4.3.12 ist also $f - c \equiv 0$.
(b): Setze $F_1 := G_1(\tau; 1, 0, 2)$, $F_2 := G_1(\tau; 0, 1, 2)$. Wie in Beispiel 4.3.4 bemerkt, liegen diese Funktionen in $M_1(\Gamma(2))$. Die ersten Terme ihrer Fourierreihen sind nach Satz 4.2.8

$$\begin{aligned} F_1(\tau) &= -\frac{\pi^2}{12} - 2\pi^2 \, e^{\pi i \tau} - 2\pi^2 \, e^{2\pi i \tau} + \cdots \\ F_2(\tau) &= \frac{\pi^2}{6} \qquad\qquad\qquad + 4\pi^2 \, e^{2\pi i \tau} + \cdots \end{aligned}$$

Daraus sieht man sofort, dass F_1 und F_2 linear unabhängig sind. Sei nun $f \not\equiv 0$ auch in $M_1(\Gamma(2))$ und $p \in H/\Gamma(2) \cup \{0, 1, \infty\}$ die Nullstelle von f (siehe Satz 4.3.12). Man kann nun $\mu, \lambda \in \mathbb{C}$ finden, sodass $\mu F_1 + \lambda F_2$ genau eine Nullstelle in p hat. Die Funktion $\frac{f}{\mu F_1 + \lambda F_2}$ liegt dann aber in $M_0(\Gamma(2))$ und ist somit konstant. □

Es folgt nun der Schluss des Beweises des Vierquadratesatzes:
Da $\vartheta^4 \in M_1(\Gamma(2))$ liegt, gibt es nach Korollar 4.3.13 komplexe Zahlen a, b so dass

$$\vartheta^4(\tau) = a \, G_1(\tau; 1, 0, 2) + b \, G_1(\tau; 0, 1, 2)$$

Der Vergleich der oben gegebenen Anfangsterme der Fouriereihen für $F_1 = G_1(\tau;1,0,2)$ und $F_2 = G_1(\tau;0,1,2)$ mit den Anfangstermen der Fourierreihe von ϑ^4

$$\vartheta^4(\tau) = 1 + 8\,e^{\pi i\tau} + 24\,e^{2\pi i\tau} + \cdots$$

zeigt, dass $a = -\frac{4}{\pi^2}$, $b = \frac{4}{\pi^2}$. Damit ist Satz 4.2.9 und somit auch der Vierquadratesatz bewiesen. $\square$

Übung 4.3.14 Sei $f \not\equiv 0$ eine Modulform vom Gewicht $2k$ für $\Gamma_0(11)$. Beweisen Sie folgende Aussagen:

i)

$$\nu_0(f) + \nu_\infty(f) + \sum_{p\in H/\Gamma_0(11)} \nu_p(f) = 2k$$

(Beweisen Sie diese Identität zuerst für den Fall, dass f keine Nullstellen auf dem Rand des Fundamentalbereiches von $\Gamma_0(11)$ hat.)

ii) Der Raum der Spitzenformen vom Gewicht 2 für $\Gamma_0(11)$ hat höchstens Dimension 1.

Kapitel 5

Die Dedekind'sche Etafunktion und Partitionen

5.1 Die Dedekind'sche Etafunktion

Die Notationen der früheren Kapitel werden beibehalten.

Definition 5.1.1 *Die Dedekind'sche η-Funktion ist wie folgt auf H definiert:*

$$\eta(\tau) := e^{\frac{\pi i \tau}{12}} \prod_{n=1}^{\infty} (1 - e^{2\pi i n \tau})$$

Man prüft leicht nach, dass die Konvergenz des obigen Produktes auf H keine Probleme bereitet.

Für die η-Funktion gelten folgende Funktionalgleichungen:

Satz 5.1.2 *a.)*

$$\eta(\tau + 1) = e^{\frac{\pi i}{12}} \eta(\tau)$$

b.)

$$\eta(-\frac{1}{\tau}) = (-i\tau)^{\frac{1}{2}} \eta(\tau)$$

wo die Quadratwurzel von $-i\tau$ über den Hauptzweig des Logarithmus definiert wird.

Beweis. a.) ist offensichtlich.
Um b.) zu zeigen, beweist man zuerst, dass

$$F(z) := \sqrt{\mathrm{Im}(z)} |\eta(z)|^2$$

$SL(2, \mathbb{Z})$-invariant ist, d.h. es gilt

$$F(\varphi_A(z)) = F(z) \; \forall \, A \in SL(2, \mathbb{Z})$$

Schreibe $\tau = x + iy$, $y > 0$, und sei $\mathrm{Re}(s) > \frac{1}{2}$. Dann lässt sich die holomorphe Funktion

$$s \longrightarrow E(\tau, s) := y^s \sum_{(m,n) \neq (0,0)} |m\tau + n|^{-2s}$$

von Übung 3.1.8 nach Übung 3.1.11 zu einer meromorphen Funktion fortsetzen, die in 0 holomorph ist. Wir werden jetzt zeigen, dass

$$-\frac{1}{2}\frac{\partial E(\tau,s)}{\partial s}|_{s=0} = \log(2\pi\sqrt{y}|\eta(\tau)|^2) \tag{5.1}$$

gilt. Weil die linke Seite von (5.1) aber nach Übung 3.1.8 $SL(2,\mathbb{Z})$-invariant ist, so gilt das natürlich auf für die rechte Seite von (5.1). Um (5.1) zu zeigen braucht man folgende Zutaten: Nach Übung 3.1.11 gilt für $\tau = x + iy$:

$$\begin{aligned}\frac{1}{2}E(\tau,s) &= \zeta(2s)y^s + \sqrt{\pi}\frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)}\zeta(2s-1)y^{1-s} \\ &+ \frac{4\pi^s\sqrt{y}}{\Gamma(s)}\sum_{n=1}^{\infty} n^{s-\frac{1}{2}}\left(\sum_{d|n}\frac{1}{d^{2s-1}}\right)K_{s-\frac{1}{2}}(2\pi ny)\,\cos(2\pi nx)\end{aligned} \tag{5.2}$$

wo

$$K_s(2x) := \frac{1}{2}\int_0^{\infty} \mathrm{e}^{-x(t+\frac{1}{t})}t^{s-1}dt$$

für $x > 0$ ist. Aus den Funktionalgleichungen der Gammafunktion ([Ahlfors] chapter 5, 2.4) folgert man, dass

$$\Gamma(-\frac{1}{2}) = -2\sqrt{\pi} \tag{5.3}$$

und dass die Gammafunktion in 0 einen einfachen Pol mit Residuum 1 hat. Folglich ist

$$\frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)}\bigg|_{s=0} = 0 \quad , \quad \frac{d}{ds}\frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)}\bigg|_{s=0} = -2\sqrt{\pi} \tag{5.4}$$

Aus der Funktionalgleichung der Zetafunktion folgt, dass

$$\zeta(0) = -\frac{1}{2},\ \zeta(-1) = -\frac{1}{12},\ \zeta'(0) = -\frac{1}{2}\log(2\pi) \tag{5.5}$$

Siehe [Titchmarsh] 2.4. Schliesslich weiss man aus Übung 3.1.10, dass

$$K_{-\frac{1}{2}}(u) = \sqrt{\frac{\pi}{2u}}\,\mathrm{e}^{-u} \tag{5.6}$$

Differenziert man nun (5.2) nach s und wertet man das Ergebnis an der Stelle $s = 0$ aus, so erhält man unter Berücksichtigung der Gleichungen (5.3), (5.4), (5.5) und (5.6)

$$\begin{aligned}\frac{1}{2}\frac{\partial}{\partial s}E(\tau,s)|_{s=0} &= \zeta(0)\log y + 2\zeta'(0) + \sqrt{\pi}\big(-2\sqrt{\pi}\big)\zeta(-1)\,y \\ &\quad +4\sqrt{y}\sum_{n=1}^{\infty}\frac{1}{\sqrt{n}}\Big(\sum_{d|n} d\Big)K_{-\frac{1}{2}}(2\pi ny)\,\cos 2\pi nx \\ &= -\frac{1}{2}\log y - \log 2\pi + \frac{\pi}{6}y + 2\sum_{n=1}^{\infty}\frac{1}{n}\Big(\sum_{d|n} d\Big)\,e^{-2\pi ny}\,\cos 2\pi nx \\ &= -\log(2\pi\sqrt{y}) - \mathrm{Re}\log e^{\frac{\pi i\tau}{6}} + 2\,\mathrm{Re}\left[\sum_{n=1}^{\infty}\Big(\sum_{d|n} d\Big)\frac{\mathrm{e}^{2\pi in\tau}}{n}\right]\end{aligned} \tag{5.7}$$

Nun gilt für $|z| < 1$

$$\begin{aligned}
\log\Big(\prod_{m=1}^{\infty}(1-z^m)\Big) &= \sum_{m=1}^{\infty}\log(1-z^m) \\
&= -\sum_{m=1}^{\infty}(z^m + \frac{z^{2m}}{2} + \frac{z^{3m}}{3} + \cdots) \\
&= -\sum_{n=1}^{\infty}\Big(\sum_{d'|n}\frac{1}{d'}\Big)z^n \\
&= -\sum_{n=1}^{\infty}\Big(\sum_{d|n}d\Big)\frac{z^n}{n}
\end{aligned}$$

Mit $z = \mathrm{e}^{2\pi i\tau}$ ergibt Einsetzen der obigen Gleichung in (5.7)

$$\begin{aligned}
-\frac{1}{2}\frac{\partial E}{\partial s}|_{s=0} &= \mathrm{Re}\Big[\log(2\pi\sqrt{y}\mathrm{e}^{\frac{\pi i\tau}{6}}\prod_{n=1}^{\infty}(1-\mathrm{e}^{2\pi in\tau})^2)\Big] \\
&= \log(2\pi\sqrt{y}|\eta(\tau)|^2)
\end{aligned}$$

also Gleichung (5.1).
Aus der $SL(2,\mathbb{Z})$-Invarianz von $F(z)$ folgert man nun:

$$\mathrm{Im}(-\frac{1}{z})|\eta(-\frac{1}{z})|^4 = \mathrm{Im}(z)|\eta(z)|^4$$

und weil $\mathrm{Im}(-\frac{1}{z}) = \frac{1}{|z|^2}\mathrm{Im}(z)$ ist, folgt weiter

$$|\eta(-\frac{1}{z})|^4 = |z|^2|\eta(z)|^4$$

also

$$\frac{|\eta(-\frac{1}{z})|}{\sqrt{|z|}|\eta(z)|} = 1$$

Also ist

$$\frac{\eta(-\frac{1}{z})}{\sqrt{z}\,\eta(z)} \tag{5.8}$$

holomorph vom Betrage 1, womit aus dem Offenheitssatz für holomorphe Funktionen folgt, dass die Funktion aus (5.8) konstant ist. Setzt man in (5.8) $z = i$ ein, dann muss die Konstante $\frac{1}{\sqrt{i}}$ sein, was genau die Aussage des Satzes ist. □

Polchinsky bemerkte einen Zusammenhang (siehe [Sarnak], Appendix 1.1) zwischen $-\frac{1}{2}\frac{\partial E}{\partial s}|_{s=0}$ und dem Laplaceoperator. Um darauf einzugehen betrachten wir zuerst eine selbstadjungierte positiv definite Matrix mit Eigenwerten $0 < \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$. Betrachtet man nun die holomorphe Funktion

$$\zeta_A(s) := \sum_{j=1}^{n}\lambda_j^{-s}$$

so ist
$$-\frac{d}{ds}\zeta_A(s)|_{s=0} = \sum_{j=1}^{n} \log(\lambda_j) = \log(\det(A))$$
also ist
$$\det(A) := \exp\left(-\frac{d}{ds}\zeta_A(s)|_{s=0}\right)$$
Hat man jetzt einen selbstadjungierten positiven Operator A auf einem Hilbertraum mit Eigenwerten $0 < \lambda_1 \leq \lambda_2 \leq \cdots$ dann definiert man für $\mathrm{Im}(s)$ genügend gross analog wie vorher
$$\zeta_A(s) := \sum_{j=1}^{\infty} \lambda_j^{-s}$$
Falls diese holomorphe Funktion in eine Umgebung vom Ursprung fortgesetzt werden kann, dann definiert man
$$\det{}'(A) := \exp\left(-\frac{d}{ds}\zeta_A(s)|_{s=0}\right)$$
Sei nun
$$L_\tau^* := \left\{\gamma \in \mathbb{R}^2 : \langle\gamma,\omega\rangle \in 2\pi\mathbb{Z} \ \forall\, \omega \in L_\tau\right\}$$
das zu L_τ duale Gitter und Δ der Laplaceoperator auf $\mathbf{R}^2/L_\tau^*$. Dann hat $-\Delta$ die Eigenfunktionen
$$\mathrm{e}^{i\langle\omega,x\rangle},\ \omega \in L_\tau$$
zu den Eigenwerten $|\omega|^2$. Also ist $\zeta_\Delta = E(\tau, s)$ und somit
$$\det{}'(-\Delta) = const\,\sqrt{\mathrm{Im}(\tau)}\,|\eta(\tau)|^2$$

Bemerkung 5.1.3 *Weil S und T die volle Modulgruppe erzeugen, folgt aus dem Satz, dass η^{24} schwach modular vom Gewicht 12 ist. Man prüft leicht nach, dass η^{24} auch die Beschränktheitsbedingung aus Definition 4.3.1 erfüllt, also eine Modulform ist. Aus*
$$\eta^{24}(\tau) = e^{2\pi i\tau}\prod_{n=1}^{\infty}(1 - e^{2\pi i n\tau})^{24}$$
folgt sofort, dass $\nu_\infty(\eta^{24}) \geq 1$ ist, also η^{24} sogar eine Spitzenform vom Gewicht 12 sein muss, d.h. es ist $\eta^{24} \in M_6^0(\Gamma)$.

Nach Korollar 3.2.4 ist
$$\Delta(z) = g_2(z)^3 - 27g_3(z)^2 = (2\pi)^{12}\sum_{n=1}^{\infty}\tau(n)\mathrm{e}^{2\pi i n z}$$
ebenfalls in $M_6^0(\Gamma)$, und $\tau(1) = 1$. Nach Satz 4.3.8 ist $\dim(M_6^0(\Gamma)) = 1$. Folglich gibt es $\lambda \in \mathbf{C}$ so dass
$$\Delta = \lambda\eta^{24}$$
Vergleich der ersten nichttrivialen Fourierkoeffizienten von Δ und η^{24} zeigt, dass $\lambda = (2\pi)^{12}$. Also gilt der Satz

Satz 5.1.4 *Es ist*
$$\Delta = (2\pi)^{12}\eta^{24}$$

Übung 5.1.5 Sei $F(\tau) := \eta(11\tau)\eta(\tau)$. Beweisen Sie

i)

$$F(\tau + 1) = -F(\tau)$$

und

$$F(\tau) = \frac{i}{\sqrt{11\tau}} F\left(\frac{-1}{11\tau}\right)$$

ii) Bestimmen Sie die ersten hundert Fourierkoeffizienten von F und F^2 (Computer!)

5.2 Partitionen

Dieser Abschnitt ist sehr kurz und soll nur das Anliegen haben, den Zusammenhang zwischen den Partitionen und der Etafunktion aufzuzeigen, aus dem man das asymptotische Verhalten der Anzahl der Partitionen ableiten kann. Die Resultate dieser asymptotischen Entwicklung werden ohne Beweis angegeben.

Definition 5.2.1 *Sei n eine natürliche Zahl. Eine Partition von n ist eine Folge natürlicher Zahlen $n_1, n_2, \ldots, n_k$, sodass*

$$n = n_1 + n_2 + \cdots + n_l$$

gilt. Zwei Partitionen sollen gleich sein, wenn sie sich nur um Permutationen unterscheiden. Die Anzahl möglicher Arten, n als Summe natürlicher Zahlen zu schreiben, bezeichnet man mit $p(n)$ =Anzahl Partitionen von n.

Übung 5.2.2 *Beweisen Sie die folgende Formel von Euler:*

$$\sum_{m=0}^{\infty} p(m)x^m = \prod_{n=1}^{\infty}(1 - x^n)^{-1},\ |x| < 1$$

Aus der Formel von Euler folgt

$$p(m) = \frac{1}{2\pi i}\int_C \prod_{n=1}^{\infty} \frac{1}{1 - x^n}\frac{dx}{x^{m+1}}$$

wo C ein Kreis mit Radius $R < 1$ um den Ursprung ist. Setzt man $x = \mathrm{e}^{2\pi i z}$ so ist also

$$p(m) = \int_\gamma \prod_{n=1}^{\infty} \frac{1}{1 - \mathrm{e}^{2\pi i n z}}\mathrm{e}^{-2\pi i m z}dz = \int_\gamma \frac{1}{\eta(z)}\mathrm{e}^{2\pi i(\frac{1}{24} - m)z}dz$$

wo γ die Strecke $[-\frac{1}{2} + iM, \frac{1}{2} + iM]$ mit genügend grossem M ist. Mittels diesem Zusammenhang kann man asymptotische Aussagen über $p(m)$ beweisen. Beispielsweise findet man in [Knopp], chapter 6, die folgende Formel bewiesen

$$p(m) = \frac{1}{4\sqrt{3}}\frac{1}{m - \frac{1}{24}}\mathrm{e}^{\pi\nu\sqrt{m - \frac{1}{24}}}\left(1 - \frac{1}{\pi\nu\sqrt{m - \frac{1}{24}}}\right) + o(\mathrm{e}^{\pi\frac{\nu}{2}\sqrt{m - \frac{1}{24}}})$$

wo $\nu = \sqrt{\frac{2}{3}}$ ist. Eine noch bessere Abschätzung, die auf Rademacher zurückgeht, findet man z.B. in [Apostol], chapter 5. Die elementare Formel

$$p(m) < \mathrm{e}^{\pi\nu\sqrt{m}}$$

wurde bereits 1916 von Hardy und Ramanujan bewiesen.

Kapitel 6

Hecke-Operatoren

Betrachten wir einige Fourierkoeffizienten $\tau(n)$ der Diskriminante (vgl. Korollar 3.2.4)

$$\begin{aligned}\Delta(z) &= g_2(z)^3 - 27g_3(z)^2 \\ &= (2\pi)^{12}\eta(\tau)^{24} \\ &= (2\pi)^{12}\sum_{n=1}^{\infty}\tau(n)\mathrm{e}^{2\pi inz}\end{aligned}$$

Einige Werte von τ werden hier angegeben:

n	1	2	3	4	5	6	7	8	9	10
$\tau(n)$	1	-24	252	-1472	4830	$-6\,048$	$-16\,744$	$84\,480$	$-113\,643$	$-115\,920$

Man erkennt zum Beispiel, dass

$$\tau(2)\tau(3) = \tau(6),\ \tau(2)\tau(5) = \tau(10)$$

woraus die Vermutung ensteht, dass τ multiplikativ ist. Tatsächlich stellte Ramanujan folgende Vermutungen auf:

(a)
$$\tau(mn) = \tau(m)\tau(n) \ \text{ für } m, n \text{ teilerfremd}$$

(b) Weiter vermutete Ramanujan folgende Abschätzung.
$$|\tau(n)| \leq n^{\frac{11}{2}}\sum_{d|n} d \qquad \forall\, n \in \mathbb{N}$$

.

Beides wurde bewiesen, nämlich 1917 bewies Mordell (a) (was wir auch tun werden, allerdings mit anderen Methoden), und der Beweis von (b) wurde 1974 von Deligne geliefert. Ein helles Licht über diese Sachverhalte werfen die Hecke-Operatoren.

6.1 Korrespondenzen

Notation 6.1.1 *Ist G eine Gruppe und U eine Untergruppe von G, dann soll im Folgenden $[G : U] = |G/U|$ den Index von U in G bezeichnen.*

Definition 6.1.2 *Sei E eine Menge und X_E die freie abelsche Gruppe über E. Eine Korrespondenz auf E (mit ganzzahligen Koeffizienten) ist ein Gruppenhomomorphismus $T : X_E \longrightarrow X_E$. Wenn es aus dem Zusammenhang klar ist, was die Menge E ist, so schreibt man X anstatt X_E.*

Bemerkung 6.1.3 Eine Korrespondenz ist durch ihrer Werte $T(x)$, $x \in E$ gegeben.

Definition 6.1.4 *Ist $F : E \longrightarrow \mathbb{C}$ eine Funktion, so definiert man*

$$\begin{aligned} TF : X &\longrightarrow \mathbb{C} \\ x &\longrightarrow \sum_{y \in E} n_y(x) F(y) \end{aligned}$$

wo $T(x) = \sum_{y \in E} n_y(x) y$.

