Über die Nullstellen von Hecke-Eigenformen

Diplomarbeit, korrigiert

Humboldt-Universität zu Berlin
Mathematisch-Naturwissenschaftliche Fakultät II
Institut für Mathematik

eingereicht von: Christian Martin Schön
geboren am: 04. August 1978 in Berlin
1. Gutachter: Prof. Ulf Kühn
2. Gutachter: Prof. Rolf-Peter Holzapfel
Berlin, den 5. April 2007

Inhaltsverzeichnis

0 Einführung

Die vorliegende Arbeit beschäftigt sich mit Modulformen; das sind komplexwertige Funktionen auf der oberen Halbebene, die gewisse Funktionalgleichungen bezüglich einer diskret operierenden Gruppe erfüllen. Aufgrund ihrer arithmetischen Eigenschaften schaffen sie eine Schnittstelle zwischen komplexer Analysis und Zahlentheorie. Die sogenannten Hecke-Eigenformen sind ausgezeichnete Modulformen zur Modulgruppe $\Gamma(1) = SL_2(\mathbb{Z})/\{\pm 1\}$.
Die Nullstellen der Hecke-Eigenformen zur Gruppe $\Gamma(1)$ sind der Gegenstand dieser Arbeit. Einige dieser Nullstellen lassen sich direkt aus einer einfachen Größe, dem Gewicht der Hecke-Eigenform ablesen und sind bekannt; diese Arbeit thematisiert jedoch die anderen, die nichttrivialen. Die Anzahl der nichttrivialen Nullstellen einer Hecke-Eigenform kann mit einer expliziten Formel aus der Theorie der Modulformen allein aus dem Gewicht der Hecke-Eigenform berechnet werden. Zwei Arten von Hecke-Eigenformen werden unterschieden: Eisensteinreihen und Hecke-Spitzenformen.
Im Fall der Eisensteinreihen ist bereits vieles bekannt. So besagt der Satz von Rankin-Swinnerton-Dyer, daß die nichttrivialen Nullstellen der Eisensteinreihen einfach sind und im Schnitt des Einheitskreises mit dem Rand des Fundamentalbereiches liegen. Darauf aufbauend zeigte W. Kohnen, daß die nichttrivialen Nullstellen der Eisensteinreihen transzendent sind und gibt eine explizite Formel zur Berechnung der Nullstellen an.
Im Fall der Hecke-Spitzenformen ist weniger bekannt. Z. Rudnick hat gezeigt, daß unter der Annahme der verallgemeinerten Riemannschen Vermutung die Nullstellen einer Hecke-Spitzenform zum Gewicht k für $k \to \infty$ bezüglich des hyperbolischen Maßes im Fundamentalbereich gleichverteilt sind. Dies macht ein Ergebnis analog zum Satz von Rankin-Swinnerton-Dyer natürlich unmöglich. Ob die nichttrivialen Nullstellen der Hecke-Spitzenformen transzendent sind oder nicht ist im allgemeinen noch unklar. Die Ähnlichkeit zwischen der Verteilung der nichttrivialen Nullstellen der Hecke-Spitzenformen und der Verteilung der CM-Punkte motiviert jedoch die naive Frage, ob es da einen Zusammenhang geben könnte oder ob diese beiden Mengen gar gleich sind.
Eine leichte Überlegung zeigt, daß die j-Werte der Nullstellen von Hecke-Eigenformen algebraisch sind, woraus mithilfe eines Satzes von M. Waldschmidt folgt, daß die Nullstellen dann entweder imaginärquadratisch oder transzendent sind.
Jedem Punkt der oberen Halbebene ist eine elliptische Kurve zugeordnet. Ein Punkt ist genau dann imaginärquadratisch, wenn die ihm zugeordnete elliptische Kurve komplexe Multiplikation hat. So ist das Problem, die Algebraizität der Nullstelle zu testen, umformulierbar zu der Fragestellung, ob

die zugehörige Kurve komplexe Multiplikation hat. J. Achter hat einen deterministischen Test entworfen, der prüft, ob eine elliptische Kurve über einem Zahlkörper komplexe Multiplikation hat.
In dieser Arbeit werden die nichttrivialen Nullstellen der Hecke-Spitzenformen zum Gewicht 24, 28, 30, 32, 34 und 38 untersucht. Das Hauptergebnis dieser Arbeit ist folgender

Satz. *Die nichttrivialen Nullstellen der Hecke-Spitzenformen zur Gruppe* $\Gamma(1)$ *und zu den Gewichten* 24, 28, 30, 32, 34 *und* 38 *sind transzendent.*

Neben dem Nachweis der Transzendenz werden auch die numerischen Näherungen der Nullstellen, sowie ihre exakten j-Werte gegeben.
Dieselbe Methode ist auch geeignet, die nichttrivialen Nullstellen der Hecke-Eigenformen zur Kongruenzuntergruppe $\Gamma_0(2)$ zu untersuchen, was in dieser Arbeit eine nachgeordnete Rolle spielt, aber die Frage aufwirft, ob es möglich wäre, in gleicher Weise die nichttrivialen Nullstellen von Hecke-Spitzenformen zur Kongruenzuntergruppe $\Gamma_0(N)$ für höhere Level N zu untersuchen. So gibt es z. B. ab dem Level $N = 11$ Hecke-Spitzenformen vom Gewicht $k = 2$, deren nichttriviale Nullstellen die Verzweigungspunkte der modularen Parametrisierung und deswegen wichtig sind.

An dieser Stelle möchte ich jenen herzlich Dank sagen, die zum Gelingen dieser Arbeit beigetragen haben, besonders Herrn Prof. Ulf Kühn, der meine Arbeit engagiert betreute und dessen Tür für meine Fragen stets offen stand, sowie Herrn Prof. Rolf-Peter Holzapfel für seine hilfreichen Hinweise und nicht zuletzt Herrn Dr. Jeff Achter, für seinen freundlichen und sachkundigen Rat.

1 Elliptische Kurven

In diesem Kapitel werden wir uns mit elliptischen Kurven beschäftigen. Zuerst definieren wir die elliptischen Kurven mit der Weierstraßschen Normalform. Dann erklären wir die Gruppenstruktur auf einer elliptischen Kurve und ihre Reduktion modulo p. Zuletzt erfolgt die Beschreibung einer elliptischen Kurve durch ihr Gitter und die Einführung der Weierstraßschen $\wp$-Funktion. Wir werden uns eng an das Buch von A. Knapp [Kn] halten.

1.1 Grundlegende Definitionen

Definition 1.1. *Eine Kubik E mit Koeffizienten aus dem Körper k, kurz E/k ist in Weierstraß-Normalform, wenn sie als Nullstellenmenge folgenden Polynoms in x, y gegeben ist:*

$$y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 \quad \textit{wobei } a_i \in k$$

Homogenisiert man dieses Polynom, so sieht man, daß der einzige Punkt dieser Kurve auf der unendlich fernen Gerade der Punkt $O := (0 : 1 : 0)$ ist. Die Kurve ist in diesem Punkt nicht singulär und hat dort die unendlich ferne Gerade als Tangente.
Seien weiter:

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \end{aligned}$$

Diese b_i benötigen wir, um folgende wichtige Konstanten zu definieren:

Definition 1.2. *Die Diskriminante Δ der Kurve E/k ist gegeben als:*

$$\Delta := -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

Der j-Wert der Kurve E/k ist gegeben als:

$$j = \frac{(b_2^2 - 24b_4)^3}{\Delta}$$

Satz 1.3. *Die Kurve E/k ist singulär genau dann, wenn $\Delta(E) = 0$.*

Beweis: siehe [Kn] Thm 3.2. □

Definition 1.4. *Eine elliptische Kurve E/k ist eine nichtsinguläre Kubik über k in Weierstraß-Normalform.*

Satz 1.5. *Sei k ein Körper mit $\mathrm{char}(k) \notin \{2,3\}$. Zu jedem $j_0 \in k$ existiert eine elliptische Kurve über k mit j-Wert j_0.*
Ist $k = \overline{k}$, dann sind zwei elliptische Kurven mit gleichem j-Wert isomorph.

Beweis: siehe [Kn] Thm 3.7.
Für $j_0 \notin \{0, 1728\}$ definieren wir

$$E_{j_0} : \; y^2 = x^3 - \frac{27}{4}\frac{j_0}{j_0 - 1728}x - \frac{27}{4}\frac{j_0}{j_0 - 1728}$$

und bemerken $j(E_{j_0}) = j_0$.
Im Fall $j_0 = 0$ definieren wir

$$E_0 : \; y^2 = x^3 + 1$$

und im Fall $j_0 = 1728$ definieren wir

$$E_{1728} : \; y^2 = x^3 + x.$$

und bemerken $j(E_0) = 0$ und $j(E_{1728}) = 1728$. □

Definition 1.6. *Die Menge der k-rationalen Punkte von E/k vereinigt mit $\{\infty\}$ bezeichnen wir mit $E(k)$.*

Da das Verhalten von $E(k)$ im Punkt ∞ gut bekannt ist, beschränken wir uns gelegentlich darauf, die k-rationalen Punkte zu betrachten.

Definition 1.7. *Eine zulässige Variablentransformation $\mathbb{A}^2(k) \to \mathbb{A}^2(k)$ ist von der Form:*

$$x = u^2x' + r \text{ und } y = u^3y' + su^2x' + t, \text{ wobei } u, r, s, t \in k \text{ und } u \neq 0.$$

Bemerkung 1.8. *Geht E' aus E durch eine zulässige Variablentransformation hervor, so gilt: $j(E) = j(E')$ und $\Delta(E) = u^{12}\Delta(E')$. Deswegen sind zwei elliptische Kurven, die mittels einer zulässigen Variablentransformation ineinander überführt werden können, isomorph.*

1.2 Elliptische Kurven als Gruppen

Bemerkung 1.9. *Das Schnittverhalten zweier nicht singulärer algebraischer Kurven F, G in einem Punkt P werden wir mit einer natürlichen Zahl $i(P, F, G)$, der sogenannten Schnittmultiplizität beschreiben. Für diese gelten folgende Eigenschaften:*

1. *$i(P, F, G) = 0$, wenn sich F und G in P nicht schneiden.*
2. *$i(P, F, G) = 1$, wenn sich F und G in P transversal schneiden.*
3. *$i(P, F, G) \geq 2$, wenn sich F und G in P schneiden und dort eine gemeinsame Tangente besitzen.*

In ähnlicher Weise kann man die Schnittmultiplizität auch für singuläre Kurven definieren. Für eine ausführlichere Einführung der Schnittmultiplizität siehe [Kn] Kapitel II.3.

Nach dem Satz von Bézout ist die Summe der Schnittmultiplizitäten einer Gerade mit einer elliptischen Kurve kleiner als vier.

Lemma 1.10. *Seien E/k eine elliptische Kurve und G eine Gerade. Dann ergibt die Summe der Schnittmultiplizitäten $\sum_P i(P, G, E)$ entweder $0, 1$ oder 3, aber nie 2.*

Beweis: siehe [Kn] Prop 2.15. □

Bemerkung 1.11. *Dabei ist es in unserem Fall nicht so wichtig zu wissen, was Schnittzahl $i(P, F, G) = 3$ genau bedeutet, sondern vielmehr, daß wir zu zwei nicht notwendigerweise verschiedenen Punkten P, Q der elliptischen Kurve E/k genau einen dritten Punkt R auf E/k finden, so daß P, Q und R auf einer Geraden liegen. Dieser kann mit P oder Q koinzidieren und wäre dann ein mehrfacher Punkt. Wir schreiben $R = PQ$.*

Satz 1.12 (Poincaré)**.** *Seien k ein Körper, E/k eine elliptische Kurve und O der Punkt $(0 : 1 : 0)$.*
Dann ist $(E(k), +)$ eine abelsche Gruppe mit O als Nullelement. Die Verknüpfung ist für alle $(P, Q) \in E(k)^2$ gegeben durch: $P + Q = O(PQ)$.
Ist $k \subset K$ eine Körpererweiterung, so ist die natürliche Inklusion $E(k) \subset E(K)$ ein Gruppenhomomorphismus.

Beweis: siehe [Kn] Thm 3.8. □

Bemerkung 1.13. *Elliptische Kurven sind der eindimensionale Spezialfall abelscher Varietäten. Siehe dazu z. B. [BL] S.71.*

Satz 1.14 (Mordell-Weil)**.** *Seien K ein Zahlkörper und E/K eine elliptische Kurve. Dann ist die abelsche Gruppe $E(K)$ endlich erzeugt.*

Beweis: siehe [Si1] Kapitel VIII. □

Bemerkung 1.15. *Wir werden die Torsionsuntergruppe von $E(K)$ mit $E(K)_{tors}$ bezeichnen. Da $E(K)$ eine endlich erzeugte, abelsche Gruppe ist gilt: $E(K) \cong \mathbb{Z}^r \oplus E(K)_{tors}$. Dabei heißt $r \in \mathbb{N}$ der Rang von $E(K)$. Der Rang einer elliptischen Kurve ist eine wichtige, aber schwer zu bestimmende Invariante.*

1.3 Reduktion modulo p

Bemerkung 1.16. *Seien E/K eine elliptische Kurve und K ein Zahlkörper mit zugehörigem Ring der ganzen Zahlen $\mathcal{O}_K$. Da $K = Quot(\mathcal{O}_K)$, sind die Koeffizienten von E von der Form $a_i = \frac{\alpha_i'}{\alpha_i}$ mit α_i und α_i' aus $\mathcal{O}_K$. Nach der zulässigen Variablentransformation $E \to E'$ mit $u = \prod \alpha_i^{-1}$ und $r = s = t = 0$ (mit den Bezeichnungen aus Definition 1.7) sind die Koeffizienten der Weierstraßschen Normalform Elemente aus $\mathcal{O}_K$. Insbesondere ist dann auch die Diskriminante von E' aus $\mathcal{O}_K$. Da $\mathcal{O}_K$ ein Dedekindring ist, ist die Primzerlegung des Ideals $(\Delta(E'))$ eindeutig.*

Definition 1.17. *Seien E/K eine elliptische Kurve mit ganzen Koeffizienten, K ein Zahlkörper mit zugehörigem Ring der ganzen Zahlen $\mathcal{O}_K$ und $\mathfrak{p} \subset \mathcal{O}_K$ ein Primideal. Wir nennen diese Weierstraßsche Normalform $\mathfrak{p}$-minimal, wenn es keine zulässige Variablentransformation $E \to E'$ gibt, so daß E' ganze Koeffizienten hat und die $\mathfrak{p}$-Potenz, die $(\Delta(E'))$ teilt kleiner ist als die, die $(\Delta(E))$ teilt.*

Definition 1.18. *Seien $r \in \mathbb{Q} \setminus \{0\}$ und p eine Primzahl. Wir schreiben $r = p^n \frac{u}{v}$ mit $u, v \in \mathbb{Z}$ und $(u,p) = (v,p) = 1$. Dann definieren wir die p-adische Norm als $|r|_p := p^{-n}$. Eine Menge $A \subset \mathbb{Q}$ heißt p-reduziert, wenn für alle $a \in A$ gilt $|a|_p \leq 1$ und es ein $\overline{a} \in A$ gibt, so daß $|\overline{a}|_p = 1$.*

Bemerkung 1.19. *Jeder Punkt $P \in \mathbb{P}^2(\mathbb{Q})$ hat einen p-reduzierten Repräsentanten.*

Definition 1.20. *Zu einer elliptischen Kurve E über $\mathbb{Q}$ und einer Primzahl p definieren wir die reduzierte Kurve modulo p wie folgt: Wir multiplizieren die Koeffizienten der Weierstraß-Normalform mit einer Konstanten, so daß sie eine p-reduzierte Teilmenge von $\mathbb{Z}$ bilden und reduzieren sie dann modulo p. So erhalten wir die Weierstraß-Normalform von E_p. Diese ist eindeutig bis auf einen skalaren Faktor bestimmt. Deswegen ist ihre Nullstellenmenge eindeutig und falls E_p nicht singulär ist, ist E_p eine elliptische Kurve über $\mathbb{F}_p$.*

Definition 1.21. *Eine Weierstraßsche Normalform heißt p-minimal, wenn die Potenz, in der die Primzahl p ihre Diskriminante teilt, nicht durch zulässige Variablentransformation vermindert werden kann. Eine global minimale Weierstraßsche Normalform ist eine Weierstraßsche Normalform, die für jede Primzahl p p-minimal ist.*

Satz 1.22 (Néron)**.** *Jede elliptische Kurve $E/\mathbb{Q}$ ist über $\mathbb{Q}$ isomorph zu einer solchen, die in global minimaler Weierstraßschen Normalform gegeben ist. Zu zwei global minimalen Weierstraßschen Normalformen einer elliptischen Kurve E gibt es eine zulässige Variablentransformation, die die eine in die andere überführt und $u = \pm 1$ und $r, s, t \in \mathbb{Z}$ erfüllt.*
Insbesondere sind die Diskriminanten gleich und Δ_{min} ist als Diskriminante der global minimalen Weierstraßschen Normalform wohldefiniert. Zu einer elliptischen Kurve E/K über einem Zahlkörper K braucht keine global minimale Weierstraßsche Normalform zu existieren. Anstelle der minimale Weierstraßsche Normalform kann man jedoch in diesem Fall ein Néron Modell der Kurve definieren, dessen Reduktion modulo Primidealen erklärt ist.

Beweis: Für den Fall $E/\mathbb{Q}$ siehe [Kn] Theorem 10.3.
Der Fall E/K, wobei K ein beliebiger Zahlkörper ist, ist ungleich schwerer. Dazu betrachtet man zu jedem Primideal $\mathfrak{p} \in Spec\,(\mathcal{O}_K)$ eine unter den zulässigen Variablentransformation aus dem lokalisierten Ring $\mathcal{O}_K$ minimale Kurve. Diese "verkleben sich in geeigneter Weise" zu einem Néron Modell. Eine präzise Beschreibung des Néron Modells erfordert die Sprache der Schemata, die wir in dieser Arbeit nicht einführen wollen. Siehe dazu z. B. [Si2] Kapitel IV.
□

Satz 1.23. *E_p ist genau dann singulär, wenn $p \mid \Delta_{min}\,(E)$.*

Beweis: klar.
□

Definition 1.24. *Die Reduktion einer elliptischen Kurve E/K modulo $\mathfrak{p}$ heißt gut, wenn $E_{\mathfrak{p}}$ nicht singulär ist, und sonst schlecht.*
Eine gute Reduktion einer elliptischen Kurve E/K modulo $\mathfrak{p}$ heißt supersingulär, wenn sie nur den trivialen $|\,\mathfrak{p}\,|$-Torsionspunkt hat, und sonst gewöhnlich.

Definition 1.25. *Zu einer elliptischen Kurve $E/\mathbb{Q}$ definieren wir den algebraischen Führer $N_E = \prod_{p\ prim} p^{f_p}$, wobei*

$$f_p = \begin{cases} 0 & \text{falls } E \text{ gute Reduktion in } p \text{ hat} \\ 1 & \text{falls } E_p \text{ eine Schleifensingularität hat} \\ 2+\delta_p & \text{falls } E_p \text{ eine Spitzensingularität hat} \end{cases}$$

wobei $\delta_p = 0$ für $p \neq 2,3$, $\delta_2 \leq 6$ und $\delta_3 \leq 3$.
Eine Formel für δ_2 und δ_3 ist in [Si2] angegeben.

Bemerkung 1.26. *Wir folgern leicht: $p \mid \Delta_{min}(E) \Leftrightarrow p \mid N_E$*

Definition 1.27. *Sei E eine elliptische Kurve über $\mathbb{Q}$. Wir definieren zu jeder Kurve E_p die Zahl $a_p := p + 1 - \#E_p(\mathbb{Z}_p)$, wobei $\#E_p(\mathbb{Z}_p)$ die Anzahl der $\mathbb{Z}_p$-Punkte von E_p bezeichnet. Die L-Reihe zur elliptischen Kurve $E/\mathbb{Q}$ ist gegeben durch:*

$$L(E,s) = \prod_{p|\Delta} \frac{1}{1-a_p p^{-s}} \prod_{p\nmid\Delta} \frac{1}{1-a_p p^{-s}+p1-2s}$$

Satz 1.28 (Hasse)**.** *Sei $E/\mathbb{Q}$ eine elliptische Kurve. Für $p \nmid \Delta$ gilt: $|p+1-\#E_p(\mathbb{F}_p)| < 2\sqrt{p}$.*
Deswegen konvergiert $L(E,s)$ für $\mathrm{Re}(s) > \frac{3}{2}$ und ist dort als absolut konvergente Dirichlet-Reihe gegeben.

Beweis: siehe [Kn] Thm 10.5. □

Satz 1.29 (Wiles et al.)**.** *Die L-Reihe zu einer elliptischen Kurve $E/\mathbb{Q}$ hat eine analytische Fortsetzung auf die ganze komplexe Ebene und erfüllt für ein geeignetes $N \in \mathbb{N}$ folgende Funktionalgleichung in $\Lambda(E,s) := N^{\frac{s}{2}}(2\pi)^{-1}\Gamma(s)L(E,s)$:*

$$\Lambda(E,s) = sgn(\Lambda)\,\Lambda(E,2-s),\ \text{wobei } sgn(\Lambda) \in \{-1,+1\}\ \text{gilt.}$$

Beweis: Siehe dazu [Hu] Thm 7.6, sowie S.314 zusammen mit Satz 9.8 in dieser Arbeit. □

1.4 Elliptische Funktionen

Definition 1.30. *Seien ω_1, ω_2 zwei $\mathbb{R}$-linear unabhänigige Elemente aus $\mathbb{C}$. Ein Gitter Λ in $\mathbb{C}$ ist die Menge der ganzzahligen Linearkombinationen von ω_1, ω_2. Wir schreiben $\Lambda = \{m\omega_1 + n\omega_2 \mid m, n \in \mathbb{Z}\}$. Im folgenden werden wir nur Gitter in $\mathbb{C}$ betrachten.*

Definition 1.31. *Zwei Gitter Λ_1, Λ_2 heißen homothetisch, wenn es ein $\alpha \in \mathbb{C}$ gibt mit $\alpha\Lambda_1 = \Lambda_2$.*

Definition 1.32. *Eine Funktion $f : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ heißt doppelt periodisch, wenn es zwei $\mathbb{R}$-linear unabhängige $\omega_1, \omega_2 \in \mathbb{C}$ mit $f(\omega_1 + z) = f(\omega_2 + z) = f(z)$ für alle $z \in \mathbb{C}$ gibt.*
Eine meromorphe, doppelt periodische Funktion heißt elliptische Funktion.
Die Menge $\{r\omega_1 + s\omega_2 \mid r, s \in [0, 1)\}$ heißt Fundamentalmasche zu f.

Beispiel 1.33. *Das wichtigste Beispiel für eine elliptische Funktion ist die Weierstraßsche $\wp$-Funktion zum Gitter Λ:*

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

Die Summe konvergiert für $z \notin \Lambda$ und die Funktion ist doppelt periodisch. Die $\wp$-Funktion ist gerade und hat einen doppelten Pol in den Gitterpunkten. Eine weitere elliptische Funktion ist:

$$\wp(z)' = 2 \sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^3}$$

$\wp(z)'$ ist eine ungerade elliptische Funktion.

Satz 1.34. *Jede gerade, elliptische Funktion ist eine rationale Funktion in $\wp(z)$. Jede elliptische Funktion f ist von der Form $f = g(\wp(z)) + \wp'(z)\, h(\wp(z))$, wobei g und h rational sind.*

Beweis: siehe [Kn] Thm 6.10. □

Korollar 1.35. *Da $(\wp'(z))^2$ als Quadrat einer ungeraden Funktion eine gerade Funktion ist, können wir $(\wp'(z))^2$ als rationale Funktion in $\wp(z)$ schreiben und ein Vergleich der Taylorentwicklungen ergibt eine Differentialgleichung der Form:*

$$(\wp')^2 = 4\wp^3 - g_4\wp - g_6,$$

wobei $g_4, g_6 \in \mathbb{C}$ nur vom Gitter abhängen.