Beispiel 6.1.5 *Das für uns wichtige Beispiel ist die Hecke-Korrespondenz, welche wie folgt definiert ist: Sei $E := \mathcal{L}$ die Menge der Gitter von $\mathbb{C}$, dann ist für $n \in \mathbb{N}$ die Hecke-Korrespondenz $T(n)$ auf X_E festgelegt durch:*

$$T(n)L = \sum_{\substack{L' \subset L \\ [L:L'] = n}} L'$$

Zusätzlich definiert man zu $\lambda \in \mathbb{C}^*$

$$R_\lambda L = \lambda L$$

Satz 6.1.6 *Man hat folgende Identitäten:*

(i)

$$R_\lambda R_\mu = R_{\lambda\mu}$$

(ii)

$$R_\lambda T(n) = T(n) R_\lambda$$

(iii)

$$T(mn) = T(m)T(n) \quad \textit{falls } m \textit{ und } n \textit{ teilerfremd}$$

(iv)

$$T(p^{n+1}) + pT(p^{n-1}) R_p = T(p^n) T(p) \quad \textit{für } p \textit{ prim}$$

(v)

$$T(m)T(n) = T(n)T(m) \quad \textit{für alle} \quad m, n \geq 0$$

Beweis. (i) und (ii) sind offensichtlich. Um (iii) zu zeigen braucht man bloss zu zeigen, dass für jedes $L'' \subset L$ vom Index mn genau ein $L' \subset L$ vom Index n existiert, sodass $L'' \subset L' \subset L$, denn dann ist

$$\begin{aligned} T(mn)L &= \sum_{\substack{L'' \subset L \\ [L:L''] = mn}} L'' = \sum_{\substack{L'' \subset L' \subset L \\ [L:L'] = n \\ [L':L''] = m}} L'' \\ &= \sum_{\substack{L' \subset L \\ [L:L'] = n}} \sum_{\substack{L'' \subset L' \\ [L':L''] = m}} L'' = \sum_{\substack{L' \subset L \\ [L:L'] = n}} T(m) L' \\ &= T(m) \sum_{\substack{L' \subset L \\ [L:L'] = n}} L' = T(m)T(n)L \end{aligned}$$

Sei $\pi : L \longrightarrow L/L''$ die Quotientenabbildung. Da L/L'' abelsch von der Ordnung mn ist, gilt nach dem Hauptsatz über endlich erzeugte abelsche Gruppen

$$L/L'' \simeq G_m \times G_n \tag{6.1}$$

wo G_m, G_n abelsche Gruppen der Ordnung m und n sind. Sei nun $L'' \subset L' \subset L$ mit $[L : L'] = n$. Es ist $\pi(L') = L'/L''$. Da aber $(L/L'')/(L'/L'') \simeq L/L'$ ist, gilt $nm = [L/L''] = [L : L'][L' : L''] = n[L' : L'']$ und somit $|L'/L''| = m$. Nennen wir den Isomorphismus von (6.1) ϕ und setzen wir $G' := \phi(\pi(L')) \subset G_m \times G_n$, so ist die Projektion $p_2(G')$ auf die zweite Komponente G_n eine Untergruppe von G_n, teilt also deren Gruppenordnung, welche n ist. Anderseits teilt aber die Gruppenordnung von $p_2(G')$ auch die Gruppenordnung von G', welche m ist. Da m, n teilerfremd sind, kann also die Gruppenordnung von $p_2(G')$ nur 1 sein. Daraus folgt, dass $G' = G_m \times \{e\}$ ist. Also ist

$$L' = \pi^{-1}(\phi^{-1}(G_m \times \{e\}))$$

Umgekehrt erfüllt $L' := \pi^{-1}(\phi^{-1}(G_m \times \{e\}))$ die Bedingung $L'' \subset L' \subset L$ und $[L : L'] = n$. Also gibt es genau eine Gruppe L' mit den verlangten Eigenschaften.
Für den Beweis von (iv) und (v) verweisen wir auf [Serre] VII, §5. □

Korollar 6.1.7 *(i) Ist p eine Primzahl, so ist $T(p^n)$ ein Polynom in $T(p)$ und R_p mit ganzzahligen Koeffizienten.*

(ii) Die Algebra, welche von den $T(p)$ und R_p, p prim, erzeugt wird, ist kommutativ und enthält alle $T(n)$.

Beweis. Übung.

Korollar 6.1.8 *Sei $k \in \mathbb{N}_0$ und $F : \mathcal{L} \longrightarrow \mathbb{C}$ eine Funktion mit $R_\lambda F = \frac{1}{\lambda^{2k}} F$. Dann ist*

$$\begin{aligned} T(m)T(n)F &= T(n)T(m)F, \text{ falls } n, m \text{ teilerfremd} \\ T(p)T(p^n)F &= T(p^{n+1})F + \frac{1}{p^{2k-1}} T(p^{n-1})F \end{aligned}$$

Beweis. Übung.

Bemerkung 6.1.9 *(i) Sei f eine schwach modulare Funktion vom Gewicht $2k$. Ist L ein Gitter in $\mathbb{C}$ und sind $\{\omega_1, \omega_2\}$ und $\{\omega_1', \omega_2'\}$ orientierte Basen von L, so ist*

$$\frac{1}{\omega_1^{2k}} f\big(\frac{\omega_2}{\omega_1}\big) = \frac{1}{\omega_1'^{\,2k}} f\big(\frac{\omega_2'}{\omega_1'}\big)$$

Deswegen kann man zu f eine Funktion $F : \mathcal{L} \longrightarrow \mathbb{C}$ mit

$$F\big(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2\big) = \frac{1}{\omega_1^{2k}} f\big(\frac{\omega_2}{\omega_1}\big)$$

assoziieren. Offenbar gilt

$$\begin{aligned} R_\lambda F &= \frac{1}{\lambda^{2k}} F \\ f(\tau) &= F(L_\tau) \quad \text{wobei } L_\tau = \mathbb{Z} + \mathbb{Z}\tau \end{aligned}$$

(ii) Ist umgekehrt $F : \mathcal{L} \longrightarrow \mathbb{C}$ eine Funktion mit $R_\lambda F = \frac{1}{\lambda^{2k}} F$, so gilt für die durch $f(\tau) = F(L_\tau)$ definierte Funktion f auf der oberen Halbebene, dass

$$f(\tau) = \frac{1}{(c\tau + d)^{2k}} f\big(\frac{a\tau + b}{c\tau + d}\big) \quad \forall A \in SL(2, \mathbb{Z})$$

Beweis. (i) Nach Satz 1.1.8 existiert eine Matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z})$, so dass

$$\begin{aligned} \omega_2' &= a\omega_2 + b\omega_1 \\ \omega_1' &= c\omega_2 + d\omega_1 \end{aligned}$$

Dann ist

$$\begin{aligned} \frac{1}{{\omega_1'}^{2k}} f\big(\frac{\omega_2'}{\omega_1'}\big) &= \frac{1}{(c\omega_2 + d\omega_1)^{2k}} f\big(\frac{a\omega_2 + b\omega_1}{c\omega_2 + d\omega_1}\big) \\ &= \frac{1}{\omega_1^{2k}} \frac{1}{(c\frac{\omega_2}{\omega_1} + d)^{2k}} f\big(\frac{a\frac{\omega_2}{\omega_1} + b}{c\frac{\omega_2}{\omega_1} + d}\big) = \frac{1}{\omega_1^{2k}} f\big(\frac{\omega_2}{\omega_1}\big) \end{aligned}$$

(ii) ist analog. □

Definition 6.1.10 *Ist f eine schwach modulare Funktion vom Gewicht $2k$ und $n \in \mathbb{N}$, so sei*

$$\big(T(n)f\big)(\tau) := T(n)F\,(L_\tau)$$

wobei F die zu f wie in Bemerkung 6.1.9 assoziierte Funktion $F : \mathcal{L} \longrightarrow \mathbb{C}$ ist.

Satz 6.1.11 *Seien $n, k \in \mathbb{N}$ und f eine schwach modulare Funktion vom Gewicht $2k$. Dann ist $T(n)f$ ebenfalls schwach modular vom Gewicht $2k$. Es gilt*

$$T(n)f(\tau) = \sum_{\substack{a \geq 1, ad = n \\ 0 \leq b < d}} \frac{1}{d^{2k}} f\left(\frac{a\tau + b}{d}\right)$$

Ferner gilt

$$f \text{ modular vom Gewicht } 2k \Longrightarrow T(n)f \text{ ist modular vom Gewicht } 2k$$

$$f \text{ Spitzenform vom Gewicht } 2k \Longrightarrow T(n)f \text{ ist Spitzenform vom Gewicht } 2k$$

Der Beweis kommt im folgenden Abschnitt.

6.2 Hecke-Operatoren

Es gelten dieselben Bezeichnungen wie im letzten Abschnitt. Wir fixieren eine natürliche Zahl k und betrachten nur schwach modulare Funktionen vom Gewicht $2k$.

Definition 6.2.1 *Die Operatoren*

$$T_n := n^{2k-1} T(n)$$

heissen Hecke-Operatoren.

Bemerkung 6.2.2 Der Faktor n^{2k-1} hat den Vorteil, dass spätere Formeln nennerfrei werden.

Lemma 6.2.3 *Sei $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ ein Gitter in $\mathbb{C}$, $n \in \mathbb{N}$ und A eine ganzzahlige Matrix der Form*

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

mit $ad = n$, $a \geq 1$, $0 \leq b < d$. Sei weiter $L(A)$ das Gitter, das von den Vektoren $\omega_1' = a\omega_1 + b\omega_2$ und $\omega_2' = d\omega_2$ aufgespannt wird. Dann ist $L(A) \subset L$ und hat den Index n in L. Jedes Gitter L' vom Index n in L kann in eindeutiger Weise als $L' = L(A)$ mit einer Matrix A der obigen Art geschrieben werden.

Beweis. Für $b = 0$ ist offenbar $[L : L(A)] = ad = n$. Ist $b > 0$ und $\Lambda := \mathbb{Z}ad\omega_1 + \mathbb{Z}bd\omega_2 = \mathbb{Z}d(a\omega_1 + b\omega_2) + \mathbb{Z}bd\omega_2 \subset \mathbb{Z}(a\omega_1 + b\omega_2) + \mathbb{Z}d\omega_2 = L(A) \subset L$, dann ist $[L : L(A)] = \frac{[L:\Lambda]}{[L(A):\Lambda]} = \frac{ad^2b}{bd} = ad = n$.
Sei nun $L' = \mathbb{Z}\omega_1'' + \mathbb{Z}\omega_2'' \subset L$ ein Untergitter vom Index n in L mit $\omega_1'' = e\omega_1 + f\omega_2$, $\omega_2'' = g\omega_1 + h\omega_2$. Dann ist $g\omega_1'' - e\omega_2'' = (gf - eh)\omega_2 \in L' \cap \mathbb{Z}\omega_2$. Es gibt dann einen primitiven Gittervektor von L' der Form $d\omega_2$ mit $d \in \mathbb{N}$ (wähle für d einfach das Minimum der Menge $\{|k| : k\omega_2 \in L'\}$. Es gibt offenbar kein anderes $d > 0$, sodass $d\omega_2$ primitiv in L' ist. Nach Lemma 1.1.7 kann man diesen primitiven Gittervektor zu einer Basis $\{\omega', d\omega_2\}$ von L' ergänzen. ω' ist natürlich eine Linearkombination $\omega' = a\omega_1 + b'\omega_2$ von ω_1 und ω_1. Also ist

$$\{a\omega_1 + b'\omega_2, d\omega_2\} \tag{6.2}$$

eine Basis von L'. Nun erhält man jede Basis von L' der Form (6.2) mit festem a und festem d (nur noch b' variabel) durch Addition eines ganzzahligen Vielfachen des zweiten Basisvektors zum ersten Basisvektor. Das sind also alle Basen der Form

$$\{a\omega_1 + (b' + qd)\omega_2,\ d\omega_2\},\ q \in \mathbb{Z} \tag{6.3}$$

Die einzig mögliche Basis der Form (6.3), bei der $0 \leq b := b' + qd < d$ gilt, wird erreicht genau für ein $q \in \mathbb{Z}$. Weil $[L : L'] = n$ ist, muss nach dem ersten Teil des Satzes $ad = n$ sein. Also gibt es genau eine Matrix A

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

mit $ad = n$, $0 \leq b < d$, sodass $L' = L(A)$ ist. □

Wir beginnen nun mit dem Beweis von Satz 6.1.11. Sei $f : H \longrightarrow \mathbb{C}$ schwach modular vom Gewicht $2k$ bezüglich Γ. Nach Definition ist

$$T(n)f(\tau) = F(T(n)(\mathbb{Z} + \mathbb{Z}\tau))$$

Mit Lemma 6.2.3 ist also

$$\begin{aligned} T(n)f(\tau) &= \sum_{\substack{a\geq 1, ad=n \\ 0\leq b<d}} F(\mathbb{Z}d + \mathbb{Z}(a\tau + b)) \\ &= \sum_{\substack{a\geq 1, ad=n \\ 0\leq b<d}} \frac{1}{d^{2k}} f(\frac{a\tau + b}{d}) \end{aligned} \tag{6.4}$$

Dies zeigt, dass $T(n)f$ meromorph ist. Dass $T(n)f$ das richtige Transformationsverhalten bezüglich $SL(2,\mathbb{Z})$ hat, haben wir bereits in Teil (ii) von Bemerkung 6.1.9 verifiziert. Damit ist der erste Teil von Satz 6.1.11 bewiesen. Ebenso sieht man, dass $T(n)f$ holomorph ist, falls f holomorph ist. Für die weiteren Teile von Satz 6.1.11 verwenden wir

Lemma 6.2.4 *Ist f schwach modular vom Gewicht $2k$ und besitzt f die Fourierentwicklung*

$$f(\tau) = \sum_{m\in\mathbb{Z}} c(m)\, e^{2\pi i m\tau}$$

so ist

$$(T_n f)(\tau) = \sum_{m\in\mathbb{Z}} \gamma(m)\, e^{2\pi i m\tau}$$

wo

$$\gamma(m) = \sum_{\substack{a|ggT(m,n)\\ a\geq 1}} a^{2k-1} c(\frac{mn}{a^2})$$

Beweis. Nach (6.4) ist

$$T(n)f(\tau) = \sum_{\substack{a\geq 1, ad=n\\ 0\leq b<d}} \frac{1}{d^{2k}} f(\frac{a\tau+b}{d})$$

Setzt man die Fourierentwicklung von f ein, so wird daraus

$$T(n)f(\tau) = \sum_{\substack{a\geq 1, ad=n\\ 0\leq b<d}} \frac{1}{d^{2k}} \left(\sum_{m\in\mathbb{Z}} c(m) \mathrm{e}^{2\pi i m \frac{a\tau+b}{d}} \right) \tag{6.5}$$

Nun ist

$$\mathrm{e}^{2\pi i m \frac{a\tau+b}{d}} = \mathrm{e}^{2\pi i b \frac{m}{d}} \mathrm{e}^{2\pi i m \frac{a\tau}{d}}$$

und

$$\sum_{b=0}^{d-1} \mathrm{e}^{2\pi i b \frac{m}{d}} = \begin{cases} d \text{ falls } d|m \\ 0 \text{ sonst} \end{cases} \tag{6.6}$$

Setzt man $m = m'd$, so ist wegen (6.5) und (6.6)

$$T(n)f(\tau) = \sum_{a\geq 1, ad=n} \frac{1}{d^{2k-1}} \left(\sum_{m'\in\mathbb{Z}} c(dm') \mathrm{e}^{2\pi i a m' \tau} \right) \tag{6.7}$$

Setzt man $l = am'$, so folgt mit (6.7), dass

$$T(n)f(\tau) = \sum_{l\in\mathbb{Z}} \sum_{\substack{a|\mathrm{ggT}(l,n)\\ a\geq 1}} \left(\frac{a}{n}\right)^{2k-1} c(\frac{ln}{a^2}) \mathrm{e}^{2\pi i l\tau}$$

was genau die Aussage des Lemmas ist. □

Der Beweis der verbliebenen Teile von Satz 6.1.11 ist nun einfach.
Ist $f(\tau) = \sum_{m\in\mathbb{Z}} c(m) \mathrm{e}^{2\pi i m\tau}$ modular, dann ist nach Definition 4.3.1 $c(m) = 0$ für alle

negativen m. Wegen Lemma 6.2.4 muss dann aber auch $\gamma(m) = 0$ für alle negativen m sein, woraus die Beschränktheitsbedingung auch für $T(n)f$ erfüllt ist. Wir haben aber bereits gezeigt, dass $T(n)$ schwach modular ist, falls f schwach modular ist, also ist $T(n)$ modular.
Ist f eine Spitzenform, so ist $c(m) = 0$ für alle $m \leq 0$. Wie oben folgert man mittels Lemma 6.2.4, dass dann auch $T(n)f$ eine Spitzenform ist. □

Korollar 6.2.5 *Sei $f \in M_k(\Gamma)$, $n \in \mathbb{N}$,*

$$f = \sum_{m=0}^{\infty} c(m) e^{2\pi i m z}$$

die Fourierdarstellung von f und

$$T_n f(z) = \sum_{m=0}^{\infty} \gamma(m) e^{2\pi i m z}$$

die Fourierdarstellung von $T_n f$. Dann gelten folgende Aussagen:

$$\begin{aligned} \gamma(0) &= c(0) \left(\sum_{d|n} d^{2k-1} \right) \\ \gamma(1) &= c(n) \end{aligned}$$

Ist $n = p$ eine Primzahl, so ist

$$\gamma(m) = \begin{cases} c(pm) \text{ falls } m \not\equiv 0 \mod p \\ c(pm) + p^{2k-1} c(\frac{m}{p}) \text{ falls } m \equiv 0 \mod p \end{cases}$$

Beweis. Folgt sofort aus Lemma 6.2.4. □

Korollar 6.2.6 *$\Delta = g_2^3 - 27 g_3^2$ ist eine Eigenfunktion jedes Hecke-Operators T_n.*

Beweis. Der Raum der Spitzenformen vom Gewicht 12 ist eindimensional und wird wegen Satz 6.1.11 auf sich abgebildet. □

Satz 6.2.7 *Für die Hecke-Operatoren auf $M_k(\Gamma)$ gelten die folgenden Rechenregeln.*

$$T_n T_m = T_{nm} \text{ falls } n, m \text{ teilerfremd sind}$$

$$T_p T_{p^n} = T_{p^{n+1}} + p^{2k-1} T_{p^{n-1}}$$

Beweis. Die Aussagen folgen unmittelbar aus den Regeln 6.1.6 für $T(n) = \frac{1}{n^{2k-1}} T_n$. □

Satz 6.2.8 *Sei $f \in M_k(\Gamma)$ eine Eigenfunktion aller Hecke-Operatoren, d.h.*

$$T_n f = \lambda_n f, \quad \forall n \in \mathbb{N}$$

und sei $f = \sum_{m=0}^{\infty} c(m) e^{2\pi i m z}$ *die Fourierdarstellung von* f*. Dann ist*

$$\begin{aligned} c(1) &\neq 0 \\ c(n) &= \lambda_n c(1),\ \forall n > 1 \end{aligned}$$

Normiert man $c(1) = 1$ *so gilt weiter:*

$$\begin{aligned} c(n)c(m) &= c(nm) \text{ falls } n, m \text{ teilerfremd} \\ c(p)c(p^n) &= c(p^{n+1}) + p^{2k-1} c(p^{n-1}) \text{ für jede Primzahl } p \end{aligned}$$

Beweis. Sei

$$T_n f(z) = \sum_{m=0}^{\infty} \gamma_n(m) \mathrm{e}^{2\pi i m z}$$

Dann ist $\gamma_n(1) = \lambda_n c(1)$ und nach Korollar 6.2.5 ist $\gamma_n(1) = c(n)$ also ist

$$c(n) = \lambda_n c(1) \quad \forall n \in \mathbb{N}$$

Wäre $c(1) = 0$, so $f \equiv 0$ im Widerspruch dazu, dass f eine Eigenfunktion ist.
Aus den Rechenregeln für T_n in Satz 6.2.7 folgt sofort, dass

$$\begin{aligned} \lambda_n \lambda_m &= \lambda_{nm} \text{ falls } n, m \text{ teilerfremd} \\ \lambda_p \lambda_{p^n} &= \lambda_{p^{n+1}} + p^{2k-1} \lambda_{p^{n-1}} \text{ für jede Primzahl } p \end{aligned}$$

□

Nach Korollar 6.2.6 ist Δ eine Eigenfunktion jedes Hecke–Operators. Satz 6.2.8 ergibt nun sofort die am Anfang des Kapitels gemachten Behauptung über die Ramanujan-Funktion $\tau(n)$.