Beweis: siehe [Kn] Thm 6.12. □

Bemerkung 1.36. *Wir können eine elliptische Funktion f auch als Funktion auf dem Quotienten $\mathbb{C}/\Lambda$ auffassen. Dieser Quotient ist eine Riemannsche Fläche von Geschlecht 1, also ein Torus. Die Addition der komplexen Zahlen vererbt sich auf den Torus.*

Satz 1.37. *Die Abbildung $\mathbb{C}/\Lambda \to E(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C})$ gegeben durch:*

$$z \mapsto \begin{cases} (\wp(z), \wp'(z), 1) & \text{für } z \notin \Lambda \\ (0,1,0) & \text{für } z \in \Lambda \end{cases}$$

ist ein biholomorpher Gruppenisomorphismus. Insbesondere ist die Kurve $E: y^2 = 4x^3 - g_4 x - g_6 = 4\left(x - \wp\left(\frac{\omega_1+\omega_2}{2}\right)\right)\left(x - \wp\left(\frac{\omega_1}{2}\right)\right)\left(x - \wp\left(\frac{\omega_2}{2}\right)\right)$ nicht singulär, da die Halbwerte der Weierstraßschen $\wp$-Funktion verschieden sind.

Beweis: siehe [Kn] Thm 6.14. und Thm 6.15. □

Bemerkung 1.38. *Sei $E/\mathbb{C}$ eine elliptische Kurve. Ist uns nur die Weierstraßsche Normalform gegeben, so ist es im allgemeinen sehr schwer, das Gitter zu der Kurve zu bestimmen, da man dazu komplizierte elliptische Integrale lösen muß.*

2 Der Endomorphismenring elliptischer Kurven und CM

Eine elliptische Kurve hat als triviale Endomorphismen $\mathbb{Z}$. In einigen Fällen ist der Endomorphismenring jedoch größer. Wir sagen dann die Kurve besitze Komplexe Multiplikation. Kurven mit Komplexer Multiplikation sind aus verschiedenen Gründen sehr interessant. Wir halten uns in diesem Kapitel eng an [Si1].

2.1 Komplexe Multiplikation

Satz 2.1. *Für zwei elliptische Kurven $E_1 = \mathbb{C}/\Lambda_1$, $E_2 = \mathbb{C}/\Lambda_2$ gilt: Die Abbildung*

$$\begin{array}{rcl} \{\alpha \in \mathbb{C} \,:\, \alpha\Lambda_1 \subset \Lambda_2\} & \to & \{\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \; mit \; \phi(0) = 0, \phi \; holomorph\} \\ \alpha & \mapsto & \phi_\alpha = \alpha z \; (mod \; \Lambda_2) \end{array}$$

ist bijektiv.

Beweis: Die skalare Multiplikation mit α ist holomorph.
(Injektivität) Ist $\phi_\alpha = \phi_\beta$, so gilt für alle $z \in \mathbb{C}$: $\alpha z \equiv \beta z \,(mod\ \Lambda_2)$. Dann ist die Abbildung $z \mapsto (\alpha - \beta)\, z$ konstant, da das Bild in Λ_2 liegt, also diskret ist. Folglich gilt: $\alpha = \beta$.
(Surjektivität) Sei nun $\phi \,:\, E_1 \to E_2$ holomorph mit $\phi(0) = 0$. Dann können wir diese Abbildung liften, so daß folgendes Diagramm kommutiert:

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{f} & \mathbb{C} \\ \downarrow{\scriptstyle \pi_1} & \circlearrowleft & \downarrow{\scriptstyle \pi_2} \\ \mathbb{C}/\Lambda_2 & \xrightarrow{\phi} & \mathbb{C}/\Lambda_2 \end{array}$$

Nun folgt für jedes $\lambda_1 \in \Lambda_1$, daß $f(z + \lambda_1) \equiv f(z)\,(mod\, \Lambda_2)\ \ \forall z \in \mathbb{C}$ gilt. Es folgt $f(z + \lambda_1) - f(z) \in \Lambda_2$ und da Λ_2 diskret ist, daß $f(z + \lambda_1) - f(z)$ nicht von z abhängt. Weiter folgt $f'(z + \lambda_1) = f'(z)\ \ \forall z \in \mathbb{C},\ \forall \lambda_1 \in \Lambda_1$. Also ist f' eine holomorphe, elliptische Funktion und somit konstant.
Deswegen ist $f = \alpha z + \gamma$ für geeignete $\alpha \in \mathbb{C},\ \gamma \in \mathbb{C}$. Aus $f(0) = 0$ folgt nun $\gamma = 0$ und aus $f(\Lambda_1) \subset \Lambda_2$ folgt $\alpha\Lambda_1 \subset \Lambda_2$ und somit $\phi = \phi_\alpha$. □

Definition 2.2. *Eine analytische Abbildung von $E_1/\mathbb{C}$ nach $E_2/\mathbb{C}$, die die Identität fixiert, heißt Isogenie.*

Satz 2.3. *Seien $E_1 = \mathbb{C}/\Lambda_1$ und $E_2 = \mathbb{C}/\Lambda_2$ zwei elliptische Kurven. Dann ist die Abbildung:*

$$\{Isogenien\, \phi :\, E_1 \to E_2\} \to \{holom.\, Funkt.\, \phi :\, \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \;\; mit\; \phi(0) = 0\}$$

bijektiv.

Beweis: (Injektivität) Da Isogenien lokal als rationale Funktionen, die überall definiert sind, gegeben sind, können wir sie mit holomorphen Funktionen (auf $\mathbb{C}/\Lambda$) identifizieren. Das geschieht klar injektiv.
(Surjektivität) Nach Satz 2.1 genügt es, Abbildungen der Form ϕ_α mit $\alpha \in \mathbb{C}^*$, $\alpha\Lambda_1 \in \Lambda_2$ zu betrachten. Damit folgt:

$$\begin{array}{rcl} E_1 & \to & E_2 \\ [\wp(z,\Lambda_1), \wp(z,\Lambda_1), 1] & \mapsto & [\wp'(\alpha z,\Lambda_2), \wp'(\alpha z,\Lambda_2), 1] \end{array}$$

Da $\alpha\Lambda_1 \in \Lambda_2$ ist, gilt für jedes $\lambda_1 \in \Lambda_1$:

$$\wp(\alpha(z+\lambda_1),\Lambda_2) = \wp(\alpha z + \alpha\lambda_1, \Lambda_2) = \wp(\alpha z, \Lambda_2)$$

$$\wp'(\alpha(z+\lambda_1),\Lambda_2) = \wp'(\alpha z + \alpha\lambda_1, \Lambda_2) = \wp'(\alpha z, \Lambda_2)$$

Somit gilt: $\wp(\alpha z,\Lambda_2), \wp'(\alpha z,\Lambda_2) \in \mathbb{C}(\wp(z,\Lambda_1), \wp'(\alpha,\Lambda_1))$ und sind somit rational abhängig von $\wp(z,\Lambda_1)$ und $\wp'(\alpha,\Lambda_1)$, was zu zeigen war. □

Korollar 2.4. *Seien $E_1 = \mathbb{C}/\Lambda_1$ und $E_2 = \mathbb{C}/\Lambda_2$ zwei elliptische Kurven. E_1 und E_2 sind genau dann isomorph, wenn Λ_1 und Λ_2 homothetisch sind, das heißt, wenn ein $\alpha \in \mathbb{C}^*$ existiert mit $\Lambda_1 = \alpha\Lambda_2$.*

Beweis: klar. □

Korollar 2.5. *Die Gruppe der Endomorphismen einer elliptischen Kurve $E = \mathbb{C}/\Lambda$ entsprechen den $\alpha \in \mathbb{C}^*$ mit $\alpha\Lambda \subset \Lambda$.*

Beweis: klar. □

Definition 2.6. *Eine Ordnung $\mathcal{O} \subset K$ des imaginärquadratischen Zahlkörpers K ist*

1. *ein Unterring von K, der die 1 enthält und*
2. *ein freier $\mathbb{Z}$-Modul vom Rang 2.*

Wegen 2. enthält $\mathcal{O}$ eine $\mathbb{Q}$-Basis von K. Deswegen ist K der Quotientenkörper von $\mathcal{O}$. Im Gegensatz zum Ring der ganzen Zahlen $\mathcal{O}_K$ braucht $\mathcal{O}$ kein Dedekindring zu sein. Insbesondere entgeht uns hier die Primfaktorzerlegung.
Mit $\mathbb{H}$ bezeichnen wir die obere Halbebene $\mathbb{H} := \{z \in \mathbb{C} \mid \mathrm{Im}\,(z) > 0\} \subset \mathbb{C}$.

Satz 2.7. *Sei $\omega_1\mathbb{Z} + \omega_2\mathbb{Z} = \Lambda$ ein Gitter in $\mathbb{C}$ und $E = \mathbb{C}/\Lambda$ die zugehörige elliptische Kurve. Wir können oBdA annehmen, daß gilt: $\tau := \frac{\omega_1}{\omega_2} \in \mathbb{H}$.*
Dann gilt entweder

1. *$End\,(E) \cong \mathbb{Z}$, oder*
2. *$\mathbb{Q}\,(\tau)$ ist eine imaginärquadratische Erweiterung von $\mathbb{Q}$ und $End\,(E)$ ist isomorph zu einer Ordnung in $\mathbb{Q}\,(\tau)$.*

Beweis: Das Gitter Λ ist homothetisch zu $\mathbb{Z} + \mathbb{Z}\tau$. Sei weiter $\mathcal{R} := \{\alpha \in \mathbb{C} : \ \alpha\Lambda \subset \Lambda\}$, also $\mathcal{R} \cong End\,(E)$.
Für jedes $\alpha \in \mathcal{R}$ gibt es dann $(a, b, c, d) \in \mathbb{Z}^4$ mit $\alpha = a + b\tau$ und $\alpha\tau = c + d\tau$. Gleichsetzen von τ liefert dann: $\alpha^2 - (a - d)\,\alpha + ad - bc = 0$. Deswegen ist α eine ganze Zahl über $\mathbb{Z}$.
Angenommen $\mathcal{R} \neq \mathbb{Z}$. Dann können wir ein $\alpha \notin \mathbb{Z}$ wählen. Daraus folgt insbesondere $b \neq 0$ und gleichsetzen von α ergibt: $b\tau^2 - (a - d)\,\tau - c = 0$. Da nun $\tau \notin \mathbb{R}$ gilt, folgt daß $\mathbb{Q}\,(\tau)$ imaginärquadratisch ist. Des Weiteren ist $\mathcal{R} \subset \mathbb{Q}\,(\tau)$ ganz über $\mathbb{Z}$ und somit eine Ordnung in $\mathbb{Q}\,(\tau)$. □

Definition 2.8 (Komplexe Multiplikation)**.** *Eine elliptische Kurve E/K hat Komplexe Multiplikation (kurz CM für complex multiplication) genau dann, wenn $End_K\,(E) \neq \mathbb{Z}$.*

Definition 2.9. *Eine elliptische Kurve E/K hat potentielle CM genau dann, wenn $E/\overline{K}$ CM hat.*

Definition 2.10 (Punkt komplexer Multiplikation)**.** *Ein Punkt $z \in \mathbb{C}$ ist genau dann ein Punkt komplexer Multiplikation (kurz: CM-Punkt), wenn ein Gitter $\Lambda \subset \mathbb{C}$ existiert mit $z\Lambda \subset \Lambda$.*

Bemerkung 2.11. *Sei $\mathcal{O}_K$ ein Ring der ganzen Zahlen des imaginärquadratischen Zahlkörpers K. Man stellt nun leicht fest, daß $\mathcal{O}_K$ ein Gitter in $\mathbb{C}$ ist und als Ring natürlich multiplikativ abgeschlossen ist. Deswegen ist $E_{\mathcal{O}_K} := \mathbb{C}/\mathcal{O}_K$ eine Kurve mit CM.*
Aus dieser Überlegung und Satz 2.7 folgt:

$$\{CM - Punkte\} = \bigcup_{\substack{[K:\mathbb{Q}]=2 \\ K \not\subset \mathbb{R}}} K$$

M. Waldschmidt gibt in [Wa] folgenden sehr interessanten Satz an:

Satz 2.12. *Sei $\tau \in \mathbb{H}$ algebraisch mit $j(\tau)$ algebraisch, dann ist τ imaginärquadratisch.*

Beweis: siehe [Wa] Cor 3.2.4. □

Korollar 2.13. *Punkte mit algebraischem j-Wert sind CM-Punkte oder transzendent.*

□

2.2 Ein kurzer Einblick in Klassenkörpertheorie und CM

Seien im Folgendem $\tau \in \mathbb{H}$ imaginärquadratisch, $K = \mathbb{Q}(\tau)$ der zugehörige Zahlkörper mit einer fixierten Einbettung in $\mathbb{C}$ und $\mathcal{O}_K$ der zugehörige Ring der ganzen Zahlen.
In der Literatur wird oft von CM als der komplexen Multiplikation mit ganz $\mathcal{O}_K$ gesprochen. Das reicht für unsere Zwecke jedoch nicht aus, weswegen wir geeignete, analoge Begriffe für den Fall komplexer Multiplikation mit einer Ordnung $\mathcal{O} \subset \mathcal{O}_K$ einführen werden.
Dieses Kapitel hält sich in Inhalt und Notation eng an [Si2] und [Co]. Analog zum Fall $\mathcal{O}_K$ definieren wir ein gebrochenes Ideal von $\mathcal{O}$ als Teilmenge von K, die ein endlich erzeugter $\mathcal{O}$-Modul und nicht Null ist.

Definition 2.14. *Das gebrochene Ideal $\mathfrak{a}$ von $\mathcal{O}$ heißt invertierbar genau dann, wenn es ein gebrochenes Ideal $\mathfrak{b}$ von $\mathcal{O}$ gibt mit $\mathfrak{ab} = \mathcal{O}$. Das gebrochene Ideal $\mathfrak{a}$ von $\mathcal{O}$ heißt Hauptideal genau dann, wenn es ein $k \in K^*$ gibt mit $\mathfrak{a} = k \cdot \mathcal{O}$.*

Satz 2.15. *Ein gebrochenes Ideal $\mathfrak{a}$ einer Ordnung $\mathcal{O}$ ist genau dann invertierbar, wenn gilt:*

$$\mathcal{O} = \{k \in K \mid k\mathfrak{a} \subset \mathfrak{a}\}.$$

(Diese Eigenschaft von gebrochenen Idealen wird im Englischen mit dem Wort proper ausgedrückt.)
Jedes gebrochene Hauptideal ist invertierbar.

Beweis: siehe [Co] Thm 7.4. □

Bemerkung 2.16. *Damit formen die invertierbaren, gebrochenen Ideale von $\mathcal{O}$ die multiplikative Gruppe $\mathcal{I}(\mathcal{O})$ mit der Untergruppe der invertierbaren, gebrochenen Hauptideale $\mathcal{P}(\mathcal{O})$. Den Quotienten $\mathcal{Cl}(\mathcal{O}) = \mathcal{I}(\mathcal{O})/\mathcal{P}(\mathcal{O})$ nennen wir die Idealklassengruppe von $\mathcal{O}$.*
Für $\mathcal{Cl}(\mathcal{O}_K)$ schreiben wir gelegentlich $\mathcal{Cl}(K)$. Die Kardinalität dieser Gruppe ist die Klassenzahl $h(K)$.

Satz 2.17. *Die Klassenzahl ist endlich.*

Beweis: siehe [Kn] Thm 4.31. □

Bemerkung 2.18. *Die Kardinalität von $\mathcal{Cl}(\mathcal{O})$ bezeichnen wir mit $h(\mathcal{O})$. Sie ist ein ganzzahliges Vielfaches von $h(K)$, also insbesondere auch endlich. Siehe [Co] Thm 7.24.*

Wir betrachten nun die Menge der elliptischen Kurven mit CM mit $\mathcal{O}$ modulo $\mathbb{C}$-Isomorphismen und schreiben: $\mathcal{Ell}(\mathcal{O}) := \frac{\{E/\mathbb{C}\ mit\ End(E/\mathbb{C})\cong\mathcal{O}\}}{\mathbb{C}-Isomorphismen}$
Wir bemerken:

$$\frac{\{E/\mathbb{C}\ mit\ End(E/\mathbb{C}) \cong \mathcal{O}\}}{\mathbb{C}-Isomorphismen} \cong \frac{\{Gitter\ \Lambda\ mit\ End(\mathbb{C}/\Lambda) \cong \mathcal{O}\}}{Homothetie}$$

Bemerkung 2.19. *Ein invertierbares, gebrochenes Ideal $\mathfrak{a} \subset \mathcal{O} \subset K \subset \mathbb{C}$ ist ein Gitter in $\mathbb{C}$.*

$$End(E_\mathfrak{a}) \cong \{\alpha \in \mathbb{C} \mid \alpha\mathfrak{a} \subset \mathfrak{a}\} = \{\alpha \in K \mid \alpha\mathfrak{a} \subset \mathfrak{a}\} = \mathcal{O}$$

Ein invertierbares, gebrochenes Ideal von $\mathcal{O}$ entspricht also einer elliptischen Kurve mit CM mit $\mathcal{O}$. Da wir uns aber nur für Homothetieklassen von Gittern bzw. Isomorphieklassen von elliptischen Kurven interessieren, genügt es Elemente der Idealklassengruppe zu betrachten.
Für ein $\overline{\Lambda} \in \mathcal{Ell}(\mathcal{O})$ findet sich nach Satz 2.7 ein Repräsentant $\Lambda := [1, \tau]$ mit $\tau \in K$. Also ist $\Lambda \subset K$ ein $\mathcal{O}$-Untermodul von K, daher ein gebrochenes $\mathcal{O}$-Ideal. Da $\overline{\Lambda} \in \mathcal{Ell}(\mathcal{O})$ ist Λ sogar ein invertierbares, gebrochenes Ideal von K.

Deswegen haben wir die bijektive Abbildung $\mathcal{Cl}(\mathcal{O}) \to \mathcal{Ell}(\mathcal{O})$ mit $\overline{\mathfrak{a}} \mapsto \mathbb{C}/\mathfrak{a}$.
Seien im Folgenden Λ ein Gitter in $\mathbb{C}$ mit $End(\mathbb{C}/\Lambda) \cong \mathcal{O}$ und $\mathfrak{a}$ und $\mathfrak{b}$ zwei invertierbare, gebrochene Ideale in $\mathcal{O}$.

Lemma 2.20. *Die Menge $\mathfrak{a}\Lambda$ ist ein Gitter in $\mathbb{C}$.*

Beweis: Da $\mathfrak{a}$ ein gebrochenes Ideal ist, können wir ein $0 \neq d \in \mathbb{Z}$ wählen, so daß $d\mathfrak{a} \subset \mathcal{O}$ gilt. Dann folgt $\mathfrak{a}\Lambda \subset \frac{1}{d}\Lambda$. Also ist $\mathfrak{a}\Lambda$ eine diskrete Untergruppe von $\mathbb{C}$. Außerdem können wir eine weitere Konstante $d' \in \mathbb{Z}$ mit $d'\Lambda \subset \mathfrak{a}\Lambda$ wählen. Deswegen spannt $\mathfrak{a}\Lambda$ ganz $\mathbb{C}$ auf und ist folglich ein Gitter in $\mathbb{C}$. □

Lemma 2.21. *Es gilt:* $End\,(\mathbb{C}/\mathfrak{a}\Lambda) \cong \mathcal{O}$.

Beweis: Für jedes $\alpha \in \mathbb{C}$ und jedes invertierbare, gebrochene Ideal $\mathfrak{a}$ gilt:

$$\alpha\mathfrak{a}\Lambda \subset \mathfrak{a}\Lambda \Leftrightarrow \mathfrak{a}^{-1}\alpha\mathfrak{a}\Lambda \subset \mathfrak{a}^{-1}\mathfrak{a}\Lambda \Leftrightarrow \alpha\Lambda \subset \Lambda$$

und somit

$$End\,(\mathbb{C}/\mathfrak{a}\Lambda) \cong \{\alpha \in \mathbb{C} \mid \alpha\mathfrak{a}\Lambda \subset \mathfrak{a}\Lambda\} = \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subset \Lambda\} = \mathcal{O}$$

□

Lemma 2.22. *Es gilt:* $\mathbb{C}/\mathfrak{a}\Lambda \cong \mathbb{C}/\mathfrak{b}\Lambda$ *genau dann, wenn* $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$.

Beweis: $\mathbb{C}/\mathfrak{a}\Lambda \cong \mathbb{C}/\mathfrak{b}\Lambda$ genau dann, wenn $\mathfrak{a}\Lambda$ und $\mathfrak{b}\Lambda$ homothetisch sind, das heißt, es existiert ein $c \in \mathbb{C}$ mit $\mathfrak{a}\Lambda = c\mathfrak{b}\Lambda$. Deswegen gilt: $c^{-1}\mathfrak{a}\mathfrak{b}^{-1}\Lambda = \Lambda = \mathfrak{a}^{-1}c\mathfrak{b}\Lambda$. Daraus folgt: $c^{-1}\mathfrak{a}\mathfrak{b}^{-1} \subset \mathcal{O}$ und $\mathfrak{a}^{-1}c\mathfrak{b} \subset \mathcal{O}$ und weiter $\mathfrak{a}^{-1}c\mathfrak{b} = \mathcal{O}$. Dann ist aber $\mathfrak{a} = c\mathfrak{b}$, also $c \in K$ und $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$. □

Satz 2.23. *Die Gruppe* $\mathcal{C}l\,(\mathcal{O})$ *wirkt mittels* $\overline{\mathfrak{a}} * \overline{\mathbb{C}/\Lambda} = \overline{\mathbb{C}/\mathfrak{a}^{-1}\Lambda}$ *einfach transitiv auf* $\mathcal{E}ll\,(\mathcal{O})$.

Beweis: Es gilt:
$\overline{\mathfrak{a}} * \left(\overline{\mathfrak{b}} * \overline{\mathbb{C}/\Lambda}\right) = \overline{\mathfrak{a}} * \overline{\mathbb{C}/\overline{\mathfrak{b}}^{-1}\Lambda} = \overline{\mathbb{C}/\overline{\mathfrak{a}}^{-1}\overline{\mathfrak{b}}^{-1}\Lambda} = \overline{\mathbb{C}/\left(\overline{\mathfrak{a}}\overline{\mathfrak{b}}\right)^{-1}\Lambda} = \left(\overline{\mathfrak{a}}\overline{\mathfrak{b}}\right) * \overline{\mathbb{C}/\Lambda}$
Seien nun $\mathbb{C}/\Lambda_1$ und $\mathbb{C}/\Lambda_2$ zwei Elemente aus $\mathcal{E}ll\,(\mathcal{O})$. Wir nehmen an, daß $\Lambda_1 = [1, \tau_1]$ und $\Lambda_2 = [1, \tau_2]$. Das ist keine Einschränkung, da uns nur die Homothetieklasse der Kurven interessiert. Wir müssen nun ein invertierbares, gebrochenes Ideal $\mathfrak{a}$ angeben mit $\overline{\mathfrak{a}} * \mathbb{C}/\Lambda_1 = \mathbb{C}/\Lambda_2$. Dazu bemerken wir, daß $\mathfrak{a}_1 = \Lambda_1$ nach Bemerkung 2.19 ein invertierbares, gebrochenes Ideal in $\mathcal{O}$ ist. Gleiches gilt dann natürlich auch für $\mathfrak{a}_2 = \Lambda_2$. Dann gilt aber mit $\mathfrak{a} = \mathfrak{a}_2^{-1}\mathfrak{a}_1$

$$\overline{\mathfrak{a}} * \mathbb{C}/\Lambda_1 = \mathbb{C}/\mathfrak{a}^{-1}\Lambda_1 = \mathbb{C}/\Lambda_2$$

Dies zeigt, daß die Wirkung transitiv ist. Daß die Wirkung einfach transitiv ist, folgt nun aus dem Lemma 2.22. □

Lemma 2.24. *Besitzt die elliptische Kurve* $E/\mathbb{C}$ *komplexe Multiplikation, so ist ihr* j*-Wert algebraisch.*

Beweis: Ein Automorphismus $\sigma \in Aut(\mathbb{C})$ wirkt auf die elliptische Kurve $E/\mathbb{C}$, indem er auf die Koeffizienten der Weierstraßschen Normalform wirkt. Es gilt: $j(E^\sigma) = j(E)^\sigma$, da der j-Wert aus den Koeffizienten der Weierstraßschen Normalform gewonnen werden kann.
Weiter gilt für $\sigma \in Aut(\mathbb{C})$, daß $End(E^\sigma) \cong End(E)$.
Da es nur endlich viele Isomorphieklassen mit dieser komplexen Multiplikation gibt und jeder Isomorphieklasse nur ein j-Wert zugeordnet wird, ist $\{j(E)^\sigma \mid \sigma \in Aut(\mathbb{C})\}$ endlich und $j(E)^\sigma$ algebraisch. □

Lemma 2.25. *Es gilt:* $\mathcal{E}\ell\ell(\mathcal{O}) \cong \frac{\{E/\overline{\mathbb{Q}} \mid End(E) \cong \mathcal{O}\}}{\overline{\mathbb{Q}} - Isomorphismen}$.