Korollar 6.2.9 *Die aus der Fourierentwicklung*

$$\Delta(z) = (2\pi)^{12} \sum_{n \in \mathbb{Z}} \tau(n) e^{2\pi i n z}$$

definierte Ramanujan-Funktion $n \mapsto \tau(n)$ *ist multiplikativ, d.h. es gilt*

$$\tau(m)\tau(n) = \tau(mn) \text{ falls } m, n \text{ teilerfremd}$$

und erfüllt darüber hinaus für jede Primzahl p *und jedes* $n \in \mathbb{N}$

$$\tau(p)\tau(p^n) = \tau(p^{n+1}) + p^{11} \tau(p^{n-1})$$

Bemerkung 6.2.10 Man kann zeigen, dass auch die Eisensteinreihen Eigenfunktionen aller Hecke-Operatoren sind. Ausserdem kann man zeigen, dass $M_k(\Gamma)$ eine Basis aus simultanen Eigenfunktionen (für alle Hecke-Operatoren) besitzt. Der Grund dafür ist, dass die Hecke-Operatoren selbstadjungiert bezüglich des Petersson Skalarprodukts

$$\langle f, g \rangle := \int_H f(x+iy) \overline{g(x+iy)} y^{2k} \frac{dxdy}{y^2}$$

sind. Siehe [Serre] VII, §5.6.1.

Kapitel 7

Die Modulkurve zu $\Gamma_0(11)$

7.1 Modulformen für $\Gamma_0(11)$

Satz 7.1.1 *Sei H die kleinste Untergruppe von $\Gamma_0(11)$, welche die Matrizen*

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 1 \\ 11 & 4 \end{pmatrix}, \begin{pmatrix} 4 & 1 \\ 11 & 3 \end{pmatrix}$$

enthält und unter Konjugation mit

$$J = \begin{pmatrix} 0 & -\frac{1}{\sqrt{11}} \\ \sqrt{11} & 0 \end{pmatrix}$$

invariant ist. Dann ist

$$H = \Gamma_0(11)$$

Dem Beweis schicken wir zwei Lemmata voraus.

Lemma 7.1.2 *Sei $p > 2$ eine Primzahl. Dann bilden die Matrizen*

$$-I,\ T,\ \left\{\begin{pmatrix} \alpha & \beta \\ p & \delta \end{pmatrix} : \alpha\delta - \beta p = 1\right\}$$

ein Erzeugendensystem für $\Gamma_0(p)$.

Beweis. Sei Γ' die von obigen Elementen erzeugte Untergruppe von $\Gamma_0(p)$. Wir zeigen, dass jedes Element

$$A = \begin{pmatrix} a & b \\ cp & d \end{pmatrix}$$

von $\Gamma_0(p)$ in Γ' liegt. Der Beweis geschieht durch Induktion nach $|c|$. Für $|c| = 0$ ist $ad = 1$, also $a = d = \pm 1$ und somit

$$A = \pm T^{\pm b}$$

Sei nun $|c| > 0$. Für beliebige α, β, δ gilt

$$\begin{pmatrix} \alpha & \beta \\ p & \delta \end{pmatrix} \begin{pmatrix} a & b \\ cp & d \end{pmatrix} = \begin{pmatrix} * & * \\ p(a + \delta c) & * \end{pmatrix} \tag{7.1}$$

Da a und c teilerfremd sind, gibt es ein $k \in \mathbb{Z}$, sodass

$$kc < a < (k+1)c$$

Da $p > 2$ ist, teilt p höchstens eine der Zahlen k, $k+1$. Man setzt:

$$\delta = \begin{cases} -k & \text{falls } p \text{ die Zahl } k \text{ nicht teilt.} \\ -(k+1) & \text{falls } p|k \end{cases}$$

Man hat offenbar

$$|a + \delta c| < |c| \tag{7.2}$$

Da $ggT(p, \delta) = 1$ ist, gibt es ganze Zahlen α und β sodass die Matrix

$$B = \begin{pmatrix} \alpha & \beta \\ p & \delta \end{pmatrix}$$

Determinante 1 hat. Die Gleichungen (7.1) und (7.2) zeigen nun aber, dass der Betrag des linken unteren Eintrag von BA echt kleiner ist als $|c|$, womit der Induktionsschritt fertig ist. $\square$

Lemma 7.1.3 *Sei $p > 2$ eine Primzahl. Wähle für jedes $0 < n < p$ eine Matrix*

$$B(n) = \begin{pmatrix} \alpha(n) & \beta(n) \\ p & \delta(n) \end{pmatrix}$$

aus $\Gamma_0(p)$, sodass $\delta(n) \equiv n \mod p$ ist. Dann ist

$$\{-I, T\} \cup \{B(n) : 0 < n < p\}$$

ein Erzeugendensystem für $\Gamma_0(p)$.

Beweis. Sei Γ' die von obigen Matrizen erzeugte Untergruppe von $\Gamma_0(p)$. Wegen Lemma 7.1.2 genügt es zu zeigen, dass alle Matrizen der Form

$$\begin{pmatrix} a & b \\ p & d \end{pmatrix}$$

mit $ad - bp = 1$ in Γ' liegen. Sei $0 < n < p$ sodass $d \equiv n \mod p$ ist. Dann gibt es ganze Zahlen x und y sodass

$$\alpha(n) + px = a, \quad \delta(n) + py = d$$

Somit ist

$$T^x B(n) T^y = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha(n) & \beta(n) \\ p & \delta(n) \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & * \\ p & d \end{pmatrix}$$

Es folgt wegen $ad - bp = 1$, dass $* = b$ sein muss (beachte, dass die Determinante von $T^x B(n) T^y$ immer noch 1 sein muss). $\square$

Wir beweisen nun **Satz 7.1.1**. Wegen Lemma 7.1.3 braucht man nur noch zu zeigen, dass für jedes $0 < n < 11$ eine Matrix $B(n)$ der Form $\begin{pmatrix} \alpha & \beta \\ p & \delta \end{pmatrix}$ mit $\delta \equiv n \mod 11$ in H liegt. Weil H invariant ist unter Konjugation mit J, sind für alle $A \in H$ die Elemente der

Form $J^{-1}AJ$ wieder in H. Wir werden nun zeigen, dass man die gewünschten Matrizen $B(n)$ mittels Konjugation mit J und der Gruppeneigenschaft von H aus den Matrizen

$$-I, T, X = \begin{pmatrix} 3 & 1 \\ 11 & 4 \end{pmatrix}, Y = \begin{pmatrix} 4 & 1 \\ 11 & 3 \end{pmatrix}$$

gewinnen kann, womit dann der Satz bewiesen wäre. Man rechnet einfach nach, dass

$$J^{-1} \begin{pmatrix} a & b \\ 11c & d \end{pmatrix} J = - \begin{pmatrix} -d & c \\ 11b & -a \end{pmatrix} \tag{7.3}$$

Mit der allgemeinen Formel (7.3) rechnet man folgende Liste von Matrizen aus:

$$B(1) = \begin{pmatrix} 1 & 0 \\ 11 & 1 \end{pmatrix} = J^{-1}T^{-1}J, \;\; B(10) = \begin{pmatrix} -1 & 0 \\ 11 & -1 \end{pmatrix} = -J^{-1}TJ$$

$$B(4) = X, \;\; B(3) = Y, \;\; B(8) = \begin{pmatrix} -4 & 1 \\ 11 & -3 \end{pmatrix} = -J^{-1}XJ$$

$$B(7) = \begin{pmatrix} -3 & 1 \\ 11 & -4 \end{pmatrix} = -J^{-1}YJ, \;\; B(5) = \begin{pmatrix} -2 & -1 \\ 11 & 5 \end{pmatrix} = -B(7)B(4)$$

$$B(9) = \begin{pmatrix} 5 & -1 \\ 11 & -2 \end{pmatrix} = J^{-1}B(5)J, \;\; B(6) = \begin{pmatrix} 2 & -1 \\ 11 & -5 \end{pmatrix} = B(4)B(7)$$

$$B(2) = \begin{pmatrix} -5 & -1 \\ 11 & 2 \end{pmatrix} = -B(5)^{-1}$$

□

Satz 7.1.4 *Setzt man*

$$F(\tau) = \eta(\tau)\eta(11\tau)$$

so ist $\gamma(\tau) := F^2(\tau)$ eine Spitzenform für $\Gamma_0(11)$ vom Gewicht 2.

Beweis. Die Holomorphie von F^2 ist klar. Wir beweisen zunächst, dass F^2 schwach modular bezüglich $\Gamma_0(11)$ ist. Dazu betrachten wir die Untergruppe

$$G := \left\{ A \in \Gamma_0(11) : F^2(\tau) = \frac{1}{(c\tau + d)^2} F^2(\varphi_A(\tau)) \quad \forall \tau \in H \right\}$$

wobei wir wieder A als

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

geschrieben haben. Wir zeigen, dass $\Gamma_0(11) \subset G$ ist. Aus der zweiten Funktionalgleichung der Etafunktion (Satz 5.1.2) folgt, dass

$$F(\tau) = \frac{i}{\sqrt{11}\tau} F(-\frac{1}{11\tau}) \tag{7.4}$$

Deshalb ist G invariant unter Konjugation mit

$$J = \begin{pmatrix} 0 & -\frac{1}{\sqrt{11}} \\ \sqrt{11} & 0 \end{pmatrix}$$

Um zu zeigen, dass $\Gamma_0(11) \subset G$ ist, muss nach Satz 7.1.1 nur noch gezeigt werden, dass die Matrizen

$$-I, T, \begin{pmatrix} 3 & 1 \\ 11 & 4 \end{pmatrix}, \begin{pmatrix} 4 & 1 \\ 11 & 3 \end{pmatrix}$$

in G liegen. Für $-I$ ist das klar. Für T folgt das aus der Funktionalgleichung

$$F(\tau + 1) = -F(\tau)$$

welche eine direkte Konsequenz aus der ersten Funktionalgleichung für die Etafunktion (siehe Satz 5.1.2) ist. Sei jetzt

$$A = \begin{pmatrix} 3 & 1 \\ 11 & 4 \end{pmatrix}$$

Nach Bemerkung 2.1.14 ist

$$11\varphi_A(\tau) = 3 - \frac{1}{11\tau + 4}$$

Man rechnet mit Hilfe der Funktionalgleichungen der Etafunktion (Satz 5.1.2) nach, dass

$$\begin{aligned} \eta(11\varphi_A(\tau)) &= \eta\left(3 - \frac{1}{11\tau + 4}\right) \\ &= e^{\frac{3\pi i}{12}} \eta\left(-\frac{1}{11\tau + 4}\right) \\ &= e^{\frac{3\pi i}{12}} \sqrt{-i(11\tau + 4)}\eta(11\tau + 4) \\ &= e^{\frac{7\pi i}{12}} \sqrt{-i(11\tau + 4)}\eta(11\tau) \end{aligned} \tag{7.5}$$

Nach Übung 2.1.15 ist

$$A = ST^{-4}ST^{-3}S$$

Offensichtlich ist

$$\varphi_{T^{-3}}\varphi_S(\tau) = -\frac{1}{\tau} - 3 = -\frac{3\tau + 1}{\tau}$$

und

$$\varphi_{T^{-4}}\varphi_S\varphi_{T^{-3}}\varphi_S(\tau) = \frac{\tau}{3\tau + 1} - 4 = -\frac{11\tau + 4}{3\tau + 1}$$

und man rechnet wieder mit Satz 5.1.2

$$\begin{aligned} \eta(\varphi_A(\tau)) &= \eta(\varphi_S\varphi_{T^{-4}}\varphi_S\varphi_{T^{-3}}\varphi_S(\tau)) \\ &= \sqrt{-i\varphi_{T^{-4}}\varphi_S\varphi_{T^{-3}}\varphi_S(\tau)}\ \eta(\varphi_{T^{-4}}\varphi_S\varphi_{T^{-3}}\varphi_S(\tau)) \\ &= \sqrt{i\frac{11\tau + 4}{3\tau + 1}}\ e^{-\frac{4\pi i}{12}}\ \eta(\varphi_S\varphi_{T^{-3}}\varphi_S(\tau)) \\ &= e^{-\frac{4\pi i}{12}} \sqrt{i\frac{11\tau + 4}{3\tau + 1}} \sqrt{i\frac{3\tau + 1}{\tau}}\ \eta(\varphi_{T^{-3}}\varphi_S(\tau)) \\ &= e^{-\frac{7\pi i}{12}} \sqrt{i\frac{11\tau + 4}{3\tau + 1}} \sqrt{i\frac{3\tau + 1}{\tau}}\ \eta(\varphi_S(\tau)) \\ &= e^{-\frac{7\pi i}{12}} \sqrt{i\frac{11\tau + 4}{3\tau + 1}} \sqrt{i\frac{3\tau + 1}{\tau}}\ \sqrt{-i\tau}\,\eta(\tau) \end{aligned}$$

Mit (7.5) ergibt sich daraus

$$F(\varphi_A(\tau)) = \sqrt{-i(11\tau + 4)}\sqrt{i\frac{11\tau + 4}{3\tau + 1}}\sqrt{i\frac{3\tau + 1}{\tau}}\sqrt{-i\tau}\,F(\tau)$$

und damit

$$F(\varphi_A(\tau))^2 = (11\tau + 4)^2 F(\tau)^2 \tag{7.6}$$

was genau die "schwache Modularität" von F^2 für

$$A = \begin{pmatrix} 3 & 1 \\ 11 & 4 \end{pmatrix}$$

ist. Eine analoge Rechnung zeigt die "schwache Modularität" von F^2 für die Matrix

$$\begin{pmatrix} 4 & 1 \\ 11 & 3 \end{pmatrix}$$

Die Rechtsnebenklassen von $\Gamma_0(11)$ werden nach Übung 4.1.10 von $Id, S, ST, \ldots, ST^{10}$ repräsentiert. Wir haben also zwei Spitzen, nämlich 0 und ∞. Um zu zeigen, dass $\gamma = F^2$ in der Spitze ∞ verschwindet, betrachte man einfach die Definition der *Eta*-Funktion:

$$\eta(\tau) = \mathrm{e}^{\frac{\pi i \tau}{12}} \prod_{n=1}^{\infty} (1 - \mathrm{e}^{2\pi i n \tau})$$

welche für alle τ in H definiert ist. Für $\tau \to \infty$ in H konvergiert obiges Produkt offenbar gegen 0, also verschwindet F^2 in ∞, d.h. $\nu_\infty(F^2) \geq 1$. Daraus folgt aber auch, dass F^2 in der Spitze 0 verschwindet, denn aus (7.4) erhält man durch Transformation der Spitze 0 nach ∞, dass F^2 in der Spitze 0 verschwindet, d.h. $\nu_0(F^2) \geq 1$. □

Bemerkung 7.1.5 Durch Einsetzen von $\tau = i$ in F lässt sich noch der richtige Zweig der Wurzel bestimmen, sodass aus (7.6)

$$F(\tau) = \frac{+1}{11\tau + 4} F\left(\frac{3\tau + 1}{11\tau + 4}\right)$$

folgt. Die richtigen Wurzelzweige für die anderen Elemente von $\Gamma_0(11)$ ergeben sich aus folgendem Korollar.

Korollar 7.1.6 *Es gibt einen Homomorphismus*

$$\varepsilon : \Gamma_0(11) \longrightarrow \{\pm 1\}$$

sodass für alle $\tau \in H$ *und alle* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(11)$ *gilt:*

$$F(\tau) = \frac{\varepsilon(A)}{c\tau + d} F\left(\frac{a\tau + b}{c\tau + d}\right)$$

wobei ε *folgendermassen festgelegt ist:*

$$\varepsilon(-I) = \varepsilon(T) = -1$$

und

$$\varepsilon \begin{pmatrix} 3 & 1 \\ 11 & 4 \end{pmatrix} = \varepsilon \begin{pmatrix} 4 & 1 \\ 11 & 3 \end{pmatrix} = 1$$

und

$$\varepsilon(J^{-1} A J) = -\varepsilon(A)$$

Beweis. Als Übung. $\square$

Wir setzen:

$$G := \vartheta_Q := \sum_{m \in \mathbb{Z}^2} \mathrm{e}^{i\pi\tau\langle m, Qm\rangle}$$

mit

$$Q = \begin{pmatrix} 2 & 1 \\ 1 & 6 \end{pmatrix}$$

Die Anfangsterme der Fourierreihe für G sind

$$G(\tau) = 1 + 2e^{2\pi i\tau} + \quad 4e^{6\pi i\tau} + 2e^{8\pi i\tau} + 4e^{10\pi i\tau} + \cdots$$

Übung 7.1.7

i) Verwenden Sie die Übung 4.2.12, um zu zeigen, dass es einen Homomorphismus

$$\chi : \Gamma_0(11) \longrightarrow \mathbb{C}^*$$

gibt, sodass für alle $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(11)$ gilt:

$$\vartheta_Q(\tau) = \frac{\chi(A)}{c\tau + d} \vartheta_Q(\varphi_A(\tau))$$

wobei

$$\chi(A) = \frac{d}{S(Q, |d|)}$$

ii) Zeigen Sie weiter, dass für $A \in \Gamma_0(11)$ gilt:

$$\chi(A) = \left(\frac{d}{11}\right)$$

wobei

$$\left(\frac{d}{11}\right) := \begin{cases} +1 & \text{falls d ein Quadrat mod 11 ist} \\ -1 & \text{sonst} \end{cases}$$

Bemerkung: Obige Schreibweise heisst Legendresymbol.

iii) Zeigen Sie, dass $\vartheta_Q^2 \in M_1(\Gamma_0(11))$.

Die Formel für die Anzahl Nullstellen aus Übung 4.3.14 besagt, dass G^2 zwei Nullstellen in $H/\Gamma_0(11)$ hat. Da aber G^2 offenbar ein Quadrat ist, folgt, dass G^2 genau eine Nullstelle der Ordnung 2 hat.