Beweis: Es bezeichne $\mathcal{E}\ell\ell_F(\mathcal{O}) \cong \frac{\{E/F \mid End(E) \cong \mathcal{O}\}}{F - Isomorphismen}$.
Sei eine Einbettung von $\overline{\mathbb{Q}} \subset \mathbb{C}$ fixiert. Wir wollen nun zeigen, daß die natürliche Abbildung $\beta : \mathcal{E}\ell\ell_{\overline{\mathbb{Q}}}(\mathcal{O}) \to \mathcal{E}\ell\ell_{\mathbb{C}}(\mathcal{O})$ bijektiv ist.
Wie gerade gezeigt ist $j(E) \in \overline{\mathbb{Q}}$ für $E \in \mathcal{E}\ell\ell(\mathcal{O})$. Zu diesem gegebenen j-Wert können wir leicht eine elliptische Kurve $E'/\mathbb{Q}(j(E))$ mit $j(E') = j(E)$ konstruieren. Da diese Kurven $\mathbb{C}$-isomorph sind, ist $\beta(E') = E$ und β ist surjektiv.
Seien E_1 und E_2 zwei Repräsentanten aus $\mathcal{E}\ell\ell_{\overline{\mathbb{Q}}}(\mathcal{O})$ mit $\beta\left(\overline{E_1}\right) = \beta\left(\overline{E_2}\right)$. Dann gilt aber bereits $j(E_1) = j(E_2)$. Damit sind E_1 und E_2 auch $\overline{\mathbb{Q}}$-isomorph, repräsentieren also dasselbe Element in $\mathcal{E}\ell\ell_{\overline{\mathbb{Q}}}(\mathcal{O})$. Deswegen ist β auch injektiv. □

Lemma 2.26. *Seien* $E \in \mathcal{E}\ell\ell(\mathcal{O})$, $\sigma \in Gal\left(\overline{K}/K\right)$ *und* $\mathfrak{a} \in \mathcal{C}\ell(\mathcal{O})$. *Dann gilt:* $(\mathfrak{a} * E)^\sigma = \mathfrak{a}^\sigma * E^\sigma$.

Beweis: Der Beweis ist lang, technisch und bei [Si2] Prop 2.5. zu finden. □

Satz 2.27. *Es existiert ein Gruppenhomomorphismus*
$F : Gal\left(\overline{K}/K\right) \to \mathcal{C}\ell(\mathcal{O})$, *der durch die Bedingung* $E^\sigma = F(\sigma) * E$ *für alle* $\sigma \in Gal\left(\overline{K}/K\right)$ *und* $E \in \mathcal{E}\ell\ell(\mathcal{O})$ *eindeutig festgelegt ist.*

Beweis: $Gal\left(\overline{K}/K\right)$ wirkt kanonisch auf $\mathcal{E}\ell\ell(\mathcal{O})$, indem die Isomorphieklasse von E auf die von E^σ abgebildet wird. Da nun $\mathcal{C}\ell(\mathcal{O})$ einfach transitiv auf $\mathcal{E}\ell\ell(\mathcal{O})$ wirkt, können wir diese Galoiswirkung auch mit einem Element aus

$\mathcal{C}\ell(\mathcal{O})$ beschreiben.
F ist ein Homomorphismus, da

$$\begin{aligned} F(\sigma\tau) * E = E^{\sigma\tau} = (E^{\sigma})^{\tau} = (F(\sigma) * E)^{\tau} = F(\tau) * (F(\sigma) * E) \\ = (F(\sigma) F(\tau)) * E \end{aligned}$$

Es bleibt zu zeigen, daß die Definition von F nicht von der Wahl der Kurve E abhängt. Dazu betrachten wir E_1 und E_2 aus $\mathcal{E}\ell\ell(\mathcal{O})$ und schreiben $E_1^{\sigma} = \overline{\mathfrak{a}}_1 * E_1$ und $E_2^{\sigma} = \overline{\mathfrak{a}}_2 * E_2$. Wegen der einfach transitiven Wirkung von $\mathcal{C}\ell(\mathcal{O})$ existiert auch ein $\overline{\mathfrak{b}}$ mit $E_2 = \overline{\mathfrak{b}} * E_1$. Dann gilt:

$$\left(\overline{\mathfrak{b}} * E_1\right)^{\sigma} = E_2^{\sigma} = \overline{\mathfrak{a}}_2 * E_2 = \overline{\mathfrak{a}}_2 * \left(\overline{\mathfrak{b}} E_1\right) = \left(\overline{\mathfrak{a}}_2 \overline{\mathfrak{b}} \overline{\mathfrak{a}}_1^{-1}\right) * E_1^{\sigma}.$$

$$\left(\overline{\mathfrak{b}} * E_1\right)^{\sigma} = \left(\overline{\mathfrak{a}}_2 \overline{\mathfrak{b}} \overline{\mathfrak{a}}_1^{-1}\right) * E_1^{\sigma} \Rightarrow E_1^{\sigma} = \left(\overline{\mathfrak{a}}_2 \overline{\mathfrak{a}}_1^{-1}\right) * E_1^{\sigma} \Rightarrow \overline{\mathfrak{a}}_1 = \overline{\mathfrak{a}}_2.$$

□

Satz 2.28. *Sei E eine elliptische Kurve, die eine Isomorphieklasse von $\mathcal{E}\ell\ell(\mathcal{O})$ repräsentiert. Dann ist $K(j(E))$ eine abelsche Körpererweiterung von K mit $[K(j(E)) : K] = h(\mathcal{O})$.*

Beweis: Sei L/K die endliche Körpererweieterung, die durch den Kern der Abbildung $F : Gal\left(\overline{K}/K\right) \to \mathcal{C}\ell(\mathcal{O})$ gegeben ist.

$$\begin{aligned} Gal\left(\overline{K}/L\right) &= ker(F) \\ &= \left\{\sigma \in Gal\left(\overline{K}/K\right) \mid F(\sigma) = 1\right\} \\ &= \left\{\sigma \in Gal\left(\overline{K}/K\right) \mid F(\sigma) * E = E\right\} && \mathcal{C}\ell(\mathcal{O})\ einfach\ transitiv \\ &= \left\{\sigma \in Gal\left(\overline{K}/K\right) \mid E^{\sigma} = E\right\} && Def.\ von\ F \\ &= \left\{\sigma \in Gal\left(\overline{K}/K\right) \mid j(E^{\sigma}) = j(E)\right\} \\ &= \left\{\sigma \in Gal\left(\overline{K}/K\right) \mid j(E)^{\sigma} = j(E)\right\} && nach\ Lemma\ 2.24 \\ &= Gal\left(\overline{K}/K(j(E))\right) \end{aligned}$$

Also gilt: $L = K(j(E))$. Auch ist $K(j(E))/K$ abelsch, da F die Gruppe $Gal(K(j(E))/K)$ injektiv auf $\mathcal{C}\ell(\mathcal{O})$ abbildet.
Allerdings ist F auch surjektiv und deshalb gilt: $[K(j(E)) : K] = \mid \mathcal{C}\ell(\mathcal{O}) \mid$.
□

Satz 2.29. *Sei $\{E_1, ..., E_n\}$ ein vollständiges Repräsentantensystem von $\mathcal{E}\ell\ell(\mathcal{O})$. Dann ist $\mathcal{J} := \{j(E_1), ..., j(E_n)\}$ die Menge aller $Gal\left(\overline{K}/K\right)$-Konjugierten von $j(E)$, wobei E ein Repräsentant einer beliebigen Isomorphieklasse von $\mathcal{E}\ell\ell(\mathcal{O})$ ist.*

Beweis: Die Repräsentanten einer Klasse aus $\mathcal{E}\ell\ell(\mathcal{O})$ haben alle dieselbe j-Invariante. Deswegen können wir auch jeder Klasse diese j-Invariante zuweisen und da verschiedene $\mathbb{C}$-Isomorphismenklassen elliptischer Kurven auch verschiedene j-Invarianten haben, haben wir eine natürliche Bijektion zwischen $\mathcal{J}$ und $\mathcal{E}\ell\ell(\mathcal{O})$. $\mathcal{C}\ell(\mathcal{O})$ wirkt transitiv auf $\mathcal{E}\ell\ell(\mathcal{O})$ und deswegen auch auf $\mathcal{J}$. Wegen F wirkt schließlich auch $Gal\left(\overline{K}/K\right)$ transitiv auf $\mathcal{J}$. □

2.3 Der Frobenius-Morphismus

Seien $\mathbb{F}_q$ im Folgenden ein endlicher Körper mit $char(\mathbb{F}_q) = p > 0$ und $m = p^r$.

Definition 2.30. *Zu einer elliptischen Kurve $E/\mathbb{F}_q$ gegeben durch die Weierstraßsche Normalform*

$$y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$$

definieren wir die Kurve $E^{(m)}/\mathbb{F}_q$ gegeben durch:

$$y^2 + a_1^m xy + a_3^m y - x^3 - a_2^m x^2 - a_4^m x - a_6^m.$$

Bemerkung 2.31. *Direktes Ausrechnen zeigt: $\Delta\left(E^{(m)}\right) = \Delta(E)^m$ und $j\left(E^{(m)}\right) = j(E)^m$. Insbesondere ist $E^{(m)}/\mathbb{F}_q$ wieder eine elliptische Kurve.*

Definition 2.32. *Der m-te Frobenius Morphismus ist definiert als:*

$$\begin{aligned} Fr_m :\ & E/\mathbb{F}_q \to E^{(m)}/\mathbb{F}_q \\ & (x, y) \mapsto (x^m, y^m) \end{aligned}$$

Satz 2.33. *Sei Fr_m der m-te Frobenius Morphismus. Dann gilt: $deg(Fr_m) = m$.*

Beweis: siehe [Si1] Prop II.2.11. □

Bemerkung 2.34. *Sei $\mathbb{F}_q$ der endliche Körper mit q Elementen. Dann wirkt die q-te Potenz auf $\mathbb{F}_q$ wie die Identität und es gilt $E^{(q)}/\mathbb{F}_q = E/\mathbb{F}_q$. Nun ist Fr_q ein Endomorphismus, der Frobenius Endomorphismus. Die Menge der Fixpunkte des Frobenius Endomorphismus ist genau die endliche Gruppe $E(\mathbb{F}_q)$.*

Seien $L/\mathbb{Q}$ ein Zahlkörper, E/L eine elliptische Kurve und $\mathfrak{P} \subset \mathcal{O}_L$ ein Primideal, so daß E gute, gewöhnliche Reduktion bei $\mathfrak{P}$ hat. Sei weiter $q_{\mathfrak{P}} = N_{L/\mathbb{Q}}(\mathfrak{P}) = \#\mathbb{F}_{\mathfrak{P}}$ die Norm des Primideals. Sei weiter $Fr_{\mathfrak{P}}$ der $q_{\mathfrak{P}}$-te Frobenius Endomorphismus auf $E_{\mathfrak{P}}$. Für $n \in \mathbb{Z}$ bezeichne $[n]$ den Endomorphismus, der durch die Multiplikation mit n gegeben ist.

Satz 2.35. *Der Frobenius Endomorphismus $Fr_{\mathfrak{P}}$ erfüllt die quadratische Gleichung $X^2 + [tr_{Fr_{\mathfrak{P}}}]X + [q_{\mathfrak{P}}]$, wobei $tr_{Fr_{\mathfrak{P}}}, q_{\mathfrak{P}} \in \mathbb{Z}$. Die Zahl $tr_{Fr_{\mathfrak{P}}}$ ist die Spur des Frobenius Endomorphismus und es gilt: $t_{Fr_{\mathfrak{P}}} = 1 + q_{\mathfrak{P}} - \#E_{\mathfrak{P}}(\mathbb{F}_{\mathfrak{P}})$.*

Beweis: Siehe [Si2] II.10.1. □

Bemerkung 2.36. *Es genügt also die Anzahl der Punkte auf der Kurve zu kennen, um das charakteristische Polynom des Frobenius Endomorphismus zu bestimmen. Eine Abschätzung der Anzahl der Punkte gibt zum Beispiel Hasse. Vergleiche mit Satz 1.28.*

Die Anzahl der Punkte einer elliptischen Kurve über einem endlichen Körper kann man mit dem Computeralgebrasystem SAGE [St2] bestimmen. Dies geschieht einfach mit dem Befehl:

$$EllipticCurve(GF(q), [a_1, a_2, a_3, a_4, a_6]).cardinality(),$$

wobei q die Anzahl der Elemente des Körpers bezeichnet und $\{a_i\}_{i=1,2,3,4,6}$ die Koeffizienten der reduzierten Kurve bezeichnen.
Wir wollen nun noch einige Aussagen über Endomorphismenringe elliptischer Kurven machen, die grundlegend für den CM-Test von J. Achter sind.

Satz 2.37. *Der Endomorphismenring einer elliptischen Kurve ist entweder*

1. $\mathbb{Z}$
2. *eine Ordnung in einem imaginärquadratischen Zahlkörper oder*
3. *eine Ordnung in einer Quaternionenalgebra.*

Beweis: Siehe [Si1] Korollar 9.4. □

Bemerkung 2.38. *Seien K ein Körper mit Charakteristik 0 und E/K eine elliptische Kurve. Dann ist der Quotientenkörper des Endomorphismenringes $Quot(End_K(E))$ entweder $\mathbb{Q}$ oder ein imaginärquadratischer Zahlkörper.*
Sei nun K ein Körper mit beliebiger Charakteristik und E/K eine gewöhnliche elliptische Kurve. Auch dann ist der Quotientenkörper des Endomorphismenringes $Quot(End_K(E))$ entweder $\mathbb{Q}$ oder ein imaginärquadratischer Zahlkörper.

Bemerkung 2.39. *Zu einer elliptischen Kurve E/K existiert eine endliche Körpererweiterung $K \subset L$, so daß gilt: $End_L(E) = End_{\overline{K}}(E)$*

Satz 2.40. *Sei p ein Primideal in $\mathcal{O}_K$, dann gibt es die Inklusion $End_K(E) \to End_{\mathbb{F}_p}(E_p)$.*

Beweis: Das ist der Spezialfall $E_1 = E_2$ des Satzes [Si2] Prop 4.4. S.124. □

3 Achters CM-Test für elliptische Kurven über Zahlkörpern

Dieses Kapitel teilt sich in zwei Teile. Im ersten beschreiben wir den Algorithmus von J. Achter und geben ein Kriterium dafür, wann eine elliptische Kurve keine potentielle CM haben kann. Im zweiten Teil erläutern wir den theoretischen Hintergrund zu dem Algorithmus.

3.1 Der Algorithmus

In seinem Artikel [Ac1] präsentiert Achter einen deterministischen Algorithmus, um elliptische Kurven über einem Zahlkörper auf CM zu testen. Dazu überprüft er das Reduktionsverhalten der Kurve bei Primstellen, deren Norm kleiner als eine vorgegebene Konstante ist.
Sei E/K die zu testende elliptische Kurve und K ein Zahlkörper.

Schritt 1

Berechne die j-Invariante der Kurve! Gilt $j(E) \in \{0, 1728\}$, so hat E CM mit i oder ρ, sonst weiter bei Schritt 2.

Schritt 2

Bezeichne (N) das Produkt der Primideale schlechter Reduktion und sei $\widetilde{K} := K\left(\sqrt{N}\right)$. Besitzt $E/\widetilde{K}$ überall gute Reduktion? Falls nein, so hat E keine CM, andernfalls weiter bei Schritt 3.

Schritt 3

Sei $\mathfrak{p}$ ein Primideal guter, gewöhnlicher Reduktion. Bestimme für $E/\widetilde{K}$ den Kandidatenkörper $F := Quot(\mathbb{Z}[Fr_{\mathfrak{p}}])$.

Schritt 4

Es gibt eine berechenbare Konstante C, so daß E genau dann CM hat, wenn für jedes Primideal $\mathfrak{p}$ von $\mathcal{O}_{\widetilde{K}}$, das über einer Primzahl $p < C$ liegt, gilt: entweder

- $E_{\mathfrak{p}}$ ist supersingulär und F ist inert oder verzweigt bei p, oder
- $End(E_{\mathfrak{p}}) \otimes \mathbb{Q} \cong F$ und F ist bei p verzweigt.

Bemerkung 3.1. *Wir werden jedoch folgendes, leicht abgewandeltes Kriterium verwenden, um zu zeigen, daß die von uns untersuchten Kurven keine CM haben. Sei E/K eine elliptische Kurve mit guter, gewöhnlicher Reduktion bei den Primstellen $\mathfrak{p}_1$ und $\mathfrak{p}_2$, so daß gilt: $End\,(E/\mathbb{F}_{\mathfrak{p}_1}) \cap End\,(E/\mathbb{F}_{\mathfrak{p}_2}) = \mathbb{Z}$. Dann hat E/K keine potentielle CM.*

3.2 Mathematische Grundlagen

Bezeichnung Sei K ein Körper und $\mathfrak{p}$ ein Primideal aus $\mathcal{O}_K$. Dann bezeichne $\mathbb{F}_{\mathfrak{p}}$ den Körper $\mathcal{O}_K/\mathfrak{p}$.

Serre und Tate zeigen in ihrem Artikel [ST1] folgenden

Satz 3.2. *Sei A/K eine abelsche Varietät mit CM über dem Zahlkörper K. Sei S_A die Menge der Bewertungen ν bei denen A schlechte Reduktion hat und m das kleinste gemeinsame Vielfache der Ordnungen der Gruppen Φ_ν für $\nu \in S_A$. Dann gibt es eine zyklische Körpererweiterung $\widetilde{K}$ von K vom Grad $2m$, so daß $A/\widetilde{K}$ überall gute Reduktion hat. Ist S_A gewöhnlich, so gibt es eine solche Körpererweiterung bereits vom Grad m.*

Beweis: Siehe [ST1] Thm 7. □

Bemerkung 3.3. *Wir haben die Gruppen Φ_ν nicht eingeführt und werden es auch nicht tun. Uns reicht die Aussage aus dem gleichen Artikel, daß Φ_ν eine Untergruppe von der Gruppe der Einheitswurzeln des CM-Körpers ist. Ist A eine elliptische Kurve, so ist S_A immer gewöhnlich.*
Die Einheiten aus dem Ganzheitsring eines imaginärquadratischen Zahlkörpers $\mathbb{Q}\left(\sqrt{d}\right)$ sind:

- $\{\pm 1, \pm i\}$, *falls* $d = -1$
- $\left\{\pm 1, \pm\frac{1}{2} \pm \frac{\sqrt{3}}{2}\right\}$, *falls* $d = -3$
- $\{\pm 1\}$ *sonst.*

Enthält eine Ordnung i (oder ρ), so enthält sie auch die Ringe der ganzen Zahlen $\mathcal{O}_{\mathbb{Q}(i)}$ (oder $\mathcal{O}_{\mathbb{Q}(\rho)}$). In beiden Fällen ist die Klassenzahl 1 und deswegen gibt es nur eine Isomorphieklasse elliptischer Kurven mit CM mit i und nur eine mit CM mit ρ. Die j-Invarianten dieser Isomorphieklassen sind 1728 und 0. Siehe [Si2] S.101f.
In den übrigen Fällen können wir aufgrund der vorangegangenen Sätze folgern, daß die elliptische Kurve E/K komplexe Multiplikation mit einem

Körper hat, der nur die Einheitswurzeln -1 und $+1$ hat und weiter, daß es eine Körpererweiterung $K \subset \widetilde{K}$ vom Grad 2 gibt, so daß $E/\widetilde{K}$ überall gute Reduktion hat. Genauer, sei (N) das Produkt aller Primideale schlechter Reduktion, dann gilt $\widetilde{K} := K\left(\sqrt{N}\right)$.

So erklärt der Satz von Serre und Tate den Schritt 2 des Algorithmus. Der Satz 3.4 sichert die Existenz eines Kandidatenkörpers und der Satz 3.5 erklärt seine Funktion.

Satz 3.4. *Sei $E/\widetilde{K}$ eine elliptische Kurve mit CM und guter Reduktion überall. Dann existiert eine berechenbare Konstante C und ein Primideal $\mathfrak{p}$, das über der rationalen Primzahl $p < C$ liegt, so daß E bei $\mathfrak{p}$ gewöhnliche, gute Reduktion hat.*

Beweis: siehe [Ac1] Lemma 2.1. □

Satz 3.5. *Zu einer elliptischen Kurve E/K mit CM gibt es einen imaginärquadratischen Körper F, so daß für jedes Primideal $\mathfrak{p}$ mit gewöhnlicher, guter Reduktion der Ring $\mathbb{Z}[Fr_{\mathfrak{p}}]$ isomorph zu einer Ordnung in F ist.*
Es gibt genau dann einen imaginärquadratischen Zahlkörper, mit dem die elliptische Kurve E/K CM hat, wenn sie CM mit F hat.

Beweis: siehe [Ac1] □

Satz 3.6. *Seien $E/\widetilde{K}$ eine elliptische Kurve mit guter Reduktion überall und F ein imaginärquadratischer Zahlkörper, dessen einzige Einheitswurzeln -1 und $+1$ sind. Dann gibt es eine berechenbare Konstante C, so dass E genau dann CM mit F hat, wenn für jedes Primideal $\mathfrak{p}$ über einer Primzahl $p < C$ gilt:*
entweder

- *$E_{\mathfrak{p}}$ ist supersingulär und F ist inert oder verzweigt bei p, oder*
- *$End(E_{\mathfrak{p}}) \otimes \mathbb{Q} \cong F$ und F ist bei p verzweigt.*

Beweis: siehe [Ac1] Lemma 2.2. □

Um zu zeigen, daß eine elliptische Kurve keine potentielle CM hat, benötigen wir noch folgende Überlegungen, die ich J. Achter [Ac2] verdanke.

Satz 3.7. *Sei E/K eine elliptische Kurve mit guter, gewöhnlicher Reduktion bei p. Sei weiter L eine endliche Körpererweiterung von K, so daß gilt $End(E/L) = End\left(E/\overline{K}\right)$ und q ein Primideal in $\mathcal{O}_L$ über p.*
Dann gilt: $Quot\left(End_{\mathbb{F}_p}(E/\mathbb{F}_p)\right) = Quot\left(End_{\mathbb{F}_q}(E/\mathbb{F}_q)\right)$.

Beweis: Nach Achter [Ac2] ist der Endomorphismenring einer gewöhnlichen, elliptischen Kurve über einem endlichen Körper bereits maximal. □

Korollar 3.8. *Sei E/K eine elliptische Kurve mit guter, gewöhnlicher Reduktion bei den Primstellen p_1 und p_2, so daß gilt: $End_{\mathbb{F}_{p_1}}(E/\mathbb{F}_{p_1}) \cap End_{\mathbb{F}_{p_2}}(E/\mathbb{F}_{p_2}) = \mathbb{Z}$.*
Dann hat E/K keine potentielle CM.

Beweis: Sei L eine endliche Körpererweiterung von K mit $End(E/L) = End\left(E/\overline{K}\right)$. Weiter seien q_1 und q_2 Primideale aus L, die über p_1 beziehungsweise über p_2 liegen. Aus dem vorangehenden Satz wissen wir, daß gilt: $Quot\left(End_{\mathbb{F}_{p_i}}(E/\mathbb{F}_{p_i})\right) = Quot\left(End_{\mathbb{F}_{q_i}}(E/\mathbb{F}_{q_i})\right)$. Daraus folgt, daß $End(E/L) \subset End_{\mathbb{F}_{q_1}}(E/\mathbb{F}_{q_1}) \cap End_{\mathbb{F}_{q_2}}(E/\mathbb{F}_{q_2}) = \mathbb{Z}$. □

4 Modulformen

In diesem Kapitel führen wir den wichtigen Begriff der Modulform ein und geben die Eisensteinreihen und die Diskriminantenfunktion als wichtige Beispiele an. Wir bemerken, daß die Modulformen einen Vektorraum bilden und bestimmen seine Dimension. Die $\frac{k}{12}$-Formel gibt uns erste Informationen über die Nullstellen der Modulformen.
Dann beschäftigen wir uns mit Modulformen zu höheren Leveln und studieren dazu insbesondere Untergruppen zu $\Gamma(1) = SL_2(\mathbb{Z})$. Dabei führen wir den Begriff Fundamentalbereich und Modulkurve ein.

4.1 Eine Einführung in Modulformen

Definition 4.1. *Bezeichne $\mathbb{H}$ die obere Halbebene der komplexen Zahlen. $\Gamma(1)$ wirkt auf $\mathbb{H}$ wie folgt:*

$$\gamma(\tau) := \frac{a\tau + b}{c\tau + d} \quad \text{für alle } \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1) \text{ und } \tau \in \mathbb{H}.$$

$\Gamma(1)$ wirkt auch auf $\mathbb{P}^1(\mathbb{Q})$: Für $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1)$

$$\gamma(\tau) = \begin{cases} \frac{a\tau+b}{c\tau+d} & \text{falls } \frac{a\tau+b}{c\tau+d} \in \mathbb{Q} \text{ und } \tau \in \mathbb{Q} \\ \frac{a}{c} & \text{falls } \frac{a}{c} \in \mathbb{Q} \text{ und } \tau = \infty \\ \infty & \text{sonst} \end{cases}$$

Bezeichne $\overline{\mathbb{H}} = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$, dann wirkt $\Gamma(1)$ auf $\overline{\mathbb{H}}$.

Im folgenden betrachten wir Funktionen $f : \overline{\mathbb{H}} \to \mathbb{C}$.

Definition 4.2. *Der Slash-Operator zum Gewicht $k \in \mathbb{N}$ und zur Matrix $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{R})$ wirkt auf der Funktion f in folgender Weise:*

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

Definition 4.3. *Eine meromorphe Funktion $f : \overline{\mathbb{H}} \to \mathbb{C}$ heißt schwach modular zum Gewicht $k \in \mathbb{N}$, wenn sie für jedes $\gamma \in \Gamma(1)$ invariant bezüglich des Slash-Operators $\mid_k \gamma$ ist.*

Bemerkung 4.4. *Die Gruppe $\Gamma(1)$ wird von den Elementen $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ und $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ erzeugt. Daher genügt es die schwache Modularität nur für die Fälle S und T zu prüfen, also zu zeigen: $f(\tau + 1) = f(\tau)$ und $f\left(\frac{-1}{\tau}\right) = \tau^k f(\tau)$.*

Bemerkung 4.5. *Aus Bemerkung 4.4 folgt, daß f eine $\mathbb{Z}$-periodische Funktion ist. Deswegen können wir zu f die Funktion $g : \mathbb{D}^\circ \to \mathbb{C}$ definieren als $f(\tau) = g(e^{2\pi i\tau})$, wobei $\mathbb{D}^\circ$ die punktierte Einheitskreisscheibe bezeichnet. Ist f holomorph, so ist auch g holomorph und hat eine Laurent-Entwicklung. Wir setzen im folgenden $q := e^{2\pi i\tau}$ und sagen, f ist holomorph in ∞, wenn sich die Funktion g holomorph im Punkt $q = 0$ fortsetzen lässt. Ist f holomorph auf $\mathbb{H}$ und in ∞, dann hat f eine Fourier-Entwicklung der Form:*

$$f(\tau) = \sum_{n=0}^{\infty} a_n(f)\, q^n$$

Definition 4.6. *Eine schwach modulare Funktion f zum Gewicht k ist eine Modulform, wenn sie holomorph auf $\mathbb{H}$ und in ∞ ist. Eine Modulform f heißt Spitzenform, wenn ihr erster Fourierkoeffizient $a_0(f) = 0$ ist.*

Beispiel 4.7. *Für k gerade, $k > 2$ definieren wir die Eisensteinreihe vom Gewicht k:*
$G_k(\tau) = \frac{(k-1)!}{2(2\pi i)^k} \sum'_{m,n} \frac{1}{(m\tau+n)^k}$. Für $k > 2$ konvergiert diese Reihe absolut. Wir wählen k gerade, da die Reihe für ungerade k Null ist. Es gilt:

$$(c\tau + d)^{-k} G_k\left(\frac{a\tau+b}{c\tau+d}\right) = \frac{(k-1)!}{2(2\pi i)^k} \sum'_{m,n} \frac{1}{((am+cn)\tau + (bm+dn))^k} = G_k(\tau),$$

da wir die Summanden beliebig permutieren können. Weiter gilt:

$$\begin{aligned}
G_k(\tau) =& \frac{(k-1)!}{2(2\pi i)^k} \sum_{n=1}^{\infty} \frac{1}{n^k} + \sum_{m=1}^{\infty} \left(\frac{(k-1)!}{2(2\pi i)^k} \sum_{n\in\mathbb{Z}} \frac{1}{(m\tau+n)^k} \right) && k \text{ gerade} \\
=& \frac{(k-1)!}{2(2\pi i)^k} \zeta(k) + \sum_{m=1}^{\infty} \left(\frac{(k-1)!}{2(2\pi i)^k} \sum_{n\in\mathbb{Z}} \frac{1}{(m\tau+n)^k} \right) && \text{Def. Zeta-Funktion} \\
=& \frac{(k-1)!}{2(2\pi i)^k} \zeta(k) + \sum_{m=1}^{\infty} \sum_{r=1}^{\infty} r^{k-1} e^{2\pi i m\tau} && \text{Lipschitz-Formel} \\
=& -\frac{B_k}{2k} + \sum_{m=1}^{\infty} \sum_{r=1}^{\infty} r^{k-1} e^{2\pi i m\tau} && B_k \text{ ist die } k\text{-te Bernoulli-Zahl} \\
=& -\frac{B_k}{2k} + \sum_{m=1}^{\infty} \sigma_{k-1}(n)\, q^n && q = e^{2\pi i\tau} \text{ und } \sigma_{k-1}(n) = \sum_{r|n} r^{k-1}
\end{aligned}$$

Die Eisensteinreihe vom Gewicht k ist eine Modulform vom Gewicht k, aber keine Spitzenform. Die Koeffizienten der Reihenentwicklung sind rational.

Beispiel 4.8. *Die Diskiminantenfunktion* $\Delta(\tau) = q\prod_{r\geq 1}(1-q^r)^{24}$ *ist eine Spitzenform vom Gewicht 12. Auch ihre Koeffizienten sind rational.*

Satz 4.9. *Das Wachstum der Fourierkoeffizienten von Modulformen läßt sich wie folgt abschätzen:*

$$a(n) = O\left(n^{k-1}\right) \text{ für } f \in M_k, \quad |\, a(n)\,| \leq \sigma(n)\, n^{\frac{k-1}{2}} \text{ für } f \in S_k,$$

wobei $\sigma(n)$ *die Anzahl der Teiler von* n *bezeichnet.*

Beweis: siehe [Za] S. 260 und [Si2] Satz 11.2. □

Bemerkung 4.10. *Die Modulformen vom Gewicht* k *bilden einen Vektorraum* M_k*, die Spitzenformen zum Gewicht* k *einen Vektorraum* S_k*. Für* $k > 2$*, gerade, gilt:* $M_k = \langle G_k\rangle \oplus S_k$*, also insbesondere* $dim S_k = dim M_k - 1$*. Mit der* Δ*-Funktion können wir zeigen, dass* $S_k \cong M_{k-12}$*. Damit ergibt sich folgende Formel für die Dimensionen:*

$$dim M_k = \begin{cases} 0 & : \quad k < 0 \text{ oder } k \text{ ungerade} \\ \left[\frac{k}{12}\right] & : \quad k \equiv 2 \bmod 12 \\ \left[\frac{k}{12}\right] + 1 & : \quad k \not\equiv 2 \bmod 12 \end{cases}$$

So ist z.B. $dim S_{12} = 1$, also sind $(240G_4)^3 - (504G_6)^2$ und Δ Vielfache voneinander. Die Vektorräume M_k haben mit $\Delta^l G_{k-12l}$ $(0 \leq l \leq \frac{k-4}{12})$ und zusätzlich $\Delta^{\frac{k}{12}}$ im Fall $k \mid 12$ eine Basis mit rationalen Koeffizienten. Insbesondere hat jede Modulform eine eindeutige Darstellung in G_4 und G_6.

Beispiel 4.11. $j(\tau) := \frac{(240G_4)^3}{\Delta}$ *ist invariant unter der Aktion von* $\Gamma(1)$*. Umgekehrt sei* $\phi(\tau)$ *eine Funktion invariant unter der Aktion von* $\Gamma(1)$ *und mit höchstens exponentiellem Wachstum in* $\mathrm{Im}(\tau) \to \infty$*, dann verhält sich* $f(\tau) = \phi(\tau)\Delta(\tau)^m$ *für* m *hinreichend groß wie eine Modulform vom Gewicht* $12m$*. Also ist* $\phi = \frac{f}{\Delta^m}$ *ein Polynom vom Grad* $\leq m$ *in* j*. Deswegen bezeichnen wir* $j(\tau)$ *als die invariante Modulfunktion.*

Lemma 4.12. *Sei* $\tau = \rho + i\sigma \in \mathbb{H}$*. Dann ist das Maß* $\frac{d\rho\, d\sigma}{\sigma^2}$ *auf der oberen Halbebene invariant unter* $SL_2(\mathbb{R})$*.*

Beweis: siehe [Kn] Lemma 8.12. □

Definition 4.13. *Für f und g aus S_k definieren wir das Petersson Skalarprodukt wie folgt:*

$$\langle f, g\rangle := \int_{\mathcal{F}} f(\rho + i\sigma)\,\overline{g(\rho + i\sigma)}\sigma^k \frac{d\rho\, d\sigma}{\sigma^2}$$

Satz 4.14. *Das Petersson Skalarprodukt hängt nicht vom gewählten Fundamentalbereich ab.*

Beweis: siehe [Kn] Thm 8.13. □

4.2 Der Fundamentalbereich von $\Gamma(1)$

Die Gruppe $\Gamma(1)$ wird erzeugt von den Elementen
$S = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ und $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1)$ wirkt auf $\tau \in \mathbb{H}$ wie folgt: $\gamma\tau = \frac{a\tau+b}{c\tau+d}$ und es gilt $S(\tau) = \frac{-1}{\tau}$ und $T(\tau) = \tau + 1$.

Definition 4.15. *Wir definieren den Fundamentalbereich*

$$\mathcal{F} := \left\{\tau \in \mathbb{H} \mid -\frac{1}{2} < Re(\tau) < 0 \text{ und } \mid \tau \mid > 1\right\} \cup \left\{\tau \in \mathbb{H} \mid 0 \le Re(\tau) \le \frac{1}{2} \text{ und } \mid \tau \mid \ge 1\right\}$$

Definition 4.16. *Zwei Punkte $\tau \in \mathbb{H}$, $\tau' \in \mathbb{H}$ nennen wir genau dann $\Gamma(1)$-äquivalent, wenn es ein $\gamma \in \Gamma(1)$ gibt mit $\tau' = \gamma\tau$.*

Satz 4.17. *Jeder Punkt in $\mathbb{H}$ ist genau zu einem Punkt in $\mathcal{F}$ $\Gamma(1)$-äquivalent.*

Beweis: siehe [Kn] Thm 8.5. □

Ist τ eine Nullstelle einer Modulform, so sind offenbar auch alle $\Gamma(1)$-äquivalenten Punkte Nullstellen dieser Modulform. Deswegen beschränken wir die Suche der Nullstellen im Folgenden auf $\mathcal{F}$.

Satz 4.18. *Die einzigen Punkte aus $\mathcal{F}$, die von einem Element $1 \neq \gamma \in \Gamma(1)$ fix gelassen werden, sind i mit dem Stabilisator $\{1, S\}$ und $\rho = e^{\pi i/3}$ mit dem Stabilisator $\left\{1, TS, (TS)^2\right\}$.*

Beweis: siehe [Ac1] Thm 8.5. □

Satz 4.19. *Für eine Modulform $f \not\equiv 0$ vom Gewicht k gilt:*

$$v_\infty(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_\rho(f) + \sum_{\tau \in \mathcal{F}\setminus\{i,\rho\}} v_\tau(f) = \frac{k}{12}$$

Beweis: siehe [Kn] Thm 8.5. □

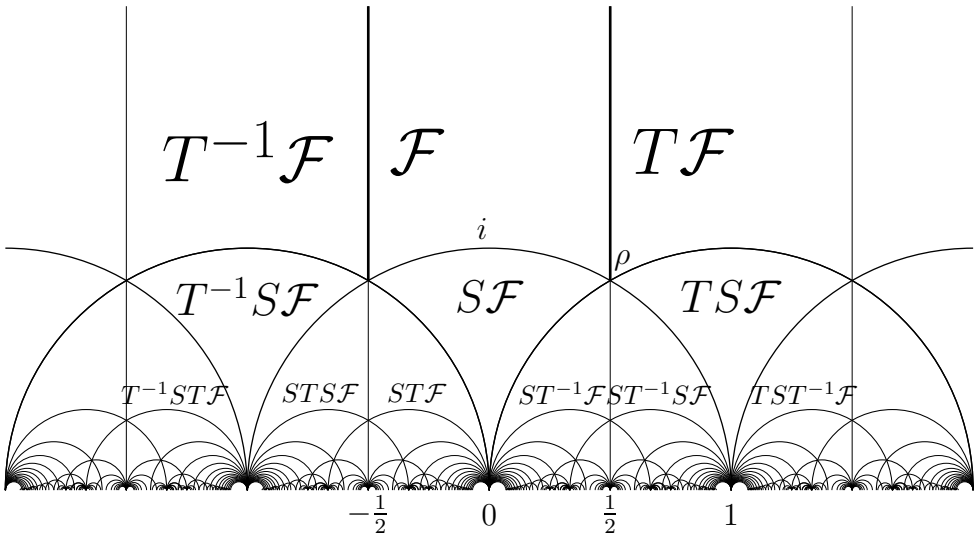

Abbildung 1: $\Gamma(1)$-Kachelung der oberen Halbebene

4.3 Heegner Punkte und ihre Verteilung

In diesem Abschnitt wollen wir uns mit einer speziellen Teilmenge der CM-Punkte beschäftigen, den Heegner Punkten.

Definition 4.20. *Zu der Fundamentaldiskriminante $d < 0$ definieren wir die Heegner Punkte:*

$$\Lambda_d = \left\{ \frac{-b+\sqrt{d}}{2a} \in \mathcal{F}_{\Gamma(1)} \mid b^2 - 4ac = d \text{ und } (a,b,c) = 1 \right\}$$

Lemma 4.21. *Zu der Fundamentaldiskriminante d gibt es genau $h\left(\mathbb{Q}\left(\sqrt{d}\right)\right)$ viele Heegner Punkte.*

Beweis: Siehe [Du] S.75. □

Satz 4.22. *Sei $d\mu(z) = \frac{3}{\pi}\frac{dx\,dy}{y^2}$, so daß $\mu\left(\mathcal{F}_{\Gamma(1)}\right) = 1$. Sei $\Omega \subset \mathcal{F}_{\Gamma(1)}$ (hyperbolisch) konvex, mit stückweise glattem Rand. Dann gibt es ein $\delta > 0$, das nur von Ω abhängt, so daß:*

$$\frac{\#(\Lambda_d \cap \Omega)}{\#\Lambda_d} = \mu(\Omega) + O\left(|d|^{-\delta}\right) \text{ für } d \to -\infty$$

Beweis: Siehe [Du] Thm.1. □

4.4 Höhere Level

Definition 4.23. *Wir definieren die Wirkung einer Untergruppe* Γ *von* $PSL_2(\mathbb{R})$ *auf der oberen Halbebene* $\overline{\mathbb{H}}$ *analog zur Wirkung von* $\Gamma(1)$.

Bisher haben wir ausschließlich Modulformen zur Gruppe $\Gamma(1)$ betrachtet. In analoger Weise können wir auch Modulformen zu Untergruppen von $\Gamma(1)$ definieren. Wir beschränken uns auf die Kongruenzuntergruppen von $\Gamma(1)$. Diese sind:

$$\begin{aligned}
\Gamma(N) &:= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \mid \begin{smallmatrix} a \equiv 1 \, mod \, N & b \equiv 0 \, mod \, N \\ c \equiv 0 \, mod \, N & d \equiv 1 \, mod \, N \end{smallmatrix} \right\} \\
\Gamma_0(N) &:= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \mid c \equiv 0 \, mod \, N \right\} \\
\Gamma^0(N) &:= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \mid b \equiv 0 \, mod \, N \right\}
\end{aligned}$$

Dabei heißt $N \in \mathbb{N}$ das Level. Wir bemerken, daß $\Gamma(1) = PSL_2(\mathbb{Z})$.

Satz 4.24. *Die Kongruenzuntergruppen von* $\Gamma(1)$ *haben endlichen Index in* $\Gamma(1)$*, den wir mit der Eulerschen* φ*-Funktion beschreiben.*

$$\varphi(N) := N \cdot \prod_{\substack{p|N \\ p \, prim}} \left(1 - p^{-1}\right) \qquad \psi(N) := N \cdot \prod_{\substack{p|N \\ p \, prim}} \left(1 + p^{-1}\right)$$

$$[\Gamma(1) : \Gamma(N)] = N \cdot \varphi(N) \cdot \psi(N) \qquad [\Gamma(1) : \Gamma_0(N)] = \psi(N)$$

Beweis: siehe [HBJ] S. 122. □

Im Folgenden sei $\Gamma \subset \Gamma(1)$ eine Untergruppe mit endlichem Index. Die Gruppe $\Gamma(1)$ wirkt transitiv auf dem $\mathbb{P}_1(\mathbb{Q})$. Das gilt nicht notwendigerweise für ihre Untergruppen, deswegen definieren wir:

Definition 4.25. *Die Bahnen bezüglich der Wirkung von* Γ *auf* $\mathbb{P}_1(\mathbb{Q})$ *nennen wir die Spitzen (cusps) von* Γ.

Definition 4.26. *Ein Punkt, dessen Stabilisatorgruppe nicht trivial, aber endlich ist, heißt elliptischer Punkt.*

Bemerkung 4.27. *Die Anzahl der Spitzen von* $\Gamma(1)$ *ist* 1*, von* $\Gamma(2)$ *ist sie* 3 *und von* $\Gamma(N)$ *ist sie* $\frac{[\Gamma(1):\Gamma(N)]}{2N}$ *für alle* $N > 2$*. Siehe [Sc] S.158.*

Auch zu einer Untergruppe Γ können wir einen Fundamentalbereich angeben. Dieser besteht z. B. aus $[\Gamma(1) : \Gamma]$ geeigneten $\Gamma(1)$-Translaten von $\mathcal{F}$.

Beispiel 4.28. *Ein Fundamentalbereich zu* $\Gamma_0(2)$ *ist* $\mathcal{F}_{\Gamma_0(2)} := \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\mathcal{F} \cup \left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)\mathcal{F} \cup \left(\begin{smallmatrix}0&-1\\1&1\end{smallmatrix}\right)\mathcal{F}$. $\mathcal{F}_{\Gamma_0(2)}$ *hat zwei Spitzen* $C_{\Gamma_0(2)} = \{0, \infty\}$. *Ein Fundamentalbereich zu* $\Gamma(2)$ *ist* $\mathcal{F}_{\Gamma(2)} := \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\mathcal{F} \cup \left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)\mathcal{F} \cup \left(\begin{smallmatrix}0&-1\\1&1\end{smallmatrix}\right)\mathcal{F} \cup \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\mathcal{F} \cup \left(\begin{smallmatrix}1&-1\\1&0\end{smallmatrix}\right)\mathcal{F} \cup \left(\begin{smallmatrix}1&-2\\1&-1\end{smallmatrix}\right)\mathcal{F}$. $\mathcal{F}_{\Gamma(2)}$ *hat drei Spitzen* $C_{\Gamma(2)} = \{0, 1, \infty\}$.

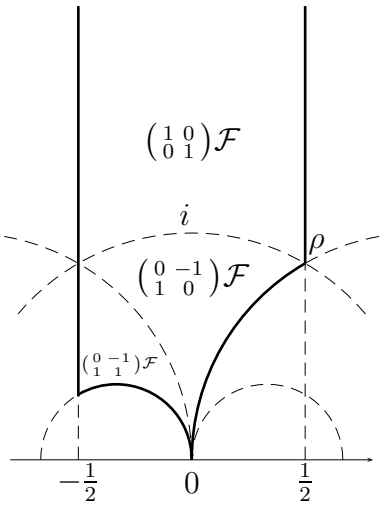

Abbildung 2: Ein Fundamentalbereich zu $\Gamma_0(2)$

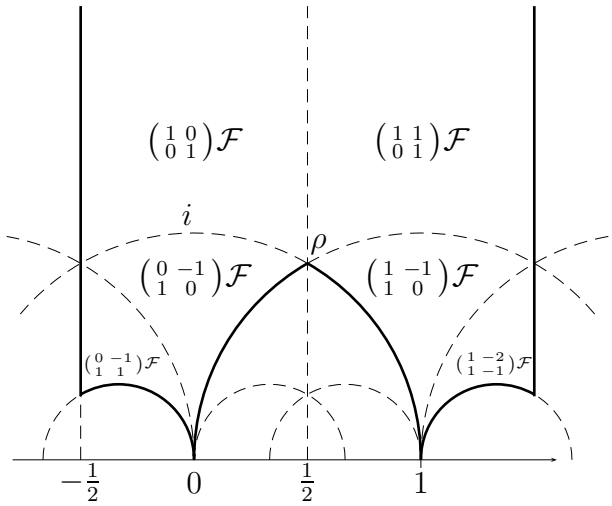

Abbildung 3: Ein Fundamentalbereich zu $\Gamma(2)$

Bemerkung 4.29. *Im Internet gibt es eine interaktive Seite [Ve] zum Zeichnen verschiedener Fundamentalbereiche.*

Definition 4.30. *Wir definieren eine Topologie auf* $\overline{\mathbb{H}}$ *wie folgt:*

- *für* $\tau \in \mathbb{H}$ *wählen wir eine offene Umgebung aus der üblichen Topologie von* $\mathbb{H}$
- *für* $\tau = i\infty$ *nehmen wir die offenen Mengen* $\{\tau \in \mathbb{H} \mid \mathrm{Im}(\tau) > c\} \cup \{\infty\}$ *für alle* $c > 0$
- *für* $\tau \in \mathbb{Q}$ *nehmen wir die offenen Mengen* $\{$*Das Innere der Kreisscheibe in* $\mathbb{H}$ *mit Radius* ϵ*, die in* τ *die reelle Achse als Tangente hat*$\} \cup \{\tau\}$ *für alle* $\epsilon > 0$

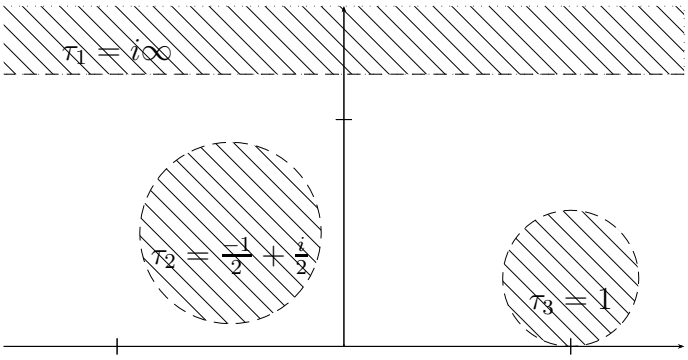

Abbildung 4: Einige offene Mengen in $\overline{\mathbb{H}}$

Bemerkung 4.31. *Diese Topologie ist verträglich mit der Gruppenwirkung einer Kongruenzuntergruppe. Mit dieser Topologie ist* $\overline{\mathbb{H}}$ *ein Hausdorffraum. Wir definieren* $Y(\Gamma) = \Gamma \setminus \mathbb{H}$ *und* $X(\Gamma) = \Gamma \setminus \overline{\mathbb{H}}$ *und bemerken, daß gilt* $Cusps(\Gamma) = X(\Gamma) - Y(\Gamma)$. *Mit der Quotiententopologie ist* $X(\Gamma)$ *ein kompakter Hausdorffraum. Darüber hinaus besitzt* $X(\Gamma)$ *auch eine komplexe Struktur und ist so eine Riemannsche Fläche.*

Definition 4.32. *Die Riemannsche Fläche* $X(\Gamma)$ *heißt die Modulkurve zu* Γ.