Man setzt

$$E(\tau) := \frac{1}{\pi i} \frac{1}{F(\tau)} \big(G(\tau)F'(\tau) - F(\tau)G'(\tau)\big)$$

Die Anfangsterme der Fourierreihe für F sind nach Übung 5.1.5

$$F(\tau) = e^{\pi i\tau} - e^{3\pi i\tau} - e^{5\pi i\tau} + e^{11\pi i\tau} + e^{15\pi i\tau} - e^{23\pi i\tau} + \cdots$$

Folglich sind die Anfangsterme der Fourierreihe für E

$$E(\tau) = 1 - 4e^{2\pi i\tau} - 10e^{4\pi i\tau} - 40e^{6\pi i\tau} - 52e^{8\pi i\tau} - 104e^{10\pi i\tau} + \cdots$$

Satz 7.1.8 *E^2 ist eine Modulform vom Gewicht 6 für $\Gamma_0(11)$. Genauer gilt:*

$$E(\tau) = \chi(A)\frac{1}{(c\tau+d)^3}E\left(\frac{a\tau+b}{c\tau+d}\right) \tag{7.7}$$

für alle $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(11)$, wobei $\chi(A) = \left(\frac{d}{11}\right)$, das Legendresymbol von d und 11 ist (vgl. Übung 7.1.7). Ausserdem ist

$$E(\tau) = \frac{i}{11^{3/2}\,\tau^3}\,E(-\frac{1}{11\,\tau})$$

Beweis. Es sei $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(11)$. Nach Korollar 7.1.6 und Übung 7.1.7 ist

$$F(\tau) = \frac{\varepsilon(A)}{c\tau+d}F(\varphi_A(\tau)) \quad , \qquad G(\tau) = \frac{\chi(A)}{c\tau+d}G(\varphi_A(\tau))$$

Daraus, und weil

$$\varphi_A'(\tau) = \frac{1}{(c\tau+d)^2}$$

(vgl. Bemerkung 2.1.8) folgt

$$\begin{aligned}
F'(\tau) &= -\frac{\varepsilon(A)c}{(c\tau+d)^2}F(\varphi_A(\tau)) + \frac{\varepsilon(A)}{(c\tau+d)^3}F'(\varphi_A(\tau)) \\
G'(\tau) &= -\frac{\chi(A)c}{(c\tau+d)^2}G(\varphi_A(\tau)) + \frac{\chi(A)}{(c\tau+d)^3}G'(\varphi_A(\tau))
\end{aligned}$$

Deshalb ist

$$\begin{aligned}
E(\tau) &= \frac{1}{\pi i}\frac{1}{F(\tau)}[G(\tau)F'(\tau) - F(\tau)G'(\tau)] \\
&= \frac{1}{\pi i}\frac{c\tau+d}{\varepsilon(A)F(\varphi_A(\tau))}\left[\frac{\chi(A)}{c\tau+d}G(\varphi_A(\tau))\left(-\frac{\varepsilon(A)c}{(c\tau+d)^2}F(\varphi_A(\tau)) + \frac{\varepsilon(A)}{(c\tau+d)^3}F'(\varphi_A(\tau))\right)\right. \\
&\qquad \left. - \frac{\varepsilon(A)}{c\tau+d}F(\varphi_A(\tau))\left(-\frac{\chi(A)c}{(c\tau+d)^2}G(\varphi_A(\tau)) + \frac{\chi(A)}{(c\tau+d)^3}G'(\varphi_A(\tau)\right)\right] \\
&= \frac{\chi(A)}{(c\tau+d)^3}E(\varphi_A(\tau))
\end{aligned}$$

Es ist einfach zu sehen, dass E^2 schwach modular vom Gewicht 6 ist. Weil aber F keine Nullstellen in H hat (Übung!), ist E holomorph. Aus der Fourierentwicklung von E ergibt sich direkt die Beschränktheitsbedingung in ∞. Nach Teil (ii) von Übung 4.2.10 ist

$$G(\tau) = \frac{1}{\sqrt{11}\,\tau}\,G(-\frac{1}{11\tau}) \tag{7.8}$$

Daraus und aus (7.4) ergibt sich sofort, dass

$$E(\tau) = \frac{i}{11^{3/2}\,\tau^3}\,E(-\frac{1}{11\,\tau})$$

Somit folgt die Beschränktheitsbedingung für E^2 an der Spitze 0 aus der Beschränktheit an der Spitze ∞. $\square$

Korollar 7.1.9

$$\mathbf{X}(\tau) := \frac{F(\tau)^2}{G(\tau)^2}$$

und

$$\mathbf{Y}(\tau) := \frac{E(\tau)}{G(\tau)^3}$$

sind Modulfunktionen für $\Gamma_0(11)$. *Ihre Fourierreihen haben ganzzahlige Koeffizienten. Die Anfangsterme der Fourierreihen sind*

$$\begin{aligned} \mathbf{X}(\tau) &= e^{2\pi i\tau} - 6e^{4\pi i\tau} + 21e^{6\pi i\tau} - 66e^{8\pi i\tau} + 209e^{10\pi i\tau} + \cdots \\ \mathbf{Y}(\tau) &= 1 - 7e^{2\pi i\tau} + 20e^{4\pi i\tau} - 96e^{6\pi i\tau} + 508e^{8\pi i\tau} + \cdots \end{aligned}$$

Die Funktion $\mathbf{X}(\tau)$ *hat – modulo* $\Gamma_0(11)$ *– eine einzige Polstelle, und diese ist eine Polstelle zweiter Ordnung. Es gilt*

$$\mathbf{X}(\tau) = \mathbf{X}(-\frac{1}{11\tau}) \quad , \qquad \mathbf{Y}(\tau) = -\mathbf{Y}(-\frac{1}{11\tau})$$

Beweis. Aus Satz 7.1.4, Übung 7.1.7 und Satz 7.1.8 folgt, dass $\mathbf{X}(\tau)$ und $\mathbf{Y}(\tau)$ unter der Operation von $\Gamma_0(11)$ invariante meromorphe Funktionen sind. Da G in den Spitzen nicht verschwindet, sind es in der Tat Modulfunktionen. Da G^2 eine doppelte Nullstelle hat, hat $\mathbf{X}(\tau)$ eine doppelte Polstelle. Um die Anfangsterme der Fourierreihe von $\mathbf{X}(\tau)$ auszurechnen, verwendet man, dass nach Übung 5.1.5 und der obigen Beschreibung der Fourierreihe von G

$$\begin{aligned} F(\tau)^2 &= 0 + e^{2\pi i\tau} - 2e^{4\pi i\tau} - e^{6\pi i\tau} + 2e^{8\pi i\tau} + e^{10\pi i\tau} + \cdots \\ G(\tau)^2 &= 1 + 4e^{2\pi i\tau} + 4e^{4\pi i\tau} + 8e^{6\pi i\tau} + 20e^{8\pi i\tau} + 16e^{10\pi i\tau} + \cdots \end{aligned}$$

Da die Fourierreihen von F und G ganzzahlige Koeffizienten haben und der erste Koeffizient von G^2 gleich 1 ist, ergibt die Neumannreihe für $1/G^2$ eine Reihe mit ganzzahligne Koeffizienten. Ähnlich untersucht man die Fourierreihe von $\mathbf{Y}(\tau)$.
Das Transformationsverhalten von $\mathbf{X}(\tau)$ und $\mathbf{Y}(\tau)$ unter der Involution $\varphi_J : \tau \mapsto \frac{-1}{11\tau}$ ergibt sich sofort aus (7.4), (7.8) und Satz 7.1.8. □

Nun kommt das Hauptanliegen dieses Abschnitts:

Satz 7.1.10 *([Klein] V.5, §11) Sei* $\mathcal{N}$ *die Nullstellenmenge der Modulform* G *auf* H *und sei* C *die elliptische Kurve*

$$C := \left\{(x,y) \in \mathbb{C}^2 \,|\, y^2 = -44x^3 + 56x^2 - 20x + 1\right\}$$

Dann ist die Abbildung

$$\begin{aligned} \Phi : (H - \mathcal{N})/\Gamma_0(11) &\longrightarrow C \setminus \{(0, \pm 1)\} \\ \tau &\longrightarrow (\mathbf{X}(\tau), \mathbf{Y}(\tau)) \end{aligned}$$

ein Homöomorphismus. Ist weiter

$$\begin{aligned} j : C &\longrightarrow C \\ (x,y) &\longrightarrow (x,-y) \end{aligned}$$

so ist

$$\Phi(\varphi_J(\tau)) = j(\Phi(\tau))$$

Beweis.

$$f := E^2 - (G^6 - 20G^4F^2 + 56G^2F^4 - 44F^6)$$

ist eine Modulform vom Gewicht 6 für $\Gamma_0(11)$. Aus den Fourierreihen von F und G sieht man, dass f in den Spitzen 0 und ∞ mit Multiplizität ≥ 4 verschwindet. Übung 4.3.14 zeigt dann, dass $f \equiv 0$. Dividieren durch G^6 ergibt, dass für alle $\tau \in H$

$$\mathbf{Y}(\tau)^2 - (1 - 20\mathbf{X}(\tau) + 56\mathbf{X}(\tau)^2 - 44\mathbf{X}(\tau)^3) = 0$$

Dies zeigt, dass die Abbildung Φ wohldefiniert ist. Die Gleichung $\Phi(\varphi_J(\tau)) = j(\Phi(\tau))$ folgt sofort aus Korollar 7.1.9.

Da F und somit $\mathbf{X}$ keine Nullstelle in H hat, ist das Bild von Φ in $C \setminus \{(0, \pm 1)\}$ enthalten. Sei nun $(x, y) \in C$ mit $x \neq 0$. Nach Übung 4.3.14 hat die Funktion $\mathbf{X}(\tau) - x$, mit Multiplizität gezählt, zwei Nullstellen in $H/\Gamma_0(11)$. Sei τ eine solche Nullstelle. Dann ist entweder $\Phi(\tau) = (x, y)$ und $\Phi(\varphi_J(\tau)) = (x, -y)$, oder es ist $\Phi(\tau) = (x, -y)$ und $\Phi(\varphi_J(\tau)) = (x, y)$. Dies zeigt, dass Φ die Menge $(H \setminus \mathcal{N})/\Gamma_0(11) \setminus \Phi^{-1}\big(\{(x, y) \in C \big|\ y = 0\}\big)$ bijektiv auf $\{(x, y) \in C \big|\ y \neq 0\}$ abbildet. Nach dem Satz über die offene Abbildung ([Ahlfors], chapter 4, 3.3) ist Φ sogar ein Homöomorphismus zwischen diesen beiden Mengen.

Sei schliesslich $(x, 0) \in C$. Wir haben bereits gezeigt, dass es höchstens zwei Punkte in $(H \setminus \mathcal{N})/\Gamma_0(11)$ gibt, die von Φ auf $(x, 0)$ abgebildet werden. Wir nehen an, es wären in der Tat zwei verschieden Punkte; nennen wir sie τ und τ'. Wähle kleine offene Kreisscheiben U um τ und U' um τ' so dass $U \cap U' = \emptyset$. Dann ist $\Phi(U) \cup \Phi(U')$ eine Umgebung V von $(x, 0)$; und $V \setminus \{(x, 0)\}$ist vermöge Φ^{-1} homöomorph zur disjunkten Vereinigung von $U \setminus \{\tau\}$ und $U' \setminus \{\tau'\}$. Da V zu einer Umgebung des Nullpunktes in der komplexen y–Ebene homöomorph ist, ist bereits $\Phi(U)$ oder $\Phi(U')$ eine Umgebung von $(x, 0)$. Dies ist unmöglich, da $\tau \in \overline{U \setminus \{\tau\}}$ und $\tau' \in \overline{U \setminus \{\tau'\}}$. □

7.2 Der Satz von Eichler-Shimura und die Vermutung von Taniyama–Shimura

In Satz 7.1.10 haben wir gesehen, dass die Modulfunktionen $\mathbf{X}(\tau)$ und $\mathbf{Y}(\tau)$ eine Bijektion zwischen $(H \setminus \mathcal{N}) \,/\, \Gamma_0(11)$ und dem Komplement endlich vieler Punkte in

$$C = \{(x, y) \in \mathbb{C}^2 \,|\, y^2 = -44x^3 + 56x^2 - 20x + 1\}$$

definieren. In Übung 1.3.10 wurde ein affin linearer Koordinatenwechsel in $\mathbb{C}^2$ mit rationalen Koeffizienten konstruiert, der C bijektiv auf

$$C' = \{(x, y) \in \mathbb{C}^2 \,|\, y^2 + y = x^3 - x^2 - 10x - 20\}$$

abbildet. In Übung 1.3.11 haben Sie für kleine Primzahlen p die Anzahl N_p der $\mathbb{F}_p$-rationalen Punkte von C', d.h. die Zahlen

$$N_p = \#\,\{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \,|\, y^2 + y = x^3 - x^2 - 10x - 20\}$$

bestimmt. Hier bezeichnet $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ den endlichen Körper mit p Elementen. Da sich C' und C nur um einen Koordinatenwechsel mit rationalen Koeffizienten unterscheiden, gilt jedenfalls für alle Primzahlen p, die nicht in den Primfaktorzerlegungen der Koeffizienten des Koordinatenwechsels auftreten, dass $N_p = \#\,\{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \,|\, y^2 = -44x^3 + 56x^2 - 20x + 1\}$.

Andererseits haben Sie in Übung 5.1.5 für kleine Primzahlen p die Fourierkoeffizienten λ_p der Spitzenform

$$\gamma(\tau) = F(\tau)^2 = \eta(\tau)^2 \cdot \eta(11\tau)^2$$

berechnet. Wir schreiben die Zahlen p, N_p, λ_p in eine Tabelle:

p	2	3	5	7	11	13	17	19	23	29	31	37
N_p	4	4	4	9	10	9	19	19	24	29	24	34
λ_p	-2	-1	1	-2	1	4	-2	0	-1	0	7	3

p	41	43	47	53	59	61	67	71	73	79	83	89	97
N_p	49	49	39	59	54	49	74	74	69	89	89	74	104
λ_p	-8	-6	8	-6	5	12	-7	-3	4	-10	-6	15	-7

und sehen, dass für Primzahlen $p \leq 100$

$$N_p = p - \lambda_p$$

In der Tat gilt $N_p = p - \lambda_p$ für alle Primzahlen p. Dies können wir in dieser Vorlesung nicht beweisen. In den folgenden Abschnitten 3 - 6 dieses Kapitels beschreiben wir aber einige Argumente, die es zumindest plausibel machen, dass $N_p = p - \lambda_p$ für alle bis auf endlich viele Primzahlen p gilt. In diesem Abschnitt wird über eine Verallgemeinerung dieser Identität (den Satz von Eichler-Shimura-Weil), und ihren Zusammenhang mit der Vermutung von Shimura-Taniyama-Weil und der Lösung der Fermat'schen Vermutung durch Wiles und Taylor berichtet (siehe auch [DDT], [Kramer], [Ribet], [Wuestholz]).

Die Mengen C und C' sind Beispiele von über $\mathbb{Q}$ definierten elliptischen Kurven. Allgemein ist eine affine, über $\mathbb{Q}$ definierte elliptische Kurve eine Menge der Form

$$\{(x,y) \in \mathbb{Q}^2 \mid y^2 + a_1\, x\, y + a_3\, y = a_0\, x^3 + a_2\, x^2 + a_4\, x + a_6\}$$

mit $a_0, a_1, a_2, a_3, a_4, a_6, \in \mathbb{Q}$, $a_0 \neq 0$.
Zwei solche elliptische Kurven heissen äquivalent, wenn sie durch einen invertierbaren affin linearen Koordinatenwechsel mit rationalen Koeffizienten ineinander übergeführt werden können. Nach Übung 1.3.10 sind also die elliptischen Kurven mit den Gleichungen

$$\begin{aligned} y^2 = &\quad -44x^3 + 56x^2 - 20x + 1 \\ y^2 + y = &\quad x^3 - x^2 - 10x - 20 \\ y^2 = &\quad 4x^3 - \tfrac{124}{3}\, x - \tfrac{41 \cdot 61}{27} \end{aligned}$$

äquivalent.

Definition 7.2.1 *Die elliptische Kurve*

$$E = \{(x,y) \in \mathbb{Q}^2 \mid y^2 + a_1\, x\, y + a_3\, y = a_0\, x^3 + a_2\, x^2 + a_4\, x + a_6\}$$

heisst modular zur Stufe N, falls es Modulfunktionen $\mathbf{X}(\tau)$, $\mathbf{Y}(\tau)$ für die Gruppe $\Gamma_0(N)$ gibt, deren Fourierkoeffizienten alle ganzzahlig sind und so dass $\tau \mapsto (\mathbf{X}(\tau), \mathbf{Y}(\tau))$ eine Abbildung vom Komplement endlich vieler $\Gamma_0(N)$-Orbits in H auf das Komplement endlich vieler Punkte in

$$E(\mathbb{C}) := \{(x,y) \in \mathbb{C}^2 \mid y^2 + a_1\, x\, y + a_3\, y = a_0 x^3 + a_2\, x^2 + a_4\, x + a_6\}$$

definiert.

Satz 7.1.10 zeigt also, dass die elliptische Kurve

$$C = \{(x, y) \in \mathbb{Q}^2 \mid y^2 = -44x^3 + 56x^2 - 20x + 1\}$$

modular zu Stufe 11 ist.
Wir können jetzt die Verallgemeinerung der oben betrachteten Identität $N_p = p - \lambda_p$ formulieren. Ist

$$E = \{(x, y) \in \mathbb{Q}^2 \mid y^2 + a_1\, x\, y + a_3\, y = x^3 + a_2\, x^2 + a_4\, x + a_6\}$$

eine über $\mathbb{Q}$ definierte elliptische Kurve, so sei für jede Primzahl p, die nicht in der Primfaktorzerlegung der Nenner von a_1, a_2, a_3, a_4, a_6 auftritt,

$$N_p(E) \;:=\; \#\,\{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \mid y^2 + a_1\, x\, y + a_3\, y = x^3 + a_2\, x^2 + a_4\, x + a_6\}$$

Satz 7.2.2 (Eichler, Shimura)
Ist E eine zur Stufe N modulare elliptische Kurve, so gibt es eine Spitzenform f für $\Gamma_0\,(N)$ vom Gewicht 2, deren Fourierentwicklung

$$f(\tau) = \sum_{n \geq 1} \lambda_n\, e^{2\pi i\, n \tau}$$

nur ganzzahlige Koeffizienten hat und so dass

$$N_p(E) \;= p - \lambda_p$$

für alle bis auf endlich viele Primzahlen p.

Wir haben oben ein spezielles Beispiel des Satzes von Eichler-Shimura betrachtet, nämlich

$$a_1 = 0,\; a_2 = -1,\; a_3 = 1,\; a_4 = -10,\; a_6 = -20$$

und $f(\tau) = \gamma(\tau) = \eta(\tau)^2\, \eta\,(11\tau)^2$. In der Tat gilt hier

$$N_p = p - \lambda_p$$

für alle Primzahlen p.

Dies lässt sich auch verallgemeinern. Dazu führen wir die Diskriminante $\triangle_E$ einer elliptischen Kurve

$$E = \{(x, y) \in \mathbb{Q}^2 \mid y^2 + a_1\, x\, y + a_3\, y = x^3 + a_2\, x^2 + a_4\, x + a_6\}$$

mit ganzzahligen Koeffizienten a_1, a_2, a_3, a_4, a_6 ein. $\triangle_E$ ist ein explizites Polynom in a_1, a_2, a_3, a_4, a_6, das genau dann verschwindet, wenn $E(\mathbb{C})$ singuläre Punkte hat. Falls $a_1 = a_2 = a_3 = 0$, so ist $\triangle_E = -16\,(4\,a_4^3 - 27\,a_6^2)$, stimmt also bis auf den Faktor -16 mit der Diskriminante des kubischen Polynoms $x^3 + a_4\, x + a_6$ überein. Man kann nun zeigen, dass es für jede elliptische Kurve E eine zu E äquivalente Kurve E' mit ganzzahligen Koeffizienten gibt, deren Diskriminante $\triangle_{E'}$ die Diskriminante $\triangle_{E''}$ aller zu E äquivalenten Kurven E'' mit ganzzahligen Koeffizienten teilt. E' heisst **minimales Modell** von E, und

$$\triangle_E^{min} := \triangle_{E'}$$

die **minimale Diskriminante** von E. Beispielsweise ist $\triangle_{C'} = -11^5$ und C' ist minimales Modell für C (siehe [Tate], § 8). Es gibt einen Algorithmus von Tate, der zu jeder elliptischen Kurve ein minimales Modell konstruiert.

Satz 7.2.3 (Igusa)
Sei E eine elliptische Kurve mit minimaler Diskriminante (d.h. $\triangle_E = \triangle_E^{min}$), die modular ist zur Stufe N. Dann gibt es eine Spitzenform vom Gewicht 2 für $\Gamma_0(N)$, deren Fourierentwicklung $f(\tau) = \sum_{n\geq 1} \lambda_n e^{2\pi i n \tau}$ nur ganzzahlige Koeffizienten hat und so dass

$$N_p(E) = p - \lambda_p$$

für alle Primzahlen p, die N nicht teilen.[1]

Die **Vermutung von Shimura-Taniyama-Weil** besagt nun, dass jede über $\mathbb{Q}$ definierte elliptische Kurve E modular zu einer gewissen Stufe N ist. Nach dem Satz von Eichler-Shimura impliziert dies, dass es eine Spitzenform f vom Gewicht 2 für $\Gamma_0(N)$ gibt, so dass $N_p(E) = p - \lambda_p$ für fast alle Primzahlen p gibt, wobei λ_n wieder die Fourierkoeffizienten von f sind (Übrigens gilt auch die Umkehrung [???]). Zusätzlich macht die Vermutung von Taniyama-Shimura-Weil eine Aussage darüber, wie sich die Stufe der Modularität N aus E bestimmt. Wir nehmen an,

$$E = \{(x,y) \in \mathbb{Q}^2 \mid g(x,y) = 0\}$$

mit

$$g(x,y) = y^2 + a_1 x y + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6$$

($a_1, a_2, a_3, a_4, a_6, \in \mathbb{Z}$) habe bereits minimale Diskriminante. Ist p eine Primzahl, so sagen wir, E habe **gute Reduktion** modulo p, falls

$$E_p := \{(x,y) \in \mathbb{F}_p \times \mathbb{F}_p \mid g(x,y) = 0\}$$

nichtsingulär ist, d.h.

$$\frac{\partial g}{\partial x}(x,y) \neq 0 \quad \text{oder} \quad \frac{\partial g}{\partial y}(x,y) \neq 0 \quad \text{für alle} \quad (x,y) \in E_p$$

Andernfalls sagen wir, E habe schlechte Reduktion modulo p. Der Einfachheit halber nehmen wir zusätzlich an, dass E **semistabil** ist, d.h. dass für alle Primzahlen p und alle $(x_0, y_0) \in E_p$ mit $\frac{\partial g}{\partial x}(x_0,y_0) = \frac{\partial g}{\partial y}(x_0,y_0) = 0$ gilt, dass die Hesse'sche

$$det \begin{pmatrix} \frac{\partial^2 g}{\partial x^2}(x_0,y_0) & \frac{\partial^2 g}{\partial x \partial y}(x_0,y_0) \\ \\ \frac{\partial^2 g}{\partial y \partial x}(x_0,y_0) & \frac{\partial^2 g}{\partial y^2}(x_0,y_0) \end{pmatrix} \neq 0$$

Geometrisch gesprochen bedeutet dies, dass jedes E_p höchstens gewöhnliche Doppelpunkte als Singularitäten hat. In dieser Situation besagt die Vermutung von Shimura-Taniyama-Weil, dass

$$N = \prod_{\substack{p \,\text{Primzahl} \\ E \,\text{hat schlechte} \\ \text{Reduktion in}\, p}} p$$

Es ist wohlbekannt, dass es nur endlich viele Primzahlen gibt, bezüglich derer E schlechte Reduktion hat.