Definition 4.33. *Das Geschlecht* $g(\Gamma)$ *einer Kongruenzuntergruppe* Γ *ist das Geschlecht der zugehörigen Modulkurve* $X(\Gamma)$.

Beispiel 4.34. *Die Gruppe* $X(\Gamma(1))$ *hat Geschlecht* 0 *und* $X(\Gamma(6))$ *hat Geschlecht* 1.

Lemma 4.35. *Sei* Γ *eine Kongruenzuntergruppe und seien weiter*

- $\mu = [\Gamma : \Gamma(1)]$
- ν_2 *und* ν_3 *die Anzahl der elliptische Punkte in* $\mathcal{F}_\Gamma$
- ν_∞ *die Anzahl der Spitzen in* $\mathcal{F}_\Gamma$

Dann gilt:

$$g(\Gamma) = 1 + \frac{\mu}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2}$$

Beweis: Siehe [Sh3] Proposition 1.40. □

4.5 Modulformen zu höherem Level

Für $A \in SL_2(\mathbb{R})$ und $k \in \mathbb{N}$ wirkt der Slash-Operator $(f \mid_k A)$ auf Funktionen $f : \mathbb{H} \to \mathbb{C}$ wie folgt:

$$(f \mid_k A)(\tau) := (c\tau + d)^{-k} \cdot f(A\tau).$$

Definition 4.36. *Eine Funktion $f : \mathbb{H} \to \mathbb{C}$ heißt Modulform vom Gewicht k zur Kongruenzuntergruppe Γ, wenn:*

1. *f ist holomorph auf $\mathbb{H}$*
2. *$f \mid_k A = f$ für alle $A \in \Gamma$*
3. *für alle $S \in SL_2(\mathbb{Z})$ hat $f \mid_k S$ eine Fourierentwicklung in $i\infty$.*

Für weitere Definitionen benötigen wir die Weierstraßsche $\wp$-Funktion:

$$\wp(\tau, z) := \frac{1}{z^2} + \sum_{0 \neq \lambda \in (\mathbb{Z} + \tau\mathbb{Z})} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right)$$

Die Halbwerte der Weierstraßschen $\wp$-Funktion sind dann:

$$e_1(\tau) := \wp\left(\tau, \frac{1}{2}\right) = -\frac{1}{6} \cdot \left(1 + 24 \cdot \sum_{n=1}^{\infty} \sigma_1^{odd}(n)\, q^n\right) \qquad \in M_2(\Gamma_0(2))$$

$$e_2(\tau) := \wp\left(\tau, \frac{\tau}{2}\right) = \frac{1}{12} \cdot \left(1 + 24 \cdot \sum_{n=1}^{\infty} \sigma_1^{odd}(n)\, q^{\frac{n}{2}}\right) \qquad \in M_2\left(\Gamma^0(2)\right)$$

$$e_3(\tau) := \wp\left(\tau, \frac{1+\tau}{2}\right) =$$

$$= -\frac{1}{12} \cdot \left(1 + 24 \cdot \sum_{n=1}^{\infty} \sigma_1^{odd}(n)\, (-1)^n\, q^{\frac{n}{2}}\right) \qquad \in M_2\left(\left(\begin{smallmatrix} 1 & 1 \\ -1 & 0 \end{smallmatrix}\right)\Gamma_0(2)\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)\right),$$

wobei $\sigma_1^{odd}(n) = \sum_{d|n,\, d\ ungerade} d$. Aus der Theorie der elliptischen Kurven folgt, daß e_1, e_2 und e_3 paarweise verschieden sind. Weiter gilt: $e_1 + e_2 + e_3 = 0$. Wir werden insbesondere folgende Funktionen benötigen:

$$\begin{aligned}
\delta &:= -\frac{3}{2} e_1 && \in M_2(\Gamma_0(2)) \\
\epsilon &:= (e_1 - e_2)(e_1 - e_3) && \in M_4(\Gamma_0(2)) \\
\widetilde{\epsilon} &:= \frac{1}{16}(e_2 - e_3)^2 && \in M_4(\Gamma_0(2)) \\
\iota &:= (e_1 - e_2)(e_1 - e_3)(e_2 - e_3)^2 && \in S_8(\Gamma_0(2)) \\
\Delta &:= (e_1 - e_2)^2 (e_1 - e_3)^2 (e_2 - e_3)^2 && \in S_{12}(\Gamma(1))
\end{aligned}$$

Definition 4.37. *Sei* Γ *eine Kongruenzuntergruppe, so daß die kompakte Riemannsche Fläche* $\mathcal{R}_\Gamma := \overline{\Gamma \setminus \mathbb{H}}$ *das Geschlecht* 0 *hat. Ein Hauptmodul* j_Γ *ist eine Modulfunktion zu* Γ*, mit der man ein Isomorphismus von* $\mathcal{R}_\Gamma$ *nach* $\mathbb{P}^1(\mathbb{C})$ *erhält, der* $i\infty$ *auf* ∞ *abbildet. Ist* j_Γ *ein Hauptmodul, so ist auch* $\alpha j_\Gamma + \beta$ *für alle* $\alpha,\ \beta \in \mathbb{C} \setminus \{0\}$ *ein Hauptmodul. Wir wählen diese Konstanten so, daß der konstante Term in der Reihenentwicklung des Hauptmoduls verschwindet und der erste Koeffizient, der nicht verschwindet* 1 *ist und nennen diesen Hauptmodul einen normalisierten Hauptmodul.*

In Zukunft werden wir stets normalisierte Hauptmoduln meinen, wenn wir von Hauptmoduln reden.

Satz 4.38. *Sei* Γ *eine Kongruenzuntergruppe, so daß die kompakte Riemannsche Fläche* $\mathcal{R}_\Gamma := \overline{\Gamma \setminus \mathbb{H}}$ *das Geschlecht* 0 *hat. Dann existiert der Hauptmodul zu* Γ *und ist eindeutig.*

Beweis: Siehe [Bo] S.407.

□

Beispiel 4.39. *Der Hauptmodul zu* $\Gamma(1)$ *ist*

$$j_{\Gamma(1)} = j - 744 = q^{-1} + 0 + 196884q + ...$$

Der Hauptmodul zu $\Gamma_0(2)$ *ist*

$$24 + q^{-1} \prod_{m>0} \left(1 - q^{2m+1}\right) = q^{-1} + 0 + 276q - 2048q^2 + ...$$

Satz 4.40 (Valenzformel)**.** *Sei* $0 \neq f \in M_k(\Gamma)$*, dann gilt:*

$$\sum_{S \in C(\Gamma)} [\Gamma(1)_S : \Gamma_S] \cdot ord_S(f) + \sum_{\tau \in \Gamma \setminus \mathbb{H}} \frac{1}{\mid \Gamma_\tau \mid} ord_\tau(f) = \frac{k}{12} [\Gamma(1) : \Gamma],$$

wobei $C(\Gamma)$ *die Spitzen von* Γ *bezeichnet und wir* Γ_S *für* $Stab_\Gamma(S)$ *schreiben.*

Beweis: siehe [HBJ] Thm 4.1.

□

Bemerkung 4.41. *Dies ist die Verallgemeinerung vom Satz 4.19.*

4.6 Eisensteinreihen zu höherem Level

Seien $N \geq 1$ und $k \geq 3$ zwei natürliche Zahlen. Seien weiter $m = (m_1, m_2)$ und $a = (a_1, a_2)$ zwei Paare ganzer Zahlen und $w = (w_1, w_2)$ ein Paar komplexer Zahlen mit der Eigenschaft $\frac{w_1}{w_2} \in \mathbb{H}$. Die Menge dieser komplexen Paare bezeichenen wir mit W. Wir schreiben $m \cong a \ mod \ N$, falls gilt $m_1 \equiv a_1 \ mod \ N$ und $m_2 \equiv a_2 \ mod \ N$. Weiter bezeichnen $\mathbb{P}^1(\mathbb{C})$ die Riemannsche Zahlenkugel und $\sum'$ die Summation, bei der nicht über den Index 0 summiert wird.

Definition 4.42. *Die homogene Eisensteinreihe* $G_{N,k,a} : W \to \mathbb{P}^1(\mathbb{C})$ *wird gegeben durch* $G_{N,k,a}((w_1, w_2)) = \sum'_{m \equiv a \ mod \ N} (m_1 w_1 + m_2 w_2)^{-k}$
Die inhomogene Eisensteinreihe $G_{N,k,a} : \mathbb{H} \to \hat{\mathbb{C}}$ *wird gegeben durch* $G_{N,k,a}(\tau) = \sum'_{m \equiv a \ mod \ N} (m_1 \tau + m_2)^{-k}$.
Wir nennen $G_{N,k,a}$ *eine primitive Eisensteinreihe, falls der größte gemeinsame Teiler* $(a_1, a_2, N) = 1$.
Wir definieren eine reduzierte Eisensteinreihe $G^*_{N,k,a}((w_1, w_2))$*:* $W \to \hat{\mathbb{C}}$ *mit*

$$G^*_{N,k,a}((w_1, w_2)) = \sum_{m \equiv a \ mod \ N, \ (m_1, m_2) = 1}{}' (m_1 w_1 + m_2 w_2)^{-k}.$$

Satz 4.43. *Für alle* a, $N \geq 1$ *und* $k \geq 3$ *sind die inhomogenen Eisensteinreihen* $G_{N,k,a}$ *Modulformen zur Gruppe* $\Gamma(N)$ *und zum Gewicht* k.

Beweis: siehe [Sc] Thm VII.1 □

Bemerkung 4.44. *Die Eisensteinreihen zu höherem Level sind eng mit den* N*-Teilungspunkten der Ableitungen der Weierstraßschen* $\wp$*-Funktion verbunden.*

$$\wp^{(k-2)}\left(\frac{a_1 w_1 + a_2 w_2}{N}, w\right) = (-1)^{k-1}(k-1)! N^k G_{N,k,a}(w),$$

wobei $\wp^{(k-2)}(z, w)$ *die* $(k-2)$*-te Ableitung nach* z *bezeichnet.*
Vergleiche [Sc] S.157.

Definition 4.45. *Sei* $\Gamma = \bigcup_{\nu=1}^{\mu} \Gamma(N) A_\nu$ *eine Kongruenzuntergruppe zum Level* N *mit* $\mu = [\Gamma : \Gamma(N)]$. *Dazu definieren wir* $G^*_{\Gamma,k,a} = \sum_{\nu=1}^{\mu} G^*_{N,k,a} \mid_k A_\nu$ *für* $(a_1, a_2) = 1$.

Satz 4.46. *Seien* $k > 2$ *gerade und* Γ *eine Kongruenzuntergruppe vom Level* N. *Dann gibt es eine Linearkombination von* $G_{N,k,a}$ *welche eine Modulform von* Γ *ist, die in allen bis auf einer beliebigen Spitze von* Γ *verschwindet. Den Unterraum der Modulformen zum Gewicht* k *von* Γ*, der von solchen Linearkombinationen erzeugt ist, nennen wir den Eisensteinraum zum Gewicht* k *von* Γ. *Seine* $\mathbb{C}$*-Dimension entspricht der Anzahl der Spitzen von* Γ.

Beweis: Siehe [Sc] Thm VII.4 □

Bemerkung 4.47. *Die Anzahl der Spitzen von* $\Gamma(N)$ *ist in Bemerkung 4.27 angegeben.*

5 Hecke-Operatoren und Hecke-Eigenformen

In diesem Kapitel erklären wir die Hecke-Operatoren. Sie wirken auf dem Vektorraum der Modulformen und haben simultane Eigenvektoren, jene Eigenformen, deren Nullstellen der Gegenstand dieser Arbeit sind.

5.1 Der Hecke-Operator auf Gittern und Modulformen

Obwohl uns eigentlich interessiert, wie der Hecke-Operator auf Modulformen wirkt, werden wir ihn zuerst auf Gittern definieren. Seien also im Folgenden $\mathcal{L}$ die Menge der echten Gitter in $\mathbb{C}$ und $\Lambda \in \mathcal{L}$. Wir definieren nun zwei Operatoren auf $Div(\mathcal{L})$.

Definition 5.1. *Für $n \in \mathbb{N}$ definieren wir den n-ten Hecke-Operator $T(n)\Lambda := \sum_{[\Lambda:\Lambda']=n} \Lambda'$ und für $c \in \mathbb{C}$ definieren wir den Homothetie-Operator $R_c\Lambda := c\Lambda$.*

Satz 5.2. *Hecke-Operator und der Homothetie-Operator operieren beide auf $Div(\mathcal{L})$, weswegen wir sie verknüpfen können und es gelten folgende Rechenregeln:*

- $R_{c_1}R_{c_2} = R_{c_1c_2}$ *für alle* $c_1, c_2 \in \mathbb{C}$
- $R_cT(n) = T(n)R_c$ *für alle* $c \in \mathbb{C}, n \in \mathbb{N}$
- $T(mn) = T(m)T(n)$ *falls* $(m,n) = 1$
- $T(m)T(n) = T(n)T(m)$ *für* $m, n \in \mathbb{N}$
- $T(p^e)T(p) = T(p^{e+1}) + pT(p^{e-1})R_p$ *falls p prim und* $e > 1$

Beweis: siehe [Si2] Thm 9.1. □

Definition 5.3. *Eine Funktion $\widetilde{f} : \mathcal{L} \to \mathbb{C}$ nennen wir homogen vom Grad $-n$, falls gilt:*

$$\widetilde{f}(\alpha\Lambda) = \alpha^{-n}\widetilde{f}(\Lambda) \text{ für alle } \alpha \in \mathbb{C}^*$$

Lemma 5.4. *Die Abbildung $f \mapsto \widetilde{f}$ gegeben durch $\widetilde{f}(\Lambda_\tau) := f(\tau)$ ist eine Bijektion zwischen den schwach modularen Funktionen zum Gewicht k und den homogenen Funktionen vom Grad $-k$.*

Beweis: siehe [Kn] S. 243. □

Definition 5.5. *Wir definieren den n-ten Hecke-Operator auf homogenen Gitterfunktionen vom Grad $-k$ wie folgt:*

$$\left(T_k(n)\,\widetilde{f}\right)(\Lambda) = n^{k-1} \sum_{[\Lambda:\Lambda']=n} \widetilde{f}(\Lambda')$$

Bemerkung 5.6. *Seien $\Lambda = (\omega_1, \omega_2)$ und $\Lambda' = (\omega_1', \omega_2')$. Es soll gelten:*

$$\begin{pmatrix}\omega_1'\\ \omega_2'\end{pmatrix} = A \begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}$$

Also ist A eine Matrix mit ganzzahligen Einträgen und Determinante n. Die allgemeinste Form einer Basis für Λ' erhalten wir, wenn wir die linke Seite der Gleichung mit einem Element aus $\Gamma(1)$ multiplizieren. Die rechte Nebenklasse $\Gamma(1)A$ ist also die Menge der Matrizen, die Λ nach Λ' abbilden.
Sei $M(n)$ die Menge der 2×2 Matrizen mit ganzzahligen Einträgen und Determinante n. Da es nur endliche viele Untergitter mit Index n zu Λ gibt, gibt es eine Zerlegung von $M(n)$ in rechte Nebenklassen der Form:

$$M(n) = \bigcup_{i=1}^{\nu(n)} \Gamma(1)\,\alpha_i$$

Das Ergebnis des Slash-Operators ist i. a. nicht $\Gamma(1)$-invariant. Eine Funktion auf der oberen Halbebene ist genau dann eine Modulform, wenn sie der Slash-Operator für alle Element aus $\Gamma(1)$ invariant lässt. Wir interessieren uns besonders für folgende Spezialfälle:

$$\begin{aligned} V_m f(\tau) &= m^{-\frac{k}{2}} \left(f \mid_k \begin{pmatrix} m & 0\\ 0 & 1\end{pmatrix}\right)(\tau) = f(m\tau) \text{ und}\\ U_m f(\tau) &= m^{\frac{k}{2}-1} \sum_{j=1}^{m} \left(f \mid_k \begin{pmatrix} 1 & j\\ 0 & m\end{pmatrix}\right)(\tau), \end{aligned}$$

wobei ($m \in \mathbb{N}$). Beide bilden Formen vom Gewicht k zum Level N auf solche vom Level mN, wie folgt ab: $V_m \sum a(n) q^n = \sum a(n) q^{mn}$ bzw. $U_m \sum a(n) q^n = \sum a(mn) q^n$. Dabei kann es vorkommen, daß das Level auch kleiner sein kann. Wir arbeiten vorerst zum Level 1.

Definition 5.7. *Aus dem Slash-Operator können wir nun den n-ten Hecke-Operator vom Gewicht k definieren:*
$T(n) f(\tau) = n^{\frac{k}{2}} \sum_{\mu \in \Gamma(1)\backslash M_n} f \mid_k \mu = n^{k-1} \sum_{\left(\begin{smallmatrix} a & b\\ c & d\end{smallmatrix}\right) \in \Gamma(1)\backslash M_n} (c\tau + d)^{-k} f\left(\frac{a\tau+b}{c\tau+d}\right)$.

Lemma 5.8. *Der Hecke-Operator bildet M_k in M_k und die Koeffizienten wie folgt ab: $a_m \mapsto \sum_{d|m,n} d^{k-1} a_{\frac{nm}{d^2}}$, also werden Spitzenformen auf Spitzenformen abgebildet.*

Beweis: siehe [Kn] Thm 8.16. □

Lemma 5.9. *Die Hecke-Operatoren zum Gewicht k erfüllen folgende Multiplikationsformel:* $T(n)T(m) = \sum_{d|m,n} d^{k-1}T\left(\frac{nm}{d^2}\right)$, *insbesondere ist die Verknüpfung kommutativ und es gilt* $T(n)T(m) = T(nm)$ *für* $(n,m) = 1$. *Sei p eine Primzahl, dann gilt* $T(p) = U_p + p^{k-1}V_p$ *und es gilt die Rekursionsformel* $T(p^{r+1}) = T(p^r)T(p) - p^{k-1}T(p^{r-1})$. *Folglich genügt es die Hecke-Operatoren* $T(p)$ *zu kennen.*

Beweis: siehe [Kn] Lemma 8.18. □

5.2 Hecke-Eigenformen

Satz 5.10. *Die Hecke-Operatoren* $T_k(n)$ *sind bezüglich des Petersson Skalarproduktes selbstadjungiert.*

Beweis: siehe [Kn] Thm 8.22. □

Lemma 5.11. *Die Hecke-Operatoren besitzen simultane Eigenformen. Ist also h eine Eigenform zu* $T(n)$ *so auch zu allen* $T(m)$.

Beweis: siehe [Kn] S.254. □

Definition 5.12. *Da der Hecke-Operator ein linearer Operator auf einem Vektorraum und selbstadjungiert bezüglich des Petersson Skalarproduktes ist, besitzt er Eigenformen, die sogenannten Hecke-Eigenformen. Das heißt, es existieren* $h \in M_k$, *so daß* $T(n)h = \lambda_n h$ *für bestimmte* λ_n *ist.*

Bemerkung 5.13. *Für die Koeffizienten von Eigenformen gilt* $\lambda_n a(m) = \sum_{d|m,n} d^{k-1}a\left(\frac{nm}{d^2}\right)$, *insbesondere gilt* $\lambda_n a(1) = a(n)$. *Daraus folgt, dass* $a(1) \neq 0$ *für* $f \not\equiv 0$, *also können wir* $a(1) = 1$ *normieren. Wir werden im Weiteren nur normierte Hecke-Eigenformen als solche bezeichnen. Für eine Hecke-Eigenform gilt* $\lambda_n = a(n)$ *und* $a(n)a(m) = \sum_{d|m,n} d^{k-1}a\left(\frac{nm}{d^2}\right)$. *Insbesondere sind für teilerfremde n, m auch* $a(n)$ *und* $a(m)$ *multiplikativ und* $a(p^r)$ *rekursiv beschreibbar, so daß es genügt, die* $a(p)$ *für p prim zu kennen.*
Siehe dazu [Za] S. 256.

Die Eisensteinreihen und Δ sind Hecke-Eigenformen. Die Hecke-Eigenformen in M_k bilden eine Basis von M_k und die Koeffizienten einer Hecke-Spitzenform sind reelle, algebraische Zahlen vom Grad $\leq dim S_k$. Siehe dazu [Za] S.257.

Definition 5.14. *Nun definieren wir die Hecke-L-Reihe einer Modulform* $f(\tau) = \sum_{m\geq 0} a(m) q^m$ *als* $L(f,s) = \sum_{m\geq 1} \frac{a(m)}{m^s}$.

Satz 5.15. *Ist f eine Hecke-Eigenform, dann haben wir das Eulerprodukt*

$$L(f,s) = \prod_{p\ prim} \left(1 + \frac{a(p)}{p^s} + \frac{a(p^2)}{p^{2s}} + ...\right) = \prod_{p\ prim} \frac{1}{1 - a(p)\, p^{-s} + p^{k-1-2s}}$$

Da die Fourrierkoeffizienten einer Modulform f folgenden Abschätzungen genügen: $a(n) = O\left(n^{k-1}\right)$, *bzw. für Spitzenformen* $a(n) = O\left(n^{\frac{k}{2}}\right)$, *konvergiert die L-Reihe* $L(f,s)$ *für* $\mathrm{Re}(s) > k$, *bzw. für* $\mathrm{Re}(s) > \frac{k}{2} + 1$ *bei Spitzenformen absolut. Die L-Reihe zu einer Spitzenform läßt sich holomorph auf ganz* $\mathbb{C}$ *fortsetzen. Die L-Reihe einer Nicht-Spitzenform läßt sich meromorph auf* $\mathbb{C}$ *fortsetzen und hat einen einzigen einfachen Pol bei* $s = k$ *mit Residuum* $\frac{(2\pi i)^k}{(k-1)!} a(0)$.