[1] dass die Gleichheit $N_p = p - \lambda_p$ in unserem Beispiel auch für $p = 11$ gilt, ist Zufall

Die Vermutung von Shimura-Taniyama-Weil spielt eine wichtige Rolle im Beweis der Fermat'schen Vermutung, der 1994 von Wiles und Taylor gegeben wurde. Es ist relativ leicht zu zeigen, dass, wenn die Fermat'sche Vermutung falsch wäre, es eine Primzahl $\ell \geq 5$ und ganze Zahlen $a, b, c \geq 1$ mit $g\,g\,T\,(a,b,c) \;= 1$, $a \equiv -1\, mod\, 4$, b gerade gäbe, so dass

$$a^\ell + b^\ell = c^\ell.$$

G. Frey hatte 1985 die Idee, einem solchen Tripel a, b, c die elliptische Kurve

$$E_{a,b,c} = \{(x,y) \;\in \mathbb{Q}^2 \,|\, y^2 = x\,(x - a^\ell)\,(x - b^\ell)\}$$

zuzuordnen. Sie ist nicht minimal, ein minimales Modell ist

$$E' = \{(x,y) \;\in \mathbb{Q}^2 \,|\, y^2 + x\,y = x^3 + \frac{b^\ell - a^\ell - 1}{4}\,x^2 - \frac{a^\ell\,b^\ell}{16}\,x\}$$

und die minimale Diskriminante ist [2]

$$\triangle^{min}_{a,b,c} \;= \;\frac{1}{2^8}\,(a\,b\,c)^{2\ell}$$

Man kann zeigen, dass $E_{a,b,c}$ semistabil wäre. Die Shimura-Taniyama-Weil-Vermutung würde somit implizieren, dass $E_{a,b,c}$ modular von der Stufe

$$N_{a,b,c} = \prod_{\substack{p\,|\,a\,b\,c \\ p\,prim}} p$$

wäre.

Andererseits vermutete Frey, dass es keine modulare elliptische Kurve geben könne, deren minimale Diskriminante das Produkt einer Zweierpotenz und einer ℓ-ten Potenz einer Zahl ist. Diese Vermutung, zusammen mit der Shimura-Taniyama-Weil-Vermutung, ergäbe dann natürlich einen Widerspruch. Im Jahre 1990 gelang es K. Ribet mit anderen Ideen als denen von Frey zu beweisen, dass $E_{a\,b\,c}$ nicht modular sein kann (siehe [Kramer] für eine kurze Beschreibung, [Ribet] für eine etwas ausführlichere). Damit war also klar, dass die Vermutung von Shimura-Taniyama-Weil die Fermat'sche Vermutung impliziert. Im allgemeinen ist die Vermutung von Shimura-Taniyama-Weil immer noch nicht gelöst. Jedoch gelang es Wiles und Taylor zu beweisen, dass elliptische Kurven der Form $E_{a,b,c}$ wie oben stets modular sein müssten. Damit war die Fermat'sche Vermutung bewiesen.

7.3 Drei Modelle für $H/\Gamma_0(11)$

In Satz 7.1.10 haben wir gesehen, dass die Kurve

$$C = \{(x,y) \in \mathbb{C}^2 \,/\, y^2 = -44\,x^3 + 56x^2 - 20x + 1\}$$

ein Modell für $H \,/\, \Gamma_0(11)$ ist. Genauer hatten wir gezeigt, dass die Abbildung $\tau \;\mapsto\; (\mathbf{X}(\tau), \mathbf{Y}(\tau)$ eine Bijektion zwischen $(H \setminus \mathcal{N}) \,/\, \Gamma_0(11)$ und $C \setminus \{(0, \pm 1)\}$ induziert. Es ist nützlich, die gesamte Quotientenmenge $H \,/\Gamma_0(11)$ als affine Kurve zu beschreiben. Dazu setzen wir

$$D := \{(u,v) \in \mathbb{C}^2 \,/\, v^2 = u^4 - 20\,u^3 + 56u^2 - 44u\}$$

[2]Führe den Koordinatenwechsel $x = 4x'$, $y = 8y' + 4x'$ durch.

Offenbar ist die Abbildung

$$\begin{array}{rcl} C \setminus \{ (0, \pm 1) \} & \longrightarrow & D \setminus \{ (0,0) \} \\ (x,y) & \longmapsto & \left(\frac{1}{x}, \frac{y}{x^2} \right) \end{array}$$

eine Bijektion. Wir setzen

$$U(\tau) := \frac{1}{\mathbf{X}(\tau)} \quad , \quad V(\tau) := \frac{\mathbf{Y}(\tau)}{\mathbf{X}(\tau)^2}$$

Da $\mathbf{X}$ keine Nullstelle auf H und eine doppelte Polstelle in τ_0 hat und $\mathbf{Y}$ eine dreifache Polstelle in τ_0 hat, sind U und V holomorphe Funktionen auf H. Sie sind offensichtlich $\Gamma_0(11)$-invariant. Ferner ist U auch φ_J-invariant, während V φ_J-antiinvariant ist, d.h. $V(\varphi_J(\tau)) = -V(\tau)$. Schliesslich haben U und V ganzzahlige Fourierreihen.

$$\begin{array}{rl} U(\tau) & = e^{-2\pi i \tau} \left[1 - (6e^{2\pi i \tau} - 21 e^{4\pi i \tau} + 66 e^{6\pi i \tau} + \cdots) \right]^{-1} \\ & = e^{-2\pi i \tau} \left(1 + 6e^{2\pi i \tau} + 15 e^{4\pi i \tau} + 30 e^{6\pi i \tau} + \cdots \right) \\ V(\tau) & = e^{-4\pi i \tau} \left(1 + 5e^{2\pi i \tau} + \ 2 e^{4\pi i \tau} - 78 e^{6\pi i \tau} + \cdots \right) \end{array}$$

Aus Satz 7.1.10 und den obigen Beobachtungen ergibt sich sofort

Satz 7.3.1 *Die Abbildung $\tau \longrightarrow (U(\tau), V(\tau))$ definiert eine Bijektion Φ_D zwischen $H \,/\, \Gamma_0(11)$ und D.*

D ist unser zweites Modell für $H \,/\, \Gamma_0(11)$.
Wir können diese Aussage von Satz 7.3.1 verfeinern zu

Satz 7.3.2 *Sei $f(\tau) = \sum_{n=-m}^{\infty} c_n e^{2\pi i\, n \tau}$ eine holomorphe und $\Gamma_0(11)$-invariante Funktion auf H. Dann gibt es eindeutig bestimmte Polynome $P(x)$, $Q(x)$ so dass*

$$f(\tau) = P\left(U\left(\tau\right)\right) + V(\tau) \cdot Q\left(U\left(\tau\right)\right)$$

Falls f nur ganzzahlige Fourierkoeffizienten hat, so haben P und Q ganzzahlige Koeffizienten.

Beweis. Wir betrachten zunächst den Fall, dass f invariant unter φ_J ist. Sei $\Gamma_0^*(11) = \Gamma_0(11) \cup \Gamma_0(11) \cdot \varphi_J$. Aus Satz 7.3.1 folgt, dass U eine Bijektion zwischen $H \,/ \Gamma_0^*(11)$ und $\mathbb{C}$ induziert. Folglich gibt es eine auf $\mathbb{C} \setminus \{0\}$ konvergente Reihe $P(x) = \sum_{j \geq 1} a_j x^j$, so dass für alle $\tau \in H$

$$f(\tau) = P\left(U\left(\tau\right)\right)$$

Da $\nu_\infty(U) = -1$, ist $a_j = 0$ für $j \geq m$. Also ist

$$P(x) = \sum_{j=0}^{m} a_j\, x^j$$

ein Polynom.
Wir setzen nun noch voraus, dass $c_n \in \mathbb{Z}$ für alle $n \in \mathbb{Z}$. Aus der Fourierreihe für U sieht man, dass der Koeffizient von $e^{-2\pi i k \tau}$ in $P\left(U(\tau)\right) = \sum_{j=0}^{m} a_j\, U\left(\tau\right)^j$ gleich

$$a_k + (\text{ganzzahliges Polynom in}\, a_{k+1}, \cdots, a_m)$$

ist. Daraus sieht man durch absteigende Rekursion, dass $a_j \in \mathbb{Z}$ für $j = m, m-1, \ldots, 1, 0$.

Nun betrachten wir den Fall, dass f antiinvariant unter φ_J ist, d.h. dass $f(\varphi_J(\tau)) = -f(\tau)$. Da $[\varphi_J(\tau_0)] = [\tau_0]$, ist $f(\tau_0) = 0$. Die Funktion $\frac{1}{V(\tau)} f(\tau)$ hat einen Pol der Ordnung ≤ 1 in τ_0. Sie hat ganzzahlige Fourierkoeffizienten, wenn f ganzzahlige Fourierkoeffizienten hat.
Deshalb ist $\tau \mapsto \frac{f(\tau)}{V(\tau)}$ eine φ_J-invariante Funktion, die die Voraussetzung des Satzes erfüllt. Nach dem bereits bewiesenen Teil gibt es ein Polynom $Q(x)$ so dass

$$\frac{1}{V(\tau)} f(\tau) = Q(U(\tau))$$

Falls f ganzzahlige Fourierkoeffizienten hat, so hat Q ganzzahlige Koeffizienten. $\square$

Um zum dritten Modell für $H / \Gamma_0(11)$ zu gelangen, bemerken wir, dass die Kurve $C = (H \backslash \mathcal{N}) / \Gamma_0(11)$ eine elliptische Kurve ist. In Übung 1.3.10 hatten wir ihre Weierstrass'sche Normalform bestimmt. Genauer hatten wir gezeigt, dass die affin lineare Transformation

$$\begin{aligned} A : \mathbb{C}^2 &\longrightarrow \mathbb{C}^2 \\ (x,y) &\longmapsto (-11x + \tfrac{14}{3}, 11y) \end{aligned}$$

die Kurve C auf

$$C'' = \{(x,y) \in \mathbb{C}^2 \,/\, y^2 = 4x^3 - \frac{124}{3}x - \frac{41 \cdot 61}{9}\}$$

abbildet. Deshalb lässt sich C nicht nur durch Modulfunktionen wie in Satz 7.1.10, sondern auch durch elliptische Funktionen parametrisieren.

Satz 7.3.3 *Es gibt über $\mathbb{R}$ linear unabhängige Elemente $\omega_1, \omega_2, \in \mathbb{C}$, so dass für den komplexen Torus $E := \mathbb{C} / \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_1$ folgendes gilt:*

i) Sei $\gamma(\tau) = F^2(\tau) = \eta^2(\tau) \cdot \eta^2(11\tau)$ die Spitzenform vom Gewicht 2 für $\Gamma_0(11)$, und $\tau_0 \in H$ eine Nullstelle von G. Dann induziert die Abbildung

$$\begin{aligned} H &\longrightarrow \mathbb{C} \\ \tau &\longmapsto \int_{\tau_0}^{\tau} \gamma(z)\, dz \end{aligned}$$

eine Injektion $I_\gamma : H / \Gamma_0(11) \longrightarrow E$.

ii) Es gibt eine Bijektion $\Psi : C \longrightarrow E \setminus \{0\}$ so dass das Diagramm

$$\begin{tikzcd}
 & E \\
(H \setminus \mathcal{N}) / \Gamma_0(11) \arrow[ur, "I_\gamma"] \arrow[dr, "\Phi"'] & \\
 & C \arrow[uu, "\Psi"']
\end{tikzcd}$$

kommutiert. Die Komponenten von Ψ^{-1} sind Linearkombinationen von $\wp(u; \omega_1, \omega_2)$ und $\wp'(u, \omega_1, \omega_2)$.

iii) Es gibt eine Bijektion $\psi_D : D \longrightarrow E \setminus \{\int_{\tau_0}^{i\infty} \gamma(z)\, dz,\ \int_{\tau_0}^{0} \gamma(z)\, dz\}$, so dass das Diagramm

$$\begin{tikzcd}
& (H \setminus \mathcal{N}) \,/\, \Gamma_0\,(11) \arrow[rr, "I_\gamma"] \arrow[dr] & & E \\
\tau \arrow[r, mapsto] & (U(\tau),\, V(\tau)) & D \arrow[ur, "\psi_D"'] &
\end{tikzcd}$$

kommutiert.

Der komplexe Torus E ist das dritte Modell für $H \,/\, \Gamma_0(11)$.

Beweis. Nach Satz 3.4.8 gibt es $\omega_1',\, \omega_2' \in \mathbb{C}$, so dass

$$g_2(\omega_1',\, \omega_2') = \frac{124}{3} \quad , \quad g_3(\omega_1',\, \omega_2') = \frac{41 \cdot 61}{9}$$

Wir setzen $E' = \mathbb{C} \,/\, \mathbb{Z}\omega_1' \oplus \mathbb{Z}\omega_2'$. Dann ist nach Satz 1.3.2 die Abbildung

$$\begin{aligned} E' \setminus \{0\} \quad &\longrightarrow C'' \\ u \quad &\longmapsto (\wp(u; \omega_1'\,,\, \omega_2')\,;\, \wp'(u; \omega_1'\,,\, \omega_2')) \end{aligned}$$

eine Bijektion. In Übung 1.3.9 wurde gezeigt, dass die Umkehrbildung gleich

$$\begin{aligned} \phi' :\ C'' \quad &\longrightarrow E' \\ p \quad &\longmapsto \textstyle\int_\infty^p \frac{dx}{y} \end{aligned}$$

ist. Dann ist $\phi' \circ A : C \to E'$ die Abbildung, die $p \in C$ den Punkt $-\int_\infty^p \frac{dx}{y}$ zuordnet. Da

$$\begin{aligned} \frac{1}{\mathbf{Y}} \frac{d\mathbf{X}}{d\tau} \quad &= \frac{G^3}{w} \cdot \frac{d}{d\tau} \frac{F^2}{G^2} \quad = \frac{\pi\, i\, F\, G^3}{G\, F' - F\, G'} \cdot \frac{2\, F F'\, G^2 - 2\, F^2\, G G'}{G^4} \\ &= 2\, \pi\, i\, F^2 \qquad = 2\, \pi\, i \gamma \end{aligned}$$

ist

$$\phi' \circ A \circ \Phi :\ (H \setminus \mathcal{N}) \,/\, \Gamma_0\,(11) \longrightarrow E'$$

die Abbildung $\tau \mapsto -2\pi\, i\, \int_{\tau_0}^{\tau} \gamma\,(z)\, d\,z$.
Wir setzen $\omega_1 := -2\,\pi\, i\, \omega_1\,,\, \omega_2 = -2\,\pi\, i\, \omega_2$ und $\phi := -2\,\pi\, i\, \phi' \circ A$. Damit ergibt sich Teil (i) und Teil (ii) der Proposition. Teil (iii) ist eine triviale Folgerung. □

Satz 7.3.3 zeigt, dass die affinen komplex algebraischen Kurven C bzw. D isomorph zum Komplement von einem bzw. zwei Punkten in dem kompakten Torus E sind. Im Fall von $D\tilde{=}H\,/\,\Gamma_0(11)$ sind die beiden Ausnahmepunkte

$$I_\gamma(i\,\infty)\;:=\;\left[\int_{\tau_0}^{i\,\infty}\gamma(z)\,dz\right]\quad\text{und}\quad I_\gamma(0)\;=\;\left[\int_{\tau_0}^{0}\gamma(z)\,dz\right]$$

Später brauchen wir eine Parametrisierung von E in der Nähe dieser beiden Ausnahmepunkte.

Lemma 7.3.4 *Es gibt eine biholomorphe Abbildung κ_∞ und κ_0 von einer Umgebung von 0 in $\mathbb{C}$ auf eine Umgebung von $I_\gamma(i\,\infty)$ bzw. $I_\gamma(0)$ in E so dass*

$$\begin{array}{rcll} I_\gamma(\tau) & = & \kappa_\infty\,(e^{2\pi\,i\,\tau}) & \textit{für } \Re\,\tau \textit{ gross genug}\\ I_\gamma(\tau) & = & \kappa_0\,(e^{-2\pi\,i\,\tau/11}) & \textit{für } \tau \textit{ klein genug}\end{array}$$

Beweis. Es sei wieder

$$\gamma(\tau)=\sum_{n\geq 1}\lambda_n\,e^{2\pi\,i\,n\tau}$$

die Fourierreihe von γ. Wir setzen

$$\kappa_\infty(z)\;=I_\gamma(i\,\infty)\;+\;\frac{1}{2\pi i}\sum_{n\geq 1}\frac{\lambda_n}{n}\,z^n$$

Da $\lambda_1\neq 0$, definiert κ_∞ eine biholomorphe Abbildung zwischen einer Umgebung von 0 in $\mathbb{C}$ und einer Umgebung von $I_\gamma\,(i\,\infty)$. Die Identität $I_\gamma(\tau)\;=\kappa_\infty\,(e^{2\pi\,i\,\tau})$ folgt direkt aus den Definitionen.

Nach (7.4) gilt

$$\gamma(z)\;=-\frac{1}{11\tau^2}\,\gamma\left(-\frac{1}{11\,z}\right)$$

und somit, da $-1/11_{\tau_0}=\tau_0$,

$$I_\gamma\,(\tau)=\int_{\tau_0}^{\tau}\gamma(z)\,dz=-\int_{\tau_0}^{\tau}\gamma\,(-\frac{1}{11z})\,\frac{d\,z}{11z^2}=-\int_{\tau_0}^{-1/11\tau}\gamma(z)\,dz=-I_\gamma\,(-\frac{1}{11\tau})\,(*)$$

Die Abbildung κ_0 wird wie oben konstruiert. □

7.4 Die Frobenius-Korrespondenz

Wir kehren zurück zu der in Abschnitt 1 betrachteten Situation, d.h. zu der Abbildung

$$\Phi:\;(H\setminus\mathcal{N})\,/\Gamma_0\,(11)\;\longrightarrow C=\{(x,y)\;\in\mathbb{C}^2\,/\,y^2\,=-44\,x^3+56\,x^2-20x+1\}$$

$$[\tau]\longmapsto\;(\mathbf{X}(\tau),\;\mathbf{Y}(\tau))$$

Es sei wieder

$$\gamma(\tau):=F^2(\tau)=\eta^2(\tau)\,\eta^2(11\tau)\;=\sum_{n\geq 1}\lambda_n\,e^{2\pi i\,n\tau}$$

und

$$N_p=\#\{(x,y)\in\mathbb{F}_p\times\mathbb{F}_p\,/\,y^2\,=\,-44x^3+56x^2-20x+1\}$$

Wir wollen Argumente geben, die es "plausibel machen", dass für alle bis auf endlich viele Primzahlen $N_p = p - \lambda_p$ gilt. Diese Argumente folgen im wesentlichen dem Beweis von [Eichler 1954]. Allerdings werden im Beweis von Eichler am Ende einige Tatsachen aus der algebraischen Geometrie verwendet, auf die wir hier nicht eingehen. Insofern bleibt bei der Darstellung hier eine Lücke.
Im Abschnitt 5 werden wir - ähnlich wie in Kapitel VI - die Fourierkoeffizienten λ_p als Eigenwerte von Hecke-Operatoren interpretieren. Die Zahlen N_p werden wir gleich mit Hilfe der "Frobeniuskorrespondenz" geometrisch interpretieren. Die Kronecker-Weber'sche Kongruenzrelation (Abschnitt 7) schliesslich gibt die Beziehung zwischen der Hecke - Korrespondenz und der Frobenius-Korrespondenz.