Beweis: Siehe [Za] S.260. □

Satz 5.16. *Eisensteinreihen sind Hecke-Eigenformen.*

Beweis: Siehe [Ko1] S.164 □

5.3 Hecke-Operatoren zu höherem Level

Definition 5.17. *Sei*

$$M(n,N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mid det\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = n,\ c \equiv 0\ mod\ N,\ (a,N) = 1 \right\}.$$

Sei weiter f eine Modulform zum Gewicht k zur Gruppe $\Gamma_0(N)$. *Wir definieren den n-ten Hecke-Operator als:*

$$T_k(n) f = n^{\frac{k}{2}-1} \sum_{\mu \in\, \Gamma_0(N)\backslash M(n,N)} f\ |_k\ \mu$$

Satz 5.18. *Sei* $f(\tau) = \sum_{n=0}^{\infty} c_n q^n$ *eine Modulform zum Gewicht k und zur Gruppe* $\Gamma_0(N)$. *Dann gilt:*

$$T_k(m) \sum_{n=0}^{\infty} c_n q^n = \sum_{n=0}^{\infty} b_n q^n,$$

wobei

$$b_n = \begin{cases} c_0 \sum_{a|m,\, a>0,\, (a,n)=1} a^{k-1} & wenn\ n = 0 \\ c_m & wenn\ n = 1 \\ \sum_{a|(n,m),\, (a,N)=1} a^{k-1} c_{\frac{nm}{a^2}} & wenn\ n > 1 \end{cases}$$

Insbesondere bildet $T_k(m)$ *Modulformen vom Gewicht k zur Gruppe* $\Gamma_0(N)$ *auf solche ab und Spitzenformen bleiben Spitzenformen.*

Beweis: Siehe [Kn] Thm. 9.15. □

Satz 5.19. *Seien $p \in \mathbb{N}$ prim und $r \in \mathbb{N}$. Der Hecke-Operator für $\Gamma_0(N)$ besitzt folgende Eigenschaften:*

- $T_k(p^r)\,T_k(p) = T_k(p^{r+1}) + p^{k-1}T_k(p^{r-1})$, *falls* $p \nmid N$
- $T_k(p^r) = T_k(p)^r$, *falls* $p \mid N$
- $T_k(m)\,T_k(n)$, *falls* $(n,m) = 1$
- *Die Algebra, die von den $T_k(n)$ erzeugt wird, wird bereits von den $T_k(p)$ erzeugt und ist kommutativ.*

Beweis: Siehe [Kn] Thm. 9.17. □

Satz 5.20. *Die Hecke-Operatoren $T_k(n)$ sind für $(n,N) = 1$ auf dem Raum der Spitzenformen zum Gewicht k und zur Gruppe $\Gamma_0(N)$ bezüglich des Petersson Skalarproduktes selbstadjungiert.*

Beweis: Siehe [Kn] Thm 9.18. □

Bemerkung 5.21. *Die Hecke-Operatoren $T_k(n)$ auf $S_k(\Gamma_0(N))$mit $(n,N) = 1$ kommutieren und sind selbstadjungiert bezüglich des Petersson Skalarproduktes, daher besitzen sie simultane Eigenvektoren, die Hecke-Eigenformen.*

6 Die Nullstellen der Hecke-Eigenformen zu $\Gamma(1)$

In diesem Kapitel beschäftigen wir uns mit der Bestimmung der nichttrivialen Nullstellen der Hecke-Eigenformen. Wir geben hierfür einen Rechenweg und einige numerische Beispiele an. Wir werden sehen, daß die j-Werte der Nullstellen algebraische Zahlen sind und folgern mit Waldschmidt, daß die Nullstellen imaginärquadratisch oder transzendent sind.

6.1 Rechenweg

Der Raum der Modulformen M_k zum Gewicht k hat die Dimension

$$d = \begin{cases} 0 & : \quad k < 0 \; oder \; k \; ungerade \\ \left[\frac{k}{12}\right] & : \quad k \equiv 2 \; mod \; 12 \\ \left[\frac{k}{12}\right] + 1 & : \quad k \not\equiv 2 \; mod \; 12 \end{cases}$$

Wir wählen eine Basis B_i mit $i \in \{1, .., d\}$ wie folgt:

$$B_i = \Delta^{i-1} \cdot (240G_4)^{3(d-i)} \cdot Rest_k$$

$$\text{wobei } Rest_k = \begin{cases} 240G_4 & : \quad k \; mod \; 12 = 4 \\ 504G_6 & : \quad k \; mod \; 12 = 6 \\ (240G_4)^2 & : \quad k \; mod \; 12 = 8 \\ 504G_6 \cdot 240G_4 & : \quad k \; mod \; 12 = 10 \\ 1 & : \quad k \; mod \; 12 = 0 \\ 504G_6 \cdot (240G_4)^2 & : \quad k \; mod \; 12 = 2 \end{cases}$$

Da Δ im Gegensatz zu G_4 und G_6 eine Spitzenform ist, sind die ersten $i-1$ Koeffizienten von B_i null und der i-te nicht null. Deswegen sind die B_i linear unabhängig. Lassen wir einen Hecke-Operator auf den B_i wirken, so können wir die Koeffizienten der Bilder explizit bestimmen und die Matrix $M \in Mat_n(\mathbb{Q})$ dieses Hecke-Operators zu dieser Basis angeben. Sei $(a_1, ..., a_d)$ ein Eigenvektor dieser Matrix, so ist $h = \sum_{i=1}^{d} a_i B_i$ eine Hecke-Eigenform vom Gewicht k. Es gilt: $h = Rest_k \cdot \sum_{i=1}^{d} a_i \frac{B_i}{Rest_k}$. Die Nullstellen von $Rest_k$ sind klar, da ρ die Nullstelle von G_4 in $\mathcal{F}$ und i die Nullstelle von G_6 in $\mathcal{F}$ ist. Im folgenden werden wir diese Nullstellen die trivialen nennen und nicht näher betrachten. Die Δ-Funktion hat keine Nullstellen in der oberen Halbebene. Deswegen hat h/Δ^{d-1} dieselben Nullstellen wie h. Zur Bestimmung der nichttrivialen Nullstellen betrachten wir

$$P(\tau) := \sum_{i=1}^{d} a_i \frac{B_i}{\Delta^{d-1} Rest_k} = \sum_{i=1}^{d} a_i j^{d-i} =: \mathcal{P}(j(\tau)).$$

Letztere fassen wir als Polynom in j auf. Die Nullstellen dieses Polynoms sind die j-Werte der gesuchten Nullstellen, insbesondere sind diese *algebraisch*.

Satz 6.1. *Die j-Werte der nichttrivialen Nullstellen der Hecke-Eigenformen sind algebraisch.*

□

Zu gegebenen j-Wert j_0 ist es jedoch nicht trivial, einen Repräsentanten in der oberen Halbebene, beziehungsweise im Fundamentalbereich zu finden. Um dies zu erreichen, betrachten wir die elliptische Kurve:

$$E_{j_0}:\ y^2 = x^3 - \frac{27}{4}\frac{j_0}{j_0 - 1728}x - \frac{27}{4}\frac{j_0}{j_0 - 1728},$$

wobei $j_0 \neq 0, 1728$ gelten soll.
Es gilt $j\left(E_{j_0}\right) = j_0$. Der Quotient der Perioden dieser elliptischen Kurve ist $\Gamma(1)$-äquivalent zu dem gesuchten τ. Diese Perioden zu berechnen ist zwar theoretisch mit Hilfe von elliptischen Integralen möglich, allerdings ist dieser Weg sehr schwierig. In einigen Fällen ist dies numerisch möglich (etwa bei reellen j-Werten mit PARI).

6.2 Numerische Ergebnisse

Zu den betrachteten Gewichten ist der Raum der Spitzenformen zweidimensional. Eine Hecke-Spitzenform bezeichnen wir mit $S_{k,a}$, wobei k das Gewicht bezeichnet und $a \in \{1, 2\}$ gilt. Die ersten nichttrivialen Nullstellen von Hecke-Eigenformen, die Spitzenformen sind, sind in Tabelle 1 aufgeführt.

6.3 Numerische Überlegungen

Bezeichne S_k weiterhin den Raum der Spitzenformen zu $\Gamma(1)$ vom Gewicht k und es gilt $d = dim\ S_k = O\left(\frac{k}{12}\right)$. Für die Koeffizienten a_n einer Spitzenform f gilt $a_n = O\left(n^{\frac{k-1}{2}}\right)$ (Vergleiche Satz 4.9.). Die Matrix M zum Hecke-Operator T_k ist eine $d \times d$ Matrix, deren Einträge sich aus den ersten d Koeffizienten von Spitzenformen berechnen. Für einen Eintrag m der Matrix gilt dann die Abschätzung $m = O\left((d-1)\, d^{\frac{(k-1)(d-1)}{2}}\right)$. Das heißt, die Einträge der Matrix werden sehr schnell sehr groß. Die QR-Zerlegung zum Ermitteln der Eigenwerte benötigt $O\left(d^3\right)$ Rechenoperationen.
Der algebraische Grad der Eigenwerte ist nach Maedas Vermutung d.

	j-Wert	Näherung mit PARI für $\tau \in \mathcal{F}$
$S_{24,1}$	$156 + 12\sqrt{144169}$	$1.31668827093162154236959\,i$
$S_{24,2}$	$156 - 12\sqrt{144169}$	$0.5 + 1.35891135936186970643239\,i$
$S_{28,1}$	$5076 + 108\sqrt{18209}$	$1.56714443425820336309028\,i$
$S_{28,2}$	$5076 - 108\sqrt{18209}$	$0.5 + 1.46937425431330922519206\,i$
$S_{30,1}$	$4128 + 96\sqrt{51349}$	$1.54910306023354897792413\,i$
$S_{30,2}$	$4128 - 96\sqrt{51349}$	$0.5 + 1.62168752025292408036404\,i$
$S_{32,1}$	$-18804 + 12\sqrt{18295489}$	$1.64986264555330829174880\,i$
$S_{32,2}$	$-18804 - 12\sqrt{18295489}$	$0.5 + 1.77754525117526278524722\,i$
$S_{34,1}$	$61272 + 72\sqrt{2356201}$	$1.91776764259776682337307\,i$
$S_{34,2}$	$61272 - 72\sqrt{2356201}$	$0.5 + 1.72198142654779792699184\,i$
$S_{38,1}$	$135420 + 4\sqrt{9737304801}$	$2.08210445183117557398867\,i$
$S_{38,2}$	$135420 - 4\sqrt{9737304801}$	$0.5 + 1.99962867145489382754831\,i$

Tabelle 1: Näherungslösungen der ersten nichttrivialen Nullstellen

6.4 Symmetrieeigenschaft der Nullstellen

Wir wollen nun die Abbildungseigenschaften der j-Funktion genauer betrachten. Sei $\tau = u + iv$. Dann gilt:

$$\overline{q(\tau)} = \overline{e^{-2\pi i(u+iv)}} = e^{-2\pi iu - 2\pi v} = q(-\overline{\tau})$$

Sei weiter M eine Modulform, deren Koeffizienten der Reihenentwicklungn *reell* sind, so gilt:

$$\overline{M(\tau)} = M(-\overline{\tau})$$

So wissen wir nun für die j-Funktion, daß sie auf dem Rand des Fundamentalbereiches und auf der imaginären Achse nur reelle Werte annimmt.
Im letzten Abschnitt haben wir gesehen, daß es zu jeder Hecke-Eigenform ein über $\mathbb{Q}$ definiertes Polynom gibt, dessen Nullstellen genau die j-Werte der Nullstellen dieser Hecke-Eigenform sind. Das heißt aber, daß zu jedem j-Wert $j(\tau)$ einer Nullstelle τ auch $\overline{j(\tau)} = j(-\overline{\tau})$ ein j-Wert einer Nullstelle ist. Deswegen liegen die Nullstellen einer Hecke-Eigenform symmetrisch zur imaginären Achse.

7 Die Nullstellen der Eisensteinreihen zu $\Gamma(1)$

Die Nullstellen der Eisensteinreihen sind bereits gut erforscht. So besagt der Satz von Rankin-Swinnerton-Dyer, daß die nichttrivialen Nullstellen der Eisensteinreihen einfach sind und auf dem Einheitskreis liegen. W. Kohnen zeigt weiter, daß sie transzendent sind und gibt eine Formel an, wie sie zu berechnen sind. In [Za] zeigt D. Zagier auf Seite 256, daß alle Eisensteinreihen Hecke-Eigenformen sind. Diese wollen wir im Folgendem eingehender untersuchen.

7.1 Der Satz von Rankin-Swinnerton-Dyer

In "On the Zeros of Eisenstein Series" [RSD] zeigen Rankin und Swinnerton-Dyer folgenden Satz:

Satz 7.1. *Die nichttrivialen Nullstellen der Eisensteinreihen im Fundamentalbereich $\mathcal{F}$ sind einfach und liegen auf dem Einheitskreis.*

Beweis: Die Eisensteinreihen sind gegeben wie folgt:

$$G_k(z) := \frac{1}{2} \sum_{(c,d)\in\mathbb{Z}^2\setminus(0,0)} (cz+d)^{-k}$$

Die Anzahl der Nullstellen der Reihe ist bekannt (nach der $\frac{k}{12}$-Formel). Sie schreiben k als $12n+s$ ($s \leq 14$) und mit der Tatsache, daß die Summe der Nullstellenordnungen in i und ρ gleich $\frac{s}{12}$ ist, genügt es zu zeigen, daß n Nullstellen auf dem Einheitskreis zwischen i und ρ liegen.
Dafür substituieren sie z mit $e^{i\theta}$, wobei $\theta \in \left(\frac{\pi}{2}, \frac{2\pi}{3}\right)$ ist und definieren

$$F_k(\theta) := e^{\frac{ik\theta}{2}} G_k\left(e^{i\theta}\right) = \frac{1}{2} \sum_{(c,d)\in\mathbb{Z}^2\setminus(0,0)} \left(ce^{\frac{i\theta}{2}} + de^{\frac{-i\theta}{2}}\right)^{-k}$$

Die vier Summanden $(c,d) = (0,\pm 1)$ oder $(\pm 1, 0)$ ergeben:
$\frac{1}{2}\left(e^{\frac{ik\theta}{2}} + e^{\frac{-ik\theta}{2}} + e^{\frac{ik\theta}{2}} + e^{\frac{-ik\theta}{2}}\right) = 2\cos(\frac{k\theta}{2})$ Die restliche Summe wird zu R_1 zusammengefaßt. Wir erhalten: $F_k(\theta) = 2\cos(\frac{k\theta}{2}) + R_1$. Ziel ist es nun zu zeigen, daß $\mid R_1 \mid \leq const < 2$, da wir dann wüssten, daß die stetige Funktion $F_k(\theta)$ n Vorzeichenwechsel hat.
Für alle $(c,d) \in \mathbb{Z}$ und für alle $\theta \in \left[\frac{\pi}{2}, \frac{2\pi}{3}\right]$ gilt:
$\mid ce^{\frac{i\theta}{2}} + de^{\frac{-i\theta}{2}} \mid^2 = \mid c\cos\left(\frac{\theta}{2}\right) + c\sin\left(\frac{\theta}{2}\right)i + d\cos\left(\frac{-\theta}{2}\right) + d\sin\left(\frac{-\theta}{2}\right)i \mid^2$
$= \left(c\cos\left(\frac{\theta}{2}\right) + d\cos\left(\frac{-\theta}{2}\right)\right)^2 + \left(c\sin\left(\frac{\theta}{2}\right) + d\sin\left(\frac{-\theta}{2}\right)\right)^2$
$= \left(c\cos\left(\frac{\theta}{2}\right) + d\cos\left(\frac{\theta}{2}\right)\right)^2 + \left(c\sin\left(\frac{\theta}{2}\right) - d\sin\left(\frac{\theta}{2}\right)\right)^2$

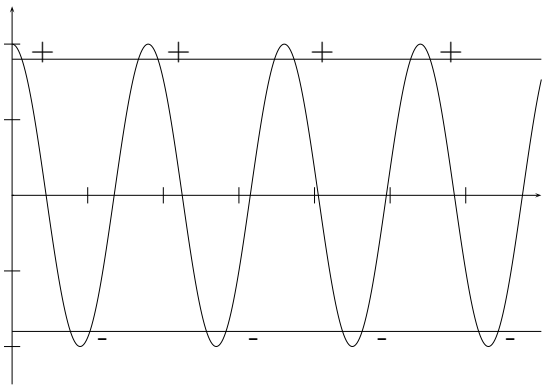

Abbildung 5: Skizze zum Beweis von RSD

$= c^2\left(\cos^2\left(\frac{\theta}{2}\right)+\sin^2\left(\frac{\theta}{2}\right)\right)+d^2\left(\cos^2\left(\frac{\theta}{2}\right)+\sin^2\left(\frac{\theta}{2}\right)\right)+2cd\cos^2\left(\frac{\theta}{2}\right)-2cd\sin^2\left(\frac{\theta}{2}\right)$
$= c^2+d^2+2cd\cos(\theta) \geq c^2+d^2+cd \geq c^2+d^2- \mid cd \mid \geq \frac{1}{2}(c^2+d^2)$

Nun stellt sich die Frage, wieviele $(c,d) \in \mathbb{Z}^2$ existieren mit $c^2+d^2=N$? Es gibt maximal $\sqrt{N}+1$ natürliche Zahlen, die für c in Frage kommen. Damit ist dann aber auch $\mid d \mid$ festgelegt. Es gibt vier Kombinationsmöglichkeiten in den Vorzeichen, aber nur zwei im Fall $c=0$. Insgesamt ergeben sich für c,d nicht mehr als $4\sqrt{N}+2$ Möglichkeiten. Weiter gilt $4\sqrt{N}+2 \leq 5\sqrt{N}$ für alle $N \geq 5$.
Für $N<10$ schätzen wir die Summanden einzeln ab.
Für $N=2$ haben wir folgende Paare: $\pm(1,1), \pm(-1,1)$. Damit ergeben sich folgende Summanden: $\pm\frac{1}{2}\cos^{-k}\left(\frac{\theta}{2}\right), \pm\frac{i}{2}\sin^{-k}\left(\frac{\theta}{2}\right)$ mit $\frac{\pi}{4}<\frac{\theta}{2}<\frac{\pi}{3}$. Somit können wir die vier Summanden weiter abschätzen zu: $1+2^{-\frac{k}{2}}$.
Für $N=5$ schätzen wir die Summanden mit $4\left(\frac{5}{2}\right)^{-\frac{k}{2}}$ ab und erhalten die Abschätzung:
$\mid R_1 \mid \leq 1+2^{\frac{-k}{2}}+4\left(\frac{5}{2}\right)^{-\frac{k}{2}}+\sum_{N=10}^{\infty}5N^{\frac{1}{2}}\left(\frac{1}{2}N\right)^{-\frac{k}{2}} \leq$
$1+2^{\frac{-k}{2}}+4\left(\frac{5}{2}\right)^{-\frac{k}{2}}+\int_{10}^{\infty}5N^{\frac{1}{2}}\left(\frac{1}{2}N\right)^{-\frac{k}{2}}dN \leq 2$
Das Integral ist für $k=12$ explizit bestimmbar und fällt monoton in k. □

Verallgemeinerungen dieses wichtigen Satzes werden in Kapitel 7.4 behandelt.

7.2 Die Transzendenz der Nullstellen der Eisensteinreihen

In seinem Artikel [Ko2] zeigt W. Kohnen:

Satz 7.2. *Die nichttrivialen Nullstellen der Eisensteinreihen sind transzendent.*

Beweis: Dafür sind wir mittlerweile gut vorbereitet. Wir erinnern uns, daß nach Kapitel 7.1 die Nullstellen der Eisensteinreihen in dem Schnitt des Einheitskreises mit dem Fundamentalbereich liegen. Desweiteren wissen wir, daß die Nullstellen der Eisensteinreihen als Nullstellen von Hecke-Eigenformen algebraische j-Werte haben und somit nach Kapitel 2.12 imaginärquadratisch oder transzendent sind.
Angenommen $z_0 \in \mathcal{F}$ sei eine imaginärquadratische Nullstelle einer Eisensteinreihe, d. h. z_0 ist Lösung einer Gleichung $az^2+bz+c=0$ mit $a,b,c \in \mathbb{Z}$ teilerfremd und $a>0$. Weiter sei $D=b^2-4ac<0$. Die $\Gamma(1)$-Translate von z_0 sind von der Form $\frac{b'+\sqrt{D}}{2a'}$.
Es seien $K=\mathbb{Q}\left(\sqrt{D}\right)$ der imaginärquadratische Zahlkörper mit Fundamentaldiskriminante D_0 und $\mathcal{O}_D$ die Ordnung in K mit Führer f, wobei $D=D_0f^2$ gilt. Die Abbildung $z \mapsto \mathbb{Z} \oplus \mathbb{Z}\frac{b+\sqrt{D}}{2a}$ induziert eine Bijektion der $\Gamma(1)$-Äquivalenzklassen imaginärquadratischer Punkte und den Äquivalenzklassen invertierbarer $\mathcal{O}_D$-Ideale. Sei $z_1=\frac{\sqrt{D}}{2}$ bzw. $z_1=\frac{-1+\sqrt{D}}{2}$. Dann entspricht z_1 der trivialen Klasse in der Klassengruppe. Aus dem Satz 2.29 folgt, daß $j(z_0)$ und $j(z_1)$ über K konjugiert sind. Sei σ der K-Morphismus, der $j(z_0)$ auf $j(z_1)$ abbildet. Sei P das Polynom mit rationalen Koeffizienten, dessen Nullstellen die j-Werte der Nullstellen der Eisensteinreihe sind, wie es z.B. in Kapitel 6.1 konstruiert ist. Wir wenden nun σ auf die Gleichung $P(j(z_0))$ an und erhalten $P(j(z_1))$, woraus folgt, daß z_1 auch Nullstelle dieser Eisensteinreihe ist. Mit den Voraussetzungen $\mid z_1 \mid = 1$ und $0 \leq Re(z_1) \leq \frac{1}{2}$ folgt $D=-3$ oder $D=-4$ und weiter $z_0=z_1=\rho$ oder $z_0=z_1=i$. □

7.3 Die exakten Nullstellen der Eisensteinreihen

In diesem Abschnitt wollen wir eine Formel zur expliziten Berechnung der Nullstellen der Eisensteinreihe E_k angeben.
Wir schreiben $k=12N+s$, mit $s \in \{4,6,8,10,0,14\}$. Sei $\mu \in \{1,..,N\}$ ein Zählindex. Sei k_0 die kleinste ganze Zahl, mit: $k_0 \geq \frac{k}{4}$. Bezeichne $e^{2\pi i\theta_\mu}$ die μ-te Nullstelle der Eisensteinreihe.

Satz 7.3. *Es gilt:*

$$Im\left(e^{2\pi i\theta_\mu}\right) = (\mu+\gamma_k)A_\mu - (\mu-1+\gamma_k)A_{\mu-1} - \gamma_k\delta_{\mu,1} - \frac{1}{8\pi}\sum_{m\geq 1}\frac{1}{m}\left(\sum_{\nu=1}^{m}(-1)^\nu\binom{m}{\nu}\left(f_{\nu,k}(A_\mu)-f_{\nu,k}(A_{\mu-1})\right)\right)$$

wobei gilt:

$$
\begin{aligned}
A_\mu &:= \sin\left(2\pi\frac{k_0+\mu}{k}\right)\\
\gamma_k &:= \begin{cases} \frac{1}{2} & : \quad wenn\ s = 6, 10, 14 \\ 0 & : \quad sonst \end{cases}\\
\delta_{\mu,1} &:= \begin{cases} 1 & : \quad wenn\ \mu = 1 \\ 0 & : \quad sonst \end{cases}\\
f_{\nu,k}(y) &:= c_k^{2\nu}\sum_{n\geq 1}\left(\sum_{n_1+..+n_\nu=n,\, n_i\geq 0} e_k(n_1)...e_k(n_\nu)\right)^2 e^{-4\pi n y}\\
c_k &:= 1+\mid\frac{2k}{B_k}\mid\sum_{n\geq 1}\sigma_{k-1}(n)\, e^{-\pi n\sqrt{3}}\\
\sigma_{k-1}(n) &:= \sum_{d|n} d^{k-1}\\
e_k(n) &:= \begin{cases} 1 & : \quad wenn\ n = 1 \\ -\frac{2k}{B_k}\sigma_{k-1}(n) & : \quad wenn\ n > 0 \end{cases}
\end{aligned}
$$

Beweis: siehe [Ko3] □

7.4 Verallgemeinerungen des Satzes von Rankin-Swinnerton-Dyer

Am Ende ihres Artikels "On the Zeros of Eisenstein Series" [RSD] behaupten die Autoren, daß sich ihr Beweis in gleicher Weise auf Eisensteinreihen anderer Modulgruppen anwenden ließe. Diese Behauptung ist jedoch im allgemeinen falsch.
Betrachten wir z. B. in der Kongruenzuntergruppe $\Gamma_0(2)$ die Eisensteinreihe zur Spitze $i\infty$ mit Gewicht 10. Ich habe berechnet, daß diese Eisensteinreihe eine Nullstelle mit j-Wert $\frac{-54000}{961}$ hat. Da der j-Wert negativ ist, kann diese Nullstelle nicht auf dem Einheitskreisbogen zwischen $\frac{1}{2}$ und $\frac{-1}{2}$ liegen. Die Nullstelle ist ungefähr: $0.5 + 0.97971294885869026i$.
Eine Verallgemeinerung des Satzes von Rankin-Swinnerton-Dyer gibt Heekyoung Hahn in ihrem Artikel "On Zeros Of Eisenstein Series For Genus Zero Fuchsian Groups"[Ha].
Wir werden uns im Folgenden wieder auf Kongruenzuntergruppen als Spezialfälle von Fuchsschen Gruppen beschränken. Zum besseren Verständnis wollen wir noch einmal den ursprünglichen Satz über die Nullstellen der Eisensteinreihen zu $\Gamma(1)$ betrachten. Alle Nullstellen im Fundamentalbereich

$\mathcal{F}_{\Gamma(1)}$ bis auf möglicherweise drei (den trivialen) haben j-Werte im Intervall $(0, 1728)$ und sind einfach.
Die Autorin verallgemeinert dies auf gute Gruppen vom Geschlecht null.