In der Vorlesung "Algebra II" haben Sie gesehen, dass algebraische Geometrie günstig über algebraisch abgeschlossenen Körpern wie $\overline{\mathbb{F}}_p$, $p\,prim$ betrieben wird. Um den Übergang von $\overline{\mathbb{F}}_p$ zu $\mathbb{F}_p$ zu machen, verwenden wir

Lemma 7.4.1 *Sei p eine Primzahl. Dann ist*

$$\mathbb{F}_p = \{x \in \overline{\mathbb{F}}_p \,/\, x^p = x\}$$

Beweis. Die multiplikative Gruppe $\mathbb{F}_p^*$ hat Ordnung $p-1$, also ist $x^{p-1} = 1$ für alle $x \in \mathbb{F}_p^*$. Folglich lösen alle p Elemente von $\mathbb{F}_p$ die Gleichung $x^p - x = 0$. Das Polynom $x^p - x$ hat aber in $\overline{\mathbb{F}}_p$ höchstens p Nullstellen. Daraus folgt die Behauptung. □

Die Abbildung $\overline{\mathbb{F}}_p \longrightarrow \overline{\mathbb{F}}_p$, $x \mapsto x^p$ heisst die Frobenius-Abbildung. Die Suche nach Punkten mit Koeffizienten in $\mathbb{F}_p$ entspricht also der Suche nach Fixpunkten "des Frobenius". Um dies konkret zu machen, setzen wir

$$C_p := \{(x,y) \in \overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p \,/\, y^2 = -44x^3 + 56x^2 - 20x + 1\}$$

und definieren die **Frobeniuskorrespondenz** $\mathcal{F}_p$ als [3]

$$\mathcal{F}_p\,(C) \;:= \{((x_1,\, y_1)\,,\, (x_2,\, y_2)) \,\in\, C_p \times C_p \,/\, x_2 = x_1^p \text{ und } y_2 = y_1^p\}$$

Ferner sei

$$\triangle\,(C_p) := \{((x_1,\, y_1)\,,\, (x_2,\, y_2)) \,\in\, C_p \times C_p \,/\, x_2 = x_1 \text{ und } y_2 = y_1\}$$

die Diagonale in $C_p \times C_p$. Offensichtlich gilt dann

Lemma 7.4.2

$$N_p = \#\,(\triangle\,(C_p) \cap \mathcal{F}_p(C))$$

Punkte von $\triangle\,(C_p) \cap \mathcal{F}_p(C)$ nennt man auch Fixpunkte der Frobeniuskorrespondenz $\mathcal{F}_p$. N_p ist also die Anzahl der Fixpunkte der Frobeniuskorrespondenz.
Im vorigen Abschnitt haben wir neben C auch die Kurve D mit der Gleichung $v^2 = u^4 - 20u^3 + 56u^2 - 44u$ betrachtet. Wir setzen also

$$\begin{aligned} D_p :=&\; \{(u,v) \in \mathbb{F}_p \times \mathbb{F}_p \,/\, v^2 = u^4 - 20u^3 + 56u^2 - 44u\} \\ \mathcal{F}_p\,(D) :=&\; \{((u_1,v_1)\,,\,(u_2,v_2)) \,\in D_p \times D_p \,/\, u_2 = u_1^p \text{ und } v_2 = v_1^p\} \\ \triangle\,(D_p) :=&\; \{(u_1,v_1)\,,\,(u_2,v_2) \,\in D_p \times D_p \,/\, u_2 = u_1 \text{ und } v_2 = v_1\} \end{aligned}$$

[3] Die Beziehung zwischen der Definition einer Korrespondenz in Kapitel VI und der Beschreibung durch geometrische Objekte wird im nächsten Abschnitt erläutert.

Da $(x,y) \mapsto \left(\frac{1}{x}, \frac{y}{x^2}\right)$ eine Bijektion zwischen $C_p \backslash \{(0,\pm 1)\}$ und $D_p \backslash \{0\}$ definiert, ist also für $p \neq 2$

$$N_p = \#\left(\triangle\,(D_p) \cap \mathcal{F}_p(D)\right) + 1 \tag{7.9}$$

7.5 Die Hecke-Korrespondenz für $\Gamma_0(11)$ und ihre Fixpunkte

Zunächst geben wir Interpretation von $H/\Gamma_0\,(11)$ als Modulraum markierter elliptischer Kurven. Es sei $\mathcal{L}_0\,(11)$ die Menge aller Paare (L, L') von Gittern in $\mathbb{C}$ mit $L \subset L'$, $[L' : L] = 11$. Wir sagen $(L_1, L_1') \cong (L_2, L_2')$ falls es $\lambda \in \mathbb{C}$ gibt mit $\lambda \cdot L_1 = L_2$, $\lambda \cdot L_1' = L_2'$. Ist $(L, L') \in \mathcal{L}_0\,(11)$ so ist das Bild von L' unter der Projektion $\mathbb{C} \longrightarrow \mathbb{C}\,/\,L$ eine Untergruppe der Ordnung 11 in $\mathbb{C}/L$. Ist umgekehrt L ein Gitter in $\mathbb{C}$ und G eine Untergruppe der Ordnung 11 von $\mathbb{C}\,/L$, so ist das Urbild von G unter der Projektion $\mathbb{C} \longrightarrow \mathbb{C}\,/L$ ein Gitter L' mit $L \subset L'$, $[L' : L] = 11$. Ferner ist $(L_1, L_1') \cong (L_2, L_2')$, genau dann, wenn es einen Isomorphismus zwischen $\mathbb{C}/L_1$ und $\mathbb{C}/L_2$ gibt, der die zu L_1' gehörende Untergruppe von $\mathbb{C}/L_1$ auf die zu L_2' gehörende Untergruppe von $\mathbb{C}/L_2$ abbildet. Deshalb nennen wir die Menge der Isomorphieklassen von $\mathcal{L}_0\,(11)$ auch die Menge der elliptischen Kurven mit ausgezeichneter Untergruppe der Ordnung 11.

Ist $\tau \in H$, so sei wie üblich $L_\tau := \mathbb{Z} \oplus \mathbb{Z}\tau$ und $L_\tau' := \mathbb{Z}\frac{1}{11} \oplus \mathbb{Z}\tau$.
Dann ist $(L_\tau, L_\tau') \in \mathcal{L}_0\,(11)$.

Satz 7.5.1 *i) Jedes $(L, L') \in \mathcal{L}_0\,(11)$ ist isomorph zu einem (L_τ, L_τ') mit $\tau \in H$.*

ii) Sind $\tau, \tau' \in H$, so ist $(L_{\tau'}, L_{\tau'}') \cong (L_\tau, L_\tau')$ genau dann, wennn es $A \in \Gamma_0(11)$ gibt mit $\varphi_A\,(\tau) = \tau'$.

Beweis. Der Beweis ist ähnlich wie der Beweis von Lemma 2.1.3 und Lemma 4.1.7.
(i) Sei $(L, L') \in \mathcal{L}_0(11)$. Wähle $\omega' \in L' \setminus L$ von minimaler Länge. Da L'/L eine Gruppe der Ordnung 11, also isomorph zu $\mathbb{Z}/11\mathbb{Z}$ ist, ist $\omega_1 := 11\,\omega' \in L$.
Wir zeigen zunächst, dass ω_1 ein primitives Element von L ist. Dazu nehmen wir an, es gäbe $n \in \mathbb{N}, n \geq 2$ so dass $\frac{1}{n} \cdot \omega_1 \in L$. Da $\omega' = \frac{1}{11}\,\omega_1 \notin L$, ist 11 kein Teiler von n. Nach dem chinesischen Restsatz gibt es $m, k \in \mathbb{Z}$, so dass $1 = m\,n + 11k$. Dann liegt

$$\frac{1}{n}\omega' = m\,\omega' + \frac{11k}{n}\omega' = m\,\omega' + k \cdot \frac{\omega_1}{n}$$

in L', da $\frac{\omega_1}{n} \in L \subset L'$. Offenbar ist $\frac{1}{n}\,\omega' \notin L$. Dies ist ein Widerspruch, da ω' minimale Länge unter allen Elementen von $L' \setminus L$ hat.
Nach Lemma 1.1.7 gibt es $\omega_2 \in L$, so dass (ω_1, ω_2) eine orientierte Basis von L bilden. Dann ist $(\omega', \omega_2) = (\frac{1}{11}\,\omega_1, \omega_2)$ eine orientierte Basis von L'. Sei $\tau := \frac{\omega_2}{\omega_1}$. Die Abbildung $z \longmapsto \frac{1}{\omega_1} \cdot z$ bildet dann (L, L') isomorph auf (L_τ, L_τ') ab.

ii) Sei zunächst $\tau' = \varphi_A(\tau)$ mit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0\,(11)$.

Schreibe $A^{-1} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$. Dann ist $c,\, c' \equiv 0 \; mod\; 11$.

Nach tz 1.1.8

$$L_\tau = \mathbb{Z}(a\,\tau + b) \,\oplus\, \mathbb{Z}(c\,\tau + d)$$

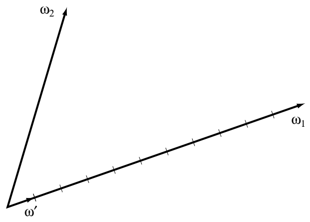

Abbildung 7.1:

Ferner ist

$$L'_\tau = \mathbb{Z}\frac{1}{11} \oplus \mathbb{Z}\tau = \mathbb{Z}\left(\frac{c'}{11}(a\tau + b) + \frac{d'}{11}(c\tau + d)\right) \oplus \mathbb{Z}\left(a'(a\tau + b) + b'(c\tau + d)\right)$$

Die Abbildung $z \longmapsto \frac{1}{c\tau + d}$ bildet L_τ bijektiv auf $L_{\tau'}$ ab. Ferner bildet sie L'_τ auf

$$\mathbb{Z}\left(\frac{c'}{11}\tau' + \frac{d'}{11}\right) \oplus \mathbb{Z}\left(a'\tau' + b'\right)$$

ab. Das Bild $\tilde{L}$ von L'_τ enthält L_τ, somit also $1, \tau'$. Da $\frac{c'}{11} \in \mathbb{Z}$, enthält es auch $\frac{d'}{11}$. Da 11 kein Teiler von d' ist, gibt es $m, k \in \mathbb{Z}$, so dass $1 = m\,d' + 11k$. Dann liegt auch $\frac{1}{11} = m \cdot \frac{d'}{11} + k \in \tilde{L}$. Folglich ist $L'_{\tau'} \subset \tilde{L}$. Da $[\tilde{L} : L_{\tau'}] = [L'_{\tau'} : L'_\tau] = 11$, folgt $\tilde{L} = L'_{\tau'}$, d.h. L'_τ wird auf $L'_{\tau'}$ abgebildet.
Sei nun umgekehrt $(L_\tau, L'_\tau) \cong (L_{\tau'}, L'_{\tau'})$. Sei $\lambda \in \mathbb{C}^*$, so dass $\lambda \cdot L_{\tau'} = L_\tau$ und $\lambda \cdot L'_{\tau'} = L'_{\tau'}$. Dann gibt es $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z})$, so dass

$$\lambda\tau' = a\tau + b/11 \quad , \quad \lambda \cdot \frac{1}{11} = c\tau + d/11$$

Somit ist $\lambda \cdot 1 = (11c)\,\tau + d$. Ferner ist b durch 11 teilbar, da ja

$$\lambda\,\tau' = a\tau + b/11 \in L_\tau = \mathbb{Z} \oplus \mathbb{Z}\tau$$

Folglich ist $\tau' = \varphi_A(\tau)$

$$\text{mit } A = \begin{pmatrix} a & b/11 \\ 11c & d \end{pmatrix} \in SL(2, \mathbb{Z})$$

□

Sei nun p eine von 11 verschiedene Primzahl. Die Hecke-Korrespondenz $T(p)$ ordnet $(L, L') \in \mathcal{L}_0(11)$ die formale Summe aller $(R, R') \in \mathcal{L}_0(11)$ mit $R \subset L$, $R' \subset L'$ und $[L : R] = [L' : R'] = p$ zu.

Lemma 7.5.2 *Sei $\tau \in H$. Dann ist $T(p)\,(L_\tau, L'_\tau)$ die formale Summe der $(p+1)$ Elemente*

$$\left(\mathbb{Z}p \oplus \mathbb{Z}(\tau + r)\,,\, \mathbb{Z}\frac{p}{11} \oplus \mathbb{Z}(\tau + r)\right) \quad , \quad 0 \le r \le p - 1 \;\textit{und}\; \left(\mathbb{Z} \oplus \mathbb{Z}p\,\tau\,,\, \mathbb{Z}\frac{1}{11} \oplus \mathbb{Z}p\tau\right)$$

Beweis. Nach Lemma 6.2.3 ist $T(p)\, L_\tau$ die formale Summe der Gitter $\mathbb{Z}(a\tau + b) \oplus \mathbb{Z}d$ mit $a\,d = p$ und $0 \leq b > d$. Ist $a\,d = p$, so ist $a = 1$, $d = p$ oder $a = p$, $d = 1$. Im ersten Fall ergeben sich mit $r = b$ die Gitter $\mathbb{Z}(\tau + r) \oplus \mathbb{Z}p\,, \quad 0 \leq r \leq p-1$; im zweiten Fall das Gitter $\mathbb{Z}p\tau \oplus \mathbb{Z}$.
$(R, R') \in \mathcal{L}_0\,(11)$ tritt genau dann als Summand in $T(p)\,(L_\tau, L'_\tau)$ auf, wenn R Summand in $T(p)\, L$ ist und R' ein Obergitter von R mit $[R' : R] = 11$ ist, das in L'_τ enthalten ist. Wir haben gerade gesehen, dass die Summanden von $T(p)\, L$ die Gitter $\mathbb{Z}\,p \oplus \mathbb{Z}\,(\tau + r), \quad 0 \leq r \leq p-1$ und $\mathbb{Z} \oplus \mathbb{Z}\,p\tau$ sind.
Sei zunächst $R = \mathbb{Z}\,p \oplus \mathbb{Z}\,(\tau + r)$ mit $0 \leq r \leq p-1$, und R' ein Obergitter wie oben, d.h.

$$\mathbb{Z}\,p \oplus \mathbb{Z}\,(\tau' + r) = R \subset R' \subset L'_\tau = \mathbb{Z}\,\frac{1}{11} \oplus \mathbb{Z}\,\tau$$

und $[R' : R] = 11$. Dann ist $[L'_\tau : R'] = p$, und somit das p-fache jedes Elements von L'_τ in R'. Insbesondere ist $\frac{p}{11} \in R'$. Deshalb ist $R' = \mathbb{Z}\,\frac{p}{11} \oplus \mathbb{Z}\,(\tau + r)$. Offenbar erfüllt $R' = \mathbb{Z}\,\frac{p}{11} \oplus \mathbb{Z}\,(\tau + r)$ alle Bedingungen.
Sei schliesslich $R = \mathbb{Z} \oplus \mathbb{Z}\,p\tau$ und wieder

$$\mathbb{Z} \oplus \mathbb{Z}\,p\tau = R \subset R' \subset L'_\tau = \mathbb{Z}\,\frac{1}{11} \oplus \mathbb{Z}\,p\tau$$

Wie oben sieht man, dass $R' = \frac{1}{11}\,\mathbb{Z} \oplus p\,\tau\,\mathbb{Z}$ □

Ist $(L, L') \in \mathcal{L}_0\,(11)$ und $\lambda \in \mathbb{C} \setminus \{0\}$, so ist $(R, R') \in \mathcal{L}_0\,(11)$ genau dann Summand von $T(p)\,(L, L')$, wenn $(\lambda R, \lambda R')$ Summand von $T(p)\,(\lambda L, \lambda L')$ ist. Deswegen induziert $T(p)$ eine Korrespondenz auf der Menge der Äquivalenzklassen von $\mathcal{L}_0\,(11)$. Nach Satz 7.5.1 ist diese Menge von Äquivalenzklassen gleich $H/\Gamma_0(11)$. Wir bezeichnen die induzierte Korrespondenz auf $H/\Gamma_0\,(11)$ mit T_p. Aus Lemma 7.5.2 ergibt sich

Korollar 7.5.3 *Die Korrespondenz T_p ordnet der Äquivalenzklasse $[\tau]$ von $\tau \in H$ die Summe der Klassen*

$$\left[\frac{\tau + r}{p}\right] \quad , \quad 0 \leq r \leq p-1 \qquad \textit{und} \quad [p\,\tau] \quad \textit{zu.}$$

Beweis. $\big(\mathbb{Z}p \oplus \mathbb{Z}(\tau + r)\,,\, \mathbb{Z}\frac{p}{11} \oplus \mathbb{Z}\,(\tau + r)\big)$ ist äquivalent zu $\big(L_{\frac{\tau+r}{p}}\,,\, L'_{\frac{\tau+r}{p}}\big)$, und $\big(\mathbb{Z} \oplus \mathbb{Z}p\tau\,,\, \mathbb{Z}\,\frac{1}{11} \oplus \mathbb{Z}\,p\tau\big) = (L_{p\tau}\,,\, L'_{p\tau})$ □

Ferner gilt

Lemma 7.5.4 *Sei* $J = \begin{pmatrix} 0 & -\frac{1}{\sqrt{11}} \\ \sqrt{11} & 0 \end{pmatrix}$. *Dann ist für* $[\tau] \in H/_{\Gamma_0(11)}$

$$\varphi_J\,(T_p\,([\tau]) = T_p\,(\varphi_J\,([\tau]))$$

Dabei bezeichnen wir die von φ_J induzierte Abbildung auf $H/_{\Gamma_0(11)}$ (missbräuchlicherweise) wieder mit φ_J.

Beweis. Sei $\tau \in H$. Da $\varphi_J^2 = i\,d$, genügt es zu zeigen, dass $\varphi_J\,(T_p\,(\varphi_J(\tau)))$ Teilmenge des $SL(2, \mathbb{Z})$ Orbits von $\{p\,\tau\} \cup \{\frac{\tau+s}{p} \,/\, 0 \leq s \leq p-1\}$ in H ist.
Die Menge $\varphi_J\,(T_p\,(\varphi_J(\tau)) = \varphi_J\,(T_p\,(\frac{-1}{11\,\tau}))$ besteht aus den Orbits von

$\varphi_J\left(\frac{-p}{11\tau}\right) = \frac{\tau}{p}$

$\varphi_J\left(\frac{-\frac{1}{11\tau}+r}{p}\right) = \varphi_J\left(\frac{(11r)\,\tau-1}{11p\,\tau}\right) = -\frac{p\,\tau}{(11r)\,\tau-1}$

Offenbar ist $\frac{\tau}{p} = \frac{\tau+s}{p}$ mit $s = 0$ und $\frac{-p\,\tau}{(11\cdot 0)\tau-1} = p\,\tau$. Sei nun $r \neq 0$. Wähle $1 \leq s \leq p-1$ so dass $11r\,s+1$ durch p teilbar ist. Dann ist

$$\frac{-p\,\tau}{(11r)\,\tau-1} = \frac{-p\,\frac{\tau}{p}}{(11r)\,\frac{\tau}{p}-\frac{1}{p}} = \frac{-p\,\frac{\tau+s}{p}+s}{11r\,\frac{(\tau+s)}{p} - \frac{11r\,s+1}{p}} = \varphi_A\left(\frac{\tau+s}{p}\right)$$

$$\text{mit } A = \begin{pmatrix} -p & s \\ 11r & -\frac{11r\,s+1}{p} \end{pmatrix} \in \Gamma_0\,(11)$$

□

Lemma 7.5.5 *T_p ist symmetrisch, d.h.*

$$[\tau'] \in T_p\,([\tau]) \iff [\tau] \in T_p([\tau'])$$

Beweis. Sei $[\tau'] \in T_p\,([\tau])$. O.B.d.A. sei

$$\tau' = p\,\tau \;\text{ oder }\; \tau' = \frac{\tau+r}{p} \quad , \quad 0 \leq r < p.$$

Im ersten Fall ist $\tau = \frac{\tau'+0}{p}$, und im zweiten Fall ist $\tau = p\tau' - r = \varphi_{\begin{pmatrix} 1 & -r \\ 0 & 1 \end{pmatrix}}(p\tau')$. □

Geometrisch lässt sich die Hecke Korrespondenz also folgendermassen beschreiben: Sei

$$\mathcal{T}_p' = \{\,(\tau,\tau') \in H \times H \,/\, \tau' = p\,\tau \text{ oder } \tau' = \frac{\tau+r}{p} \text{ für ein } r = 0,\ldots,p-1\}$$

und $\mathcal{T} \subset H\,/\Gamma_0(11) \times H\,/\Gamma_0\,(11)$ das Bild von $\mathcal{T}_p'$ unter der Projektion von $H \times H$ auf $H\,/\Gamma_0\,(11) \times H\,/\Gamma_0\,(11)$. Für jedes $[\tau] \in H\,/\Gamma_0\,(11)$ trifft die Menge

$$\{([\tau]\,,\,[\tau'])\,/\,[\tau'] \in H\,/\,\Gamma_0\,(11)\}$$

die Menge $\mathcal{T}_p$ in den (mit Multiplizität gezählt) $p+1$ Punkten $[\frac{\tau+r}{p}]$, $0 \leq r \leq p-1$ und $[p\,\tau]$. $T_p([\tau])$ ist die formale Summe dieser Schnittpunkte.