Definition 7.4. *Die Kongruenzuntergruppe Γ heißt gut für das Gewicht k, wenn gilt:*

1. *Die Eisensteinreihe $E_k^{i\infty}(\Gamma)$ hat reelle Fourierkoeffizienten, wenn sie existiert.*

2. *Der Raum $M_k(\Gamma)$ hat eine Basis mit Formen mit reellen Fourierkoeffizienten.*

Bemerkung 7.5. *Die Gruppen $\Gamma_0(N)$ sind für alle N und k gut. Die Gruppe $\Gamma_0(N)$ hat genau dann Geschlecht null, wenn gilt:*

$$N \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\}.$$

Siehe dazu [Pa].

Entscheidend für den Satz ist es, daß wir für eine gute Gruppe Γ einen ganz speziellen Fundamentalbereich $\mathcal{F}_\Gamma$ finden können. Sei h die Breite in der Spitze in $i\infty$, dann soll gelten:

$$\mathcal{F}_\Gamma \subset \left\{ z \in \mathbb{H} \mid \frac{-h}{2} \leq Re(z) \leq \frac{h}{2} \right\}$$

Bezeichne $\partial\mathcal{F}_\Gamma$ den Rand des Fundamentalbereiches und $y_0 := \inf\left\{y \mid \pm\frac{h}{2} + iy \in \partial\mathcal{F}_\Gamma\right\}$ dann bezeichnen wir $L := \left\{x + iy \mid x = \pm\frac{h}{2} \text{ und } y \geq y_0\right\}$ als die seitlichen Ränder und ihr Komplement $A := \partial\mathcal{F}_\Gamma \setminus L$ als die unteren Bögen.
Diese unteren Bögen sollen mit einer stückweise differenzierbaren Funktion $z_A := x_A + iy_A : [0,1] \to A$ parametrisiert werden. Sei $f(t) = \frac{y_A'(t)}{\left(j_{\mathcal{F}_\Gamma} \circ z_A\right)'(t)}$, wobei $j_{\mathcal{F}_\Gamma}$ den kanonischen Hauptmodul bezeichnet.
Sei $Crit_{\mathcal{F}_\Gamma} := \{t \in [0,1] \mid f(t) \text{ verschwindet oder ist nicht definiert}\}$. Verschwindet f in t, so hat z_A im Punkt $z_A(t)$ eine Tangente parallel zur reellen Achse, wie etwa im Punkt i bei $\mathcal{F}_{\Gamma(1)}$. Ist f in t nicht definiert, so ist z_A im Punkt $z_A(t)$ nicht differenzierbar, wie etwa im Punkt ρ bei $\mathcal{F}_{\Gamma(2)}$.
Wir sagen, f ändert in t_0 sein Vorzeichen, falls für alle hinreichend kleinen $\varepsilon_1, \varepsilon_2 > 0$ gilt: $f(t_0 - \varepsilon_1) f(t_0 + \varepsilon_2) < 0$.

Definition 7.6. *Wir definieren einen Fundamentalbereich $\mathcal{F}_\Gamma$ als annehmbar, wenn wir seine unteren Bögen mit einer stückweise stetigen Funktion parametrisieren können, so daß gilt:*

1. *Der Hauptmodul $j_{\mathcal{F}_\Gamma}$ nimmt auf $\partial_{\mathcal{F}_\Gamma}$ nur reelle Werte an.*
2. *Die Menge $Crit_{\mathcal{F}_\Gamma}$ ist diskret.*
3. *Wenn $\gamma z_a(t_0) = z_a\left(\hat{t}_0\right)$ für ein $\gamma \in \Gamma$ und für $t_0, \hat{t}_0$ in $Crit_{\mathcal{F}_\Gamma}$, dann wechselt f in t_0 genau dann sein Vorzeichen, wenn es auch in $\hat{t}_0$ sein Vorzeichen wechselt.*

Satz 7.7. *Sei Γ eine gute Gruppe vom Geschlecht null mit einem annehmbaren Fundamentalbereich $\mathcal{F}_\Gamma$. Seien die Fourierkoeffizienten von j_Γ reell und existiere die Eisensteinreihe $E_k^{i\infty}(\Gamma)$. Dann existiert eine endliche Konstante $c(\mathcal{F}_\Gamma)$, die nur vom Fundamentalbereich $\mathcal{F}_\Gamma$ und nicht von $E_k^{i\infty}(\Gamma)$ abhängt, so daß die Nullstellen von $E_k^{i\infty}(\Gamma)$ bis auf möglicherweise $c(\mathcal{F}_\Gamma)$ viele, j_Γ-Werte besitzen, die einfach und reell sind und im Intervall $\left[j_\Gamma\left(\frac{-h}{2} + iy_0\right), \infty\right)$ liegen.*

Beweis: siehe [Ha]. □

Beispiel 7.8. *Mit den Funktionen aus Kapitel 4.5 können wir für $\Gamma_0(2)$ analog zum Fall $\Gamma(1)$ die j-Werte der Nullstellen der Hecke-Eigenformen bestimmen.*

k	$j_{\Gamma(1)}$-*Wert der Nullstelle*
8	$\frac{27000}{289}$
10	$\frac{-54000}{961}$
12	$\frac{-173515500-28633500\sqrt{249}}{477481}$
14	$\frac{-108196128000-6654150000\sqrt{267}}{29822521}$
	$\frac{-108196128000+6654150000\sqrt{267}}{29822521}$

Jayce Getz verallgemeinert den Satz von Rankin-Swinnerton-Dyer, indem er das Ergebnis auf die Gap-Funktion ausdehnt.

Definition 7.9. *Für Gewicht $k \geq 4$ definieren wir die Gap-Funktion $F_k(z) \in M_k(\Gamma(1))$ als die eindeutige Modulform mit Fourierentwicklung*

$$F_k(z) = 1 + \sum_{n \geq dim\ M_k(\Gamma(1))} c(n)\, q^n$$

Satz 7.10. *Die nichttrivialen Nullstellen der Gap-Funktion haben ganze algebraische j-Wert im Intervall $[0, 1728]$.*

Beweis: siehe [Ge] □

Eine weitere Verallgemeinerung des Satzes von Rankin-Swinnerton-Dyer auf einzelne Fricke-Gruppen wird in den aktuellen Arbeiten von Junichi Shigezumi gezeigt. Siehe dazu [Sh2], [TM] und [Sh1].

8 Die Nullstellen der Hecke-Spitzenformen zu $\Gamma(1)$

Der Fall der Nullstellen der Hecke-Spitzenformen ist ungleich schwerer als der der Eisensteinreihen. So haben wir zum Beispiel nicht den Satz von Rankin-Swinnerton-Dyer. Der Satz von Rudnick zeigt uns, daß auch ein ähnliches Ergebnis nicht möglich sein wird. Mithilfe des von Achter vorgestellten Algorithmus werden wir für einige Nullstellen zeigen, daß die zugehörigen elliptischen Kurven keine CM besitzen, die Nullstellen also transzendent sind.

8.1 Die Verteilung der Nullstellen der Hecke-Eigenformen, die Spitzenformen sind

Im letzten Abschnitt haben wir gesehen, daß die Nullstellen der Eisensteinreihen, also jenen Hecke-Eigenformen, die keine Spitzenformen sind, auf dem Einheitskreis liegen. Gern hätten wir ein ähnliches Ergebnis auch für die Spitzenformen. Dies wird wegen der im folgenden vorgestellten Ergebnissen nicht möglich sein.
Zeév Rudnick zeigt in seinem Artikel [Ru] folgenden Satz:

Satz 8.1. *Sei $\{f_k\}$ eine Folge von Hecke-Eigenformen mit $f_k \in S_k$ zur Kongruenzuntergruppe $\Gamma(1)$. Unter Annahme der Verallgemeinerten Riemannschen Vermutung gilt:*
Die Nullstellen von f_k sind für $k \to \infty$ in $\mathcal{F}$ bezüglich des normalisierten, hyperbolischen Maßes $dV(z) = \frac{3}{\pi}\frac{dxdy}{y^2}$ gleichverteilt.

Beweis: siehe [Ru]. □

Bemerkung 8.2. *Vergleichen wir dieses Ergebnis mit dem aus Satz 4.22 über die Gleichverteilung der Heegner Punkte, so könnte man vermuten, daß es einen Zusammenhang zwischen Heegner Punkten und den nichttrivialen Nullstellen der Hecke-Spitzenformen gibt. Wir werden jedoch von einigen dieser Nullstellen zeigen, daß sie transzendent sind. Da Heegner Punkte algebraisch sind, können diese beiden Mengen nicht gleich sein und die Vermutung eines Zusammenhanges wird nicht bestärkt.*

8.2 Die Algebraizität der Nullstellen

Korollar 8.3. *Die Nullstellen der Hecke-Eigenformen sind entweder imaginärquadratisch oder transzendent.*

Beweis: klar, nach Satz 2.12 und Satz 6.1. □

Wir haben im Satz 7.2 gesehen, daß die Nullstellen der Eisensteinreihen transzendent sind. Gilt dies auch für die Nullstellen der Hecke-Spitzenformen? Wir wollen versuchen, diese Frage in einigen Fällen zu entscheiden, indem wir die der Nullstelle zugehörige elliptische Kurve auf CM testen.
Achters Test im Kapitel 3.1 benutzt, daß es bei elliptischen Kurven E über einem Zahlkörper K mit CM eine quadratische Körpererweiterung $K \subset \widetilde{K}$ gibt, so daß $E/\widetilde{K}$ überall gute Reduktion hat. Sei j_0 der j-Wert der zu untersuchenden Nullstelle. Wir betrachten die elliptische Kurve:

$$E_{j_0}:\ y^2 = x^3 - \frac{27}{4}\frac{j_0}{j_0 - 1728}x - \frac{27}{4}\frac{j_0}{j_0 - 1728}.$$

Die Koeffizienten stammen aus dem Körper $K := \mathbb{Q}(j_0)$. Nach einer geeigneten zulässigen Variablentransformation können wir annehmen, daß die Koeffizienten Elemente aus dem Ring der ganzen Zahlen $\mathcal{O}_K$ sind. Deswegen ist auch die Diskriminante $\Delta(j_0)$ ein Element aus $\mathcal{O}_K$. Der Ring der ganzen Zahlen $\mathcal{O}_K$ ist als solcher ein Dedekindring. Insbesondere existiert eine eindeutige Zerlegung des Ideals $(\Delta(j_0)) = \prod p_i^{e_i}$ in Primelemente. Da bei der allgemeinen zulässigen Variablentransformation $x = u^2x' + r,\ y = u^3y' + su^2x' + t$ mit $u, r, s, t \in K,\ u \neq 0$ sich die Diskriminante wie folgt verändert: $\Delta' = \frac{\Delta}{u^{12}}$, können wir eine elliptische Kurve über K finden, deren Diskriminante sich von $(\Delta(j_0))$ nur um einen Faktor der Form $(q_1^{a_1}....q_n^{a_n})^{12}$ unterscheidet. Deswegen besitzt unsere Kurve genau für die p_i schlechte Reduktion, für die gilt: $e_i \not\equiv 0\ mod\ 12$. Weiter bemerken wir, daß die Primteiler (insbesondere jene mit schlechter Reduktion) stets mit ihrem Konjugierten zusammen auftreten, da wir ein Hauptideal zerlegen.
Folgen wir dem Beispiel Achters und setzen $(N) := \prod_{i|e_i \not\equiv 0\ mod\ 12} p_i$ und $\widetilde{K} := K\left(\sqrt{N}\right)$, so bemerken wir $N \in K$ und $\left[\widetilde{K} : K\right] = 2$. Nun kann es schwierig sein die Primzerlegung der Diskriminante zu bestimmen; stattdessen wollen wir ihre Norm betrachten. Dann gilt:

Satz 8.4. *Sei $\prod_{i=1}^{r} p_i^{e_i} = N_{K/\mathbb{Q}}(\Delta(E)) \in \mathbb{Z}$ die Primfaktorzerlegung von $N_{K/\mathbb{Q}}(\Delta(E))$. Existiert ein $\overline{i} \in \{1, ..., r\}$ mit $e_{\overline{i}}\ mod\ 6 \neq 0$, so hat E keine CM über K.*

Beweis: Es gilt:

$$\begin{aligned} N_{\widetilde{K}/\mathbb{Q}}(\Delta(E)) &= \prod N_{\widetilde{K}/\mathbb{Q}}(p_i)^{e_i} = \prod N_{K/\mathbb{Q}}\left(N_{\widetilde{K}/K}(p_i)\right)^{e_i} = \prod N_{K/\mathbb{Q}}(p_i)^{e_i} \\ &= N_{K/\mathbb{Q}}(\Delta(E))^2 \end{aligned}$$

Sollte einer der Primfaktoren von $N_{K/\mathbb{Q}}(\Delta(E))^2$ in einer Häufigkeit auftreten, die nicht durch 12 teilbar ist, so wissen wir, daß es zu diesem j-Wert keine Kurve $E/\widetilde{K}$ gibt, die überall gute Reduktion hat, da eine zulässige Variablentransformation die Exponenten der Primfaktoren der Diskriminante stets um Vielfache von 12 verändert. Somit hätte diese Nullstelle keine CM über K.

□

Hier nun einige Rechenergebnisse:

j-Wert	$N_{K/\mathbb{Q}}(\Delta(E_j))$	CM über K?
$156+12\sqrt{144169}$	$2^{115}3^{62}5^67^{18}$	nein
$156-12\sqrt{144169}$	$2^{115}3^{62}5^67^{18}$	nein
$5076+108\sqrt{18209}$	$2^{115}3^{18}5^67^{18}11^9$	nein
$5076-108\sqrt{18209}$	$2^{115}3^{18}5^67^{18}11^9$	nein
$4128+96\sqrt{51349}$	$2^{72}3^{44}5^611^21409^9$	nein
$4128-96\sqrt{51349}$	$2^{72}3^{44}5^611^21409^9$	nein
$-18804+12\sqrt{18295489}$	$2^{117}3^{62}5^87^{18}11^{20}$	nein
$-18804-12\sqrt{18295489}$	$2^{117}3^{62}5^87^{18}11^{20}$	nein
$61272+72\sqrt{2356201}$	$2^{106}3^{49}5^67^{18}17^279^9$	nein
$61272-72\sqrt{2356201}$	$2^{106}3^{49}5^67^{18}17^279^9$	nein
$135420+4\sqrt{9737304801}$	$2^{58}3^{35}5^913^9193^9883^9$ $1171^92567371^25051^2$	nein
$135420-4\sqrt{9737304801}$	$2^{58}3^{35}5^913^9193^9883^9$ $1171^92567371^25051^2$	nein

Tabelle 2: CM über K?

Um aber zu entscheiden, ob die Nullstellen transzendent sind, genügt es nicht, CM auszuschließen, sondern vielmehr müssen wir auch potentielle CM ausschließen.

Satz 8.5. *Die nichttrivialen Nullstellen der Hecke-Eigenformen zum Gewicht* 24, 28, 30, 32, 34 *und* 38 *sind transzendent.*

Beweis: Nach Satz 7.2 sind die Nullstellen der Eisensteinreihen transzendent. Es genügt also die Nullstellen der Spitzenformen zu untersuchen. In Kapitel 8.2 haben wir bereits die j-Invarianten der Nullstellen berechnet. Wir bestimmen zu jeder eine elliptische Kurve, die wir mit verschiedenen Primidealen reduzieren und schließen mit Korollar 3.8, daß die Nullstelle keine potenzielle CM hat, also nach Korollar 8.3 transzendent ist. Die Ergebnisse stehen in Tabelle 3.

Zum besseren Verständnis der Tabellen wollen wir hier das Beispiel der

j-Wert	p_1	p_2
$156+12\sqrt{144169}$	$\left(5, \frac{1+\sqrt{144169}}{2}-2\right)$	$\left(6007, \frac{1+\sqrt{144169}}{2}\right)$
	$\mathbb{Q}\left(\sqrt{-11}\right)$	$\mathbb{Q}\left(\sqrt{-3\cdot 7393}\right)$
$5076+108\sqrt{18209}$	$\left(5, \frac{1+\sqrt{18209}}{2}+1\right)$	$\left(569, \frac{1+\sqrt{18209}}{2}\right)$
	$\mathbb{Q}\left(\sqrt{-11}\right)$	$\mathbb{Q}\left(\sqrt{-10}\right)$
$4128-96\sqrt{51349}$	$\left(5, \frac{1+\sqrt{51349}}{2}-2\right)$	$\left(11, \frac{1+\sqrt{51349}}{2}\right)$
	$\mathbb{Q}\left(i\right)$	$\mathbb{Q}\left(\sqrt{-43}\right)$
$-18804+12\sqrt{18295489}$	$\left(23, \frac{1+\sqrt{18295489}}{2}\right)$	$\left(5, \frac{1+\sqrt{18295489}}{2}-2\right)$
	$\mathbb{Q}\left(\sqrt{-19}\right)$	$\mathbb{Q}\left(i\right)$
$61272+72\sqrt{2356201}$	$\left(29, \frac{1+\sqrt{2356201}}{2}-2\right)$	$\left(11, \frac{1+\sqrt{2356201}}{2}\right)$
	$\mathbb{Q}\left(\sqrt{-35}\right)$	$\mathbb{Q}\left(\sqrt{-10}\right)$
$135420-4\sqrt{9737304801}$	$\left(405721033, \frac{1+\sqrt{9737304801}}{2}-2\right)$	$\left(5, \frac{1+\sqrt{9737304801}}{2}\right)$
	$\mathbb{Q}\left(\sqrt{-36603606}\right)$	$\mathbb{Q}\left(i\right)$

Tabelle 3: Ergebnisse bei Achters Test auf potentielle CM

Nullstelle mit j-Wert $156+12\sqrt{144169}$ exemplarisch vorrechnen. Sei dazu

$$\begin{aligned} E_{144169}: \quad y^2 =& x^3 - \frac{27}{4}\frac{j}{j-1728}x - \frac{27}{4}\frac{j}{j-1728} \\ y^2 =& x^3 + \left(\frac{-4212}{(-6288+48\sqrt{144169})} - \frac{324\sqrt{144169}}{(-6288+48\sqrt{144169})}\right)x \\ & - \frac{4212}{(-6288+48\sqrt{144169})} - \frac{324\sqrt{144169}}{(-6288+48\sqrt{144169})} \end{aligned}$$

mit einer zulässigen Variablentransformation mit $u=\frac{4}{48}(j-1728)$ erhalten wir dann:

$$y^2 = x^3 + \left(-185227887942 + 380450466\sqrt{144169}\right) x \\ - 44253295928664408 + 109907780320584\sqrt{144169}$$

Die Kurve E_{144169} hat den j-Wert $156 + 12 * \sqrt{144169}$. Seien $p_1 = (5, \frac{1+\sqrt{144169}}{2} - 2)$ und $p_2 = (6007, \frac{1+\sqrt{144169}}{2})$.
Dann ist E_{144169} reduziert bei p_1: $y^2 = x^3 + x + 4$. Mithilfe von SAGE [St2] bestimmen wir, daß diese Kurve im Körper $\mathbb{F}_5$ genau 9 rationale Punkte hat. Aus dem Satz 2.35 folgt: $Frob_{p1} = \frac{-3}{2} + \frac{1}{2}\sqrt{-11}$. Die Kurve E_{144169} reduziert bei p_2: $y^2 = x^3 + 2317x + 4368$ hat 6051 rationale Punkte in $\mathbb{F}_{6007}$ und es folgt: $Frob_{p2} = \frac{-43}{2} + \frac{1}{2}\sqrt{-22179}$
Beide Reduktionen sind gut, da die Primideale nicht das Diskriminantenideal teilen und gewöhnlich, da die Spur des Frobenius jeweils nicht null ist. Damit ergeben sich dir Kandidatenkörper $F_1 = \mathbb{Q}(\sqrt{-11})$ und $F_2 = \mathbb{Q}(\sqrt{-3 \cdot 7393})$ mit entsprechenden Ringen der ganzen Zahlen. Der Schnitt dieser beiden Ringe ist trivial. Daher hat $E_{156+12\sqrt{144169}}$ keine CM und unsere Nullstelle ist transzendent.

□

Für die Eisensteinreihen konnten wir die exakten Nullstellen mit Hilfe einer Formel angeben, die auch den Satz von Rankin-Swinnerton-Dyer benutzt. Dieses Ergebnis läßt sich deshalb so nicht verallgemeinern.

9 Nullstellen als Verzweigungspunkte

Eine elliptische Kurve $E/\mathbb{Q}$ wird nach dem Satz von Wiles von einer Modulkurve $X_0(N)$ endlich überlagert. Aus der Eichler-Shimura Theorie folgt, daß der Homomorphismus von $X_0(N)$ nach $E/\mathbb{Q}$ sich über eine Hecke-Spitzenform $f \in S_2^{new}(\Gamma_0(N))$ definieren läßt. Die nichttrivialen Nullstellen von f sind dann die Verzweigungspunkte des Morphismus und deswegen von großem Interesse.
Das kleinste Level N für das $S_2^{new}(\Gamma_0(N)) \neq \{0\}$ ist 11.

9.1 Eichler-Shimura Theorie

Sei $f \in S_2^{new}(\Gamma_0(N))$ eine Hecke-Spitzenform mit rationalen Koeffizienten. Wir fixieren $\tau_0 \in \mathbb{H}$ und definieren $F(\tau) := \int_{\tau_0}^{\tau} f(\zeta)\, d\zeta$. Da f analytisch ist, ist F unabhängig vom Integrationsweg. Für $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \gamma \in \Gamma_0(N)$ bemerken wir:

$$\begin{aligned} F(\gamma(\tau)) &= \int_{\tau_0}^{\gamma(\tau)} f(\zeta)\, d\zeta = \int_{\gamma(\tau_0)}^{\gamma(\tau)} f(\zeta)\, d\zeta + \int_{\tau_0}^{\gamma(\tau_0)} f(\zeta)\, d\zeta \\ &= \int_{\tau_0}^{\tau} f(\gamma(\zeta))\, \gamma'(\zeta)\, d\zeta + \int_{\tau_0}^{\gamma(\tau_0)} f(\zeta)\, d\zeta \\ &= \int_{\tau_0}^{\tau} (c\tau + d)^2 f(\zeta) \frac{1}{(c\tau + d)^2} d\zeta + \int_{\tau_0}^{\gamma(\tau_0)} f(\zeta)\, d\zeta \\ &= F(\tau) + \int_{\tau_0}^{\gamma(\tau_0)} f(\zeta)\, d\zeta =: F(\tau) + \phi_{f,\tau_0}(\gamma) \end{aligned}$$

Lemma 9.1. *$\phi_{f,\tau_0}(\gamma) = \int_{\tau_0}^{\gamma(\tau_0)} f(\zeta)\, d\zeta$ hängt nicht von τ_0 ab.*

Beweis: Sei $F_1(\tau) = F(\tau) + \int_{\tau_1}^{\tau_0} f(\zeta)\, d\zeta$ für $\tau_1 \in \mathbb{H}$. Dann gilt:

$$\begin{aligned} \phi_{f,\tau_0} = \phi_{f,\tau_1} &\Leftrightarrow F(\gamma(\tau)) - F(\tau) = F_1(\gamma(\tau)) - F_1(\tau) \\ &\Leftrightarrow F(\gamma(\tau)) = F_1(\gamma(\tau)) - \int_{\tau_1}^{\tau_0} f(\zeta)\, d\zeta \\ &\Leftrightarrow \int_{\tau_0}^{\gamma(\tau)} f(\zeta)\, d\zeta = \int_{\tau_1}^{\gamma(\tau)} f(\zeta)\, d\zeta + \int_{\tau_0}^{\tau_1} f(\zeta)\, d\zeta \end{aligned}$$

□

Deswegen werden wir im Folgendem $\phi_f(\gamma)$ für $\phi_{f,\tau_0}(\gamma)$ schreiben.

Lemma 9.2. *ϕ_f ist ein Gruppenhomomorphismus zwischen $\Gamma_0(N)$ und einer additiven Untergruppe von $\mathbb{C}$.*

Beweis:

$$\begin{aligned}\phi_f(\gamma_1\gamma_2) &= \int_{\tau_0}^{\gamma_1\gamma_2(\tau_0)} = \int_{\tau_0}^{\gamma_1(\tau_0)} + \int_{\gamma_1(\tau_0)}^{\gamma_1\gamma_2(\tau_0)} = \phi_f(\gamma_1) + \int_{\tau_0}^{\gamma_2(\tau_0)} \\ &= \phi_f(\gamma_1) + \phi_f(\gamma_2)\end{aligned}$$

□

Bemerkung 9.3. *Die elliptischen Elemente von $\Gamma_0(N)$ liegen im Kern von ϕ_f, da sie endliche Ordnung haben. Mit etwas mehr Aufwand kann man auch zeigen, daß die parabolischen Elemente von $\Gamma_0(N)$ im Kern von ϕ_f liegen. Dies findet man z. B. in [Kn].*

Bemerkung 9.4. *Wenn $\phi_f(\Gamma_0(N))$ ein Gitter ist, so wollen wir es mit Λ_f bezeichnen. Dies ist genau dann der Fall, wenn die Menge der Bilder der Erzeuger von $\Gamma_0(N)$ zwei $\mathbb{R}$-linear unabhängige Elemente enthält. Das Gitter Λ_f ist wohldefiniert, da $F(\gamma(\tau)) - F(\tau) \in \Lambda_f$.*

Satz 9.5. *Für eine Hecke-Neuform $f \in S_2^{new}(\Gamma_0(N))$ vom Gewicht 2 zu $\Gamma_0(N)$ ist Λ_f ein Gitter und es existiert der Homomorphismus*

$$F:\ \Gamma_0(N) \setminus \mathbb{H} \bigcup \mathbb{P}^1(\mathbb{Q}) \cong X_0(N) \to \mathbb{C}/\Lambda_f \cong E_f \tag{1}$$

Beweis: Siehe [Kn] Theorem 11.74. □

Über die Existenz des Morphismus F hinaus besagt die Eichler-Shimura Theorie, daß E_f über $\mathbb{Q}$ definiert werden kann und daß die Faktoren des Eulerproduktes der L-Reihen $L(s, E)$ und $L(s, f)$ bis auf endlich viele Primzahlen übereinstimmen, wobei f normalisiert wird.

9.2 Verzweigungspunkte

Seien f eine Hecke-Neuform vom Gewicht 2 zu $\Gamma_0(N)$ und $F:\ X_0(N) \to E_f(\mathbb{C})$ gegeben wie in Gleichung 1.
Wir können das Geschlecht g von $X_0(N)$ mit der Formel aus 4.35 berechnen und wissen, daß eine elliptische Kurve immer Geschlecht 1 hat. Aus der Riemann-Hurwitz Formel folgt, daß es genau $2g-2$ kritische Punkte gibt, gezählt mit der entsprechenden Vielfachheit.

Satz 9.6. *Die kritischen Punkte der Überlagerung $F:\ X_0(N) \to E_f(\mathbb{C})$ sind die Nullstellen der Differentialform $dF = 2\pi i f(z)\,dz$, also die Nullstellen von f, die nicht von den Polstellen von dz aufgehoben werden.*

□

Die Polstellen von dz, aufgefaßt als Differentialform in $X_0(N)$ sind bekannnt. Siehe dazu zum Beispiel [De1] S.52.

$$Div(dz) = -\left(\sum_{j=1}^{\nu_\infty} S_j + \frac{1}{2}\sum_{j=1}^{\nu_2} E_{2,j} + \frac{2}{3}\sum_{j=1}^{\nu_3} E_{3,j}\right),$$

wobei S_j die Spitzen, $E_{2,j}$ die elliptischen Punkte der Ordnung 2 und $E_{3,j}$ die elliptischen Punkte der Ordnung 3 bezeichnet.

9.3 Taniyama-Weil, Wiles

Definition 9.7. *Eine elliptische Kurve $E/\mathbb{Q}$ heißt modular oder Weilkurve, wenn es ein $N \in \mathbb{N}$ gibt, so daß die Modulkurve $X_0(N)$ eine endliche Überlagerung von $E/\mathbb{Q}$ ist.*

Satz 9.8 (Modular Elliptic Curves Conjecture)**.** *Jede elliptische Kurve $E/\mathbb{Q}$ ist modular.*

Beweis: Dies ist der Satz von Wiles. In dieser Allgemeinheit wurde er von Wiles, Breuil, Conrad, Diamond und Taylor bewiesen.
Siehe [Hu] S.333. □

Bemerkung 9.9. *Der Satz 1.29 über die Funktionalgleichung von $L(E,s)$ folgt aus dem Satz 9.8, da es für jede elliptische Kurve $E/\mathbb{Q}$ eine endliche Überlagerung durch eine Modulkurve gibt, also insbesondere ein $N \in \mathbb{N}$ und ein $f \in S_2^{new}(\Gamma_0(N))$, so daß die L-Reihen $L(E,s)$ und $L(f,s)$ bis auf endlich viele Primzahlen übereinstimmen und $L(f,s)$ eine Funktionalgleichung erfüllt.*

Definition 9.10. *Der analytische Rang einer elliptischen Kurve $E/\mathbb{Q}$ ist die Nullstellenordnung der L-Reihe $L(E,s)$ an der Stelle $s = 1$.*

Definition 9.11. *Für $N > 1$ heißt das Bild von $I = \{iy \mid \infty \geq y \geq 0\}$ in $X_0(N)$ der Fundamentalbogen von $X_0(N)$. Ein fundamentaler kritischer Punkt ist ein kritischer Punkt bezüglich der modularen Überlagerung, der im Fundamentalbogen liegt.*

Satz 9.12 (Mazur-Swinnerton-Dyer)**.** *Der analytische Rang eine elliptischen Kurve $E/\mathbb{Q}$ ist kleiner oder gleich der Anzahl der fundamentalen kritischen Punkte ungerader Ordnung.*

Beweis: Siehe [MSD] Theorem auf Seite 10. □

Bemerkung 9.13. *Sei $E/\mathbb{Q}$ eine elliptische Kurve. Aus der Birch-Swinnerton-Dyer Vermutung folgt unter anderem, daß der Rang von $E(\mathbb{Q})$ und der analytische Rang von E gleich sind. Mit Kenntnissen über die Nullstellen von Hecke-Eigenformen können wir so eine obere Schranke für den Rang von $E(\mathbb{Q})$ angeben.*

Bemerkung 9.14. *Die Bilder der Nullstellen von $f \in S_2^{new}(\Gamma_0(N))$ in der zugehörigen elliptischen Kurve sind sicher wichtige Punkte. Sie auf geometrische Eigenschaften zu untersuchen, könnte ein interessanter Ansatzpunkt für zukünftige Arbeiten sein.*

10 Anhang

Hier wird der Maple10-Programmcode zur Berechnung der Hecke-Eigenformen zu $\Gamma(1)$ angegeben.

10.1 Programmcode

```
INITIALISIERUNG

with(numtheory):
with(algcurves):
readlib(mtaylor):
interface(warnlevel=1):
reihenlaenge:=50:
Digits:=150:
interface(displayprecision=10):
q:=proc(t)
exp(2*Pi*I*t):
end proc:
anzeig:=proc(H,t)
a:=coeff(H,q,0):
for i to t do
    a:=a+coeff(H,q,i)*q^i:
end do:
sort(a);
end proc:

easy:=proc(n)
a:=numer(n)*simplify(evala(Norm(denom(n))))/denom(n)/simplify(evala(Norm(denom(n)))):
a:=simplify(a);
end proc:

normalmachen:=proc(n)
nenner:=expand(denom(n)):
zaehler:=expand(numer(n)):
if (not(Im(nenner)=0))
then a:=Re(nenner)-Im(nenner):
     nenner:=expand(nenner*a):
     zaehler:=expand(zaehler*a):
end if:
a:=simplify(zaehler/nenner);
end proc:

K:=4:
E[K] := sort(1 + 2/Zeta(1-K) *sum(sigma[K-1](n)*q^n,n=1..reihenlaenge)):
K:=6:
E[K] := sort(1 + 2/Zeta(1-K) *sum(sigma[K-1](n)*q^n,n=1..reihenlaenge)):
DR:=sort(mtaylor( ( (E[4])^3 -(E[6])^2)/1728, q, reihenlaenge)):

fkoeff:=proc(n)
a:=binomial(-1/2,n)^2;
end proc:
movetostr:=proc(t)
a:=t:
a:=a-trunc(Re(a)):
while (abs(Re(a))>0.5) do
if (Re(a)<0) then a:=a+1:
             else a:=a-1:
end if:
```

```
end do:
a;
end proc:

movetof:=proc(t)
aa:=t:
aa:=movetostr(aa):
while(abs(aa)<1) do
                 b:=-1/aa:
                aa:=movetostr(b):
                end do:
aa;
end proc:

ffunktion:=fkoeff(0):
for i to reihenlaenge do ffunktion:=ffunktion+fkoeff(i)*q^i:
end do:

"Hecke-Operator":
hecke:=proc(B,H,N,k,d)
A:=0:
for i to H do
if ((H mod i)= 0) then
    if (igcd(i,N)=1) then A:=A+(i^(k-1)*coeff(B,q,0)):
    end if:
end if:
end do:
for j to d do
    for i to H do
        if ((igcd(j,H) mod i)=0) then
            if (igcd(i,N)=1) then A:=A+(i^(k-1)*coeff(B,q,(j*H/(i*i)))*q^j):
            end if:
         end if:
    end do:
end do:
A;
end proc:
interface(warnlevel=4):
PROGRAMMSTART

N:=1:
k:=24:
Gewicht:=k;
d:=k/12-(k mod 12)/12+1:
if (k mod 12 = 2) then d:=d-1; end if:
Dimension:=d;
NS:=k/12; "ANZAHL DER NULLSTELLEN":
"ERZEUGUNG DER BASIS":

for i to d do B[i]:=expand(DR^(i-1)*(E[4])^(3*(d-i))):
end do:

if ((k mod 12)=2) then
    for i to d do B[i]:=expand(B[i]*E[6]^2):
    end do:
end if:

if ((k mod 12)=4) then
    for i to d do B[i]:=expand(B[i]*E[4]):
    end do:
end if:
```

```
if ((k mod 12)=6) then
    for i to d do B[i]:=expand(B[i]*E[6]):
    end do:
end if:


if ((k mod 12)=8) then
    for i to d do B[i]:=expand(B[i]*E[4]*E[4]):
    end do:
end if:


if ((k mod 12)=10) then
    for i to d do B[i]:=expand(B[i]*E[6]*E[4]):
    end do:
end if:

for i to d do
for j to nops(B[i])-reihenlaenge+5 do
    B[i]:=B[i]-coeff(B[i],q,j+reihenlaenge)*q^(j+reihenlaenge):
end do:
end do:

"Normierung der Basis":
for i to d do B[i]:=sort(B[i]/coeff(B[i],q,i-1)):
end do:
print("Basis B[i] normiert.");
 "Hier wird der HECKE-OPERATOR gewaehlt:":
H:=nextprime(N);
H:=2:
for i to d do
    C[i]:=hecke(B[i],H,N,k,d);
end do:
for i to d do
for j to d do
m[i,j]:=coeff(C[i],q,j-1):
end do:
end do:

for j to d do
for h to d-1 do
i:=h+1:
for l to h do
m[j,i]:=m[j,i]-(m[j,l]*coeff(B[l],q,i-1))
end do:
end do:
end do:

f:= (i,j) -> m[j,i]:
M:=Matrix(d,f);
 (EW,EV):=LinearAlgebra[Eigenvectors](M):
for i to d do
for j to d do
EV[i,j]:=Re(EV[i,j]):
EW[i]:=Re(EW[i]):
end do:
end do:
(EW,EV);

"Die HECKE-EIGENFORMEN sind:";
for i to d do
    HE[i]:=0:
```

```
end do:
for i to d do
    for j to d do
        HE[i]:=HE[i]+Re(EV[j,i])*B[j]:
end do:
if (not(coeff(HE[i],q,1)=0)) then HE[i]:=HE[i]/coeff(HE[i],q,1): end if:
end do:


for j to d do
print(anzeig(HE[j],8));
print(_____________________________________________________________);
end do:
"Nullstellensuche";
for i to d do
poly[i]:=0:
for j to d do
poly[i]:=poly[i]+(EV[j,i] *J^(d-j));
end do:
print(poly[i]);
print(_____________________________________);
end do:
"Loesung fuer die Polynome in J":
for i to d do
  if (type (poly[i],constant))
    then SOLJ[i]:="speziell";
    else SOLJ[i]:=[(allvalues(RootOf(poly[i],J)))]:
  end if:
  print(SOLJ[i]);
  print(_____________________________________);
end do:
```

10.2 Auszug aus [Ac2]

*If E is an elliptic curve over a field K of characteristic 0, then End(E)_0, the field of fractions of End(E), is either Q or a quadratic imaginary field.
* If E is an _ordinary_ elliptic curve over a field K of arbitrary characteristic, the same classification holds.
* An elliptic curve E/K acquires all its endomorphisms over a finite extension L of K.
* As a general principle, symmetry groups and endomorphism rings tend to be upper semicontinuous. In particular, this means that if p is a prime of K, then there's an inclusion End(E) -> End(E_p).

With this in mind, let's look at your question.

Let L be some finite extension of K such that End(E_L) = End(E_{\bar K}).

Let q_1 and q_2 be primes of L over p_1 and p_2. Then End(E_{p_i})_0 = End(E_{q_i})_0 = F_i. (The endomorphism ring can't get any bigger as we pass from K/p_i to L/q_i, as it is already maximal. This is typical for ordinary elliptic curves over finite fields, but need not happen in general.)

Then End(E_L) is naturally a subring of F_1 and of F_2, thus is just the integers.

Literatur

[Ac1] *J. D. Achter:* Detecting complex multiplication. Computational aspects of algebraic curves. Lecture Notes Ser. Comput. **13**. World Sci. Publ., Hackensack, NJ, 2005, 38–50.

[Ac2] *J. D. Achter:* E-mail an den Autor, 2006.

[Ap] *T. M. Apostol:* Modular functions and dirichlet series in number theory. 2 ed.. Graduate Texts in Mathematics **41**. Springer-Verlag.

[BL] *C. Birkenhake*, *H. Lange:* Complex abelian varieties. Second ed.. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences] **302**. Springer-Verlag, Berlin, 2004.

[Bo] *R. E. Borcherds:* Monstrous moonshine and monstrous Lie superalgebras. Invent. Math. **109** (1992), 405–444.

[Co] *D. A. Cox:* Primes of the form x^2+ny^2. John Wiley & Sons Inc., New York, 1989, Fermat, class field theory and complex multiplication.

[De1] *C. Delaunay:* Formes modularies et invariants de courbes elliptiques définies sur $\mathbb{Q}$, 2002, Thèse Université Bordeaux I.

[De2] *C. Delaunay:* Critical and ramification points of the modular parametrization of an elliptic curve. J. Théor. Nombres Bordeaux **17** (2005), 109–124.

[Du] *W. Duke:* Hyperbolic distribution problems and half-integral weight Maass forms. Invent. Math. **92** (1988), 73–90.

[Ge] *J. Getz:* A generalization of a theorem of Rankin and Swinnerton-Dyer on zeros of modular forms. Proc. Amer. Math. Soc. **132** (2004), 2221–2231 (electronic).

[Ha] *H. Hahn:* On zeros of Eisenstein series for genus zero Fuchsian groups. arXiv.org **arXiv:math.NT/0603625** (2006).

[HBJ] *F. Hirzebruch*, *T. Berger*, *R. Jung:* Manifolds and modular forms. Friedr. Vieweg & Sohn, Braunschweig, 1992, With appendices by Nils-Peter Skoruppa and by Paul Baum.

[Hu] *D. Husemöller:* Elliptic curves. Second ed.. Graduate Texts in Mathematics **111**. Springer-Verlag, New York, 2004, With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen.

[Kn] *A. W. Knapp:* Elliptic curves. Mathematical Notes **40**. Princeton University Press, 1992.

[Ko1] *N. Koblitz:* Introduction to elliptic curves and modular forms. Graduate Texts in Mathematics **97**. Springer-Verlag, New York, 1984.

[Ko2] *W. Kohnen:* Transcendence of zeros of Eisenstein series and other modular functions. Comment. Math. Univ. St. Pauli **52** (2003), 55–57.

[Ko3] *W. Kohnen:* Zeros of Eisenstein series. Kyushu J. Math. **58** (2004), 251–256.

[MSD] *B. Mazur*, *P. Swinnerton-Dyer:* Arithmetic of Weil curves. Invent. Math. **25** (1974), 1–61.

[Pa] *S. Pauli:* Kongruenzuntergruppentabelle nach Geschlecht. http://www.math.tu-berlin.de/ pauli/congruence/congruence.html.

[RSD] *F. K. C. Rankin*, *H. P. F. Swinnerton-Dyer:* On the zeros of eisenstein series. Bull. London Math. Soc. **2** (1970), 169, 170.

[Ru] *Z. Rudnick:* On the asymptotic distribution of zeros of modular forms. Int. Math. Res. Not. **34** (2005), 2059–2074.

[Sc] *B. Schoeneberg:* Elliptic modular functions: an introduction. Springer-Verlag, New York, 1974, Translated from the German by J. R. Smart and E. A. Schwandt, Die Grundlehren der mathematischen Wissenschaften, Band 203.

[Sh1] *J. Shigezumi:* A detailed note on the zeros of Eisenstein series for $\Gamma_0^*(5)$ and $\Gamma_0^*(7)$. arXiv.org **arXiv:math.NT/0607247** (2006).

[Sh2] *J. Shigezumi:* On the zeros of Eisenstein series for $\Gamma_0^*(5)$ and $\Gamma_0^*(7)$. arXiv.org **arXiv:math.NT/0607409** (2006).

[Sh3] *G. Shimura:* Introduction to the arithmetic theory of automorphic functions. Publications of the Mathematical Society of Japan **11**. Princeton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kanô Memorial Lectures, 1.

[Si1] *J. H. Silverman:* The arithmetic of elliptic curves. Graduate texts in Mathematics **106**. Springer, 1986.

[Si2] *J. H. Silverman:* Advanced topics in the arithmetics of elliptic curves. Graduate texts in Mathematics **151**. Springer, 1994.

[ST1] *J.-P. Serre*, *J. Tate:* Good reduction of abelian varieties. Ann. of Math. (2) **88** (1968), 492–517.

[St2] *W. Stein:* Sage online calculator. http://modular.math.washington.edu/calc/.

[TM] *J. S. Tsuyoshi Miezaki, Hiroshi Nozaki:* On the zeros of Eisenstein series for $\Gamma_0^*(2)$ and $\Gamma_0^*(3)$. arXiv.org **arXiv:math.NT/0607408** (2005).

[Ve] *H. A. Verrill:* Fundamental domain drawer. http://www.math.lsu.edu/verrill/fundomain, Java.

[Wa] *M. Waldschmidt:* Nombres transcendants et groupes algébriques. Astérisque (1987), 218 (French, with English summary), With appendices by Daniel Bertrand and Jean-Pierre Serre.

[Za] *Zagier:* From number theory to physics, Papers from the Meeting on Number Theory and Physics held in Les Houches, March 7–16, 1989, pp. xiv+690.

Abbildungsverzeichnis

Tabellenverzeichnis

Index

Selbstständigkeitserklärung

Ich erkläre, daß ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Ich erkläre mich einverstanden, daß ein Exemplar meiner Diplomarbeit in der Bibliothek des Institutes für Mathematik verbleibt.

Thesenblatt

Wir betrachten die Nullstellen der Hecke-Eigenformen zu der Gruppe $\Gamma(1) = SL_2(\mathbb{Z}) / \{\pm 1\}$ im Fundamentalbereich $\mathcal{F}_{\Gamma(1)}$. Hecke-Eigenformen sind entweder Eisensteinreihen oder Hecke-Spitzenformen. Während über die Nullstellen der Eisensteinreihen bereits vieles bekannt ist, wie zum Beispiel der Satz von Rankin-Swinnerton-Dyer oder der Satz von Kohnen, weiß man wenig über die Nullstellen der Hecke-Spitzenformen.
Spitzenformen haben eine Nullstelle im Punkt $i\infty$ und weitere in den Punkten i und $\rho = \frac{1+i\sqrt{3}}{2}$, deren Vielfachheit nur vom Gewicht der Spitzenform abhängt. Alle weiteren Nullstellen nennen wir die nichttrivialen Nullstellen.

Lemma. *Die j-Werte der Nullstellen der Hecke-Spitzenformen sind algebraisch.*

Aus einem Satz von M. Waldschmidt folgern wir weiter, daß die nichttrivialen Nullstellen imaginärquadratisch oder transzendent sind. Dies ist jedoch mit numerischen Ergebnissen nicht zu entscheiden. Deswegen formen wir das Problem in eine Entscheidung über CM bei elliptischen Kurven um. Eine komplexe Zahl mit algebraischem j-Wert ist transzendent, wenn die elliptische Kurve zu diesem j-Wert keine komplexe Multiplikation besitzt.
Wir benutzen den CM-Test von J. Achter, um eine elliptische Kurve auf komplexe Multiplikation zu testen. Bei diesem wird ein Kandidatenkörper konstruiert, von dem man weiß, das der Endomorphismenring der elliptischen Kurve eine Ordnung im Ring der ganzen Zahlen des Kandidatenkörpers ist. Gelingt es nun, zwei Kandidatenkörper zu konstruieren, bei denen der Durchschnitt der Ringe der ganzen Zahlen dieser Kandidatenkörper nur $\mathbb{Z}$ ist, so hat die elliptische Kurve keine komplexe Multiplikation und die entsprechende Nullstelle ist transzendent.
Dies konnten wir für die nichttrivialen Nullstellen der Hecke-Spitzenformen zu kleinen Gewichten nachweisen.

Satz. *Die nichttrivialen Nullstellen der Hecke-Spitzenformen zur Gruppe* $\Gamma(1)$ *und zu den Gewichten* 24, 28, 30, 32, 34 *und* 38 *sind transzendent.*

Wir wissen, daß die nichttrivialen Nullstellen der Eisensteinreihen immer transzendent sind und so motiviert dieser Satz die Vermutung, daß das auch für Hecke-Spitzenformen, mithin für alle Hecke-Eigenformen gilt.