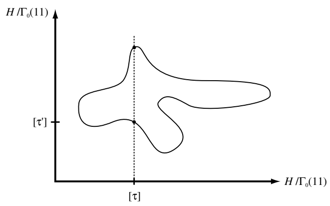

Abbildung 7.2:

Der Raum $M_1^0(\Gamma_0(11))$ der Spitzenformen vom Gewicht für $\Gamma_0(11)$ ist eindimensional (Übung 4.3.14) und hat als erzeugendes Element

$$\gamma(\tau) = F^2(\tau) = \eta(\tau)^2\,\eta(11\tau)^2$$

Wie in Satz 6.1.11 sieht man, dass der Hecke-Operator T_p durch

$$(T_p\, f)(\tau) = p\, f(p\,\tau) + \frac{1}{p}\sum_{r=0}^{p-1} f\,(\frac{\tau+r}{p}) \tag{7.10}$$

auf $M_1^0(\Gamma_0(11))$ operiert, und dass

$$T_p\,(\gamma) = \lambda_p\,\gamma \tag{7.11}$$

wobei λ_p den p-ten Fourierkoeffizienten von γ bezeichnet.

Um λ_p geometrisch zu interpretieren, gehen wir wie in Abschnitt 7.3 von $H\,/\,\Gamma_0(11)$ zu dem komplexen Torus $E := \mathbb{C}/_{\mathbb{Z}\,\omega_1 \oplus \mathbb{Z}\,\omega_2}$ über. Genauer verwenden wir die Injektion

$$I_\gamma : H\,/\Gamma_0\,(11) \longrightarrow E$$

$$\tau \longmapsto \int_{\tau_0}^{\tau} \gamma\,(z)\,d\,z$$

von Satz 7.3.3. Nach (7.4) ist

$$I_\gamma\,(\varphi_J\,(\tau)) = -I_\gamma\,(\tau)$$

Es sei K der Abschluss des Bildes von $\mathcal{T}_p$ unter $I_\gamma \times I_\gamma$ in $E \times E$. Die Lemmata 7.5.4 und 7.5.5 zeigen, dass die Involutionen $(u_1,\,u_2) \longmapsto (-u_1,\,-u_2)$ und $(u_1,\,u_2) \longmapsto (u_2,\,u_1)$ auf $E \times E$ die Menge K auf sich abbilden.

Ist $u = \Phi\,(\tau)$, so ist $\phi\,(T_p\,\tau)$ gleich der formalen Summe der Punkte $u' \in E$ mit $(u,\,u') \in K$ (mit Multiplizität gezählt). Ist allgemeiner B eine komplexe Untermannigfaligkeit von $E \times E$, so definiert B eine Korrespondenz auf E, die jedem $u \in E$ die formale Summe aller u' zuordnet, für die $(u,\,u')$ im Durchschnitt $(\{u\} \times E) \cap B$ liegt (mit Multiplizität gezählt). Wir nennen deshalb K die Hecke-Korrespondenz auf E. Wir nennen einen Punkt $u \in E$ **Fixpunkt** der durch K definierten Korrespondenz, wenn $(u,\,u) \in K$. Sie entsprechen Schnittpunkten von K mit der Diagonalen

$$\triangle\,(E) = \{(u_1, u_2)\, \in\, E \times E\,/\,u_1 = u_2\}$$

in $E \times E$.

Satz 7.5.6 *Es gibt eine meromorphe Funktion k auf $E \times E$, die*

- *eine einfache Nullstelle längs K hat,*
- *längs $\{0\} \times E$ und $E \times \{0\}$ mit Multiziplität λ_p verschwindet. Falls $\lambda_p < 0$, meinen wir damit, dass k längs dieser Mengen Polstellen der Ordnung $|\lambda_p|$ hat,*
- *längs $I_\gamma\,((T_p\,\tau_0) \times E)$ und $E \times I_\gamma\,(T_p\,\tau_0))$ Pole der Ordnung 1 hat,*
- *längs $\triangle\,(E)$ eine λ_p-fache Polstelle hat*

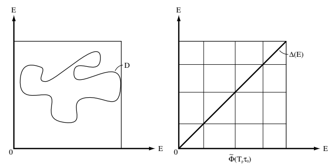

Abbildung 7.3:

- *sonst überall holomorph ist*

Es gilt $k\,(-u_1,-u_2) = k\,(u_1,u_2) = k(u_1,u_2)$ *für alle* $u_1, u_2 \in E$.

Beweis. Wir zeigen zunächst, dass für alle $\tau \in H$

$$\int_{p\,\tau_0}^{p\,\tau} \gamma\,(z)\,d\,z + \sum_{r=0}^{p-1} \int_{\frac{\tau_0+r}{p}}^{\frac{\tau+r}{p}} \gamma\,(z)\,d\,z - \lambda_p \int_{\tau_0}^{\tau} \gamma\,(z)\,d\,z = 0 \quad (*) \tag{7.12}$$

Zum Beweis differenzieren wir die linke Seite der Gleichung nach τ. Es ergibt sich nach dem Hauptsatz der Differential- und Integralrechnung

$$p \cdot \gamma\,(p\,\tau) + \sum_{r=0}^{p-1} \frac{1}{p} \gamma\,(\frac{\tau+r}{p}) \; - \lambda_p \gamma\,(\tau) = T_p\,\gamma\,(\tau) \; - \lambda_p\,\gamma\,(\tau) = 0$$

Also ist die linke Seite von (7.12) unabhängig von τ. Setzt man $\tau = \tau_0$, so folgt (7.12).

Ist $n_1\,p_1 + \cdots + n_r\,p_r \quad (n_i \in \mathbb{Z}\,, p_i \in H)$ ein Element der freien abel'schen Gruppe über H, so sei $I_\gamma\,(n_1\,p_1 + \cdots + n_r\,p_r) := n_1\,I_\gamma\,(p_1) \; + \cdot\, n_r\,I_\gamma\,(p_1)$, wobei die Addition auf der rechten Seite in dem Torus $E = \mathbb{C}\,/\mathbb{Z}\,\omega_1 \,\oplus\, \mathbb{Z}\,\omega_2$ erfolgt. Nach Konstruktion von I_γ folgt aus (7.12) und Korollar 7.5.3,

$$I_\gamma\,(T_p\tau) - I_\gamma\,(T_p\tau_0) - \lambda_p\; I_\gamma\;(\tau)\; + \lambda_p\; \cdot 0 = 0 \quad \text{in } E = \mathbb{C}\,/\mathbb{Z}\omega_1 \,\oplus\, \mathbb{Z}\omega_2$$

für alle $\tau \in H$.
Nach Satz 1.3.7 gibt es also für jedes $\tau \in H$ eine meromorphe Funktion g_τ auf E mit einer λ_p-fachen Nullstelle in 0, einer einfachen Nullstelle in $I_\gamma\,(T_p\,\tau)$ und einfachen Polstellen in $I_\gamma\,(T_p\,\tau_0)$ und λ_p-fachen Polstellen in $I_\gamma(\tau)$. Ist $u = I_\gamma(\tau)$ so sei $\hat{g}_u := g_\tau$. Die Funktion $\hat{g}_u$ hat

- eine λ_p-fache Nullstelle in 0
- einfache Nullstellen in den Punkten u', für die $(u,\,u') \,\in\, K$
- einfache Polstellen in $I_\gamma\,(T_p\,\tau_0)$
- eine λ_p-fache Polstelle in u

und ist sonst holomorph.[4] Die Funktion $\hat{g}_u := g_\tau$ ist bis auf Multiplikation mit einem Skalar eindeutig bestimmt.

[4] Falls einige der genannten Punkte zusammenfallen, so müssen die Null- und Polstellen natürlich mit Multiplizität gezählt werden.

Wähle nun $\tilde{u} \in E \setminus (\{0\} \cup \Phi(T_p \tau_0))$. Für jedes $u \in E$ sei $k(u, -)$ die Vielfache der Funktion $\hat{g}_u$, die an der Stelle $\tilde{u}$ den Wert $\hat{g}_{\tilde{u}}(u)$ annimmt. Da K symmetrisch ist, hat k die gewünschten Null- und Polstellen.
Die Null- und Polstellenmengen von k sind nach Lemma 7.5.4 invariant unter der Involution $(u_1, u_2) \mapsto (-u_1, -u_2)$ auf $E \times E$. Da k durch seine Null- und Polstellenmenge eindeutig bestimmt ist, gibt es $\varepsilon \in \{\pm 1\}$, so dass $k(-u_1, -u_2) = \varepsilon\, k(u_1, u_2)$ für alle $(u_1, u_2)\, E \times E$. Betrachtet man k in einer Umgebung von $(0,0)$, so folgt $\varepsilon = +1$. Analog folgt aus Lemma 7.5.5 , dass $k(u_2, u_1) = k(u_1, u_2)$. □

Bemerkung 7.5.7 *In der Sprache der algebraischen Geometrie [Griffiths–Harris] p. 284 besagt Satz 7.5.6, dass die Korrespondenz D auf $E \times E$ Valenz $-\lambda_p$ hat.*

Korollar 7.5.8 *K scheidet $\triangle(E)$ in (mit Multiplizität gezählt) $2(p+1-\lambda_p)$ Punkten.*

Beweis. Sei d die Anzahl (mit Multiziplität gezählt) der Schnittpunkte von K mit der Diagonalen $\triangle(E)$. Wähle eine meromorphe Funktion φ auf E, die in 0 eine λ_p-fache Nullstelle hat. Die Einschränkung der Funktion $\varphi(u_1 - u_2)\, k(u_1, u_2)$ auf $\triangle(E)$ hat dann nach Satz 7.5.6

- d Nullstellen in den Punkten von $K \cap \triangle(E)$
- eine $2\lambda_p$-fache Nullstelle in $(\{0\} \times E) \cap \triangle(E) = (E \times \{0\}) \cap \triangle(E)$
- zweifache Polstellen in jedem der $p+1$ Punkte von
  $(I_\gamma(T_p\tau_0) \times E) \cap \triangle(E) = (E \times I_\gamma(T_p\tau_0)) \cap \triangle(E)$

Nach Satz 1.2.6 ist $d + 2\lambda_p = 2(p+1)$ □

Bemerkung 7.5.9 *Korollar 7.5.8 besagt, dass die Hecke-Korrespondenz $2(p+1-\lambda_p)$ Fixpunkte hat.*

Wir betrachten nun noch die exceptionellen Punkte $I_\gamma(0)$ und $I_\gamma(i\infty)$ von Lemma 7.3.4 genauer.

Lemma 7.5.10 *Die Schnittmultiplizität von K und $\Delta(E)$ in den Punkten $(I_\gamma(0), I_\gamma(0))$ und $(I_\gamma(i\infty), I_\gamma(i\infty))$ ist gleich 2.*

Beweis. Wir beweisen diese Aussage für den Punkt $(I_\gamma(i\infty), I_\gamma(i\infty))$. Sei $\kappa_\infty : U_0 \longrightarrow U_\infty$ die biholomorphe Abbildung zwischen einer Umgebung U_0 von 0 in $\mathbb{C}$ und einer Umgebung U_∞ von $I_\gamma(i\infty)$ in E, die in Lemma 7.3.4 beschrieben wird. Nach Korollar 7.5.3 ist $K \cap (U_\infty \times U_\infty)$ die Vereinigung der Bilder von U_0 unter den beiden Abbildungen

$$\begin{aligned} z &\longmapsto (\kappa_\infty(z), \kappa_\infty(z^p)) \qquad \text{und} \\ z &\longmapsto (\kappa_\infty(z^p), \kappa_\infty(z)) \end{aligned}$$

Daraus folgt das Lemma sofort. □

7.6 Erzeugende für das Ideal der Hecke-Korrespondenz

In Abschnitt 5 haben wir den p-ten Fourierkoeffizienten λ_p der Spitzenform γ in Zusammenhang gebracht mit der Anzahl $|\, K \cap \triangle(E)\,|$ der Fixpunkte der Korrespondenz K auf $E \times E$. (Bemerkung 7.5.9). Genauer gilt $|\, K \cap \triangle\,(E)\,| \; = 2\,(p+1-\lambda_p)$. Unser Ziel ist es, einzusehen, dass die Anzahl der Fixpunkte der Korrespondenz K gleich $2\,(N_p+1)$ ist, wobei $N_p - 1$ die Anzahl der Fixpunkte der Frobeniuskorrespondenz $\mathcal{F}_p\,(D)$ auf $D_p \times D_p$ ist (Abschnitt 3). Um dies zu tun, verwenden wir den in Satz 7.3.3 konstruierten Isomorphismus $\Psi_D \,:\, D \longrightarrow E \setminus \{I_\gamma(0), I_\gamma(i\,\infty)\}$ und setzen

$$\mathcal{K} := (\Psi_D \,\times\, \Psi_D)^{-1}\,(K)$$

Offenbar ist $\mathcal{K}$ das Bild $\mathcal{I}_p$ unter dem Isomorphismus $\Phi_D \,\times\, \Phi_D$ zwischen $H \,/\, \Gamma_0\,(11) \,\times H \,/\, \Gamma_0\,(11)$ und $D \times D$ von Satz 7.3.1. In diesem Abschnitt wollen wir u.a. zeigen, dass das Ideal $\mathcal{I}$ von $\mathcal{K}$ in $D \times D$ von Polynomen mit ganzzahligen Koeffizienten erzeugt wird. Betrachtet man diese Polynome dann modulo p, so erhält man Funktionen auf $D_p \times D_p$. Deren gemeinsame Nullstellenmenge nennen wir die Reduktion $\mathcal{K}_p$ von $\mathcal{K}$ modulo p. Im nächsten Abschnitt werden wir dann zeigen, dass $\mathcal{K}_p$ mit $\mathcal{F}_p \cup \mathcal{F}_p^*$ übereinstimmt, wobei $\mathcal{F}_p = \mathcal{F}_p\,(D)$ die Frobeniuskorrespondenz auf D aus Abschnitt 3 bezeichnet. Dies ermöglicht es dann, die Anzahl der Fixpunkte der Frobeniuskorrespondenz mit der Anzahl der Fixpunkte der Hecke-Korrespondenz zu vergleichen.

Die Idee, Gleichungen für $\mathcal{K}$ zu konstruieren, ist folgende: Falls $p \;=\; \Phi_D(\tau) \;\in\, D$, so ist

$$\begin{aligned} \mathcal{K} \cap (\,\{p\} \,\times\, D) \;&=\; \{p\} \,\times\, \Phi_D\,(T_p\,\tau)\,\} \\ &= \Big\{\, \big(\Phi_D(\tau)\,,\, \Phi_D(p\,\tau)\big)\,,\, \big(\Phi_D(\tau)\,,\, \Phi_D(\tfrac{\tau}{p})\big)\,,\, \cdots\,,\, \big(\Phi_D\,(\tau)\,,\, \Phi_D\,(\tfrac{\tau+p-1}{p})\big) \Big\} \end{aligned}$$

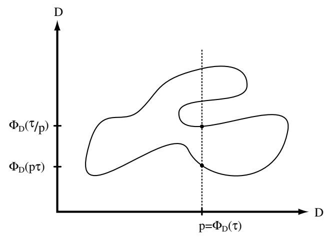

Abbildung 7.4:

Ist φ eine meromorphe Funktion auf D, so ist $f \,:=\, \varphi \circ \Phi$ eine Modulfunktion. Die Werte von φ an den Stellen $\Phi_D\,(T_p\,\tau)$ sind $f\,(p\,\tau)\,;\, f\,(\frac{\tau}{p})\,, \cdots, f\,(\frac{\tau+p-1}{p})$. Bezeichnet σ_j das j-te elementarsymmetrische Polynom in $p\,+\,1$ Variablen

$$x^{p+1} - \sigma_1\,(x_0, \cdots, x_p)\,x^p - \cdots - \sigma_{p+1}\,(x_0, \cdots, x_p) \;=\; \prod_{i=0}^{p}\,(x - x_i))$$

so sind die Werte von φ an den Stellen $\Phi_D\,(T_p\,\tau)$ die Nullstellen von

$$x^{p+1} - s_1\,x^p - \cdots - s_{p+1}$$

mit $s_j = \sigma_j\,(f\,(p\,\tau)\,,\, f\,(\frac{\tau}{p})\,,\, \ldots\,,\, f\,(\frac{\tau+p-1}{p}))$.

Lemma 7.6.1 *Sei $f(\tau)$ eine $\Gamma_0(11)$-invariante holomorphe Funktion. Für $j = 1, \ldots, p+1$ sind*

$$\tau \longmapsto \sigma_j \left(f(p\,\tau)\ , f(\frac{\tau}{p}), \ldots, f(\frac{\tau+p-1}{p}) \right) \tag{7.13}$$

$\Gamma_0(11)$-invariante Funktionen. Hat f nur ganzzahlige Fourierkoeffizienten, so gilt das auch für die Funktionen in (7.13).

Beweis. Da T_p auf $H\,/\,\Gamma_0\,(11)$ definiert ist, ist klar, dass symmetrische Funktionen von $f\,(T_p\,\tau)$ wieder $\Gamma_0\,(11)$-invariant sind. Hat f nur ganzzahlige Fourierkoeffizienten, so ist

$$(x - f(p\,\tau)) \cdot \prod_{\tau=0}^{p-1} \left(x - f\,(\frac{\tau + r}{p}) \right)$$

ein Polynom in x, dessen Koeffizienten Reihen in $e^{2\pi i\,\tau/p}$ sind, deren Koeffizienten jeweils ganze Zahlen sind. Da der Koeffizient von x^j schwach modular ist, sind die Koeffizienten bei $e^{2\pi i\,j/p}$, $j \notin p\,\mathbb{Z}$ gleich Null. □

Satz 7.6.2 *Sei $\varphi\,(u,\,v) \;=\; \varphi_0\,(u) \;+ v\,\varphi_1\,(u)$, wobei $\varphi_0,\,\varphi_1$ Polynome in einer Variablen mit ganzzahligen Koeffizienten sind. Dann gibt es ein Polynom G_φ in drei Variablen mit ganzzahligen Koeffizienten, so dass für alle $(u,\,v)\;\in D$ die Nullstellenmenge von*

$$w \mapsto G_\varphi\,(w,\,u,\,v)$$

gleich der Menge $\{\varphi\,(u',\,v')\,/\,((u,\,v)\,,\,(u',\,v'))\;\in \mathcal{K}\}$ der Werte von φ auf dem Bild von $(u,\,v)$ unter der Korrespondenz $\mathcal{K}$ ist.

Beweis. Setze $f(\tau) := \varphi\,(U(\tau),\,V(\tau))$. Dies ist eine holomorphe $\Gamma_0(11)$-invariante Funktion. Nach Lemma 7.6.1 gibt es holomorphe $\Gamma_0(11)$-invariante Funktionen $f_1, \cdots, f_{p+1}$ mit ganzzahligen Fourierkoeffizienten, so dass $(w - f(p\,\tau)) \cdot \prod_{r=0}^{p-1}(w - f\,(\frac{\tau+r}{p})) = w^{p+1} + f_1(\tau)\,w^p + \cdots + f_{p+1}(\tau)$. Nach Satz 7.3.2 ist

$$f_j(\tau) = P_j(U(\tau)) + v(\tau)\,Q_j\,(U(\tau))$$

mit ganzzahligen Polynomen P_j , Q_j. Wir setzen

$$G_\varphi(w,\,u,\,v) := w^{p+1} + \sum_{j=0}^{p} (P_{j+1}\,(u) \;+ v\,Q_{j+1}\,(u))\,w^{p+j}$$

□

Wir bezeichnen mit $\mathcal{I}$ das Ideal aller polynomialen Funktionen auf $D\,\times\,D$, die auf $\mathcal{K}$ verschwinden.

Satz 7.6.3 *$\mathcal{I}$ wird von den Polynomen $G_\varphi(\varphi(u_2, v_2),\,u_1,\,v_1)$ mit $\varphi(u,\,v) = \varphi_0(u) + v\,\varphi_1(v)$; $\varphi_0, \varphi_1 \in \mathbb{Z}\,[u]$, erzeugt.*

Beweis. Nach Satz 7.6.2 sind die Funktionen $G_\varphi(\varphi(u_2,\,v_2)\,u_1,\,v_1)$ auf Punkten von $\mathcal{K}$ gleich Null, liegen also in $\mathcal{I}$. Ist $((u_1, v_1),\,(u_2, v_2))\;\in\,\mathcal{K}$, so wähle eine Funktion φ mit $\varphi\,(u_2,\,v_2) \neq \varphi\,(u_2',\,v_2')$ für alle $(u_2',\,v_2')e\,D$ mit $((u_1, v_1),\,(u_2',\,v_2'))\;\in \mathcal{K}$.

Dann ist (wieder nach Satz 7.6.2) $G_\varphi(\varphi(u_2, v_2), (u_1, v_1)) \neq 0$. Aus diesen Überlegungen folgt, dass die gemeinsame Nullstellenmenge der Funktionen

$$\begin{aligned} D \times D &\longrightarrow \mathbb{C} \\ ((u_1 v_1), (u_2 v_2)) &\longmapsto G_\varphi(\varphi(u_2, v_2), u_1, v_1) \end{aligned}$$

gleich $\mathcal{K}$ ist. Nach dem Hilbert'schen Nullstellensatz ist also $\mathcal{I}$ das Radikalideal des von den $G_\varphi(\varphi(u_2, v_2))$ erzeugten Ideals $\mathcal{I}'$. Man kann nachprüfen, dass es für jeden glatten Punkt von $\mathcal{K}$ ein φ gibt, so dass $G_\varphi(\varphi(u_2, v_2)$ in diesem Punkt mit Multiplizität 1 verschwindet. Daraus folgt, dass $\mathcal{I} = \mathcal{I}'$. □

Bemerkung 7.6.4 *Die Abbildung ψ_D von Satz 7.3.3 ist ein Isomorphismus zwischen D und $E \setminus \{I_\gamma(0), I_\gamma(i\infty)\}$. Es folgt also aus Bemerkung 7.5.9 und Lemma 7.5.10, dass die Korrespondenz $\mathcal{K}$ auf D gerade $2(p - \lambda_p - 1)$ Fixpunkte hat. Genauer gesagt: Bezeichnet*

$$\triangle(D) := \{((u_1, v_1), (u_2, v_2)) \in D \times D \,/\, u_1 = u_2 \text{ und } v_1 = v_2\},$$

so besteht $\mathcal{K} \cap \triangle(D)$ aus (mit Multiplizität gezählt) $2(p - \lambda_p - 1)$ Punkten. Nach Konstruktion sind diese Punkte die gemeinsamen Nullstellen aller Polynome $G_\varphi(\varphi(u, v), u, v))$.

7.7 Die Kronecker - Weber'sche Kongruenzrelation

In Abschnitt 6 hatten wir jedem ganzzahligen Polynom $\varphi(u, v) = \varphi_0(u) + v\,\varphi_1(u)$ das ganzzahlige Polynom $G_\varphi(w, u, v)$ zugeordnet, dessen Nullstellen für festes (u, v) gerade die Werte von φ auf dem Bild von (u, v) unter der Hecke-Korrespondenz sind.

Satz 7.7.1 *Sei $\varphi(u, v) = \varphi_0(u) + v\,\varphi_1(u)$ ein ganzzahliges Polynom. Dann ist*

$$G_\varphi(w, u, v) \equiv (w - \varphi(u, v)^p) \cdot (w^p - \varphi(u, v))$$

modulo p.

Korollar 7.7.2 *Es sei*

$$\mathcal{F}_p(D) := \{ ((u_1, v_1), (u_2, v_2)) \in D_p \times D_p \,/\, u_2 = u_1^p \text{ und } v_2 = v_1^p \}$$

die Frobeniuskorrespondenz auf $D_p \times D_p$, und

$$\mathcal{F}_p^*(D) := \{ ((u_1, v_1), (u_2, u_2)) \in D_p \times D_p \,/\, u_2^p = u_1 ,\, v_2^p = v_1$$

die Duale der Frobeniuskorrespondenz. Dann erzeugen die Restklassen der Polynome $G_\varphi(\varphi(u_2, v_2), u_1, v_1)$ das Ideal von

$$\mathcal{F}_p(D) \cup \mathcal{F}_p^*(D) \text{ in } D_p \times D_p$$

Beweis. des Korollars: Mit Hilfe des binomischen Lehrsatzes sieht man, dass für alle Polynome $\varphi(u, v)$ mit Koeffizienten in $\mathbb{F}_p$

$$\varphi(u, v)^p = \varphi(u^p, v^p)$$

Also ist

$$G_\varphi(\varphi(u_2, v_2), u_1, v_1) \equiv (\varphi(u_2, v_2) - \varphi(u_1^p, v_1^p)) \cdot (\varphi(u_2^p, v_2^p) - \varphi(u_1, v_1)).$$

Der Beweis ist nun ähnlich wie der von Satz 7.6.3 □

Zum Beweis von Satz 7.7.1 benutzen wir

Lemma 7.7.3 *Sei*

$$f(\tau) = \sum_n c_n \, e^{2\pi\, i\, n\, \tau}$$

eine Fourierreihe mit ganzzahligen Koeffizienten c_n.

i) $f(\tau)^p - f(p\,\tau)$ *hat durch* p *teilbar Fourierkoeffizienten.*

ii) $f(\tau) - \prod_{r=0}^{p-1} f(\frac{\tau+r}{p})$ *hat durch* p *teilbare Fourierkoeffizienten.*

iii) Sind $\sigma_1, \cdots, \sigma_{p-1}$ *die ersten* $p-1$ *elementarsymmetrischen Polynome in* p *Variablen, so haben* $\sigma_j\left(f(\frac{\tau}{p}), \cdots, f(\frac{\tau+p-1}{p})\right)$ *durch* p *teilbare Fourierkoeffizienten.*

Beweis. (i) Nach dem binomischen Lehrsatz ist

$$f(\tau)^p = \sum c_n^p \, e^{2\pi i\, n\, p\tau} + \quad \text{(Terme mit durch } p \text{ teilbaren Fourierkoeffizienten)}$$

Ausserdem ist nach dem kleinen Satz von Fermat $c_n^p - c_n = c_n\,(c_n^{p-1} - 1)$ durch p teilbar.

ii) Setze $\zeta = e^{2\pi i/p}$. Dann ist

$$\begin{aligned} f(\tfrac{\tau+r}{p}) \quad &= \sum c_n \, \zeta^{n\,r} \, e^{2\pi\, i\, n\, \tau\, /\, p} \\ \Rightarrow \prod_{r=0}^{p-1} f\left(\tfrac{\tau+r}{p}\right) \quad &= \sum_m \sum_{n_0+\cdots+n_{p-1}=m} c_{n_0} \cdots c_{n_{p-1}} \, e^{\frac{2\pi\, i\, \tau}{p} m} \, \zeta^{n_1+2\,n_2+\cdots(p-1)n_{p-1}} \end{aligned}$$

Für $m \in \mathbb{N}$ sei

$$I(m) := \{\, (n_0, \cdots, n_{p-1}) \,/\, n_0 + \cdots + n_{p-1} = m \;;\;\; n_0, \cdots, n_{p-1} \text{ nicht alle gleich} \,\}$$

Dann ist

$$\begin{aligned} \prod_{r=0}^{p-1} f(\frac{\tau+r}{p}) \quad &= \quad \sum_m \sum_{(n_0,\ldots,p_{p-1})\,\in I(m)} c_{n_0} \ldots c_{n_{p-1}} \, e^{2\pi i \frac{m}{p}\tau} \, \zeta^{0 n_0 + 1 n_1 + \ldots\,(p-1)\, n_p} \\ &+ \quad \sum_n c_n^p \, e^{2\pi i \tau n} \, \zeta^{n\cdot(0+1+\cdots+(p-1))} \end{aligned} \tag{7.14}$$

Da $c_n^p \equiv c_n \mod p$ nach dem kleinen Satz von Fermat und $\zeta^{n\,(0+1+\ldots p-1)} = \zeta^{n\,p\,\frac{p-1}{2}} = 1$, hat die Differenz

$$\sum_n c_n^p \, e^{2\pi i \tau n} \zeta^{n\cdot(0+1+\cdots+(p-1))} - f(\tau)$$

durch p teilbare Fourierkoeffizienten.

Die zyklische Gruppe $\mathcal{Z}$ der Ordnung p operiert auf $I(m)$ durch Vertauschung. Da p prim ist, ist diese Operation ist fixpunktfrei. Ist $(n_0, \ldots, n_{p-1}) \in I\,(m)$ so liegt $(n'_0, \ldots, n'_p)$ im $\mathcal{Z}$-Orbit von $(n_0, \ldots, n_{p-1})$ genau dann, wenn es k gibt, so dass $n'_i = n_{i+k}$ (Indizies mod n). In diesem Fall ist $c_{n_0} \ldots c_{n_{p-1}} = c_{n'_0} \ldots c_{n'_{p-1}}$ und

$$\begin{aligned} (0\cdot n_0 + 1\cdot n_1 + \cdots + (p-1)\, n_{p-1}) \;-\; (0\cdot n'_0 + 1\cdot n'_1 + \cdots + (p-1) n'_{p-1}) \\ \equiv k\cdot\,(n_0 + \cdots + n_{p-1}) \;\equiv k\cdot m \mod p. \end{aligned}$$

Folglich ist

$$\sum_{\substack{(n'_0,\dots,n'_{p-1})\\ \text{im } \mathbb{Z}\text{-Orbit}\\ \text{von } (n_0,\dots,n_p)}} c_{n'_0}\cdots c_{n'_{p-1}}\,\zeta^{0\cdot n'_0+\cdots+0n'_{p-1}} = c_{n_0}\cdots c_{n_{p-1}}\cdot\zeta^{n_1+2n_2+\cdots+(p-1)\,n_{p-1}}\sum_{k=0}^{p-1}\zeta^{k\cdot m}$$

Nun ist

$$\sum_{k=0}^{p-1}\zeta^{k\,m} = \begin{cases} 0 \text{ für } m & \neq 0 \mod p \\ p \text{ für } m & \not\equiv 0 \mod p \end{cases}$$

Der erste Term auf der rechten Seite von (7.14) hat also durch p teilbare Fourierkoeffizienten.

iii) Sei $1 \leq j \leq p-1$ fest. Dann ist

$$f(\frac{\tau}{p})^j = \sum_n \sum_{0\leq\nu\leq p-1} b_{n,\nu}\,\zeta^\nu e^{\frac{2\pi i n}{p}\tau}$$

wobei $b_{n,\nu}$ nur von den c_n abhängt. $f(\frac{\tau+r}{p})^j$ entsteht aus $f(\frac{\tau}{p})^j$, indem man ζ durch ζ^r ersetzt. Folglich ist

$$\sum_{r=0}^{p-1} f(\frac{\tau+r}{p})^j = \sum_n \sum_{0\leq\nu\leq p-1} b_{n,\nu}\,e^{\frac{2\pi i n}{p}\tau}\cdot\sum_{r=0}^{p-1}\zeta^{r\nu}$$

Wiederum hat $\sum_{r=0}^{p-1} f(\frac{\tau+r}{p})^j$ durch p teilbare Fourierkoeffizienten. Da in $\mathbb{F}_p$ das elementarsymmetrische Polynom $\sigma_j\,(x_0,\cdots,x_{p-1})$ als Polynom in $(x_0+\cdots+x_{p-1})$, ... , $(x_0^j+\cdots+x_{p-1}^j)$ geschrieben werden kann (vgl. [Weber], §46) folgt die Behauptung. □

Beweis von Satz 7.7.1: Sei $\varphi(u,v) = \varphi_0(u) + v\varphi_1(u)$ ein ganzzahliges Polynom. Setze $f(\tau) := \varphi(U(\tau),V(\tau))$. Dann ist $f(\tau)$ eine $\Gamma_0(11)$-invariante holomorphe Funktion mit ganzzahligen Fourierkoeffizienten. Wir setzen

$$s_j\,(\tau) := \frac{1}{p}\,\sigma_j\big(f(\frac{\tau}{p}),\cdots,f(\frac{\tau+p-1}{p})\big) \quad ,j=1,\dots,p-1$$

Nach Teil (iii) von Lemma 7.7.3 hat s_j ganzzahlige Fourierkoeffizienten. Dann ist

$$\begin{aligned}
G_\varphi(w, \quad & U(\tau),V(\tau)) = \\
= \quad & (w-f(p\,\tau)\,)\cdot\Big(w^p - p\,s_1(\tau)\,w^{p-1} - \cdots - p\,s_{p-1}(\tau)\,w - \prod_{r=0}^{p-1} f(\frac{\tau+r}{p})\Big) \\
= \quad & w^{p+1} - \big[f(p\,\tau) + p\,s_1(\tau)\big]\,w^p \\
& +p\,\big[s_1(\tau)\,f(p\,\tau) - s_2(\tau)\big]\,w^{p-1} + \cdots + p\,\big[s_{p-2}(\tau)f(p\tau) - s_{p-1}(\tau)\big]\,w^2 \\
& +\big[p\,s_{p-1}(\tau)\,f(p\,\tau) - \prod_{r=0}^{p-1} f(\frac{\tau+r}{p})\big]\,w \;+\; f(p\,\tau)\prod_{r=0}^{p-1} f(\frac{\tau+r}{p}).
\end{aligned}$$

Für $j = 1, \ldots, p-2$ sind die Funktionen

$$s_j(\tau)\, f(p\,\tau) - s_{j+1}(\tau)$$

$\Gamma_0(11)$-invariant, holomorph auf H, und sie haben ganzzahlige Fourierkoeffizienten. Dasselbe gilt nach Teil (i) und (ii) von Lemma 7.7.3 auch für

$$\frac{1}{p}\big[f(p\tau)\ + p\, s_1(\tau) - f(\tau)^p\big]$$

$$\frac{1}{p}\big[p\, s_{p-1}\, f(p\tau) - \prod_{r=0}^{p-1} f(\frac{\tau+r}{p})\ + f(\tau)\big]$$

$$\frac{1}{p}\big[f(p\tau) \prod_{r=0}^{p-1} f(\frac{\tau+r}{p})\ -\ f(\tau)^{p+1}\big]\ =$$

$$\frac{1}{p}\big[f(p\tau) - f(\tau)^p\big] \prod_{r=0}^{p-1} f(\frac{\tau+r}{p})\ +\ \frac{1}{p}\, f(\tau)^p \big[\prod_{r=0}^{p-1} f(\frac{\tau+r}{p}) - f(\tau)\big]$$

Nach Satz 7.3.2 gibt es also ganzzahlige Polynome $g_1(u,\, v), \ldots, g_{p+1}(u,\, v)$, so dass

$$\begin{aligned} G_\varphi(w,\, U(\tau),\, V(\tau)) \quad &= \quad w^{p+1} - f(\tau)^p\, w^p - f(\tau)\, w - f(\tau)^{p+1} \\ &+ \quad p \cdot [\, g_1(U(\tau)\,, V(\tau))\, w^p + \cdots + g_{p+1}(U(\tau),\, V(\tau))\,] \end{aligned}$$

Folglich ist

$$G_\varphi(w,\, u,\, v)\ =\ (w - \varphi(u,\, v)^p\,)\,(w^p - \varphi(u,\, v))\ +\ p\,[\, g_1(u,\, v)\, w^p + \cdots + g_{p+1}(u,\, v)\,]$$

□

Satz 7.6.3 zeigt, dass die Polymome $G_\varphi(\varphi(u_2, v_2),\, u_1,\, v_1)$ mit $\varphi(u,\, v) = \varphi_0(u) + v\, \varphi_1(v)$; $\varphi_0,\, \varphi_1 \in \mathbb{Z}[u]$ das Ideal $\mathcal{I}$ der Hecke-Korrespondenz erzeugen. Nach Korollar 7.7.2 erzeugen ihre Restklassen modulo p das Ideal $\mathcal{I}_p$ von $\mathcal{F}_p(D) \cup \mathcal{F}_p^*(D)$. Es ist einleuchtend – aber nicht trivial zu beweisen (siehe Übung 7.7.4) – dass die Schnittmultipizität der Hecke-Korrespondenz mit der Diagonalen $\Delta(D)$ gleich der Schnittmultipizität der Nullstellenmenge von $\mathcal{I}_p$ mit $\Delta(D_p)$ ist, dass heisst

$$\sharp\ \mathcal{K} \cap \Delta(D)\ \ =\ \sharp\ (\mathcal{F}_p(D) \cup \mathcal{F}_p^*(D)) \cap \Delta(D_p) =\ \ 2\sharp\ \mathcal{F}_p(D) \cap \Delta(D_p)$$

(mit Multiplizitäten gezählt). Nach Bemerkung 7.6.4 und (7.9) würde daraus

$$2(N_p - 1) = 2(p - \lambda_p - 1)$$

also

$$N_p = p - \lambda_p$$

folgen.

Übung 7.7.4 Finde ein Polynom $f(x,y) \in \mathbb{Z}[x,y]$ so dass $\{(x,y) \in \mathbb{C}^2 \,|\, f(x,y) = 0\}$ aus unendlich vielen Punkten besteht, während $\{(x,y) \in \overline{\mathbb{F}}_p^2 \,|\, f(x,y) = 0\} = \emptyset\,$!

Literaturverzeichnis

[Ahlfors] L. Ahlfors: *Complex Analysis.* Mc Graw–Hill 1979

[Apostol] T. Apostol: *Modular Functions and Dirichlet Series in Number Theory.* Springer 1976 / 1990

[Conway] J. Conway: *Monsters and Moonshine.* Math. Intelligencer 2 (4), 165-171 (1980)

[DDT] H. Darmon, F. Diamond, R. Taylor: *Fermat's last theorem.* In: Current Developments in Mathematics 1995; Herausgeber R.Bott, A.Jaffe, S.T.Yau. International Press 1994

[Dym–McKean] H. Dym, H. Mc Kean: *Fourier Series and Integrals.* Academic Press 1972

[Eichler 1954] M. Eichler: *Quaternäre quadratische Formen und die Riemann'sche Vermutung für die Kongruenzzetafunktion.* Arch. Math. 5, 355-366 (1954)

[Eichler 1963] M. Eichler: *Einführung in die Theorie der algebraischen Zahlen und Funktionen.* Birkhäuser 1963

[Ford] L. Ford: *Automorphic Functions.* Mc Graw-Hill 1929, Chelsea Reprint 1951

[Griffiths–Harris] Ph. Griffiths, J. Harris: *Principles of Algebraic Geometry.* J. Wiley & Sons, 1978

[Igusa] J. Igusa: *Kroneckerian Model of fields of elliptic modular functions.* Amer. J. Math. 81, 436-453 (1959)

[Kanigel] R. Kanigel: *Der das Unendliche kannte. Das Leben des genialen Mathematikers Srinivasa Ramanujan.* Vieweg Verlag 1993

[Koecher–Krieg] M. Koecher, A. Krieg: *Elliptische Funktionen und Modulfunktionen* Springer 1998

[Klein] F. Klein: *Vorlesungen über die Theorie der elliptischen Modulfunktionen II.* Leipzig 1892

[Knopp] M. Knopp: *Modular Functions in Analytic Number Theory.* Markham Publishing Company, 1970

[Kramer] J. Kramer: *Über die Fermat-Vermutung.* El. Math. 50, 12-25 (1995)

[Lehner] J. Lehner: *Discontinuous Groups and Automorphic Functions.* AMS 1964

[Mumford] D. Mumford: *Tata Lectures on Theta I.* Birkhäuser 1983

[Ribet] K. Ribet: *Galois Representations and Modular Forms.* Bull. AMS 32, 375-402 (1995)

[Sarnak] P. Sarnak: *Some Applications of Modular Forms.* Cambridge University Press, 1990

[Serre] J. P. Serre: *Cours d'Arithmétique.* Presses Universitaires de France, 1970 (englische Ausgabe: A Course in Arithmetic. Springer, 1973)

[Shimura] G. Shimura: *Introduction to the Arithmetic Theory of Automorphic Functions.* Princeton University Press, 1971

[Tate] J. Tate: *The Arithmetic of Elliptic Curves.* Inventiones Math. 23, 179-206 (1974)

[Titchmarsh] E. Titchmarsh: *The Theory of the Riemann Zeta–function* Second Edition, revised by D. Heath–Browm. Oxford University Press 1986.

[Weber] H. Weber: *Lehrbuch der Algera I.* Chelsea Reprint

[Weil] A. Weil: *Elliptic Functions according to Eisenstein and Kronecker.* Springer Verlag, 1976

[Wuestholz] G. Wüstholz: *Elliptische Kurven, Modulkurven, Galoisdarstellungen und ihr Zusammenhang mit der Fermat'schen Vermutung.* Skript, ETH Zürich 1995